PROGRAM BOOK

2023 방산기술보호 컨퍼런스

2023 Defense Technology Security Conference

2023. 8. 4.(금) | 소피텔 앰배서더 서울 (잠실)

「기술고도화 대응을 위한 방산기술보호와 수출통제 전략」

Defense Technology Security and Export Control Strategy
in Responding to Technological Advancement

주최 Hosted by 방위사업청 후원 Sponsored by 대한민국 국방부 Ministry of National Defense 외교부 산업통상자원부

목차
Contents

2023 Defense Technology Security Conference 2023 방산기술보호 컨퍼런스

프로그램

시 간	프로그램
09:30 - 10:00	등 록
10:00 - 10:10	개회사 | **권영철** 방위사업청 국방기술보호국장
10:10 - 10:30	기념사진 촬영 / Coffee Break
10:30 - 12:00	**SESSION 1** 신기술 출현에 따른 국제적 정책 동향
	Back to Basics: 효과적인 기술 보안 프로그램의 핵심 요소 | **Mr. Scott Nelson** 미국 방산기술보호본부 동북아 팀장
	국내외 안보 강화를 위한 방산 무역 통제 | **Mr. Phillip R. Davis II** 미국 국무부 지역안보무기이전과 외무관
	기술적 우위의 유지 방안 - 이탈리아의 골든 파워(Golden Power) 입법 | **Lt.Col. Baldassare Bologna** 이탈리아 국방사무/국가군수국 과장
	신기술 발전과 수출통제 및 규범 정립 | **이혜진** 외교부 수출통제·제재담당관실 외무서기관
	Q&A
12:00 - 13:30	공식 오찬
13:30 - 14:45	**SESSION 2** 첨단 방위산업의 발전과 수출, 그리고 기술보호
	한국 방위산업기술 보호·수출통제 정책 및 법령 소개 | **김주철** 방위사업청 기술보호과장
	방산기술수출, 단계별 주요 이슈 | **이상진** 김·장 법률사무소 변호사
	방산기술보호를 위한 기술적 대책 및 절차 | **장희진** 국방과학연구소 국방첨단과학기술연구원 사이버기술센터팀장
	국제 수출통제제도 경향과 기술보호 측면의 시사점 | **류세희** 전략물자관리원 국제체제팀장
	Q&A
14:45 - 15:00	휴식 / Coffee Break
15:00 - 16:15	**SESSION 3** 기술의 발전과 앞으로의 과제
	K-국방을 위한 미래도전기술 | **박진호** 동국대학교 국방안전연구센터장
	방산기술보호 등급분류 및 조치를 위한 평가방법 | **정석재** 광운대학교 방위사업학과 교수
	Post K-방산을 위한 방산기술보호 정책 방향 | **심의칠** 한화에어로스페이스 경영지원실보안팀 차장
	양자암호통신 기술 및 동향 | **신정환** KT 인프라DX연구소 융합기술원 팀장
	Q&A
16:15 - 16:20	폐회사

Program

TIME	PROGRAM
09:30 - 10:00	Check-In
10:00 - 10:10	Opening Remarks | **Mr. Yeongcheol Kwon** Director General, Defense Technology Policy and Security Bureau, DAPA
10:10 - 10:30	Group Photo / Coffee Break
10:30 - 12:00	**SESSION 1** International Policy Trends in Response to Emerging Technologies
	Back to Basics: Essentials of an Effective Technological Security Program | **Mr. Scott Nelson** Deputy Chief, Regional Engagement Division, DTSA, U.S.
	Controlling Defense Trade for Greater National and International Security | **Mr. Phillip R. Davis II** Foreign Affairs Officer, RSAT, U.S. Department of State, U.S.
	Maintaining Technology Advantage - Italian Golden Power Legislation | **Lt.Col. Baldassare Bologna** Section Leader, Secretariat General of Defence/ National Armaments Directorate, Italy
	Establishment of Export Control and Norms in Response to the Advancement of New Technologies | **Ms. Hyejin Lee** Deputy Director, Export Control and Sanctions Division, Ministry of Foreign Affairs
	Q&A
12:00 - 13:30	Luncheon
13:30 - 14:45	**SESSION 2** Advancement, Export, and Technology Security of Cutting-Edge Defense Industries
	Defense Technology Security & Export Control Policy of ROK | **Mr. Joochul Kim** Director, Defense Technology Security Division, DAPA
	Defense Technology Export and Key Issues | **Mr. Sangjin Lee** Attorney at law, Kim & Chang
	Technical Measures and Procedures for Defense Technology Protection | **Ms. Heejin Jang** Team Leader, Advanced Defense S&T Research Institute -Cyber Technology Center, ADD
	Trends in International Export Control Regimes and Implications for Technology Protection | **Mr. Sehee Ryu** Director, Multilateral Export Controls Team, Policy Support Department, KOSTI
	Q&A
14:45 - 15:00	Coffee Break
15:00 - 16:15	**SESSION 3** Technological Advancements and Future Challenges
	Future Challenges Technology for K-Defense | **Prof. Jinho Park** Director, Defense Security Research Center, Dongguk University
	Assessment Method for Classification and Measures in Defense Technology Security | **Prof. Sukjae Jeong** Professor, Department of Defense Acquisition Program, KwangWoon University
	Defense Technology Protection Direction For Post K-Defense | **Mr. Euichil Sim** Deputy Senior Manager, Hanwha Aerospace Co., Ltd.
	Quantum Key Distribution Technology and Trends | **Mr. Jeonghwan Shin** Team Leader, Infra DX Lab, Institute of Convergence Technology, KT Coporation
	Q&A
16:15 - 16:20	Closing

연사소개 | Speaker

SESSION 1 신기술 출현에 따른 국제적 정책 동향
International Policy Trends in Response to Emerging Technologies

미국 방산기술보호본부 동북아 팀장 | **Mr. Scott Nelson**
Deputy Chief, Regional Engagement Division, DTSA, U.S.
Mr. Scott Nelson

Back to Basics: 효과적인 기술 보안 프로그램의 핵심 요소
Back to Basics: Essentials of an Effective Technological Security Program

· 2006~2010	미 공군성 국제협력 부차관 관할 대외공개 및 무기 부서 Foreign Disclosure and Weapons Division for the Deputy Undersecretary of the Air Force, International Affairs
· 2010~2013	DCSA 최종용도 모니터링 프로그램 매니저 End-Use Monitoring Program Manager for U.S. Central Command, DSCA
· 2013~2016	미국 국방안보협력국(DSCA) 무기체계 애널리스트 Weapon Systems Analyst, Defense Security Coorperation Agency(DSCA)
· 2016~2020	DTSA 동북아 및 남아메리카 지역정책 선임 고문 Senior Regional Policy Advisor for Northeast Asia and South America, DTSA
· Present	미국 방산기술보호본부(DTSA) 동북아 팀장 Deputy Chief, Regional Engagement Division, Defense Technology Security Administration(DTSA)

미국 국무부 지역안보무기이전과 외무관 | **Mr. Phillip R. Davis II**
Foreign Affairs Officer, RSAT, U.S. Department of State, U.S.
Mr. Phillip R. Davis II

국내외 안보 강화를 위한 방산 무역 통제
Controlling Defense Trade for Greater National and International Security

· 2018	미 연방 재난관리청 입법담당관 Legislative Affairs Specialist at Federal Emergency Management Administration
· 2020~2022	프레지던트 매니지먼트 펠로우(PMF) Presidential Management Fellow (PMF)
· 2022~	미 국무부 정치군사국 지역안보무기이전과 외무관, 동아시아태평양 포트폴리오 매니저 Foreign Affairs Officer for the U.S. Department of State, Bureau of Political-Military Affairs, Regional Security and Arms Transfers, East Asian Pacific Portfolio Manager

이탈리아 국방사무/국가군수국 과장 I **Lt.Col. Baldassare Bologna**

Section Leader, Secretariat General of Defence/National Armaments Directorate, Italy

Lt.Col. Baldassare Bologna

기술적 우위의 유지 방안 - 이탈리아의 골든 파워(Golden Power) 입법
Maintaining Technology Advantage - Italian Golden Power Legislation

· 2004~2008	ITALFOR BOSNIA 사령관 법률고문 ITALFOR BOSNIA – Commander Legal Advisor
· 2014~2018	이탈리아 육군일반참모 법률사무국 국제협정 과장 IT GENERAL ARMY STAFF – Legal Office - International Agreements Section Leader
· 2016~2018~2021	코소보군 사령관 법률고문 KOSOVO FORCE – Commander Legal Advisor
· 2020~	이탈리아 국방사무/국가군수국 국제협정 법률고문 및 과장 General Secretariat of Defence/ National Armaments Directorate -International Agreements Legal Advisor - Section Leader

외교부 수출통제·제재담당관실 외무서기관 I **이혜진**

Deputy Director, Export Control and Sanctions Division, Ministry of Foreign Affairs

Ms. Hyejin Lee

신기술 발전과 수출통제 및 규범 정립
Establishment of Export Control and Norms in Response to the Advancement of New Technologies

· 2016~2018	주유엔대표부 1등/2등서기관 First/Second Secretary, ROK Mission to the United Nations, New York
· 2018~2020	주마다가스카르대사관 참사관 Counselor, ROK Embassy to Madagascar
· 2020~2022	주중국대사관 1등서기관 First Secretary, ROK Embassy to the People's Republic of China
· 2022~	외교부 군축비확산담당관실 외무서기관 Deputy Director, Disarmament and Nonproliferation Division
· 2023~	외교부 수출통제·제재담당관실 외무서기관 Deputy Director, Export Control and Sanctions Division

연사소개 | Speaker

SESSION 2 첨단 방위산업의 발전과 수출, 그리고 기술보호
Advancement, Export, and Technology Security of Cutting-Edge Defense Industries

방위사업청 기술보호과장 | **김주철**
Director, Defense Technology Security Division, DAPA
Mr. Joochul Kim

한국 방위산업기술 보호·수출통제 정책 및 법령 소개
Defense Technology Security & Export Control Policy of ROK

- 2019~2020 방위산업진흥국 원가관리과 총괄
  Deputy Director, Cost Management Division
- 2020~2021 조직인사담당관 공무원인사팀장
  Director, Organization and Personnel Management Division
- 2022 감시전자사업부 피아식별장비사업팀장
  Director, Identification Friend or Foe Equipment Program Team
- 2022~ 국방기술보호국 기술보호과장
  Director, Defense Technology Security Division

김·장 법률사무소 변호사 | **이상진**
Attorney at law, Kim & Chang
Mr. Sangjin Lee

방산기술수출, 단계별 주요 이슈
Defense Technology Export and Key Issues

- 2009~ 김·장 법률사무소
  Kim & Chang
- 2019~ 방위사업청 방산수출심의위원회 위원
  Deliberative Committee Member for Defense Export, DAPA
- 2020~ 방위사업청 국고보조금지원대상자선정위원회 위원
  Member, Committee on Selection of Persons Eligible for Government Subsidies, DAPA
- 2020~ 방위사업청 실태조사심의위원회 위원
  Deliberative Committee Member for Defense Technology Protection Status Investigation, Defense Acquisition Program Administration (DAPA)
- 2023~ 국방부 방위산업기술보호위원회 위원
  Deliberative Committee Member for Defense Technology Protection, Ministry of National Defense

국방과학연구소 국방첨단과학기술연구원 사이버기술센터팀장 I **장희진**
Team Leader, Advanced Defense S&T Research Institute - Cyber Technology Center, ADD
Ms. Heejin Jang

방산기술보호를 위한 기술적 대책 및 절차
Technical Measures and Procedures for Defense Technology Protection

- **2004~2014** 국방과학연구소 2기술연구본부 선임연구원
  Senior Researcher, 2nd R&D Institute, ADD
- **2015~** 국방과학연구소 국방첨단과학기술연구원 사이버기술센터 책임연구원
  Principal Researcher, Advanced Defense S&T Research Institute- Cyber Technology Center, ADD
- **2021~** 국방과학연구소 국방첨단과학기술연구원 사이버기술센터 팀장
  Team Leader, Advanced Defense S&T Research Institute- Cyber Technology Center, ADD

전략물자관리원 국제체제팀장 I **류세희**
Director, Multilateral Export Controls Team, Policy Support Department, KOSTI
Mr. Sehee Ryu

국제 수출통제제도 경향과 기술보호 측면의 시사점
Trends in International Export Control Regimes and Implications for Technology Protection

- **2011~2016** 전략물자관리원 품목분석팀 책임연구원
  Principal Researcher of Controlled Items Classification Team, Korean Security Agency of Trade and Industry
- **2017~2018** 전략물자관리원 심사판정실장
  Director of Controlled Items Classification Team, Korean Security Agency of Trade and Industry
- **2019~2021** 전략물자관리원 제재분석실장
  Director of Sanction Analysis Team, Korean Security Agency of Trade and Industry
- **2022~** 전략물자관리원 국제체제팀장
  Director of Multilateral Export Controls Team, Korean Security Agency of Trade and Industry

연사소개 | Speaker

SESSION 3 기술의 발전과 앞으로의 과제
Technological Advancements and Future Challenges

동국대학교 국방안전연구센터장 | **박진호**
Director, Defense Security Research Center, Dongguk University
Prof. Jinho Park

K-국방을 위한 미래도전기술
Future Challenges Technology for K-Defense

· Present	동국대학교 국방안전연구센터 센터장 Director of the center, Defense Security Research Center, Dongguk University
	동국대학교 AI소프트웨어융합학부 교수 Professor, Division of AI Software Convergence, Dongguk University

광운대학교 방위사업학과 교수 | **정석재**
Professor, Department of Defense Acquisition Program, KwangWoon University
Prof. Sukjae Jeong

방산기술보호 등급분류 및 조치를 위한 평가방법
Assessment Method for Classification and Measures in Defense Technology Security

· 2013~	광운대학교 대학원 방위사업학과 교수 Prof. of Defense Acquisition Program at KwangWoon Univ. Graduate School
· 2021~	방위사업청 정책연구심의위원회 Policy Research Review Committee at Defense Acquisition Program Administration
· 2022~	방위사업청 국제경쟁력강화지원사업 관리위원회 International Competitiveness Support Project Management Committee at Defense Acquisition Program Administration
· 2023~	방위사업청 주관 계약학과 사업 총괄 General Manager of Contract Department Project organized by the Defense Acquisition Program Administration

한화에어로스페이스 경영지원실보안팀 차장 I **심의칠**

Deputy Senior Manager, Hanwha Aerospace Co., Ltd

Mr. Euichil Sim

Post K-방산을 위한 방산기술보호 정책 방향
Defense Technology Protection Direction For Post K-defense

- **2016~2018** 대한항공 항공우주사업본부 전략기획실
  Koreanair Aerospace Business Division Strategic & Planning Team
- **2019~2022** 대한항공 항공우주사업본부 사업영업부 무인기 수출전략담당
  Koreanair Aerospace Business Division UAV Export Strategic Team
- **2020~2022** 방산보안협의회 중앙회 사무총장
  Secretary General of Defense Industry Technology Council
- **2021~** 서울지역방산보안협의회 사무국장
  Executive Director of Defense Industry Technology Council of Seoul
- **2022~** 한화에어로스페이스 경영지원실 보안팀
  Hanwha Aerospace Manage Support Office Security Team

KT 인프라DX연구소 융합기술원 팀장 I **신정환**

Team Leader, Infra DX Lab, Institute of Convergence Technology, KT Coporation

Mr. Jeonghwan Shin

양자암호통신 기술 및 동향
Quantum Key Distribution Technology and Trends

- **2013~2015** 양자정보과학기술센터(University of Southern California) 연구원
  Center for Quantum Information Science and Technology(University of Southern California), Visiting Scholar
- **2016~2017** 고려대 스마트양자통신센터 연구원
  Research Fellow, Smart quantum communication center, Korea University
- **2017~** KT 융합기술원 팀장
  Team leader, Institute of Convergence Technology, KT

2023 Defense Technology Security Conference 2023 방산기술보호 컨퍼런스

SESSION 1

신기술 출현에 따른 국제적 정책 동향

International Policy Trends in Response to Emerging Technologies

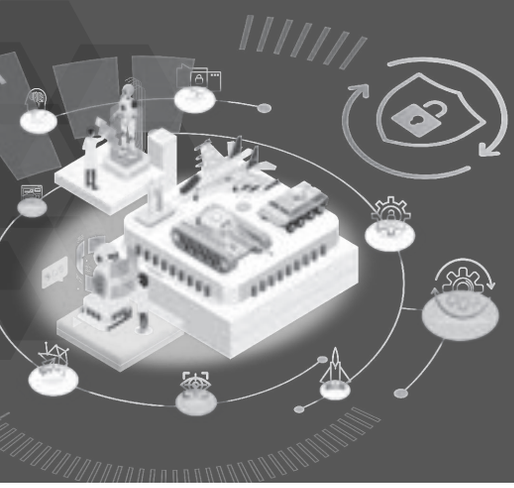
---

Back to Basics: 효과적인 기술 보안 프로그램의 핵심 요소
Back to Basics: Essentials of an Effective Technological Security Program

국내외 안보 강화를 위한 방산 무역 통제
Controlling Defense Trade for Greater National and International Security

기술적 우위의 유지 방안 - 이탈리아의 골든 파워(Golden Power) 입법
Maintaining Technology Advantage - Italian Golden Power Legislation

신기술 발전과 수출통제 및 규범 정립
Establishment of Export Control and Norms in Response to the Advancement of New Technologies



주제발표 1.

Back to Basics: 효과적인 기술 보안 프로그램의 핵심 요소

Back to Basics: Essentials of an Effective Technological Security Program

미국 방산기술보호본부 동북아 팀장 I **Mr. Scott Nelson**
Deputy Chief, Regional Engagement Division, DTSA, U.S.
Mr. Scott Nelson

UNCLASSIFIED

방산기술보호본부

"경쟁력 확보"

DEFENSE TECHNOLOGY SECURITY ADMINISTRATION
ENSURING THE EDGE

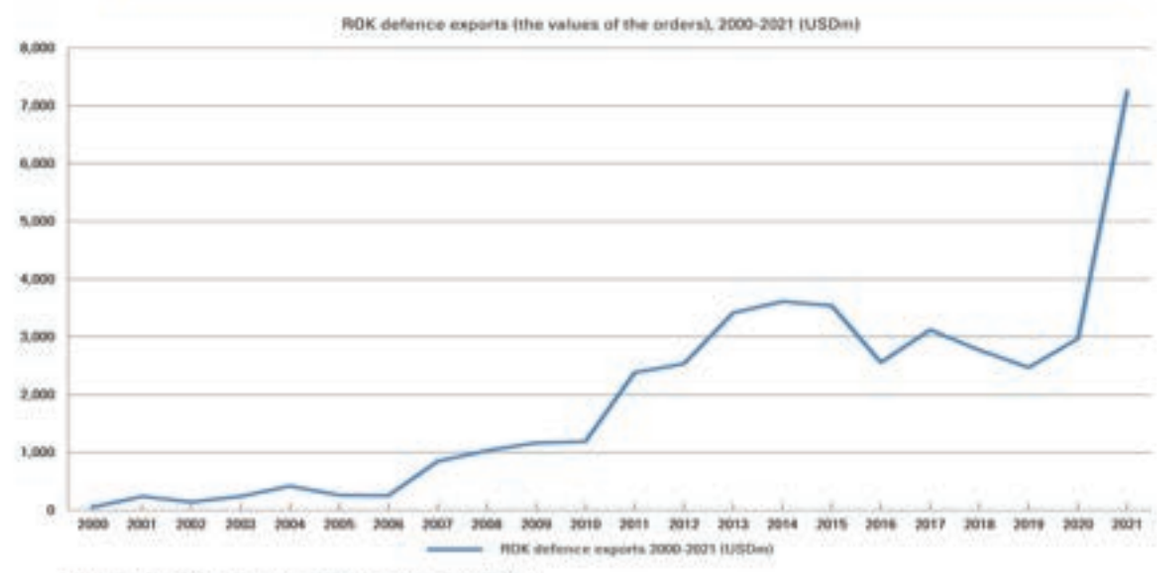
제7차 국제 방산기술보호 컨퍼런스
2023년 8월

Mr. Scott Nelson
동북아 팀장

UNCLASSIFIED

2000-2021 대한민국 방위산업 수출

POLICY



Source: Republic of Korea Defense Acquisition Program Administration (DAPA)

UNCLASSIFIED


UNCLASSIFIED
2000-2022 대한민국 방위산업 수출
POLICY
2022
UNCLASSIFIED


UNCLASSIFIED
기술보호가 중요한 이유
POLICY
•전투원
•비용
•시간
•우방국 및 파트너
UNCLASSIFIED

UNCLASSIFIED

시나리오 제시

다음 중 한 개는 다른 것이다.

- 명시된 목적은 정보 전달
- 파트너들이 목적 혹은 동기에 관해 투명하지 않을 수도 있음

UNCLASSIFIED

UNCLASSIFIED

더이상 '스파이 대 스파이' 구도가 아님

과거	현재
▶ 정보 요원 ▶ 정보 요원들에 의해 고용된 인원	▶ 정보 요원 ▶ 정보 요원들에 의해 고용된 인원 ▶ *해커* ▶ *사업가* ▶ *학계* ▶ *연구자* ▶ *외교관* ▶ *가치 있는 대상에 접근할 수 있는 모든 사람*

UNCLASSIFIED

UNCLASSIFIED

기술 획득 방법

- 각국에서 다양한 수단을 통해 군사 및 이중용도 기술 · 장비, 특수 역량 · 기능과 여타 민감한 정보(기밀 정보 포함)를 얻고자 함
  - 해외직접투자(합병, 인수, 합작 투자)
  - 기술 수출
- 민감한 정보에 접근하는 다른 수단
  - 협력 연구 및 개발 프로그램(잠재적으로 군사 분야 응용이 가능한 신흥 기술 협력)
  - 과학 교류
  - 불법적 수단(절도, 착취)

UNCLASSIFIED

UNCLASSIFIED

오늘날 세계 시장의 현실

최첨단 기술
이중용도 기술

무역의 세계화

이러한 역학관계는 비확산 및 기술 안보를 위협하는 도전 과제를 야기함

- 최종용도 검증
- 전용 방지
- 민감한 상업 정보 이전을 차단하기 위한 높은 요구수준
- 상업적 혁신은 방위 혁신에 직결됨
- 학술적 · 상업적 연구개발의 세계적 공유
- 상호연결된 공급망으로 인해 의존성과 취약성 발달

UNCLASSIFIED


UNCLASSIFIED
정보 및 기술 보안의 축
POLICY
PROTECT
WHOLE of GOVERNMENT
LEGISLATION
NATIONAL COLLABORATION
CAPABILITY
INTENT
CHECKS & BALANCES
VARYING INTERESTS
STATUTORY AUTHORITIES
COMPLIANCE SYSTEMS
ENFORCEMENT
INFLUENCERS
- DEFENSE INDUSTRY
- TRADE ASSOCIATIONS
- THINK TANKS
- ACADEMIA
UNCLASSIFIED


UNCLASSIFIED
물리적 보안
•보안 구역 접근 통제
•컨테이너 접근 통제
SECURITY CLEARANCE REQUIRED
TO ENTER THIS AREA!
UNCLASSIFIED


UNCLASSIFIED
정보 보안
Classified Military Information (CMI)
• Application of proper handling, marking, storage, dissemination, and destruction requirements for TS, S, and C
• Application of Security Classification Guide(s)
• Application of Program Protection Plan(s)
• Application of distribution statements
• Application of work performed on classified contracts
• Application of policy regarding security violations and weaknesses
TOP SECRET
TOP SECRET
SECRET
CONFIDENTIAL
UNCLASSIFIED


UNCLASSIFIED
작전 보안
•작전 보안(OPSEC)은 적군이 악용할 수 있는 정보를 보호하는 절차이다.
UNCLASSIFIED

UNCLASSIFIED

국가안보 전략

- 오늘날 지정학적 경쟁과 국가 안보, 경제, 민주주의의 미래에는 기술이 중심적임
- 핵심 및 신흥 기술이 각국 경제를 개편하고, 군대를 변혁시키고, 전 세계를 재구성할 준비가 되어 있음

- 세계 안보 및 경제를 변화시킬 근본적 기술을 개발하고 활용하기 위한 경쟁이 심화되는 상황

- '혁신'을 19회 언급함
- '현대 산업 및 혁신 전략 시행'이라는 제목의 장을 포함함
- '기술'이라는 제목의 장을 포함함

미국은 이러한 기술이 미국 국민 및 뜻이 일치하는 민주국가의 안보, 번영, 가치를 보장하는 세계를 위한 굳건한 의지를 지니고 있습니다.

UNCLASSIFIED

기술 이전에서 미 국방부의 역할

무기수출통제법
(탄약목록)
대외원조법
(G2G)

수출관리법
(이중용도 및 일부 탄약 물품)
미 특허청
(비밀 유지 명령)

원자력법
("특수 핵물질")

해외 투자 및 보안법
(해외 기업에 의한 미국 기업 인수)

원자력법
(핵 장비 · 물질)

UNCLASSIFIED

UNCLASSIFIED

국방부 검토국

미국 군대:

- 미 해군 및 해병대 – 해군 국제 프로그램 사무소(Navy-IPO)
- 미 공군 – 대외공개국 국제사무국장(SAF/IAPD)
- 미 육군 – 방산 수출·협력 담당 육군 부차관보(DASA(DE&C))

국방부:

- 국방안보협력국(DSCA)
- 합동 참모 본부(JCS/J5)
- 정책 담당 국장(USDP)
- 획득·유지 담당 국장(USD A&S)
- 연구·공학 담당 국장(USD R&E)
- 국가안보국(NSA)

- **여타 국방부 기관(국방정보국, 국방정보시스템국, 조달청, 국가지리정보국, 국가정찰국 등)**

UNCLASSIFIED

UNCLASSIFIED

핵심기술에 관한 법적 개혁

- 2019년 국방 수권 법안으로 인해 전략적 경쟁자들의 핵심 기술 모색에 대응할 수 있는 새로운 당국이 마련됨
  - *수출통제개혁법(ECRA)*
  - *외국인투자위험심사현대화법(FIRRMA)*
- 미국 핵심기술이 확보되는 경로를 포착하기 위해 수출통제와 해외직접투자 심사가 결합됨
- ECRA에 따른 요건 중 하나는 수출통제와 해외 투자 심사 모두를 위해 핵심 및 신흥 기술을 식별하는 것임

JOHN S. McCAIN
NATIONAL DEFENSE AUTHORIZATION ACT
FOR FISCAL YEAR 2019

CONFERENCE REPORT

H.R. 5515

목표는 다자간 수출통제체제 내 핵심 및 신흥 기술을 식별하고 다자적으로 합의된 통제 장치를 수립하는 것

UNCLASSIFIED

국가 산업 안보 프로그램

- 미승인 기밀정보 접근 탐지 및 억제
- 적군 및 미국 기밀정보를 표적으로 삼는 여타 세력의 위협에 대응

"...국가 산업 안보 프로그램은 기밀정보를 보호하고 국가의 경제 및 기술적 이해관계를 보존하기 위한 단일적이며 통합되었고 응집력 있는 산업 안보 프로그램으로서 작용할 것"

1993년 1월 8일자 12829호 행정명령

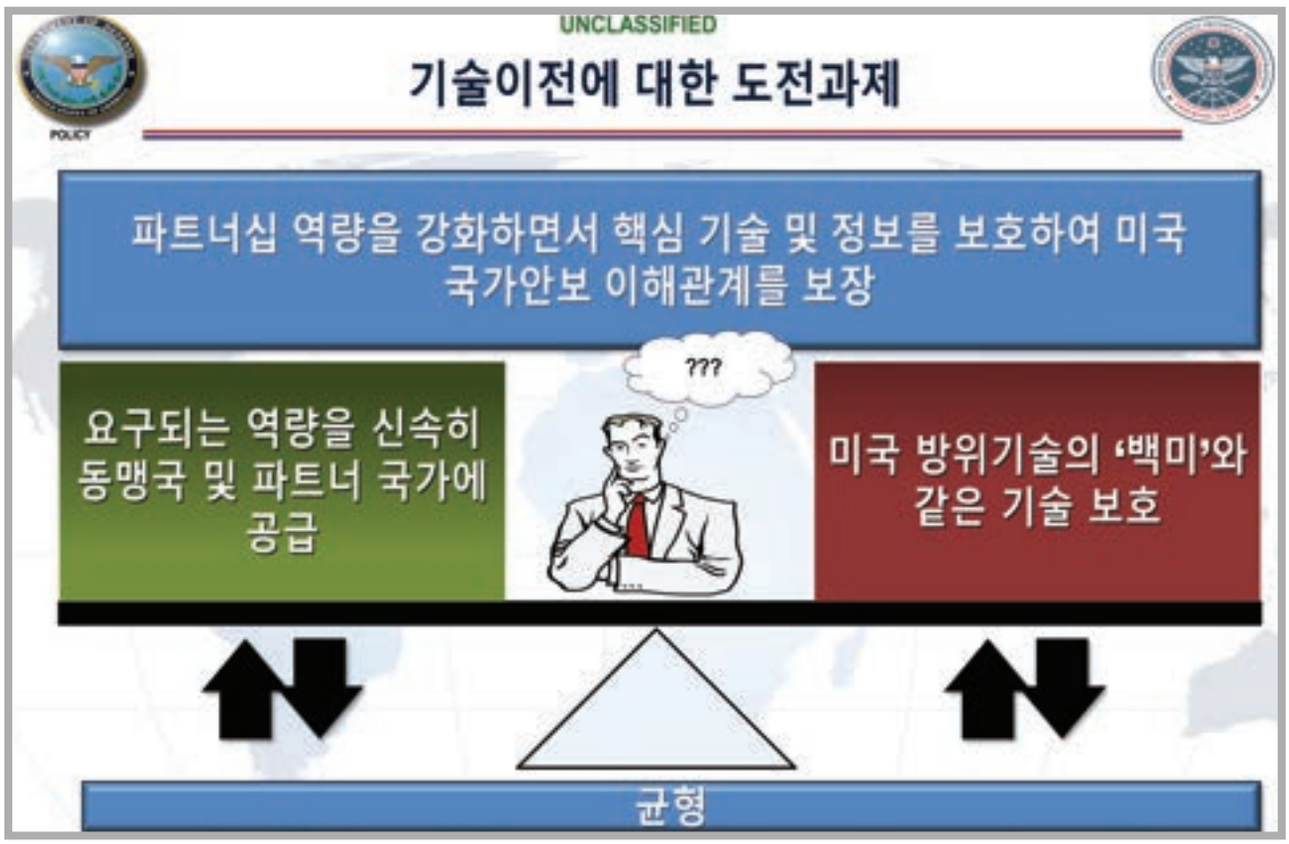
UNCLASSIFIED

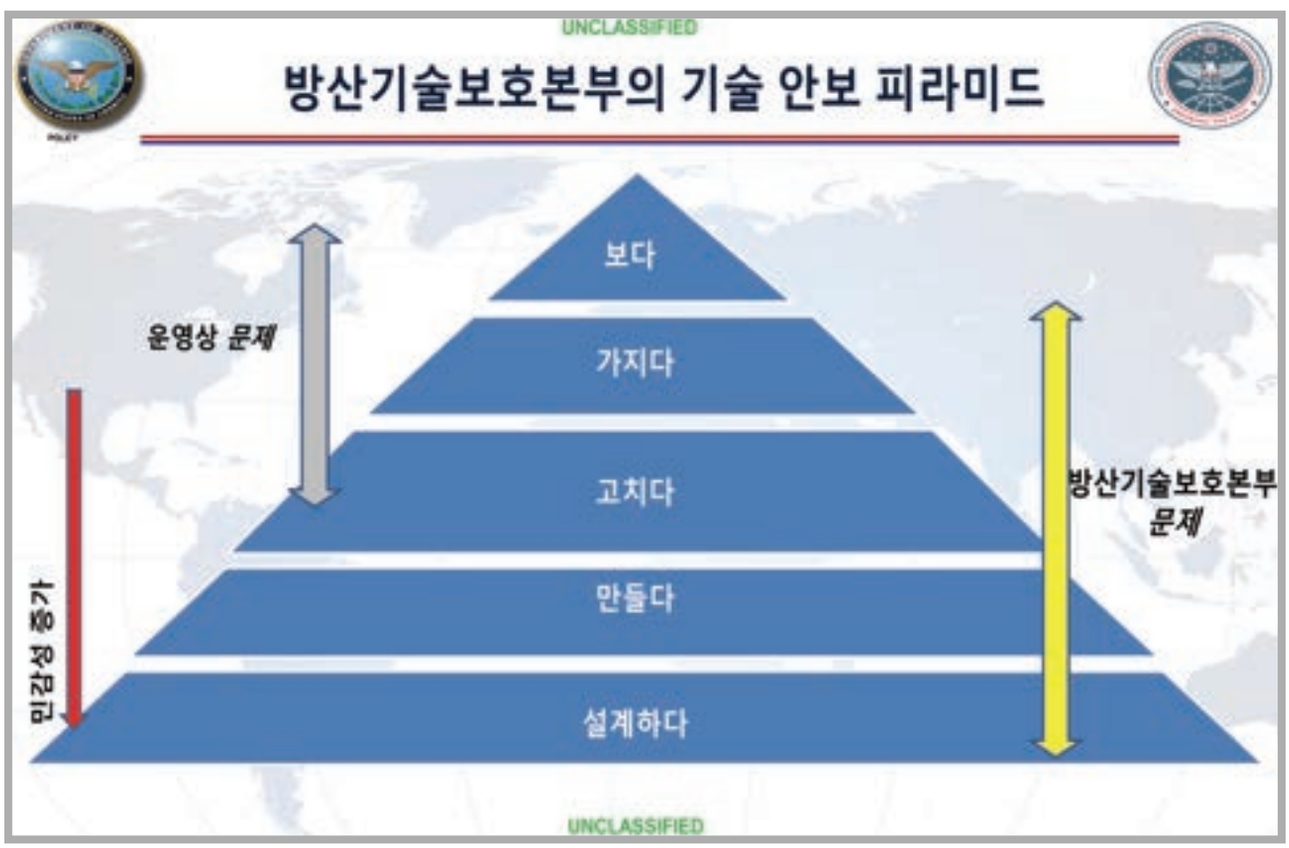
UNCLASSIFIED

방위기술 안보

- 미국 방위기술의 보호 및 안보는 미국 방위기술 공급에 내재되어 있음
- 기초 합의 협정, 다자적 수출통제체제, 최종용도 검사 프로그램은 핵심적인 보증을 제공함
- 파트너 국가 간의 방위기술 보호는 제로섬 게임과 같음

UNCLASSIFIED


UNCLASSIFIED
기술이전에 대한 도전과제
파트너십 역량을 강화하면서 핵심 기술 및 정보를 보호하여 미국 국가안보 이해관계를 보장
요구되는 역량을 신속히 동맹국 및 파트너 국가에 공급
???
미국 방위기술의 '백미'와 같은 기술 보호
균형


UNCLASSIFIED
방산기술보호본부의 기술 안보 피라미드
보다
가지다
고치다
만들다
설계하다
운영상 문제
민감성 증가
방산기술보호본부 문제
UNCLASSIFIED

UNCLASSIFIED

국방부 기술이전 검토

- **국가안보에 미치는 영향을 평가할 때 고려되는 요소:**

지역, 국가, 기술	상호운용성
기술 수준	국제 합의
최종용도 및 최종사용자 이력	해외 가용성
군사작전 영향	기밀 데이터 이전

UNCLASSIFIED

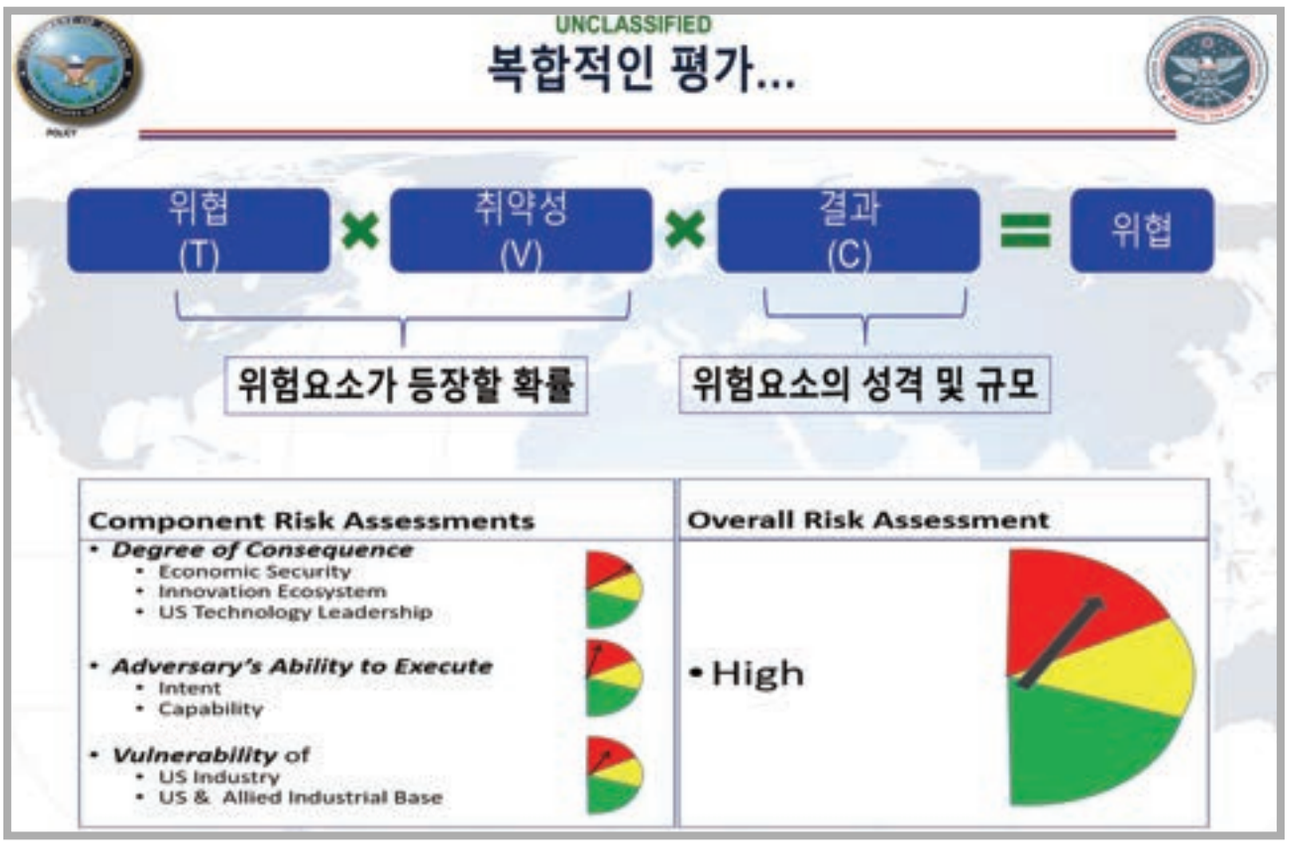
UNCLASSIFIED

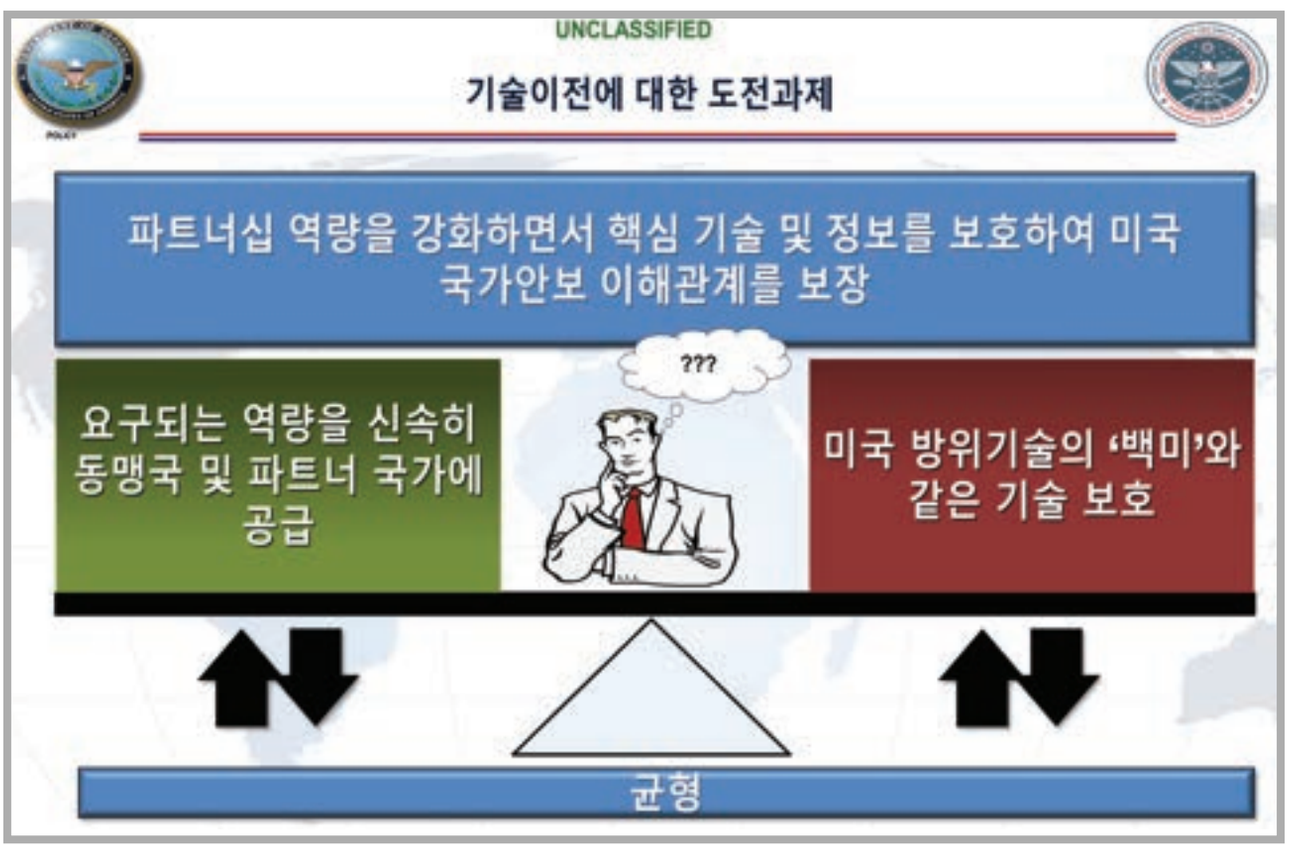
분석

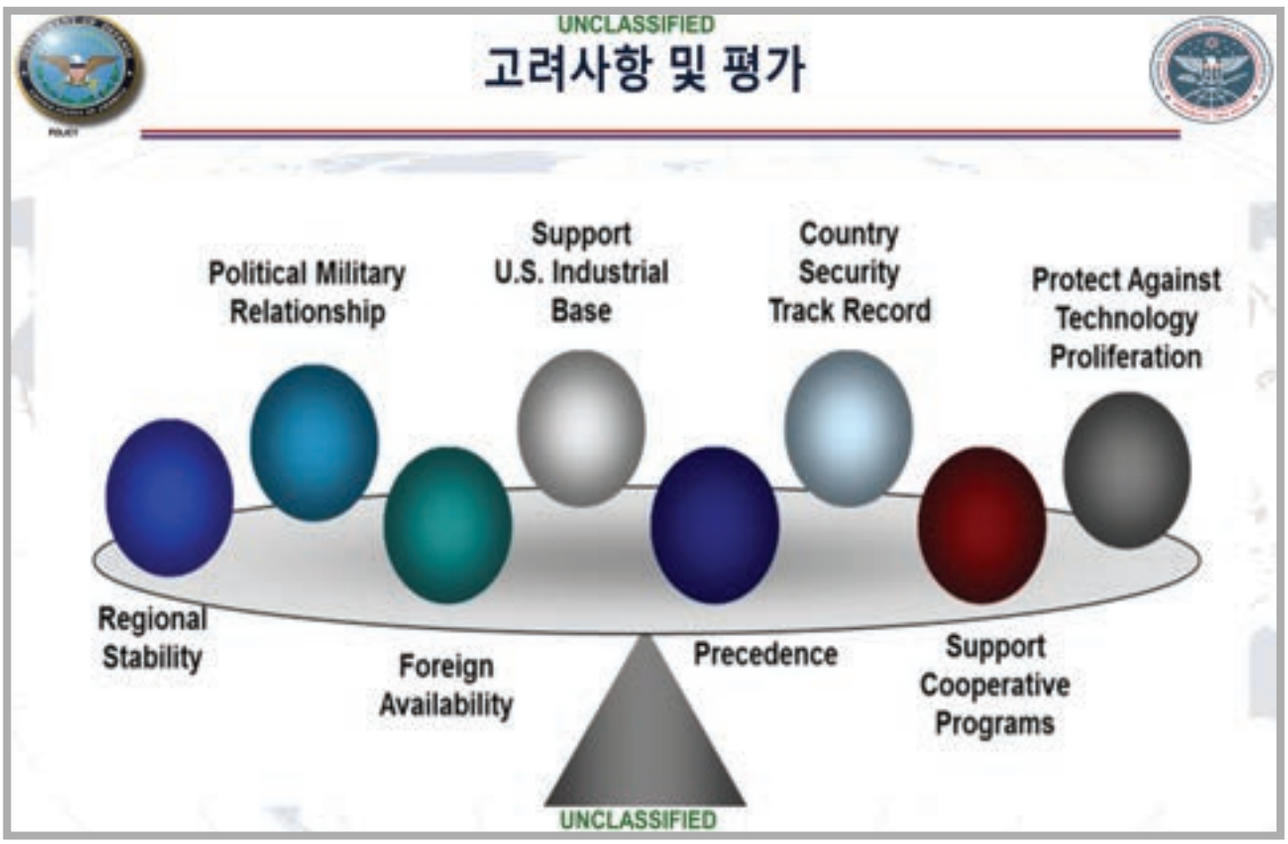
- 기술의 최종사용자, 그 활동과 관계에 초점을 맞춘 분석

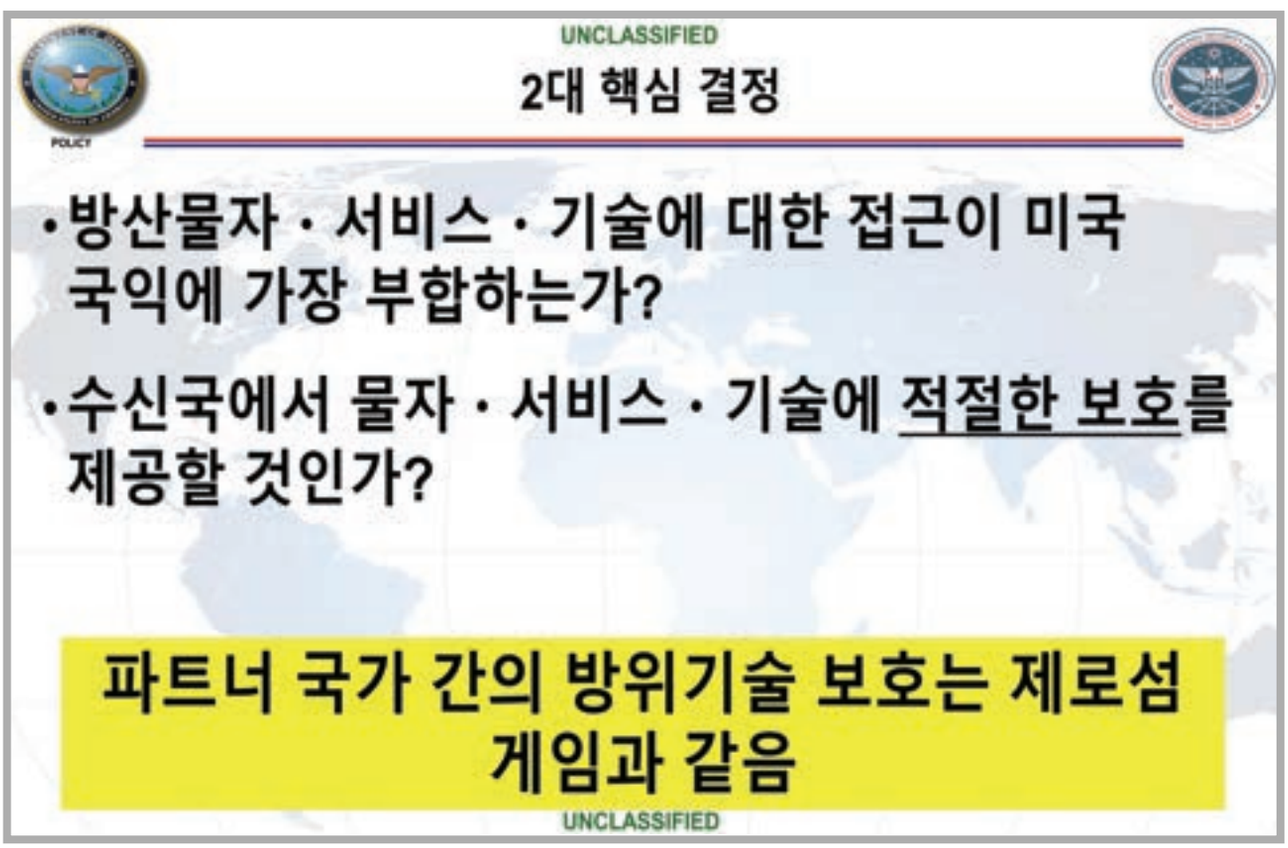
- **개인** 개인 행실 이력
  제3자와의 사업관계
- **기업** 기업, 소유권, 관계 이력
- **국가** 본부 위치, 현장 사무소, 자금 흐름

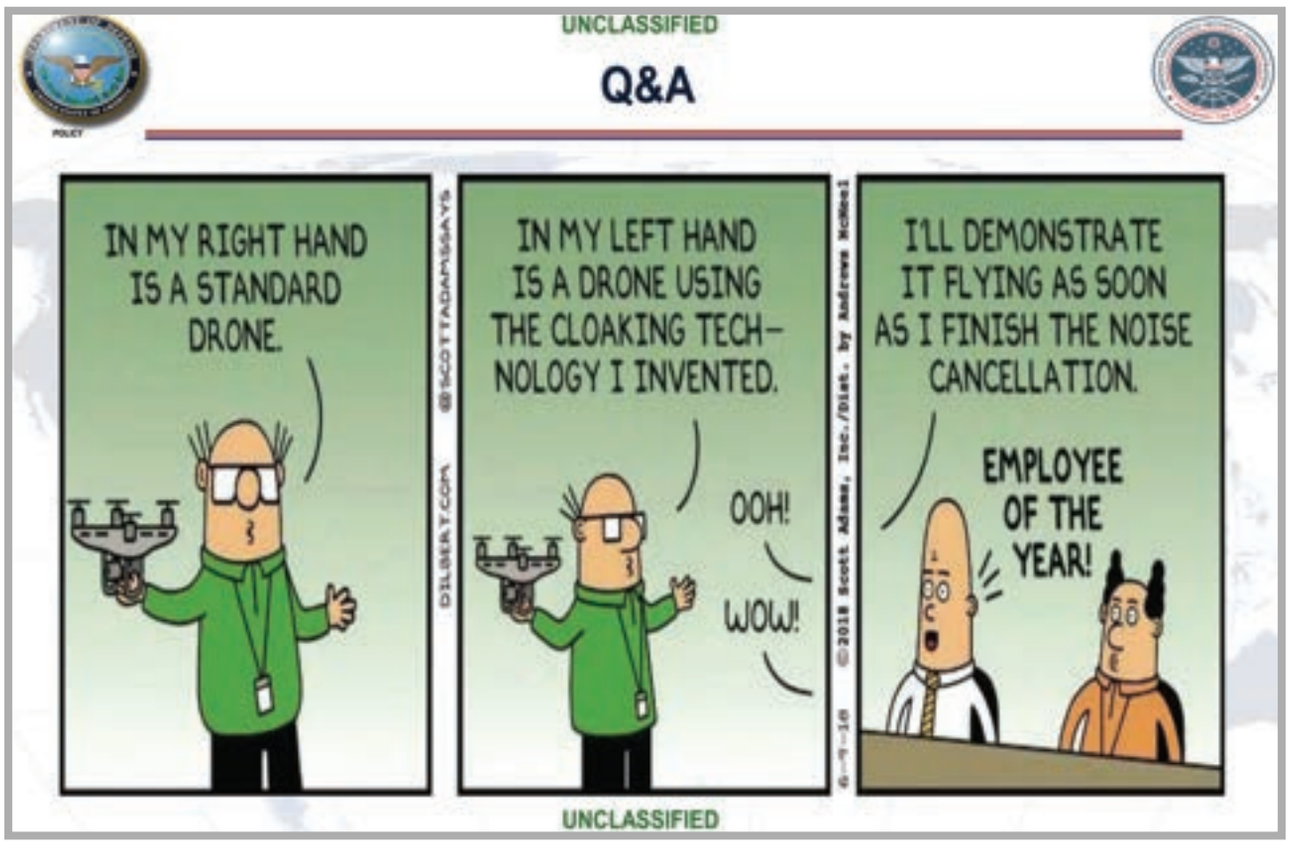
UNCLASSIFIED


UNCLASSIFIED
복합적인 평가...
위협 (T)
취약성 (V)
결과 (C)
위협
위험요소가 등장할 확률
위험요소의 성격 및 규모
Component Risk Assessments
Degree of Consequence
Economic Security
Innovation Ecosystem
US Technology Leadership
Adversary's Ability to Execute
Intent
Capability
Vulnerability of
US Industry
US & Allied Industrial Base
Overall Risk Assessment
• High


UNCLASSIFIED
기술이전에 대한 도전과제
파트너십 역량을 강화하면서 핵심 기술 및 정보를 보호하여 미국 국가안보 이해관계를 보장
요구되는 역량을 신속히 동맹국 및 파트너 국가에 공급
???
미국 방위기술의 '백미'와 같은 기술 보호
균형


UNCLASSIFIED
고려사항 및 평가
Political Military Relationship
Support U.S. Industrial Base
Country Security Track Record
Protect Against Technology Proliferation
Regional Stability
Foreign Availability
Precedence
Support Cooperative Programs
UNCLASSIFIED


UNCLASSIFIED
2대 핵심 결정
• 방산물자 · 서비스 · 기술에 대한 접근이 미국 국익에 가장 부합하는가?
• 수신국에서 물자 · 서비스 · 기술에 적절한 보호를 제공할 것인가?
파트너 국가 간의 방위기술 보호는 제로섬 게임과 같음
UNCLASSIFIED


UNCLASSIFIED
Q&A
IN MY RIGHT HAND IS A STANDARD DRONE.
IN MY LEFT HAND IS A DRONE USING THE CLOAKING TECH-NOLOGY I INVENTED.
OOH!
WOW!
I'LL DEMONSTRATE IT FLYING AS SOON AS I FINISH THE NOISE CANCELLATION.
EMPLOYEE OF THE YEAR!
DILBERT.COM @SCOTTADAMSSAYS
©2018 Scott Adams, Inc./Dist. by Andrews McMeel
UNCLASSIFIED

UNCLASSIFIED

Defense Technology Security Administration

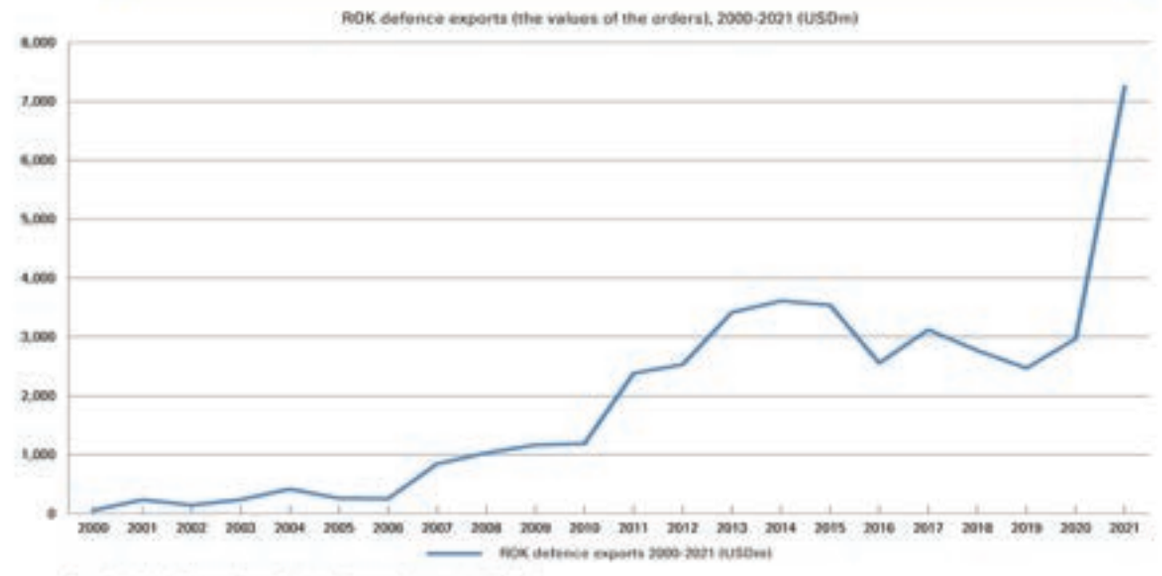
"ENSURING THE EDGE"

7th International Defense Technology Security Conference
August 2023

Mr. Scott Nelson
Deputy Chief, Regional Engagement Division

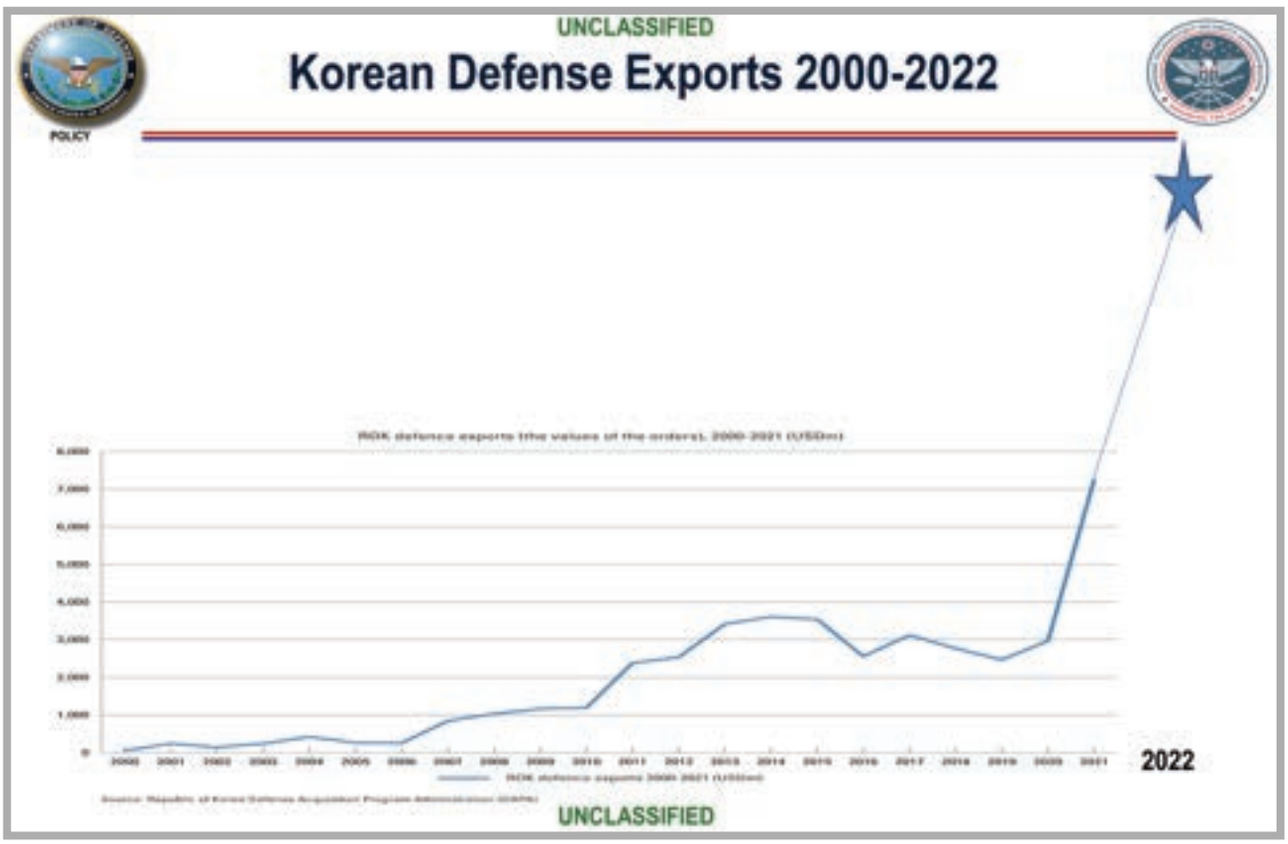
UNCLASSIFIED

Korean Defense Exports 2000-2021



Source: Republic of Korea Defense Acquisition Program Administration (DAPA)

UNCLASSIFIED


UNCLASSIFIED
Korean Defense Exports 2000-2022
POLICY
2022
UNCLASSIFIED


UNCLASSIFIED
Why Technology Security?
POLICY
•Warfighter
•Cost
•Time
•Allies & Partners
UNCLASSIFIED


UNCLASSIFIED
Consider a Scenario...
One of these is not like the other
• Explicit goal is to transfer information
• Partners may not be transparent about goals, or incentives
UNCLASSIFIED


UNCLASSIFIED
Not Just "Spy Vs. Spy" Anymore
THEN
Intelligence officers
People recruited by intelligence officers
NOW
Intelligence officers
People recruited by intelligence officers
Hackers
Businesspeople
Academics
Researchers
Diplomats
Anyone else who can get their hands on something of value
UNCLASSIFIED

UNCLASSIFIED

Technology Acquisition Methods

- **Countries seek military and dual-use technology and equipment, unique capabilities and skills, and other sensitive information (including classified information) through various means:**
  - Foreign direct investments (mergers, acquisitions, joint ventures)
  - Technology exports
- **Other means of accessing sensitive technology**
  - Cooperative research and development programs (collaboration on emerging technologies with potential military applications)
  - Scientific exchanges
  - Illicit means (theft, exploitation)

UNCLASSIFIED

UNCLASSIFIED

Today's Global Market Reality

Advanced High-Technology Dual-Use Technologies

Globalization of Commerce

This dynamic creates challenges for nonproliferation and technology security:

- Verifying end-use
- Preventing diversion
- High-bar to deny transfer of sensitive commercial technologies
- Commercial innovation directly translates to defense innovation
- Global sharing of academic and commercial R&D
- Interlinked supply chains create dependencies and vulnerabilities

UNCLASSIFIED


UNCLASSIFIED
Information & Technology Security Pillars
POLICY
PROTECT
WHOLE of GOVERNMENT
LEGISLATION
NATIONAL COLLABORATION
CAPABILITY
INTENT
CHECKS & BALANCES
VARYING INTERESTS
STATUTORY AUTHORITIES
COMPLIANCE SYSTEMS
ENFORCEMENT
INFLUENCERS
- DEFENSE INDUSTRY
- TRADE ASSOCIATIONS
- THINK TANKS
- ACADEMIA
UNCLASSIFIED


UNCLASSIFIED
Physical Security
•Controlling access to secure areas
•Controlling access to containers
SECURITY CLEARANCE REQUIRED
TO ENTER THIS AREA!
UNCLASSIFIED


UNCLASSIFIED
Information Security
Classified Military Information (CMI)
• Application of proper handling, marking, storage, dissemination, and destruction requirements for TS, S, and C
• Application of Security Classification Guide(s)
• Application of Program Protection Plan(s)
• Application of distribution statements
• Application of work performed on classified contracts
• Application of policy regarding security violations and weaknesses
TOP SECRET
SECRET
CONFIDENTIAL
UNCLASSIFIED


UNCLASSIFIED
Operations Security
• Operations Security, or OPSEC, is the process by which we protect information that an adversary could use against us.
UNCLASSIFIED

UNCLASSIFIED

National Security Strategy

- Technology is central to today's geopolitical competition and the future of our national security, economy, and democracy.
- Critical and emerging technologies are poised to retool economies, transform militaries, and reshape the world.
- Competition to develop and deploy foundational technologies that will transform our security and economy is intensifying.

- Mentions "innovation" 19 times
- Contains a Section titled: "*Implementing a Modern Industrial and Innovation Strategy*"
- Contains a Section titled: "*Technology*"

The United States is committed to a world where these technologies ensure the security, prosperity, and values of the American people and like-minded democracies.

UNCLASSIFIED

DoD's Role in Technology Transfers

UNCLASSIFIED

UNCLASSIFIED

DoD's Review Agencies

U.S. Military Services:

- U.S. Navy and U.S. Marine Corps - Navy International Programs Office (Navy-IPO)
- U.S. Air Force – Under Secretary for International Affairs, Foreign Disclosure Division (SAF/IAPD)
- U.S. Army – Deputy Assistant Secretary of the Army, Defense Exports & Cooperation (DASA (DE&C))

DoD:

- Defense Security Cooperation Agency (DSCA)
- Joint Chiefs of Staff (JCS/J5)
- Under Secretary for Policy (USDP)
- Under Secretary for Acquisition and Sustainment (USD A&S)
- Under Secretary for Research and Engineering (USD R&E)
- National Security Agency (NSA)

- **Other DOD Agencies (DIA, DISA, DLA, NGA, NRO, etc.)**

UNCLASSIFIED

UNCLASSIFIED

Statutory Reforms Addressing Critical Technology

- 2019 National Defense Authorization Act provided new authorities to respond to strategic competitors' pursuit of critical technologies.
  - *Export Control Reform Act (ECRA)*
  - *Foreign Investment Risk Review Modernization Act (FIRRMA)*
- Export controls and foreign direct investment screening were blended to capture the pathways by which critical U.S. technologies are acquired.
- One of the requirements under ECRA is to identify critical and emerging technologies, for both export controls and for screening foreign investments.

JOHN S. McCAIN
NATIONAL DEFENSE AUTHORIZATION ACT
FOR FISCAL YEAR 2019

CONFERENCE REPORT

H.R. 5515

The objective is to identify critical and emerging technologies in the multilateral export control regimes and establish multilaterally-agreed controls.

UNCLASSIFIED

National Industrial Security Program

- Detect and deter unauthorized access of classified information
- Counter the threat posed by adversaries and others who target U.S. classified information

*"...the National Industrial Security Program shall serve as a single, integrated, cohesive industrial security program to protect classified information **and** to preserve our Nation's economic and technological interests."*

Executive Order 12829 of January 8, 1993

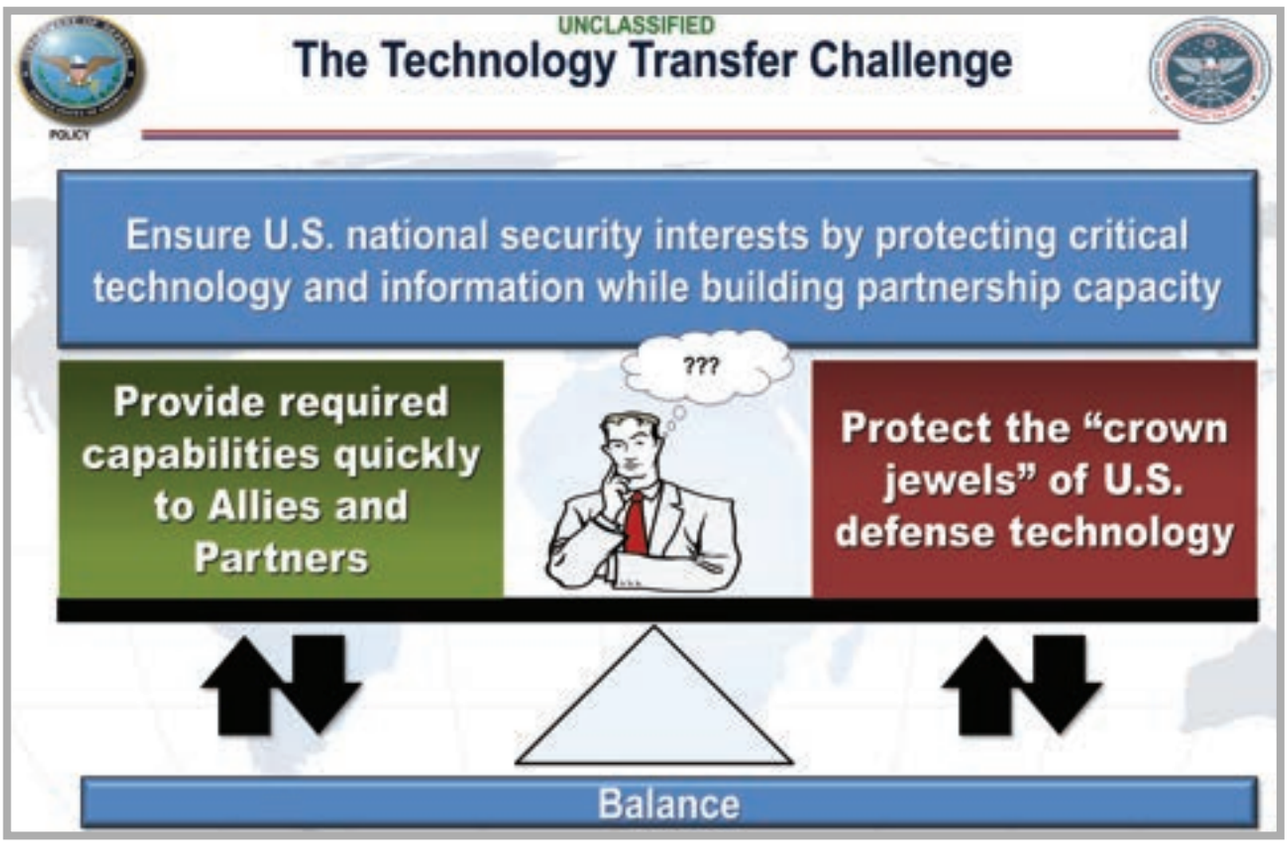
UNCLASSIFIED

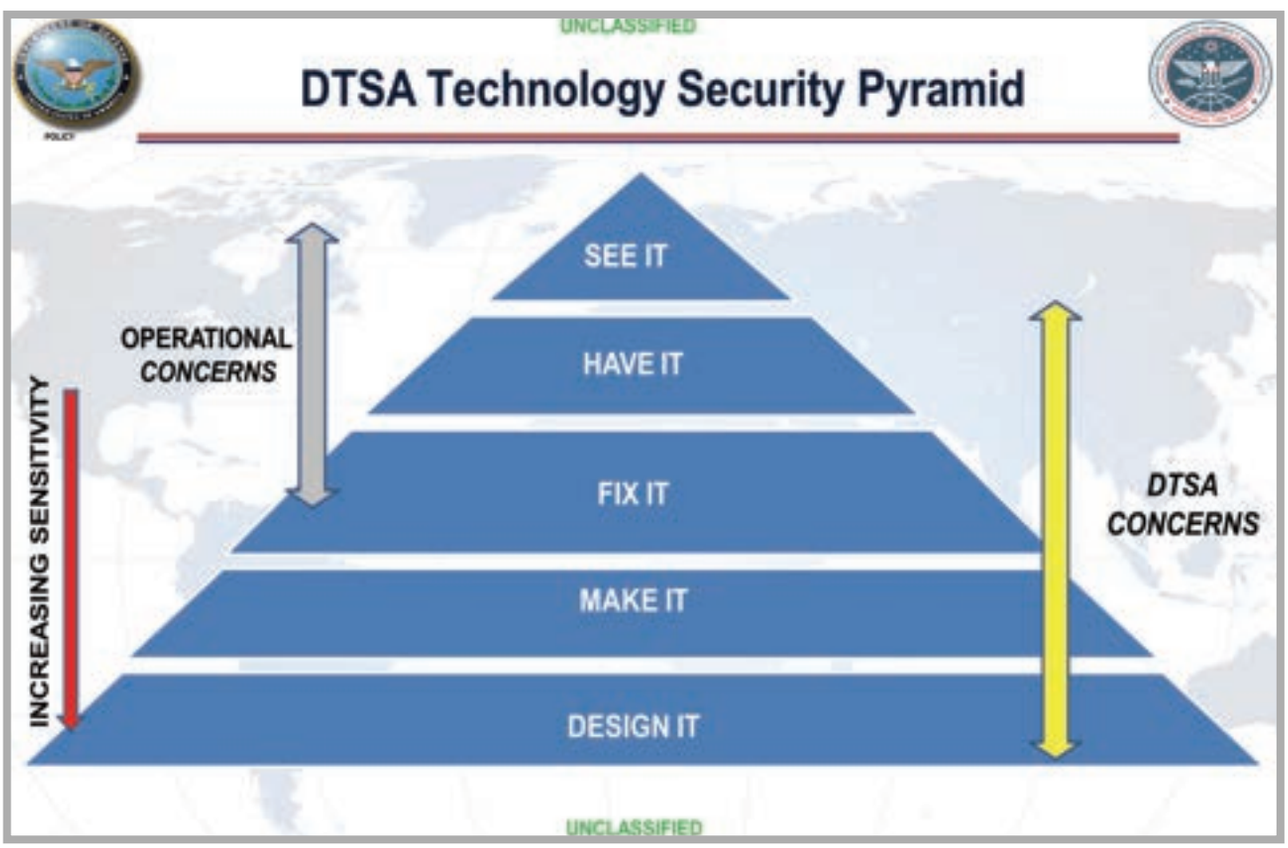
UNCLASSIFIED

Defense Technology Security

- The protection/security of U.S. defense technology is inherent in the provision of U.S. defense technology.
- Foundational/enabling agreements, multi-lateral export control regimes, and end-use monitoring programs provide key assurances.
- Defense technology security among Partners is zero-sum.

UNCLASSIFIED


UNCLASSIFIED
The Technology Transfer Challenge
POLICY
Ensure U.S. national security interests by protecting critical technology and information while building partnership capacity
???
Provide required capabilities quickly to Allies and Partners
Protect the "crown jewels" of U.S. defense technology
Balance


UNCLASSIFIED
DTSA Technology Security Pyramid
POLICY
SEE IT
HAVE IT
FIX IT
MAKE IT
DESIGN IT
OPERATIONAL CONCERNS
INCREASING SENSITIVITY
DTSA CONCERNS
UNCLASSIFIED

UNCLASSIFIED

DoD Review of Technology Transfers

- **Factors considered when assessing impact on national security:**

Region, Country, & Technology	Interoperability
Level of Technology	International Agreements
End User and End Use History	Foreign Availability
Military Operational Impact	Classified Data Transfers

UNCLASSIFIED

UNCLASSIFIED

Analyze

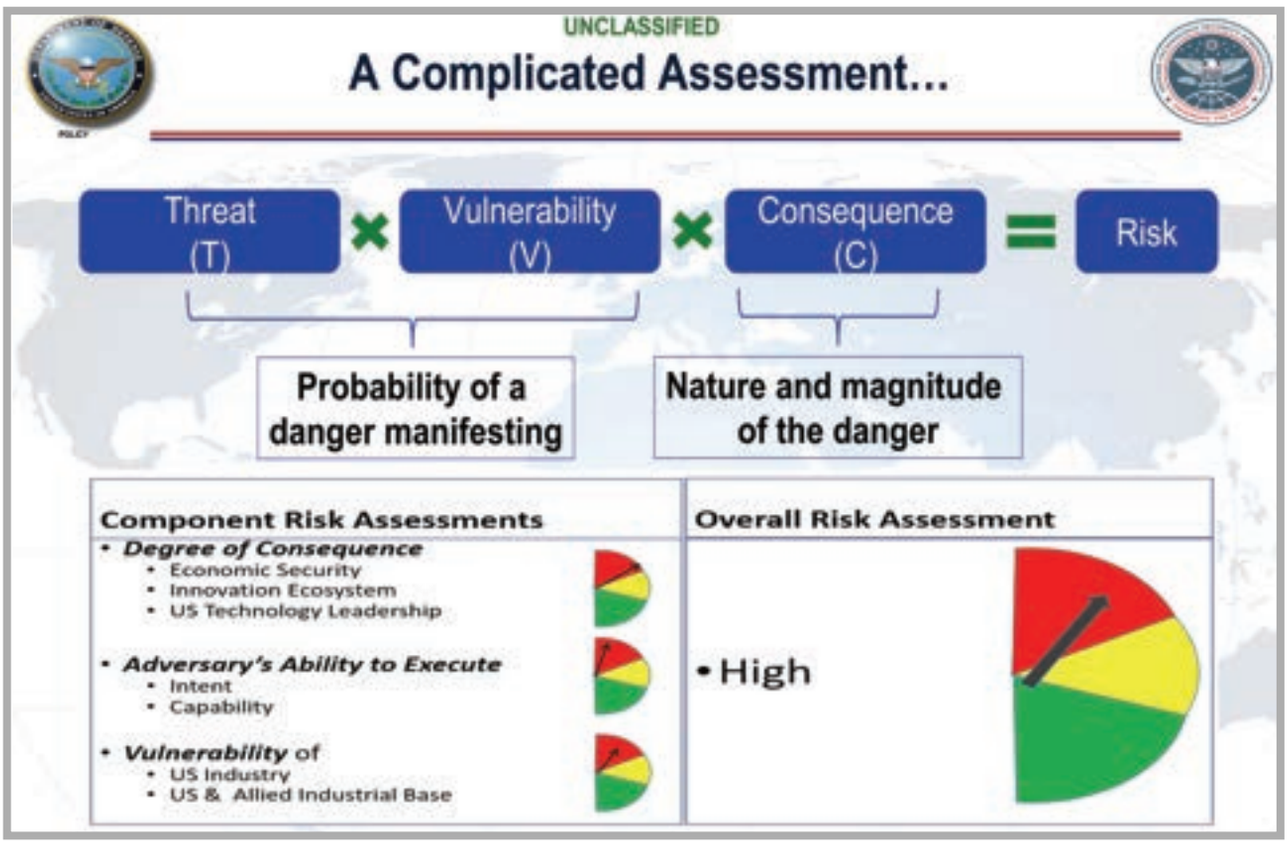
- Analysis focuses on technology end-user, its activities, and relationships

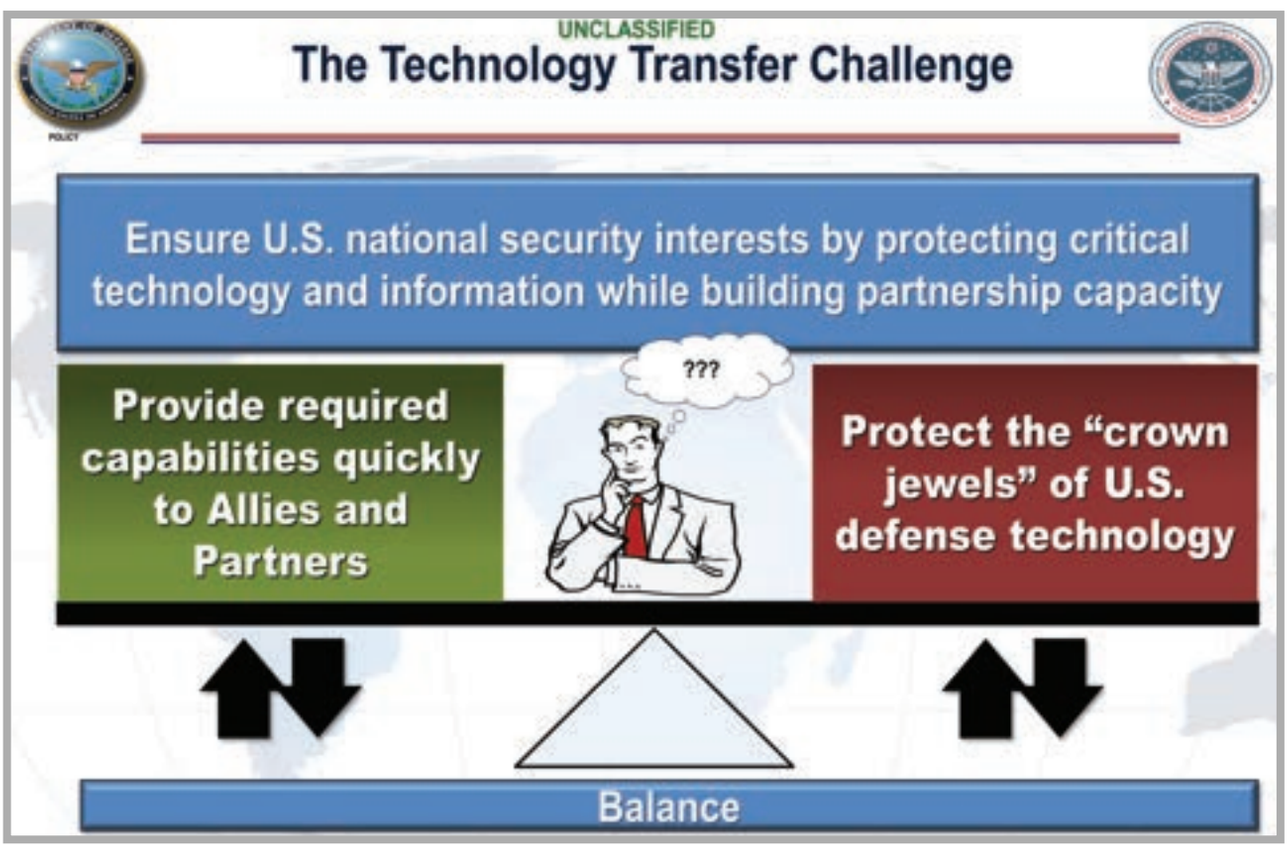
- **Individual** — History of person's conduct and business relationship with third parties

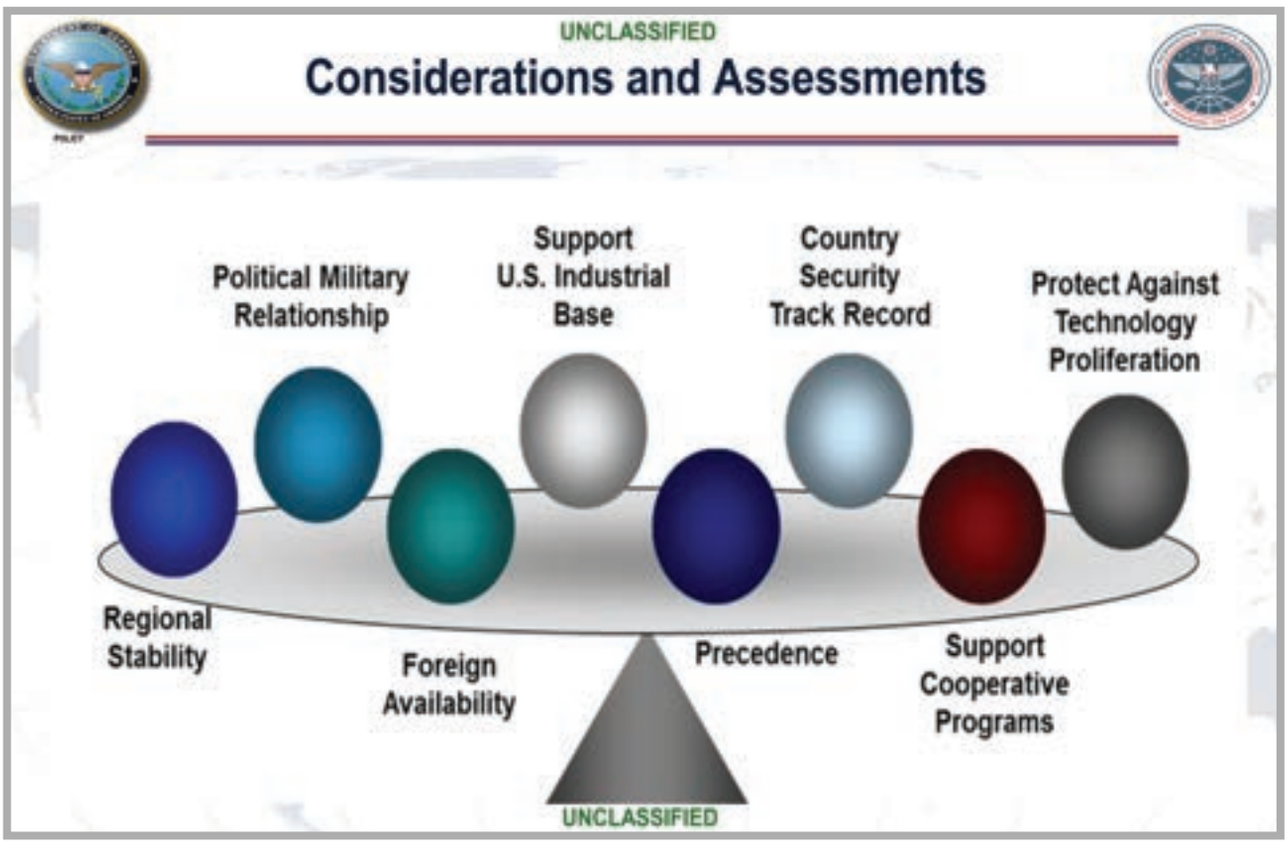
- **Entity** — History of entity, ownership, relationships

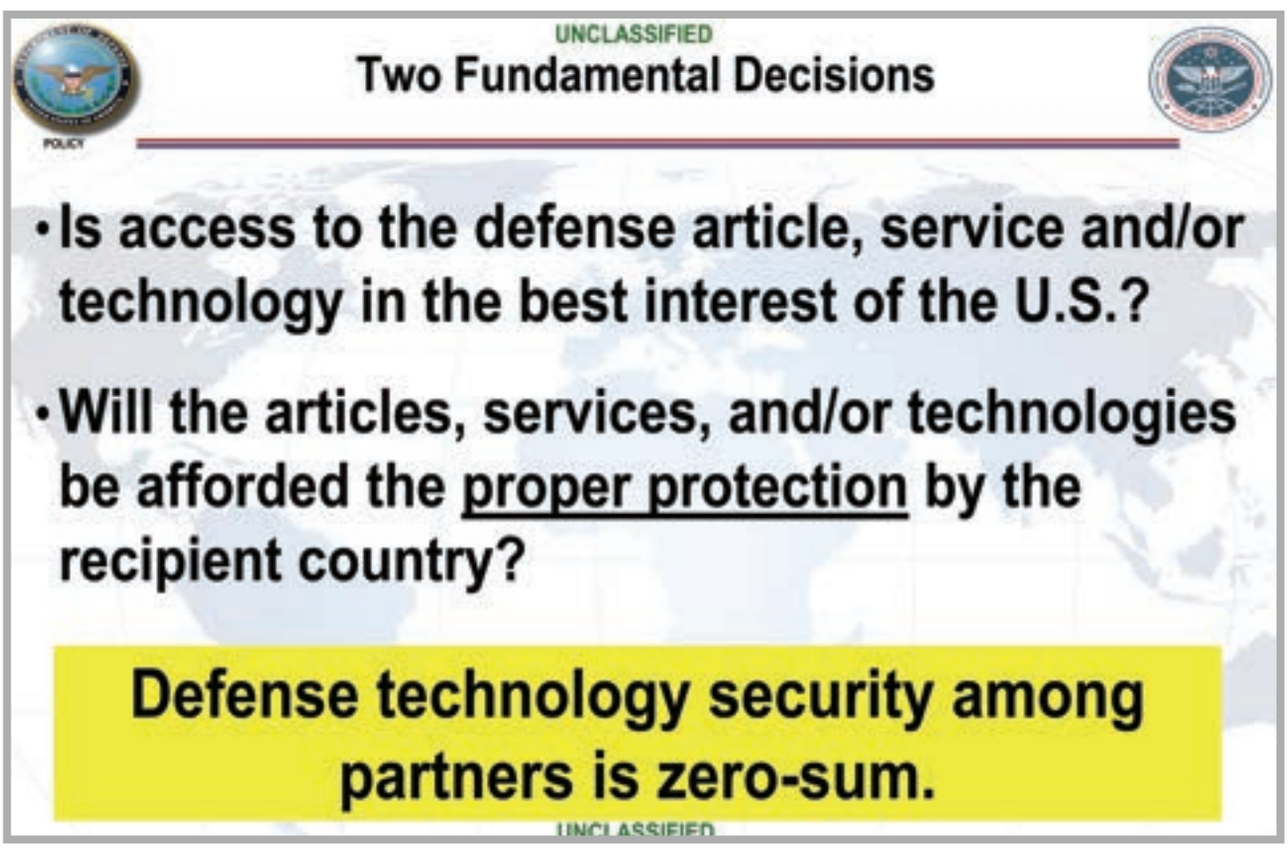
- **Country** — Headquarters location, field offices, financial trails

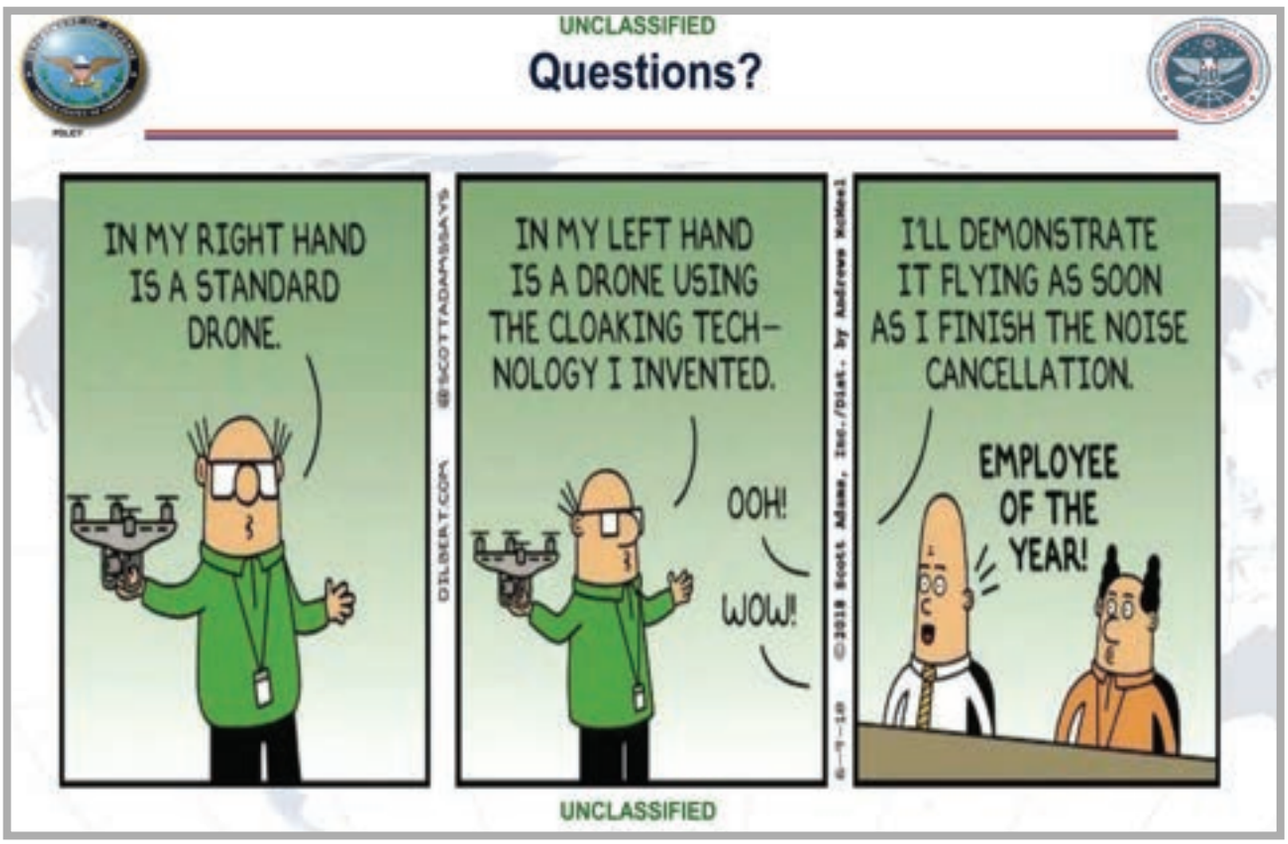
UNCLASSIFIED

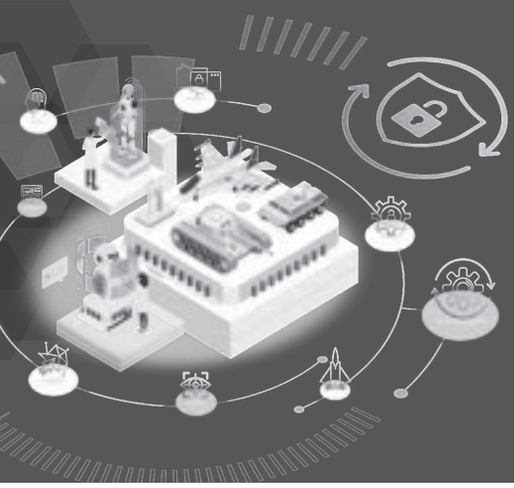

UNCLASSIFIED
A Complicated Assessment…
Threat (T)
Vulnerability (V)
Consequence (C)
Risk
Probability of a danger manifesting
Nature and magnitude of the danger
Component Risk Assessments
Degree of Consequence
Economic Security
Innovation Ecosystem
US Technology Leadership
Adversary's Ability to Execute
Intent
Capability
Vulnerability of
US Industry
US & Allied Industrial Base
Overall Risk Assessment
• High


UNCLASSIFIED
The Technology Transfer Challenge
Ensure U.S. national security interests by protecting critical technology and information while building partnership capacity
Provide required capabilities quickly to Allies and Partners
???
Protect the "crown jewels" of U.S. defense technology
Balance


UNCLASSIFIED
Considerations and Assessments
Political Military Relationship
Support U.S. Industrial Base
Country Security Track Record
Protect Against Technology Proliferation
Regional Stability
Foreign Availability
Precedence
Support Cooperative Programs
UNCLASSIFIED


UNCLASSIFIED
Two Fundamental Decisions
• Is access to the defense article, service and/or technology in the best interest of the U.S.?
• Will the articles, services, and/or technologies be afforded the proper protection by the recipient country?
Defense technology security among partners is zero-sum.


UNCLASSIFIED
Questions?
IN MY RIGHT HAND IS A STANDARD DRONE.
IN MY LEFT HAND IS A DRONE USING THE CLOAKING TECH-NOLOGY I INVENTED.
OOH!
WOW!
I'LL DEMONSTRATE IT FLYING AS SOON AS I FINISH THE NOISE CANCELLATION.
EMPLOYEE OF THE YEAR!
DILBERT.COM @SCOTTADAMSSAYS
©2018 Scott Adams, Inc./Dist. by Andrews McMeel
UNCLASSIFIED

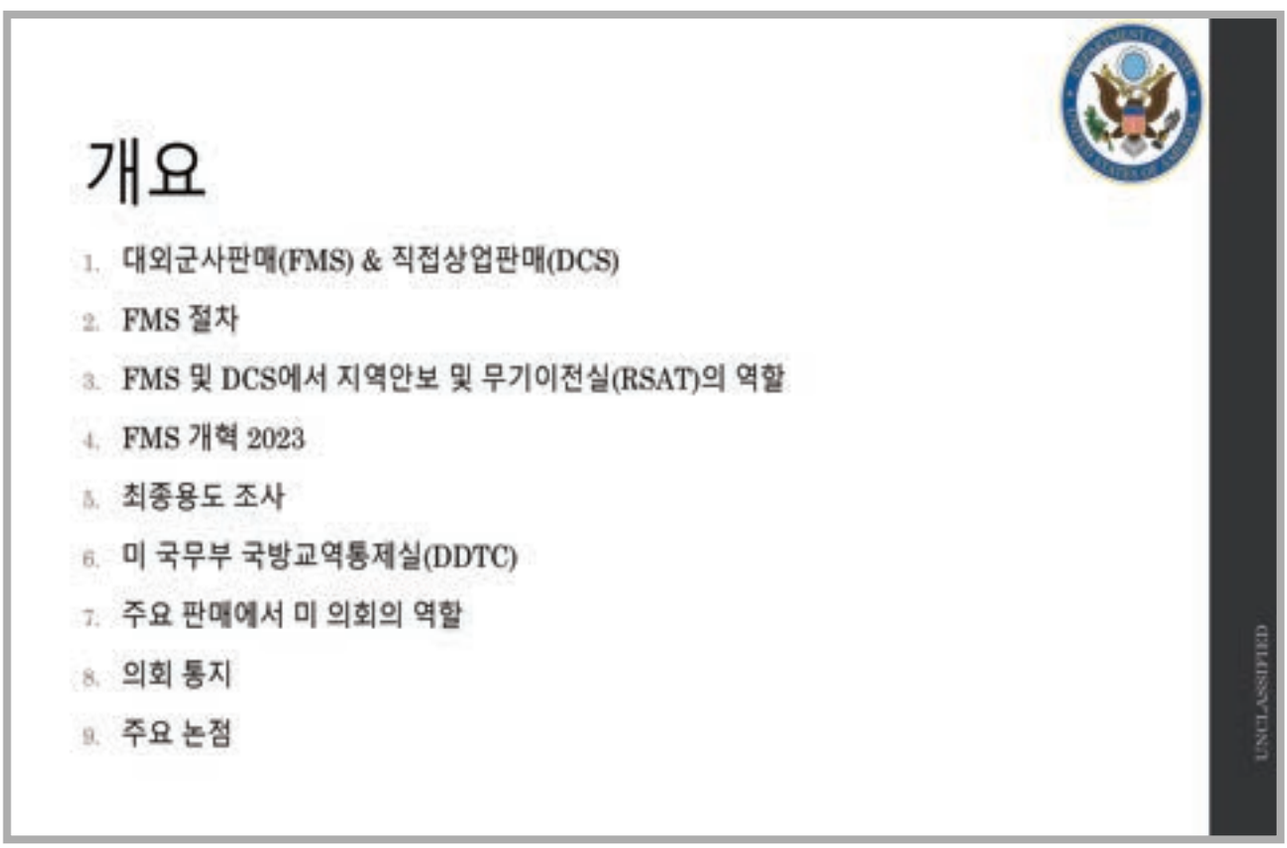


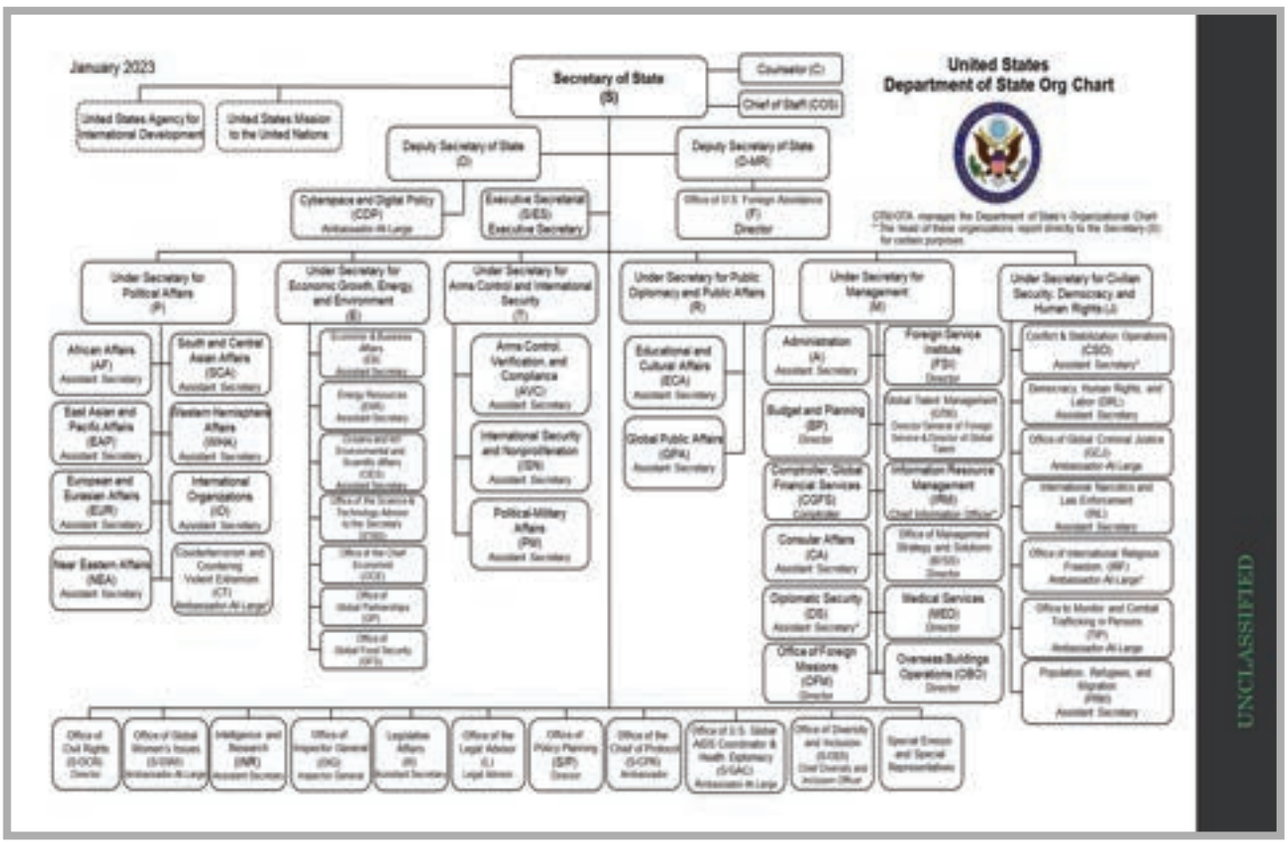
주제발표 2.

국내외 안보 강화를 위한 방산 무역 통제
Controlling Defense Trade for Greater National and International Security

미국 국무부 지역안보무기이전과 외무관 I **Mr. Phillip R. Davis II**
Foreign Affairs Officer, RSAT, U.S. Department of State, U.S.
Mr. Phillip R. Davis II


DEPARTMENT OF STATE
UNITED STATES OF AMERICA
직접상업판매&
대외군사판매
2023 방산기술보호 컨퍼런스
2023년 8월 4일
UNCLASSIFIED


개요
1. 대외군사판매(FMS) & 직접상업판매(DCS)
2. FMS 절차
3. FMS 및 DCS에서 지역안보 및 무기이전실(RSAT)의 역할
4. FMS 개혁 2023
5. 최종용도 조사
6. 미 국무부 국방교역통제실(DDTC)
7. 주요 판매에서 미 의회의 역할
8. 의회 통지
9. 주요 논점
UNCLASSIFIED


January 2023
United States Department of State Org Chart
Secretary of State (S)
Counselor (C)
Chief of Staff (COS)
United States Agency for International Development
United States Mission to the United Nations
Deputy Secretary of State (D)
Deputy Secretary of State (D-MR)
Cyberspace and Digital Policy (CDP) Ambassador-At-Large
Executive Secretariat (S/ES) Executive Secretary
Director
Under Secretary for Political Affairs (P)
Under Secretary for Economic Growth, Energy and Environment (E)
Under Secretary for Arms Control and International Security (T)
Under Secretary for Public Diplomacy and Public Affairs (R)
Under Secretary for Management (M)
Under Secretary for Civilian Security, Democracy and Human Rights (J)
African Affairs (AF) Assistant Secretary
South and Central Asian Affairs (SCA) Assistant Secretary
East Asian and Pacific Affairs (EAP) Assistant Secretary
Western Hemisphere Affairs (WHA) Assistant Secretary
European and Eurasian Affairs (EUR) Assistant Secretary
International Organizations (IO) Assistant Secretary
Near Eastern Affairs (NEA) Assistant Secretary
Arms Control, Verification, and Compliance (AVC) Assistant Secretary
International Security and Nonproliferation (ISN) Assistant Secretary
Political-Military Affairs (PM) Assistant Secretary
Educational and Cultural Affairs (ECA) Assistant Secretary
Global Public Affairs (GPA) Assistant Secretary
Administration (A) Assistant Secretary
Budget and Planning (BP) Director
Comptroller, Global Financial Services (CGFS) Comptroller
Consular Affairs (CA) Assistant Secretary
Diplomatic Security (DS) Assistant Secretary
Office of Foreign Missions (OFM) Director
Foreign Service Institute (FSI) Director
Information Resource Management (IRM) Chief Information Officer
Office of Management Strategy and Solutions (M/SS) Director
Medical Services (MED) Director
Overseas Buildings Operations (OBO) Director
Conflict & Stabilization Operations (CSO) Assistant Secretary
Democracy, Human Rights, and Labor (DRL) Assistant Secretary
Office of Global Criminal Justice (GCJ) Ambassador-At-Large
International Narcotics and Law Enforcement (INL) Assistant Secretary
Office of International Religious Freedom (IRF) Ambassador-At-Large
Office to Monitor and Combat Trafficking in Persons (TIP) Ambassador-At-Large
Population, Refugees, and Migration (PRM) Assistant Secretary
Office of Civil Rights (S-OCR) Director
Office of Global Women's Issues (S-GWI) Ambassador-At-Large
Intelligence and Research (INR) Assistant Secretary
Office of Inspector General (OIG) Inspector General
Legislative Affairs (H) Assistant Secretary
Office of the Legal Advisor (L) Legal Advisor
Office of Policy Planning (S/P) Director
Office of the Chief of Protocol (S-CPR) Ambassador
Special Envoys and Special Representatives
UNCLASSIFIED


대외군사판매(FMS) & 직접상업판매(DCS)
대외군사판매
• 정부 대 정부. 국무부 판매 승인 후 국방부에서 시행
직접상업판매
• 국무부에서 국제 무기거래규정(ITAR)에 의해 통제되는 상업수출대상 방산물자 라이선스 검토 및 승인. 국방부 검토 대상.
UNCLASSIFIED

FMS & DCS에서 지역안보 및 무기이전실(RSAT)의 역할

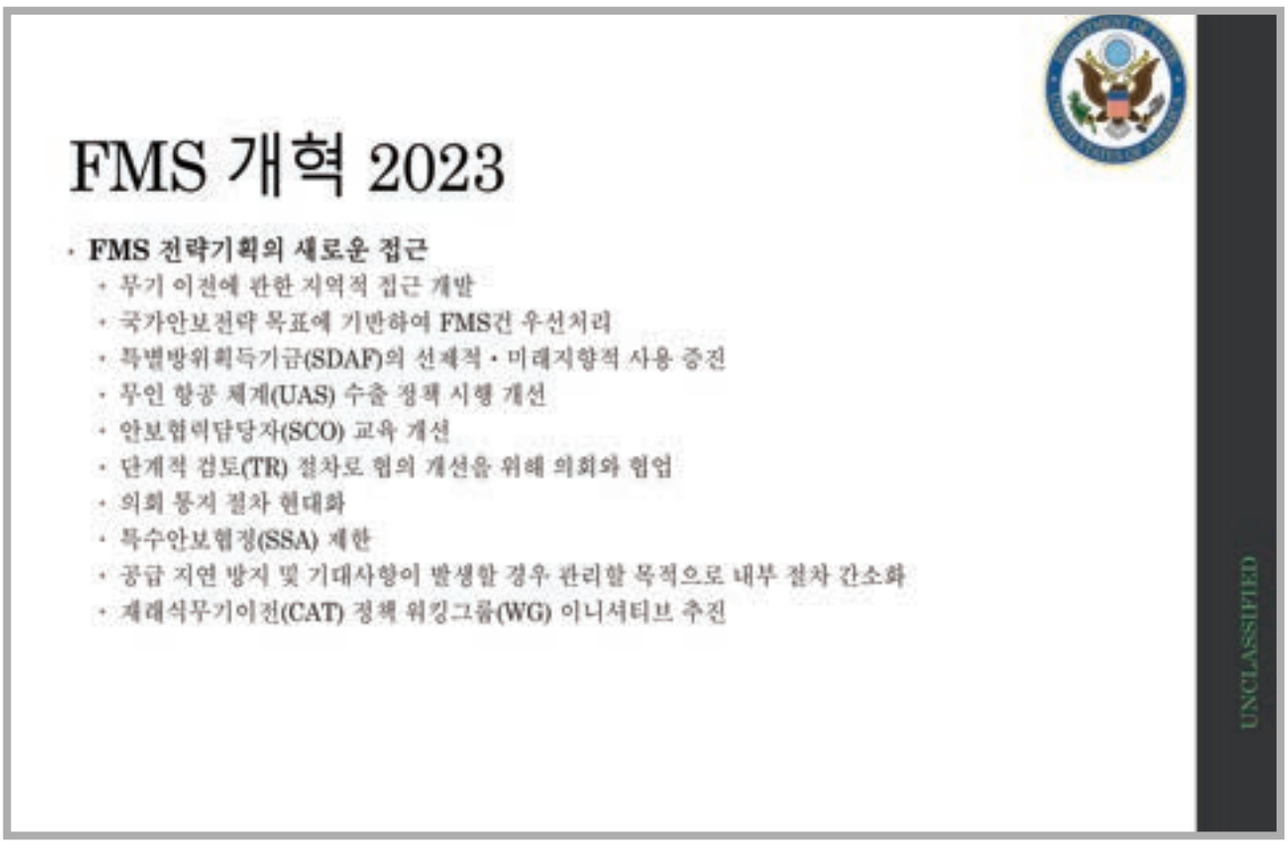
- 모든 FMS 건에서 의사결정 조율
- DCS 라이선스에 관한 정책 제언 제공(국방교역통제실 승인)
- 무기 이전에 관한 대외정책 관점 제시
- 한 시점만이 아닌 전 과정에 걸쳐 제언 제공
- 미 방산물자 획득 관련 요건 및 활동에 관해 파트너들과 접촉
- 산업계와 접촉 유지
  - 마케팅
  - 파트너 접촉
  - 대회
  - 변호

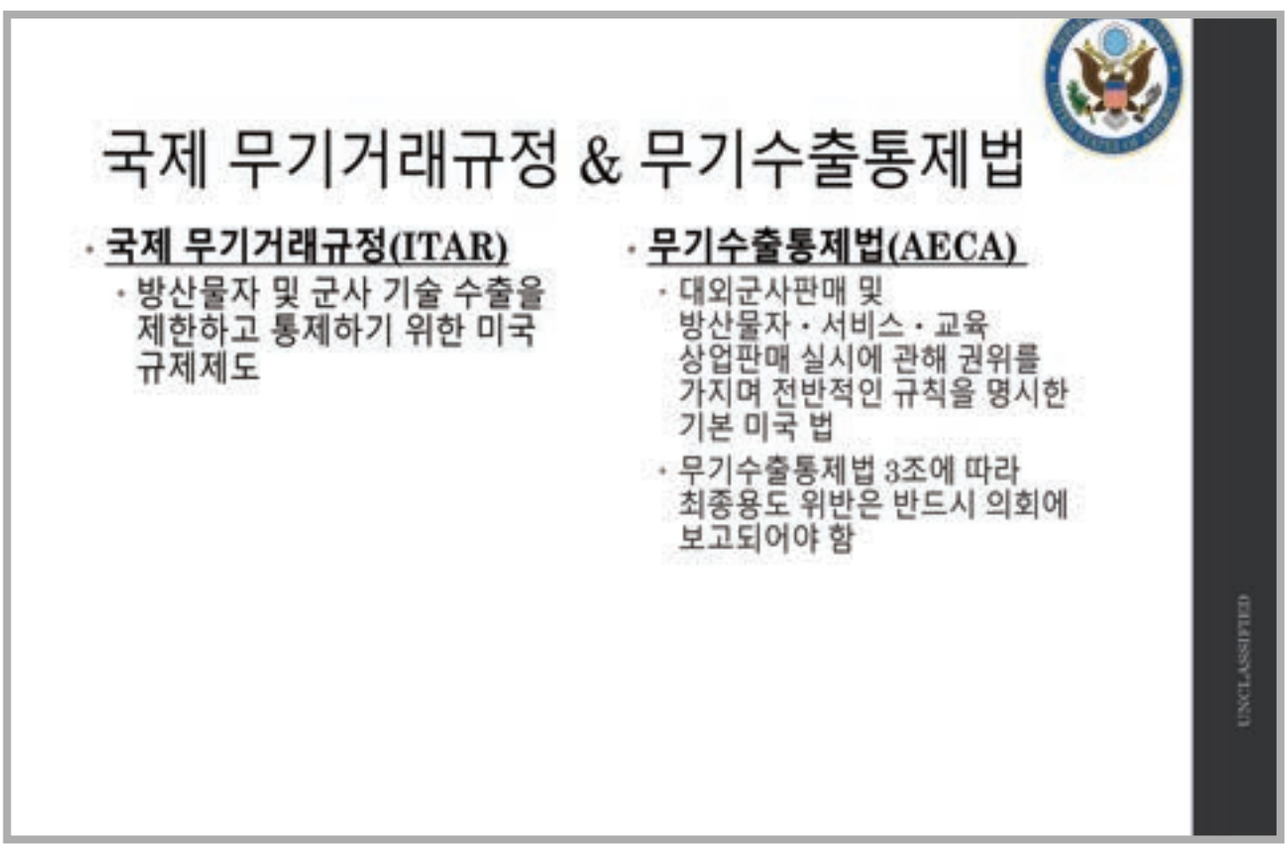
UNCLASSIFIED

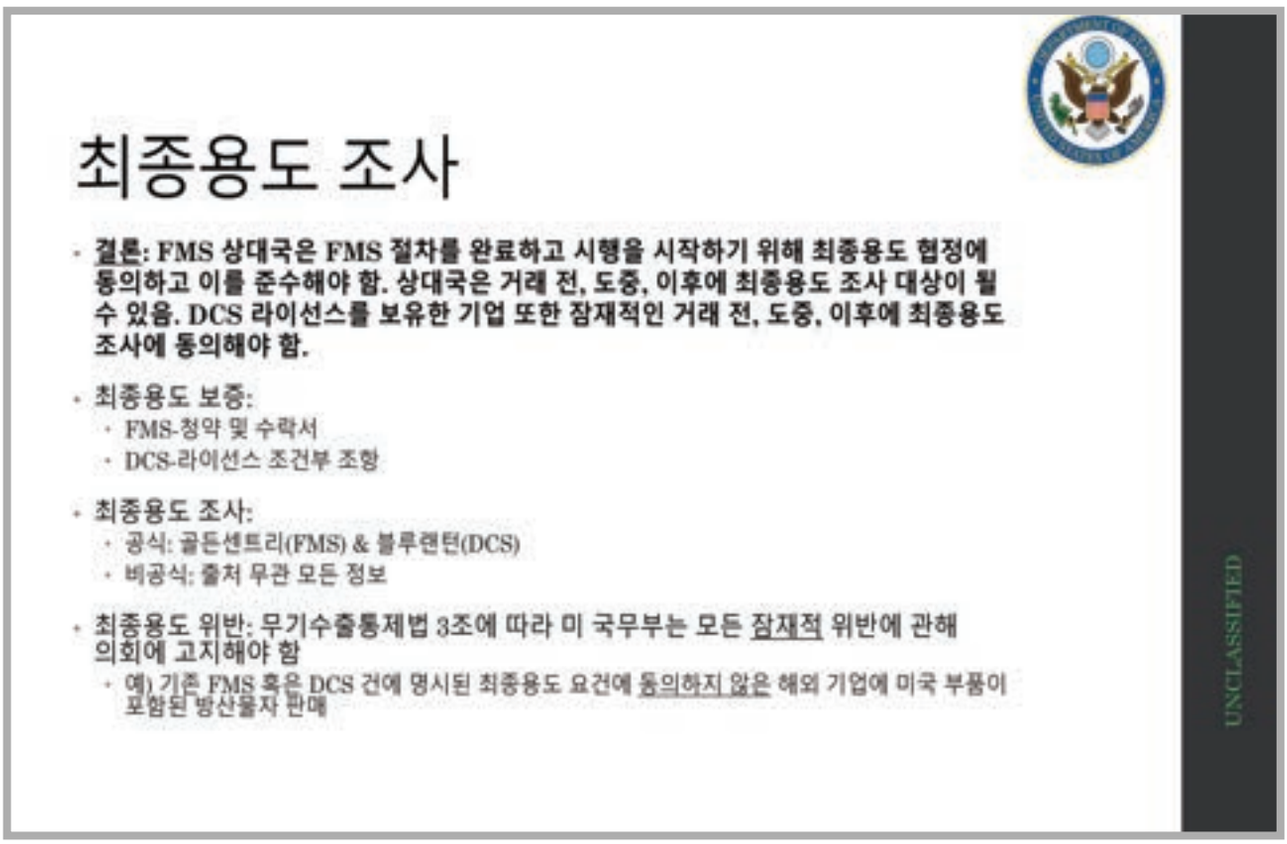
FMS 절차

- 미 정부(USG)와 파트너 국가 간 정부 대 정부 협정: 청약 및 수락서(LOA)
- '완성품 접근(total package approach)' 개념에 기반
- 요청서(LOR)를 통해 가격 책정 · 가용성, 기술 보호 및 공개, 대외정책 검토 절차 착수
- 판매를 추진할 수 있으며 국가가 LOA에 동의하고 지불을 시작할 경우, 국가를 대변하여 계약 절차 시작

UNCLASSIFIED


FMS 개혁 2023
• FMS 전략기획의 새로운 접근
• 무기 이전에 관한 지역적 접근 개발
• 국가안보전략 목표에 기반하여 FMS건 우선처리
• 특별방위획득기금(SDAF)의 선제적·미래지향적 사용 증진
• 무인 항공 체계(UAS) 수출 정책 시행 개선
• 안보협력담당자(SCO) 교육 개선
• 단계적 검토(TR) 절차로 협의 개선을 위해 의회와 협업
• 의회 통지 절차 현대화
• 특수안보협정(SSA) 제한
• 공급 지연 방지 및 기대사항이 발생할 경우 관리할 목적으로 내부 절차 간소화
• 재래식무기이전(CAT) 정책 워킹그룹(WG) 이니셔티브 추진
UNCLASSIFIED


국제 무기거래규정 & 무기수출통제법
• 국제 무기거래규정(ITAR)
• 방산물자 및 군사 기술 수출을 제한하고 통제하기 위한 미국 규제제도
• 무기수출통제법(AECA)
• 대외군사판매 및 방산물자·서비스·교육 상업판매 실시에 관해 권위를 가지며 전반적인 규칙을 명시한 기본 미국 법
• 무기수출통제법 3조에 따라 최종용도 위반은 반드시 의회에 보고되어야 함
UNCLASSIFIED

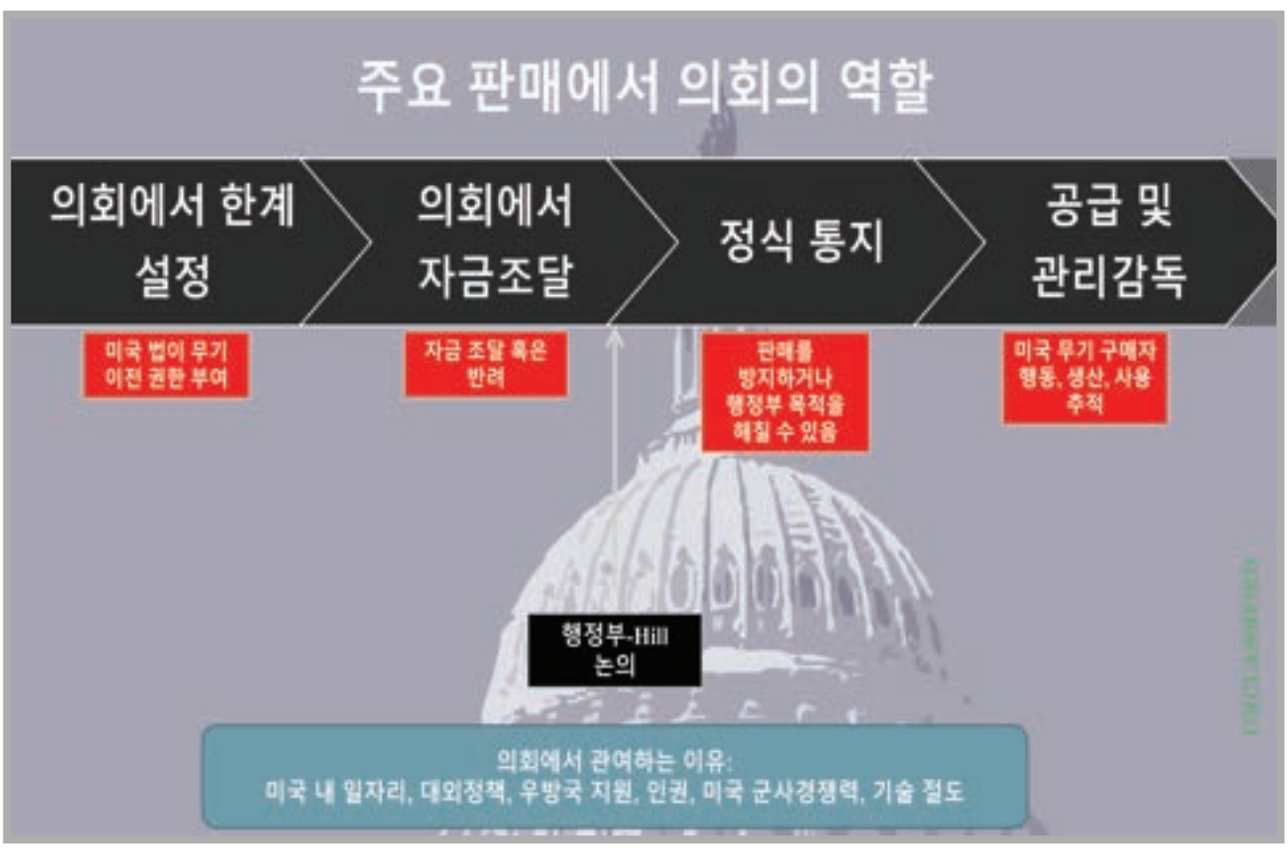

최종용도 조사
• 결론: FMS 상대국은 FMS 절차를 완료하고 시행을 시작하기 위해 최종용도 협정에 동의하고 이를 준수해야 함. 상대국은 거래 전, 도중, 이후에 최종용도 조사 대상이 될 수 있음. DCS 라이선스를 보유한 기업 또한 잠재적인 거래 전, 도중, 이후에 최종용도 조사에 동의해야 함.
• 최종용도 보증:
• FMS-청약 및 수락서
• DCS-라이선스 조건부 조항
• 최종용도 조사:
• 공식: 골든센트리(FMS) & 블루랜턴(DCS)
• 비공식: 출처 무관 모든 정보
• 최종용도 위반: 무기수출통제법 3조에 따라 미 국무부는 모든 잠재적 위반에 관해 의회에 고지해야 함
• 예) 기존 FMS 혹은 DCS 건에 명시된 최종용도 요건에 동의하지 않은 해외 기업에 미국 부품이 포함된 방산물자 판매
UNCLASSIFIED


국방교역통제실(DDTC)
• DCS 규제기관
• 판매 라이선스 획득 요건 개요 제공
• 상대국 및 계약업체의 준수를 보장
• 무기수출통제법(AECA) 및 국제 무기거래규정(ITAR) 집행
• 블루랜턴을 통해 DCS 최종용도 조사 실시
• 무기수출통제법 3조에 따라 모든 최종용도 잠재 위반을 의회에 보고
UNCLASSIFIED

주요 판매에서 의회의 역할

- 모든 FMS 및 DCS 건은 미 국무부에서 건별로 검토
- FMS 및 DCS 시행 방식에 있어서 의회가 주요 역할을 함
- 의회가 FMS 및 DCS에 관여하는 이유는?
  - 미국 법이 무기 이전 방식을 규정함
  - 의회가 자금 조달을 승인 및 반려함
  - 의회는 미 행정부의 목적을 차단 혹은 변경할 권한이 있음
  - 의회가 미국 내 무기 구매자 행동, 생산, 사용을 추적함

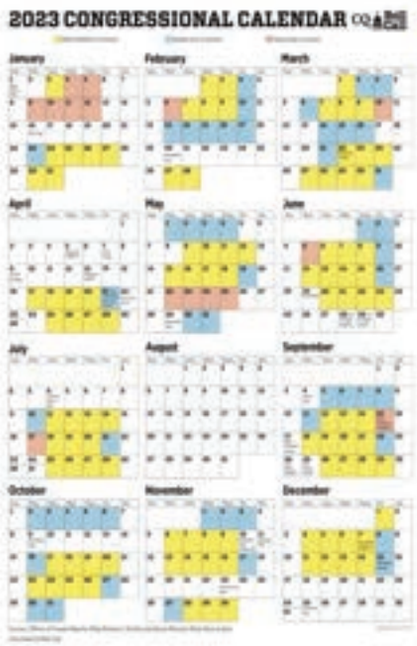
UNCLASSIFIED



의회 통지(대한민국)

- 20일간 단계적 검토 기간
- 15일간 정식 통지 기간
- 2,500만 달러 한계점(주요 방산물자)
- 1억 달러 한계점(비주요 방산물자)
- 3억 달러 한계점(군건설)
- DCS 한정 - 소화기 대상 100만 달러 한계점

- **참고: 모든 판매건은 의회 개회 여부에 따라 지연될 수 있음**



UNCLASSIFIED

재래식 무기 이전(CAT) 정책

- **결론: 모든 FMS 및 DCS 건은 CAT 정책에 개괄된 지침에 따라 검토 대상이며 따라서 지침을 충족하지 않을 경우 지연 혹은 취소될 수 있음**
- CAT 정책은 미 정부기관이 제안된 안보 부문 지원, G2G 이전, 미 군사장비의 허가받은 상업판매를 검토 및 평가하는 체계를 제공함
- 개정된 CAT 정책에서는 이전받은 자가 이전된 무기를 인권 침해 행위를 범하거나 조력할 '가능성이 크다고' 판단될 경우 미국은 어떠한 이전도 승인하지 않을 것임을 명시함

- CAT 정책 목표:
  - 파트너 국가 역량 강화
  - 미국 방산기반 지원
  - 미국 군대의 기술 경쟁력 강화
  - 해외 파트너십 강화 및 상호운용성 증대
  - 대량살상무기 확산 방지
  - 미 정부가 민간 피해 위험을 줄이는 방향으로 파트너와 협력하도록 유도
  - 파트너 국가들이 세계 안보에 기여하는 역량을 강화함으로써 미국 동맹관계를 재활성화

UNCLASSIFIED

국제 안보 환경

- 미국, 우크라이나에 400억 달러 이상 군사 지원 제공
- 우크라이나 내 전쟁으로 각국이 자체 안보 파트너십을 재검토하게 됨
- 미국은 지속적으로 세계 평화 및 안보에 굳건한 의지를 가지고 있음
- 미국이 지속적인 군사력 배치를 통해 남한 방위에 기여했으며, 대한민국 방위 활동을 지원하기 위해 미국 장비 및 기술을 이전해 온 한-미 관계는 70년을 넘어 지속됨
- 전 세계적으로 위협이 증가하는 상황에서 미국은 세계 평화를 유지하기 위해 필요한 군사 장비 및 기술 이전을 통해 대한민국과의 안보 동맹관계 강화를 기대함

UNCLASSIFIED

주요 논점

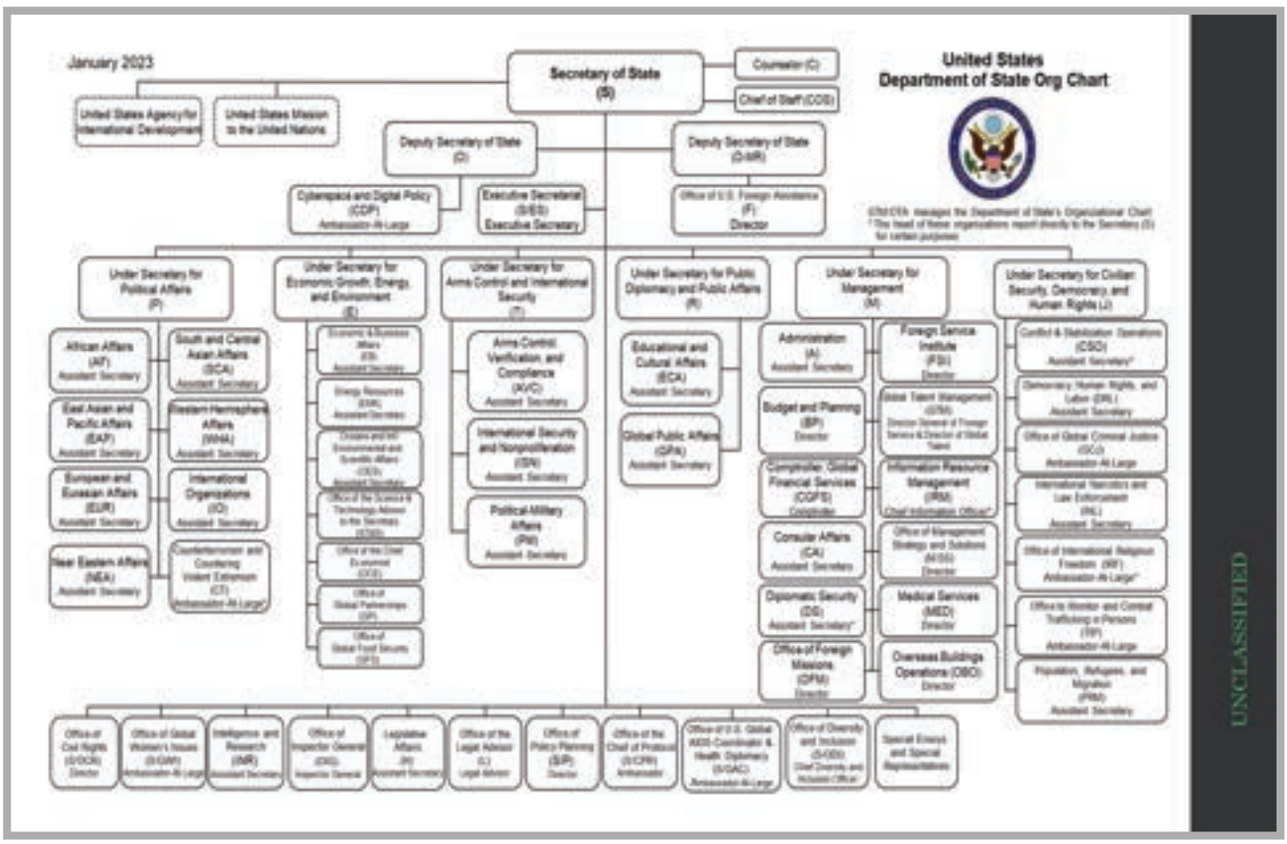
- FMS 및 DCS 절차는 하루아침에 이루어지지 않습니다. 절차가 난관에 봉착하거나, 지연되거나, 취소될 수 있는 많은 여지가 있습니다.
- 방위교역 통제 관련 지침은 미국 및 동맹국과 파트너 국가들의 이익을 보호하기 위한 것입니다.
- 미국은 대한민국과 오래도록 번영하는 관계 지속을 희망하며, 세계 평화에 대한 대한민국의 지속적인 관심과 기여에 감사드립니다.

UNCLASSIFIED


연락처
PM/RSAT EAP/SCA팀:
Tammy Rutledge, 팀 리더, RutledgeTJ@state.gov
Phil Davis, 외무관, DavisPR@state.gov
PM/DDTC:
블루랜턴 문의:
PM-DTCP-CEA@state.gov
국방교역통제실 대응팀:
DDTCCustomerService@state.gov
UNCLASSIFIED


DEPARTMENT OF STATE
UNITED STATES OF AMERICA
Direct Commercial Sales & Foreign Military Sales
Defense Technology Security Conference 2023
August 4,2023
UNCLASSIFIED


Overview
1. Foreign Military Sales (FMS) & Direct Commercial Sales (DCS)
2. FMS Process
3. Role of RSAT in FMS & DCS
4. FMS Reform 2023
5. End-Use Monitoring
6. Directorate of Defense Trade Controls (DDTC)
7. Role of Congress in Major Sales
8. Congressional Notification
9. Key Points
UNCLASSIFIED


January 2023
United States Department of State Org Chart
Secretary of State (S)
Counselor (C)
Chief of Staff (COS)
United States Agency for International Development
United States Mission to the United Nations
Deputy Secretary of State (D)
Deputy Secretary of State (D-MR)
Cyberspace and Digital Policy (CDP) Ambassador-At-Large
Executive Secretariat (S/ES) Executive Secretary
Office of U.S. Foreign Assistance (F) Director
Under Secretary for Political Affairs (P)
Under Secretary for Economic Growth, Energy, and Environment (E)
Under Secretary for Arms Control and International Security (T)
Under Secretary for Public Diplomacy and Public Affairs (R)
Under Secretary for Management (M)
Under Secretary for Civilian Security, Democracy, and Human Rights (J)
African Affairs (AF) Assistant Secretary
South and Central Asian Affairs (SCA) Assistant Secretary
East Asian and Pacific Affairs (EAP) Assistant Secretary
Western Hemisphere Affairs (WHA) Assistant Secretary
European and Eurasian Affairs (EUR) Assistant Secretary
International Organizations (IO) Assistant Secretary
Near Eastern Affairs (NEA) Assistant Secretary
Counterterrorism and Countering Violent Extremism (CT) Ambassador-At-Large
Arms Control, Verification, and Compliance (AVC) Assistant Secretary
International Security and Nonproliferation (ISN) Assistant Secretary
Political-Military Affairs (PM) Assistant Secretary
Educational and Cultural Affairs (ECA) Assistant Secretary
Global Public Affairs (GPA) Assistant Secretary
Administration (A) Assistant Secretary
Budget and Planning (BP) Director
Comptroller, Global Financial Services (CGFS) Comptroller
Consular Affairs (CA) Assistant Secretary
Diplomatic Security (DS) Assistant Secretary*
Office of Foreign Missions (OFM) Director
Foreign Service Institute (FSI) Director
Information Resource Management (IRM) Chief Information Officer*
Medical Services (MED) Director
Overseas Buildings Operations (OBO) Director
Office of Civil Rights (S/OCR) Director
Office of Inspector General (OIG) Inspector General
Legislative Affairs (H) Assistant Secretary
Office of the Legal Advisor (L) Legal Advisor
Office of Policy Planning (S/P) Director
Special Envoys and Special Representatives
UNCLASSIFIED


Foreign Military Sales (FMS) & Direct Commercial Sales (DCS)
Foreign Military Sales
· Government-to-government; Department of Defense implements after State approves sale
Direct Commercial Sales
· State reviews and approves licenses for International Traffic in Arms Regulations (ITAR)-controlled defense articles for commercial export, subject to review by Department of Defense
UNCLASSIFIED

The Role of RSAT in FMS & DCS

- Coordinate decision making on all FMS cases
- Provide policy input on DCS licenses (authorized by DDTC)
- Provide foreign policy lens to arms transfers
- Provide input throughout the process, not just one point
- Engage with partners about requirements and efforts to obtain U.S. defense articles
- Maintain contact with industry
  - Marketing
  - Partner engagement
  - Competitions
  - Advocacy

UNCLASSIFIED

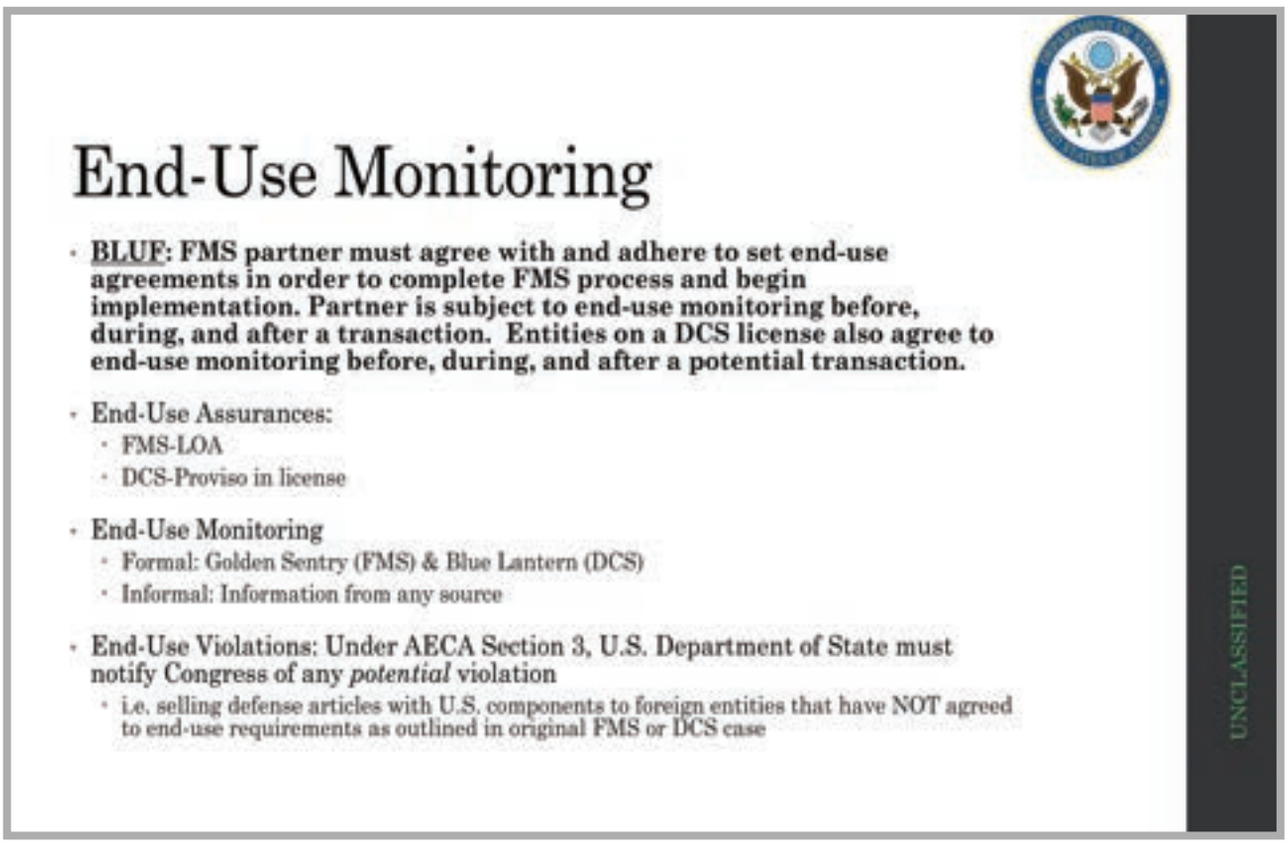
FMS Process

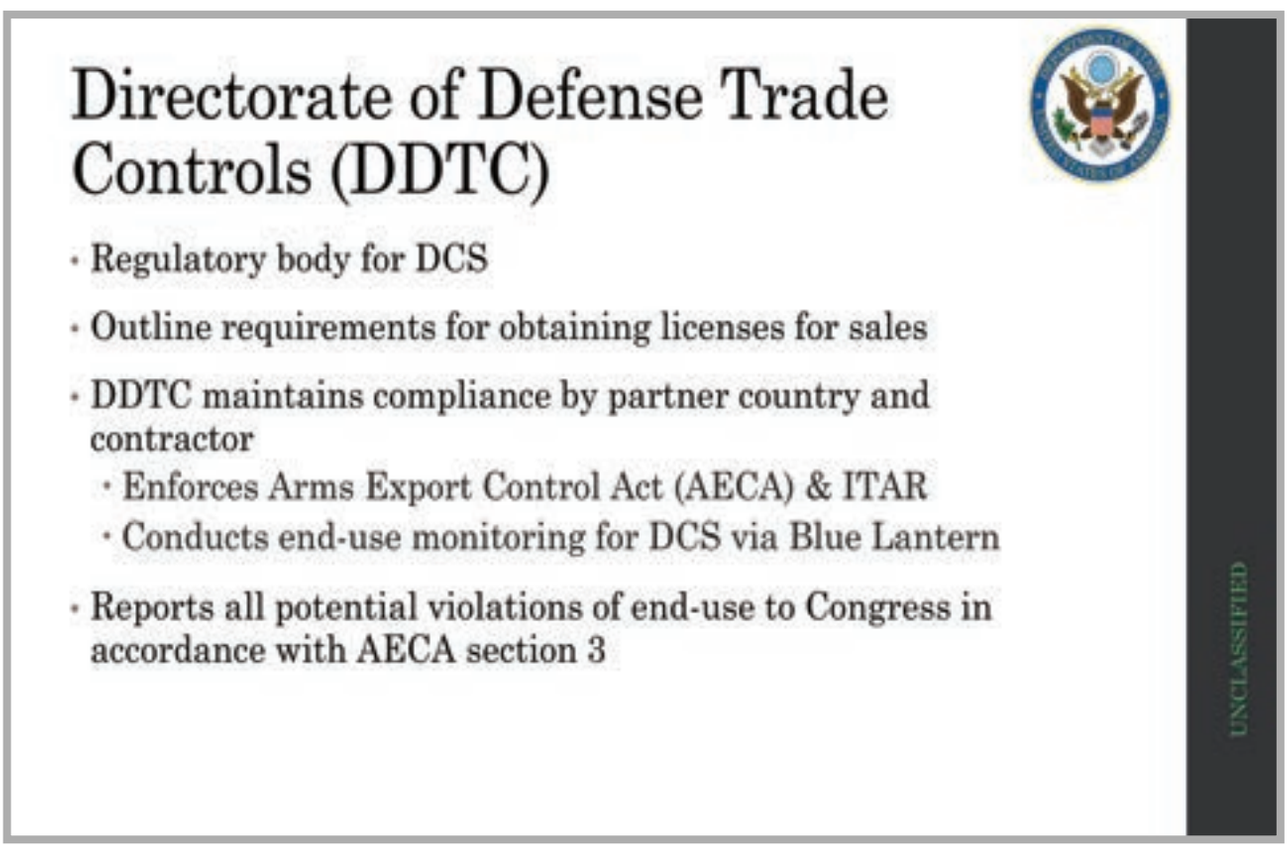
- Government-to-government agreement between U.S. Government (USG) and partner country: Letter of Offer and Acceptance (LOA)
- Based on the concept of a "total package approach"
- Letters of Request (LOR) initiate the process for reviewing pricing and availability, technology security and disclosure, and foreign policy
- If able to proceed with sale and country agrees to LOA and begins payment, contracting process on behalf of the country begins

UNCLASSIFIED


FMS Reform 2023
A new approach to FMS Strategic Planning
Developing a regional approach to arms transfers
Prioritizing cases for FMS based on National Security Strategy goals
Promoting proactive, forward-looking uses of the Special Defense Acquisition Fund (SDAF)
Refining implementation of the Unmanned Aerial System (UAS) Export Policy
Improving Security Cooperation Officer (SCO) Training
Working with Congress to improve consultation through the Tiered Review (TR) Process
Modernizing the Congressional Notification Process
Limiting Special-Security Arrangements (SSAs)
Streamlining internal processes to avoid delivery delays and manage expectations where they occur
Advancing the Conventional Arms Transfer (CAT) Policy Working Group (WG) initiatives
UNCLASSIFIED


ITAR & AECA
International Traffic in Arms Regulations (ITAR)
The ITAR is a U.S. regulatory regime to restrict and control the export of defense articles and military tech
Arms Export Control Act (AECA)
The AECA is the basic U.S. law providing authority and general rules for the conduct of Foreign Military Sales and commercial sales of defense articles, defense services, and training.
Under AECA Section 3, end-use violations MUST be reported to Congress
UNCLASSIFIED

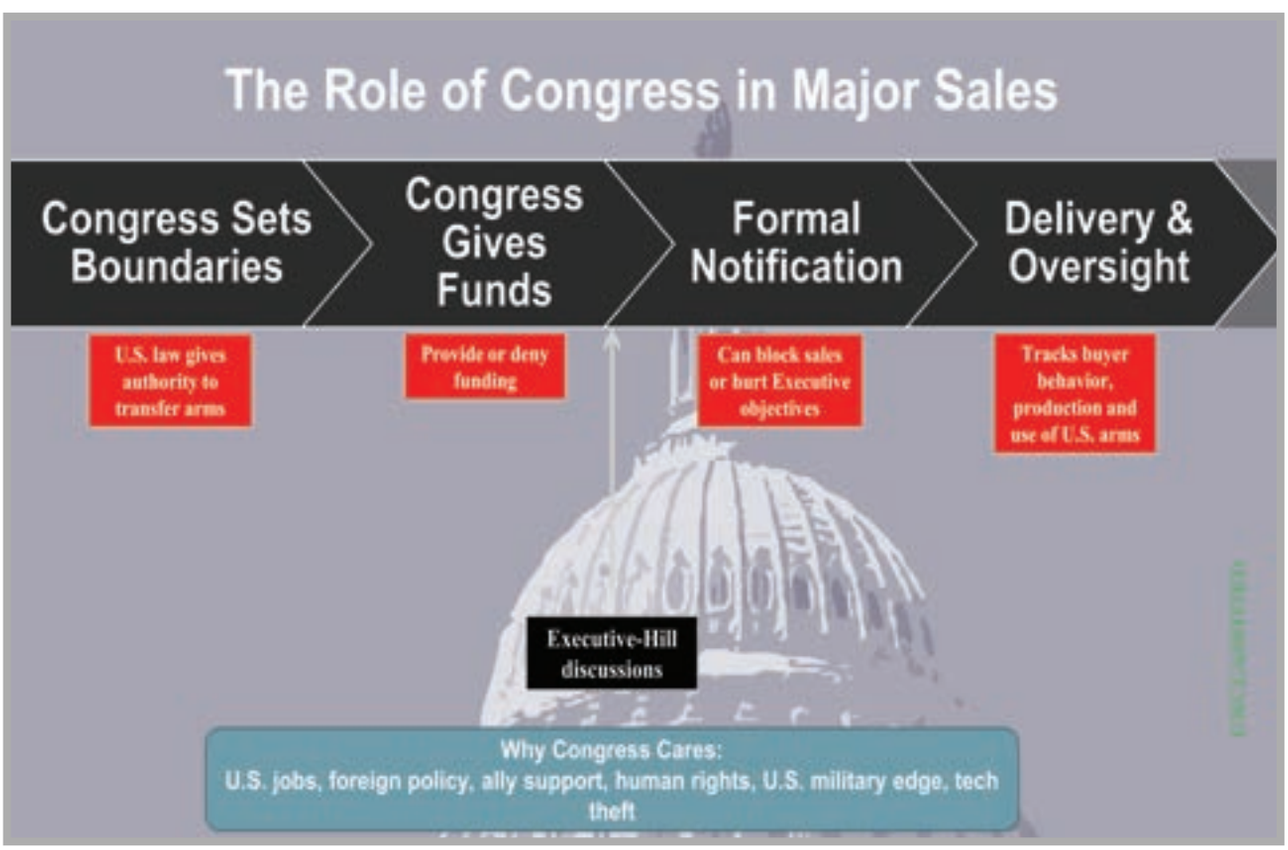

End-Use Monitoring
BLUF: FMS partner must agree with and adhere to set end-use agreements in order to complete FMS process and begin implementation. Partner is subject to end-use monitoring before, during, and after a transaction. Entities on a DCS license also agree to end-use monitoring before, during, and after a potential transaction.
End-Use Assurances:
FMS-LOA
DCS-Proviso in license
End-Use Monitoring
Formal: Golden Sentry (FMS) & Blue Lantern (DCS)
Informal: Information from any source
End-Use Violations: Under AECA Section 3, U.S. Department of State must notify Congress of any potential violation
i.e. selling defense articles with U.S. components to foreign entities that have NOT agreed to end-use requirements as outlined in original FMS or DCS case
UNCLASSIFIED


Directorate of Defense Trade Controls (DDTC)
Regulatory body for DCS
Outline requirements for obtaining licenses for sales
DDTC maintains compliance by partner country and contractor
Enforces Arms Export Control Act (AECA) & ITAR
Conducts end-use monitoring for DCS via Blue Lantern
Reports all potential violations of end-use to Congress in accordance with AECA section 3
UNCLASSIFIED

Role of Congress in Major Sales

- All FMS and DCS cases are reviewed by U.S. Department of State on a *case-by-case* basis.
- Congress plays a key role in the way in which FMS & DCS are conducted.
- Why does Congress care about FMS & DCS?
  - U.S. law dictates the way in which arms are transferred
  - Congress approves/denies funding
  - Congress reserves the right to block or alter objectives of the U.S. executive branch
  - Congress tracks buyer behavior, production, and use of U.S. arms

UNCLASSIFIED



Congressional Notification (ROK)

- 20-day Tier Review Period
- 15-day Formal Notification Period
- $25M Threshold (Major Defense Articles)
- $100M Threshold (Non-Major Defense Articles)
- $300M Threshold (MILCON)
- DCS ONLY - $1M Threshold on Small Arms

- **NOTE: All sales are subject to delays based upon whether Congress is in session**

UNCLASSIFIED

Conventional Arms Transfer (CAT) Policy

- **BLUF: All FMS & DCS cases are subject to scrutiny based on the guidelines outlined within the CAT Policy and are therefore subject to delays or cancellation if they do not meet guidelines**
- The CAT Policy provides a framework under which USG agencies review and evaluate proposed security sector assistance, government-to-government transfers, and licensed commercial sales of U.S. origin military equipment
- The revised CAT Policy notes that the U.S. will not authorize any transfer if we assess that it is "more likely than not" that the arms transferred will be used by the recipient to commit or facilitate the commission of human rights abuses.

- The CAT Policy aims to:
  - Build partner capacity
  - Support the U.S. defense industrial base
  - Bolster the U.S. military's technological edge
  - Strengthen foreign partnerships and increase interoperability
  - Prevent proliferation of weapons of mass destruction
  - Direct USG to work with partners to reduce the risk of civilian harm
  - Revitalize America's alliances by strengthening partners' ability to contribute to global security

UNCLASSIFIED

International Security Landscape

- The U.S. has delivered >$40 billion in military assistance to Ukraine
- Conflict in Ukraine has led countries to reevaluate their own security partnerships
- The U.S. continues to be a stalwart partner for peace and security across the globe
- The U.S.-ROK relationship has spanned 70 years as the U.S. has assisted in the defense of the southern peninsula through a constant military presence, as well as transfers of U.S. equipment and technologies to assist the ROK in its self-defense efforts
- As global threats continue to mount, we look forward to strengthening our security relationship with the ROK through the transfer of necessary military equipment and technology to pursue global peace initiatives

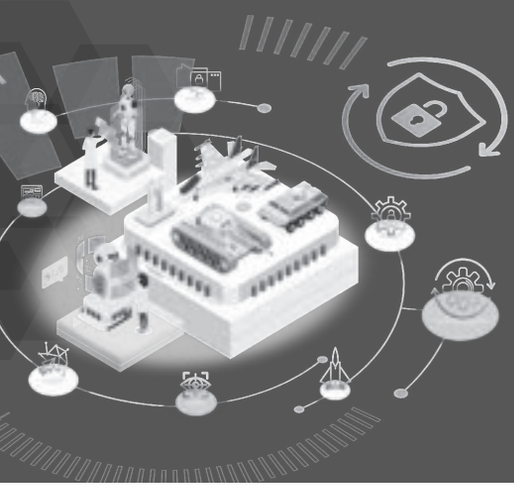
UNCLASSIFIED

Key Points

- The FMS and DCS processes are not overnight processes. There are many places in which the process may be snagged, delayed, or cancelled.
- The guidelines that outline defense trade controls are to protect the interests of the United States and its allies and partners
- We look forward to continuing a long, prosperous relationship with the Republic of Korea, and we thank you for your continued interest and support of global peace initiatives!

UNCLASSIFIED


Contact Information
PM/RSAT EAP/SCA Team:
Tammy Rutledge, Team Lead, RutledgeTJ@state.gov
Phil Davis, Foreign Affairs Officer, DavisPR@state.gov
PM/DDTC:
For Blue Lantern inquiries:
PM-DTCP-CEA@state.gov
DDTC Response Team:
DDTCCustomerService@state.gov
UNCLASSIFIED



주제발표 3.

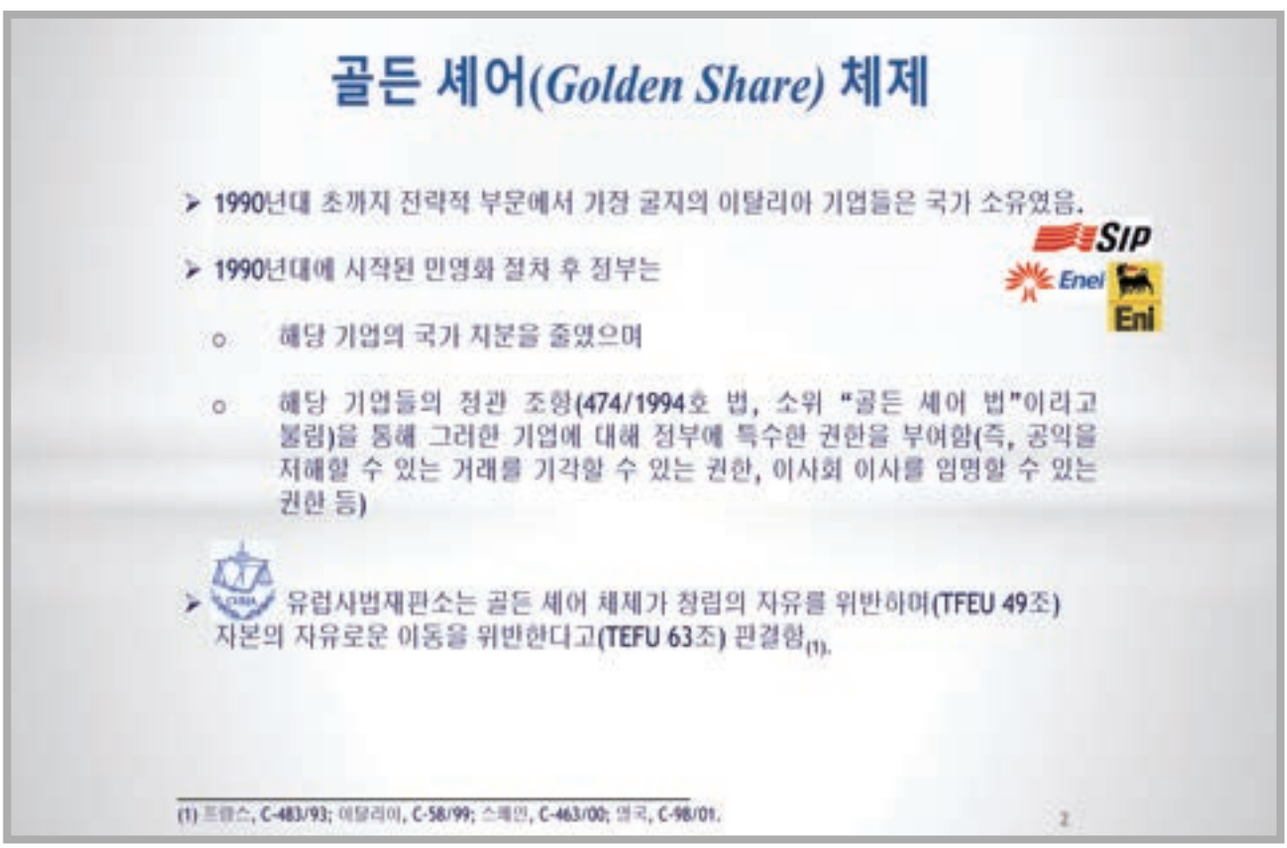
기술적 우위의 유지 방안 -
이탈리아의 골든 파워(Golden Power) 입법

Maintaining Technology Advantage -
Italian Golden Power Legislation

이탈리아 국방사무/국가군수국 과장 I **Lt.Col. Baldassare Bologna**
Section Leader, Secretariat General of Defence/National Armaments Directorate, Italy

Lt.Col. Baldassare Bologna


기술적 우위의 유지 방안—이탈리아의
골든 파워(Golden Power) 입법
Lt. C. Baldassare BOLOGNA
1


골든 셰어(Golden Share) 체제
➢ 1990년대 초까지 전략적 부문에서 가장 굴지의 이탈리아 기업들은 국가 소유였음.
➢ 1990년대에 시작된 민영화 절차 후 정부는
○ 해당 기업의 국가 지분을 줄였으며
○ 해당 기업들의 정관 조항(474/1994호 법, 소위 "골든 셰어 법"이라고 불림)을 통해 그러한 기업에 대해 정부에 특수한 권한을 부여함(즉, 공익을 저해할 수 있는 거래를 기각할 수 있는 권한, 이사회 이사를 임명할 수 있는 권한 등)
➢ 유럽사법재판소는 골든 셰어 체제가 창립의 자유를 위반하여(TFEU 49조) 자본의 자유로운 이동을 위반한다고(TEFU 63조) 판결함(1).
(1) 프랑스, C-483/93; 이탈리아, C-58/99; 스페인, C-463/00; 영국, C-98/01.
2

골든 파워(*Golden Power*) 체제

21/2012호 입법명령에 따라 "골든 세어" 체제를 "골든 파워" 체제로 교체함. 새로운 조항은 다음과 같음

- 정부는 법에 의해 부여된 **특수 권한**을 특정 **전략적 부문 및 자산**에 관련해서만 행사할 수 있다.
- 골든 파워 권한 행사 조건은 다음과 같다.
  - 명백히 사전 상황으로 정의되어야 함
  - 국익에 위협("실제 위협")이 되는 특정 상황으로 제한되어야 함
  - 객관적이어야 함
  - 비율에 맞아야 함
  - 차별적이지 않아야 함
- 골든 파워는 국영 혹은 민영기업과 관련없이 법에 의해 전략적 부문에서 운영하거나 전략적 자산을 보유한 모든 기업을 대상으로 행사될 수 있다.
- 정부에 의해 시행된 조치는 행정법원에 의해 법적 검토 대상이 된다.

3

법적 체계

- **21/2012호 입법명령**
  - DPCM 2014년 8월 6일
  - DPCM 108/2014호
  - DPCM 133/2022호
- **185/'90호 법 (*수출 규제*)**

- **투자 심사 관련 EU 규제 2019/452호**

투자 심사에 대한 국가 입법

4

적용 범위:
대상 거래 부문 및 유형 (1)

방위 및 국가안보 (1조)

- ITA/EU/비EU 기업에 의한 방위 및 국가안보 부문에서 전략적 사업을 진행하는 회사 지분 확보
- 회사 합병 혹은 합병 해체, 회사 혹은 해당 지사나 계열사의 이전, 해외에 등록된 사무소의 이전, 법인 목적 변경, 회사 해체, 투표권 관련 정관 개정, 유형 및 무형자산이나 그 사용권 판매 혹은 해당 자산의 사용에 영향을 미치는 규제 제정에 관련된 이사회 혹은 이해관계자 회의 결의안

5G 기술 (1-bis조)

5G 네트워크 설계, 시행, 유지보수 및 운영 관련 자산 및 서비스 구입, 또는 관련 첨단기술 부품 획득에 관한 비EU 기업과의 협의 종결

5

적용 범위:
대상 거래 부문 및 유형 (2)

에너지, 교통, 통신 및 첨단기술 부문 (2조)

- (법에 의해 명시된) 전략적 자산의 소유권, 통제, 사용, 가용성에 (간접적일지라도) 영향을 미칠 수 있는 ITA/EU/비EU 기업과의 결의안, 조치, 혹은 거래
- 회사 합병 혹은 합병 해제, 등록된 사무소의 해외 이전, 회사 해체, 투표권 관련 정관 수정, 회사 혹은 지사 이전에 관련된 ITA/EU/비EU 기업과의 결의안, 조치, 혹은 거래
- 전략적 자산의 담보 제공
- 비EU기업에 의한 지분 획득

첨단기술 부문은 2017년에 도입되었으며 필수 인프라(데이터 저장 및 처리, 금융 인프라 포함), 인공지능, 로봇공학, 반도체, 이중용도 기술, 네트워크 안보, 우주 및 핵 기술, 필수자원 공급망, 중요 정보 접근 및 통제를 포함함

6

골든 파워 조치

- 지분 획득 완화 조치 부과
- 지분 획득 차단
- 기업체 결의안 완화 조치 기각 혹은 부과
- 성사된 거래 기각

7

방위 및 국가안보

골든 파워 행사 조건

- 지분 획득 완화 조치 부과

  물자, 정보 안보, 기술 이전, 수출 통제를 보호하기 위해 필요할 경우

- 지분 획득 차단

  거래 후 구매자가 국가 방위 및 국가 안보 이익에 어긋나는 방향으로 투표권 비중을 직접 혹은 간접적으로 보유하게 될 경우

- 기업체 결의안 완화 조치 기각 혹은 부과

  관련 결의안(또는 그 기반이 되는 거래)이 이탈리아 국가 및 국제 방위의 안보에 영향을 미치는 상황을 야기할 수 있을 경우

8

에너지, 교통, 통신 및 첨단기술

골든 파워 행사 조건 (1)

- 성사된 기업체 결의안 완화 조치 기각 혹은 부과

  성사된 결의안, 조처, 혹은 거래로 인해 에너지 전파 그리드 운영, 에너지 발전소, 에너지 획득 지속성과 관련된 공익에 심각하고 실제적인 위험이 야기될 수 있을 경우

- 성사 거래 기각

  완화 조처 부과가 그러한 위험을 제한하기 위해 충분치 않을 경우

9

에너지, 교통, 통신 및 첨단기술

골든 파워 행사 조건 (2)

비EU 기업이 에너지, 교통, 통신 및 첨단기술 부문의 전략적 자산을 보유한 이탈리아 기업의 지분을 획득하며, 해당 획득으로 인해 **비EU 기업**에 해당 이탈리아 기업에 대한 통제력을 부여할 경우 정부는 다음과 같은 조처를 취할 수 있다.

- **완화 조치 부과**
- **성사 거래 기각**

권한 행사 조건

a) 국제법 원칙을 위반하거나 테러리스트 혹은 범죄 조직과 관계 있는 국가와 구매자 간 어떠한 관계의 존재 여부
b) 거래 시행으로 말미암아지는 구조가 에너지 획득 지속성과 에너지 네트워크 · 발전소 안보 및 운영을 보장하는 데 적절한지 여부

10

5G 기술

골든 파워 행사 조건

➢ 완화 조치 부과

해당 계약 혹은 협의에 네트워크 및 네트워크를 통해 전달되는 데이터의 진실성과 안보를 저해할 수 있는 취약성 요소의 여지가 있을 경우

➢ 성사 거래 기각

완화 조치 부과가 그러한 위험을 제한하기 위해 충분치 않을 경우

11

절차상 규칙 (1)

성사된 거래 고지

관련 기업은 결의/구입일 10일 내에 성사된 거래에 관해 정부(각료회의 행정조율부서)에 고지해야 함(의무 고지)

관련 기업(들)의 고지는 다음 사항을 포함해야 함

- 채택을 위해 기업체에 발송된 결의안
- 산업 프로젝트, 재정 계획, 획득 프로젝트의 상세한 설명, 구매자 개요
- 노동력에 대한 영향(있을 경우)
- 고지한 자의 신분증 사본
- 연락처로 지정된 법인

12

절차상 규칙 (2)

성사된 거래 평가

- «골든 파워 행사 조율 그룹»이라는 특정 위원회가 성사된 거래 평가를 담당함
- 조율 그룹은 다양한 부처 소속 위원으로 구성됨
  - 외무부
  - 내무부
  - 국방부
  - 재무부
  - 경제발전부
  - 인프라 교통부
  - 각료회의 유럽정책부서
  - 각료회의 경제정책 기획 및 조율 담당 부서
  - 각료회의 의장 군사 고문
  - 각료회의 의장 외교 고문

13

절차상 규칙 (3)

성사된 거래 평가

- 조율 그룹이 쟁점의 기반에 관한 주도 기관을 임명함
- 조율 그룹은 청문회를 위해 관련 기업을 소환할 수 있음
- 조율 그룹은 15영업일 내에 판결을 내려야 함
- 15영업일의 제한은 추가 정보를 요청하도록 최대 10일까지 1회에 한해 정지될 수 있음
- 평균 심사 기간은 12일임

14

절차상 규칙 (4)

최종 결정 및 법적 검토

- 주도 기관이 골든 의위 행사 관련 제안서 초안 작성
- 제안서 초율 그룹에 제출. 조율 그룹에서는 초안을 검토하고 최종 제안서가 토대로 할 의견을 낼 수 있음

- 최종 제안서 각료회의에 송부. 각료회의에서는 최종 제안을 통과, 수정, 혹은 기각할 수 있음
- 각료회의 의장령으로 최종 결정 내려짐

- 관련자들은 행정 재판소에서 최종 결정에 항소할 수 있음

15

절차상 규칙 (5)

최종 결정 및 법적 검토

- 각료회의 명령으로 감시 위원회 임명
- 감시 위원회는 필요하다고 판단될 경우 감시, 점검, 통제 시행
- 평균적으로 6개월마다 시행함

16

무효의 경우 및 처벌 조치

성사된 거래가 무효일 경우

정부의 조건에 위배되는 모든 성사된 거래는 무효이며, 정부는 상황의 복구를 지시할 수 있다. 이때 복구 비용은 위배자가 부담한다.

Civil 처벌 조치

고지 의무 위배 시

정부 부과 조치 위배 시

관련자는 최소 관련 회사 통합 매출액(최신 재무 제표에 따른 금액)의 1%에서 최대 거래액 2배까지 이를 수 있는 벌금을 지불한다.

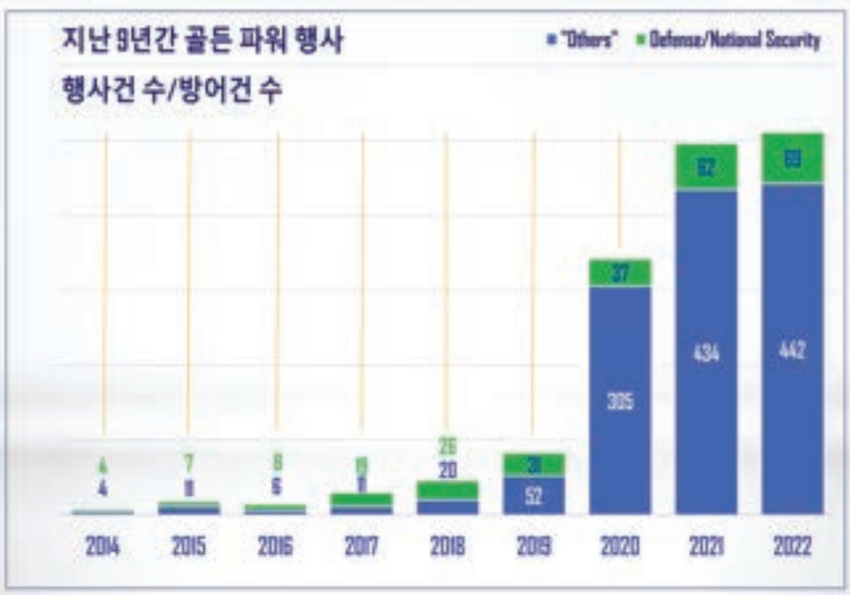
17

의회 연간 보고 (1)

각료회의 의장은 매년 조율 그룹에 포함된 부처의 도움을 받아 의회에 시행된 활동에 관한 보고서를 제출한다. 보고서는 특정 건 및 특수 권한 행사의 이유가 된 공익을 명시해야 한다.

18

연간 의회 보고 (2)



19

결론

- 매년 사건의 수 증가
- 방위 및 국가안보 "핵심 부문"
- 포괄적 접근
- 유럽 체계

20


2023 DEFENSE TECHNOLOGY SECURITY CONFERENCE
Defense Technology Protection and Export Control Strategies for Coping with Technological Advancement
Mantaining Technology Advantage:
Italian Golden Power legislation
Lt. C. Baldassare BOLOGNA
Italian Secretariat General of Defence/National Armaments Directorate
1


The "Golden Share" regime
Until the beginning of the 1990's, the most relevant Italian companies operating in strategic sectors were formally State-owned.
SIP
Enel
Eni
Following the privatization process, started in 1990's, the Government:
reduced the shares owned by the State into such companies;
provided the Government with special powers over such companies (e.g., the power to veto transactions that could impair relevant public interests; the right to appoint a member of the board of directors, etc.) through a provision in the companies' Articles of Association (Law no. 474/1994, so called "Golden Share Act").
The European Court of Justice ruled that golden share regimes violated the freedom of establishment (Art. 49 TFEU) and the free movement of capital (Art. 63 TFEU)(1).
(1) France, case C-483/93; Italy, case C-58/99; Spain,case C-463/00; the United Kingdom, case C-98/01.
2

The "*Golden Power*" regime

Legislative Decree no. 21/2012 replaced the "Golden Share" regime with the "Golden Power" regime. According to the new provisions:

- the Government can exercise the **special powers** provided by the Law only with reference to specific **strategic sectors and assets**;
- the conditions for the exercise of the golden powers are devised to be:
  - clearly defined *ex ante*
  - limited to certain specific situations that constitute a threat to the national interests ("Actual Threat")
  - objective
  - proportional
  - non-discriminatory
- the golden powers can be exercised over every company that operates in strategic sectors or owns strategic assets specified by the law, irrespective of its State or private nature;
- the measures implemented by the Government are subject to judicial review by the Administrative Court.

3

The Legal Framework

- **Legislative Decree no. 21/2012**
  - DPCM 6 August 2014
  - DPCM n. 108/2014
  - DPCM n. 133/2022
- **Law no. 185/'90 (*Export Regulation*)**

- **EU Regulation 2019/452 on Investments screening**

National legislation on Investment screening

4

Scope of application: sectors and types of covered transactions (1)

DEFENSE AND NATIONAL SECURITY (Art. 1)

- Acquisition of shares in companies engaged **in strategic activities** in the defense and national security sector by **ITA/EU/non-EU entity**
- Resolutions of the board of directors or of the shareholders' meeting concerning merger or demerger of companies, transfer of the company or branches thereof or subsidiaries, transfer of the registered office abroad, change of corporate purpose, dissolution of the company, amendment of the articles of association on the subject of voting rights, sales of property or use rights relating to tangible or intangible assets or the assumption of restrictions that affect their use

5G TECHNOLOGY (Art. 1-bis)

Conclusion of agreements with a **non-EU entity** concerning the purchase of goods and services related to the design, implementation, maintenance, and operation of 5G networks, and/or the acquisition of related high-tech components.

5

Scope of application: sectors and types of covered transactions (2)

ENERGY, TRANSPORT, COMMUNICATION and HIGH-TECH SECTORS (Art.2)

- resolutions, actions or transactions with ITA/EU/non-EU entity that may affect (even indirectly) ownership, control, use and availability of the strategic assets (identified by law);
- resolutions, actions or transactions with **ITA/EU/non-EU entity** concerning merger, demerger of the company, transfer abroad of the registered office, change of corporate purpose, dissolution of the company, modification of the articles of association on the subject of voting rights, transfer of the company or branches thereof;
- provision of strategic assets as collateral;
- acquisition of stakes by a **non EU entity.**

High-Tech sectors were introduced in 2017 and include, for example, critical infrastructure (including storage and handling of data and financial infrastructure), Artificial intelligence, robotics, semiconductors, dual use technologies, network security, space and nuclear technology, supply chain of critical resources, and access and control of critical information.

6

The Golden Powers Measures

- Imposition of mitigation measures on the acquisition of shares
- Block of the acquisition of shares
- Veto/Imposition of mitigation measures on resolutions of corporate bodies
- Veto the covered transaction

7

Defense and National Security

Golden Powers and exercise criteria

- Imposition of mitigation measures on the acquisition of shares

  If necessary to safeguard supplies, security of information, transfer of technology and export controls

- Block of the acquisition of shares

  If, following the transaction, the purchaser would directly or indirectly hold a percentage of the voting capital such as to prejudice national defense and national security interests

- Veto/Imposition of mitigation measures on resolutions of corporate bodies

  If the relevant resolution (and/or the underlying transaction) may trigger a situation affecting the safety of the Italian national and international defense

8

Energy, Transport, Communication and Hi-Tech

Golden Powers and exercise criteria (1)

- Imposition of mitigation measures on covered resolutions of corporate bodies

  If the covered resolution, action or transaction may give rise to serious and actual risks for the public interest in connection with the operation of the energy transmission grids, energy plants and the continuity of energy procurements

- Veto the covered transaction

  When the imposition of mitigation measures would not be sufficient to limit such risks

9

Energy, Transport, Communication and Hi-Tech

Golden Powers and exercise criteria (2)

When **NON-EU** entities acquire shares of an Italian company owning strategic assets in the fields of energy, transport, communication and hi-tech, and that acquisition grants the NON-EU entity the control over the Italian company, the Government can:

- **Impose mitigation measures**
- **Veto the covered transaction**

Criteria for the exercise

a) the existence of any relationship between purchaser and countries that that violate principles of international law or that have relationships with terrorists or criminal organizations
b) whether the structure resulting from the implementation of the transaction is appropriate to ensure the continuity of the procurements, and the security and operations of energy networks and plants

10

5G Technology

Golden Powers and criteria for the exercise

- **Imposition of mitigation measures**

  If the contract/agreement has elements indicating the presence of vulnerability factors that could compromise the integrity and the security of networks and data passing through them

- **Veto the covered transaction**

  When the imposition of mitigation measures would not be sufficient to limit such risks

11

Procedural Rules (1)

Notice of the covered transaction

The concerned company shall notify the Government (Presidency of the Council of Ministers - Department for administrative coordination) the covered transaction within 10 days of the date of the resolution/purchase (**mandatory notice**).

The Notification by the concerned Entity/ies must contain:

- the resolution sent to the corporate body for its adoption
- industrial project, financial plan, detailed description of the acquisition project, profile on the purchaser
- impact on labor force, if any
- ID copy of the subscriber of the notification
- Designation of legal person as POC

12

Procedural Rules (2)

Assessment of the covered transaction

- A specific Committee, the «*Coordination Group for the exercise of golden powers*», is the body in charge of the assessment of the covered transactions.
- The Coordination Group is composed by members by various administrations:
  - Ministry of Foreign Affairs and International Cooperation;
  - Ministry of Interior Affairs;
  - Ministry of Defense;
  - Ministry of the Economy and Finance;
  - Ministry of Economic Development;
  - Ministry of Infrastructure and Transport;
  - Department for European policies of the Presidency of the Council of Ministers;
  - Department for planning and coordination of the economic policy of the Presidency of the Council of Ministers;
  - Military Adviser to the President of the Council of Ministers;
  - Diplomatic Adviser to the President of the Council of Ministers.

13

Procedural Rules (3)

Assessment of the covered transaction

- The Coordination Group appoints the lead agency on the basis of the matter at issue
- The Committee may call the concerned Entities for an hearing
- The Committee shall deliberate on the issue within 15 working days
- The deadline of 15 working days can be suspended only once up to maximum 10 days to request additional information
- The average of the screening timeframe is 12 days

14

Procedural Rules (4)

Final decision and judicial review

- The lead agency drafts a proposal concerning the exercise of golden powers;
- The proposal is submitted to the Coordination Group that can release observations, on the ground of which the final proposal is taken;

- The final proposal is transmitted to the Council of Ministers that can confirm, modify or reject the final proposal
- The final decision is taken by a Decree of the President of the Council of Ministers

- The parties can challenge the final decision before the Administrative Court

15

Procedural Rules (5)

Final decision and judicial review

- A monitoring Committee is appointed by decree of the Council of Ministers
- The Committee carries out inspection, examination, control when it consider necessary
- On average every 6 months

16

Invalidity and Penalties

Invalidity of the covered transaction

Any covered transaction carried out in violation of the Government's terms and conditions is null and void, and the Government may mandate the reinstatement of the situation at one's expenses.

Civil penalties

in case of violation of the of the notification obligations

in case of violation of the of the measures imposed by the Government

the concerned party shall pay amount of the fine ranges from a minimum of 1% of the consolidated turnover of the concerned company (as resulting from the latest financial statements) to a maximum of twice the value of the transaction

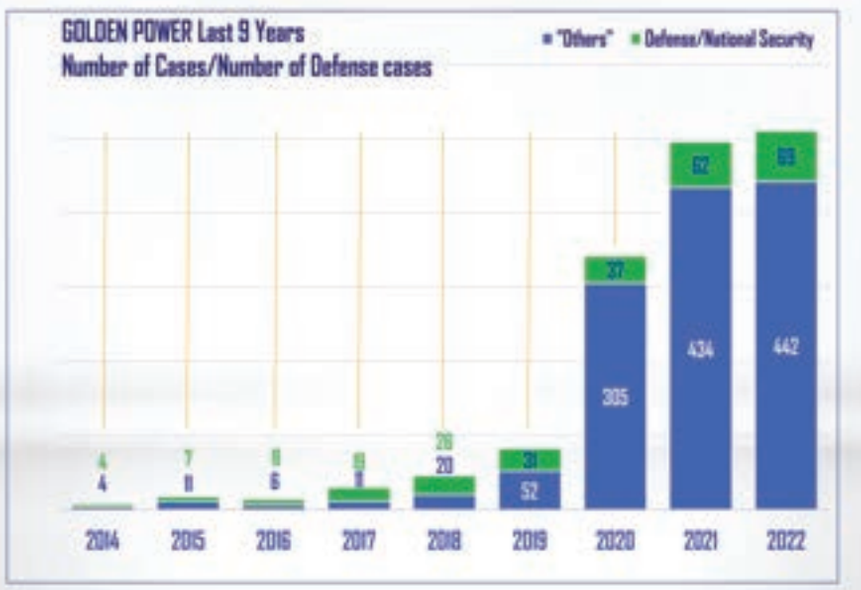
17

Annual Report to the Parliament (1)

On an annual basis, the President of the Council of Ministers, assisted by the Administrations involved in the Coordination Group, shall transmit to the Parliament a report on the activities carried out with particular reference to specific cases and public interests that motivated the exercise of special powers.

18

Annual Report to the Parliament (2)

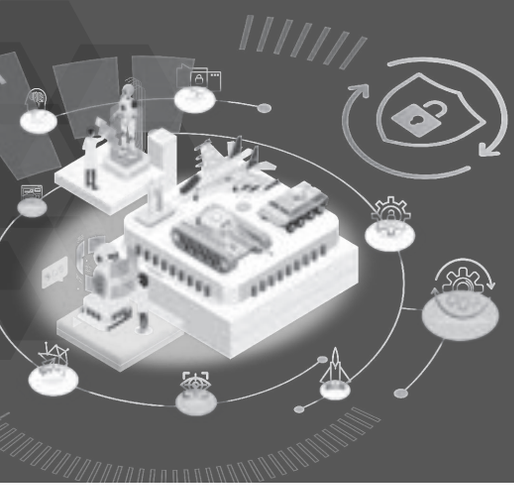


19

Conclusions

- Increase in cases year on year
- Defense and National Security "core Sector"
- Comprehensive approach
- European Framework

20



주제발표 4.

신기술 발전과 수출통제 및 규범 정립

Establishment of Export Control and Norms in Response to the Advancement of New Technologies

외교부 수출통제·제재담당관실 외무서기관 I **이혜진**
Deputy Director, Export Control and Sanctions Division,
Ministry of Foreign Affairs
Ms. Hyejin Lee

내외 귀빈 여러분, 안녕하십니까?
2014년 이래 우리 방위사업청이 매해 개최해 온《방산기술보호 국제컨퍼런스》금년도 회의에 참석하게 되어 영광입니다.
특히 올해는 '기술고도화 대응을 위한 방산기술보호와 수출통제 전략'이라는 시의적절한 주제 하에 회의가 개최되는 만큼, 더욱 실천적이고 정책 함의가 풍성한 논의가 이뤄질 것으로 기대가 됩니다.

(신흥기술 발전과 정책 환경 변화)
오늘날 자율살상무기(LAWS) 체계, 사이버 무기, 우주공간의 전장화, 인공지능(AI)의 발전 등은 그 자체만으로, 또는 기존의 재래식 전쟁 수단과의 결합을 통하여 이미 현대전의 성패를 가르는 수단으로 자리 잡았다 하여도 과언이 아닐 것입니다.

신흥·첨단기술의 빠른 발전에 따른 이러한 변화는 급변하는 국제 안보환경 속에서 각국의 안보 위협 인식을 높이고, 국방 및 안보 정책에 있어 기술 보안/기술 안보를 점차 중요한 고려 요소로 만들고 있습니다.

고사양 AI 학습용 반도체칩 및 이를 설계·생산하는데 필요한 장비, 무인무기체계 훈련용 데이터셋을 운용할 정도의 수퍼컴퓨팅 능력에 대한 전략 경쟁 상대의 접근을 차단하는 것이 정책 수단이 아닌 정책 목표가 되고 있습니다. 신기술을 이용한 무기체계가 빠르게 진화하고 있는 만큼, 방산기술보호 패러다임 또한 급속도로 전환하고 있습니다.

(수출통제의 정책적 중요성 및 범주 확대)
이러한 변화에 대응하여 주요 첨단기술 보유국 정부 및 방산 분야는 공히 두 가지 방책을 동시에 강구하기 위해 나섰습니다. 첫째는 기술격차 확대를 위한 일련의 연구개발 장려 정책의 강화입니다. 보다 중요한 두 번째는 안보적인 우려가 있는 상대 국가의 기술 추격 내지 직·간접적 방식을 동원한 기술 획득을 막기 위한 각종 수단의 강화입니다.

특히 이 두 번째 차원에서, 종래 국제 비확산 규범을 강화하는 수단으로서 기능하여 왔던 미사일기술통제체제(MTCR), 바세나르체제 등 다자 수출 통제체제 및 무기거래조약(ATT)에도 점차 국가안보 내지 인권 침해 목적 사용 가능성 등 비확산에 국한되지 않은 사유에 입각한 품목 및 기술 심의와 통제를 면밀히 하자는 새로운 역할이 부여되거나, 그 부여 필요성이 갈수록 중요하게 논의되고 있습니다.

기술경쟁 시대에 다자·양자 수출통제 정책이 점차 주요국의 핵심 외교 정책 수단으로 부각되고 있는 것입니다.

다자적인 통제기제가 원활하게 작동하지 않을 경우 인식을 공유하는 국가들 간의 공조에 입각한 타개책을 모색하고, 수출통제 조치 보다 폭넓게 적용될 수 있는 이중용도 연구(DURC), 자본 투자 및 인적 교류 관련 조치도 검토해 나가자는 흐름이 대두하고 있으며, 우리 방산기술보호 법령 및 정책에서 보시듯 방산기술 분야도 예외가 아닙니다.

(신흥기술의 책임있는 군사적 이용을 위한 국제 규범 정립 노력)
신흥기술의 활용과 규제에 대한 각국의 인식이 다른 만큼, 신흥기술 발전에 수반되는 필연적 위험성에 공동 대응하자는 국제사회의 규범 논의는 그 진전이 매우 더딘 상황입니다. 그러나, 신흥기술 혁신의 불가결한 기반인 인공지능 및 첨단 컴퓨팅 능력 관련, AI의 '군사적인 측면의 이용'에 있어서 만큼은 악의적 파급효과를 막기 위한 책임 있는 이용 원칙⊠규범을 정립하자는 논의를 현재 한국, 미국 및 네덜란드 등 몇몇 국가가 선도하고 있습니다.

인공지능의 책임 있는 군사적 이용에 관한 원칙과 모범 관행 정립 및 공유에 관해 정부, 산업계, 학계 등을 아우르는 논의의 장을 제공하고 있는 'REAIM' 회의가 금년 초 한국과 네덜란드 공동 주최로 네덜란드에서 개최되었으며, 제2차 회의는 내년 중 한국에서 개최될 예정입니다. 오늘 자리하신 방산 분야 우리 업계 차원의 적극적인 참여 및 입장 개진이 회의의 실질적인 성공을 결정하는 중요한 부분인 만큼, 많은 참여를 부탁드립니다.

(신흥기술 발전에 따른 정책에 있어 민관 협력의 중요성)
점차 중요해지는 신기술 관련 수출통제 정책을 입안하고 총괄 시행하는 부서로서, 저희 외교부 수출통제제재담당관실은 입안되는 정책이 실질적으로 기업들의 혁신을 지원하고, 기술 우위를 보호하며, 동시에 외교적 목표 및 국가 안보를 강화하는 방향으로 나아갈 수 있도록 하는데 최우선적인 중요성을 부여하고 있습니다.

또한 이를 이행하는 데 있어, 기술혁신을 일궈온 주체인 산업계와 정부간의 긴밀한 소통과 관여의 중요성을 절감하고 있습니다.

산업계와의 관여가 긴요한 분야 중 하나는 재래무기의 불법 국제이전을 방지하기 위한 국제 수출통제 조약 체계인 무기거래조약(ATT)입니다.

무기거래조약은 방산기술이 아닌 미사일, 군함, 전투기, 탄환 같은 재래식 무기 이전을 통제하는 규범이 아닌가 아마도 생각하실 것입니다. 그러나, 신기술이 재래무기와 결합될 때 낳을 수 있는 파급적 효과를 감안한다면, 우리가 막으려는 방산기술 유출 위험과 무기거래조약이 규제하려는 불안정 세력으로의 무기 유입 및 전용 위험은 궤를 같이 합니다.

이러한 점에 착안하여 우리 정부는 지난 수 년간 무기거래조약 관련 다자 논의에 적극적으로 참여하여 왔습니다. 그 역할을 국제사회로부터 인정받아, 작년 8월부터 무기거래조약 의장국을 수임하여 “책임있는 국제 무기 이전을 위한 산업계의 역할”에 대한 논의를 주도하고 있습니다.

우리가 특히 이 의제를 선정하게 된 것은, 현장의 최일선에서 무기 및 방산기술 이전에 관한 모범적인 관행 정립을 선도해 나가고 있는 우리 산업계와의 소통 및 정보 공유 없이는 실효적인 수출통제 규범은 가능하지 않다는 인식이 있었기 때문입니다.

아울러, 주요국 정부가 속속들이 도입하는 수출통제 및 첨단기술 보호 조치들이 산업계에 미치는 영향과 기업들의 이행 준수 의무 부담이 커지는 가운데, 방산업계의 이익과 예측가능성이 담보될 수 있도록 산관 협력을 증진할 필요성도 크게 작용하였습니다.

지금까지 말씀드린 사항을 바탕으로 방산기술보호에 관한 오늘 컨퍼런스에 참석해 주신 모든 분들께 상호 지속적인 소통 및 관여가 긴요하다는 점을 다시금 강조드리고자 합니다.

특히, △정부가 방산업계의 전략적 이해를 고려하고 국제 규범 논의 및 다자 수출통제체제 신규 통제품목 논의시 이를 반영하는 일, △산업계가 방산물자의 국제 이전시 높은 자율준수 책임을 가지고 관련 규정을 이행해 나가는 일, △인권 관련 주의의무 이행 등을 기반으로 신뢰할 수 있는 방산수출 주체로 평가받고 비확산 규범 강화에 기여하는 일 등에 있어 정부와 민간의 소통이 점점 중요해지고 있습니다.

정부는 방산업계와의 소통 확대에 열려 있으며, 신기술이 이끌어가는 안보환경 변화 속에서 산업계와의 협력을 기반으로 우리 독자적인 차원 및 한미동맹 공조 하의 첨단 방산기술 보호 및 기술혁신 투자 확대를 성취해 나가기를 기대합니다.

감사합니다.

Distinguished Guests, greetings.

It is an honor to participate in this year's Defense Technology Security Conference, which Defense Acquisition Program Administration DAPA has been hosting each year since 2014.
Especially since this year's theme is the timely topic of "Defense Technology Security and Export Control Strategy in Responding to Technological Advancement," I am looking forward to engaging in practical discussions with rich policy implications.

(Advances in Emerging Technology and Changes in Policy Environment)
It is not an exaggeration to say that today's Lethal Autonomous Weapons systems, cyberweapons, space turning into a battlefield, and advances in AI have already been established as a means of determining the fate of modern warfare, either in themselves or in combination with existing conventional arms.

These changes, borne out of rapid developments in emerging and advanced technology, heighten the awareness of security threats for countries around the world in the volatile international security environment and render technology security an increasingly important aspect of consideration in defense and security policies.

It is now a goal of policies, not a means, to deny access to supercomputing capacities enough to operate a dataset to train unmanned weapon systems, highly sophisticated semiconductors for AI learning, and equipment necessary to design and produce these chips for strategic competitors. As weapon systems using new technology are rapidly evolving, the paradigm of defense technology security is transitioning at a breakneck pace as well.

(The Strategic Importance and Expanding Categories of Export Controls)
In response to these changes, governments in possession of advanced technologies and the defense sector are seeking to devise two courses of action at once. The first is to strengthen a series of policies to encourage R&D in order to widen the technological divide. The second, which is more important, is to strengthen various means to prevent certain countries with security risks from catching up on or acquiring technology directly or indirectly.

Especially in regard to the second course of action, new responsibilities to fine-tune evaluations and controls of items and technologies that are based upon reasons not confined to non-proliferation, such as for the possible purpose of violating national security or human rights, are being conferred or being discussed as necessary to be conferred, on multilateral export control regimes, such as the Missile Technology Control Regime and the Wassenaar Arrangement, which have previously functioned to reinforce international non-proliferation norms.

Thus, multilateral and bilateral export control policies are increasingly being emphasized as key foreign policy tools for major countries in this era of technological competition.

In the same vein, a trend is emerging to seek a solution based on the coordination of countries with common perceptions, as well as reviewing Dual Use Research of Concern and measures concerning capital investment and human resource exchanges that can be applied more broadly than export controls if a multilateral control mechanism does not function smoothly.

And as you can see from our laws and policies for defense technology security, the defense security sector is also not an exception.

(Efforts to Establish International Regulations for the Responsible Military Use of Emerging Technology)
Since each country has differing perceptions on the use and regulation of emerging technology, progress is slow regarding international regulations to jointly respond to the inevitable dangers that developments in emerging technology entail. However, the Republic of Korea, the United States of America, the Netherlands, and a few other countries are leading discussions to establish responsible use principles and norms to prevent malicious ramifications in terms of "the military use" of AI, regarding AI and advanced computing capacities that are the indispensable foundation of innovations in emerging technology.

The Responsible Artificial Intelligence in the Military Domain Summit, which provides a platform for discussions on establishing and sharing principles and best practices for the responsible military use of AI for governments, industries, and academia, was held in the Netherlands earlier this year with Korea and the Netherlands as co-hosts. The second summit is set to be held in Korea next year. I encourage all of you to take part in this summit, as the defense industry's active participation and expression of opinions are critical factors that will determine the tangible success of the conference.

(The Importance of Public-Private Partnerships in Policies in Response to the Advancement of Emerging Technology)
The Export Control and Sanctions Division of the Korean Ministry of Foreign Affairs; which develops, oversees, and executes export control policies regarding increasingly important new technologies; prioritizes the practical support of innovation for companies, protection of technology advantages, and the reinforcement of diplomatic goals and national security in the policies we draft.

In implementation, we are keenly aware of the importance of close communication and mutual involvement between the government and the industry, which has been a principal agent in technological innovation.

One of the fields in which cooperation with the industry is essential is the Arms Trade Treaty, an international treaty to prevent the illegal international transfer of conventional arms.

You may think that the ATT regulates conventional weapon transfers, such as missiles, warships, combat planes, and ammunition, not defense technology. However, considering the far-reaching impacts that could occur when new technology is combined with conventional arms, the defense technology leakage risk we are trying to prevent, and the risk of weapon outflow and diversion to unstable forces that the ATT regulates, are in parallel.

For this reason, our government has actively participated in multilateral discussions regarding the ATT for the past several years. The international community has recognized our efforts, and since last August, Korea has assumed the ATT presidency, leading discussions regarding "the Role of Industry for Responsible International Transfer of Conventional Arms."

This particular theme was selected based on our awareness that a realistic export control regime is impossible without communicating and sharing information with the industry, which is leading the establishment of best practices for weapon and defense technology transfers in the frontiers of the field.

Furthermore, as major countries' implementation of export control and advanced technology security measures have an increasing impact on the industry, and as companies are more pressured to comply with these measures, the need to promote cooperation between the industry and government in order to ensure the profits and predictability of the defense industry was an important factor as well.

Based on what I have explained so far, I would like to emphasize again the urgent need for continuous mutual communication and participation of all the guests who have joined us for today's Defense Technology Security Conference. In particular, public-private communication is becoming increasingly important for various reasons:

First, the government must consider the defense industry's strategic interests and take them into account when discussing international regulations and new items to be controlled by the multilateral export control regime.

Second, the industry must comply with relevant regulations with a high sense of responsibility in the international transfer of defense goods.

And third, the industry needs to be recognized as a reliable defense exporter based on the implementation of human rights due diligence and reinforcement of the non-proliferation regime.

The government is open to expanding communication with the defense industry, achieving advanced defense technology, and increasing investments for technological innovation, both on our own terms and under the alliance between Korea and the U.S., based on cooperation with the industry amid changes in the global security environment spearheaded by new technology.

Thank you.

2023 Defense Technology Security Conference 2023 방산기술보호 컨퍼런스

SESSION 2

첨단 방위산업의 발전과 수출, 그리고 기술보호

Advancement, Export, and Technology Security of Cutting-Edge Defense Industries

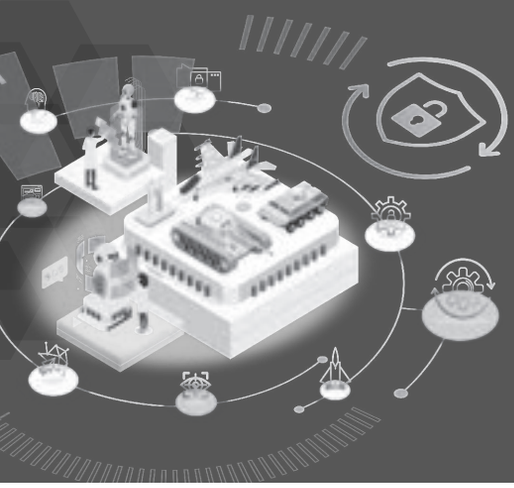
---

한국 방위산업기술 보호·수출통제 정책 및 법령 소개
Defense Technology Security & Export Control Policy of ROK

방산기술수출, 단계별 주요 이슈
Defense Technology Export and Key Issues

방산기술보호를 위한 기술적 대책 및 절차
Technical Measures and Procedures for Defense Technology Protection

국제 수출통제제도 경향과 기술보호 측면의 시사점
Trends in International Export Control Regimes and Implications for Technology Protection



2023 Defense Technology Security Conference 2023 방산기술보호 컨퍼런스

주제발표 1.

한국 방위산업기술 보호·수출통제 정책 및 법령 소개

Defense Technology Security & Export Control Policy of ROK

방위사업청 기술보호과장 I **김주철**

Director, Defense Technology Security Division, DAPA

Mr. Joochul Kim

한국 방위산업기술 보호·수출 통제 정책 및 법령 소개

2023. 8. 3.

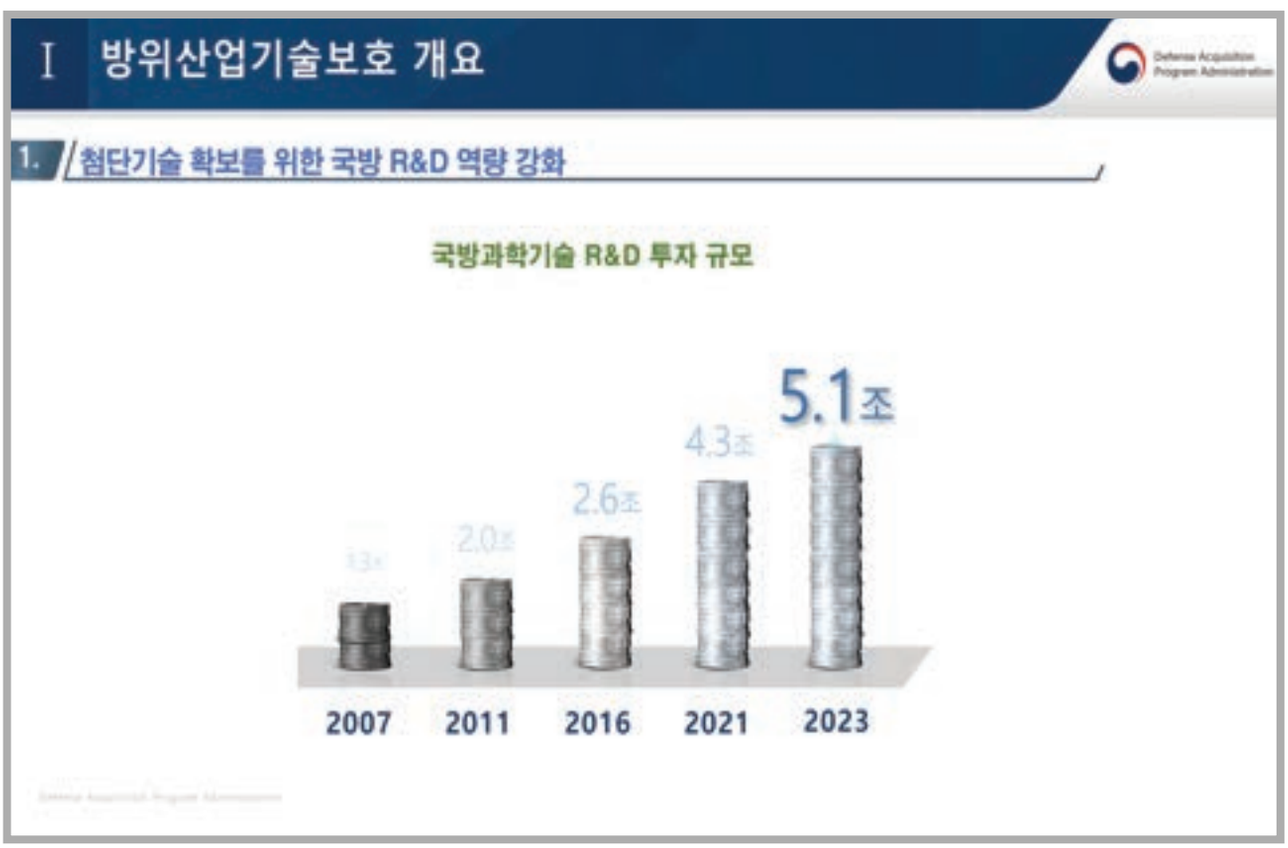
Defense Acquisition Program Administration

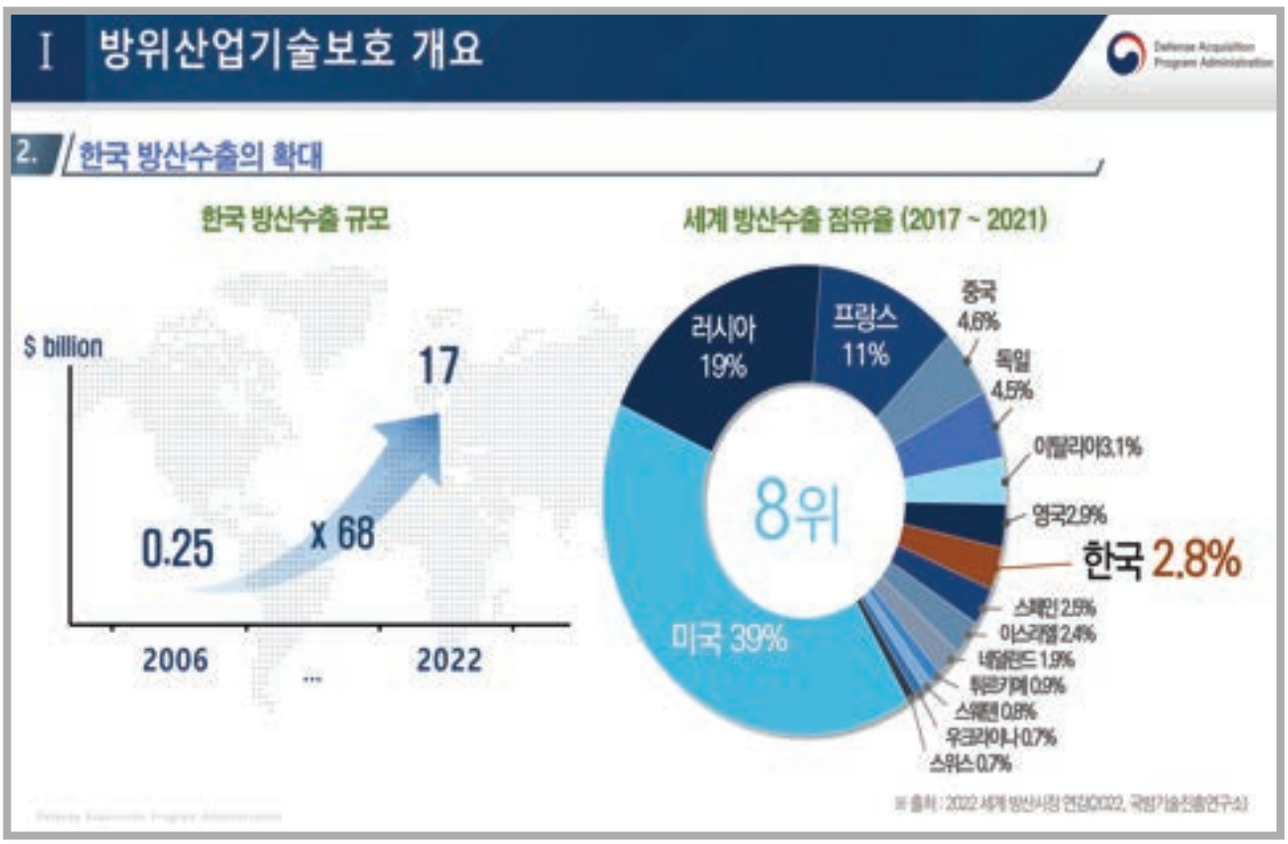
1

INDEX

Defense Acquisition Program Administration


Ⅰ. 방위산업기술보호 개요
Defense Acquisition
Program Administration


Ⅰ 방위산업기술보호 개요
1. 첨단기술 확보를 위한 국방 R&D 역량 강화
국방과학기술 R&D 투자 규모
5.1조
4.3조
2.6조
2.0조
2007
2011
2016
2021
2023


I 방위산업기술보호 개요
2. 한국 방산수출의 확대
한국 방산수출 규모
$ billion
17
x 68
0.25
2006
...
2022
세계 방산수출 점유율 (2017 ~ 2021)
러시아 19%
프랑스 11%
중국 4.6%
독일 4.5%
이탈리아 3.1%
영국 2.9%
한국 2.8%
스페인 2.5%
이스라엘 2.4%
네덜란드 1.9%
튀르키예 0.9%
스웨덴 0.8%
우크라이나 0.7%
스위스 0.7%
8위
미국 39%


I 방위산업기술보호 개요
3. 첨단기술 획득에 따른 한국 무기체계의 고도화
KF-21
Surion
C-Star
K2
K9
Jangbogo


Ⅰ 방위산업기술보호 개요
4. 증대되는 방산기술 유출 위협
내부자 자료 유출
외부 사이버 공격


Ⅱ. 국방기술보호국 소개
Defense Acquisition
Program Administration

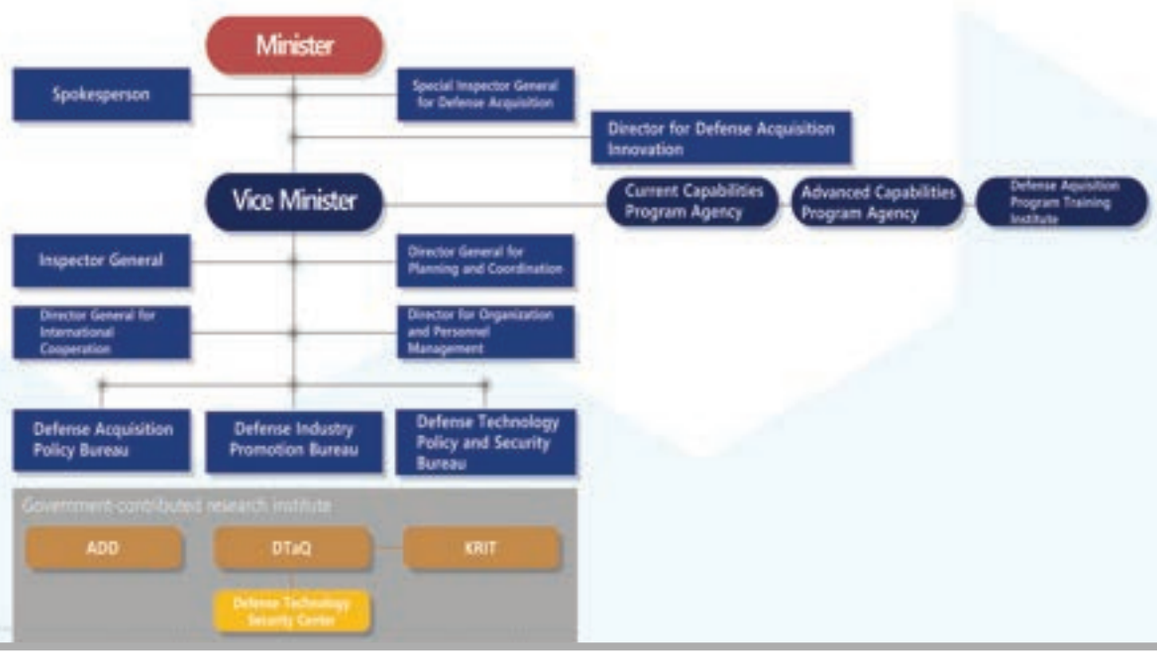
Ⅱ 국방기술보호국 소개

1. 한국 방산기술보호 발전의 역사

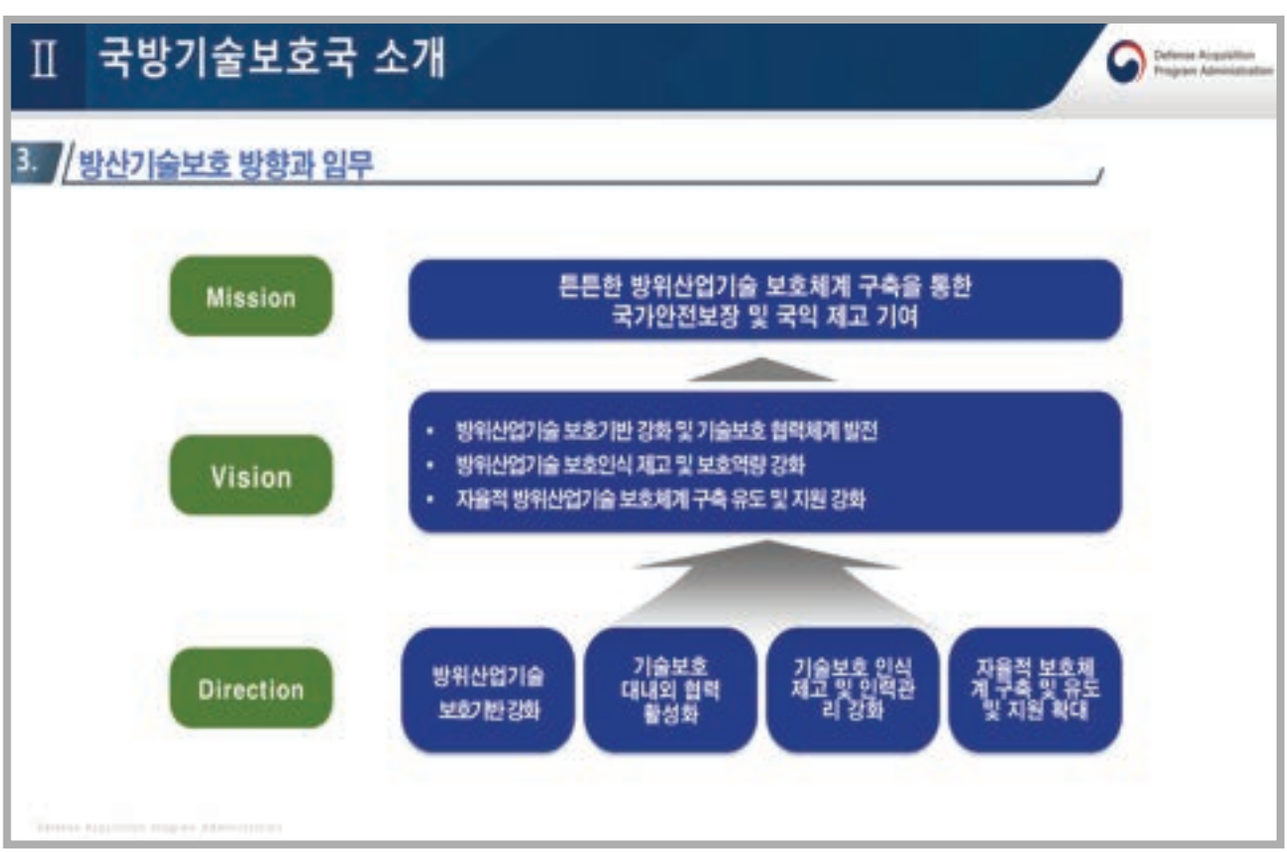
- 전략물자 수출입 허가 제도 도입 : 1989
- 4대 국제 수출통제 체제 가입 : 2001
  - * 바세나르 체제(WA), 미사일 기술 통제 체제(MTCR), 호주 그룹(AG), 핵 공급국 그룹(NSG)
- 방위사업청 설립 : 2006
- 방산기술통제관 신설 : 2012
- 「방위산업기술보호법」 제정 : 2015
- 무기거래조약(ATT) 가입 : 2017
- 방산기술통제관 → 국방기술보호국 조직 개편 : 2018
- 기품원 內 방산기술보호센터 신설 : 2022

Ⅱ 국방기술보호국 소개

2. 방위사업청 조직도




Ⅱ 국방기술보호국 소개
2. 방위사업청 조직도
Minister
Spokesperson
Special Inspector General for Defense Acquisition
Director for Defense Acquisition Innovation
Vice Minister
Current Capabilities Program Agency
Advanced Capabilities Program Agency
Defense Acquisition Program Training Institute
Inspector General
Director General for Planning and Coordination
Director General for International Cooperation
Director for Organization and Personnel Management
Defense Acquisition Policy Bureau
Defense Industry Promotion Bureau
Defense Technology Policy and Security Bureau
Government-connected research institute
ADD
DTaQ
KRIT
Defense Technology Security Center
Defense Technology Policy Division
• 방위사업청 소관 기술의 관리에 관한 업무
• 국방과학기술혁신에 관한 시행계획 수립
• ADD 운영에 대한 지도·감독
Defense Technology Security Division
• 방위산업기술 보호 관련 정책의 수립 및 제도 개선
• 방위산업기술 지정 변경 해제 및 관정
• 방위산업기술의 보호를 위한 실태조사 시행
Defense Technology License & Control Division
• 전략물자 관정 및 수출 허가
• 방위산업물자 및 국방과학기술 등의 수출허가·승인
• 수입물품의 최종사용자 증명에 관한 업무
Defense Technology Innovation Division
• 핵심기술개발 사업계획 수립과 사업 조정·통제·관리
• 국방과학기술 정보관리업무
• ADD, DTaQ 기술 기획 및 사업에 대한 지도·감독


Ⅱ 국방기술보호국 소개
3. 방산기술보호 방향과 임무
Mission
튼튼한 방위산업기술 보호체계 구축을 통한
국가안전보장 및 국익 제고 기여
Vision
• 방위산업기술 보호기반 강화 및 기술보호 협력체계 발전
• 방위산업기술 보호인식 제고 및 보호역량 강화
• 자율적 방위산업기술 보호체계 구축 유도 및 지원 강화
Direction
방위산업기술 보호기반 강화
기술보호 대내외 협력 활성화
기술보호 인식 제고 및 인력관리 강화
자율적 보호체계 구축 및 유도 및 지원 확대

Ⅱ 국방기술보호국 소개

4. 방산기술보호센터 (국방기술품질원)

국방기술품질원 DTaQ

방산기술보호센터

- 방산분야 사이버 위협에 대한 사고대응·진단, 보안관제 및 기술통제 등의 집행업무를 수행하기 위한 전문기관 설립 ('22.7월)
- (사고대응·진단) 방산업체 사이버 침해 사고 발생시 보안전문가를 통한 초기 대응조치, 사전예방을 위한 컨설팅 및 유관기관 협력 실시
- (기술통제) 안전한 연구개발과 방산수출을 위한 방위산업기술 판정 및 수출허가 심사 지원
- (기타 지원) 통합실태조사, 중소·중견기업 지원 사업, 방위산업기술 보호교육 등 기술보호 지원업무 수행

Ⅲ. 기술보호 법령 및 정책

Defense Acquisition
Program Administration

Ⅲ 기술보호 법령 및 정책

1. 「방위산업기술 보호법」 제정 배경

목 적

▲ 방위산업기술 체계적 보호 ▲ 관련 기관 지원 ▲ 국제조약 등 의무 이행

➡ 경제 국가 안전 보장, 국가신뢰도 제고

대내외적 기술보호 강화

- 국가 안보자산 및 전략적 경제 자원으로서의 방위산업기술 인식 전환
- 세계 각국은 자국 방산기술 보호 및 수출 통제 강화 중

방위산업 경쟁력 기반

- 방산수출 증가, 기술수준 향상에 따른 기술유출 위협 증가
- 해외시장에서 국내기업 경쟁력 확보 및 잠재적 수출시장 보호

Ⅲ 기술보호 법령 및 정책

2. 「방위산업기술 보호법」 제15조 국제협력

법 제15조(국제협력)

정부는 방위산업기술의 보호에 관한 국제협력을 촉진하기 위하여 수출입 대상국가와 협력체계 구축, 전문인력 교류 등 필요한 사업을 추진할 수 있다.

시행령 제20조(국제협력 사업의 범위)

법 제15조에 따라 국제협력이 필요한 사업은 다음 각 호와 같다.

- 방위산업기술 보호를 위한 국제적 차원의 협력체계 구축사업 및 기술보호 제도·정책 공유
- 방위산업기술 보호를 위한 기술적 방법에 대한 국제적 조사·연구
- 방위산업기술 보호에 관한 전문인력의 국제 교류 등

Ⅲ 기술보호 법령 및 정책

3. 「방위산업기술 보호법」에 따른 보호 체계

방위산업기술 보호체계

- **보호대상 기술의 식별 및 관리체계**
  - ① 대상기관이 보유하고 있거나 연구개발을 통하여 확보한 기술 중 방위산업기술을 **분류·식별하는 체계**
  - ② 방위산업기술과 관련된 정보를 체계적으로 축적·관리할 수 있도록 하는 **인적·물적 체계**
- **인원통제 및 시설보호체계**
  - ① 방위산업기술 보호책임자의 임명, 보호구역의 설정 및 출입 제한을 통한 **인원통제 체계**
  - ② 보호구역에 보안장비 설치를 통한 방위산업기술에 대한 불법적인 접근을 탐지하는 **시설보호체계**
- **정보호호체계**
  - ① 방위산업기술을 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 **보안체계**
  - ② 컴퓨터바이러스 등으로부터 방위산업기술 침해를 방지하기 위한 소프트웨어 설치를 통한 **보호체계**
  - ③ 방위산업기술 정보에 대한 침입을 탐지·차단하기 위한 방화벽 및 보안관제 시스템 설치를 통한 **보호체계**
  - ④ 방위산업기술 정보에 접속하는 시스템·컴퓨터 등에 대한 **외부망 차단체계**

Ⅲ 기술보호 법령 및 정책

4. 중소·중견기업 기술보호체계 구축 지원

기술유출방지시스템 구축 지원

- 맞춤형 컨설팅을 통해 기업의 현 기술보호수준 점검 후 기업 환경에 맞는 기술보호체계 추천 및 구축 비용 일부 지원

통합보안장비 임차료 지원

- 기업의 보안관제에 필요한 방화벽, 침입방지시스템 등 다양한 정보보호 솔루션을 하나로 통합한 통합보안장비의 임차료를 지원

Defense Acquisition Program Administration

Ⅲ 기술보호 법령 및 정책

5. 사이버 취약점 점검

사이버 취약점 점검

- 대상 : 방산업체 및 협력업체 등
- 점검내용 : 인터넷 서버, 보안장비 및 네트워크 장비 등에 대해 모의해킹, 해킹메일 대응훈련 등을 실시
- 진단결과를 분석하여 사이버 보안 매뉴얼을 제작·배포

모의해킹, 해킹메일 대응훈련 → 취약점 진단·분석 → 피드백 / 사이버보안 매뉴얼 제작·배포

Ⅲ 기술보호 법령 및 정책

6. 방위산업기술 보호를 위한 실태조사

실태조사 (법 제12조)

- 방위사업청장은 방위산업기술 보호를 위하여 필요한 경우 대상기관의 방위산업기술 보호체계의 구축·운영에 대한 실태조사 실시
- 필요한 경우에는 정보수사기관을 포함한 관계 행정기관의 장에게 협조 요청

실태조사 범위

- 대상기관의 방위산업기술 보호체계 구축 운영 현황
- 방위산업기술 보호에 필요한 대책 수립·시행 현황
- 수출 및 국내이전 시 방위산업기술 보호에 필요한 대책 수립 현황
- 그 밖에 방위산업기술 보호체계의 구축·운영 현황을 파악하기 위하여 실태조사를 할 필요가 있는 사항

실태조사 관련 법 제재 (법 제13조)

- 실태조사 결과, 방위산업기술 보호체계 구축·운영이 부실하다고 판단되는 경우 개선권고 처분
  - 개선권고를 이행하지 않거나 불성실하게 이행한다고 판단되는 경우 시정명령 조치

Ⅲ 기술보호 법령 및 정책

7. 미국 CMMC 대비 한국 방산기술보호 인증제도 추진

▶ CMMC (Cybersecurity Maturity Model Certification) 2.0

- 미국 정부사업에 참여하는 자국업체 및 국외협력업체의 사이버보안능력을 평가하여 등급(Level1~3)을 부여하는 인증제도
- 미국은 현재 CMMC 2.0 법제화(Rule-making Process) 진행 중

▶ 방위사업청(국방기술보호국) CMMC 대응 전략

- 現 통합실태조사를 보완하여 CMMC 대비
  * 방향) 통합 실태조사 완료 시 Level 1 인증 취득, Level 2는 필요 시 추가 인증 (+α 개념)
- 한국 방산기술보호 인증제도 구축을 위한 정책연구과제 진행 중('23년 후반기 까지)
- 한국 방산기술보호 인증제도 수립 후 미국과 상호인정(MRA) 추진 예정

Ⅳ. 수출통제 제도

Defense Acquisition
Program Administration

Ⅳ 수출통제 제도

1. 국제수출통제체제와 한국의 수출통제 제도

· 한국은 주요 국제수출통제체제에 가입하고 **국제 기준에 따라 국내법 반영 및 수출통제를 실시**하고 있음

대외무역법 (전략물자 수출입 고시, 1986년 시행)

- WA(42개국, 1996 가입)
- NSG(48개국, 1995가입)
- MTCR(35개국, 2001가입)
- AG(43개국, 1996가입)

- 무기거래조약(ATT, 2017) 발효

* ECEU위원회는 AG 및 NSG의 Observer 자격으로 참여
- 생물무기 금지협약 (BWC, 1975), 화학무기금지협약 (CWC, 1997)

Ⅳ 수출통제 제도

2. 수출허가 심사환경 변화

수출허가 심사 소요 증가

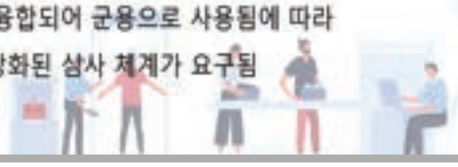
· 군용전략물자의 무분별한 확산을 막기 위해 방위사업청에서는 개별 신청 건에 대해 수출허가 심사 중

· 국제방산시장의 확대와 국제협력의 증가로 물자 및 기술의 수출허가 심사 소요가 증가하고 있음

심사의 기술적 난이도 상승

· 기존과 다른 새로운 물자 및 기술에 대한 검토로 기술적 난이도가 상승하고,

· 또한 다양한 기술이 융합되어 군용으로 사용됨에 따라 세밀하고 전문성이 강화된 심사 체계가 요구됨



Ⅳ 수출통제 제도

3. 수출허가 심사 제도

다양하고 전문성을 갖춘 검토기관 참여

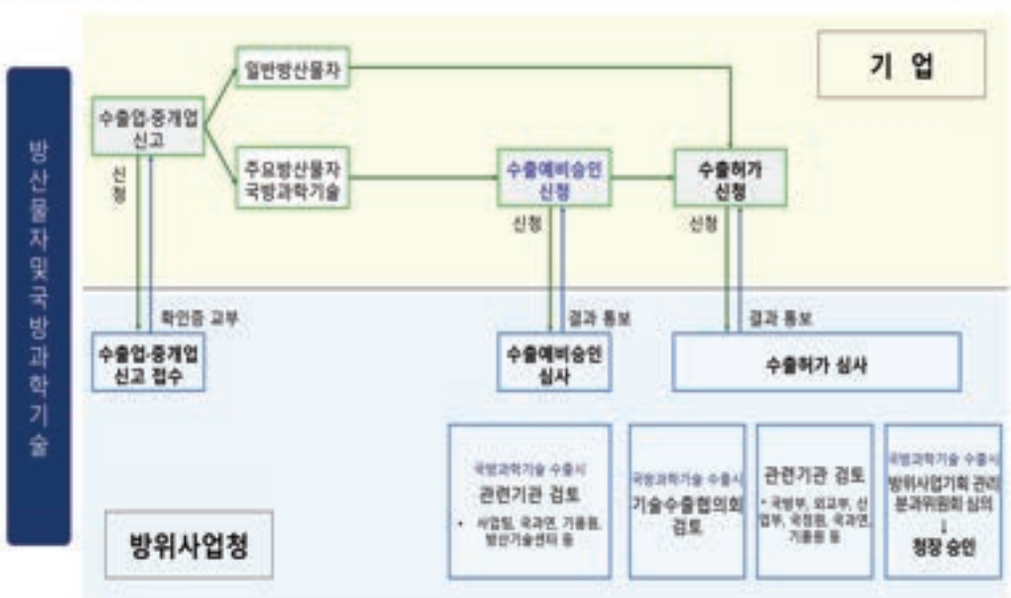
- 수출허가 심사를 위해 다양한 분야의 전문성을 갖춘 기관이 검토에 참여하고 있음
- 국방부, 각 군, 외교부, 산업통상자원부, 국가정보원, 경찰청, 방위사업청 등 관련 정부기관 뿐만 아니라
- 국방과학연구소, 국방기술품질원 등 연구기관과 필요시 학계도 참여중

수출예비승인 제도

- 특히 주요 방산물자와 국방과학기술은 수출허가를 받기 전에 수출예비승인 제도를 시행하여 더욱 수출허가 절차를 강화하였음
- 물품이나 기술을 수출하기 전 관련 상담을 하기 위해서는 사전에 수출예비승인 허가가 필요함

Ⅳ 수출통제 제도

4. 수출허가 절차

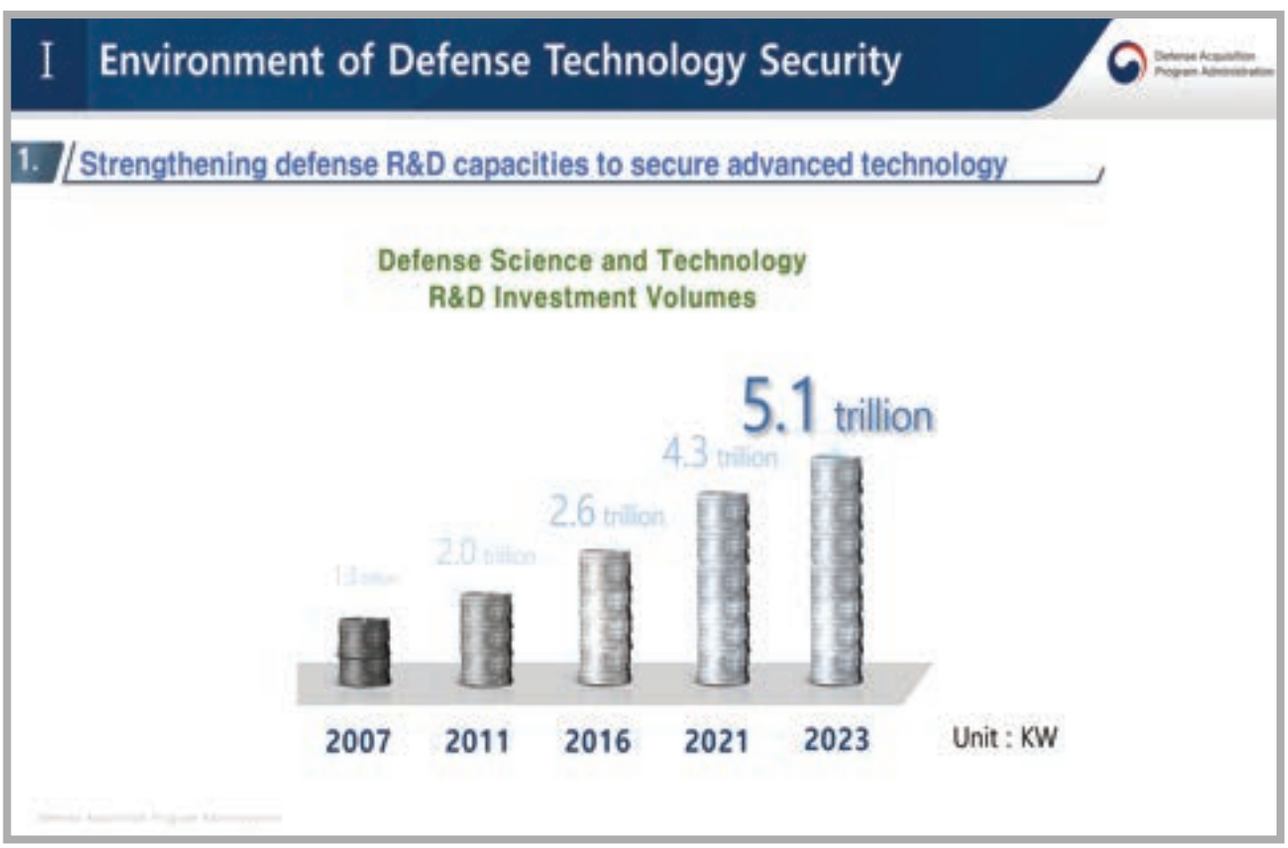


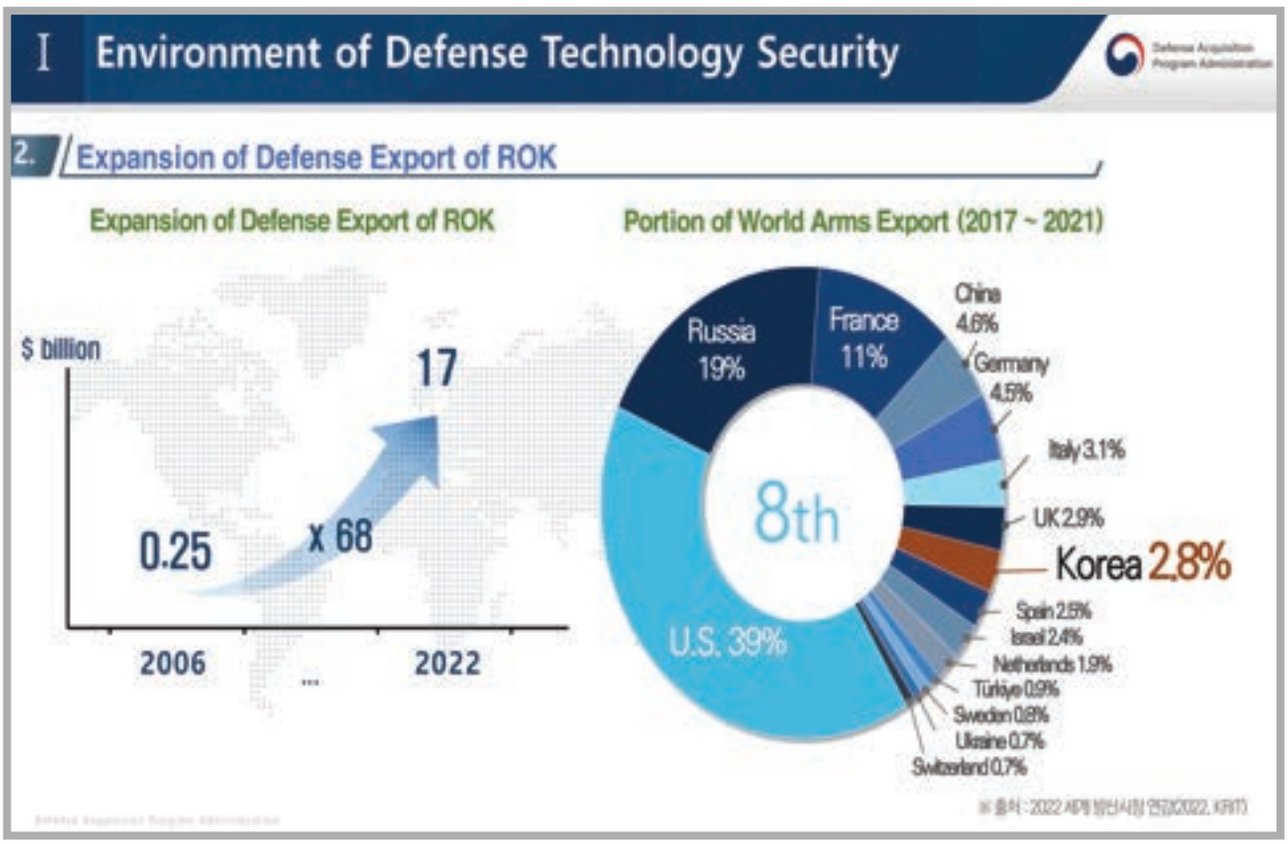

Defense Acquisition
Program Administration
Thank you


Technology Security &
Export Control Policy
4 August 2023
Defense Acquisition
Program Administration


INDEX
Ⅰ. Environment of Defense Technology Security
Ⅱ. Defense Technology Policy & Security Bureau, DAPA
Ⅲ. Technology Security Policy
Ⅳ. Export Control Policy
Defense Acquisition
Program Administration

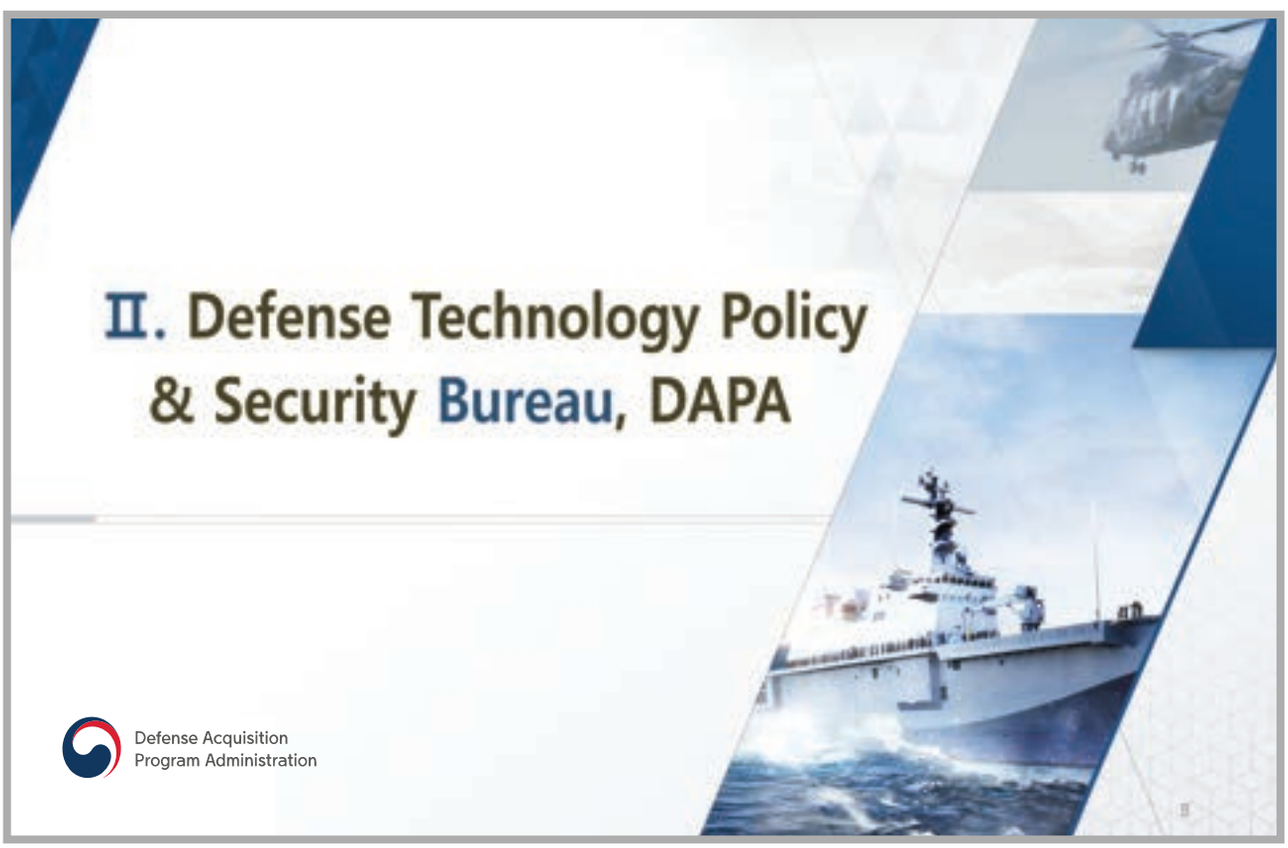

I . Environment of Defense Technology Security
Defense Acquisition Program Administration


I Environment of Defense Technology Security
1. Strengthening defense R&D capacities to secure advanced technology
Defense Science and Technology R&D Investment Volumes
5.1 trillion
4.3 trillion
2.6 trillion
2.0 trillion
2007
2011
2016
2021
2023
Unit : KW


I Environment of Defense Technology Security
2. Expansion of Defense Export of ROK
Expansion of Defense Export of ROK
$ billion
0.25
x 68
17
2006
...
2022
Portion of World Arms Export (2017 ~ 2021)
Russia 19%
France 11%
China 4.6%
Germany 4.5%
Italy 3.1%
UK 2.9%
Korea 2.8%
Spain 2.5%
Israel 2.4%
Netherlands 1.9%
Türkiye 0.9%
Sweden 0.8%
Ukraine 0.7%
Switzerland 0.7%
8th
U.S. 39%


I Environment of Defense Technology Security
3. Produce advanced weapon systems with cutting-edge technologies
KF-21
Surion
C-Star
K2
K9
Jangbogo


I Environment of Defense Technology Security
4. Increasing Defense Technology Security Threat
Material leakage by insiders
Cyberattacks from outside


II. Defense Technology Policy & Security Bureau, DAPA
Defense Acquisition Program Administration

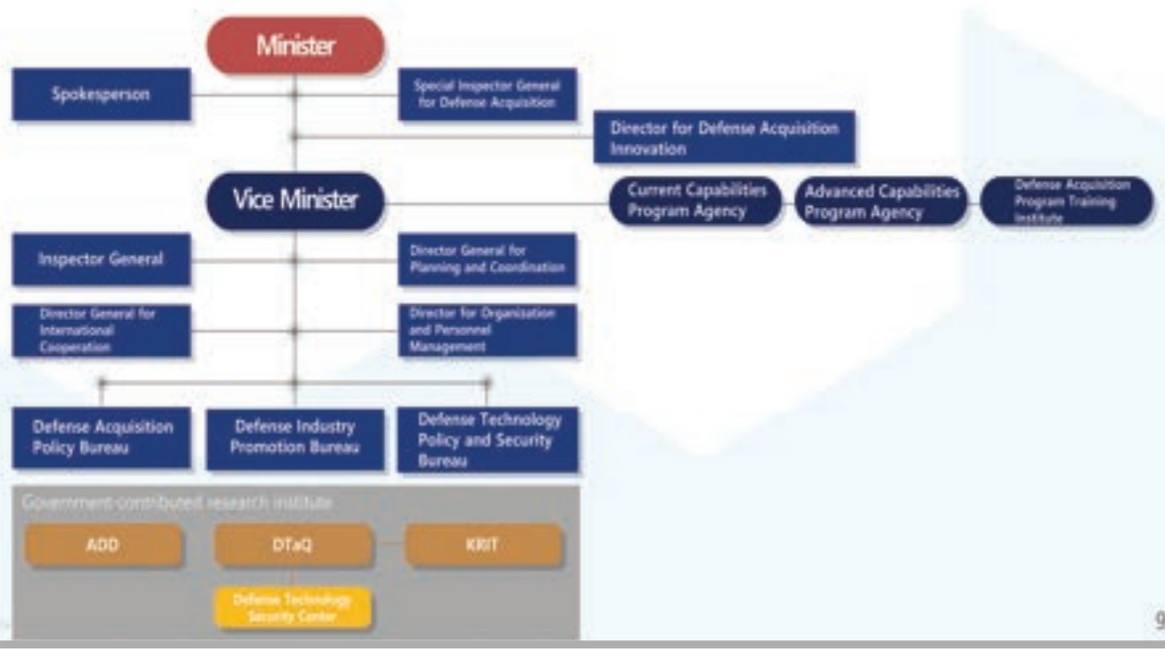
Ⅱ Defense Technology Policy & Security Bureau, DAPA

1. History of ROK Defense Technology Security Development

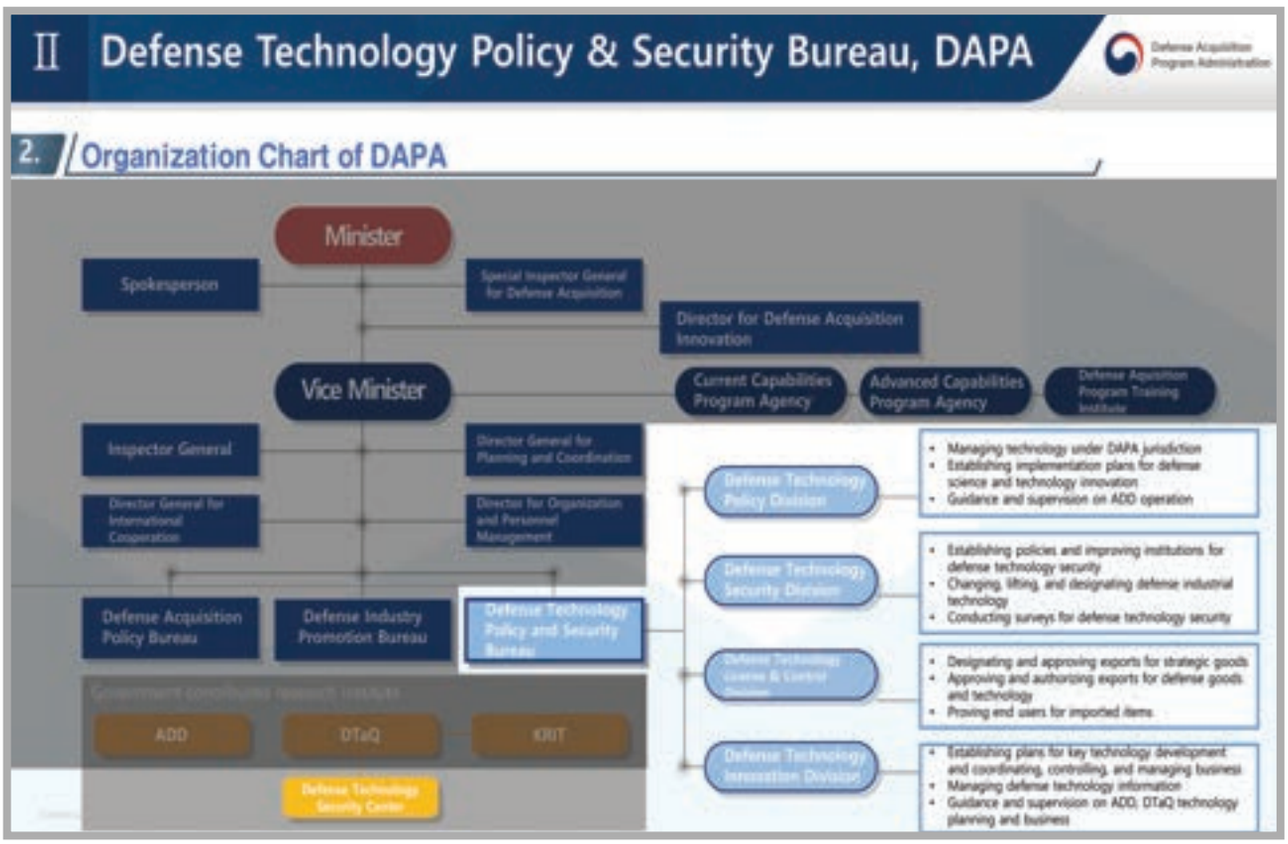
- Introduced strategic item import/export licensing system : 1989
- Joined the four multilateral export control regimes : 2001
  * Wassenar Arrangement (WA), Missile Technology control Regime (MTCR), The Australia Group (AG), Nuclear Suppliers Group (NSG)
- Established DAPA : 2006
- Newly organized Defense Technology Control Bureau : 2012
- Enacted Defense Technology Security Act : 2015
- Joined ATT (Arms Trade Treaty) : 2017
- Reorganized the bureau into Defense Technology Policy & Security Bureau : 2018
- Established Defense Technology Security Center in DTaQ : 2022

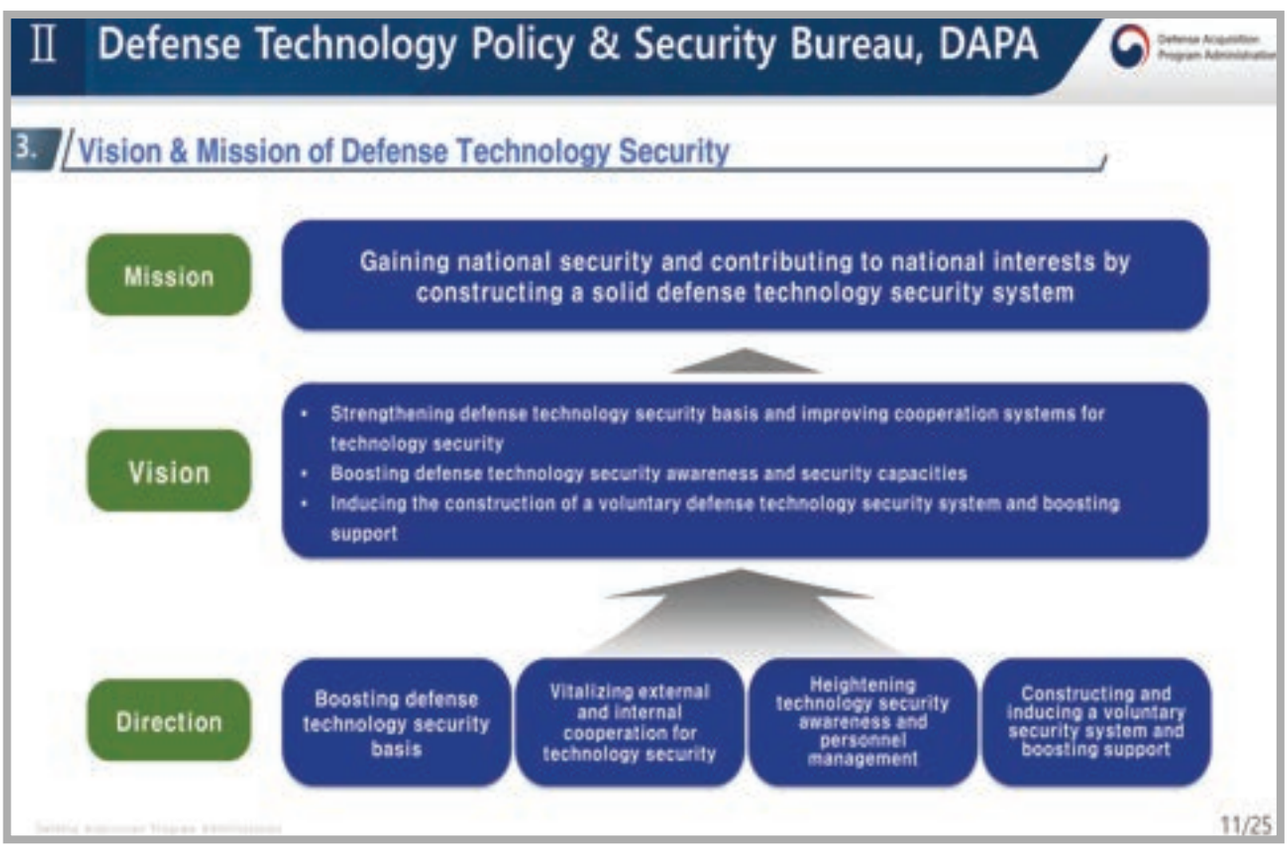
Ⅱ Defense Technology Policy & Security Bureau, DAPA

2. Organization Chart of DAPA



9/25


Ⅱ Defense Technology Policy & Security Bureau, DAPA
2. Organization Chart of DAPA
Minister
Spokesperson
Special Inspector General for Defense Acquisition
Director for Defense Acquisition Innovation
Vice Minister
Current Capabilities Program Agency
Advanced Capabilities Program Agency
Defense Acquisition Program Training Institute
Inspector General
Director General for Planning and Coordination
Director General for International Cooperation
Director for Organization and Personnel Management
Defense Acquisition Policy Bureau
Defense Industry Promotion Bureau
Defense Technology Policy and Security Bureau
ADD
DTaQ
KRIT
Defense Technology Security Center
Defense Technology Policy Division
Managing technology under DAPA jurisdiction
Establishing implementation plans for defense science and technology innovation
Guidance and supervision on ADD operation
Defense Technology Security Division
Establishing policies and improving institutions for defense technology security
Changing, lifting, and designating defense industrial technology
Conducting surveys for defense technology security
Defense Technology Control Division
Designating and approving exports for strategic goods
Approving and authorizing exports for defense goods and technology
Proving end users for imported items
Defense Technology Innovation Division
Establishing plans for key technology development and coordinating, controlling, and managing business
Managing defense technology information
Guidance and supervision on ADD, DTaQ technology planning and business


Ⅱ Defense Technology Policy & Security Bureau, DAPA
3. Vision & Mission of Defense Technology Security
Mission
Gaining national security and contributing to national interests by constructing a solid defense technology security system
Vision
Strengthening defense technology security basis and improving cooperation systems for technology security
Boosting defense technology security awareness and security capacities
Inducing the construction of a voluntary defense technology security system and boosting support
Direction
Boosting defense technology security basis
Vitalizing external and internal cooperation for technology security
Heightening technology security awareness and personnel management
Constructing and inducing a voluntary security system and boosting support
11/25

Ⅱ Defense Technology Policy & Security Bureau, DAPA

4. Defense Technology Security Center (DTaQ)

국방기술품질원 (DTaQ)

Defense Technology Security Center

- Established a dedicated organization for responding and diagnosing defense cyber threat incident and performing administrative tasks such as security control and technology control (July, '22)
- (Incident Response and Diagnosis) Initial response through a security expert in case of cyberattack on a defense business, consulting for prevention and cooperation with relevant organizations
- (Technology Control) Designating and supporting export authorization approvals on defense technology for safe R&D and defense export
- (Other Support) Technology security support including comprehensive surveys, SME support, and defense technology security training

Ⅲ. Technology Security Law & Policy

Defense Acquisition Program Administration

Ⅲ Technology Security Law & Policy

1. Background for enactment of the 「Defense Technology Security Law」

Purpose

▲ Systematic protection of defense technology ▲ Support for relevant organizations ▲ Executing duties including international treaties

➡ Ensuring economic and national security, boosting national credibility

Improving domestic and overseas technology security

▶ Transitioning awareness on defense technology as a national security asset and strategic economic resource

▶ Countries around the world are protecting their defense technology and strengthening export controls

Basis of defense industry competitiveness

▶ Increase of technology leakage threats due to increases in defense exports and improvements in technology level

▶ Securing domestic competitiveness in the global market and protecting potential export markets

Ⅲ Technology Security Law & Policy

2. Article 15 (International Cooperation) of Defense Technology Security Act

Act. Article 15 (International Cooperation)

The government may initiate necessary business such as constructing a cooperation system with export and import countries, and professional personnel exchanges, in order to promote international cooperation for defense technology security.

Enforcement decree. Article 20 (Scope of International Cooperation)

International cooperation is necessary for the following operations according to Article 15.

- Constructing international cooperation systems and sharing technology security systems and policies for defense technology security
- International investigations and research on technical methods of defense technology security
- International exchanges between professional personnel for defense technology security

Ⅲ Technology Security Law & Policy

3. The security system according to the 「Defense Technology Security Act」

Defense Technology Security System

Identification and management system for protected technology	① **A system for identifying and managing** defense technology among the technologies secured through R&D or held by the target organization
	② **A human and material system** to systematically accumulate and manage defense technology information
Personnel management and facility protection system	① **A personnel control system** through appointing a defense technology security officer, explaining and limiting access to protected areas
	② **A facility protection system** that detects illegal access to defense technology by installing security equipment in protected areas
Information security system	① **A security system** using encryption technology to safely store and transmit defense technology
	② **A security system** with software to prevent defense technology infringement from computer viruses
	③ **A security system** with a security control system and firewall to detect and block invasion of defense technology information
	④ **A blocking system for external networks** against systems or computers accessing defense technology information

Ⅲ Technology Security Law & Policy

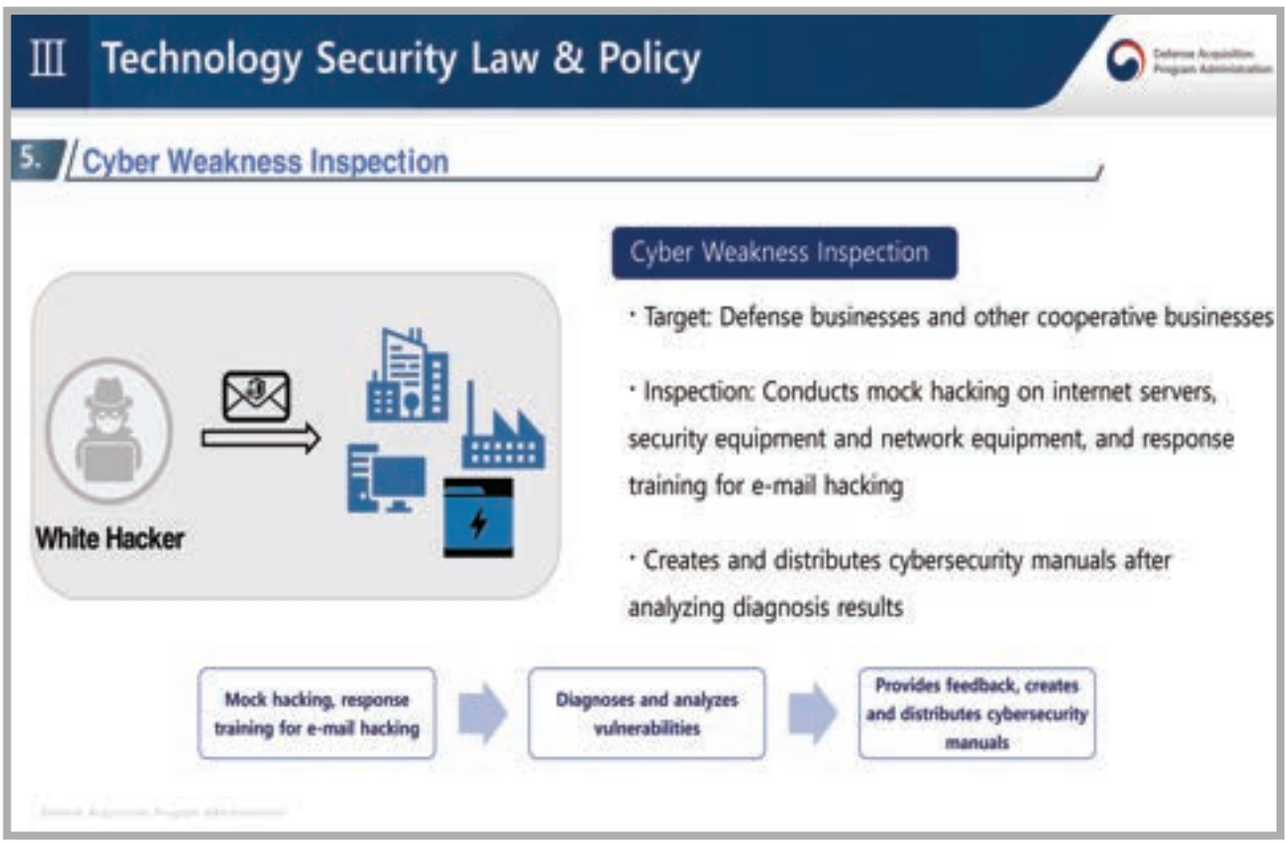
4. Support for constructing SME technology security systems

Support for constructing a technology leakage prevention system

· Recommends technology security systems that suit the company environment and supports part of the construction costs after inspecting the company's current technology security level through customized consulting

Rent support for integrated security equipment

· Supports rent for integrated security equipment, which includes various information security solutions such as firewalls for company security control and invasion prevention systems


Ⅲ Technology Security Law & Policy
5. Cyber Weakness Inspection
White Hacker
Cyber Weakness Inspection
· Target: Defense businesses and other cooperative businesses
· Inspection: Conducts mock hacking on internet servers, security equipment and network equipment, and response training for e-mail hacking
· Creates and distributes cybersecurity manuals after analyzing diagnosis results
Mock hacking, response training for e-mail hacking
Diagnoses and analyzes vulnerabilities
Provides feedback, creates and distributes cybersecurity manuals


Ⅲ Technology Security Law & Policy
6. Investigation of Current Status for Security of Defense Technology
Investigation (Article 12)
▶ Minister of DAPA conducts surveys on target organizations' defense technology security system construction and operation if necessary for defense technology security
▶ Requires cooperation of heads of relevant administrative organizations, including investigative agencies, if necessary
Scope
▶ Target organizations' defense technology security system construction and operation
▶ Defense technology security solution establishment and implementation
▶ Solutions for defense technology security in case of exports or domestic transfers
▶ Other points to survey in order to perceive status quo of defense technology security system construction and operation
Legal Sanctions related to Investigation (Article 13)
▶ Recommends improvements if defense technology security system construction and operation are judged insufficient as a result of the survey
* Issues correction orders if the recommendations are not carried out or carried out in an insufficient way

Ⅲ Technology Security Law & Policy

7. Korean Defense Technology Security Certification System in preparation of the U.S. CMMC

▶ CMMC (Cybersecurity Maturity Model Certification) 2.0

- A certification system that confers levels 1-3 by evaluating the cybersecurity capacities of U.S. and overseas cooperators in USG business
- The U.S. is currently in the rule-making process for CMMC 2.0

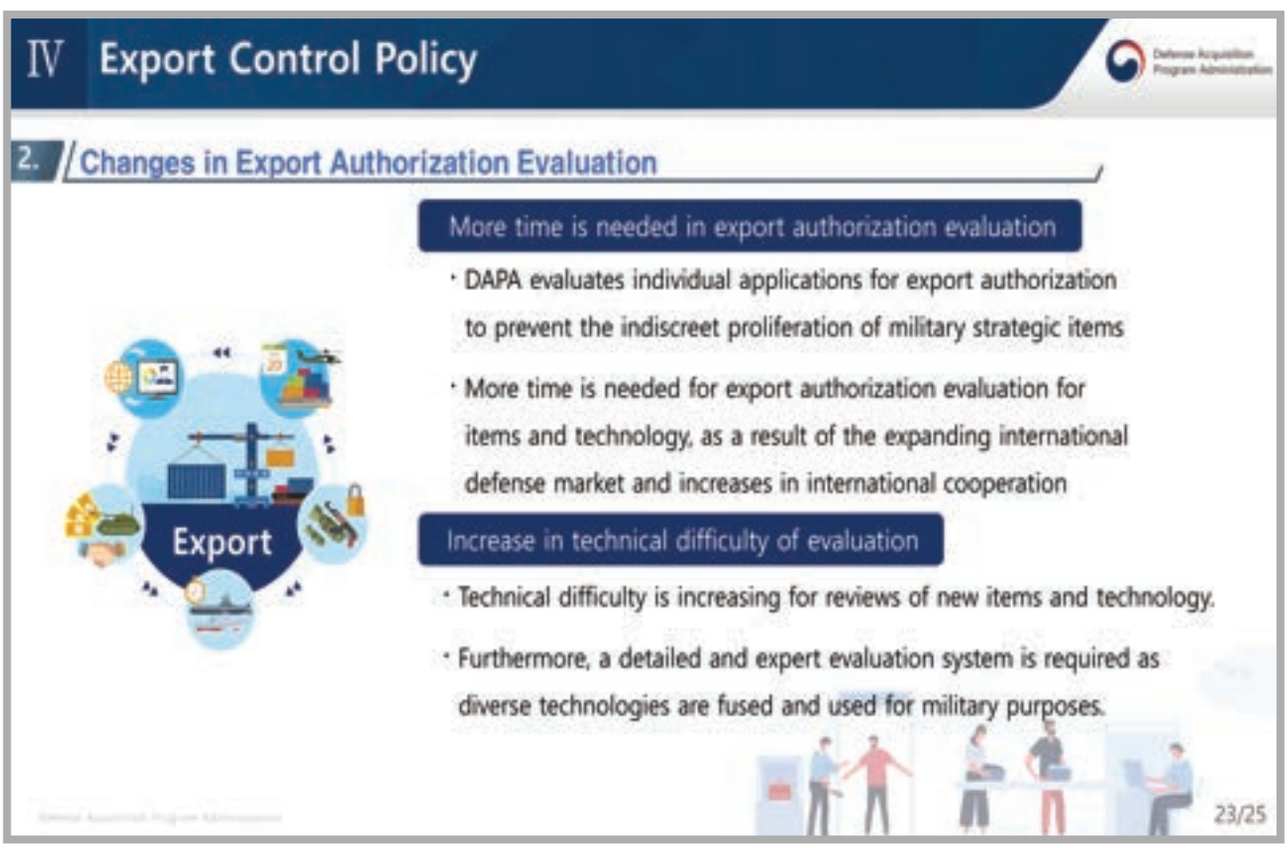
▶ CMMC Response Strategy by DAPA

- Preparing for CMMC by complementing the current integrated survey
  * Direction) Acquires Level 1 certification after completing the integrated survey; Level 2 requires additional certification if needed (extra)
- Working on policy research to construct a Korean defense technology security certification system (by the end of '23)
- Set to pursue MRA with the U.S. after establishing a Korean defense technology security certification system

Ⅳ. Export Control Policy

Defense Acquisition Program Administration


Ⅳ Export Control Policy
1. International Export Control Regime and ROK' s Export Control
· ROK has joined a major international export control regime, controlling exports according to international standards, and reflecting said standards in domestic laws.
Foreign Trade Act (Public Announcement of Imports and Exports of Strategic Items, enforced in 1986)
WA (42 countries, joined in 1996)
Mexico (1 country)
NSG (48 countries, joined in 1995)
MTCR
India (1 country)
Republic of South Africa, Russia (2 countries)
Brazil (1 country)
Belarus
China
Kazakhstan
Serbia
(4 countries)
MTCR (35 countries, joined in 2001)
Greece, the Netherlands, Norway, New Zealand, Denmark, Germany, Luxembourg, the U.S., Belgium, Bulgaria, Sweden, Switzerland, Spain, Argentina, Ireland, UK, Austria, Ukraine, Italy, Japan, the Czech Republic, Canada, Turkey, Portugal, Poland, France, Finland, Hungary, Australia, ROK (30 countries; "가" region or "가-1" region)
Iceland (1 country)
Latvia, Romania, Lithuania, Malta, Slovakia Slovenia, Estonia, Croatia (8 countries)
Cyprus (1 country)
The Australia Group
AG (43 countries, joined in 1996)
· Arms Trade Treaty (ATT, 2017) took effect
* Participated as an Observer of AG and NSG in EC (European Commission)
- Biological Weapons Convention (BWC, 1975), Chemical Weapons Convention (CWC, 1997)
22/25


Ⅳ Export Control Policy
2. Changes in Export Authorization Evaluation
More time is needed in export authorization evaluation
· DAPA evaluates individual applications for export authorization to prevent the indiscreet proliferation of military strategic items
· More time is needed for export authorization evaluation for items and technology, as a result of the expanding international defense market and increases in international cooperation
Export
Increase in technical difficulty of evaluation
· Technical difficulty is increasing for reviews of new items and technology.
· Furthermore, a detailed and expert evaluation system is required as diverse technologies are fused and used for military purposes.
23/25

Ⅳ Export Control Policy

3. Export Authorization Evaluation System

Diverse expert review agencies participate

- Expert agencies in diverse fields participate in reviews for export authorization evaluation
- Including relevant government agencies such as the Ministry of National Defense, the military, the Ministry of Foreign Affairs, the Ministry of Trade, Industry and Energy, the National Intelligence Service, the Korean National Police Agency, and DAPA
- and research institutes such as the Agency for Defense Development and the Defense Agency for Technology and Quality, and academia if necessary

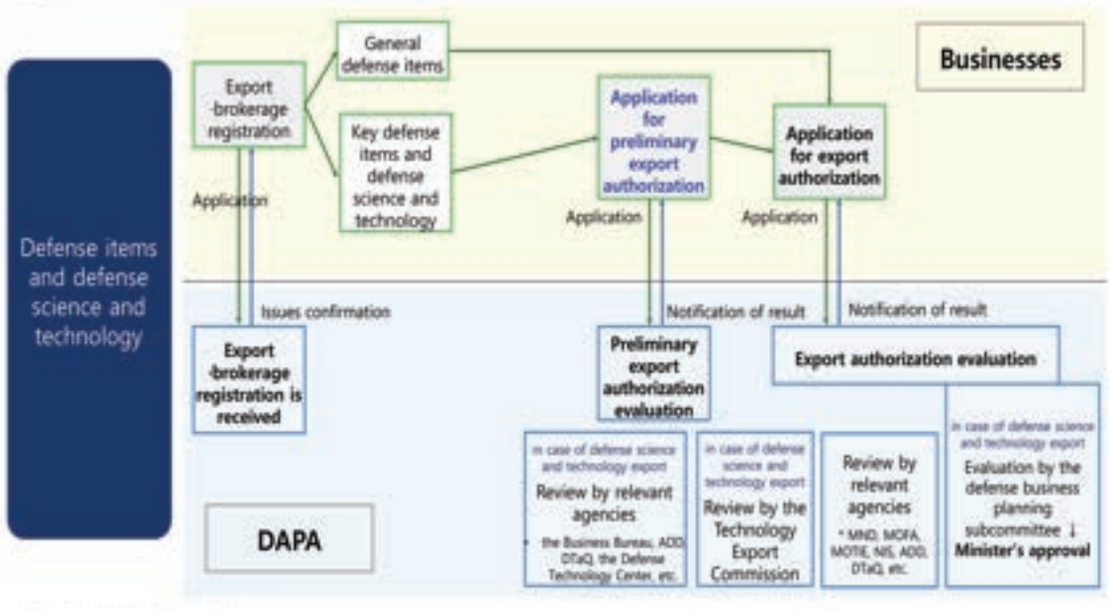
Preliminary export authorization system

- The export authorization process has especially been further strengthened for key defense items and defense technology by implementing a preliminary export authorization system
- A preliminary export authorization is necessary in advance for consultations before exporting items or technology

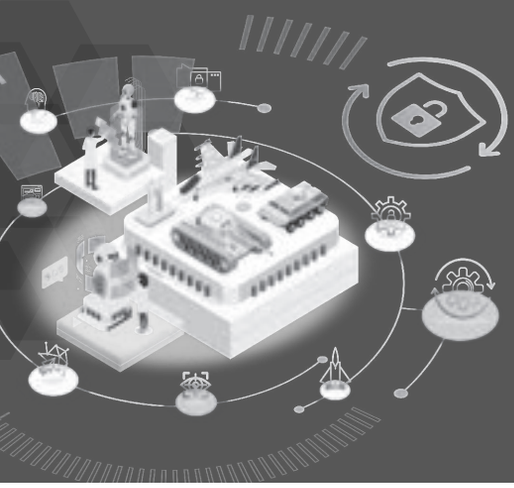
24/25

Ⅳ Export Control Policy

4. Export Authorization Process




Defense Acquisition
Program Administration
Thank you



2023 Defense Technology Security Conference 2023 방산기술보호 컨퍼런스

주제발표 2.

방산기술수출, 단계별 주요 이슈

Defense Technology Export and Key Issues

김·장 법률사무소 변호사 I **이상진**

Attorney at law, Kim & Chang

Mr. Sangjin Lee

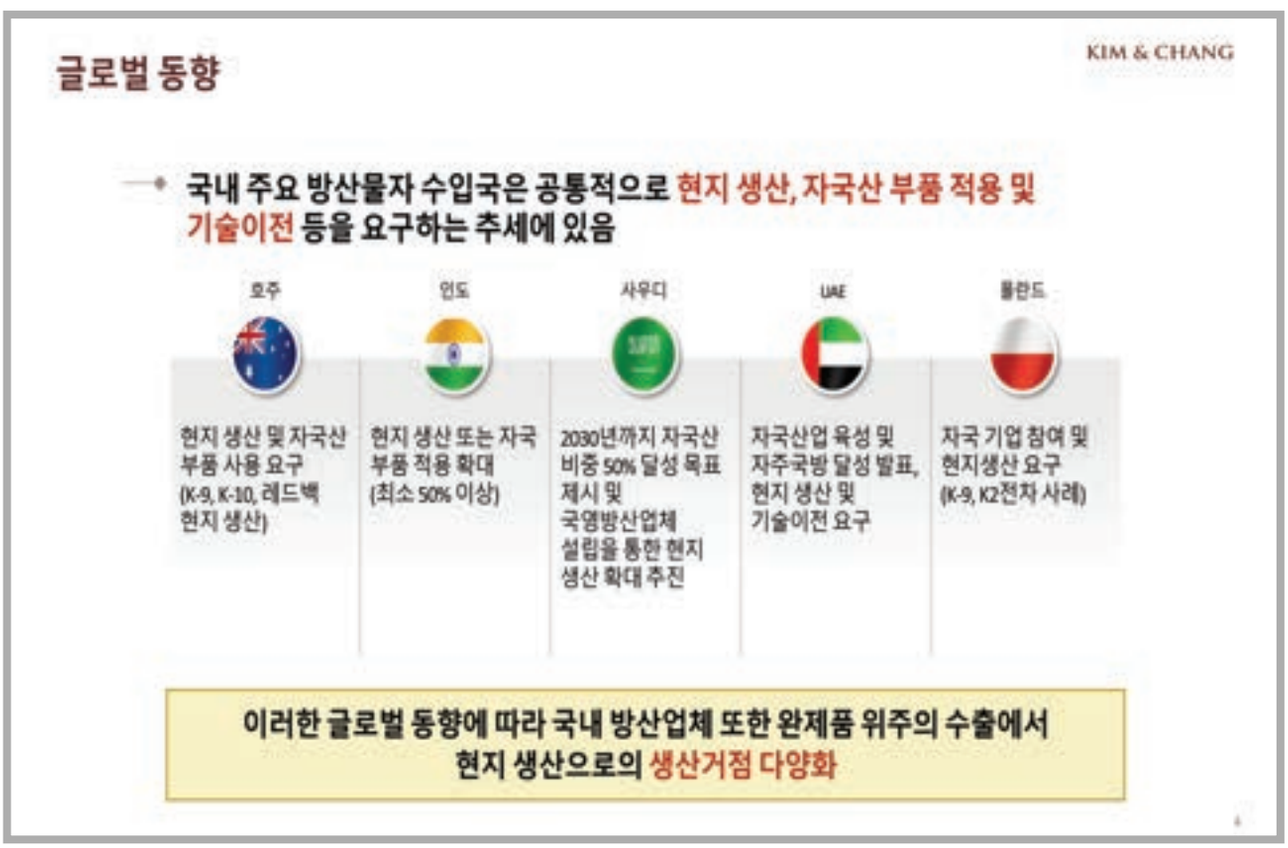
KIM & CHANG

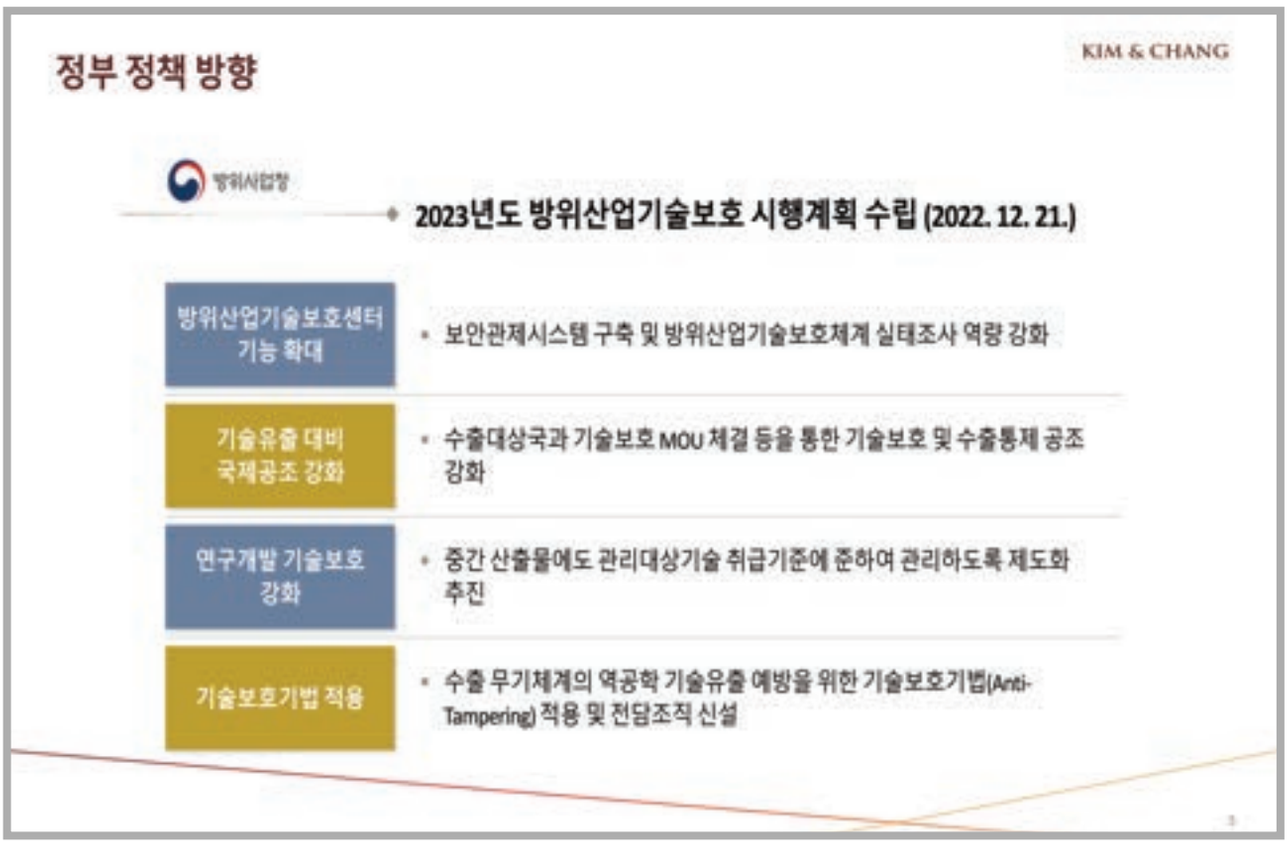
방산기술 수출, 단계별 주요 이슈

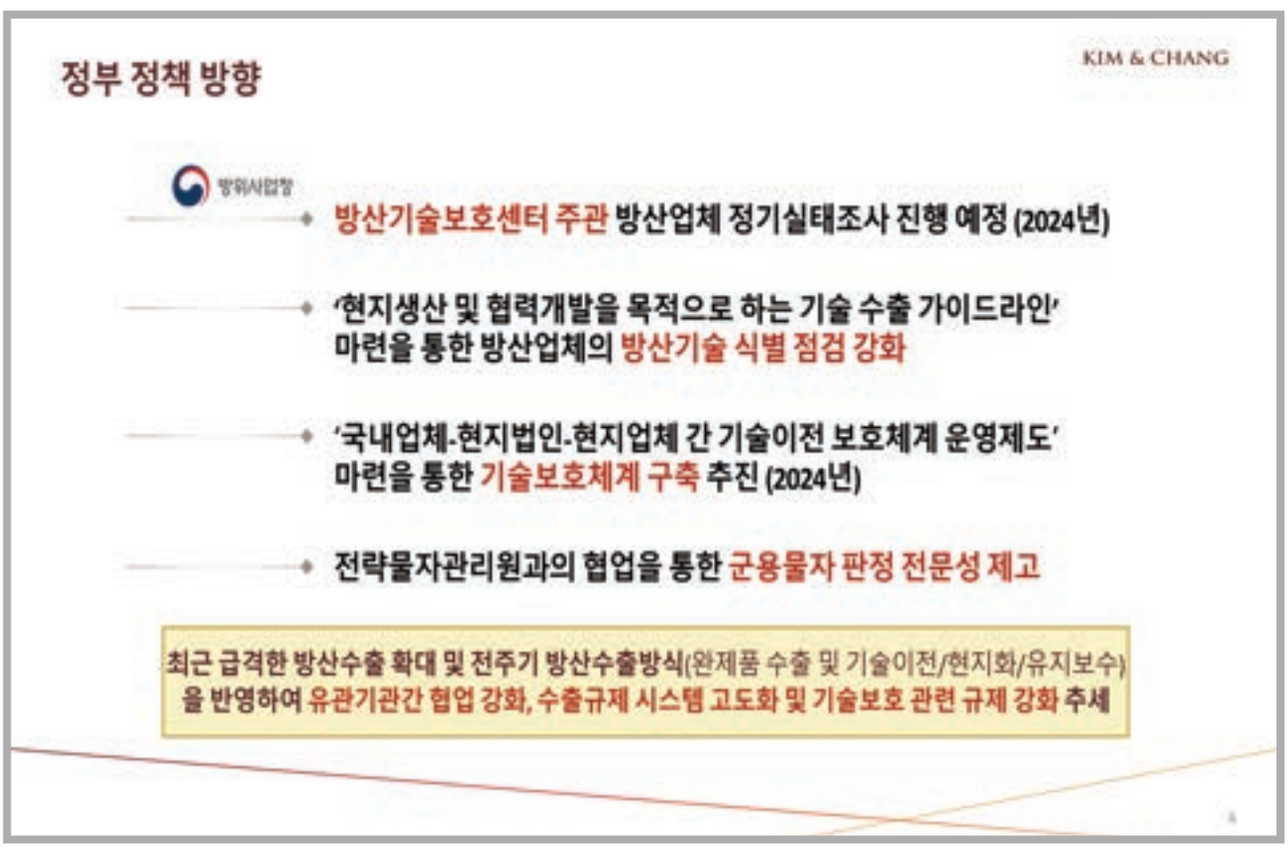
KIM & CHANG

목 차


I. 방산수출 관련 주요 동향


글로벌 동향
KIM & CHANG
국내 주요 방산물자 수입국은 공통적으로 현지 생산, 자국산 부품 적용 및 기술이전 등을 요구하는 추세에 있음
호주
현지 생산 및 자국산 부품 사용 요구 (K-9, K-10, 레드백 현지 생산)
인도
현지 생산 또는 자국 부품 적용 확대 (최소 50% 이상)
사우디
2030년까지 자국산 비중 50% 달성 목표 제시 및 국영방산업체 설립을 통한 현지 생산 확대 추진
UAE
자국산업 육성 및 자주국방 달성 발표, 현지 생산 및 기술이전 요구
폴란드
자국 기업 참여 및 현지생산 요구 (K-9, K2전차 사례)
이러한 글로벌 동향에 따라 국내 방산업체 또한 완제품 위주의 수출에서 현지 생산으로의 생산거점 다양화

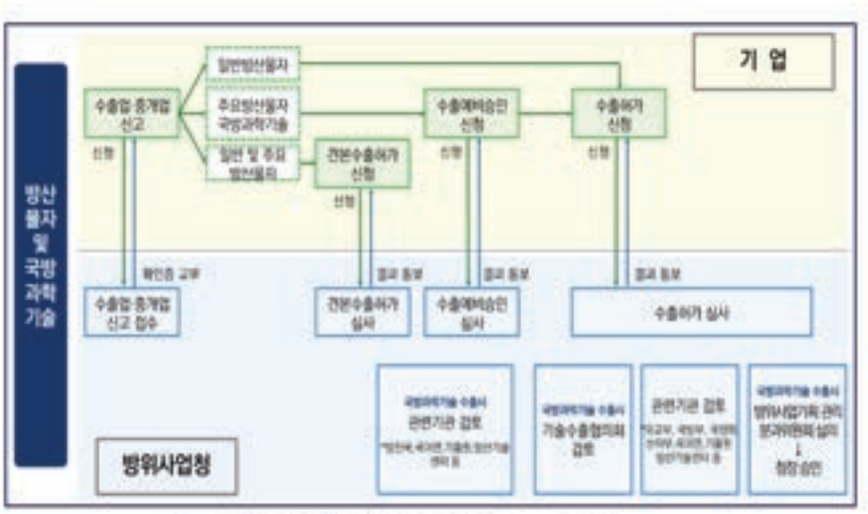

정부 정책 방향
KIM & CHANG
방위사업청
2023년도 방위산업기술보호 시행계획 수립 (2022. 12. 21.)
방위산업기술보호센터 기능 확대
• 보안관제시스템 구축 및 방위산업기술보호체계 실태조사 역량 강화
기술유출 대비 국제공조 강화
• 수출대상국과 기술보호 MOU 체결 등을 통한 기술보호 및 수출통제 공조 강화
연구개발 기술보호 강화
• 중간 산출물에도 관리대상기술 취급기준에 준하여 관리하도록 제도화 추진
기술보호기법 적용
• 수출 무기체계의 역공학 기술유출 예방을 위한 기술보호기법(Anti-Tampering) 적용 및 전담조직 신설


정부 정책 방향
KIM & CHANG
방위사업청
방산기술보호센터 주관 방산업체 정기실태조사 진행 예정 (2024년)
'현지생산 및 협력개발을 목적으로 하는 기술 수출 가이드라인' 마련을 통한 방산업체의 방산기술 식별 점검 강화
'국내업체-현지법인-현지업체 간 기술이전 보호체계 운영제도' 마련을 통한 기술보호체계 구축 추진 (2024년)
전략물자관리원과의 협업을 통한 군용물자 판정 전문성 제고
최근 급격한 방산수출 확대 및 전주기 방산수출방식(완제품 수출 및 기술이전/현지화/유지보수)을 반영하여 유관기관간 협업 강화, 수출규제 시스템 고도화 및 기술보호 관련 규제 강화 추세

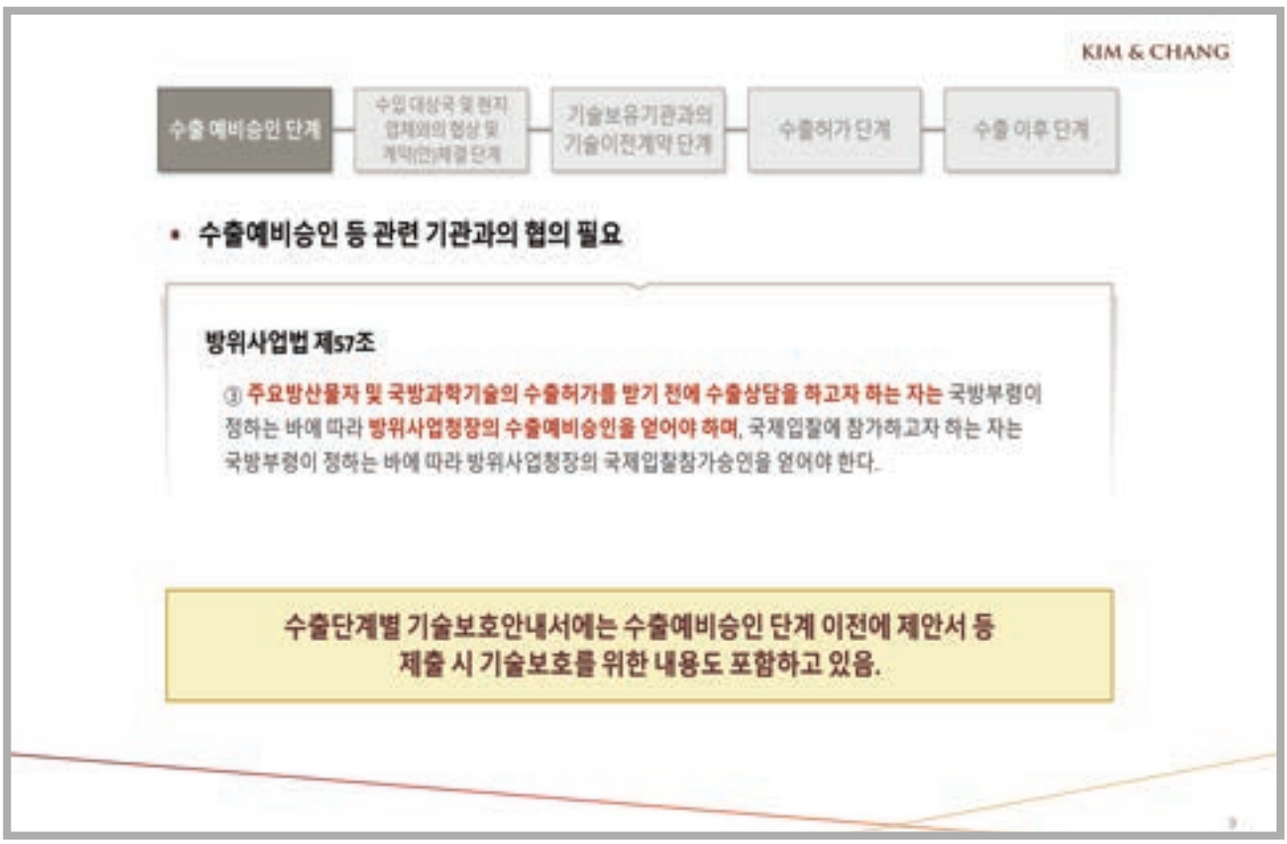
II. 방산기술 수출, 단계별 주요 이슈

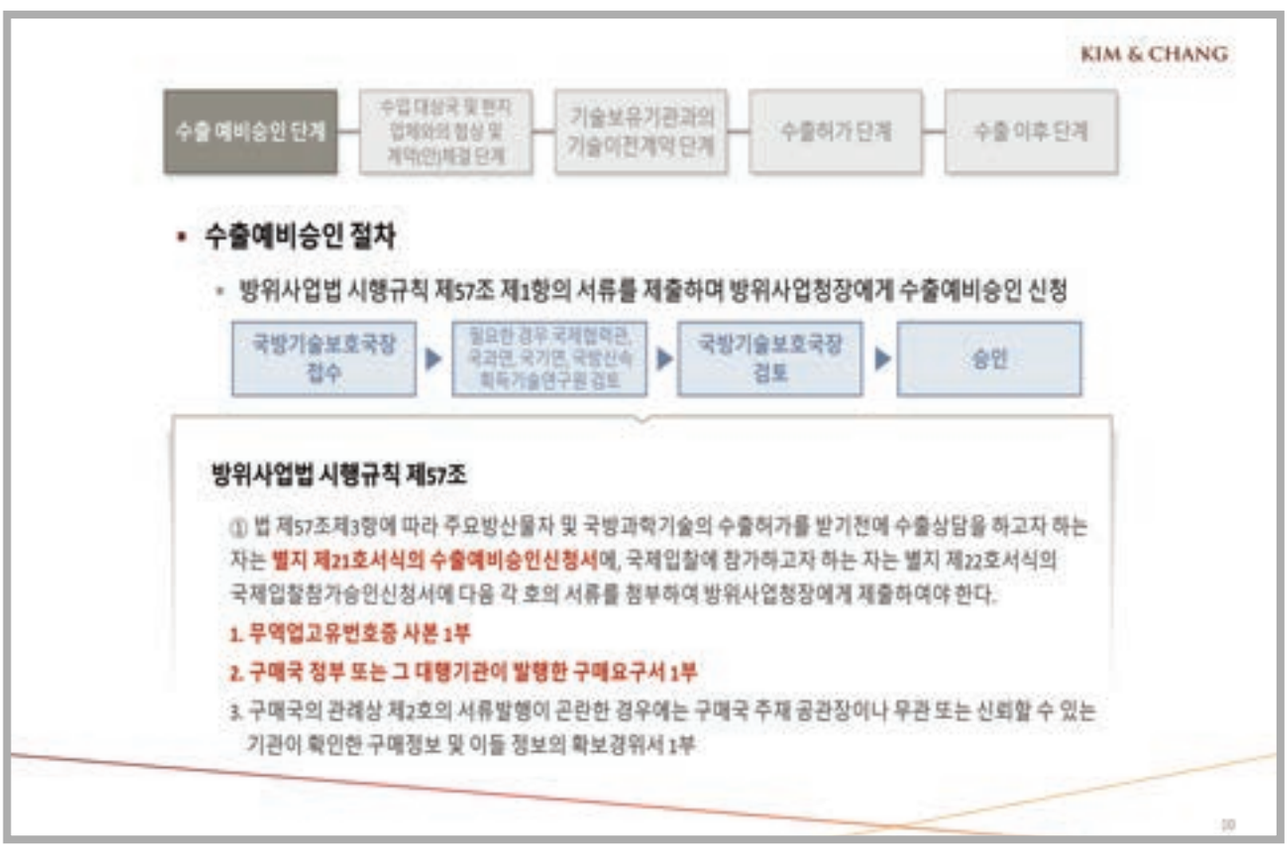
방산물자 및 국방과학기술(방위산업기술) 수출 절차 개관

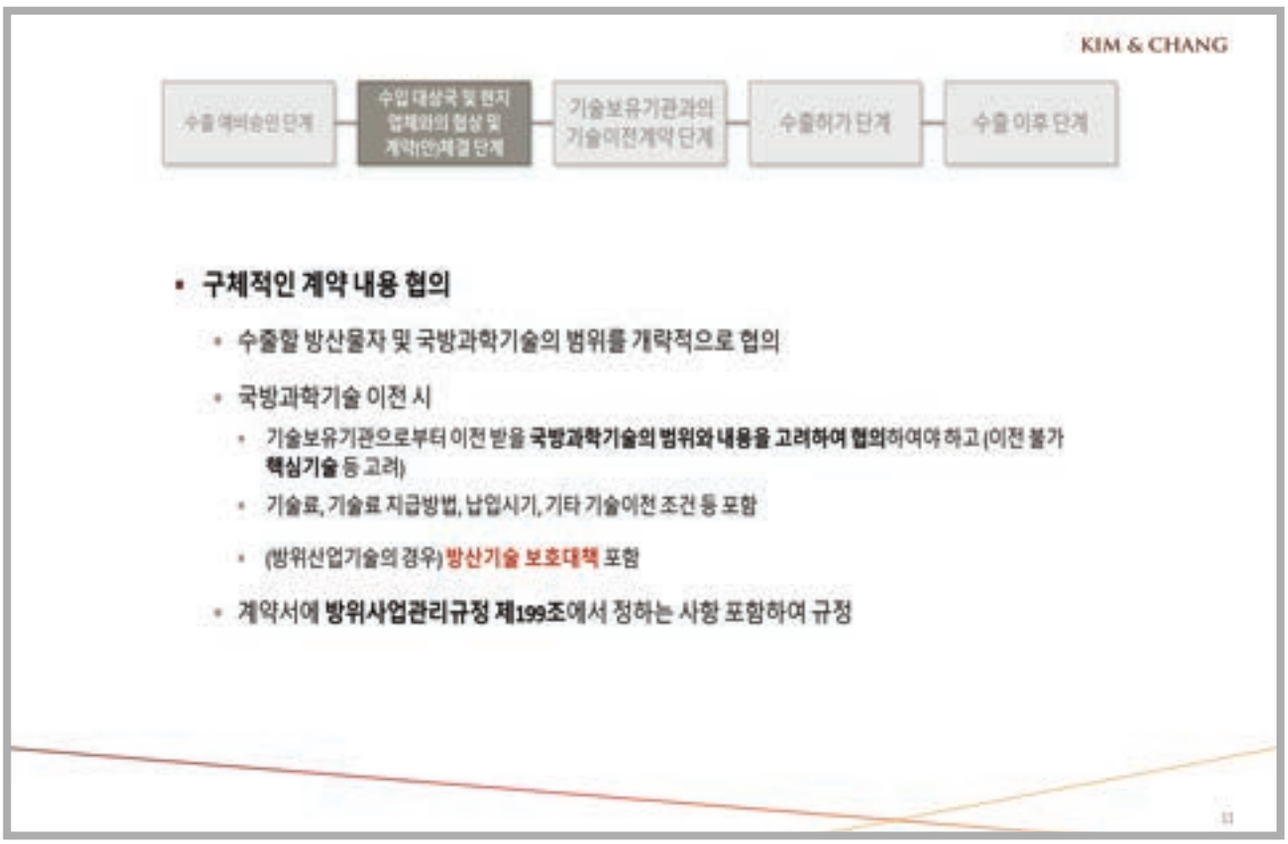
KIM & CHANG

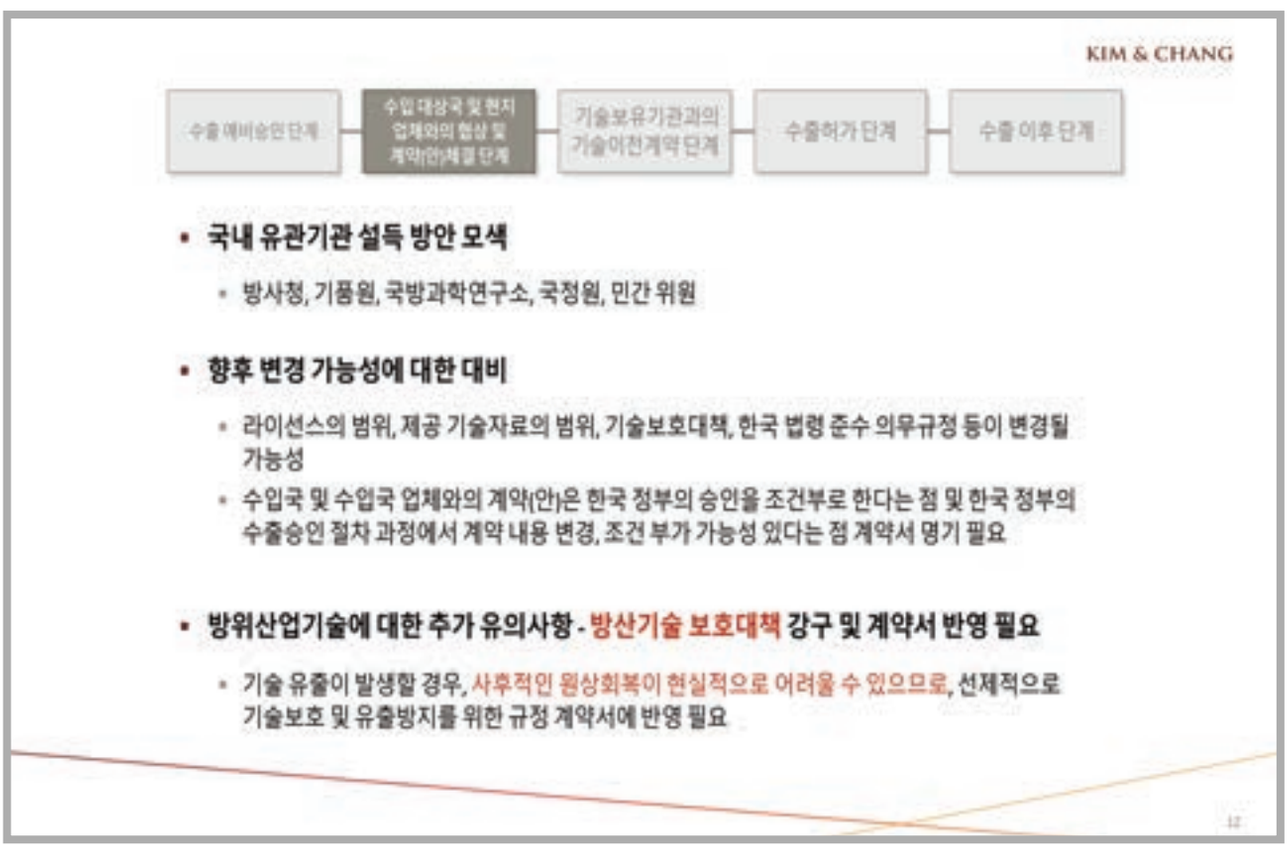


자료 : 방위사업청, 「방산 수출입 제도 가이던스」, 2022. 8.

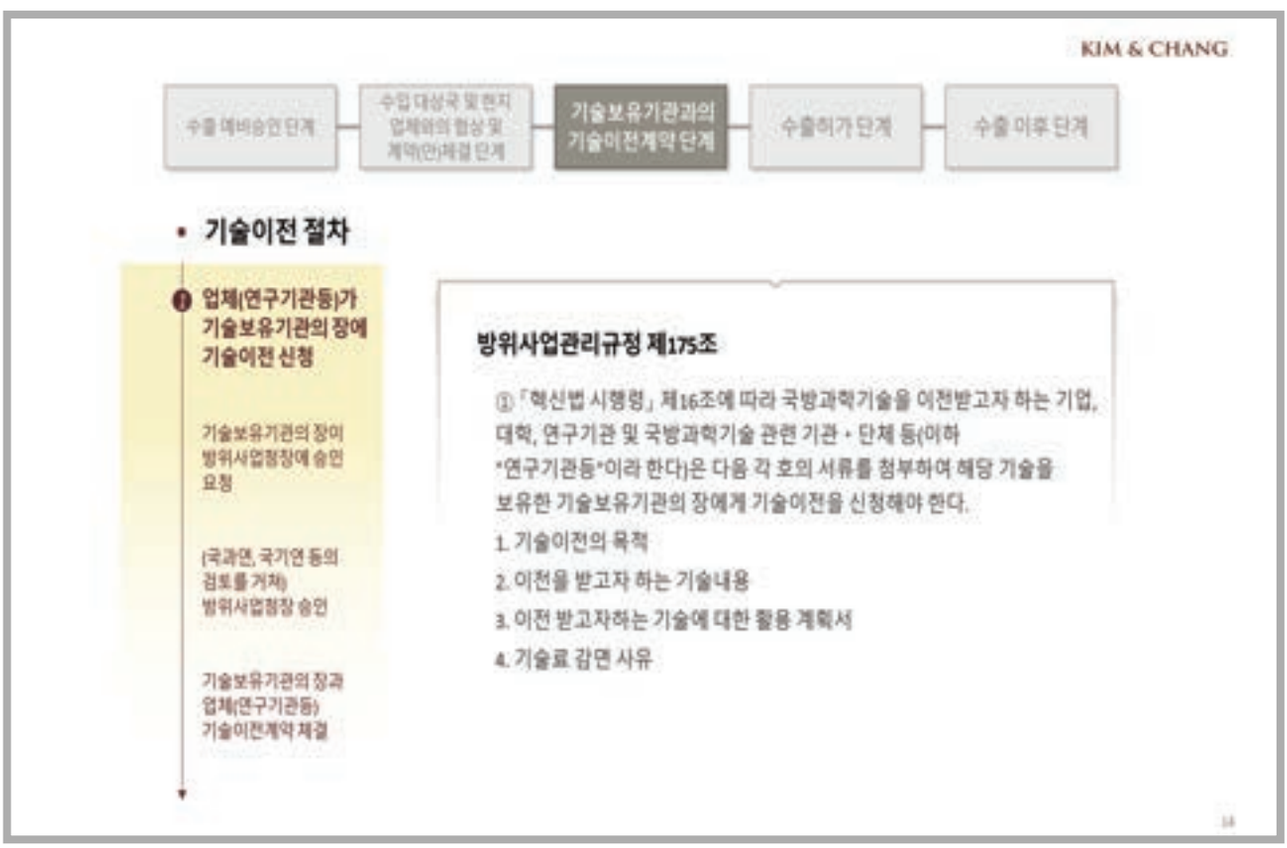

KIM & CHANG
수출 예비승인 단계
수입 대상국 및 현지 업체와의 협상 및 계약(안)체결 단계
기술보유기관과의 기술이전계약 단계
수출허가 단계
수출 이후 단계
• 수출예비승인 등 관련 기관과의 협의 필요
방위사업법 제57조
③ 주요방산물자 및 국방과학기술의 수출허가를 받기 전에 수출상담을 하고자 하는 자는 국방부령이 정하는 바에 따라 방위사업청장의 수출예비승인을 얻어야 하며, 국제입찰에 참가하고자 하는 자는 국방부령이 정하는 바에 따라 방위사업청장의 국제입찰참가승인을 얻어야 한다.
수출단계별 기술보호안내서에는 수출예비승인 단계 이전에 제안서 등 제출 시 기술보호를 위한 내용도 포함하고 있음.

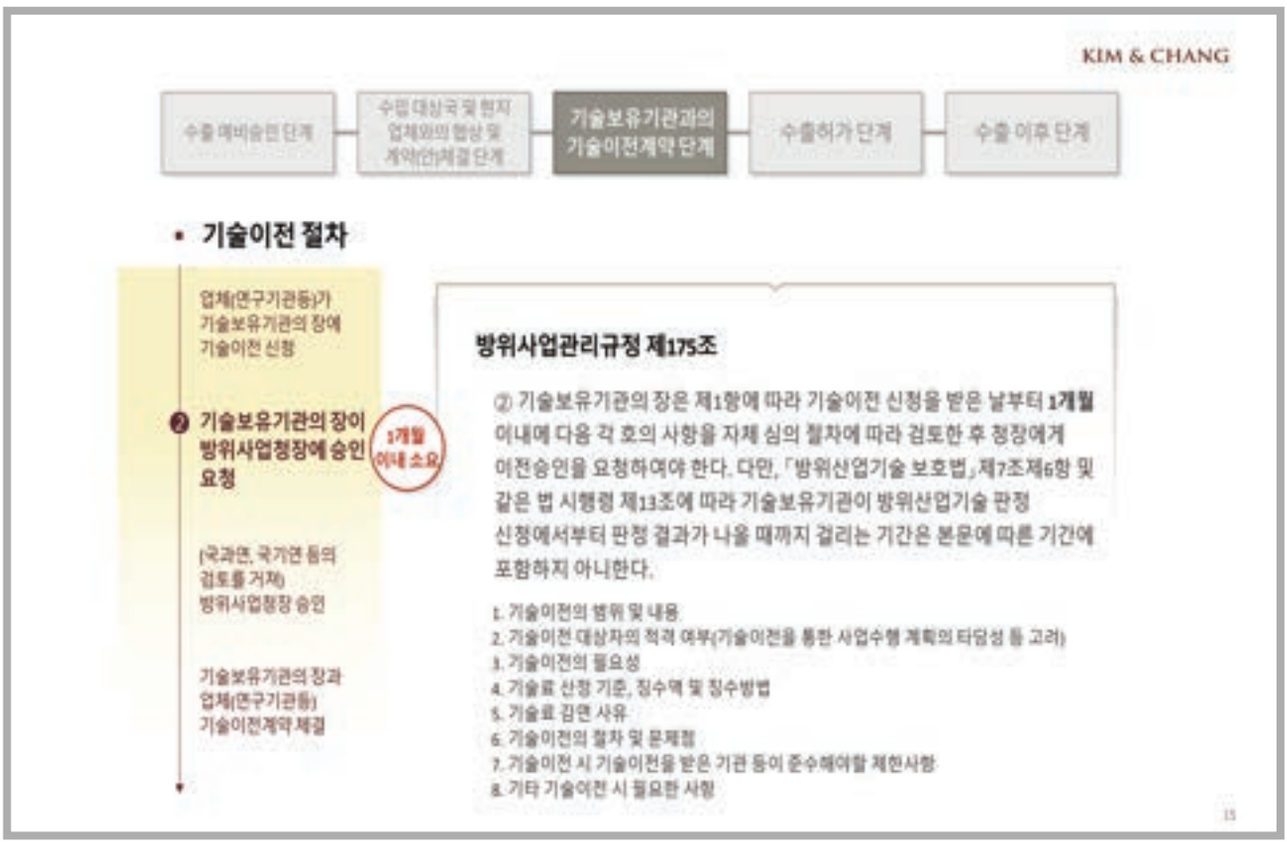

KIM & CHANG
수출 예비승인 단계
수입 대상국 및 현지 업체와의 협상 및 계약(안)체결 단계
기술보유기관과의 기술이전계약 단계
수출허가 단계
수출 이후 단계
• 수출예비승인 절차
▪ 방위사업법 시행규칙 제57조 제1항의 서류를 제출하며 방위사업청장에게 수출예비승인 신청
국방기술보호국장 접수
필요한 경우 국제협력관, 국과연, 국기연, 국방신속획득기술연구원 검토
국방기술보호국장 검토
승인
방위사업법 시행규칙 제57조
① 법 제57조제3항에 따라 주요방산물자 및 국방과학기술의 수출허가를 받기전에 수출상담을 하고자 하는 자는 별지 제21호서식의 수출예비승인신청서에, 국제입찰에 참가하고자 하는 자는 별지 제22호서식의 국제입찰참가승인신청서에 다음 각 호의 서류를 첨부하여 방위사업청장에게 제출하여야 한다.
1. 무역업고유번호증 사본 1부
2. 구매국 정부 또는 그 대행기관이 발행한 구매요구서 1부
3. 구매국의 관례상 제2호의 서류발행이 곤란한 경우에는 구매국 주재 공관장이나 무관 또는 신뢰할 수 있는 기관이 확인한 구매정보 및 이들 정보의 확보경위서 1부

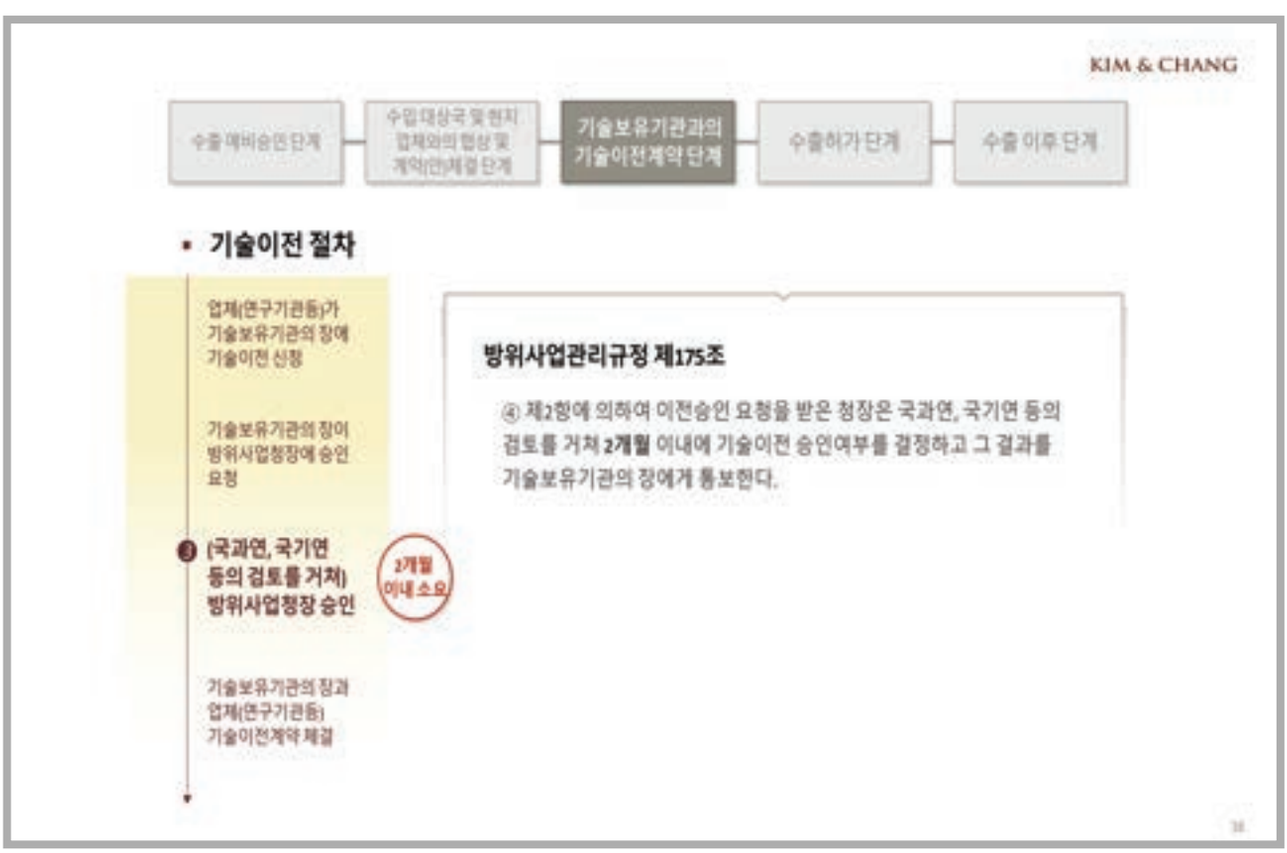

KIM & CHANG
수출 예비승인 단계
수입 대상국 및 현지 업체와의 협상 및 계약(안)체결 단계
기술보유기관과의 기술이전계약 단계
수출허가 단계
수출 이후 단계
▪ 구체적인 계약 내용 협의
◦ 수출할 방산물자 및 국방과학기술의 범위를 개략적으로 협의
◦ 국방과학기술 이전 시
◦ 기술보유기관으로부터 이전 받을 국방과학기술의 범위와 내용을 고려하여 협의하여야 하고 (이전 불가 핵심기술 등 고려)
◦ 기술료, 기술료 지급방법, 납입시기, 기타 기술이전 조건 등 포함
◦ (방위산업기술의 경우) 방산기술 보호대책 포함
◦ 계약서에 방위사업관리규정 제199조에서 정하는 사항 포함하여 규정

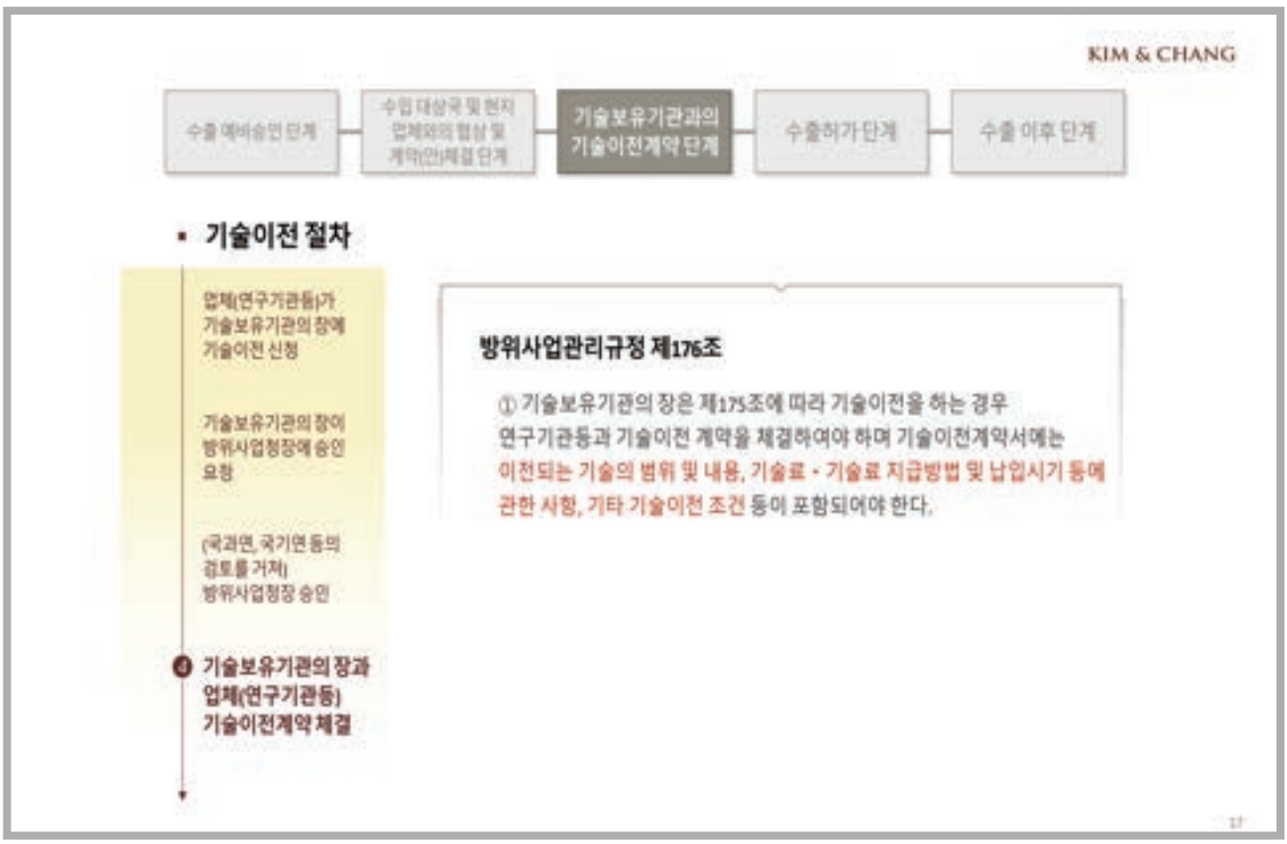

KIM & CHANG
수출 예비승인 단계
수입 대상국 및 현지 업체와의 협상 및 계약(안)체결 단계
기술보유기관과의 기술이전계약 단계
수출허가 단계
수출 이후 단계
▪ 국내 유관기관 설득 방안 모색
◦ 방사청, 기품원, 국방과학연구소, 국정원, 민간 위원
▪ 향후 변경 가능성에 대한 대비
◦ 라이선스의 범위, 제공 기술자료의 범위, 기술보호대책, 한국 법령 준수 의무규정 등이 변경될 가능성
◦ 수입국 및 수입국 업체와의 계약(안)은 한국 정부의 승인을 조건부로 한다는 점 및 한국 정부의 수출승인 절차 과정에서 계약 내용 변경, 조건 부가 가능성 있다는 점 계약서 명기 필요
▪ 방위산업기술에 대한 추가 유의사항 - 방산기술 보호대책 강구 및 계약서 반영 필요
◦ 기술 유출이 발생할 경우, 사후적인 원상회복이 현실적으로 어려울 수 있으므로, 선제적으로 기술보호 및 유출방지를 위한 규정 계약서에 반영 필요


KIM & CHANG
수출 예비승인 단계
수입 대상국 및 현지 업체와의 협상 및 계약(안)체결 단계
기술보유기관과의 기술이전계약 단계
수출허가 단계
수출 이후 단계
• 국방연구개발사업을 통하여 얻어지는 개발성과물은 국유로 귀속되므로, 국과연 등 기술보유기관으로부터 기술이전을 받아야 함
국방과학기술혁신 촉진법 제10조
① 제8조에 따라 계약 또는 협약을 체결한 국방연구개발사업을 통해 얻어지는 개발성과물은 원칙적으로 국가의 소유로 한다.
• 이전받을 구체적인 국방과학기술의 범위와 내용 협의
• 기술보유기관에 기술이전신청을 하여 방사청의 승인을 얻어야 함

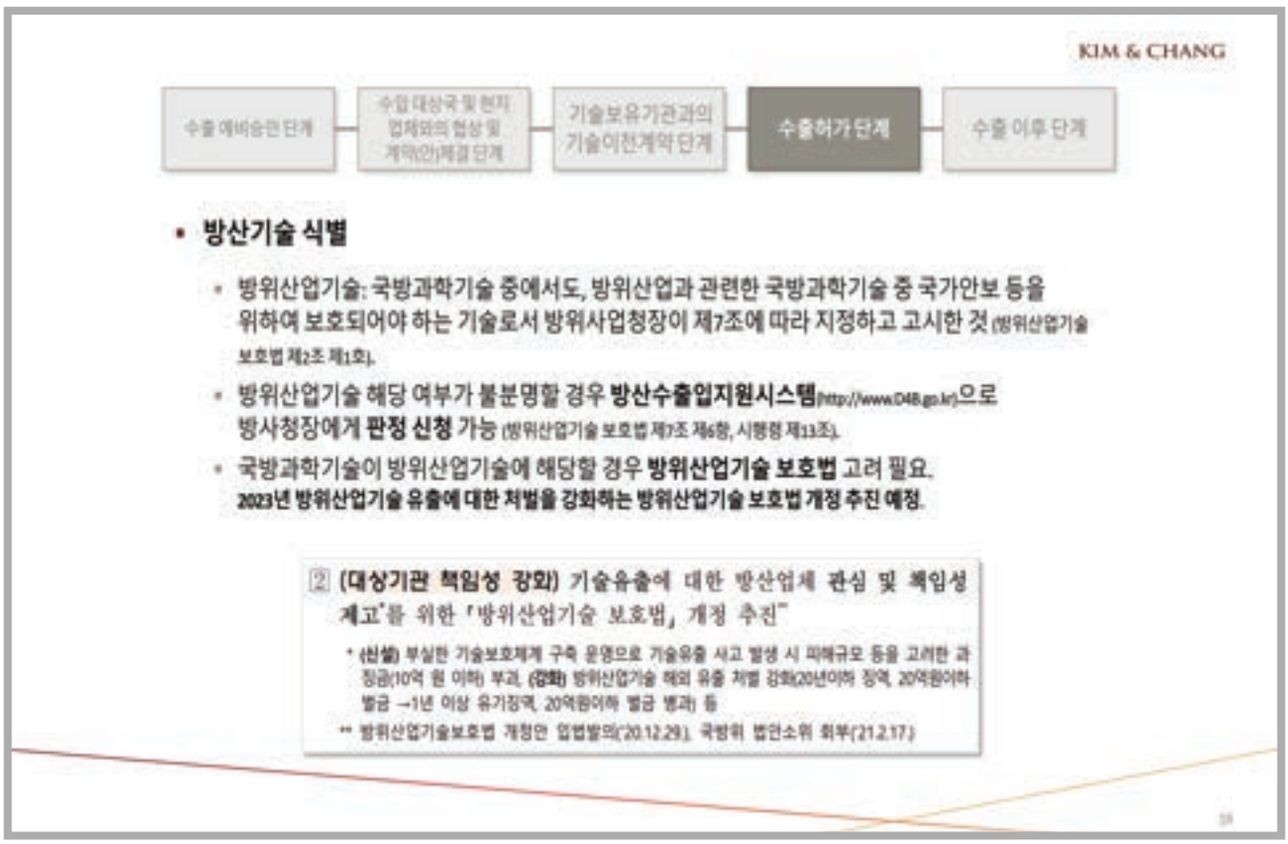

KIM & CHANG
수출 예비승인 단계
수입 대상국 및 현지 업체와의 협상 및 계약(안)체결 단계
기술보유기관과의 기술이전계약 단계
수출허가 단계
수출 이후 단계
• 기술이전 절차
업체(연구기관등)가 기술보유기관의 장에 기술이전 신청
기술보유기관의 장이 방위사업청장에 승인 요청
(국과연, 국기연 등의 검토를 거쳐) 방위사업청장 승인
기술보유기관의 장과 업체(연구기관등) 기술이전계약 체결
방위사업관리규정 제175조
① 「혁신법 시행령」 제16조에 따라 국방과학기술을 이전받고자 하는 기업, 대학, 연구기관 및 국방과학기술 관련 기관·단체 등(이하 "연구기관등"이라 한다)은 다음 각 호의 서류를 첨부하여 해당 기술을 보유한 기술보유기관의 장에게 기술이전을 신청해야 한다.
1. 기술이전의 목적
2. 이전을 받고자 하는 기술내용
3. 이전 받고자하는 기술에 대한 활용 계획서
4. 기술료 감면 사유

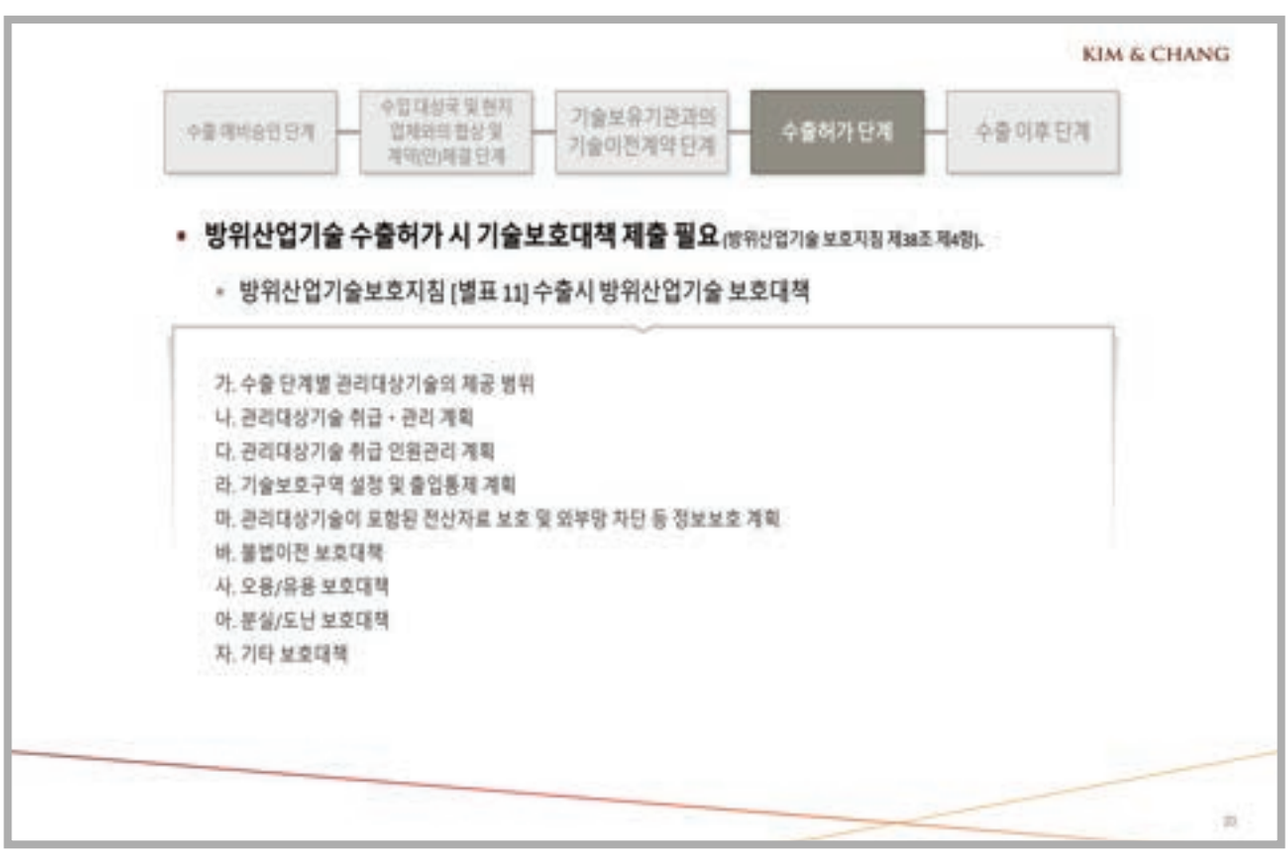

KIM & CHANG
수출 예비승인 단계
수입 대상국 및 현지 업체와의 협상 및 계약(안)체결 단계
기술보유기관과의 기술이전계약 단계
수출허가 단계
수출 이후 단계
• 기술이전 절차
업체(연구기관등)가 기술보유기관의 장에 기술이전 신청
❷ 기술보유기관의 장이 방위사업청장에 승인 요청
1개월 이내 소요
(국과연, 국기연 등의 검토를 거쳐) 방위사업청장 승인
기술보유기관의 장과 업체(연구기관등) 기술이전계약 체결
방위사업관리규정 제175조
② 기술보유기관의 장은 제1항에 따라 기술이전 신청을 받은 날부터 1개월 이내에 다음 각 호의 사항을 자체 심의 절차에 따라 검토한 후 청장에게 이전승인을 요청하여야 한다. 다만, 「방위산업기술 보호법」 제7조제6항 및 같은 법 시행령 제13조에 따라 기술보유기관이 방위산업기술 판정 신청에서부터 판정 결과가 나올 때까지 걸리는 기간은 본문에 따른 기간에 포함하지 아니한다.
1. 기술이전의 범위 및 내용
2. 기술이전 대상자의 적격 여부(기술이전을 통한 사업수행 계획의 타당성 등 고려)
3. 기술이전의 필요성
4. 기술료 산정 기준, 징수액 및 징수방법
5. 기술료 감면 사유
6. 기술이전의 절차 및 문제점
7. 기술이전 시 기술이전을 받은 기관 등이 준수해야할 제한사항
8. 기타 기술이전 시 필요한 사항


KIM & CHANG
수출 예비승인 단계
수입 대상국 및 현지 업체와의 협상 및 계약(안)체결 단계
기술보유기관과의 기술이전계약 단계
수출허가 단계
수출 이후 단계
• 기술이전 절차
업체(연구기관등)가 기술보유기관의 장에 기술이전 신청
기술보유기관의 장이 방위사업청장에 승인 요청
❸ (국과연, 국기연 등의 검토를 거쳐) 방위사업청장 승인
2개월 이내 소요
기술보유기관의 장과 업체(연구기관등) 기술이전계약 체결
방위사업관리규정 제175조
④ 제2항에 의하여 이전승인 요청을 받은 청장은 국과연, 국기연 등의 검토를 거쳐 2개월 이내에 기술이전 승인여부를 결정하고 그 결과를 기술보유기관의 장에게 통보한다.


KIM & CHANG
수출 예비승인 단계
수입 대상국 및 현지 업체와의 협상 및 계약안 체결 단계
기술보유기관과의 기술이전계약 단계
수출허가 단계
수출 이후 단계
▪ 기술이전 절차
업체(연구기관등)가 기술보유기관의 장에 기술이전 신청
기술보유기관의 장이 방위사업청장에 승인 요청
(국과연, 국기연 등의 검토를 거쳐) 방위사업청장 승인
❹ 기술보유기관의 장과 업체(연구기관등) 기술이전계약 체결
방위사업관리규정 제176조
① 기술보유기관의 장은 제175조에 따라 기술이전을 하는 경우 연구기관등과 기술이전 계약을 체결하여야 하며 기술이전계약서에는 이전되는 기술의 범위 및 내용, 기술료 · 기술료 지급방법 및 납입시기 등에 관한 사항, 기타 기술이전 조건 등이 포함되어야 한다.

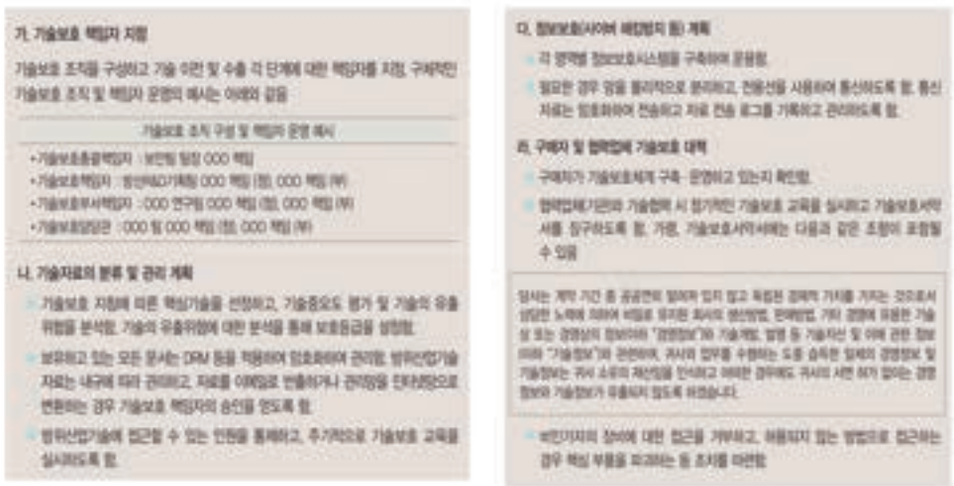

KIM & CHANG
수출 예비승인 단계
수입 대상국 및 현지 업체와의 협상 및 계약안 체결 단계
기술보유기관과의 기술이전계약 단계
수출허가 단계
수출 이후 단계
▪ 기술이전계약서 내용
◦ 기술료 부과금액 · 납부시기 · 방법, 기술이전과 관련하여 연구기관등의 준수사항 및 계약위반에 따른 손해배상 청구사항을 포함하여, 방위사업관리규정 제176조 제2항 각호에서 정하는 사항 포함시켜야 함.
▪ 기술료 산정(절차의 복잡 및 장기화) 및 기술료 감면 여부 협의:
◦ "국방과학 기술료 산정·징수방법 및 징수절차 등에 관한 고시" 최근 개정되어 경상기술료 감면에 관한 특례 조항 연장됨
국방과학 기술료 산정·징수방법 및 징수절차 등에 관한 고시 부칙 제2조
"수출촉진을 위하여 국방과학기술을 활용하여 수출하는 경우에는 제4조제3항제1호 및 제4조제5항제2호에도 불구하고 이 고시 시행일부터 2024년 12월 31일 까지 경상기술료를 제4조제3항제1호의 경우 순조달가격의 0.5%, 제4조제5항제2호의 경우 순판매가격의 1%로 감면한다. 이 경우 방위사업청장의 승인을 요하지 않는다."
▪ (가능하다면) 수입국과의 협상(계약) 내용에 기술보유기관과의 기술이전계약 내용 반영


KIM & CHANG
수출 예비승인 단계
수입 대상국 및 현지 업체와의 협상 및 계약(안)체결 단계
기술보유기관과의 기술이전계약 단계
수출허가 단계
수출 이후 단계
• 방산기술 식별
• 방위산업기술: 국방과학기술 중에서도, 방위산업과 관련한 국방과학기술 중 국가안보 등을 위하여 보호되어야 하는 기술로서 방위사업청장이 제7조에 따라 지정하고 고시한 것 (방위산업기술 보호법 제2조 제1호).
• 방위산업기술 해당 여부가 불분명할 경우 방산수출입지원시스템(http://www.D4B.go.kr)으로 방사청장에게 판정 신청 가능 (방위산업기술 보호법 제7조 제6항, 시행령 제13조).
• 국방과학기술이 방위산업기술에 해당할 경우 방위산업기술 보호법 고려 필요.
2023년 방위산업기술 유출에 대한 처벌을 강화하는 방위산업기술 보호법 개정 추진 예정.
2 (대상기관 책임성 강화) 기술유출에 대한 방산업체 관심 및 책임성 제고를 위한 「방위산업기술 보호법」 개정 추진"
* (신설) 부실한 기술보호체계 구축 운영으로 기술유출 사고 발생 시 피해규모 등을 고려한 과징금(10억 원 이하) 부과, (강화) 방위산업기술 해외 유출 처벌 강화(20년이하 징역, 20억원이하 벌금 →1년 이상 유기징역, 20억원이하 벌금 병과) 등
** 방위산업기술보호법 개정안 입법발의('20.12.29.), 국방위 법안소위 회부('21.2.17.)


KIM & CHANG
수출 예비승인 단계
수입 대상국 및 현지 업체와의 협상 및 계약(안)체결 단계
기술보유기관과의 기술이전계약 단계
수출허가 단계
수출 이후 단계
• 방위산업기술 수출허가 시 기술보호대책 제출 필요 (방위산업기술 보호지침 제38조 제4항).
• 방위산업기술보호지침 [별표 11] 수출시 방위산업기술 보호대책
가. 수출 단계별 관리대상기술의 제공 범위
나. 관리대상기술 취급·관리 계획
다. 관리대상기술 취급 인원관리 계획
라. 기술보호구역 설정 및 출입통제 계획
마. 관리대상기술이 포함된 전산자료 보호 및 외부망 차단 등 정보보호 계획
바. 불법이전 보호대책
사. 오용/유용 보호대책
아. 분실/도난 보호대책
자. 기타 보호대책

KIM & CHANG

[참고] 방사청, 국정원 방위산업기술 수출단계별 기술보호 안내서(2023)



ㄱ. 기술보호 책임자 지정

기술보호 조직을 구성하고 기술 이전 및 수출 각 단계에 대한 책임자를 지정, 구체적인 기술보호 조직 및 책임자 운영의 예시는 아래와 같음

기술보호 조직 구성 및 책임자 운영 예시

- 기술보호총괄책임자 : 보안팀 팀장 000 책임
- 기술보호책임자 : 방산제품기획팀 000 책임 (정), 000 책임 (부)
- 기술보호부서책임자 : 000 연구팀 000 책임 (정), 000 책임 (부)
- 기술보호담당관 : 000 팀 000 책임 (정), 000 책임 (부)

ㄴ. 기술자료의 분류 및 관리 계획

- 기술보호 지침에 따른 핵심기술을 선정하고, 기술중요도 평가 및 기술의 유출 위험을 분석함. 기술의 유출위험에 대한 분석을 통해 보호등급을 설정함.
- 보유하고 있는 모든 문서는 DRM 등을 적용하여 암호화하여 관리함. 방위산업기술 자료는 내규에 따라 관리하고, 자료를 이메일로 반출하거나 관리망을 단차원으로 변환하는 경우 기술보호 책임자의 승인을 얻도록 함.
- 방위산업기술에 접근할 수 있는 인원을 통제하고, 주기적으로 기술보호 교육을 실시하도록 함.

ㄷ. 정보보호시스템 구축 계획

- 각 방역별 정보보호시스템을 구축하여 운영함.
- 필요한 경우 망을 물리적으로 분리하고, 전용선을 사용하여 통신하도록 함. 통신 자료는 암호화하여 전송하고 자료 전송 로그를 기록하고 관리하도록 함.

ㄹ. 구매처 및 협력업체 기술보호 대책

- 구매처가 기술보호체계 구축·운영하고 있는지 확인함.
- 협력업체(기관)와 기술협력 시 참가하는 기술보호 교육을 실시하고 기술보호서약서를 징구하도록 함. 가령, 기술보호서약서에는 다음과 같은 조항이 포함될 수 있음

당사는 계약 기간 중 공공연히 알려져 있지 않고 독립된 경제적 가치를 가지는 갑으로서 상당한 노력에 의하여 비밀로 유지된 회사의 생산방법, 판매방법, 기타 경영에 유용한 기술상 또는 경영상의 정보이며 "경영정보"와 기술제품, 설계 등 기술자산 및 이에 관한 정보이며 "기술정보"의 관련하여, 귀사의 업무를 수행하는 도중 습득한 일체의 경영정보 및 기술정보는 귀사 소유의 재산임을 인식하고 어떠한 경우에도 귀사의 서면 허가 없이는 경영정보와 기술정보가 유출되지 않도록 유의합니다.

- 비인가자의 장비에 대한 접근을 거부하고, 허용되지 않는 방법으로 접근하는 경우 책임 부품을 파괴하는 등 조치를 마련함

KIM & CHANG

수출 예비승인 단계 | 수입 대상국 및 현지 업체와의 협상 및 계약(안)체결 단계 | 기술보유기관과의 기술이전계약 단계 | **수출허가 단계** | 수출 이후 단계

- **방산기술 식별 관련 주요 이슈**
  - **수출 대상 방위산업기술 식별 절차 고도화 경향**
  - **기술명세서 작성** 관련
    - 방사청 기술보호과는 **객관성이 담보된 방산기술 식별 및 기술명세서 작성하여 제출할 것**을 요구
    - 방위산업기술을 **구체적이고 세부적으로 구분**한 후, **방산기술 해당 여부 또는 비해당 여부에 대한 합리적이고 객관적인 식별근거를 제시**할 것을 요구함
    - **보호종류의 형태별** 식별 필요 (방위산업기술 보호지침 제3조, 제12조)

[방위산업기술 보호지침 제3조]

① 대상기관이 보호하여야 할 종류(이하 "보호종류"이라 한다)는 다음 각 호와 같다.

1. 방위산업기술 등의 도면(관련 소프트웨어를 포함한다) 및 품질보증 요구서
2. 방위산업기술 등을 설명하는 규격서 및 보고서
3. 방위산업기술 등이 포함된 견본, 시제품, 전자매체기록, 기술자료(Technical Data)
4. 그 밖에 방위산업기술 등을 포함하는 자료


KIM & CHANG
수출 예비승인 단계
수입 대상국 및 현지 업체와의 협상 및 계약(안)체결 단계
기술보유기관과의 기술이전계약 단계
수출허가 단계
수출 이후 단계
▪ 방산기술 식별 관련 주요 이슈 (기술명세서 관련)
◦ 기술보유기관의 방산기술 식별 및 업체 자체 보유 방산기술의 식별 필요 (TDP, MDP)
◦ 업체 자체 심의회 결과 및 국과연의 심의회 결과 반영 필요
◦ 기술수출협의회 준비에 앞서 방사청의 요구 사항 확인 필요


KIM & CHANG
수출 예비승인 단계
수입 대상국 및 현지 업체와의 협상 및 계약(안)체결 단계
기술보유기관과의 기술이전계약 단계
수출허가 단계
수출 이후 단계
▪ 기술 수출 허가를 위한 기술수출협의회 절차
◦ 기술수출협의회에서 수출허가 전 기술수출 가능 여부 검토
방위사업관리규정 제183조
③ 국방기술보호국장은 기술수출 허가 신청 전에 기술수출 가능여부를 검토하기 위하여 국방기술보호국장을 위원장으로 하고 방위산업진흥국, 방위사업정책국, 국제협력관, 사업본부, 국방부, 국가정보원, 군사안보지원사령부, 국과연, 국기연, 방산기술센터, 관련 공공기관을 포함한 외부 민간전문가 및 방산업체 등이 참여하는 기술수출협의회를 운영한다.
◦ 절차 진행 중 제기되는 반대의견 및 기술유출에 대한 우려에 대한 대응 방안 강구
◦ 기술수출협의회 자료 준비
◦ 주요 내용: 사업 및 기술수출 개요, 기술분류 검토결과, 기술보호 대책, 기술수출로 인한 국내 파급효과 등
◦ "대량 기술이전"에 대한 우려를 불식시킬 수 있는 논리 개발 및 자료 준비 필요

KIM & CHANG

수출 예비승인 단계 | 수입 대상국 및 현지 업체와의 협상 및 계약(안)체결 단계 | 기술보유기관과의 기술이전계약 단계 | **수출허가 단계** | 수출 이후 단계

- **기술수출협의회 절차 관련 주요 이슈**
  - 수출/이전 대상 방산물자, 국방과학기술의 범위, 내용의 적절성 심의: 이전 불가한 핵심 기술의 존부, 범위 등 검토
    - 핵심 설계기술, 핵심원자재 및 핵심부품 제조 기술, 핵심S/W 이전 여부 등에 대한 집중 심의
  - 방산기술 보호대책 강구 및 반영
  - 현지 업체 실태조사(audit) 가능 여부 확인
  - 현지 업체의 보안조치능력 점검
  - subcontractor, subsidiaries에 대한 기술이전 시 이들 업체에 대한 추가적인 보안대책 마련
  - 우방국/비우방국 여부에 따른 고려
  - 기술수출협의회/분과위원회 절차 중 협의된 내용, 부가된 조건 등을 수입국과의 계약 내용에 반영하도록 수입국 및 수입국 업체와의 추가 협상

KIM & CHANG

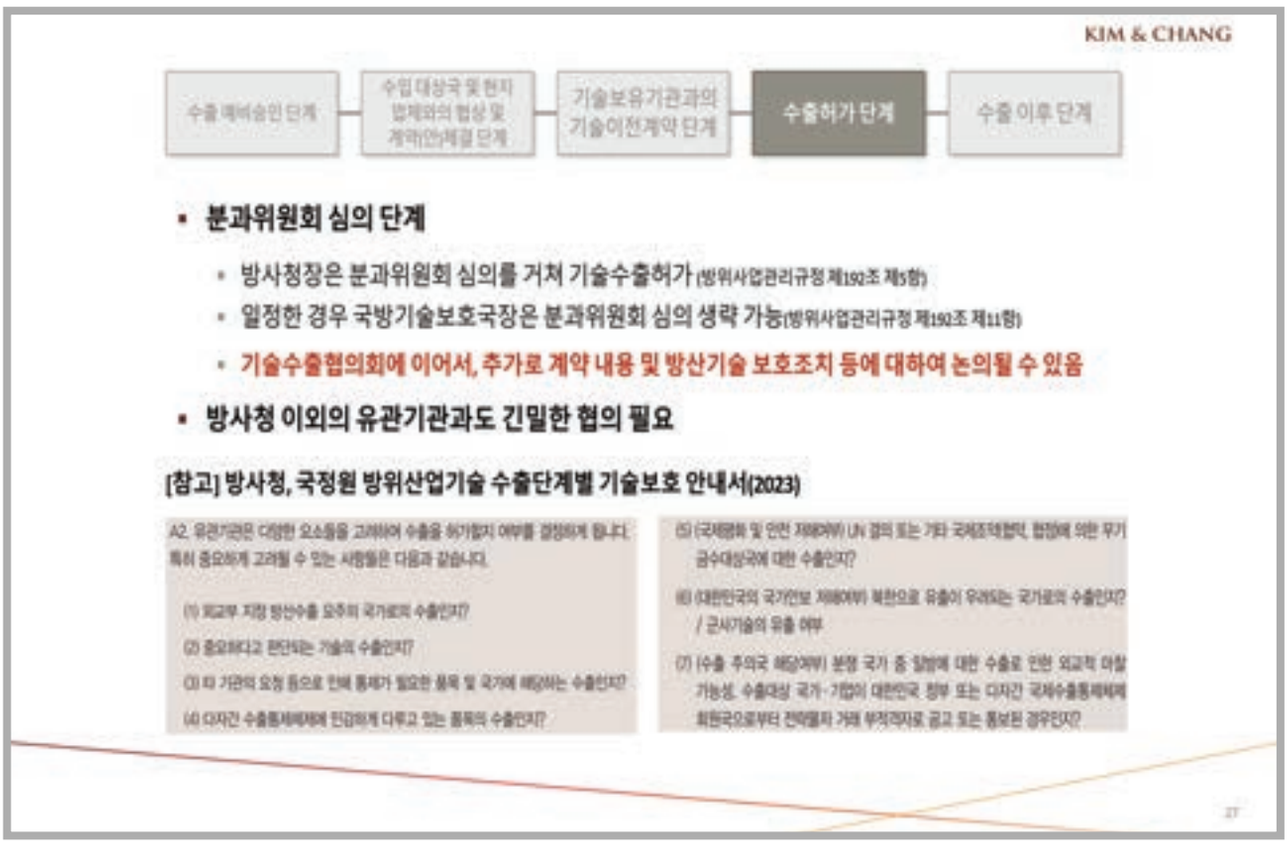
수출 예비승인 단계 | 수입 대상국 및 현지 업체와의 협상 및 계약(안)체결 단계 | 기술보유기관과의 기술이전계약 단계 | **수출허가 단계** | 수출 이후 단계

- **수출허가 신청서 제출**
  - 수출허가신청서와 방위사업관리규정 제192조 제5항의 문서 제출

방위사업관리규정 제192조

⑤ 기술을 수출하고자 하는 기술보유기관 및 업체는 규칙 별지 제19호의 수출허가신청서에 다음 각 호의 서류를 갖추어 분과위원회 심의를 거쳐 청장의 허가를 받아야 한다. 절충교역에 의하여 기술을 수출하는 경우에도 또한 같다.

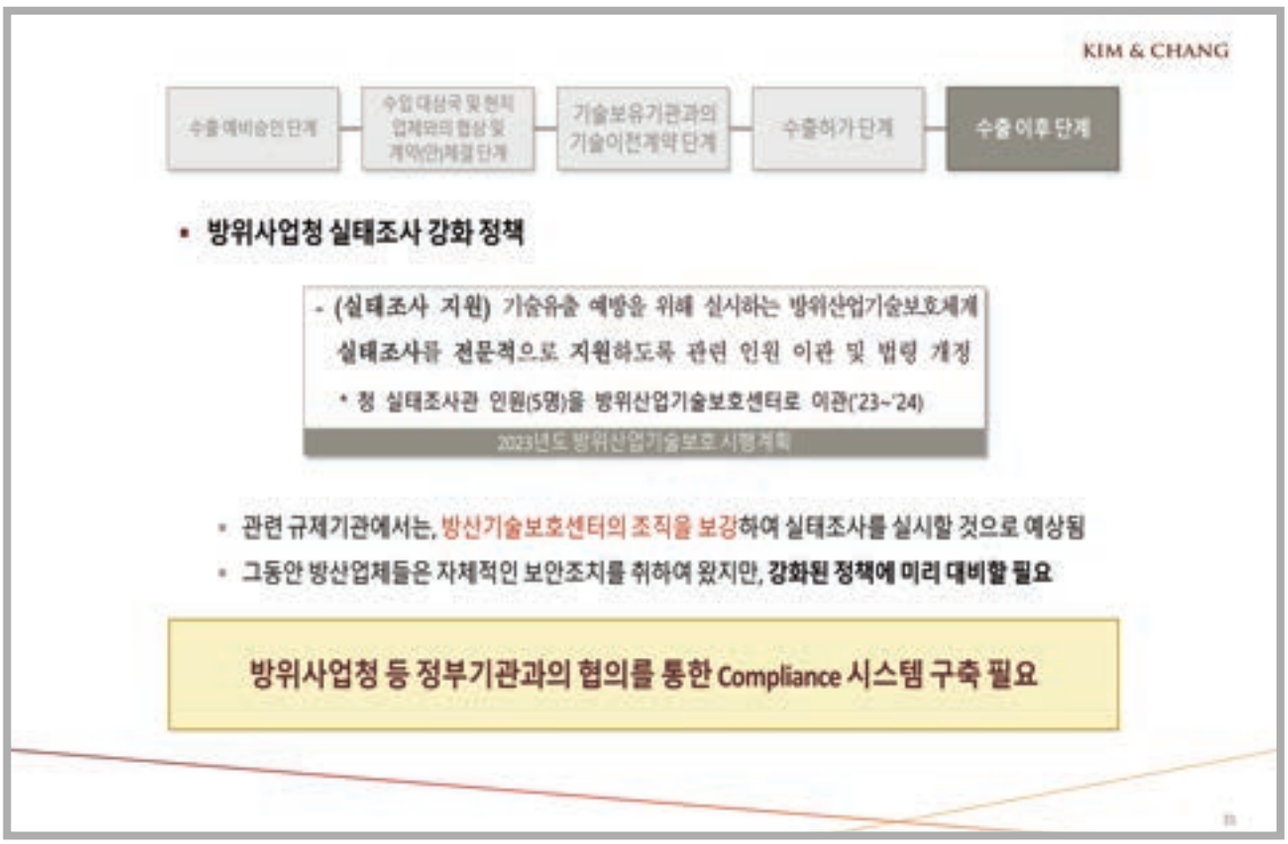
1. **수출계약안** 1부
2. 당해 기술획득경위서 및 기술보유기관과의 **기술이전계약서** 1부
3. 수출상대국 및 수출허가를 받고자 하는 자와의 **관계설명서** 1부
4. 당해 기술의 수출로 인한 국내외의 **파급효과설명서** 1부
5. 제183조제3항에 따른 **기술수출협의회 검토 결과**
6. 방위산업기술의 경우, 「방위산업기술 보호지침」 별표 1(1)(수출시 방위산업기술 보호대책) 1부


KIM & CHANG
수출 예비승인 단계
수입 대상국 및 현지 업체와의 협상 및 계약(안)체결 단계
기술보유기관과의 기술이전계약 단계
수출허가 단계
수출 이후 단계
▪ 분과위원회 심의 단계
▪ 방사청장은 분과위원회 심의를 거쳐 기술수출허가 (방위사업관리규정 제192조 제5항)
▪ 일정한 경우 국방기술보호국장은 분과위원회 심의 생략 가능(방위사업관리규정 제192조 제11항)
▪ 기술수출협의회에 이어서, 추가로 계약 내용 및 방산기술 보호조치 등에 대하여 논의될 수 있음
▪ 방사청 이외의 유관기관과도 긴밀한 협의 필요
[참고] 방사청, 국정원 방위산업기술 수출단계별 기술보호 안내서(2023)
A2. 유관기관은 다양한 오소등을 고려하여 수출을 허가할지 여부를 결정하게 됩니다. 특히 중요하게 고려될 수 있는 사항들은 다음과 같습니다.
(1) 외교부 지정 방산수출 요주의 국가로의 수출인지?
(2) 중요하다고 판단되는 기술의 수출인지?
(3) 타 기관의 요청 등으로 인해 통제가 필요한 품목 및 국가에 해당하는 수출인지?
(4) 다자간 수출통제체제에 민감하게 다루고 있는 품목의 수출인지?
(5) (국제평화 및 안전 저해여부) UN 결의 또는 기타 국제조약협약, 협정에 의한 무기 금수대상국에 대한 수출인지?
(6) (대한민국의 국가안보 저해여부) 북한으로 유출이 우려되는 국가로의 수출인지? / 군사기술의 유출 여부
(7) (수출 주의국 해당여부) 분쟁 국가 중 일방에 대한 수출로 인한 외교적 마찰 가능성, 수출대상 국가·기업이 대한민국 정부 또는 다자간 국제수출통제체제 회원국으로부터 전략물자 거래 부적격자로 공고 또는 통보된 경우인지?
27

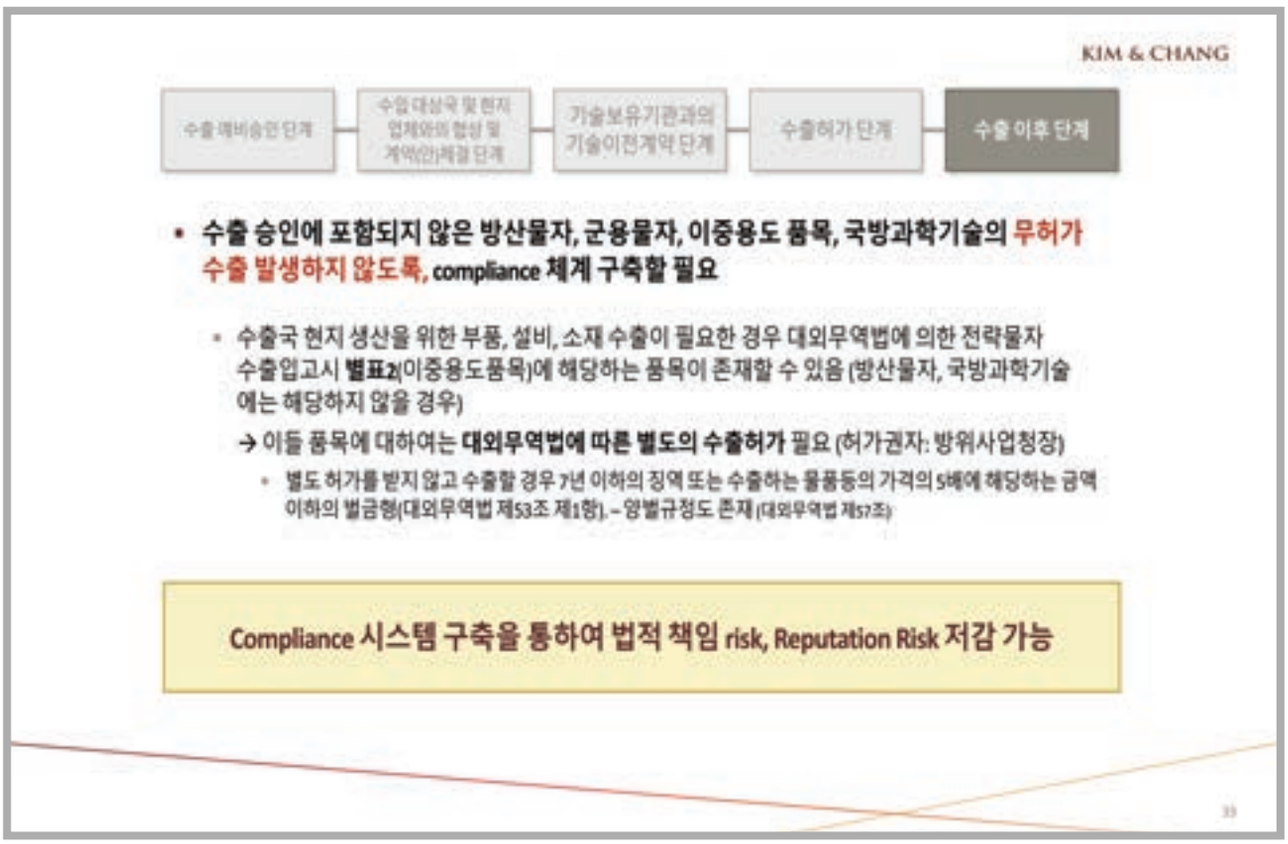

KIM & CHANG
수출 예비승인 단계
수입 대상국 및 현지 업체와의 협상 및 계약(안)체결 단계
기술보유기관과의 기술이전계약 단계
수출허가 단계
수출 이후 단계
▪ 무허가 수출 시 제재
▪ 거짓 또는 부정한 방법으로 수출허가를 받거나 허가를 받지 않고 국방과학기술 수출할 경우 10년 이하의 징역이나 금고 또는 1억원 이하의 벌금에 처해짐 (방위사업법 제62조 제2항)
▪ 사전에 수출허가를 받았어야 함에도 인식 부족으로 간과하여 문제 발생 시 사업적 영향은 물론 회사의 평판에도 악영향 초래
▪ 수출허가를 간과하고 수출하는 경우 수출입 제한 등의 행정처분
28


KIM & CHANG
수출 예비승인 단계
수입 대상국 및 현지 업체와의 협상 및 계약(안)체결 단계
기술보유기관과의 기술이전계약 단계
수출허가 단계
수출 이후 단계
• 방위사업청 방위산업기술에 대한 (정기/수시) 실태조사 대비 필요
방위산업기술 보호지침 제38조
⑤ 국방기술보호국장은 대상기관 및 전항 후단의 수출 상대방이 제4항에 따른 보호대책을 준수하는지를 확인할 수 있다. 이 경우 대상기관의 장은 특별한 사유가 없으면 확인에 협조하여야 한다.
• 방위산업기술 보호지침 [별표 12]에서 각 카테고리별로 실태조사 항목 상세히 규정:
1. 기술의 식별·관리, 2. 인원통제, 3. 시설보호, 4. 정보보호, 5. 연구개발 및 수출·국내이전 시 기술보호/방산협력업체 기술보호
• 특히, 방위산업기술에 대한 기술보호대책 적용 여부 실태조사 가능
• 실태조사 결과 부실함이 드러난 경우, 개선권고 → 시정명령 → 과태료 부과 가능


KIM & CHANG
수출 예비승인 단계
수입 대상국 및 현지 업체와의 협상 및 계약(안)체결 단계
기술보유기관과의 기술이전계약 단계
수출허가 단계
수출 이후 단계
• 실태조사 결과에 따른 시정명령 등
방위산업기술 보호지침 제43조
① 방위사업청장은 실태조사를 실시하는 경우에 별표 12의 실태조사 핵심 점검항목 등을 고려하여 방위산업기술 보호체계 구축·운영 현황에 대한 부실 여부 등을 판단하고, 필요한 경우에는 법 제13조제2항에 따라 대상기관의 장에게 개선을 권고할 수 있다.
방위산업기술 보호지침 제44조
① 방위사업청장은 제43조제1항에 따른 개선권고를 이행하지 않거나 불성실하게 이행한다고 판단되는 경우 대상기관의 장에게 시정을 명할 수 있다.
방산기술보호법 제24조
① 다음 각 호의 어느 하나에 해당하는 사람에게는 3천만원 이하의 과태료를 부과한다.
2. 제13조제3항에 따른 시정명령을 이행하지 아니한 사람


KIM & CHANG
수출 예비승인 단계
수입 대상국 및 현지 업체와의 협상 및 계약(안)체결 단계
기술보유기관과의 기술이전계약 단계
수출허가 단계
수출 이후 단계
▪ 방위사업청 실태조사 강화 정책
- (실태조사 지원) 기술유출 예방을 위해 실시하는 방위산업기술보호체계 실태조사를 전문적으로 지원하도록 관련 인원 이관 및 법령 개정
* 청 실태조사관 인원(5명)을 방위산업기술보호센터로 이관('23~'24)
2023년도 방위산업기술보호 시행계획
▪ 관련 규제기관에서는, 방산기술보호센터의 조직을 보강하여 실태조사를 실시할 것으로 예상됨
▪ 그동안 방산업체들은 자체적인 보안조치를 취하여 왔지만, 강화된 정책에 미리 대비할 필요
방위사업청 등 정부기관과의 협의를 통한 Compliance 시스템 구축 필요

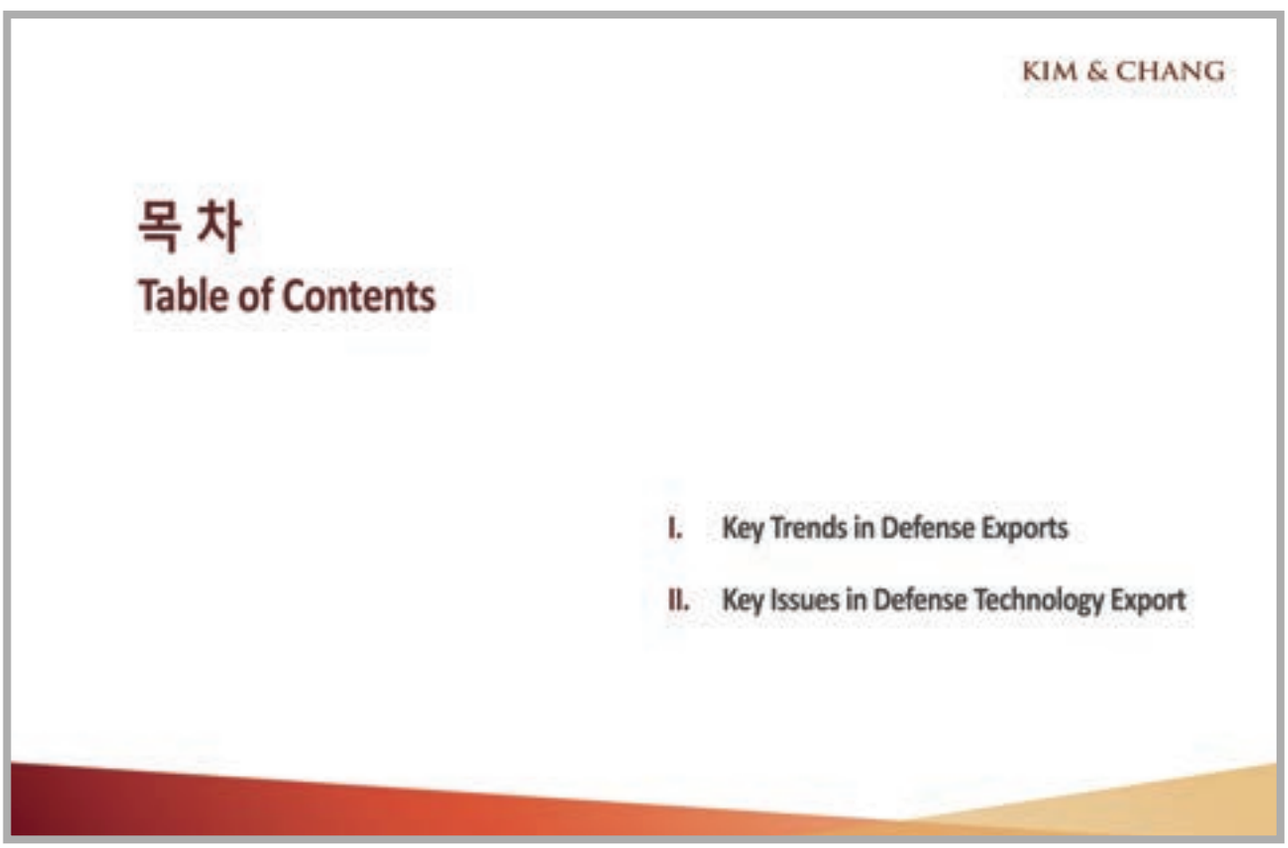

KIM & CHANG
수출 예비승인 단계
수입 대상국 및 현지 업체와의 협상 및 계약(안)체결 단계
기술보유기관과의 기술이전계약 단계
수출허가 단계
수출 이후 단계
▪ 현지 업체들에 대한 수시 보안 점검 필요
▪ 특히 물자와 기술을 수출하고, 국내 인력이 해외에 파견될 경우, 수입국가와 수입회사에서는 최대한 회사의 기술정보를 파악해 내기 위해 노력할 것이 예상됨
▪ 이에 대비하여 기술 유출을 방지하기 위한 철저한 보안관리 체계 구축(내부 규정이나 관련 계약들을 통한 이중, 삼중의 보호조치)이 요구됨
▪ 실태조사 관련 조항 협의 필요


KIM & CHANG
수출 이후 단계
• 수출 승인에 포함되지 않은 방산물자, 군용물자, 이중용도 품목, 국방과학기술의 무허가 수출 발생하지 않도록, compliance 체계 구축할 필요
• 수출국 현지 생산을 위한 부품, 설비, 소재 수출이 필요한 경우 대외무역법에 의한 전략물자 수출입고시 별표2(이중용도품목)에 해당하는 품목이 존재할 수 있음 (방산물자, 국방과학기술에는 해당하지 않을 경우)
→ 이들 품목에 대하여는 대외무역법에 따른 별도의 수출허가 필요 (허가권자: 방위사업청장)
• 별도 허가를 받지 않고 수출할 경우 7년 이하의 징역 또는 수출하는 물품등의 가격의 5배에 해당하는 금액 이하의 벌금형(대외무역법 제53조 제1항). – 양벌규정도 존재 (대외무역법 제57조)
Compliance 시스템 구축을 통하여 법적 책임 risk, Reputation Risk 저감 가능

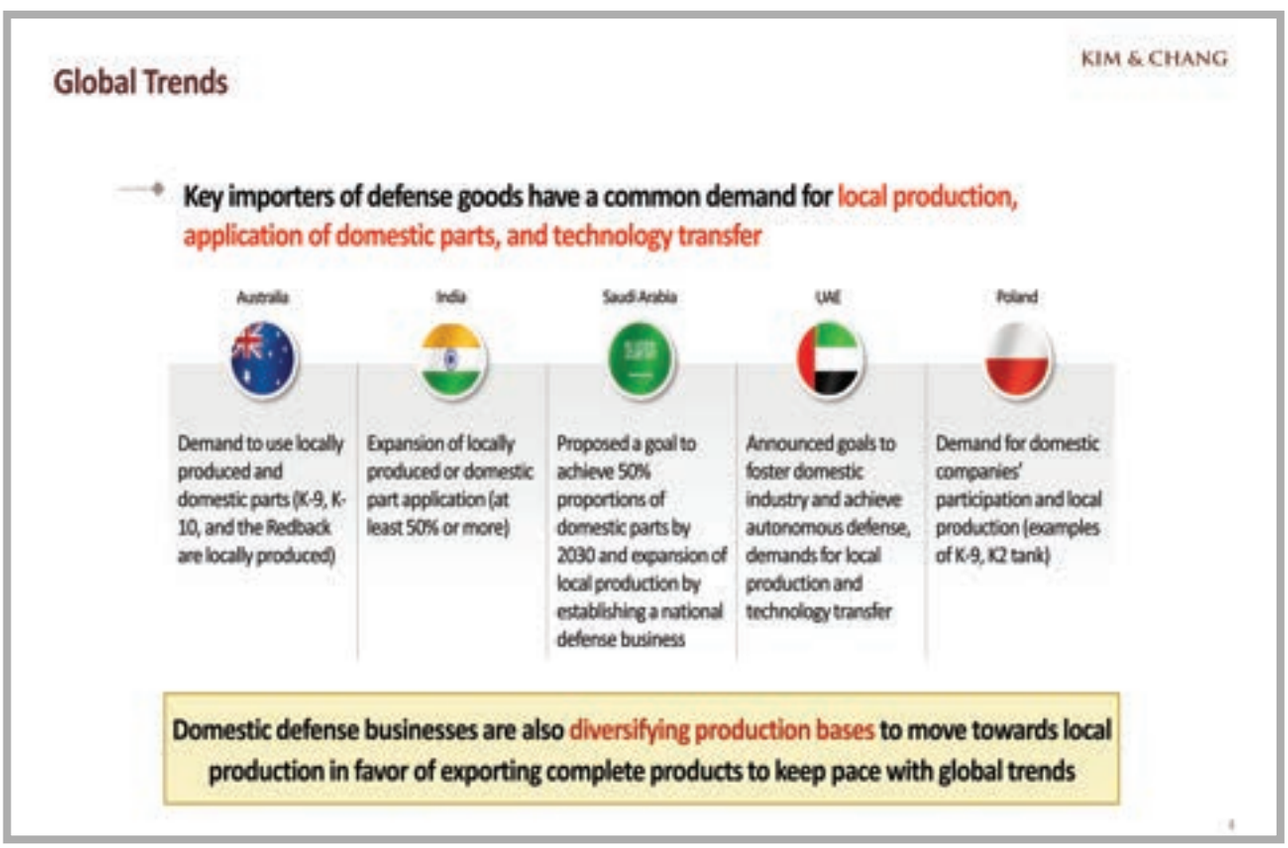

Questions & Answers

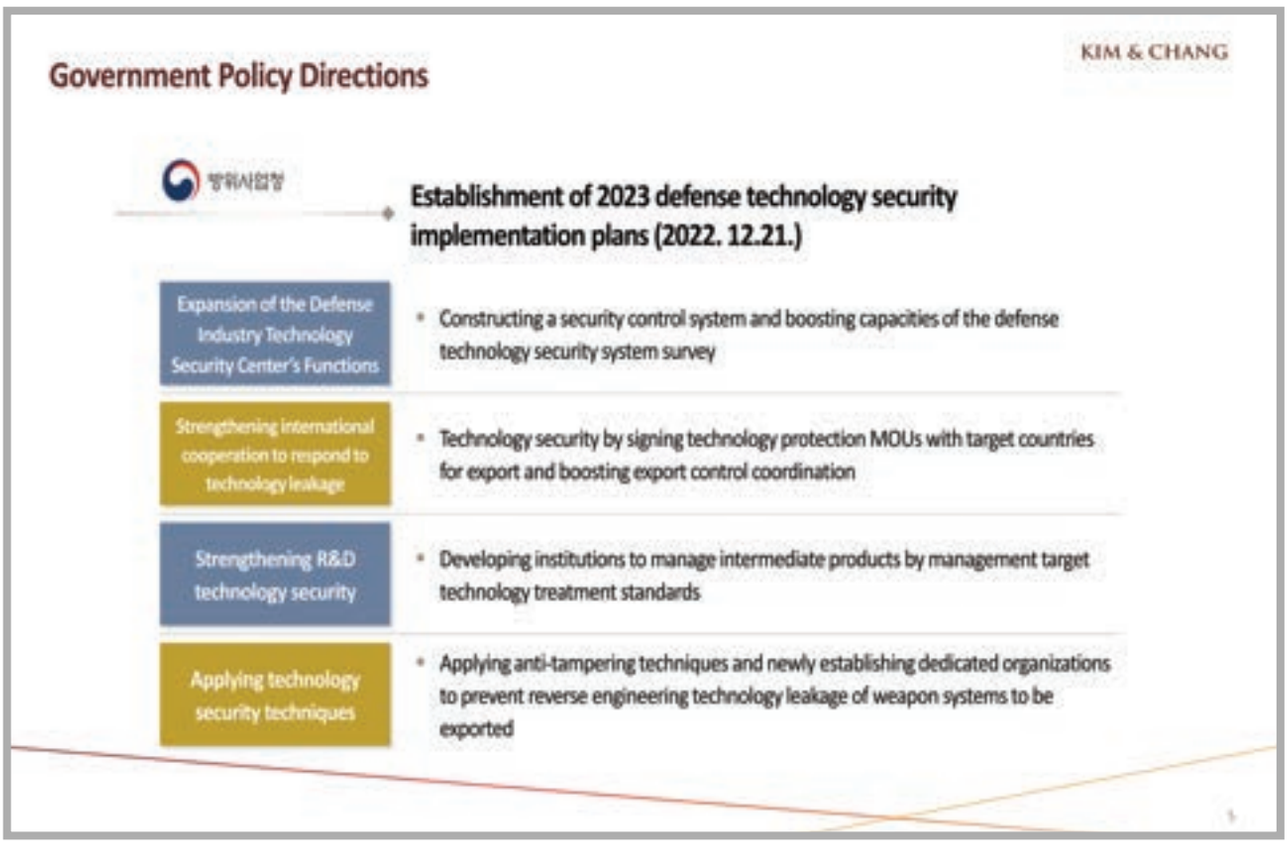

감사합니다
KIM & CHANG


KIM & CHANG
Defense Technology Export and Key Issues


KIM & CHANG
목 차
Table of Contents
I. Key Trends in Defense Exports
II. Key Issues in Defense Technology Export


I. Key Trends in Defense Exports


Global Trends
KIM & CHANG
Key importers of defense goods have a common demand for local production, application of domestic parts, and technology transfer
Australia
India
Saudi Arabia
UAE
Poland
Demand to use locally produced and domestic parts (K-9, K-10, and the Redback are locally produced)
Expansion of locally produced or domestic part application (at least 50% or more)
Proposed a goal to achieve 50% proportions of domestic parts by 2030 and expansion of local production by establishing a national defense business
Announced goals to foster domestic industry and achieve autonomous defense, demands for local production and technology transfer
Demand for domestic companies' participation and local production (examples of K-9, K2 tank)
Domestic defense businesses are also diversifying production bases to move towards local production in favor of exporting complete products to keep pace with global trends

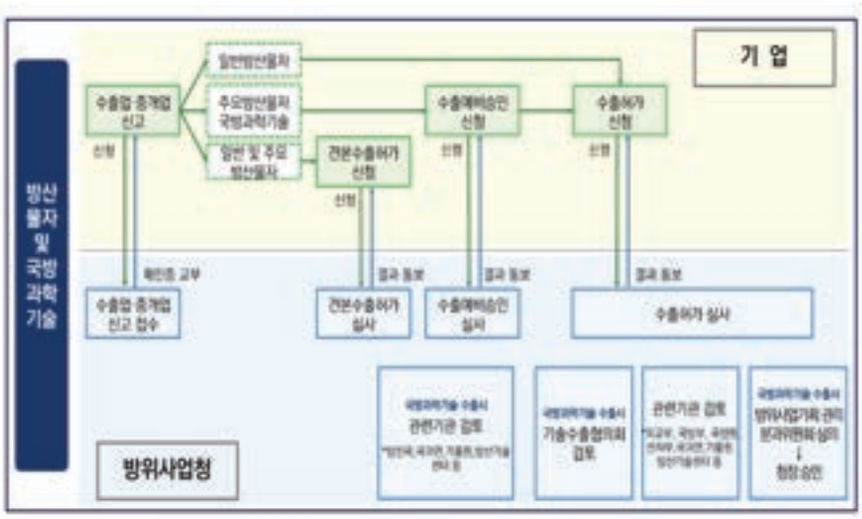

Government Policy Directions
KIM & CHANG
방위사업청
Establishment of 2023 defense technology security implementation plans (2022. 12.21.)
Expansion of the Defense Industry Technology Security Center's Functions
• Constructing a security control system and boosting capacities of the defense technology security system survey
Strengthening international cooperation to respond to technology leakage
• Technology security by signing technology protection MOUs with target countries for export and boosting export control coordination
Strengthening R&D technology security
• Developing institutions to manage intermediate products by management target technology treatment standards
Applying technology security techniques
• Applying anti-tampering techniques and newly establishing dedicated organizations to prevent reverse engineering technology leakage of weapon systems to be exported


Government Policy Directions
KIM & CHANG
방위사업청
Set to conduct a regular investigation for defense companies, supervised by the Defense Industry Security Center (2024)
Boosting identification and investigation of defense business' defense technologies by establishing a "Technology Export Guideline for Local Production and Local Development"
Initiating the construction of a technology security system by establishing a "Technology Transfer Security System Managing Institution between Domestic Businesses, Local Corporations, and Local Businesses" (2024)
Boosting expertise of military goods decisions through collaborating with KOSTI
Recently, cooperation between relevant institutions, export control systems, and technology security regulations are being heightened in consideration of dramatic increases in defense exports and life-cycle defense export methods (exporting completed products and technology transfers, localization, and maintenance)

II. Key Issues in Defense Technology Export

Overview of Defense goods and Defense Science and Technology Export Procedures

KIM & CHANG



Reference: DAPA, 「Defense Import and Export Guidance」, 2022. 8.

KIM & CHANG

Preliminary export authorization → Negotiation and contract (proposal) signing with the importing country and local businesses → Technology transfer contract with the agency in possession of technology → Export authorization → After export

- **Need for consultation with relevant agencies including preliminary export authorization**

Article 57 of the Defense Acquisition Program Act

③ **A person who intends to hold an export consulting meeting for major defense materials and defense technology shall obtain preliminary export approval from the Minister of the Defense Acquisition Program Administration**, as prescribed by Ordinance of the Ministry of National Defense, and each person, who intends to participate in international bidding, shall obtain approval for participation in international bidding from the Minister of the Defense Acquisition Program Administration, as prescribed by Ordinance of the Ministry of National Defense.

The technology security manual for each stage of exports also includes content on technology security before preliminary export authorization, in case of submitting proposals, etc.

KIM & CHANG

Preliminary export authorization → Negotiation and contract (proposal) signing with the importing country and local businesses → Technology transfer contract with the agency in possession of technology → Export authorization → After export

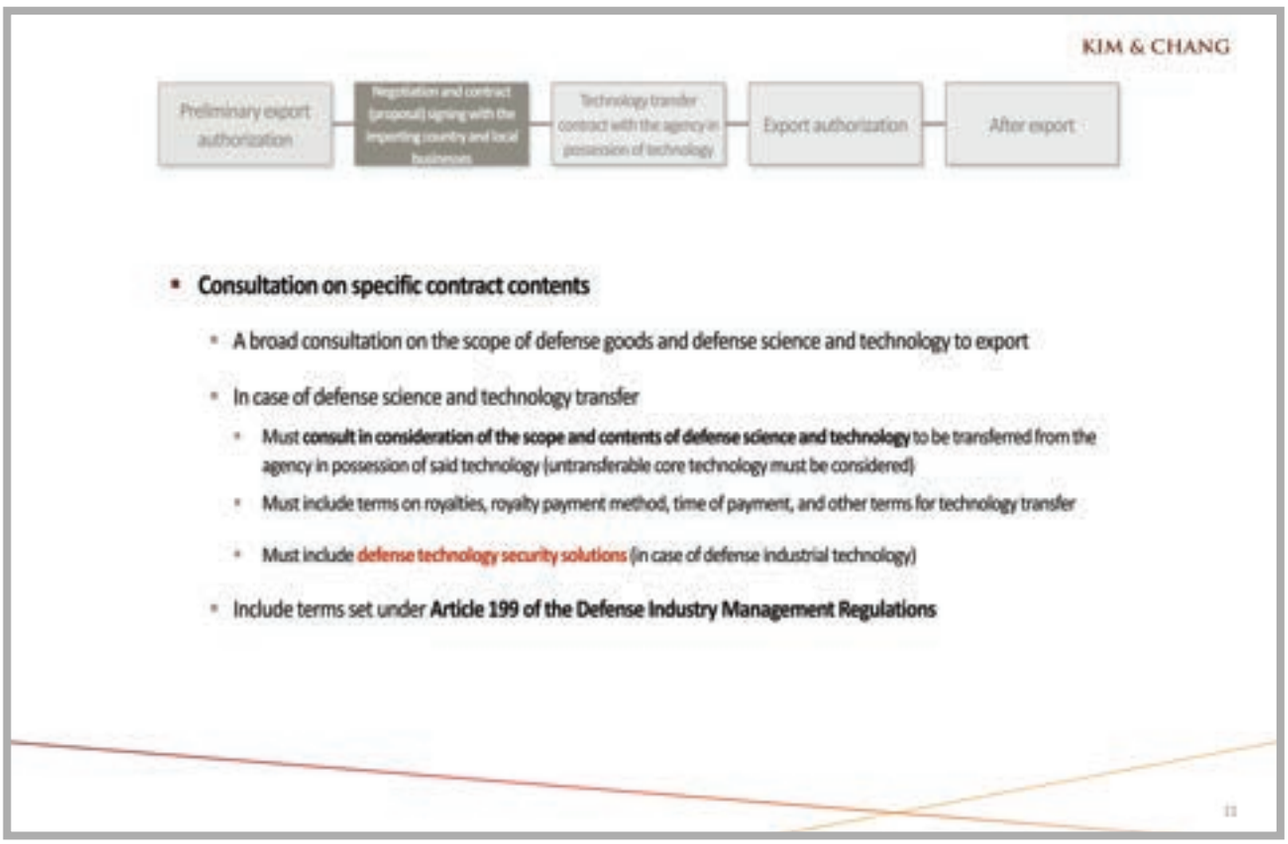
- **Preliminary export authorization**
  - Needs to submit documents specified in Clause 1 of Article 57 of the Defense Acquisition Program Act, and apply for preliminary export authorization to the minister of DAPA

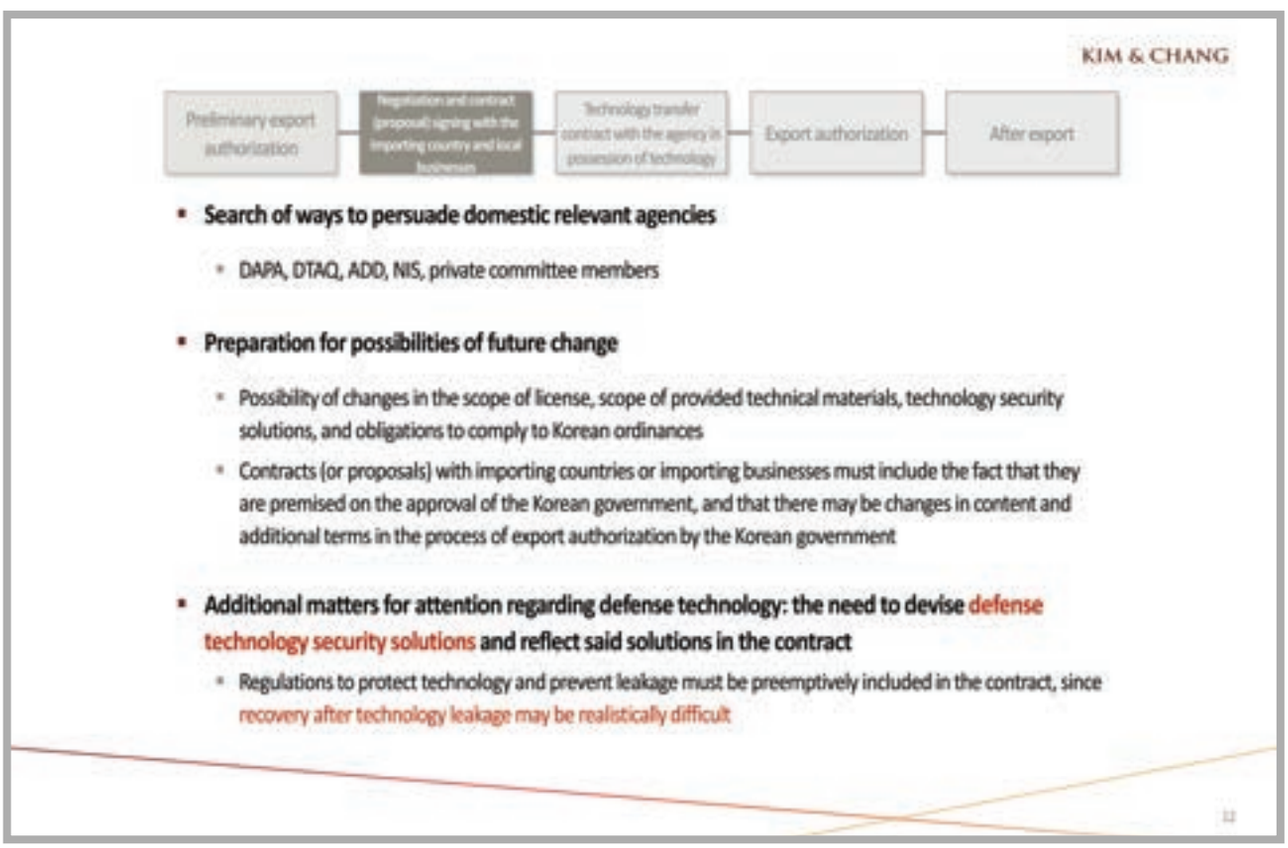
Application to the head of the Defense Technology Security Division ▶ Review by the international cooperation division, ADD, KRIT, and the Defense Rapid Acquisition Technology Institute if necessary ▶ Review by the head of the Defense Technology Security Division ▶ Approval

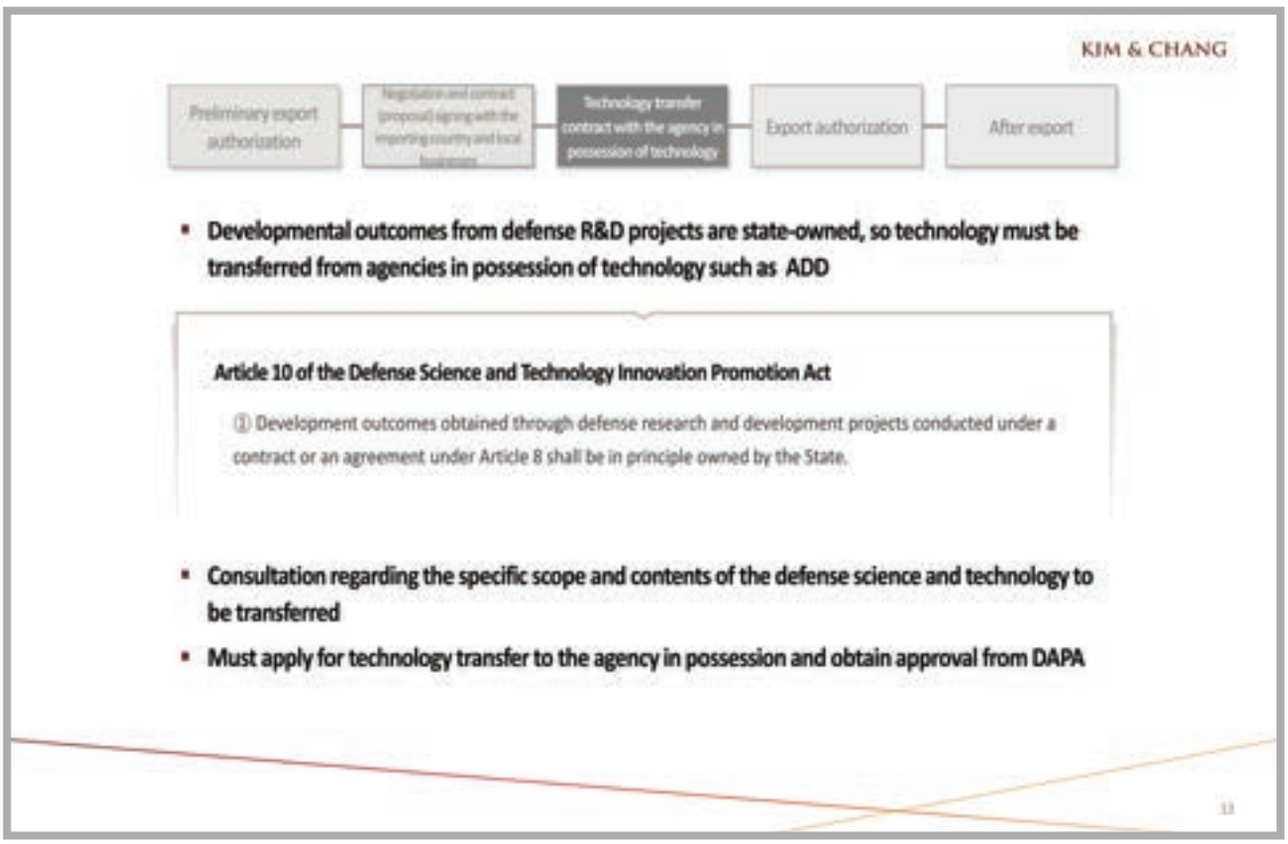
Article 57 of the Enforcement Rules on the Defense Acquisition Program Act

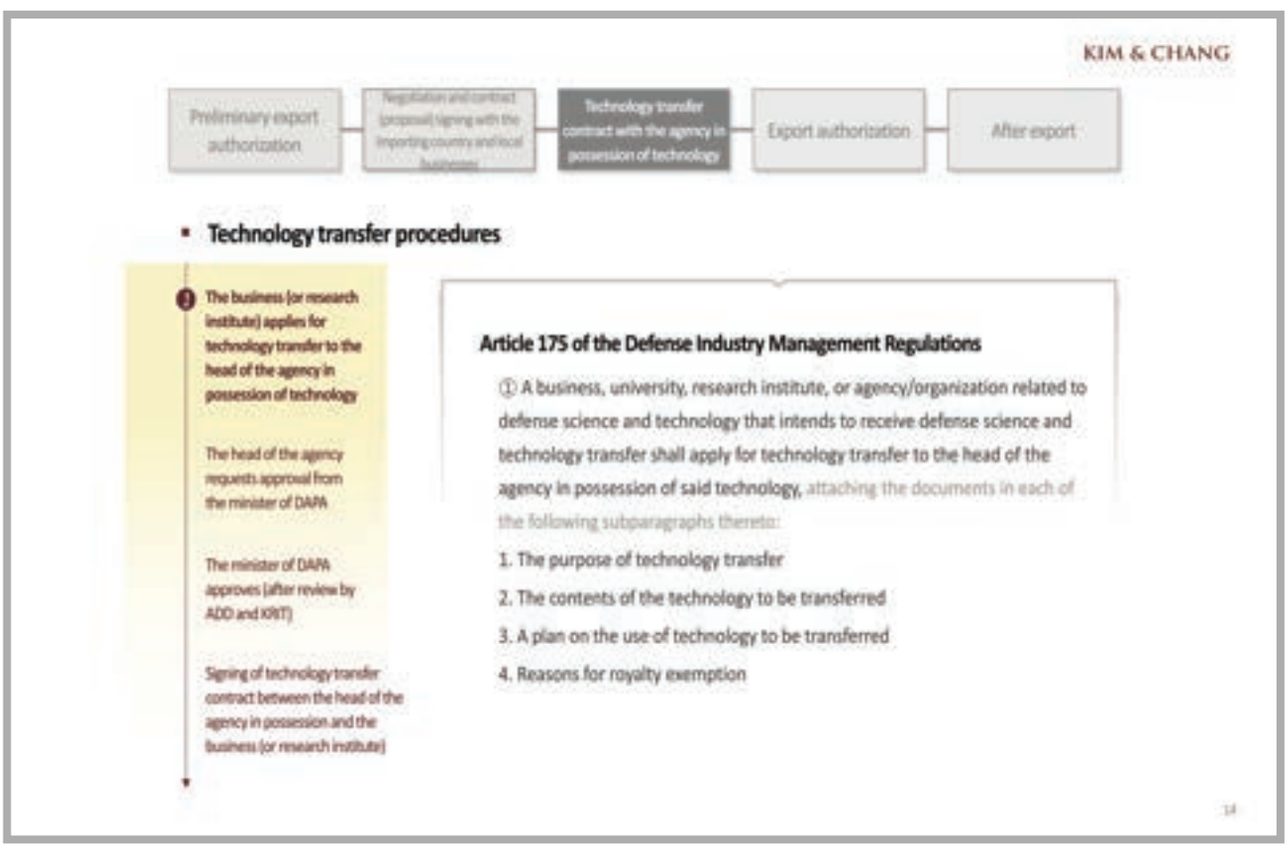
① A person who intends to engage in business negotiations before obtaining permission for exporting major defense materials and national defense science and technology under Article 57 (3) of the Act shall submit an application for preliminary approval for export in Form No. 21, and a person who intends to participate in international bidding, an application for approval for participation in international bidding in Form No. 22 to the Administrator of the Defense Acquisition Program Administration, attaching the documents in each of the following subparagraphs thereto:

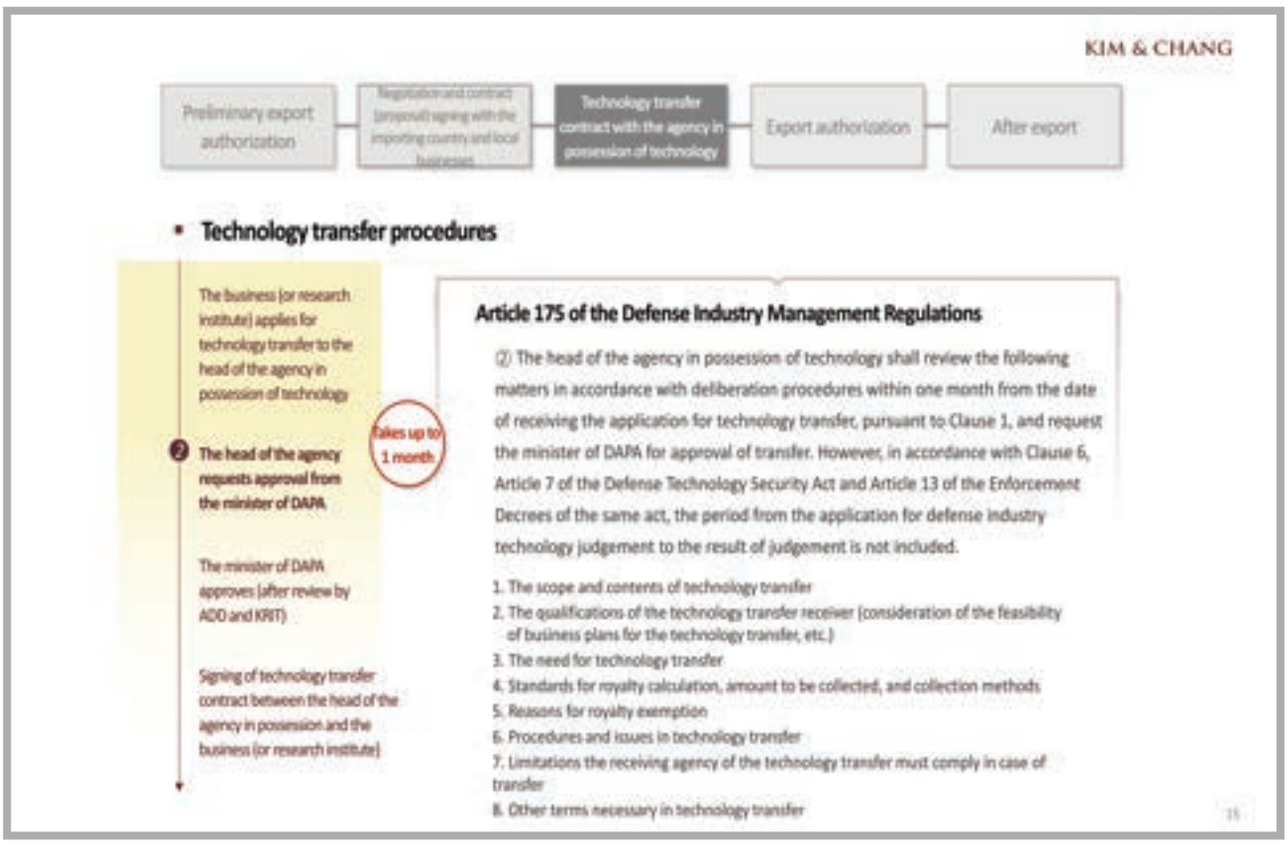
1. A copy of certificate of report on trading business;
2. A copy of request for purchase issued by the government of the purchasing country or the agent thereof; and
3. In cases where issuance of the document under subparagraph 2 is difficult due to the practices of the purchasing country, a copy of statement on information on the purchase as confirmed by the head of or a military attache to a legation in the purchasing country or any reliable organization, and account of obtaining the information.

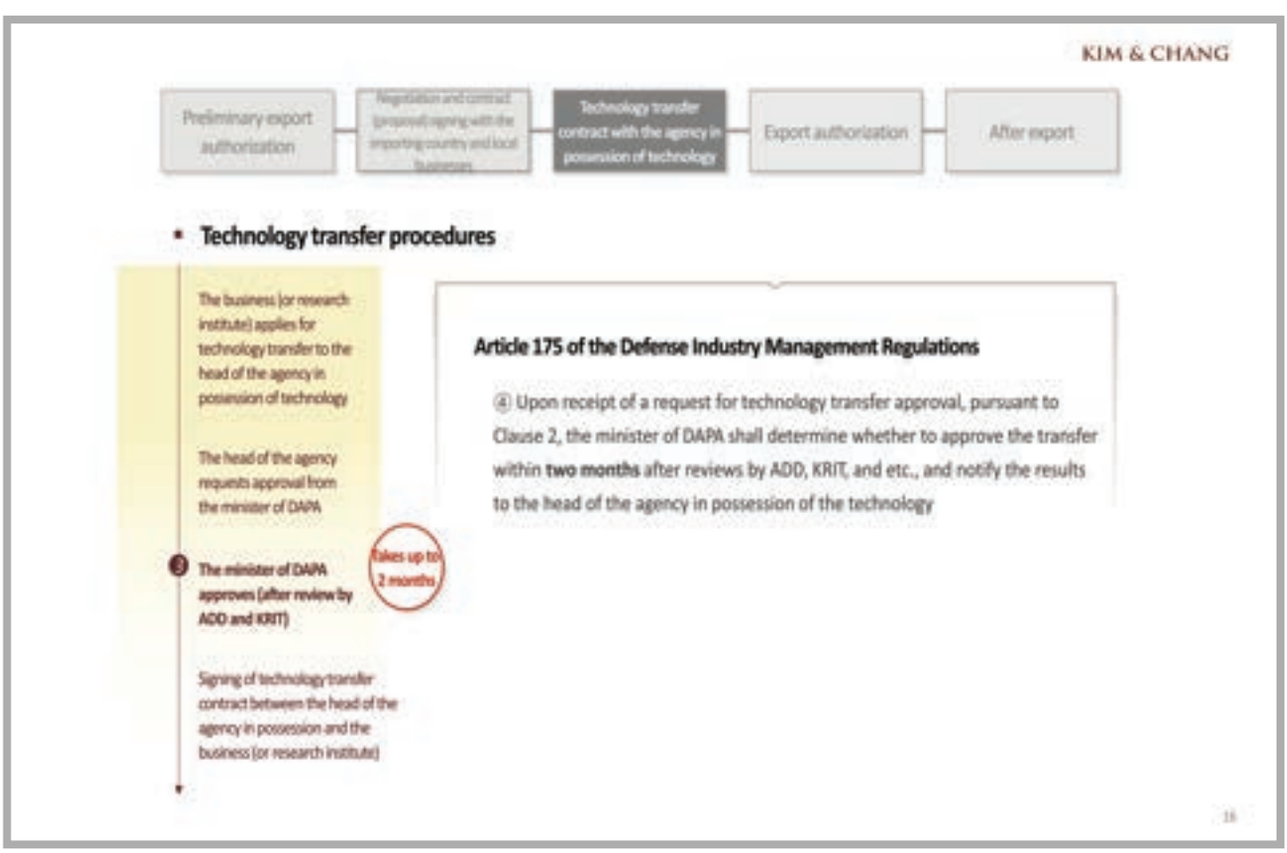

KIM & CHANG
Preliminary export authorization
Registration and contract (proposal) signing with the importing country and local businesses
Technology transfer contract with the agency in possession of technology
Export authorization
After export
Consultation on specific contract contents
A broad consultation on the scope of defense goods and defense science and technology to export
In case of defense science and technology transfer
Must consult in consideration of the scope and contents of defense science and technology to be transferred from the agency in possession of said technology (untransferable core technology must be considered)
Must include terms on royalties, royalty payment method, time of payment, and other terms for technology transfer
Must include defense technology security solutions (in case of defense industrial technology)
Include terms set under Article 199 of the Defense Industry Management Regulations


KIM & CHANG
Preliminary export authorization
Registration and contract (proposal) signing with the importing country and local businesses
Technology transfer contract with the agency in possession of technology
Export authorization
After export
Search of ways to persuade domestic relevant agencies
DAPA, DTAQ, ADD, NIS, private committee members
Preparation for possibilities of future change
Possibility of changes in the scope of license, scope of provided technical materials, technology security solutions, and obligations to comply to Korean ordinances
Contracts (or proposals) with importing countries or importing businesses must include the fact that they are premised on the approval of the Korean government, and that there may be changes in content and additional terms in the process of export authorization by the Korean government
Additional matters for attention regarding defense technology: the need to devise defense technology security solutions and reflect said solutions in the contract
Regulations to protect technology and prevent leakage must be preemptively included in the contract, since recovery after technology leakage may be realistically difficult


KIM & CHANG
Preliminary export authorization
Negotiation and contract (proposal) signing with the importing country and local businesses
Technology transfer contract with the agency in possession of technology
Export authorization
After export
Developmental outcomes from defense R&D projects are state-owned, so technology must be transferred from agencies in possession of technology such as ADD
Article 10 of the Defense Science and Technology Innovation Promotion Act
① Development outcomes obtained through defense research and development projects conducted under a contract or an agreement under Article 8 shall be in principle owned by the State.
Consultation regarding the specific scope and contents of the defense science and technology to be transferred
Must apply for technology transfer to the agency in possession and obtain approval from DAPA


KIM & CHANG
Preliminary export authorization
Negotiation and contract (proposal) signing with the importing country and local businesses
Technology transfer contract with the agency in possession of technology
Export authorization
After export
Technology transfer procedures
The business (or research institute) applies for technology transfer to the head of the agency in possession of technology
The head of the agency requests approval from the minister of DAPA
The minister of DAPA approves (after review by ADD and KRIT)
Signing of technology transfer contract between the head of the agency in possession and the business (or research institute)
Article 175 of the Defense Industry Management Regulations
① A business, university, research institute, or agency/organization related to defense science and technology that intends to receive defense science and technology transfer shall apply for technology transfer to the head of the agency in possession of said technology, attaching the documents in each of the following subparagraphs thereto:
1. The purpose of technology transfer
2. The contents of the technology to be transferred
3. A plan on the use of technology to be transferred
4. Reasons for royalty exemption


KIM & CHANG
Preliminary export authorization
Negotiation and contract (proposal) signing with the importing country and local businesses
Technology transfer contract with the agency in possession of technology
Export authorization
After export
Technology transfer procedures
The business (or research institute) applies for technology transfer to the head of the agency in possession of technology
Takes up to 1 month
❷ The head of the agency requests approval from the minister of DAPA
The minister of DAPA approves (after review by ADD and KRIT)
Signing of technology transfer contract between the head of the agency in possession and the business (or research institute)
Article 175 of the Defense Industry Management Regulations
② The head of the agency in possession of technology shall review the following matters in accordance with deliberation procedures within one month from the date of receiving the application for technology transfer, pursuant to Clause 1, and request the minister of DAPA for approval of transfer. However, in accordance with Clause 6, Article 7 of the Defense Technology Security Act and Article 13 of the Enforcement Decrees of the same act, the period from the application for defense industry technology judgement to the result of judgement is not included.
1. The scope and contents of technology transfer
2. The qualifications of the technology transfer receiver (consideration of the feasibility of business plans for the technology transfer, etc.)
3. The need for technology transfer
4. Standards for royalty calculation, amount to be collected, and collection methods
5. Reasons for royalty exemption
6. Procedures and issues in technology transfer
7. Limitations the receiving agency of the technology transfer must comply in case of transfer
8. Other terms necessary in technology transfer


KIM & CHANG
Preliminary export authorization
Negotiation and contract (proposal) signing with the importing country and local businesses
Technology transfer contract with the agency in possession of technology
Export authorization
After export
Technology transfer procedures
The business (or research institute) applies for technology transfer to the head of the agency in possession of technology
The head of the agency requests approval from the minister of DAPA
Takes up to 2 months
❸ The minister of DAPA approves (after review by ADD and KRIT)
Signing of technology transfer contract between the head of the agency in possession and the business (or research institute)
Article 175 of the Defense Industry Management Regulations
④ Upon receipt of a request for technology transfer approval, pursuant to Clause 2, the minister of DAPA shall determine whether to approve the transfer within two months after reviews by ADD, KRIT, and etc., and notify the results to the head of the agency in possession of the technology

KIM & CHANG

Preliminary export authorization → Negotiation and contract (proposal) signing with the importing country and local businesses → **Technology transfer contract with the agency in possession of technology** → Export authorization → After export

- **Technology transfer procedures**

① The business (or research institute) applies for technology transfer to the head of the agency in possession of technology

② The head of the agency requests approval from the minister of DAPA

③ The minister of DAPA approves (after review by ADD and KRIT)

④ **Signing of technology transfer contract between the head of the agency in possession and the business (or research institute)**

Article 176 of the Defense Industry Management Regulations

① In case of technology transfer under Article 175, the head of the agency in possession of the technology shall enter into a technology transfer contract with the research institute, etc., and the technology transfer contract shall include the scope and contents of the technology being transferred, royalties and royalty payment methods as well as period of payment, and other terms of technology transfer.

17

KIM & CHANG

Preliminary export authorization → Negotiation and contract (proposal) signing with the importing country and local businesses → **Technology transfer contract with the agency in possession of technology** → Export authorization → After export

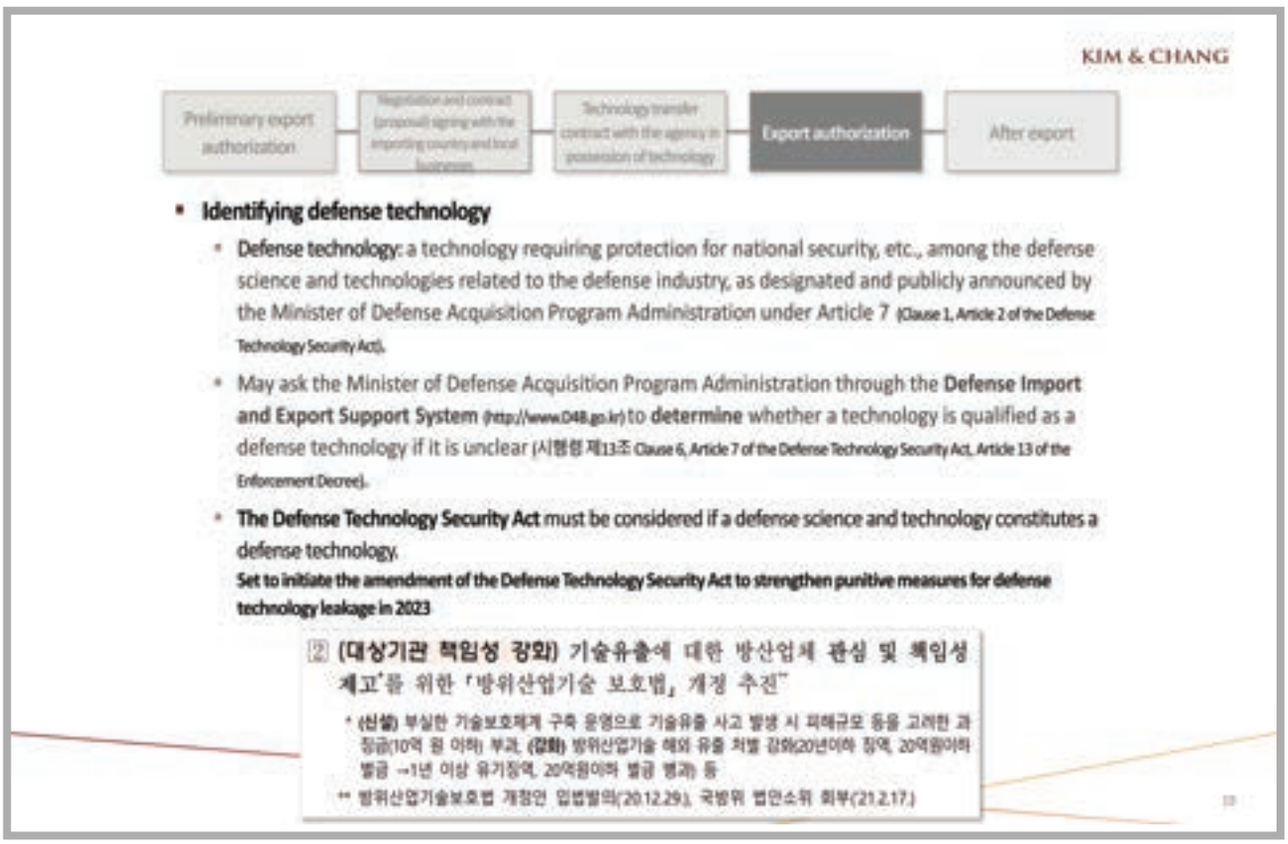
- **Contents of technology transfer contracts**
  - Must **include terms specified in Clause 2, Article 176 of the Defense Industry Management Regulations**, including royalty amount and payment period and methods, terms of compliance for research institutes, and damage compensation claims from violation of the contract
- **Consultation on royalty calculation (complex and prolonged procedures) and royalty exemption:**
  - **The notice on defense science royalty calculation, collection methods, and collection procedure** has been amended recently, extending the special case clause for running royalty exemption.

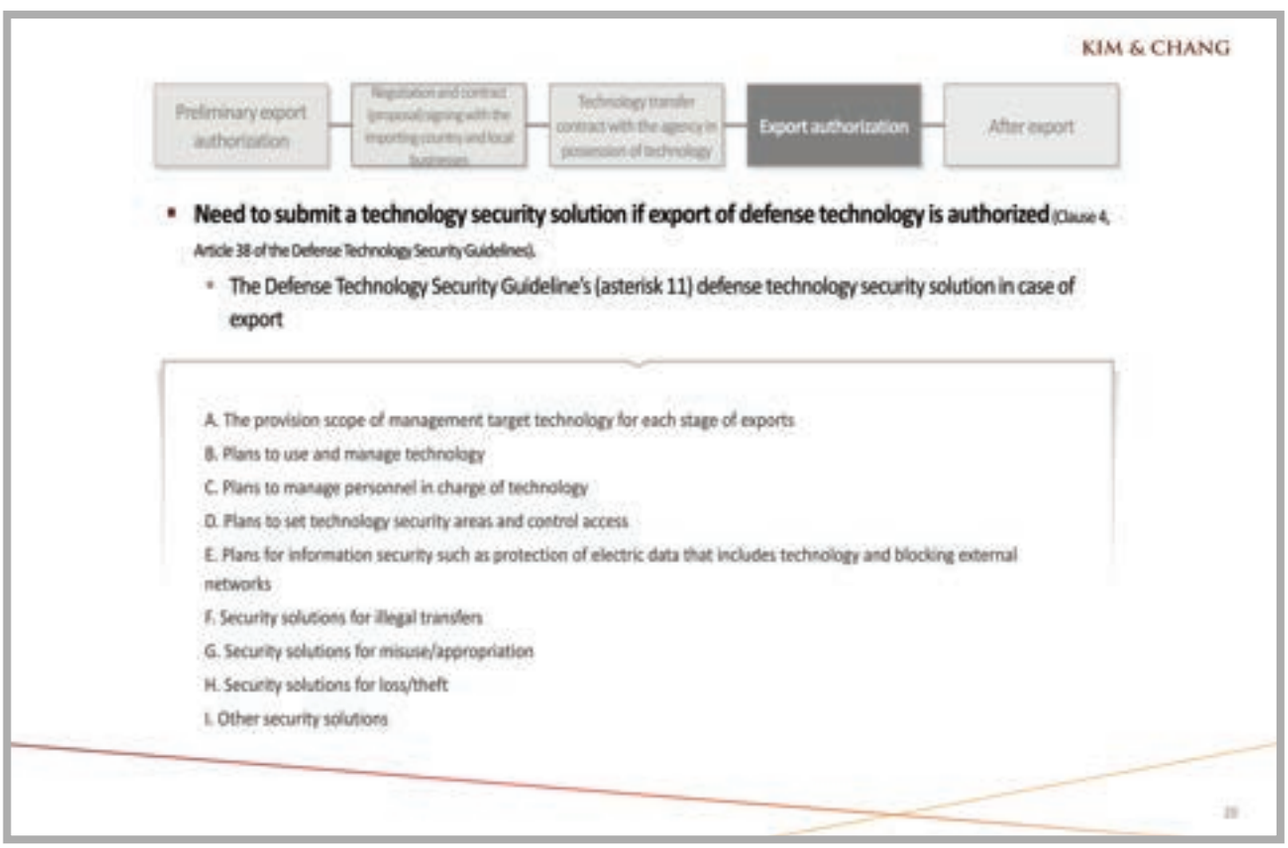
Article 2 of the Addendum to the Notice on defense science royalty calculation, collection methods, and collection procedure

"When exporting defense science and technology to promote exports, the running royalty shall be reduced to 0.5% of the net acquisition price in case of No. 1, Clause 3, Article 4, and 1% of the net sales price in case of No. 2, Clause 5, Article 4 until December 31, 2024, in spite of No. 1, Clause 3, Article 4 and No. 2, Clause 5, Article 4. In this case, approval from the minister of DAPA is not required."

- **Reflect contents of technology transfer contract with the agency in possession in negotiations (or contracts) with importing countries** (if possible)

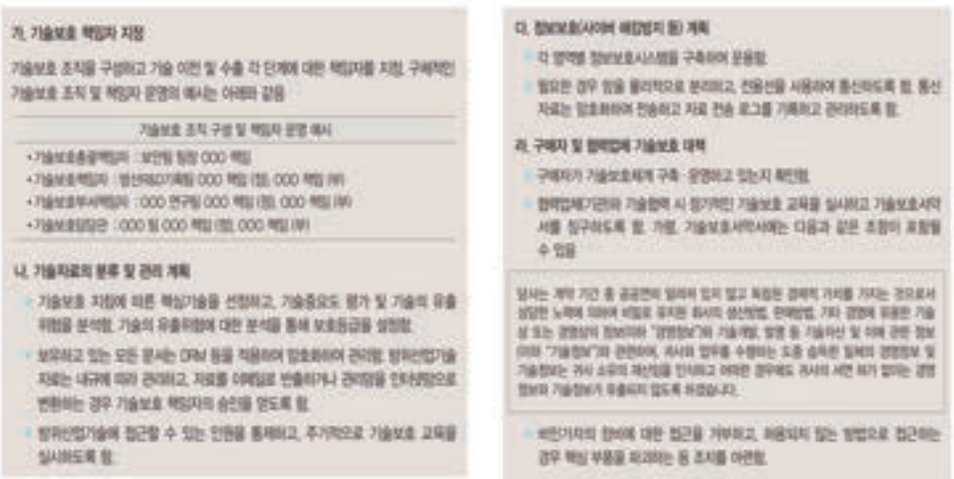
18


KIM & CHANG
Preliminary export authorization
Export authorization
After export
Identifying defense technology
Defense technology: a technology requiring protection for national security, etc., among the defense science and technologies related to the defense industry, as designated and publicly announced by the Minister of Defense Acquisition Program Administration under Article 7 (Clause 1, Article 2 of the Defense Technology Security Act).
May ask the Minister of Defense Acquisition Program Administration through the Defense Import and Export Support System (http://www.D48.go.kr) to determine whether a technology is qualified as a defense technology if it is unclear (시행령 제13조 Clause 6, Article 7 of the Defense Technology Security Act, Article 13 of the Enforcement Decree).
The Defense Technology Security Act must be considered if a defense science and technology constitutes a defense technology.
Set to initiate the amendment of the Defense Technology Security Act to strengthen punitive measures for defense technology leakage in 2023
(대상기관 책임성 강화) 기술유출에 대한 방산업체 관심 및 책임성 제고*를 위한 「방위산업기술 보호법」 개정 추진**
* (현행) 부실한 기술보호체계 구축 운영으로 기술유출 사고 발생 시 피해규모 등을 고려한 과징금(10억 원 이하) 부과, (강화) 방위산업기술 해외 유출 처벌 강화(20년이하 징역, 20억원이하 벌금 → 1년 이상 유기징역, 20억원이하 벌금 병과) 등
** 방위산업기술보호법 개정안 입법발의('20.12.29.), 국방위 법안소위 회부('21.2.17.)


KIM & CHANG
Preliminary export authorization
Export authorization
After export
Need to submit a technology security solution if export of defense technology is authorized (Clause 4, Article 38 of the Defense Technology Security Guidelines).
The Defense Technology Security Guideline's (asterisk 11) defense technology security solution in case of export
A. The provision scope of management target technology for each stage of exports
B. Plans to use and manage technology
C. Plans to manage personnel in charge of technology
D. Plans to set technology security areas and control access
E. Plans for information security such as protection of electric data that includes technology and blocking external networks
F. Security solutions for illegal transfers
G. Security solutions for misuse/appropriation
H. Security solutions for loss/theft
I. Other security solutions

KIM & CHANG

[Reference] DAPA and NIS's Technology Security Manual for each stage of defense technology exports (2023)



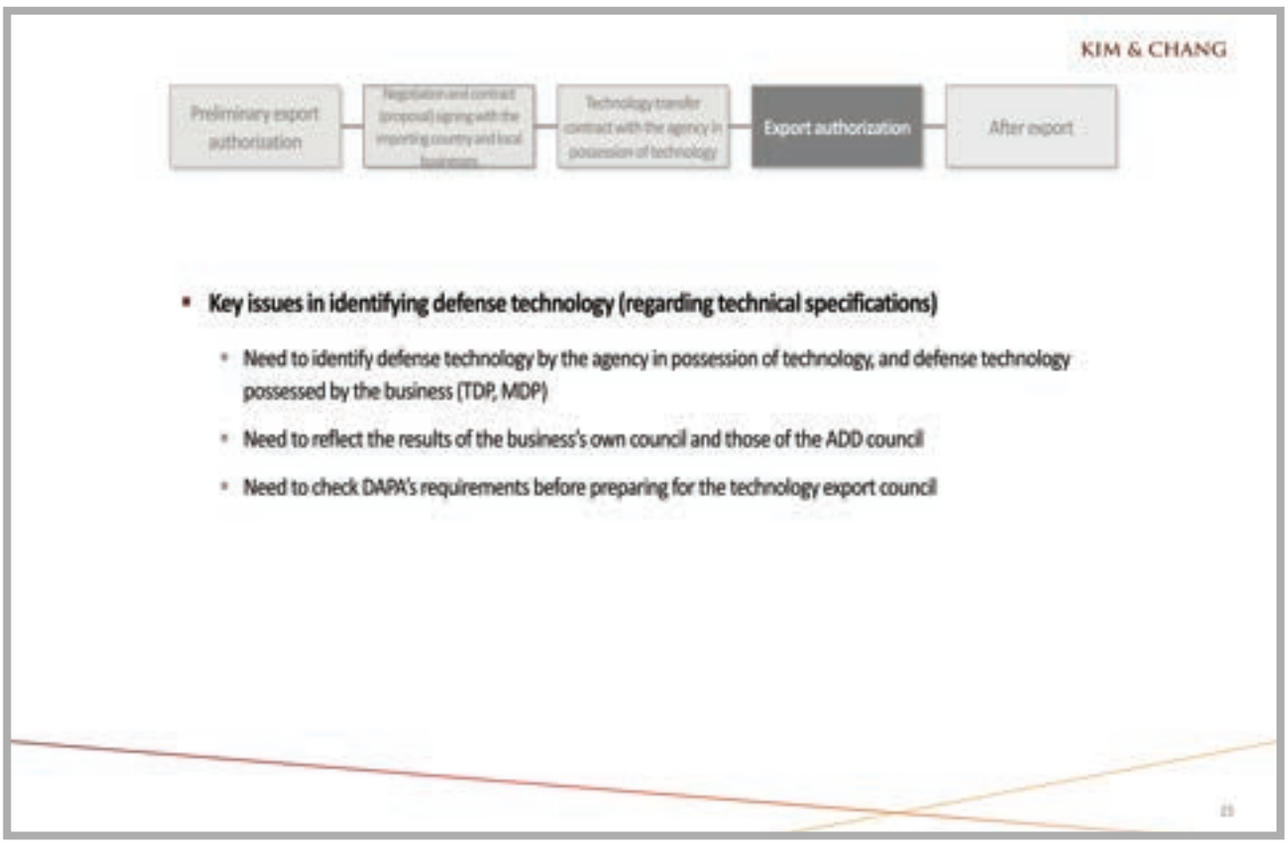
KIM & CHANG

- **Key issues in identifying defense technology**
  - Advances in identification procedures for defense technology to be exported
  - Regarding **technical specifications**
    - The Technology Security Division in DAPA requires the objective identification of defense technology and the submission of technical specifications
    - Requires a specific and detailed classification of defense technology, as well as the provision of reasonable and objective grounds for identification regarding whether it is defense technology or not
    - Need to identify each form of **each type to be protected** (Article 3 and 12 of the Defense Technology Security Guidelines)

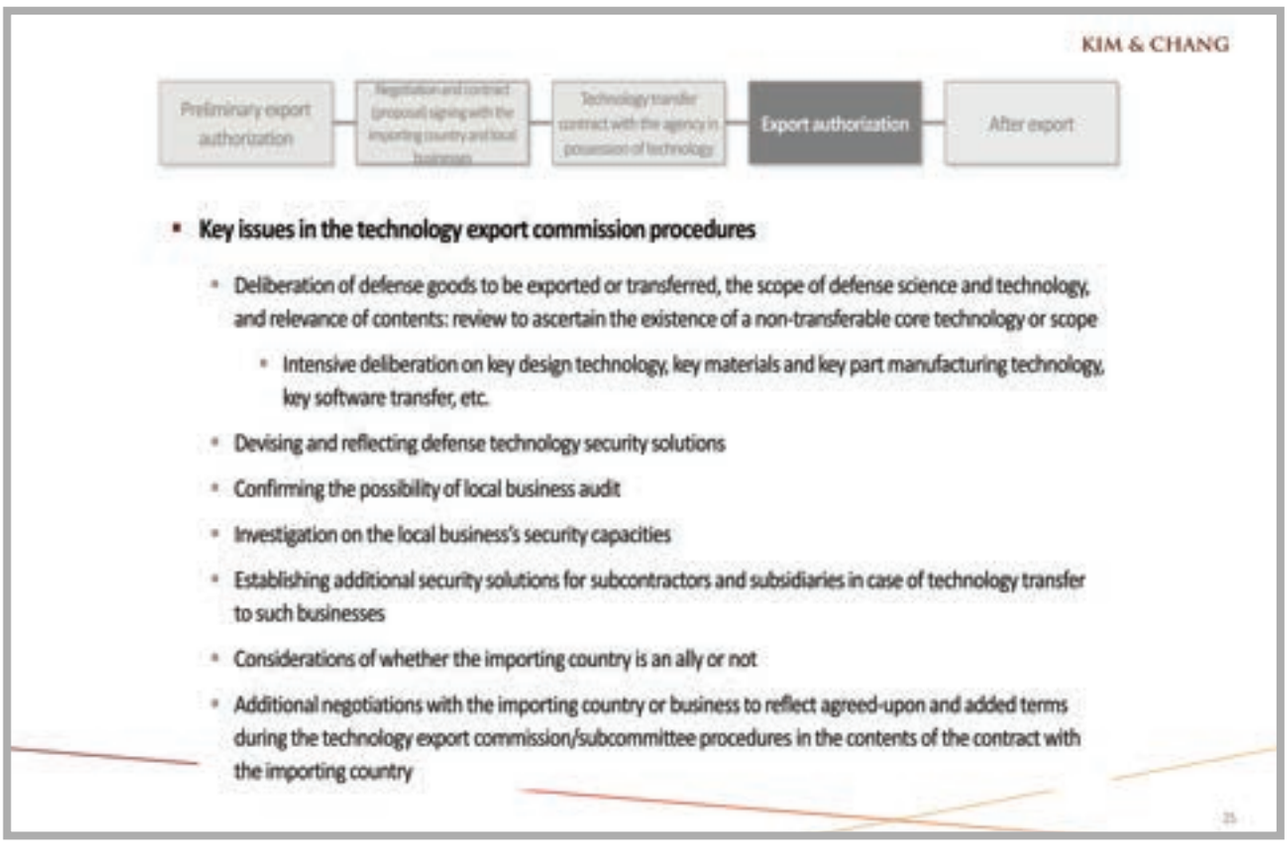
[Article 3 of the Defense Technology Security Guidelines]

① The types to be protected by target organizations (hereinafter "protected types") are as follows:

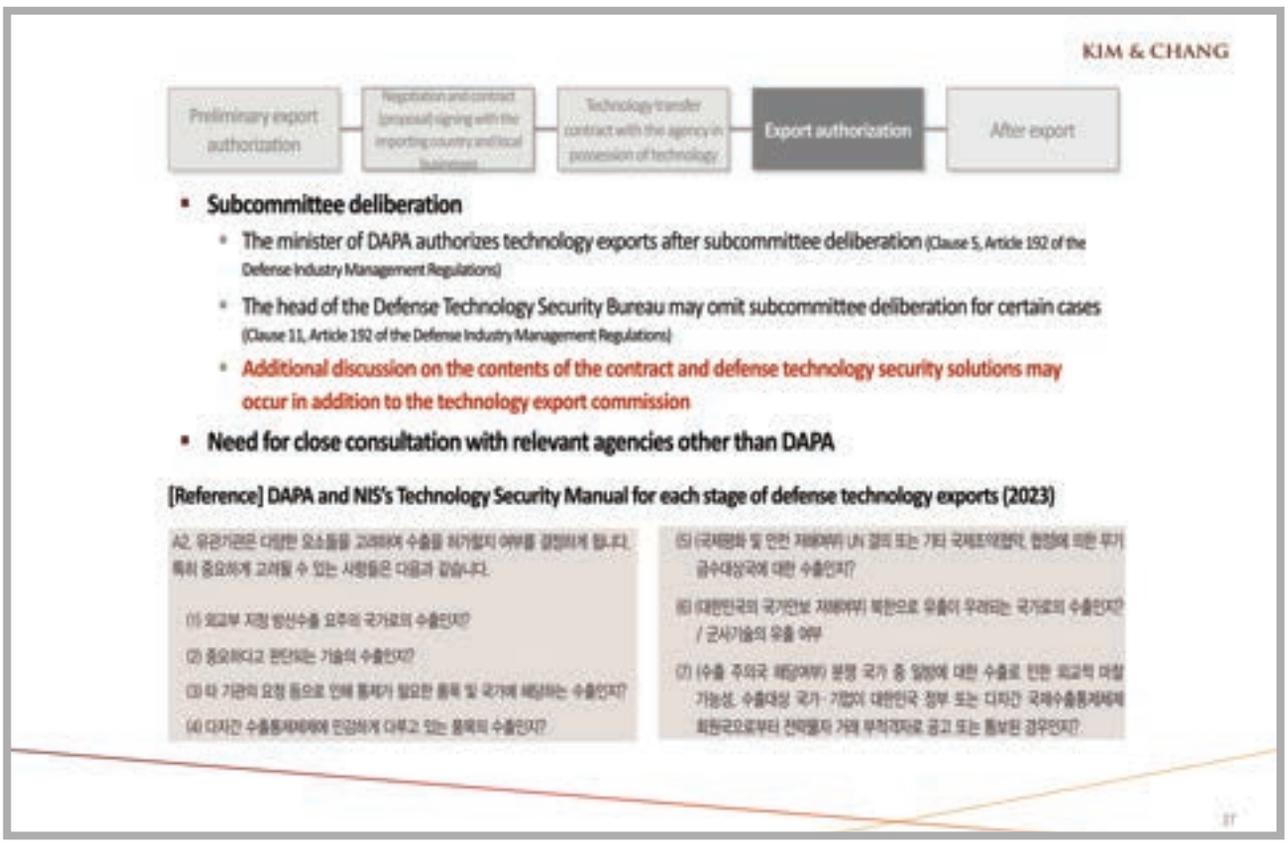
1. A floor plan of the defense technology (including relevant software) and a quality assurance requirement
2. Specifications and a report describing the defense technology
3. Samples, prototypes, electronic media records, and technical data involving the defense technology
4. Other materials involving the defense technology

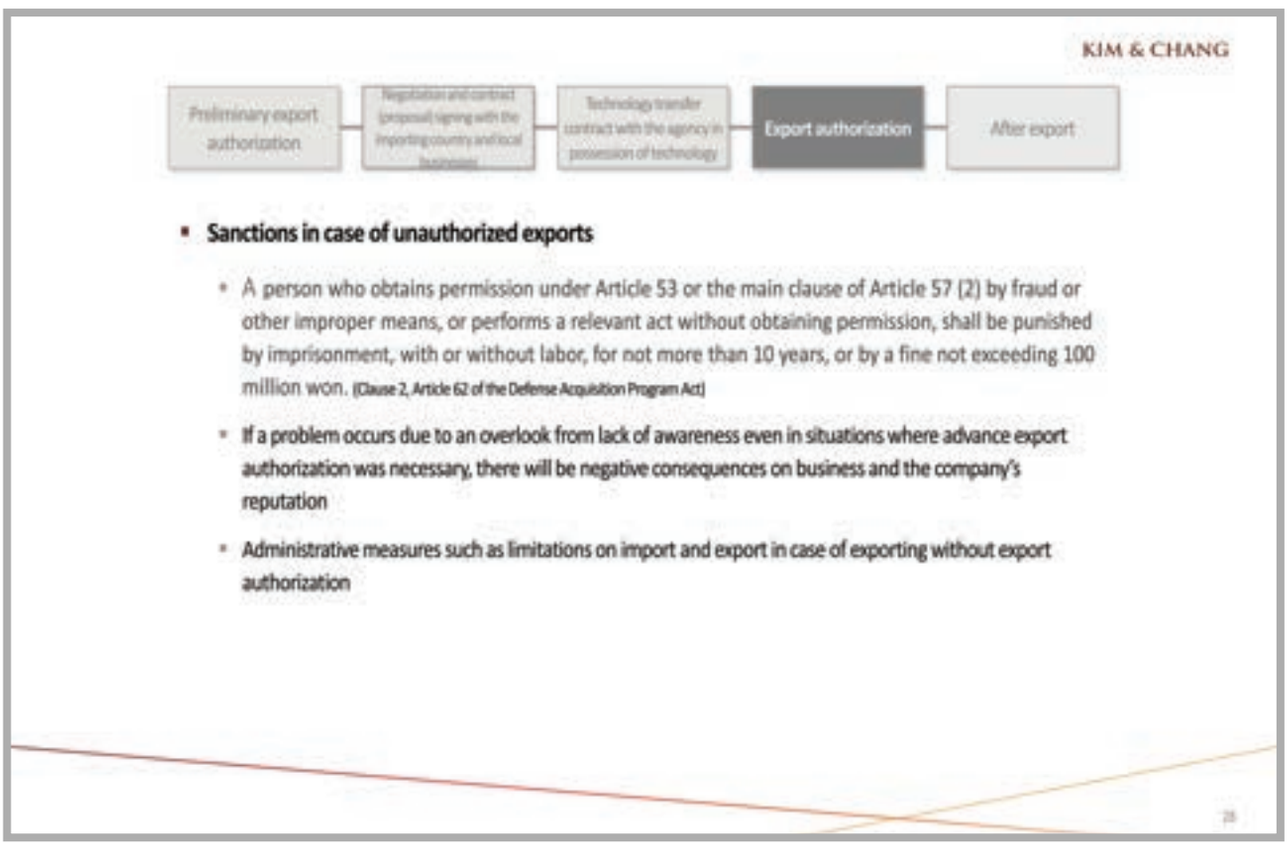

KIM & CHANG
Preliminary export authorization
Export authorization
After export
Key issues in identifying defense technology (regarding technical specifications)
Need to identify defense technology by the agency in possession of technology, and defense technology possessed by the business (TDP, MDP)
Need to reflect the results of the business's own council and those of the ADD council
Need to check DAPA's requirements before preparing for the technology export council

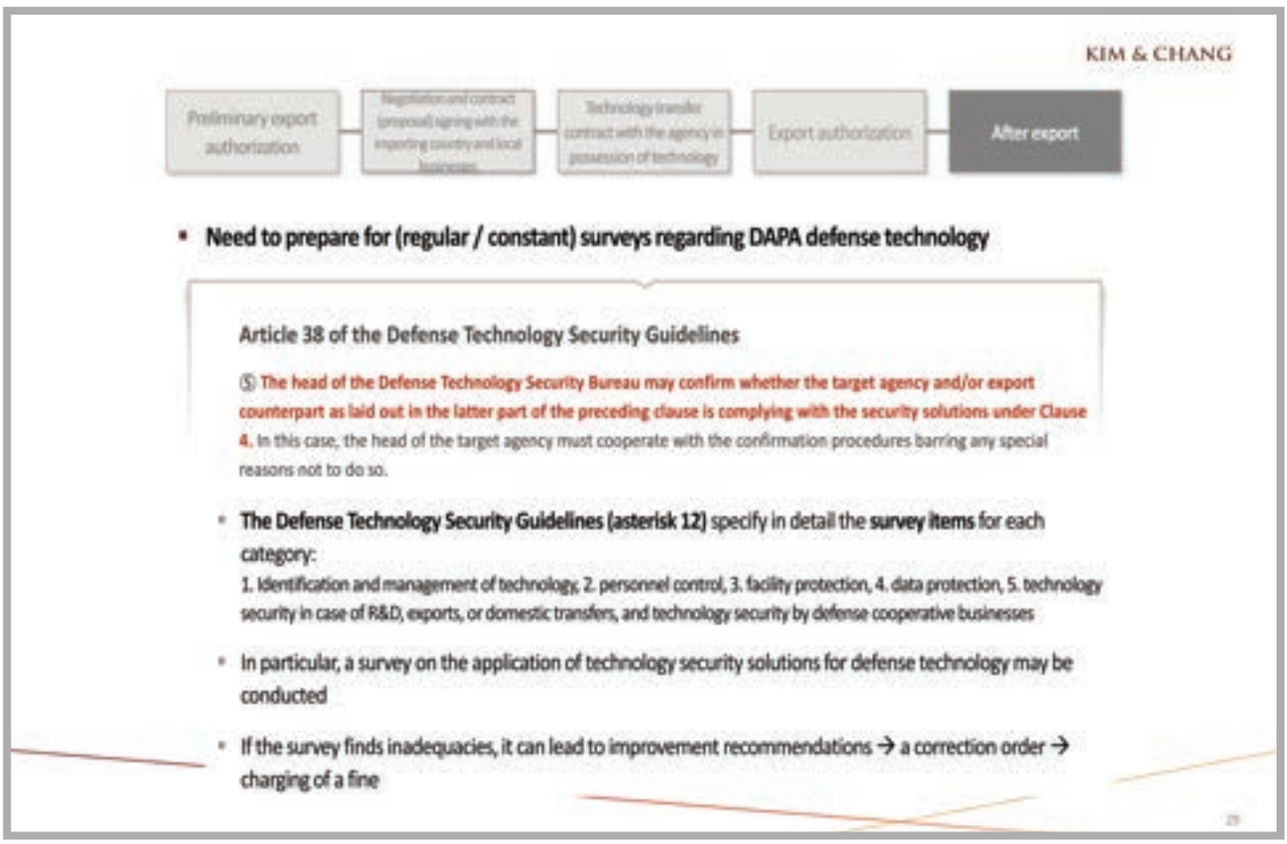

KIM & CHANG
Preliminary export authorization
Export authorization
After export
Technology export commission procedures for technology export authorization
The technology export commission reviews whether the technology may be exported before export authorization
Article 183 of the Defense Industry Management Regulations
③ The head of the Defense Technology Security Bureau heads a technology export commission, joined by external civil experts and defense businesses including the Defense Industry Promotion Bureau, the Defense Business Policy Bureau, the International Cooperation Bureau, the Business Headquarters, the Ministry of Defense, NIS, the Defense Counterintelligence Command, ADD, KRIT, the Defense Technology Center, and relevant public agencies in order to review technology exports before export authorization is applied for.
Devising response strategies for opposition during the procedure and concerns about technology leakage
Preparing materials for the technology export commission
Key contents: an overview of operations and technology exports, review results of technology classification, technology security solutions, domestic ramifications as a result of technology export, etc.
"It is necessary to develop logic and prepare materials to dispel concerns about "large-scale technology transfer"

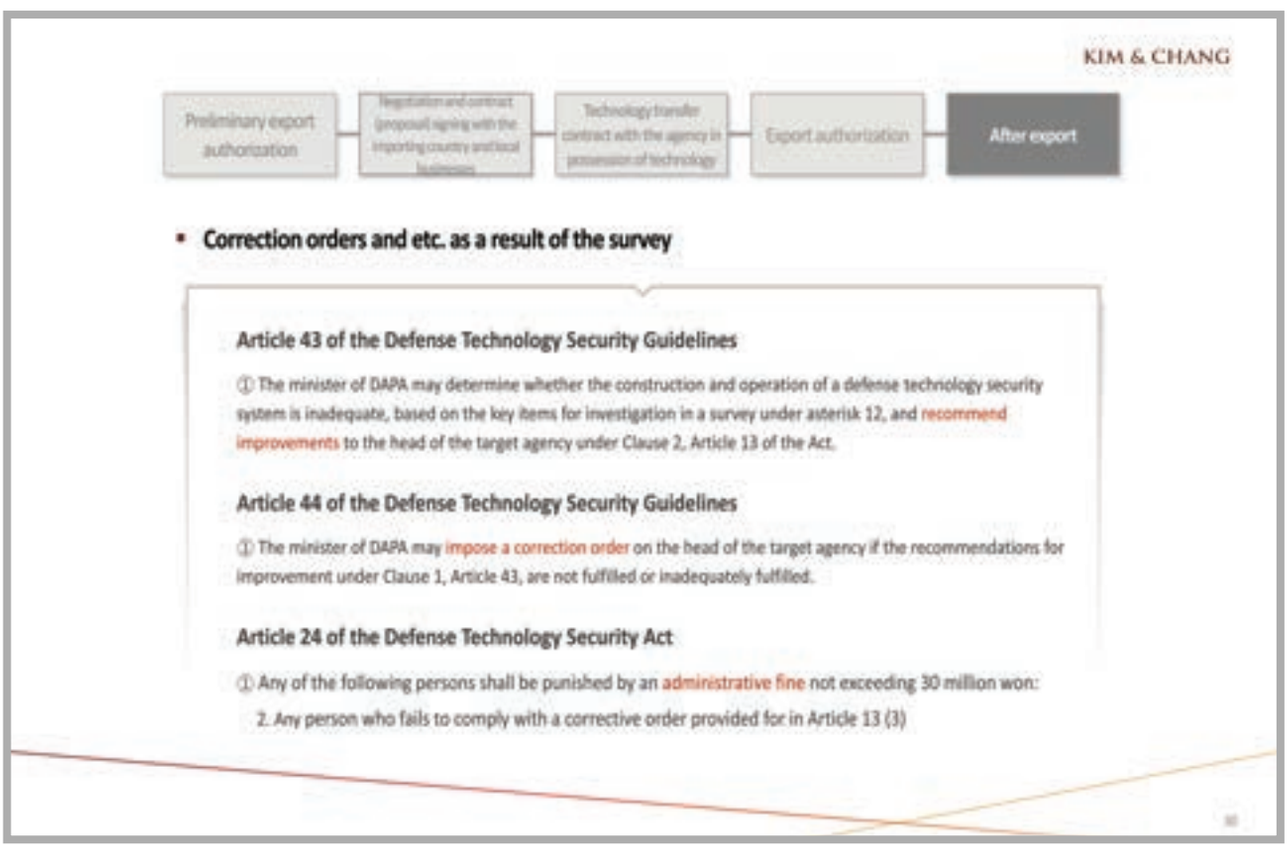

KIM & CHANG
Preliminary export authorization
Negotiation and contract (proposal) signing with the importing country and local businesses
Technology transfer contract with the agency in possession of technology
Export authorization
After export
Key issues in the technology export commission procedures
Deliberation of defense goods to be exported or transferred, the scope of defense science and technology, and relevance of contents: review to ascertain the existence of a non-transferable core technology or scope
Intensive deliberation on key design technology, key materials and key part manufacturing technology, key software transfer, etc.
Devising and reflecting defense technology security solutions
Confirming the possibility of local business audit
Investigation on the local business's security capacities
Establishing additional security solutions for subcontractors and subsidiaries in case of technology transfer to such businesses
Considerations of whether the importing country is an ally or not
Additional negotiations with the importing country or business to reflect agreed-upon and added terms during the technology export commission/subcommittee procedures in the contents of the contract with the importing country


KIM & CHANG
Preliminary export authorization
Negotiation and contract (proposal) signing with the importing country and local businesses
Technology transfer contract with the agency in possession of technology
Export authorization
After export
Submitting application for export authorization
Submit an export authorization application and the documents specified in Clause 5, Article 192 of the Defense Industry Management Regulations
Article 192 of the Defense Industry Management Regulations
① An agency or business in possession of technology that intends to export said technology shall obtain permission from the minister of DAPA after subcommittee deliberation, with the following documents attached to the export authorization application under Form 19 of the Regulations. The same shall also apply to technology exports through offsets.
1. 1 copy of the export contract proposal
2. 1 copy of the technology acquisition report and technology transfer contract with the agency in possession of said technology
3. 1 copy of a description of the relationship between the importing country and the person who intends to obtain export authorization
4. 1 copy of a description of the ramifications, both domestic and overseas, from exporting the technology of concern
5. The technology export commission's review results under Clause 3, Article 183
6. 1 copy of asterisk 11 of the Defense Technology Security Guidelines (a defense technology security solution in case of export) for defense technology

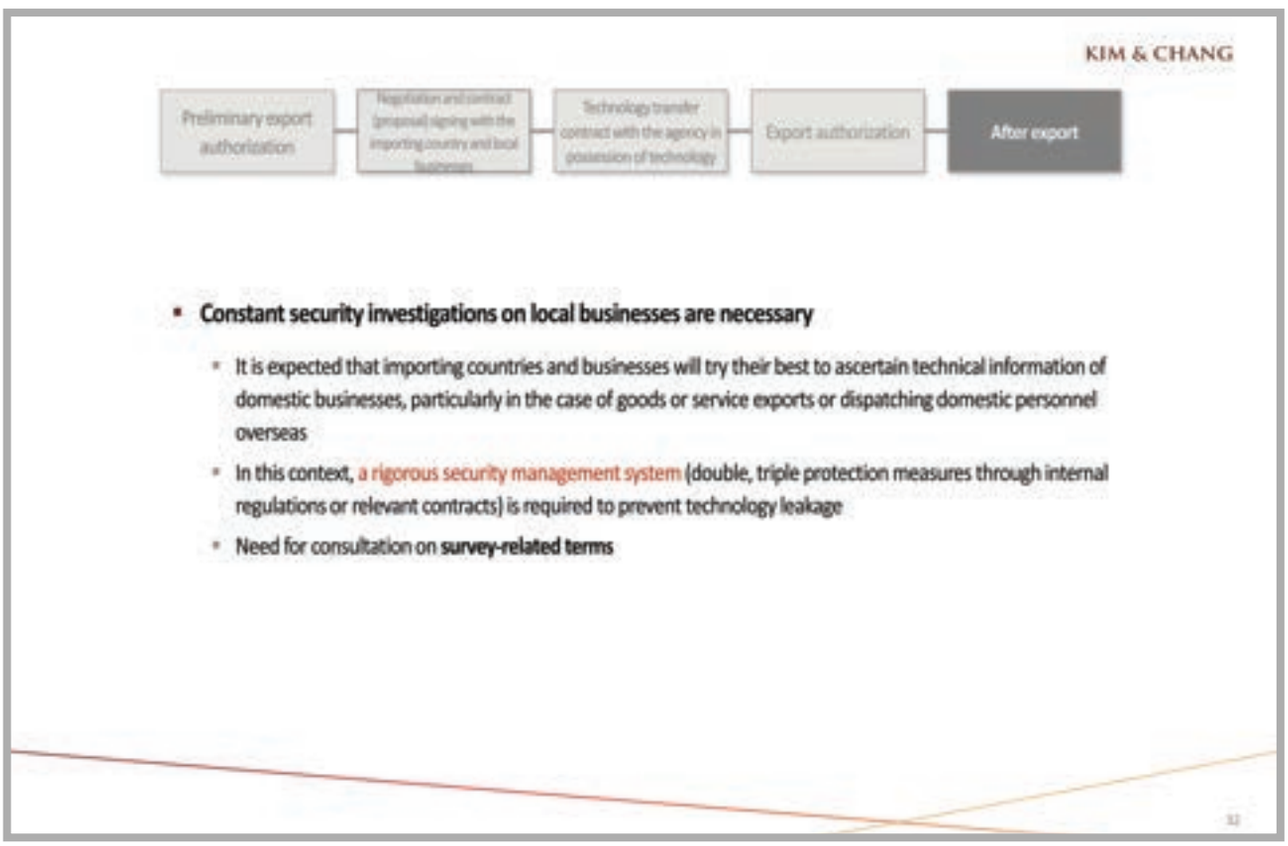

KIM & CHANG
Preliminary export authorization
Export authorization
After export
Subcommittee deliberation
The minister of DAPA authorizes technology exports after subcommittee deliberation (Clause 5, Article 192 of the Defense Industry Management Regulations)
The head of the Defense Technology Security Bureau may omit subcommittee deliberation for certain cases (Clause 11, Article 192 of the Defense Industry Management Regulations)
Additional discussion on the contents of the contract and defense technology security solutions may occur in addition to the technology export commission
Need for close consultation with relevant agencies other than DAPA
[Reference] DAPA and NIS's Technology Security Manual for each stage of defense technology exports (2023)

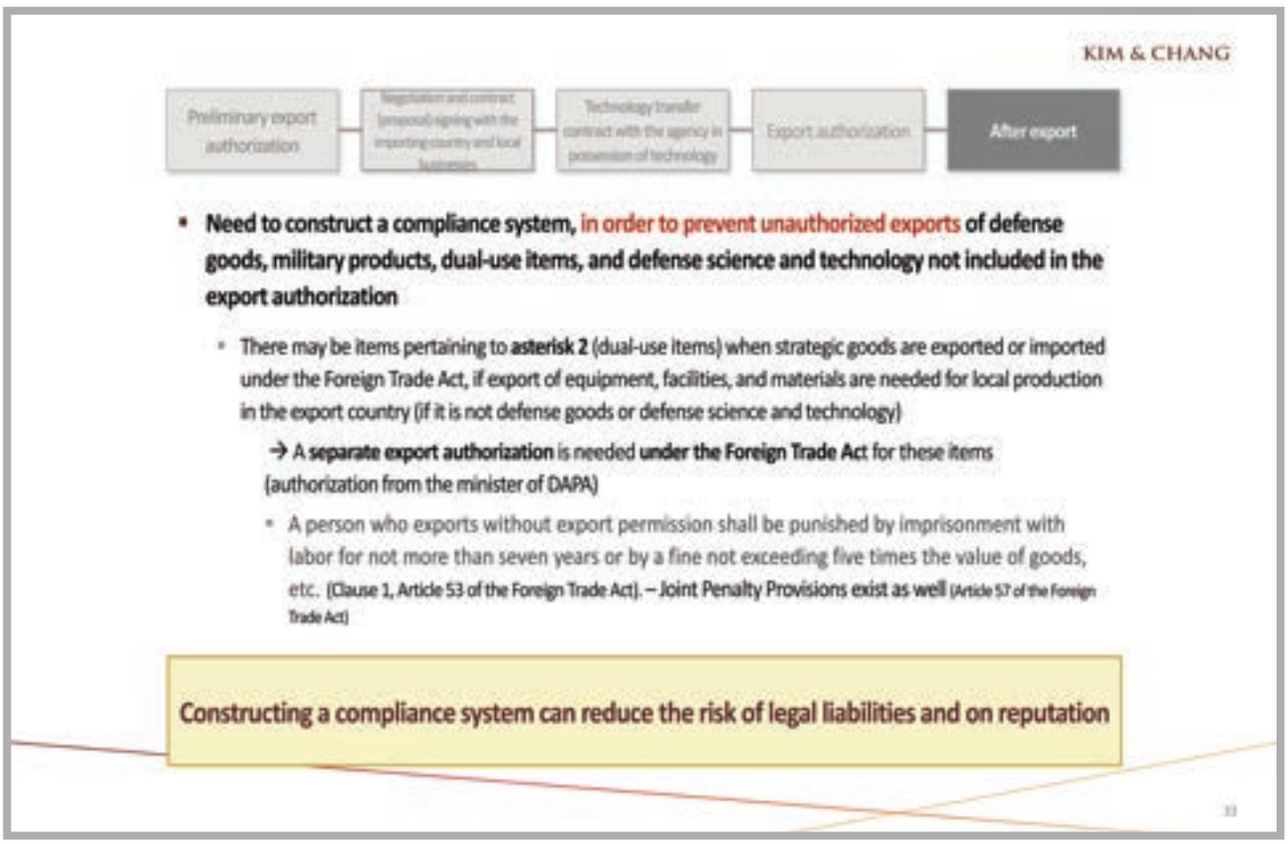

KIM & CHANG
Preliminary export authorization
Export authorization
After export
Sanctions in case of unauthorized exports
A person who obtains permission under Article 53 or the main clause of Article 57 (2) by fraud or other improper means, or performs a relevant act without obtaining permission, shall be punished by imprisonment, with or without labor, for not more than 10 years, or by a fine not exceeding 100 million won. (Clause 2, Article 62 of the Defense Acquisition Program Act)
If a problem occurs due to an overlook from lack of awareness even in situations where advance export authorization was necessary, there will be negative consequences on business and the company's reputation
Administrative measures such as limitations on import and export in case of exporting without export authorization


KIM & CHANG
Preliminary export authorization
Export authorization
After export
Need to prepare for (regular / constant) surveys regarding DAPA defense technology
Article 38 of the Defense Technology Security Guidelines
⑤ The head of the Defense Technology Security Bureau may confirm whether the target agency and/or export counterpart as laid out in the latter part of the preceding clause is complying with the security solutions under Clause 4. In this case, the head of the target agency must cooperate with the confirmation procedures barring any special reasons not to do so.
The Defense Technology Security Guidelines (asterisk 12) specify in detail the survey items for each category:
1. Identification and management of technology, 2. personnel control, 3. facility protection, 4. data protection, 5. technology security in case of R&D, exports, or domestic transfers, and technology security by defense cooperative businesses
In particular, a survey on the application of technology security solutions for defense technology may be conducted
If the survey finds inadequacies, it can lead to improvement recommendations → a correction order → charging of a fine


KIM & CHANG
Preliminary export authorization
Export authorization
After export
Correction orders and etc. as a result of the survey
Article 43 of the Defense Technology Security Guidelines
① The minister of DAPA may determine whether the construction and operation of a defense technology security system is inadequate, based on the key items for investigation in a survey under asterisk 12, and recommend improvements to the head of the target agency under Clause 2, Article 13 of the Act.
Article 44 of the Defense Technology Security Guidelines
① The minister of DAPA may impose a correction order on the head of the target agency if the recommendations for improvement under Clause 1, Article 43, are not fulfilled or inadequately fulfilled.
Article 24 of the Defense Technology Security Act
① Any of the following persons shall be punished by an administrative fine not exceeding 30 million won:
2. Any person who fails to comply with a corrective order provided for in Article 13 (3)

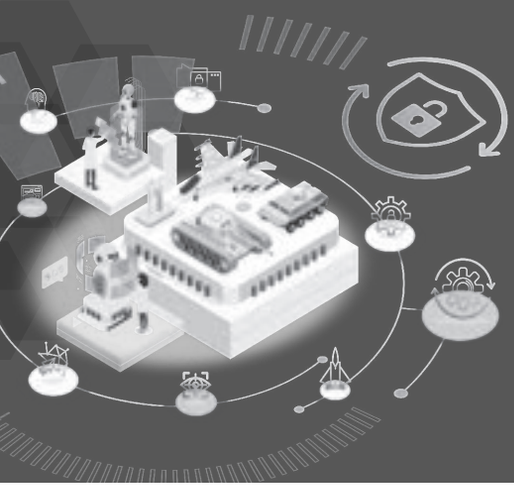

KIM & CHANG
Preliminary export authorization
Negotiation and contract (proposal) signing with the importing country and local businesses
Technology transfer contract with the agency in possession of technology
Export authorization
After export
Policies to strengthen DAPA's surveys
- (실태조사 지원) 기술유출 예방을 위해 실시하는 방위산업기술보호체계 실태조사를 전문적으로 지원하도록 관련 인원 이관 및 법령 개정
* 청 실태조사관 인원(5명)을 방위산업기술보호센터로 이관('23~'24)
2023년도 방위산업기술보호 시행계획
Surveys are expected to be conducted after reinforcing the Defense Technology Security Center's organization by relevant regulatory institutions
Defense businesses had previously been implementing security measures of their own, but they need to prepare in advance for reinforced policies
Need to construct a Compliance system through consulting with a government agency, such as DAPA


KIM & CHANG
Preliminary export authorization
Negotiation and contract (proposal) signing with the importing country and local businesses
Technology transfer contract with the agency in possession of technology
Export authorization
After export
Constant security investigations on local businesses are necessary
It is expected that importing countries and businesses will try their best to ascertain technical information of domestic businesses, particularly in the case of goods or service exports or dispatching domestic personnel overseas
In this context, a rigorous security management system (double, triple protection measures through internal regulations or relevant contracts) is required to prevent technology leakage
Need for consultation on survey-related terms


KIM & CHANG
Preliminary export authorization
Export authorization
After export
Need to construct a compliance system, in order to prevent unauthorized exports of defense goods, military products, dual-use items, and defense science and technology not included in the export authorization
There may be items pertaining to asterisk 2 (dual-use items) when strategic goods are exported or imported under the Foreign Trade Act, if export of equipment, facilities, and materials are needed for local production in the export country (if it is not defense goods or defense science and technology)
→ A separate export authorization is needed under the Foreign Trade Act for these items (authorization from the minister of DAPA)
A person who exports without export permission shall be punished by imprisonment with labor for not more than seven years or by a fine not exceeding five times the value of goods, etc. (Clause 1, Article 53 of the Foreign Trade Act). – Joint Penalty Provisions exist as well (Article 57 of the Foreign Trade Act)
Constructing a compliance system can reduce the risk of legal liabilities and on reputation


Questions & Answers


감사합니다
Thank You
KIM & CHANG

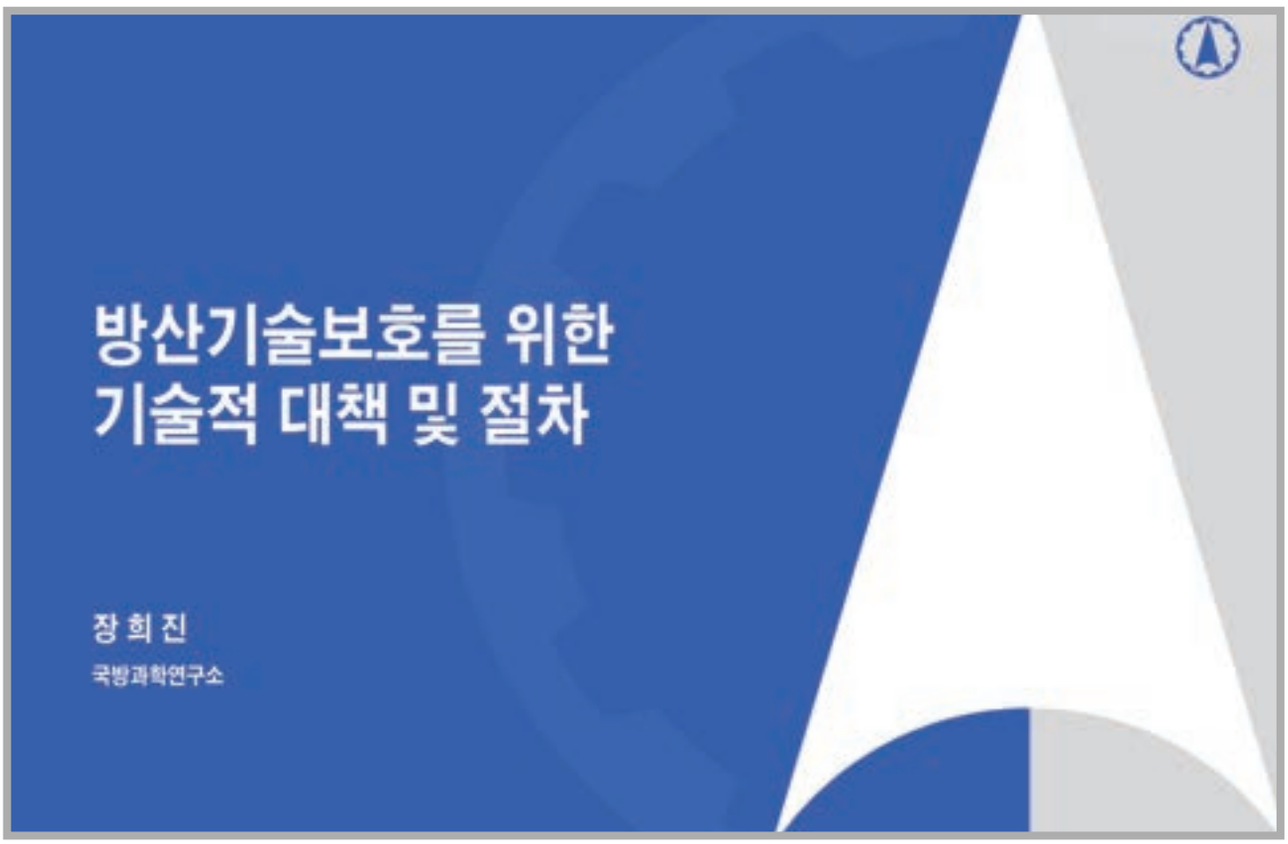


주제발표 3.

방산기술보호를 위한 기술적 대책 및 절차

Technical Measures and Procedures for Defense Technology Protection

국방과학연구소 국방첨단과학기술연구원 사이버기술센터팀장 I **장희진**
Team Leader, Advanced Defense S&T Research Institute - Cyber Technology Center, ADD
Ms. Heejin Jang


방산기술보호를 위한
기술적 대책 및 절차
장 희 진
국방과학연구소


순서
무기체계 사이버 위협과 물리적 공격
안티탬퍼 개요
사례 중심의 안티탬퍼 주요 절차
민간분야와 국방분야 기술보호
맺음말

무기체계 사이버 위협과 물리적 공격

❖ 무기체계에 대한 사이버 위협
- 무기체계 기밀성, 무결성, 가용성 손상하는 원인, 행위, 사건

❖ 주요 무기체계 사이버 위협
- 네트워크 레벨 위협
  - 통신을 통한 데이터 획득

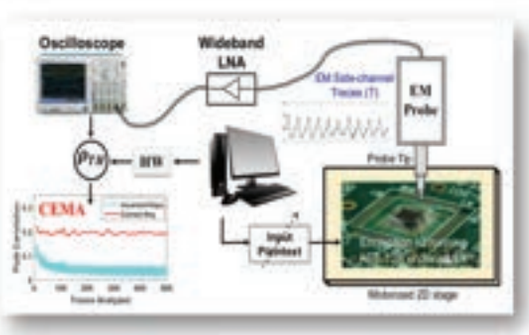
원격 공격

- 보드 레벨 위협
  - 디버그 인터페이스를 통한 메모리 읽기
  - 시리얼 인터페이스를 통한 메모리 읽기
  - 전력분석공격, 글리치 공격 등을 통한 데이터 획득
- 칩 레벨 위협
  - FIB(Focused Ion Beam) 장치를 활용한 보안 센서 우회
  - 전자 현미경을 이용한 메모리 읽기

물리적 공격

무기체계 사이버 위협과 물리적 공격

❖ 물리적 공격 유형
- 비파괴적 공격
  - 부채널 공격
    - 타이밍 분석, 전자파 분석, 전력 분석
  - 오류주입 공격
    - 전압, 온도, 클럭 또는 타이밍 활용
  - SW 공격
    - 외부 인터페이스를 통해 소프트웨어적 통신 방법으로 공격



- 파괴적 공격
  - 시스템 레벨 공격
    - PCB 메시 등 보호장치 해체
    - 솔더마스크 제거, 레이어 분해
  - 칩 레벨 공격
    - 칩 분해, 마이크로프로빙

안티탬퍼 개요

❖ 안티탬퍼 개념

- 역공학을 통한 대응 방안 개발, 비의도적 기술 이전, 시스템 변조를 방해/지연하여 중요 기술 보호

> *System engineering activities intended to deter and/or delay exploitation of critical program information(CPI) in U.S. defense system in domestic and export configurations to impede counter-measure development, unintended technology transfer, or alteration of a system due to reverse engineering.*
>
> ----------DoDD 5200.47E, *Anti-Tamper(AT)*,2015

안티탬퍼 개요

❖ 안티탬퍼 범위

- 시스템에 대한 물리적 소유를 전제로 함
- 시스템을 소유하지않고 원격으로 소유가 가능한 경우가 증가함에 따라 안티탬퍼 경계가 모호해지고 있음

> *Anti-tamper experts typically assume that an adversary will obtain physical possession of the system containing the CPI to be reverse engineered in which case, …. However, tampering can also be attempted remotely(i.e., without first acquiring possession of the system).*
> ---Donald Firesmith, *System Resilience*, Software Engineering Institute(SEI), 2019

안티탬퍼 개요

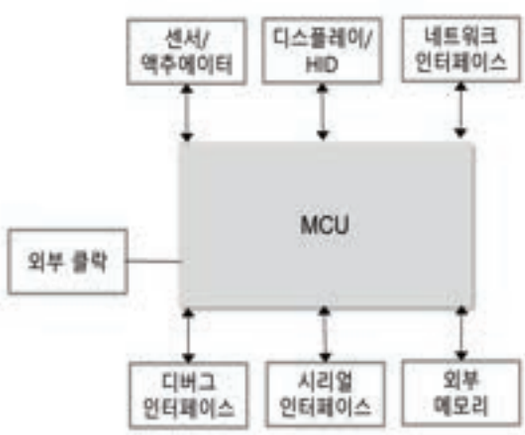
❖ 안티탬퍼 기술 분류

구분	설명
Tamper Deterrence [억제]	● 비인가자가 사전에 접근을 시도하지 못하도록 하는 방법 • 접근방지장치가 있음을 인지하게 하거나, 법적인 조치를 한다는 문구를 삽입하여 접근을 차단하는 방법 • Coating나 Seal을 통해, 물리적 접근 시 흔적을 남기게 하는 방법
Tamper Resistance [방지]	● 비인가자의 접근을 지연 및 저지, 방해하는 기법 • 특수 볼트와 같이 일반적인 공구로는 접근을 어렵게 한다든지, 용접, 접착 등과 같이 임의의 개폐나 접근을 차단하는 방법 • SW에 난독화, 암호화 또는 접근차단 프로그램 등의 적용
Tamper Detection [감지]	● 비인가자가 비정상적인 방법으로 시스템에 접근하였을 경우, 시스템이 알 수 있도록 하는 기법 • 기계적 매커니즘(예, 스위치), 다양한 센서(초도, 압력, 전자파 등) 또는 특수 회로(Mesh Circuit) 등을 통해, 비인가자의 접근을 감지
Tamper Response [대응]	● 비인가자의 비정상적인 방법에 의한 접근을 인지한 경우, 시스템 또는 구성품이 반응하여 특정 조치 또는 기법을 수행 • 데이터나 암호키 삭제 또는 장치의 물리적 파괴 등을 포함

무엇을 보호할 것인가?

❖ 보호 대상

- MCU 내 코드, 데이터, 키(저장, 실행)
- MCU, 센서/액추에이터 간 데이터
- MCU, 디스플레이/HID 간 데이터
- MCU, 네트워크 인터페이스 간 통신 데이터
- 외부 메모리 내 데이터

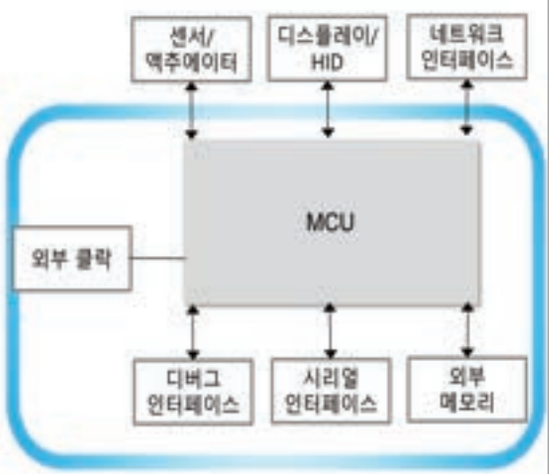


무엇으로부터 보호할 것인가?

- ❖ 시스템 레벨 물리적 공격
  - ● MCU 내 코드, 데이터, 키
    - • 전자파, 전력 분석 등을 이용한 부채널 공격
    - • 온도, 전압, 클럭 등을 이용한 오류주입 공격
    - • JTAG, UART, SPI 등 외부 인터페이스를 통한 SW 공격
  - ● MCU, 센서/액추에이터 간 데이터
  - ● MCU, 디스플레이/HID 간 데이터
  - ● MCU, 네트워크 인터페이스 간 통신 데이터
    - • 데이터 스니핑/스푸핑
    - • 리플레이 공격

어떻게 보호할 것인가?

- ❖ 보호 대상을 포함하는 경계 정의
- ❖ 경계 보호
  - ● 하우징
    - • 조도 센서, 압력 센서, 진동 센서
  - ● PCB 메시
- ❖ 경계 내 안티탬퍼 기술 적용
  - ● 전자파, 전력 분석 등을 이용한 부채널 공격
    - • 마스킹, 하이딩
  - ● 온도, 전압, 클럭 등을 이용한 오류주입 공격
    - • 온도 센서, 전압 모니터, 클럭 모니터
  - ● JTAG, UART, SPI 등 외부 인터페이스를 통한 SW 공격
    - • 비활성화, 접속감지센서
    - • 암호화, 난독화
  - ● 데이터 스니핑/스푸핑
    - • 암호화
  - ● 리플레이 공격
    - • 프로토콜 레벨 대응

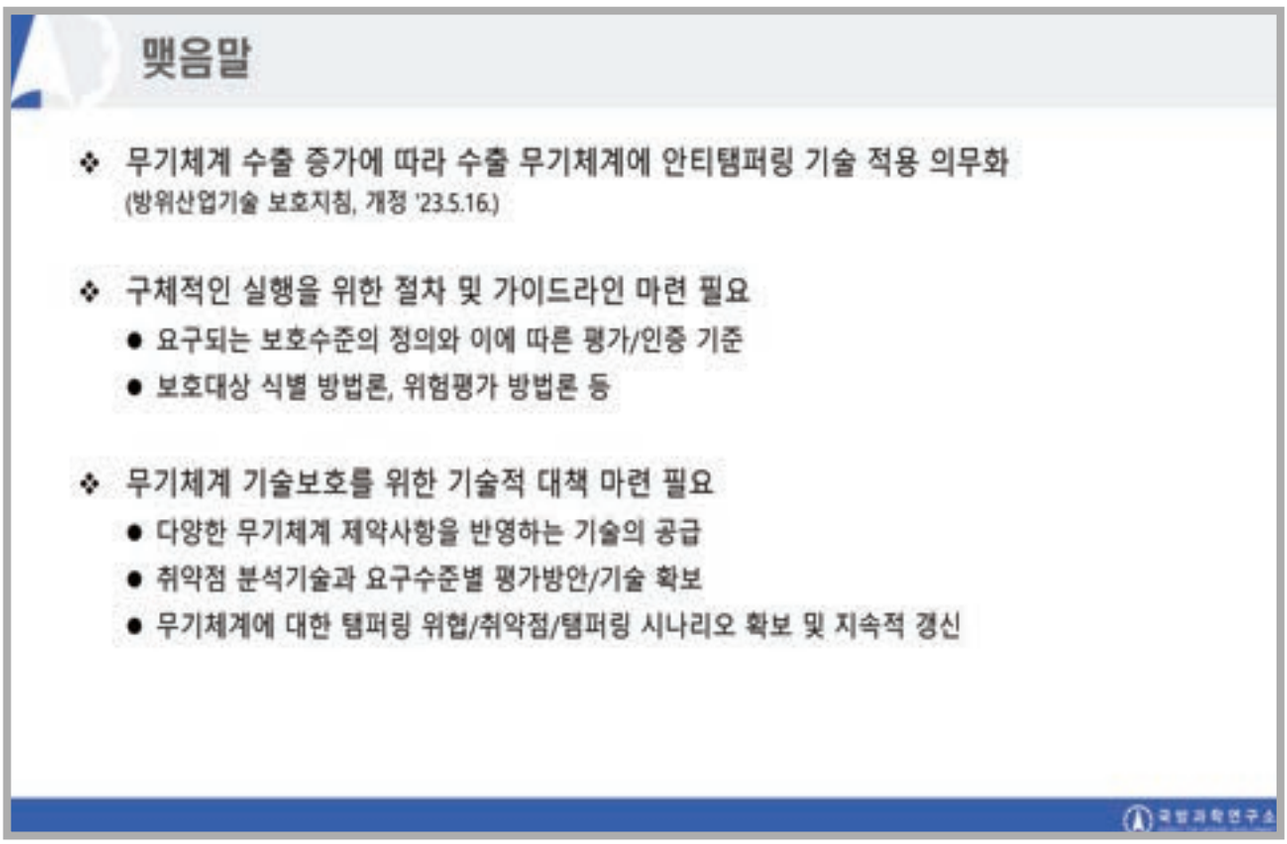


민간분야와 국방분야 기술보호

- 물리적 접근(공격)으로부터 보호 필요
  - 암호모듈, 스마트 카드, 스마트미터, 스마트폰 등
- 주요 인증 기준
  - CC(Common Criteria)
  - FIPS(Federal Information Processing Standards)

민간분야와 국방분야 기술보호

- 보호대상의 중요도와 예상되는 공격 수준
  - 무기체계 기술 유출은 무기체계 기대수명 단축 및 군사적 우위 약화로 이어짐
  - 무기체계 기술 탈취 시도는 국가적 차원에서 이루어짐
- 엄격한 무기체계 운용환경조건
- 무기체계 고유의 기능/성능 유지
  - 실시간성, 형상, 소모전력 등


맺음말
❖ 무기체계 수출 증가에 따라 수출 무기체계에 안티탬퍼링 기술 적용 의무화
(방위산업기술 보호지침, 개정 '23.5.16.)
❖ 구체적인 실행을 위한 절차 및 가이드라인 마련 필요
● 요구되는 보호수준의 정의와 이에 따른 평가/인증 기준
● 보호대상 식별 방법론, 위험평가 방법론 등
❖ 무기체계 기술보호를 위한 기술적 대책 마련 필요
● 다양한 무기체계 제약사항을 반영하는 기술의 공급
● 취약점 분석기술과 요구수준별 평가방안/기술 확보
● 무기체계에 대한 탬퍼링 위협/취약점/탬퍼링 시나리오 확보 및 지속적 갱신


Technical Measures and Procedures
for Defense Technology Protection
Heejin Jang
ADD

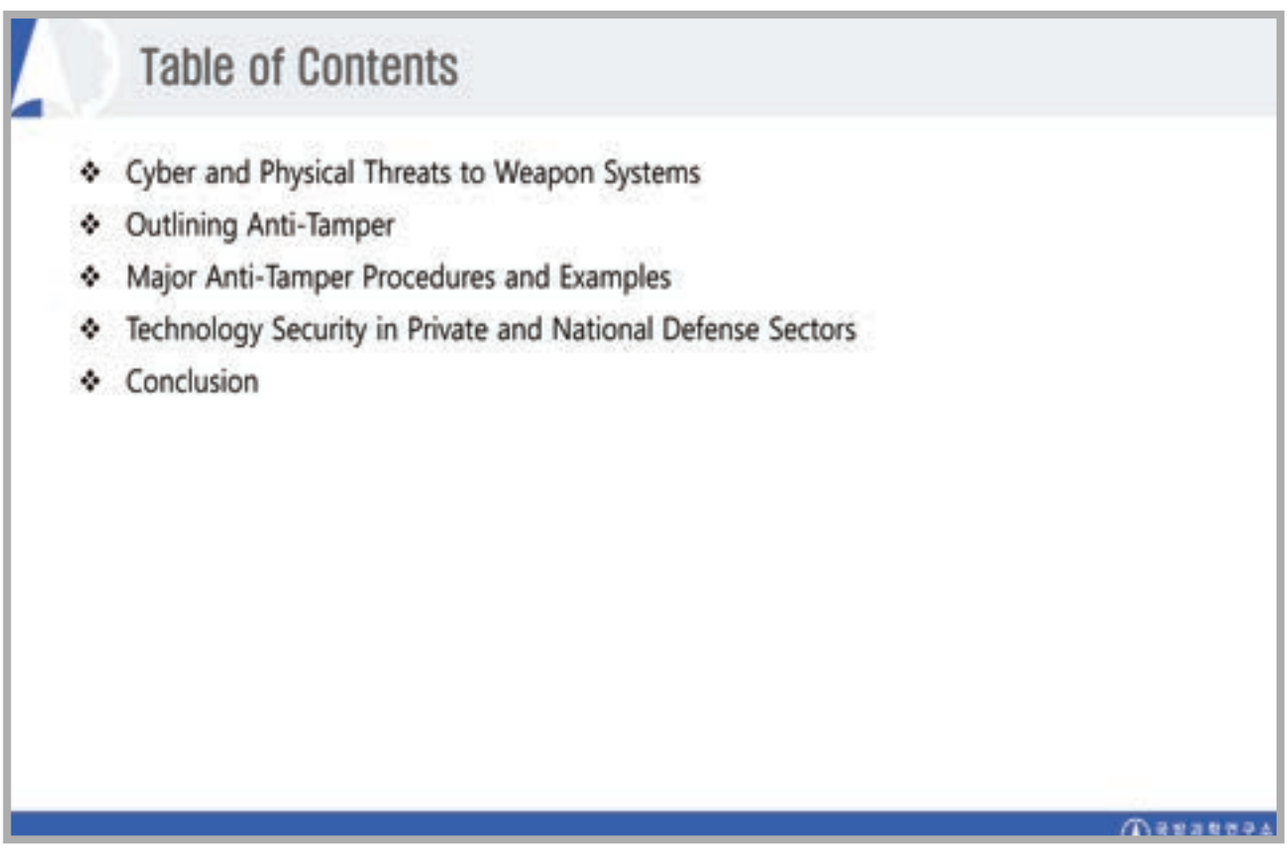


Table of Contents
Cyber and Physical Threats to Weapon Systems
Outlining Anti-Tamper
Major Anti-Tamper Procedures and Examples
Technology Security in Private and National Defense Sectors
Conclusion

Cyber and Physical Threats to Weapon Systems

❖ Cyber Threats to Weapon Systems

- Reasons, acts, and events that damage weapon systems' confidentiality, integrity, and availability

❖ Major Cyber Threats to Weapon Systems

- Threats on the Network Level
  - Data acquisition through communications

Remote Attacks

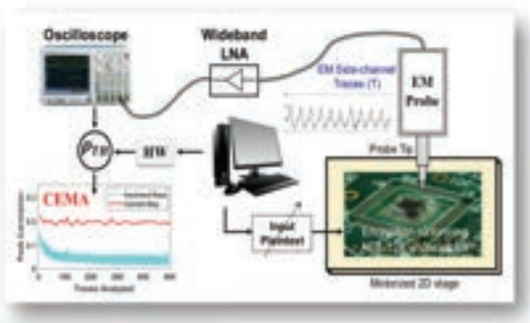
- Threats on the Board Level
  - Reading memory through debug interface
  - Reading memory through serial interface
  - Data acquisition through power analysis attack, glitch attack
- Threats on the Chip Level
  - Circumventing security sensors with FIB devices
  - Reading memory with electron microscopes

Physical Attacks

Cyber and Physical Threats to Weapon Systems

❖ Types of Physical Attacks

- Non-Destructive Attacks
  - Subchannel Attacks
    - Timing, electromagnetic waves, and power analysis
  - Fault Injection Attacks
    - Utilizing voltage, temperature, clock, and timing
  - SW Attacks
    - A software communication method of attacking through an outside interface



- Destructive Attacks
  - Attacks on the System Level
    - Dismantling protective equipment such as PCB Mesh
    - Removing solder mask, dismantling layers
  - Attacks on the Chip Level
    - Disassembling chips, microprobing

Outlining Anti-Tamper

❖ Concept of Anti-Tamper

- Protecting critical technology by development of response strategies through reverse engineering, unintended technology transfer, and disrupting or delaying system modulation

> *System engineering activities intended to deter and/or delay exploitation of critical program information(CPI) in U.S. defense system in domestic and export configurations to impede counter-measure development, unintended technology transfer, or alteration of a system due to reverse engineering.*
>
> ----------DoDD 5200.47E, *Anti-Tamper(AT)*,2015

Outlining Anti-Tamper

❖ Range of Anti-Tamper

- Prerequisite of physical possession of the system
- Anti-tamper borders are becoming ambiguous as it becomes increasingly possible to possess the system remotely

> *Anti-tamper experts typically assume that an adversary will obtain physical possession of the system containing the CPI to be reverse engineered in which case, …. However, tampering can also be attempted remotely(i.e., without first acquiring possession of the system).*
> ---Donald Firesmith, *System Resilience*, Software Engineering Institute(SEI), 2019

Outlining Anti-Tamper

❖ Classification of Anti-Tamper Technology

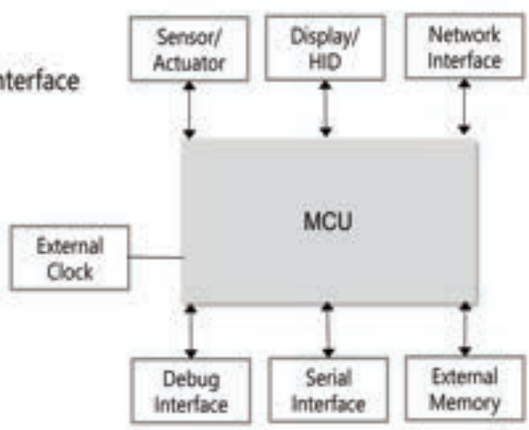
Classification	Description
Tamper Deterrence	● **Preemptively denying access to unauthorized persons** • Blocking access by letting accessors know of an access control system, or inserting a message warning of legal measures • Making physical approaches leave traces through coating or seals
Tamper Resistance	● **Delaying, blocking, disrupting access by unauthorized persons** • Blocking arbitrary make and break or access (such as welding and adhesion) by making access difficult by ordinary tools such as special bolts • Applying obfuscation, encoding, or access-blocking programs to SW
Tamper Detection	● **Making sure the system is aware of unauthorized persons accessing the system through abnormal means** • Detecting unauthorized access through a mechanical mechanism (e.g. a switch), various sensors (e.g. illumination, pressure, waves), or special circuits (e.g. mesh circuit)
Tamper Response	● **Performance of certain measures or techniques by the system or parts in response to unauthorized persons' abnormal access** • Includes deleting data or encryption keys, or physical destruction of the device

What to Protect?

Major Anti-Tamper Procedures and Examples

❖ Objects of Protection

- Codes, data, keys (storage, execution) within MCU
- Data between MCU and sensors/actuators
- Data between MCU and displays/HID
- Communications data between MCU and network interface
- Data within external memory



Major Anti-Tamper Procedures and Examples

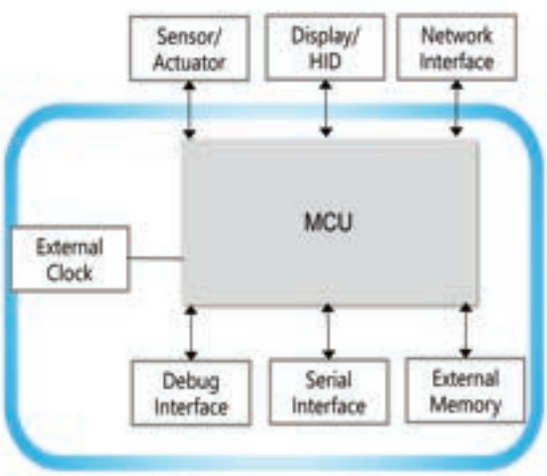
What to Protect From?

- ❖ Physical Attacks on the System Level
  - Codes, Data, Keys within MCU
    - Subchannel attack using electromagnetic waves or power analysis
    - Fault injection attack using temperature, voltage, clock
    - SW attack through an external interface such as JTAG, UART, SPI
  - Data between MCU and Sensors/Actuators
  - Data between MCU and Display/HID
  - Communications Data between MCU and Network Interface
    - Data sniffing/spoofing
    - Replay attack

Major Anti-Tamper Procedures and Examples

How to Protect?

- ❖ Defining Borders that Include Objects of Protection
- ❖ Protecting Borders
  - Housing
    - Illumination, pressure, vibration sensors
  - PCB Mesh
- ❖ Applying Anti-Tamper Technology within Borders
  - Subchannel attack using electromagnetic waves or power analysis
    - Masking, hiding
  - Fault injection attack using temperature, voltage, clock
    - Temperature sensors, voltage monitors, clock monitors
  - SW attack through an external interface such as JTAG, UART, SPI
    - Deactivation, access detection sensors
    - Encryption, obfuscation
  - Data sniffing/spoofing
    - Encryption
  - Replay attack
    - Response on the protocol level

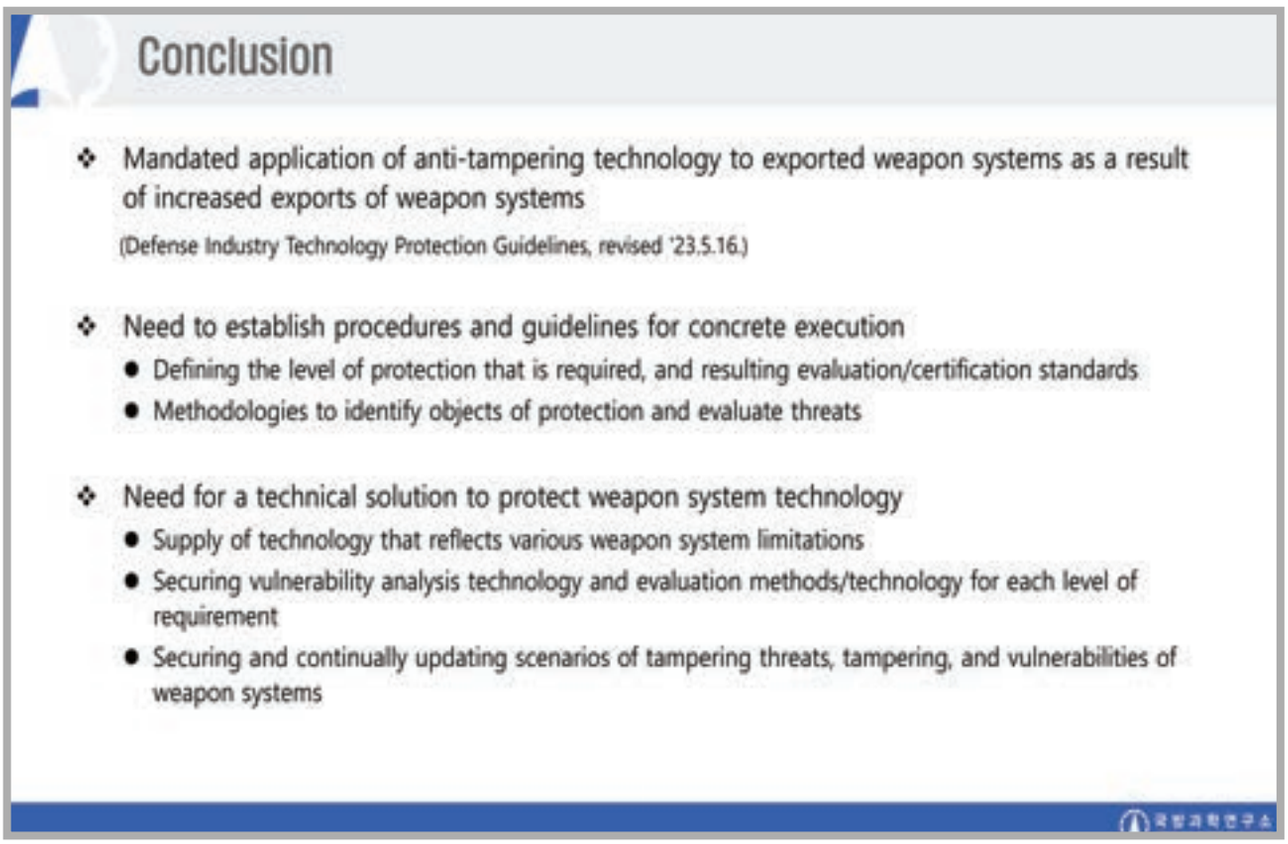


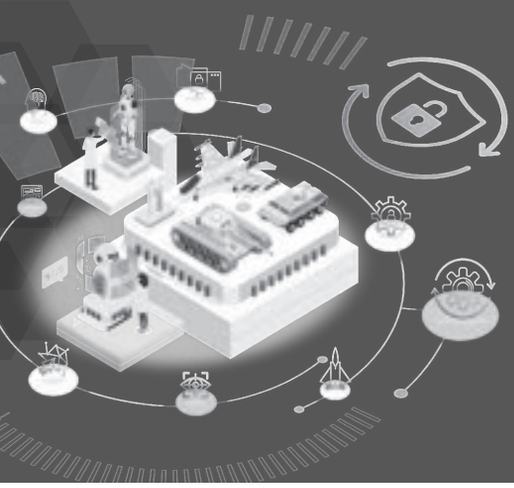
Technology Security in Private and National Defense Sectors

- ❖ Need to Protect from Physical Access (Attacks)
  - Encryption modules, smart cards, smart meters, smartphones
- ❖ Major Certifications
  - CC (Common Criteria)
  - FIPS (Federal Information Processing Standards)

Technology Security in Private and National Defense Sectors

- ❖ Importance of the object of protection and expected level of attack
  - Leakage of weapon system technology leads to shortening the life expectancy of weapon systems and weakening military advantage
  - Attempts to hijack weapon system technology are made on a national basis
- ❖ Rigorous operating environment standards for weapon systems
- ❖ Maintaining functions and performance unique to a weapon system
  - Realtime, configuration, power consumption, etc.


Conclusion
❖ Mandated application of anti-tampering technology to exported weapon systems as a result of increased exports of weapon systems
(Defense Industry Technology Protection Guidelines, revised '23.5.16.)
❖ Need to establish procedures and guidelines for concrete execution
● Defining the level of protection that is required, and resulting evaluation/certification standards
● Methodologies to identify objects of protection and evaluate threats
❖ Need for a technical solution to protect weapon system technology
● Supply of technology that reflects various weapon system limitations
● Securing vulnerability analysis technology and evaluation methods/technology for each level of requirement
● Securing and continually updating scenarios of tampering threats, tampering, and vulnerabilities of weapon systems



주제발표 4.

국제 수출통제제도 경향과 기술보호 측면의 시사점

Trends in International Export Control Regimes and Implications for Technology Protection

전략물자관리원 국제체제팀장 I **류세희**
Director, Multilateral Export Controls Team, Policy Support Department, KOSTI
Mr. Sehee Ryu

'23 방산기술보호 컨퍼런스

국제 수출통제제도 경향과 기술보호 측면의 시사점 (Trends in International Export Control Regimes and Implications for Technology Protection)

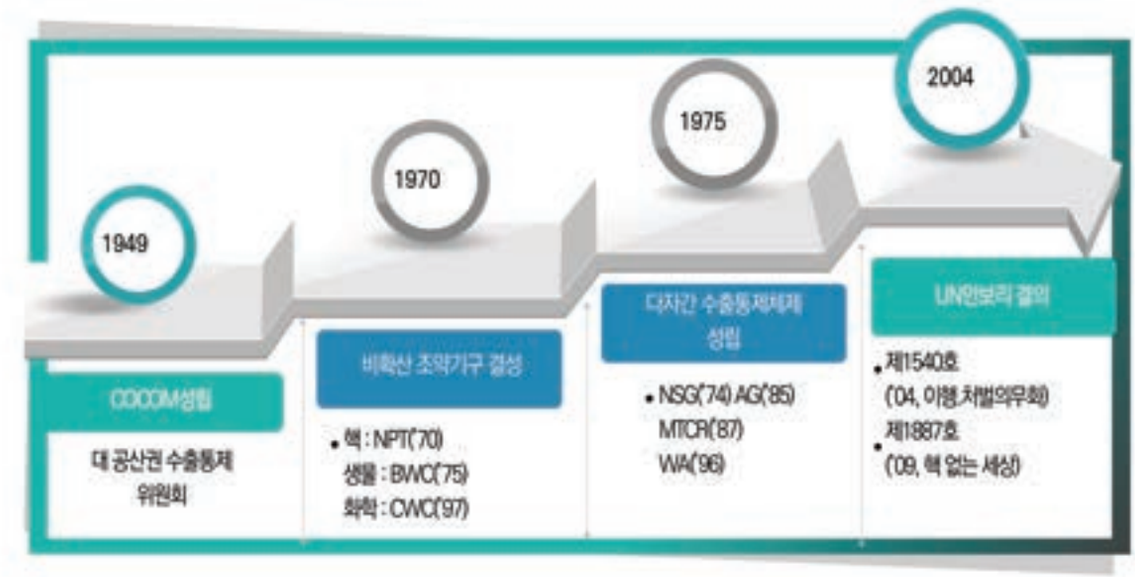
전략물자관리원
국제체제팀
류세희 팀장

+82-2-6000-6380
shryu@kosti.or.kr

kosti

국제수출통제체제 연혁

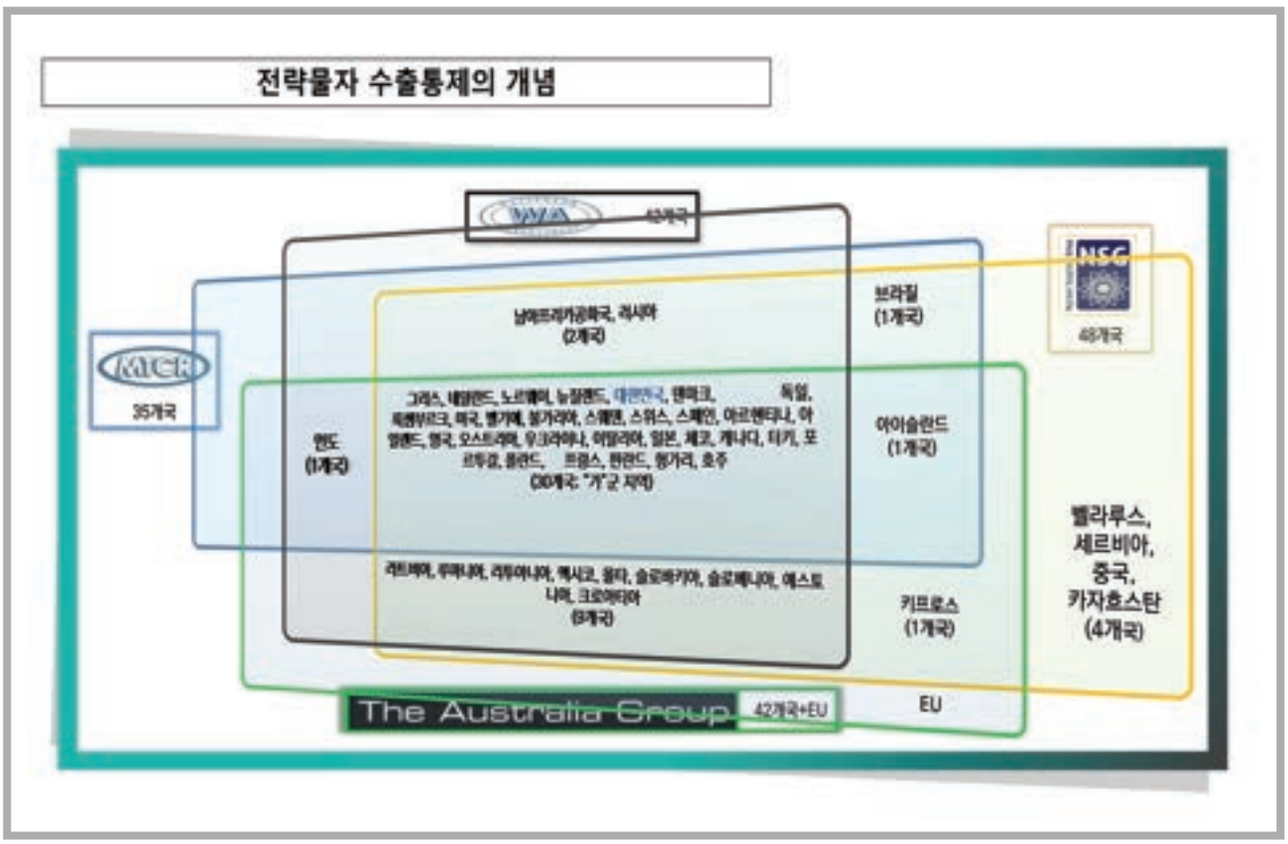
o 연도별 수출통제체제 변화내용



국제수출통제체제 연혁

구분	국제수출통제체제				비확산조약	
	바세나르체제 (WA)	핵공급국그룹 (NSG)	미사일기술통제체제 (MTCR)	호주그룹 (AG)	화학무기금지협약 (CWC)	생물무기금지협약 (BWC)
설립	1996	1978	1987	1985	1997	1975
회원국	42개국	48개국	35개국	43개국	193개국	174개국
한국 가입	1996	1995	2001	1996	1997	1987
통제 대상	재래식 무기 (총기, 화약 등) 및 이중용도품목 (소재, 기계, 전자, 화학 등)	원자력 전용물품 및 이중용도품목 (원심분리기 등)	미사일 관련 물품 (미사일, 로켓, 항법장치 등)	생화학 무기 원료 및 제조장치 (바이러스, 독소 등)	1,2,3종 독성 화학물질 및 원료	국제적으로 규정한 품목은 없으나 국내 화학생물무기 금지법에 67종의 생물작용체 규정

전략물자 수출통제의 개념



수출통제 기본사항

- Kevin Wolf (前 미국 상무부 수출통제 담당 차관보)

- 수출통제란 다음을 규율하는 규칙을 의미함

1. 다양한 종류의 국가안보, 대외정책 목적을 달성하기 위해
2. 물품, 기술, 소프트웨어, 서비스를
3. 목적지, 최종용도, 최종사용자로
4. 자국민 및 외국인에 의해 수출, 재수출 및 이전하는 것

수출통제의 개념도

행위 / 행위자	물리적 요소 ("Goods," "Commodities," "Defense Articles")	정보 ("Technology," "Technical Data")	소프트웨어	서비스 ("Defense services" or WMD-related "activities")
목적지 (Countries or regions, for listed items, or embargoed destinations for all else)				
최종용도 (e.g., WMD end uses regardless of item's classification)				
최종사용자 (e.g., SDNs or Entity List entities, regardless of item's classification)				

바세나르체제 최신 아웃리치 발표자료

Ambassador Jaideep Mazumdar · 2023 Plenary Chair

Ambassador Dr. Gyorgy Molnar · Head of Secretariat

Purposes

Participating States seek to contribute to regional and international security and stability by promoting:

- transparency and
- greater responsibility

in transfers of **Conventional Arms** and **Dual-Use Goods & Technologies**, thus preventing:

- destabilising accumulations and
- acquisition by terrorists


WA Control Lists
Munitions List
• 22 Categories
• 300 entries
Dual-Use List
• 9 Categories
• Over 1,000 entries
• Sensitive List


List Review Process
Market Trends
Developments in International Security
List Review
Advances in Technology

The Munitions List

Only one criterion:
the military characteristics.

Concept of
"Specially designed or modified for military use"

The Dual-Use List

Dual Use Goods and Technologies are intended for
Civil-use applications
They can also be used for military applications

Because WA does not seek to impede bona fide civil transactions, by using generic parameters which would capture civil market goods

Criteria are **multiple and complex**

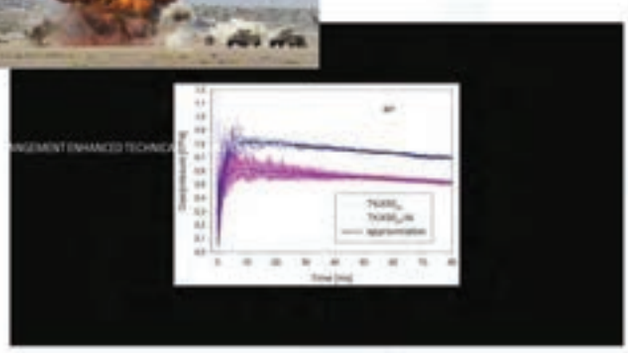
Annex E

LIST CHANGES 2018-2022
Categories 1, 2, 7, 8, 9.

Enhanced Technical Briefing 19 June 2023

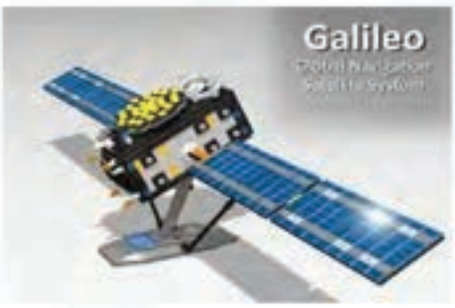
Changes to Categories 1, 2, 7, 8, 9.

CAT 1 List "EXPLOSIVES". EDNA and TKX-50 added to the list.



Changes to Categories 1, 2, 7, 8, 9.

7.A. *Satellite Navigation Systems* replace *Global Navigation Satellite Systems*



Changes to Categories 1, 2, 7, 8, 9.

8.A.2.o.4. Permanent Magnet, including Rim-Driven, propulsion

Changes to Categories 1, 2, 7, 8, 9.

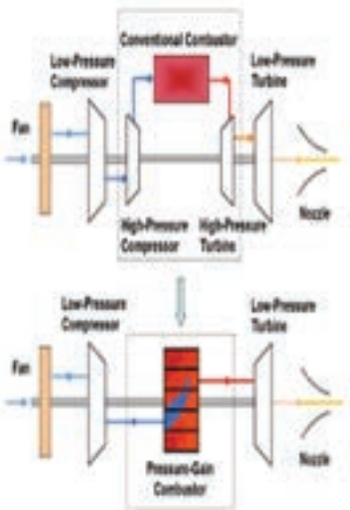
9.A.4.h. Sub-orbital craft.

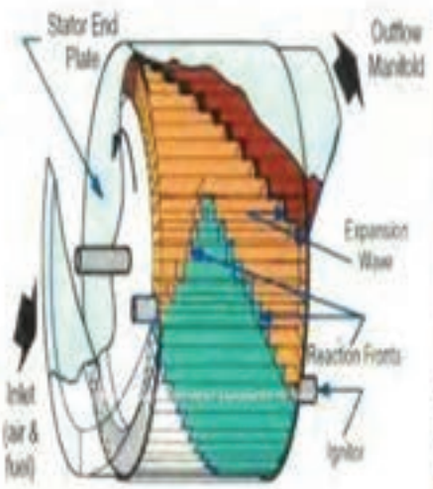
Changes to Categories 1, 2, 7, 8, 9.

9.A.4.g. Aircraft specially designed or modified to be Air-launch Platforms for space launch vehicles or sub-orbital craft.

Changes to Categories 1, 2, 7, 8, 9.

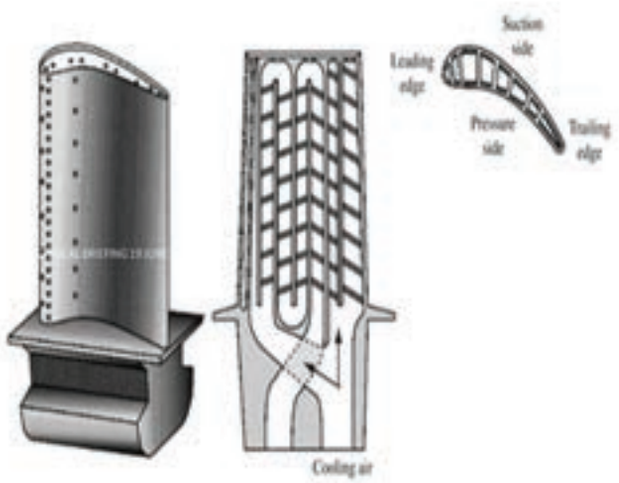
9.E.3.a.2.e. Pressure Gain Combustion





Changes to Categories 1, 2, 7, 8, 9.

9.E.3.k. Supersonic Enabling Technology.



Annex F

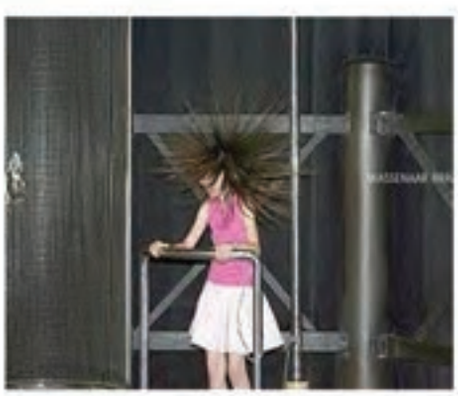
LIST CHANGES 2018-2022

Categories 3, 4, 5 Part 1, 5 Part 2, 6.

Enhanced Technical Briefing 19 June 2023

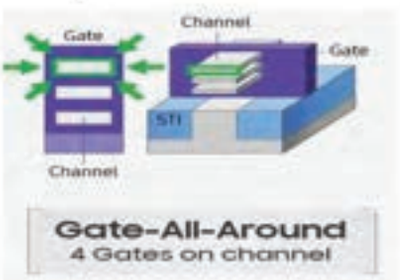
Changes to Categories 3, 4, 5 Part 1, 5 Part 2, 6.

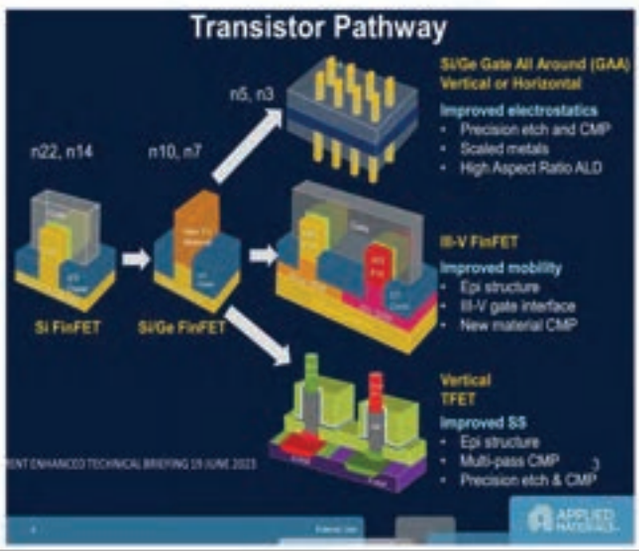
3.D.5. Software for restoring operation of microcircuits or computers after Electromagnetic Pulse (EMP) or Electrostatic Discharge (ESD)



Changes to Categories 3, 4, 5 Part 1, 5 Part 2, 6.

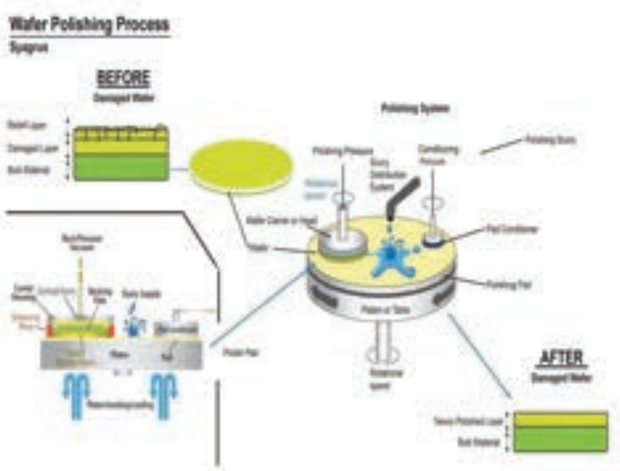
3.D.6. Electronic Computer-Aided Design (ECAD) Software for the development of Gate All-Around Field-Effect Transistor (GAAFET) circuits.

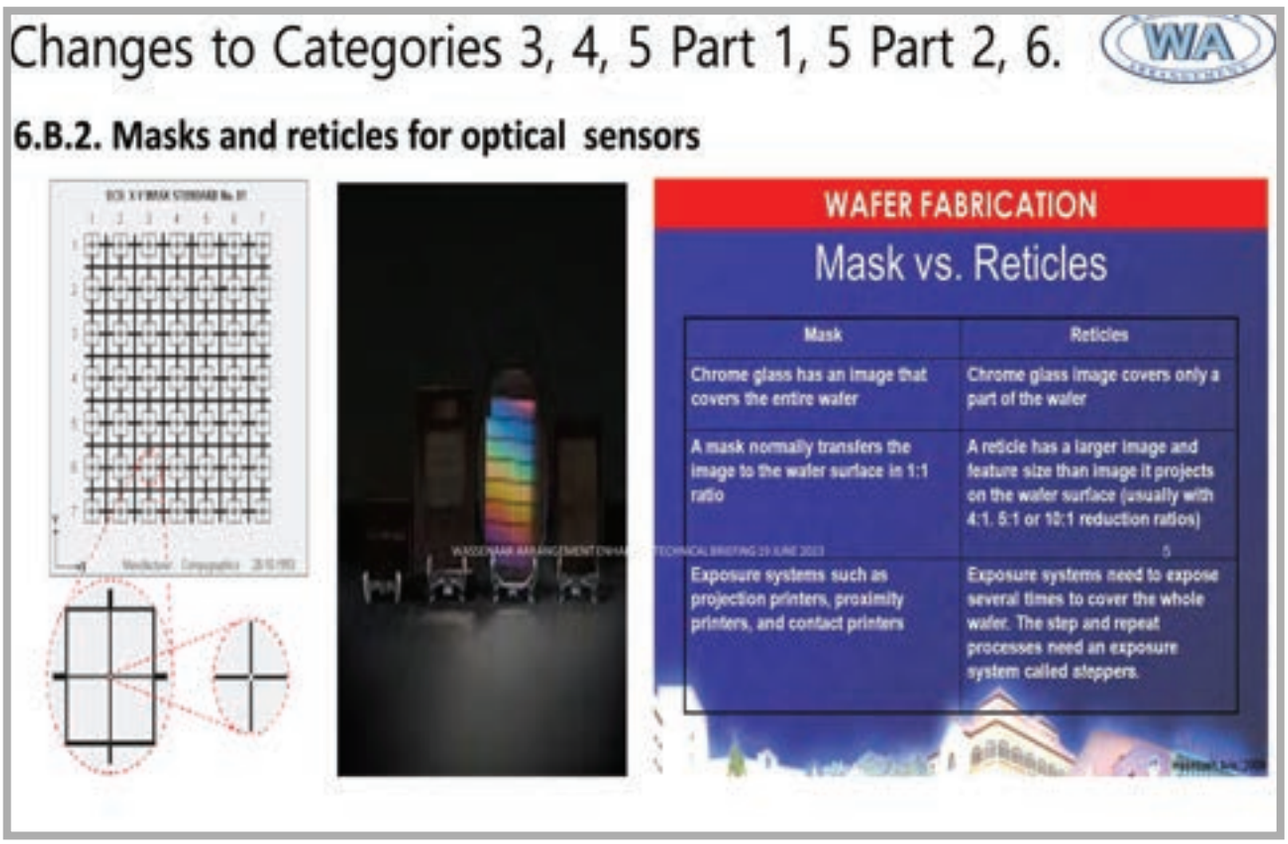


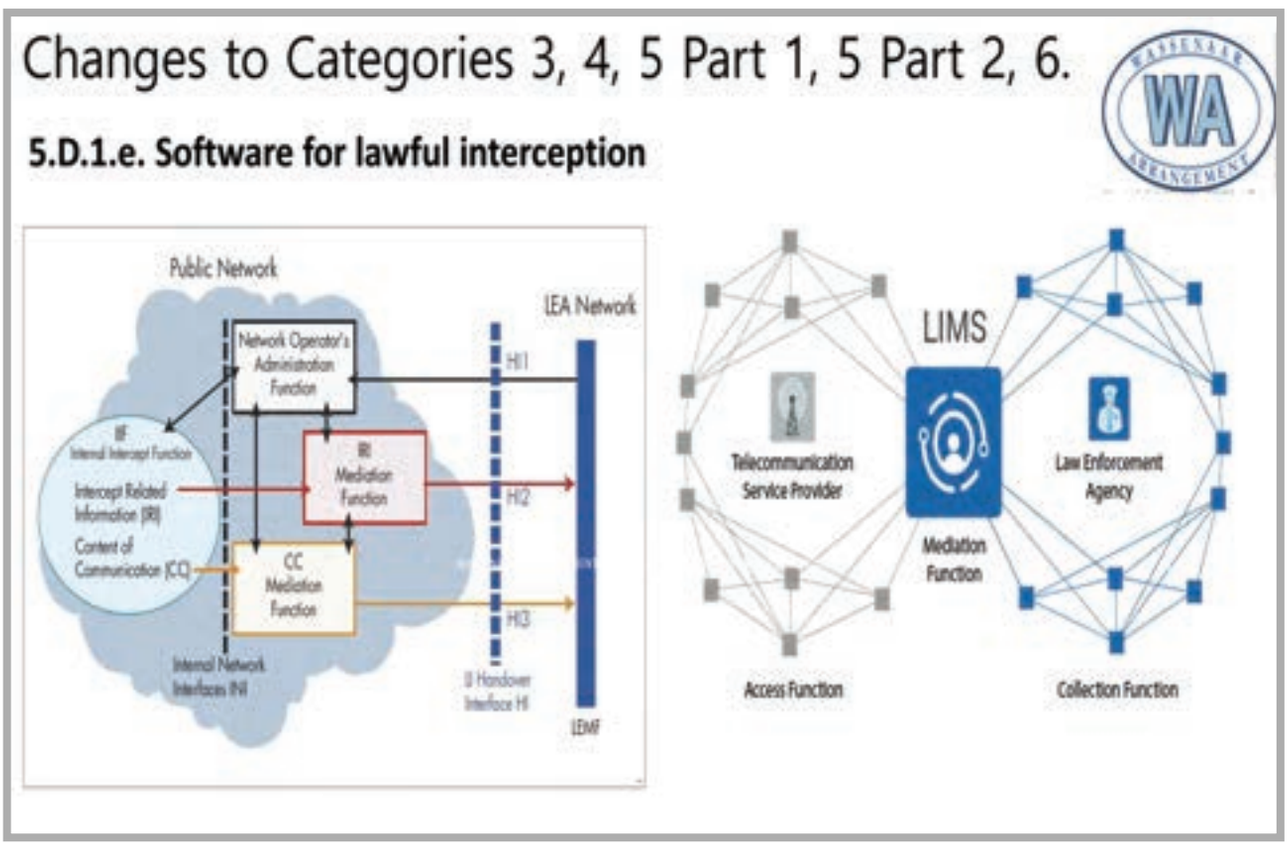


Changes to Categories 3, 4, 5 Part 1, 5 Part 2, 6.

3.E.4. Technology for high-surface quality slicing, grinding or polishing of 300 mm silicon wafers.




Changes to Categories 3, 4, 5 Part 1, 5 Part 2, 6.
WA
6.B.2. Masks and reticles for optical sensors
WAFER FABRICATION
Mask vs. Reticles
Mask
Reticles
Chrome glass has an image that covers the entire wafer
Chrome glass image covers only a part of the wafer
A mask normally transfers the image to the wafer surface in 1:1 ratio
A reticle has a larger image and feature size than image it projects on the wafer surface (usually with 4:1, 5:1 or 10:1 reduction ratios)
Exposure systems such as projection printers, proximity printers, and contact printers
Exposure systems need to expose several times to cover the whole wafer. The step and repeat processes need an exposure system called steppers.

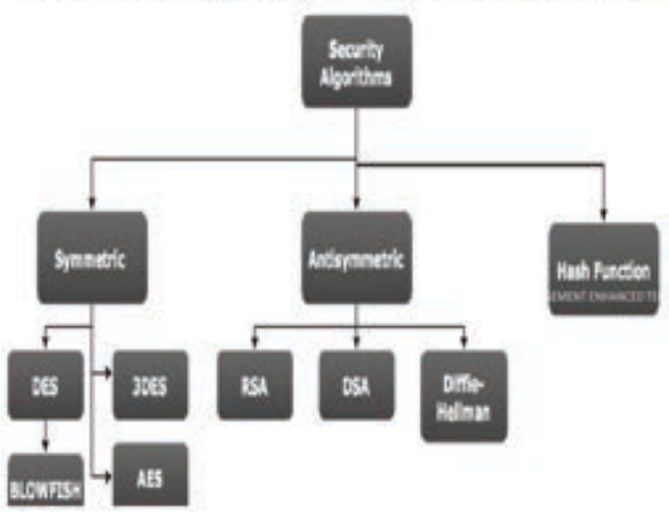

Changes to Categories 3, 4, 5 Part 1, 5 Part 2, 6.
WA
5.D.1.e. Software for lawful interception
Public Network
LEA Network
Network Operator's Administration Function
IRI Mediation Function
CC Mediation Function
Intercept Related Information (IRI)
Content of Communication (CC)
HI1
HI2
HI3
Internal Network Interfaces INI
X Handover Interface HI
LEMF
LIMS
Telecommunication Service Provider
Mediation Function
Law Enforcement Agency
Access Function
Collection Function

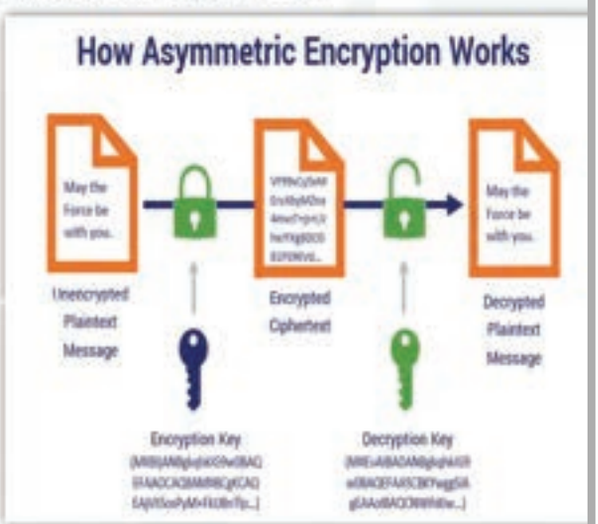
Changes to Categories 3, 4, 5 Part 1, 5 Part 2, 6.

5.A.4.b. Digital Investigation (Forensic) tools

Changes to Categories 3, 4, 5 Part 1, 5 Part 2, 6.

5.A.2.a. *Described security algorithm* replaces *In excess of 56 Bits*
5.A.2.a. Technical Note 2.c. new entry for *asymmetric algorithm*



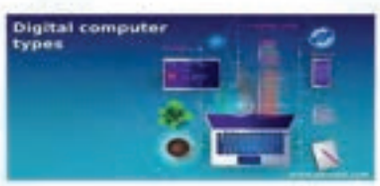


Changes to Categories 3, 4, 5 Part 1, 5 Part 2, 6.

In addition to these significant new entries, many control threshold values throughout the List have been updated to keep pace with the constant evolution of technology. This is in particular the case for :

- **Digital Computers**
- **Lasers**
- **Signal analysers, Signal generators or Frequency synthesisers**

These updates are intended to exclude from the controls items having increasing legitimate civil use and ensure that only items of strategic concern remain controlled.



Annex G

LIST CHANGES 2018-2022
Munitions List

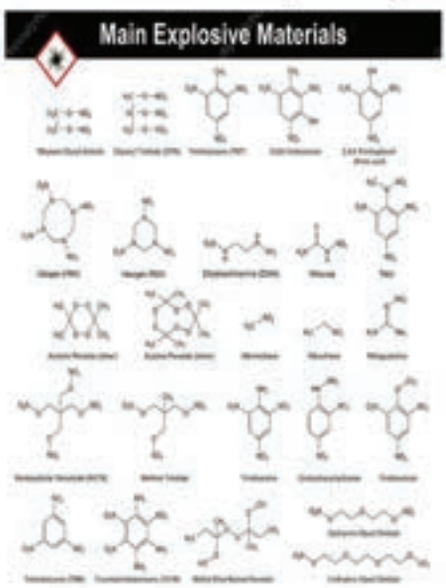
Enhanced Technical Briefing · 19 June 2023

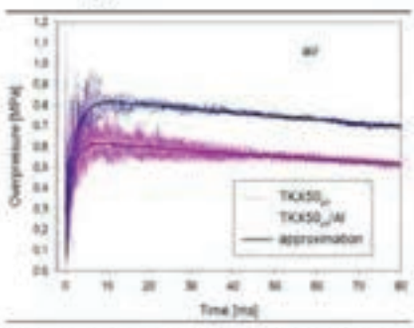
Changes to the Munitions List

The criteria for the Munitions List are more binary (specially designed/not specially designed) than the DU List. Therefore, most of the newest or most advanced weapons are already controlled under an existing item. Changes are mostly intended to clarify the list, improve its readability for exporters and licensing officers, or exclude obsolete items having no military significance.

Changes to the Munitions List

ML 8.a.43. TKX-50 explosive (new entry)





Explosives of military concern are normally added to the DU List and to the ML

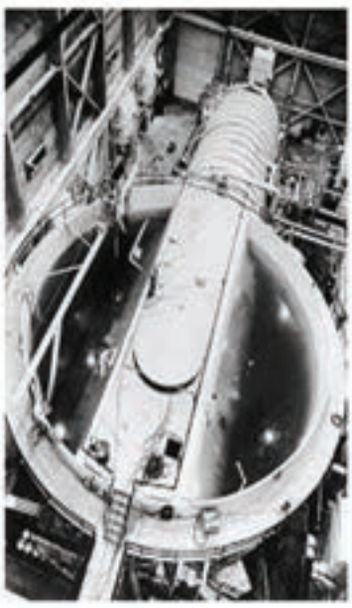
ML8.a.33. "Explosives" not listed elsewhere in ML8.a. and having any of the following:

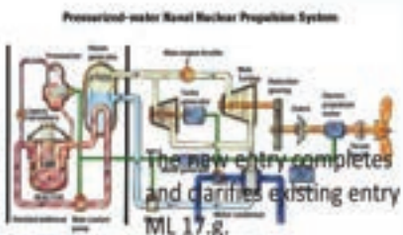
a.Detonation velocity exceeding 8,700 m/s, at maximum density, or

b.Detonation pressure exceeding 34 GPa (340 kbar);

Changes to the Munitions List

ML9.h. Nuclear power generating equipment or propulsion equipment (new entry)





The new entry completes and clarifies existing entry ML 17.g.

Changes to the Munitions List

ML13.c. Helmets and specially designed components and accessories

~~*c. Helmets manufactured according to military standards or specifications, or comparable national standards, and specially designed helmet shells, liners, or comfort pads, therefor;*~~

~~*Note 2 ML13.c. does not apply to* **conventional steel helmets,** *neither modified or designed to accept, nor equipped with any type of accessory device.*~~

c. Helmets and specially designed components and accessories therefor, as follows:

1.Helmets manufactured according to military standards or specifications, or comparable national standards;

2.Shells, liners, or comfort pads, specially designed for helmets specified in ML13.c.1.;

3.Add-on ballistic protection elements, specially designed for helmets specified in ML13.c.1.

The new text clarifies the status of components and accessories sometimes exported separately.

Changes to the Munitions List

ML 10. Note 6. decontrol of vintage aero-engines

Messerschmidt 262 (Seattle Museum) and its 1942 JUMO Axial compressor Turbojet Engine.

Changes to the Munitions List

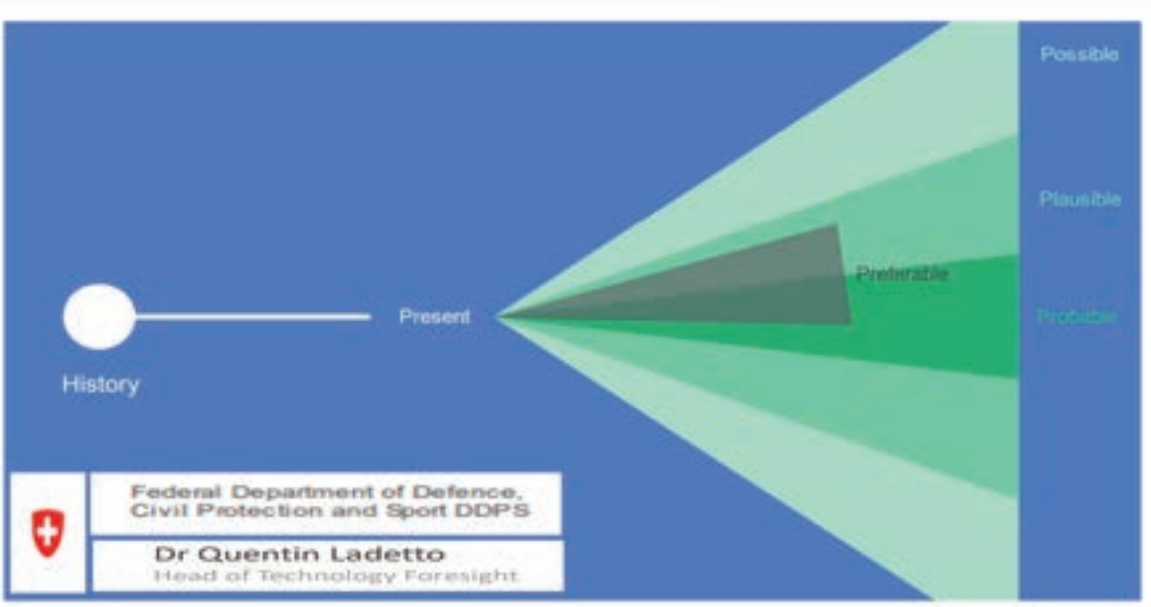
ML 21.b.5 Software specially designed or modified for the conduct of military offensive cyber operations (new entry)

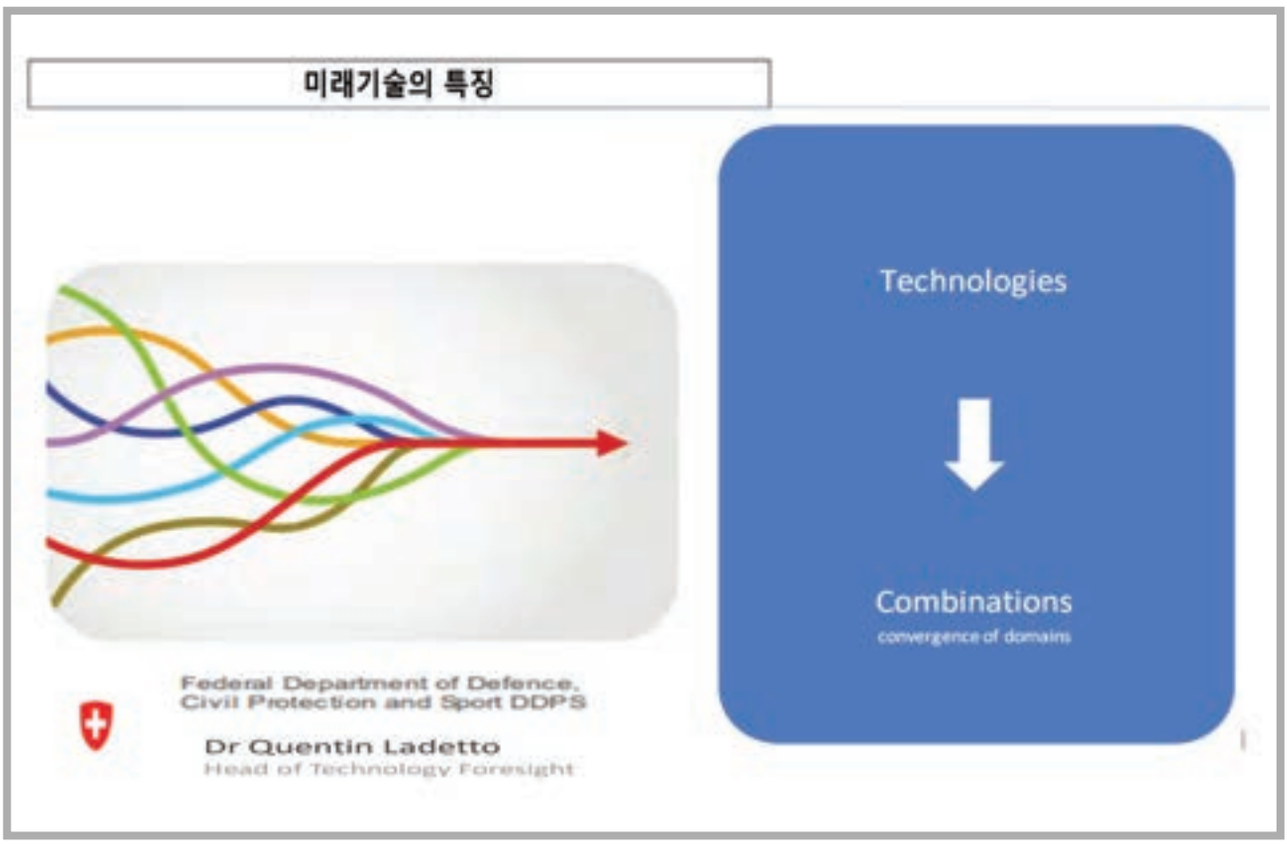
Changes to the Munitions List

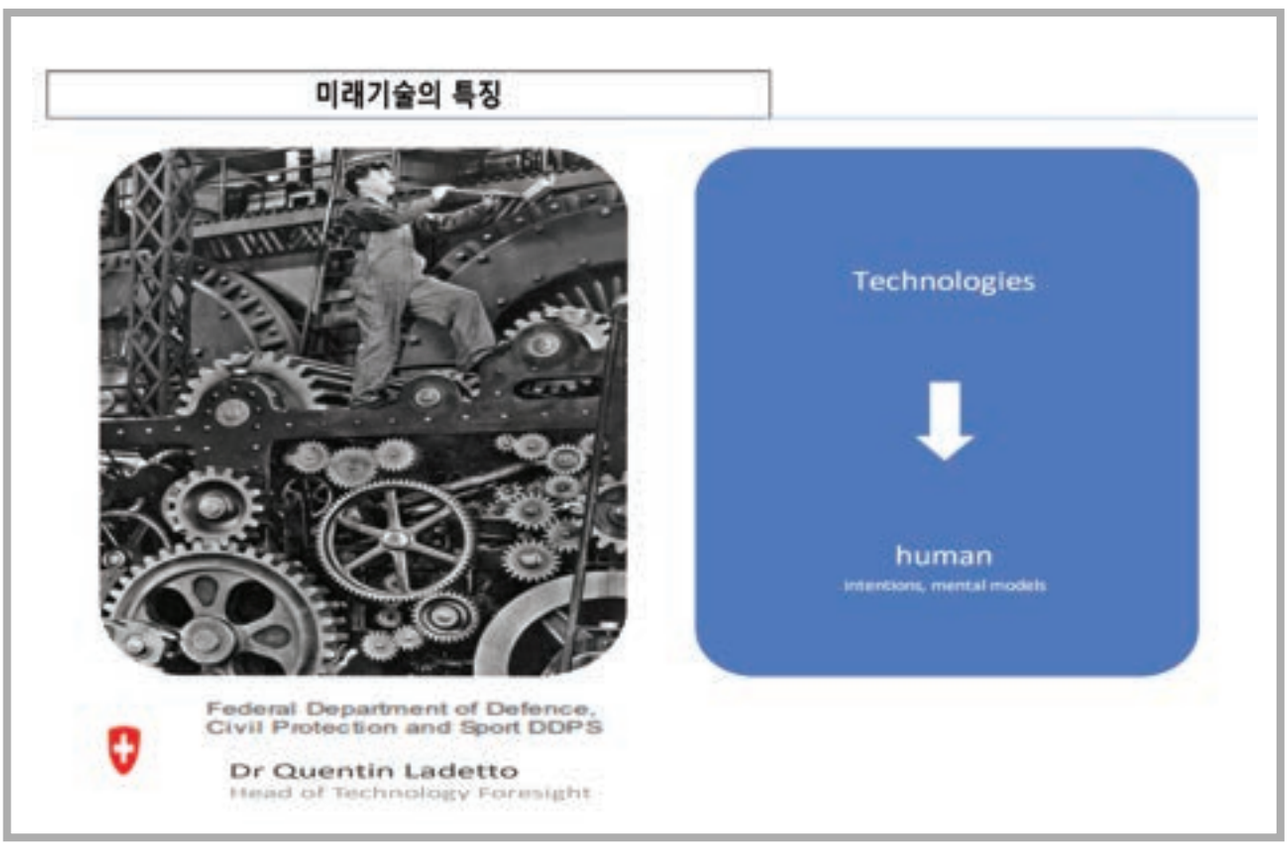
MORE CLARIFICATIONS…

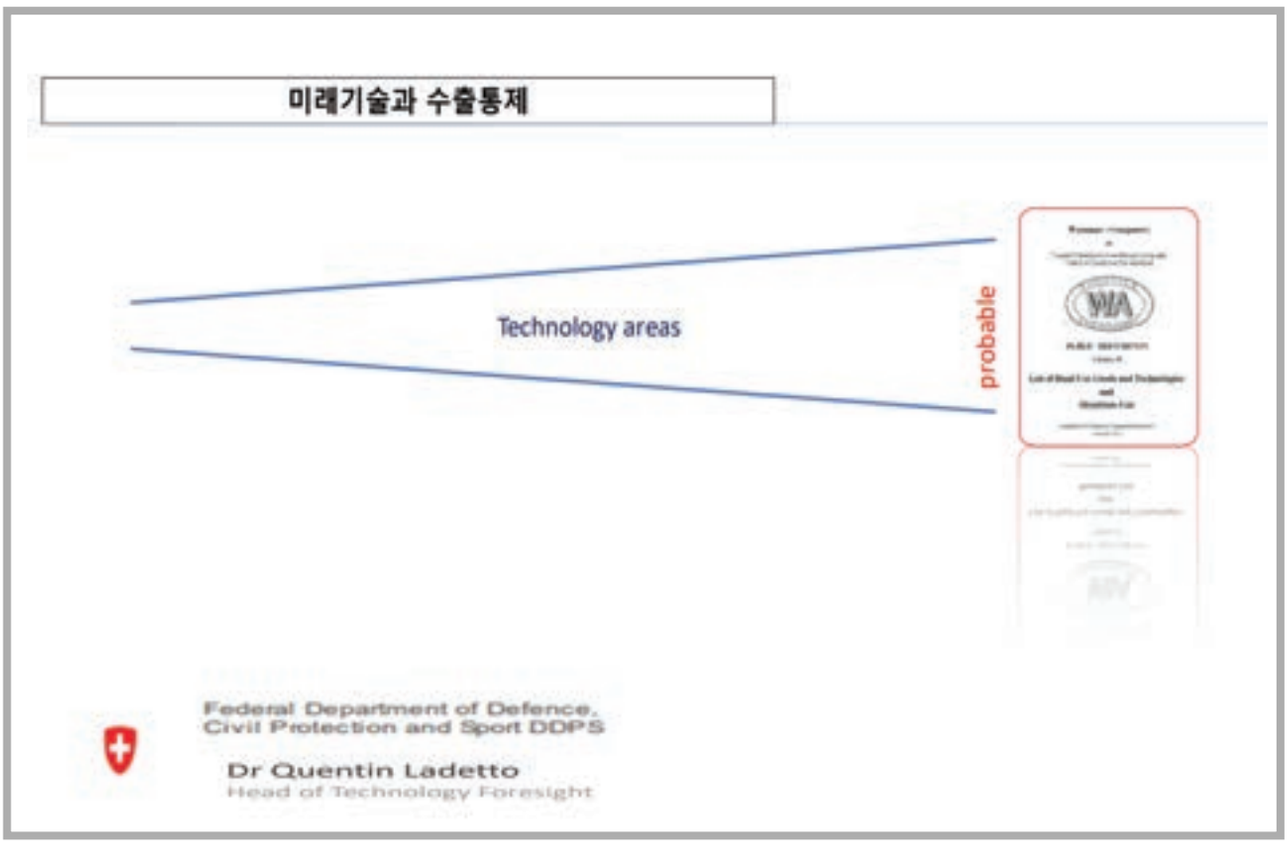
- *Comparable national standards* replaced with *equivalent standards;*
- Non-sensitive ground equipment excluded from ML 10 controls;
- *Gun-mountings* clarified;
- *Cyphering processes* replaced with *cryptographic functionality;*
- *Protective goggles* clarified.

미래기술의 특징




미래기술의 특징
Technologies
Combinations
convergence of domains
Federal Department of Defence,
Civil Protection and Sport DDPS
Dr Quentin Ladetto
Head of Technology Foresight


미래기술의 특징
Technologies
human
intentions, mental models
Federal Department of Defence,
Civil Protection and Sport DDPS
Dr Quentin Ladetto
Head of Technology Foresight


미래기술과 수출통제
Technology areas
probable
Federal Department of Defence, Civil Protection and Sport DDPS
Dr Quentin Ladetto
Head of Technology Foresight


수출통제 대상의 확대
o 신흥기술
슈퍼컴퓨팅, 양자컴퓨팅
"빅데이터" 분석
인공지능
로봇공학
초음속
생명공학

2018 미국 ECRA(Export Control Reform Act)

o **미국 내 신흥기술, 기반기술의 식별**
(Emerging & Foundational Technologies)

1. 미국의 국가안보에 중요한 기술로서(critical)
2. Defense Production Act에 정의되지 않은 것

• 2018. 11. 19 공지 후 의견 수렴

o **선정기준 및 특징**

1. 신속한 속도로 개발 및 응용되는 기술
2. 관련 민간품목과 동일한 공급망 체계를 통해 군 전용 가능 물품이 생산됨
3. 통제가 시의적절하게 적용되어야 하는 기술
   (1) 외국군 및 우려 생산자에 의한 개발 개연성 또는 관측이 공유되어야 함
   (2) 외국경쟁자의 첨단기술 평가는 어떤 통제가 합의되어야 하는지에 대해 도움이 됨
   (3) 공급망내 품목, 참가자는 다자통제전까지 논리적으로 임시통제 대상 될 수 있음

2018 미국 ECRA 14개 신흥기술 목록

(1) Biotechnology, such as:
(i) Nanobiology; (ii) Synthetic biology; (iii) Genomic and genetic engineering; (iv) Neurotech.

(2) Artificial intelligence (AI) and machine learning technology, such as: (i) Neural networks and deep learning (e.g., brain modelling, time series prediction, classification); (ii) Evolution and genetic computation(e.g., genetic algorithms, genetic programming); (iii) Reinforcement learning; (iv) Computer vision (e.g., object recognition, image understanding); (v) Expert systems (e.g., decision support systems, teaching systems); (vi) Speech and audio processing (e.g., speech recognition and production); (vii) Natural language processing (e.g., machine translation); (viii) Planning (e.g., scheduling, game playing);

(ix) Audio and video manipulation technologies (e.g., voice cloning, deep fakes); (x) AI cloud technologies; (xi) AI chipsets.

(3) Position, Navigation, and Timing(PNT) technology.

(4) Microprocessor technology, such as:
(i) Systems-on-Chip (SoC); (ii) Stacked Memory on Chip.

(5) Advanced computing technology, such as:
(i) Memory-centric logic.

(6) Data analytics technology, such as:
(i) Visualization; (ii) Automated analysis algorithms;
(iii) Context-aware computing

(7) Quantum information and sensing technology, such as (i) Quantum computing; (ii) Quantum encryption;
(iii) Quantum sensing.

2018 미국 ECRA 14개 신흥기술 목록

(8) Logistics technology, such as: (i) Mobile electric power; (ii) Modeling and simulation; (iii) Total asset visibility; (iv) Distribution-based Logistics Systems (DBLS).	**(12) Hypersonics,** such as: (i) Flight control algorithms; (ii) Propulsion technologies; (iii) Thermal protection systems; (iv) Specialized materials (for structures, sensors, etc.).
(9) Additive manufacturing (e.g., 3D printing);	**(13) Advanced Materials,** such as:
(10) Robotics such as: (i) Micro-drone and micro-robotic systems; (ii) Swarming technology; (iii) Self-assembling robots; (iv) Molecular robotics; (v) Robot compliers; (vi) Smart Dust.	(i) Adaptive camouflage; (ii) Functional textiles (e.g., advanced fiber and fabric technology); (iii) Biomaterials.
(11) Brain-computer interfaces, such as (i) Neural-controlled interfaces; (ii) Mind-machine interfaces; (iii) Direct neural interfaces; (iv) Brain-machine interfaces.	**(14) Advanced surveillance technologies**, such as: Faceprint and voiceprint

스위스 미래 관심 기술

12 technology domains of interest **for Switzerland**

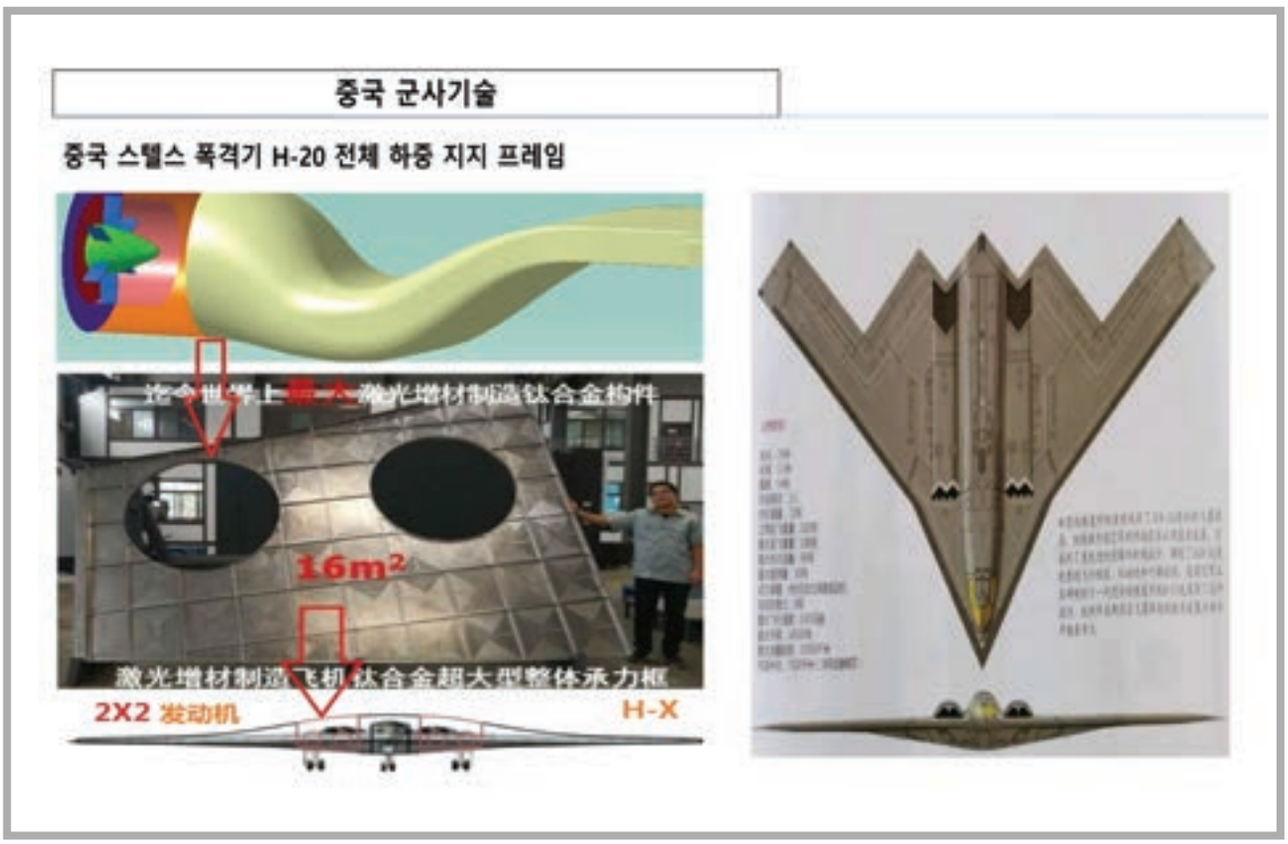
- #IOT
- #Robotics
- #HumanPerformance
- #NewMaterials
- #AdditiveManufacturing
- #SpaceTechnologies
- #AI
- #Augmented/VirtualReality
- #SyntheticBiology
- #Quantum
- #HypersonicMissiles/Vectors
- #ElectromagneticSpectrum

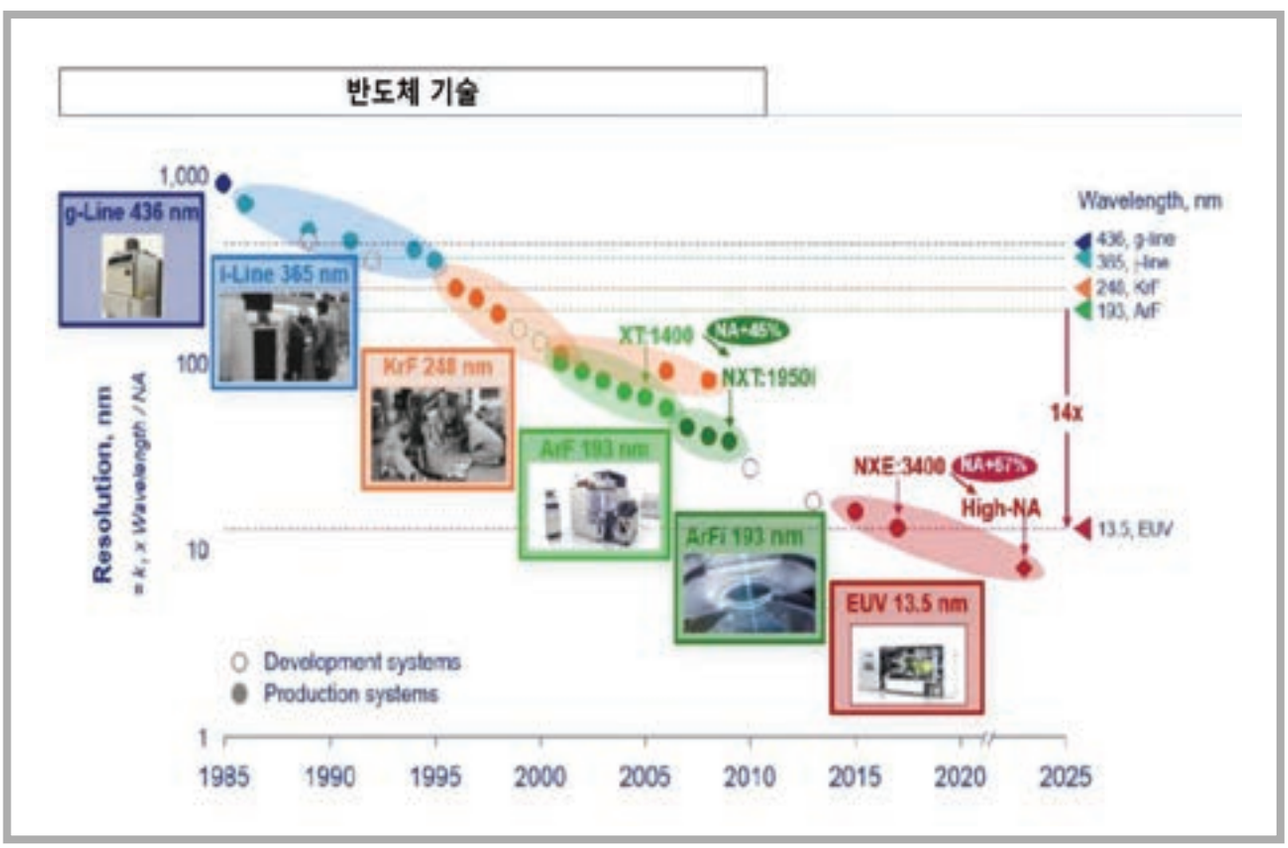
중국 군사기술

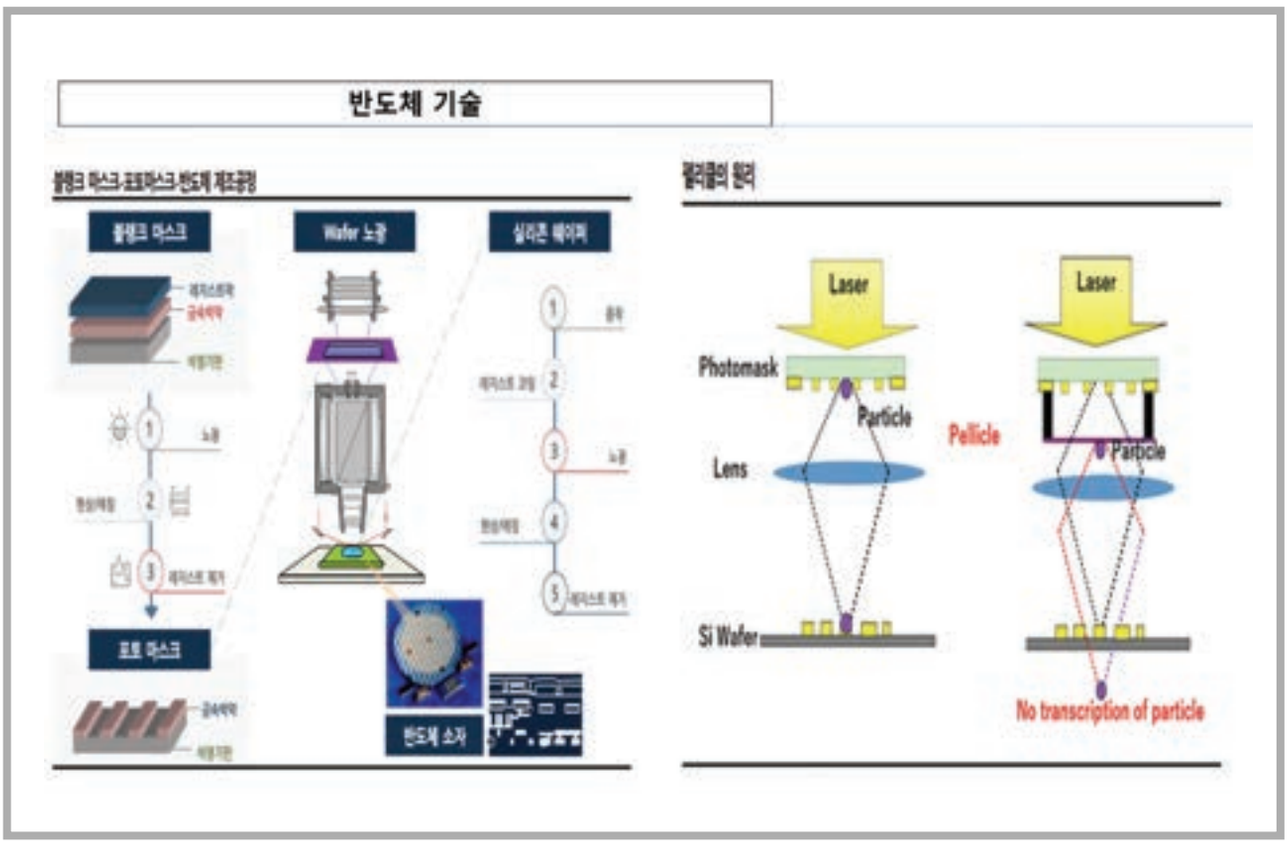
< 중국 전자기술그룹, 병기공업그룹의 전자전 장비 >

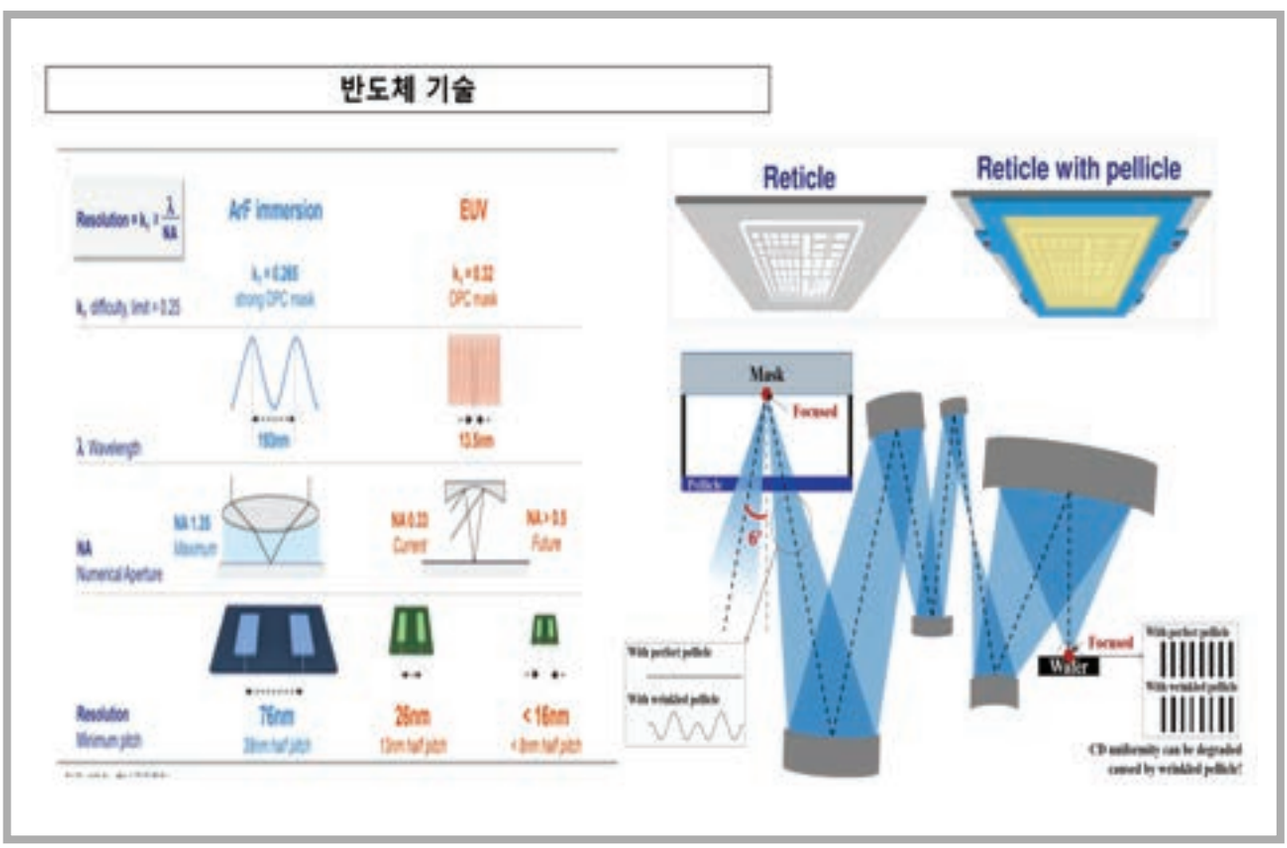
중국 군사기술

중국 스텔스 전투기 J-31 및 관련 엔진 후부지지 프레임


중국 군사기술
중국 스텔스 폭격기 H-20 전체 하중 지지 프레임
16m²
2X2 发动机
H-X


반도체 기술
g-Line 436 nm
i-Line 365 nm
KrF 248 nm
ArF 193 nm
ArFi 193 nm
EUV 13.5 nm
XT:1400
NA+45%
NXT:1950i
NXE:3400
NA+67%
High-NA
14x
Wavelength, nm
436, g-line
365, i-line
248, KrF
193, ArF
13.5, EUV
Resolution, nm
= k1 x Wavelength / NA
1,000
100
10
1
Development systems
Production systems
1985
1990
1995
2000
2005
2010
2015
2020
2025


반도체 기술
블랭크 마스크
Wafer 노광
실리콘 웨이퍼
포토 마스크
반도체 소자
펠리클의 원리
Laser
Photomask
Particle
Lens
Si Wafer
Laser
Pellicle
Particle
No transcription of particle


반도체 기술
ArF immersion
EUV
λ Wavelength
NA
Numerical Aperture
Resolution
Reticle
Reticle with pellicle
Mask
Focused
Pellicle
Wafer

수출통제 안건 사례

3B001.f Lithography equipment as follows:
1. a. A light source wavelength equal to or shorter than 193 nm; or b. Capable of ... a pattern with ...MRF of 45 nm or ...;
Technical Note:
The 'Minimum Resolvable Feature size' (MRF) is calculated by the following formula:
MRF = {(light source wavelength in nm) × (K factor)} / maximum numerical aperture, where K factor = ~~0.35~~ 0.25

3B001.f 리소그래피(lithography) 장비로서 ...
1. a. 광원의 파장이 193 nm 미만인 것; 또는
b. '최소 분해 선폭'(MRF)이 45 nm 이하인 패턴을 생성할 수 있는 것;
기술해설:
'최소 분해 선폭'(MRF)은 다음 공식에 의해 계산된다.
MRF = {(노출광원파장(nm)) × (K factor)} / 개구수(numerical aperture(NA)) 여기에서, K factor = 0.35

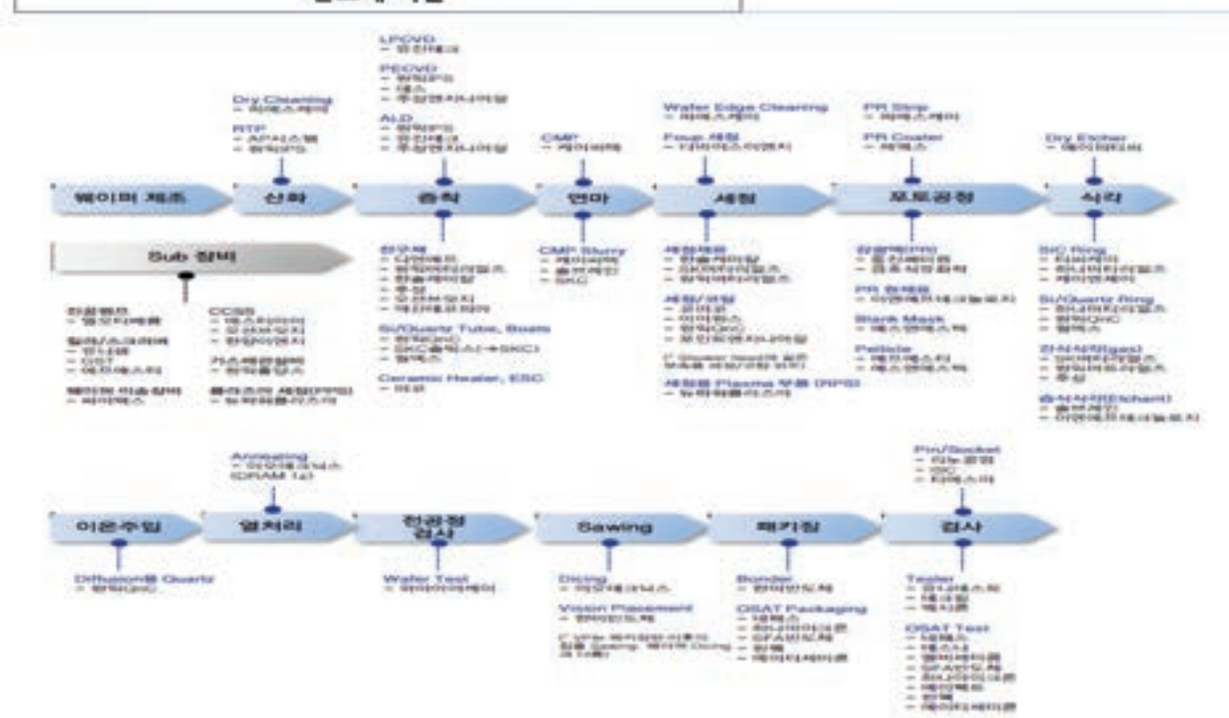
3B001.g Masks and reticles, designed for integrated circuits specified in 3A001; 'EUV' masks and reticles

3B001.g 3A001에 해당하는 집적회로를 위해 설계된 마스크 또는 망선(reticles)

3C002.a Resists designed for semiconductor lithography as follows: 1. Positive resists adjusted (optimised) for use at wavelengths less than 193 nm but equal to or greater than 15 nm; ...

3C002.a 반도체 리소그래피를 위해 설계된 레지스트로써 다음 중 하나의 것:
1. 15 nm 이상 193 nm 보다 작은 파장에서 사용할 수 있도록 최적화된 양성 레지스트 ...

반도체 기술



미국 독자수출통제

- 미국 고유 통제기준

3B991 Equipment not controlled by 3B001 for the manufacture of electronic "parts," "components" and materials, and "specially designed" "parts," "components" and "accessories" therefor.

License Requirements, Reason for Control: AT

b. Equipment "specially designed" for the manufacture of semiconductor devices, integrated circuits and "electronic assemblies", as follows, and systems incorporating or having the characteristics of such equipment:

미국 독자수출통제

- 미국 고유 통제기준

b.1.h. "Stored program controlled" equipment for the selective removal (etching) by means of anisotropic dry methods (e.g., plasma), as follows:

b.1.h.1. Batch types having either of the following:

b.1.h.1.a. End-point detection, other than optical emission spectroscopy types; or

b.1.h.1.b. Reactor operational (etching) pressure of 26.66 Pa or less;

미국 독자수출통제

➢ **10월 7일 BIS EAR 개정**

❶ 반도체 ※ 10.21일부터 발효

- **특정사양(연산능력 300TFLOPS,** 데이터 입출력속도 **600GB/S** 이상)의 **첨단 컴퓨팅 칩**
  - 제3국에서 생산된 고사양 GPU 등도 허가 없이 중국 수출 불가
- **특정사양(연산능력 100PFLOPS** 이상)의 **수퍼컴퓨터에 최종사용되는 모든 제품**
  - 제3국에서 생산된 제품도 수퍼컴퓨터 개발·생산 목적이면 허가 필요
- **美 우려거래자(Entity List)**에 등재된 **중국의 28개 반도체·수퍼컴퓨터** 관련 기업에 수출되는 모든 제품
  - 제3국에서 특정 사양의 기술·SW·장비로 만든 제품도 허가 필요

※ 상기 3개 품목은 거부추정 원칙이 적용되어, 허가 가능성 낮음

미국 독자수출통제

➢ **10월 7일 BIS EAR 개정**

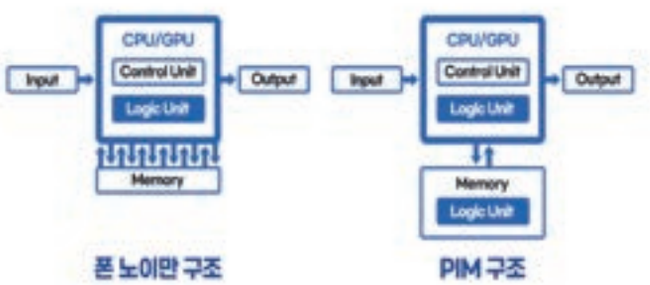
❷ 반도체 장비 ※ 10.7일부터 발효

- 다음 기준을 충족하는 **반도체 생산목적**인 경우, **장비를 포함하여 모든 미국 수출통제 품목은 허가 없이 중국 수출 불가**
  - 로직칩 : **FinFET** 구조 또는 **16/14nm** 이하
  - D램 : **18nm** 이하
  - 낸드 : **128단** 이상
- 새로이 통제대상에 편입된 **고사양 '증착장비'도 수출제한**
- **중국 기업에는 원칙적으로 허가가 거부(presumption of denial)**되는 한편, 우리 기업과 같이 **중국 내 다국적 기업에는 사안별 심사(case-by-case review)**를 통해 허가 발급

미국 독자수출통제

[PIM 기술 개념도]

PIM(Processing-in-Memory)은 메모리 내부에
연산 작업에 필요한 프로세서 기능을 더한 차세대 신개념 융합기술



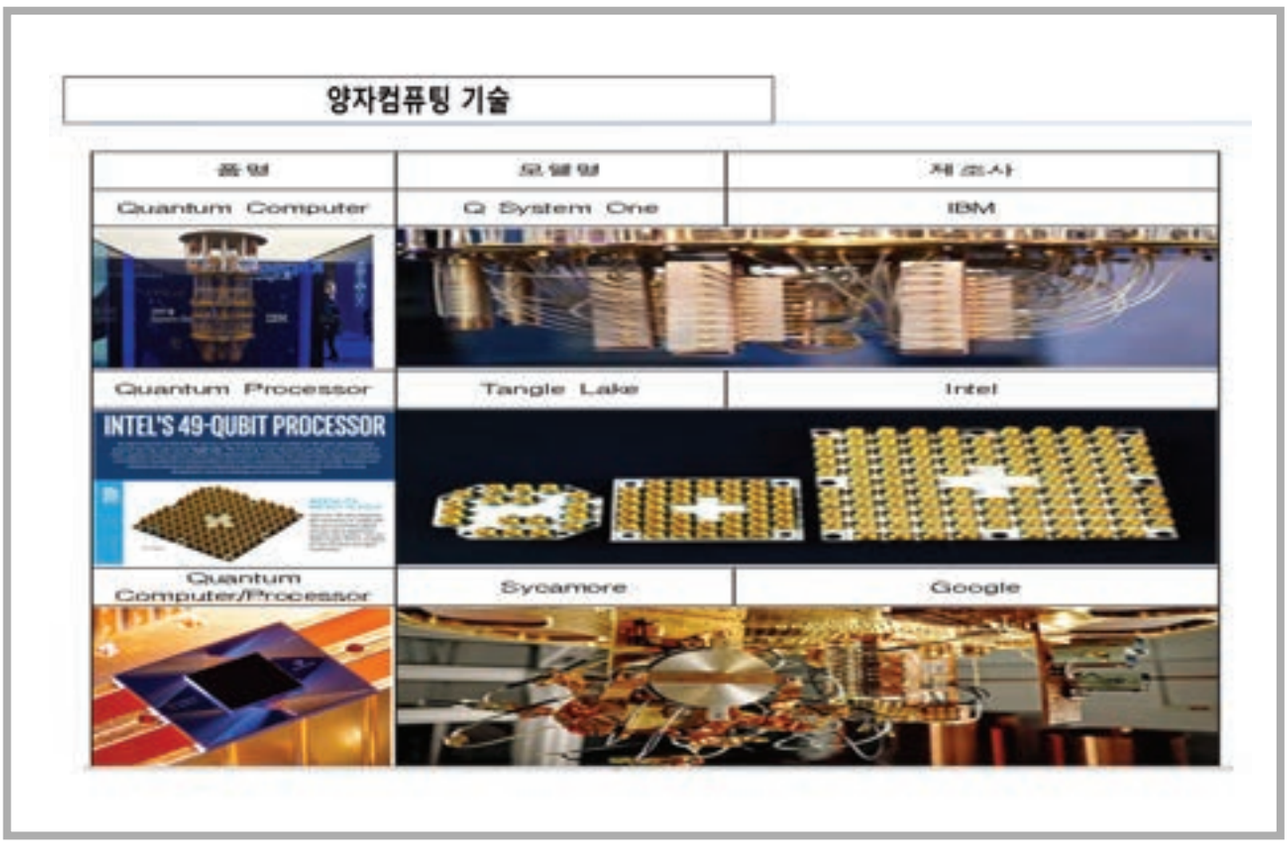
폰 노이만 구조 PIM 구조

*Control Unit : 제어부 *Logic Unit : 연산부

< 삼성전자 PIM(Processing-in-Memory) >

미국 독자수출통제

< 하이닉스 HBM3(고대역 메모리(High Bandwidth Memory, HBM) >


양자컴퓨팅 기술
품명
모델명
제조사
Quantum Computer
Q System One
IBM
Quantum Processor
Tangle Lake
Intel
INTEL'S 49-QUBIT PROCESSOR
Quantum Computer/Processor
Sycamore
Google


양자컴퓨터
양자, 나노와 디지털을 넘어
양자물리학:
물질의 궁극적 원리 → 궁극적 기술
20세기 정보통신기술
양자물리학
정보이론
소프트웨어/운영체제
양자정보과학
21세기 정보통신기술
양자물리학→하드웨어, 소프트웨어, 운영체제에 적극적으로 이용
→ 양자컴퓨터 / 양자암호 / 양자센서, 양자계측, 양자이미징
* 고등과학원 김재완 부원장님 자료참조
2022 노벨물리학상
Alain Aspect
John F. Clauser
Anton Zeilinger
얽힌 광자 실험으로 벨 부등식이 위배됨을 보이고,
양자정보과학을 개척한 공로
2012 노벨물리학상
Haroche
Wineland
단일 양자계를 조작하고 측정한 공로 → 양자정보연구에 공헌

▸ 양자컴퓨터

o 미국은 200 큐비트 이상 컴퓨터에서 현재는 34 큐비트 이상 컴퓨터를 전략물자로 지정* 제안
현재 국제수준에서 가장 인접한 2개의 물리적 큐비트의 Controlled Not Gate에 일어나는 Average Error를 'CNOT 에러'로 정의하고 있는데 의미는?

* 전략물자 지정요건이 단순한 큐비트 숫자로 결정되는 것이 아닌 Fully Controlled, Connected, Working, Physical 등 여러가지 조건을 동시에 만족하면서 34 큐비트 이상

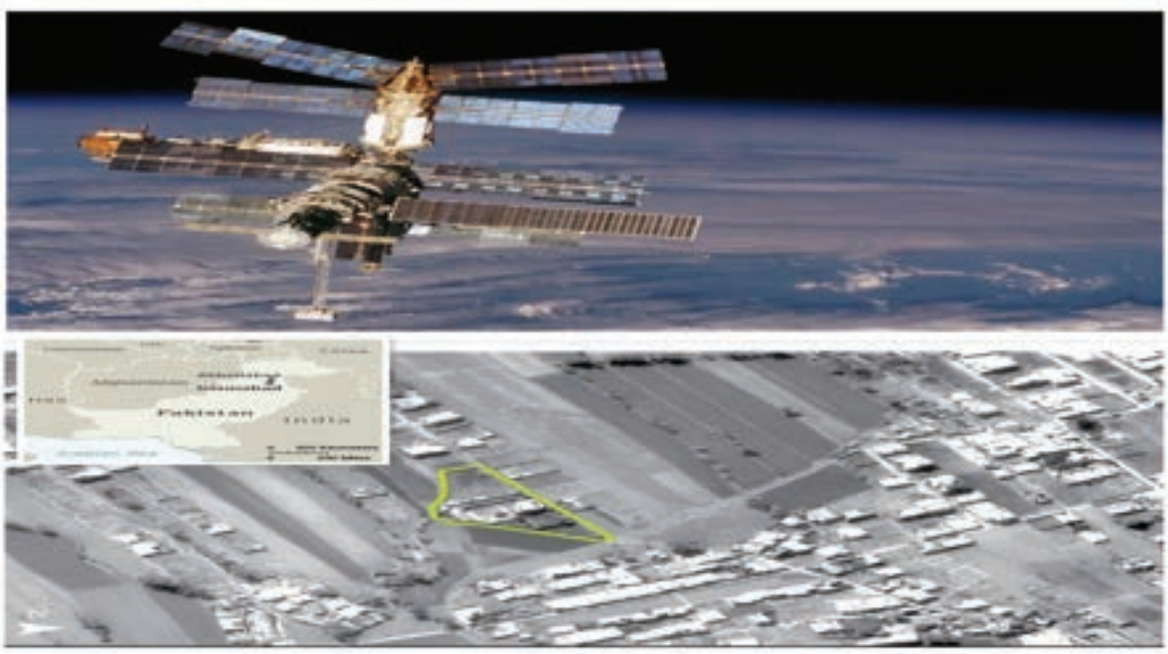
- 양자컴퓨터에서는 큐비트들의 조작을 통해 계산을 하는데, 큐비트 하나를 조작하는 싱글큐비트 게이트 여러 종류와 이외에, 큐비트 두 개를 한꺼번에 조작하는 Two-qubit gate들 중 하나는 꼭 필요

※ 두 큐비트 게이트들 중 대표적인 것이 CNOT gate이고, 두 큐비트 게이트로는 이것 하나만 있어도 충분. 두 큐비트 게이트로 조작할 큐비트 두 개 중 하나를 제어 큐비트(control qubit), 나머지 하나를 대상 큐비트(target qubit)라고 호칭

- 제어 큐비트의 상태가 0일 때에는 대상 큐비트의 상태를 그대로 두고, 제어 큐비트의 상태가 1일 때에는 대상 큐비트에 NOT 연산. 그래서 이를 제어형 NOT 게이트 (Controlled-NOT gate) 또는 CNOT gate라고 호칭
그런데, 두 큐비트 게이트는 일반적으로 싱글 큐비트 게이트보다 어렵고 오류가 생길 확률도 높음

※ 미국 IBM에서 송도 연세대에 양자컴퓨팅 도입하였지만, 서비스용(기술개발 등에 대해서는 전혀 오픈하지 않는 게 원칙. 독일에도 IBM 양자컴퓨팅이 있지만, 외부인에 대해 사용목적 이외 접근을 엄격하게 금지)

인공지능 딥러닝 기술



수출통제 안건 사례

"Software" specially designed or modified for training a deep learning model to automate ...

a. Providing a graphical user interface ...

b. Performing ...

c. Training a deep learning model to detect ...

딥러닝 모델을 교육하기 위해 특별히 설계되거나 수정되어 공중 또는 위성 소스의 이미지 ...

1. 그래픽 사용자 인터페이스 제공 ...

2. ... 수행

3. 딥러닝 모델 훈련 ...

연구내용

MQ-9 Reaper(Predator B)

➢ <최신동향 사례> MTCR 부속서 Caregory Ⅰ, Ⅱ 관련논의

□ Cat Ⅰ : 사거리 300km 이상·탑재중량 500kg 이상 미사일 완제품 및 부분품

- 탄도미사일(ballistic missile)·우주발사체(space launch vehicle)·관측로켓(sounding rocket) 등 로켓 시스템과 순항미사일(cruise missile)·표적기(target drone)·무인정찰기(reconnaissance drone)등 무인비행체 시스템
- 로켓 단·재진입체·엔진 등 상기 부분품, 생산시설 -> WMD 운반과 직접 관계있는 장비·기술

* 허가지침 : 수출국의 사전동의 없이 개조, 복제, 재수출 금지 ("강한 거부추정")
  - 신고용도 외 미사용 + 수입국 정부 보증(허가없이 제3자 미이전), 예외적 수출가능
  (단, Category Ⅰ 품목 생산시설 이전금지, WMD 운반목적 Category Ⅱ 품목은 Category Ⅰ 품목과 동일)

□ Cat Ⅱ : 상기 미사일 부품·기술, 사거리 300km 이상 · 탑재중량 500kg 미만 미사일

- 추진제·구조용 복합재·항법장치·비행제어장치·항공전자장비·발사지원 장비·시설 · 시험장비 · 탐지최소화(stealth) 기술 등 Category Ⅰ 품목에 사용되는 이중용도 부품, 장비 및 기술
- 미사일, 로켓, UAV -> WMD 운반과 직접 관계없는 장비·기술

연구내용

- <최신동향 사례> **NSG, WA** 적층가공기계 관련논의

1.B.8 Additive Manufacturing Machines with all the following characteristics:

a. having a controlled atmosphere ...

b. using a ...

미국 오크리지 국립연구소
원자로 핵심설계 연구개발프로젝트
(노심 시제품 출시)

영국 세필스대 첨단제조기술연구센터(AMRC)
소형모듈원자로(SMR) 주요부품 생산기술
(압력용기 제작 3년 -> 6개월 단축)

결론

o **국제체제 수출통제범위가 무기관련 품목에서 일반품목으로 확대될 것으로 예상**

- 반도체, 인공지능, 기타 정보기술은 거의 모든 무기와 일반제품에 적용 전망
- 안건별 다자, 소다자, 양자 협의 형태의 복합적 협상 예상
- 국제체제 대응과 국가 R&D, 산업 육성 전략 연계 필요

o **향후 첨단기술 확보 및 보호 능력이 국가 경제 및 안보의 지속가능성 결정**

- 전 세계 수출 경쟁 격화 및 공급망 이슈 부각
- 군사 및 상업용 기술의 획기적 발전과 융복합 예상
- 원천기술 확보 및 관리 능력이 미래의 국가안보(National Security) 좌우

Q & A

'23 Defense Technology Security Conference

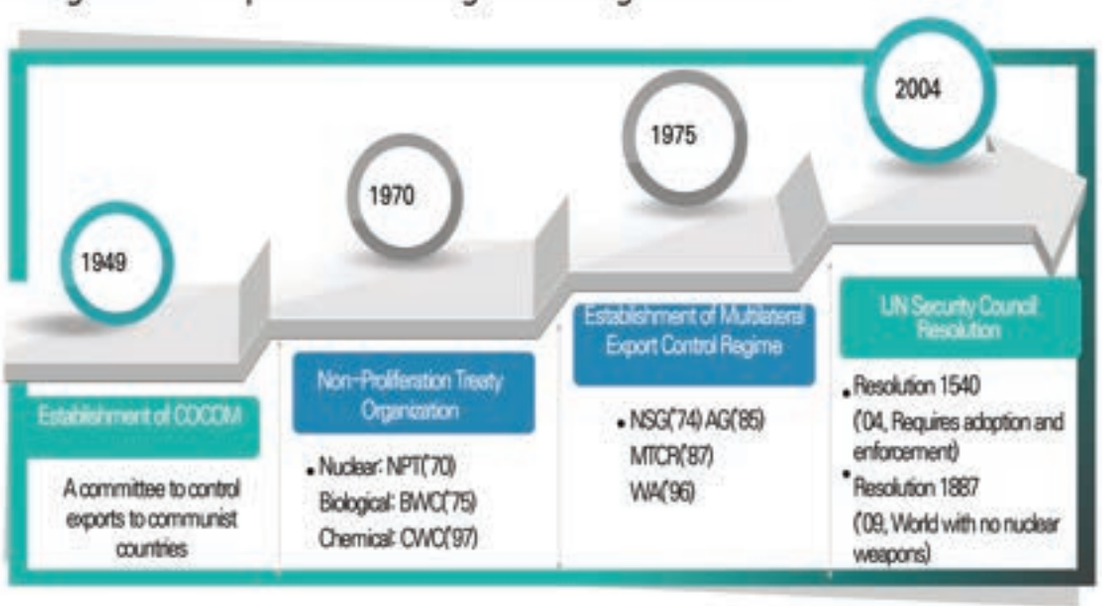
Trends in International Export Control Regimes and Implications for Technology Protection

Sehee Ryu
Director, Multilateral Export Controls Team
KOSTI
+82-2-6000-6380
shryu@kosti.or.kr

kosti

History of International Export Control Regimes

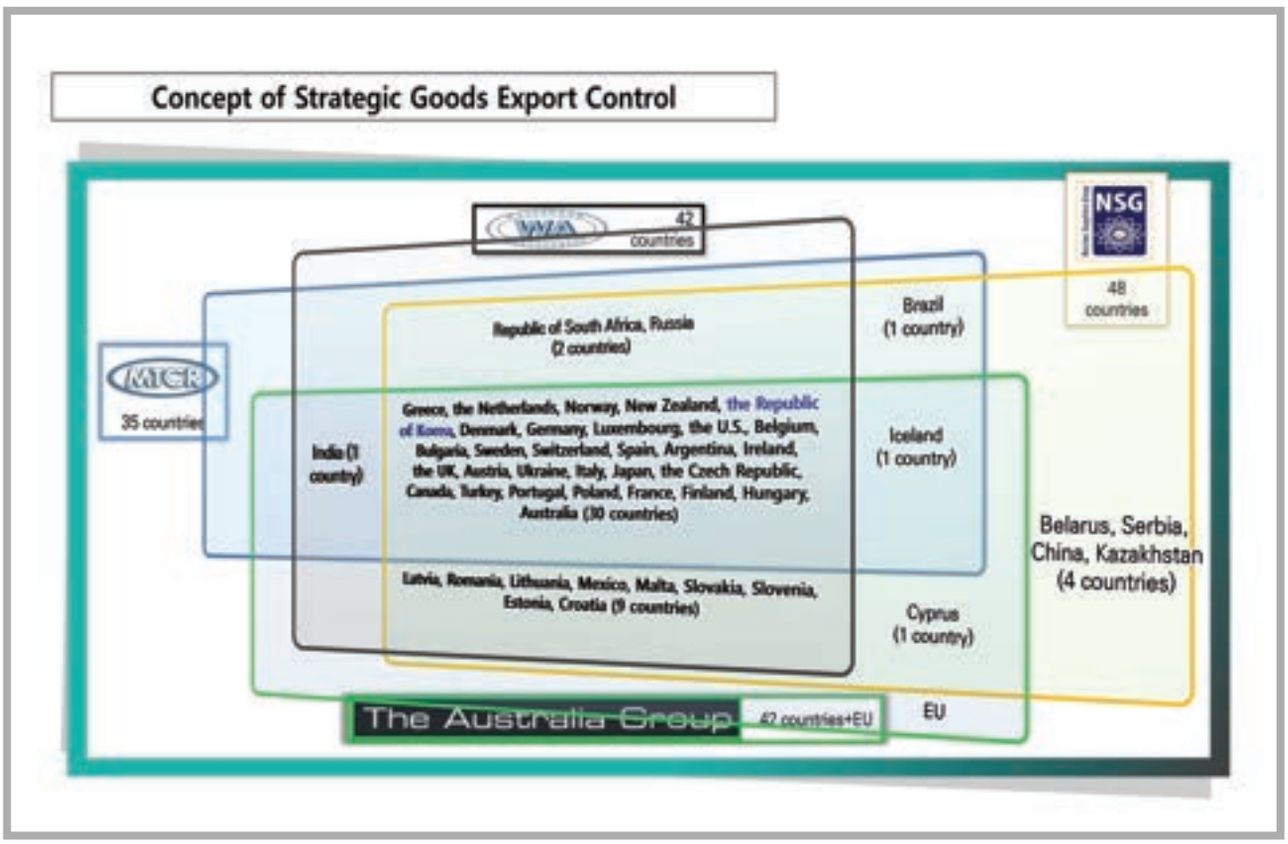
o Changes in the Export Control Regime through the Years



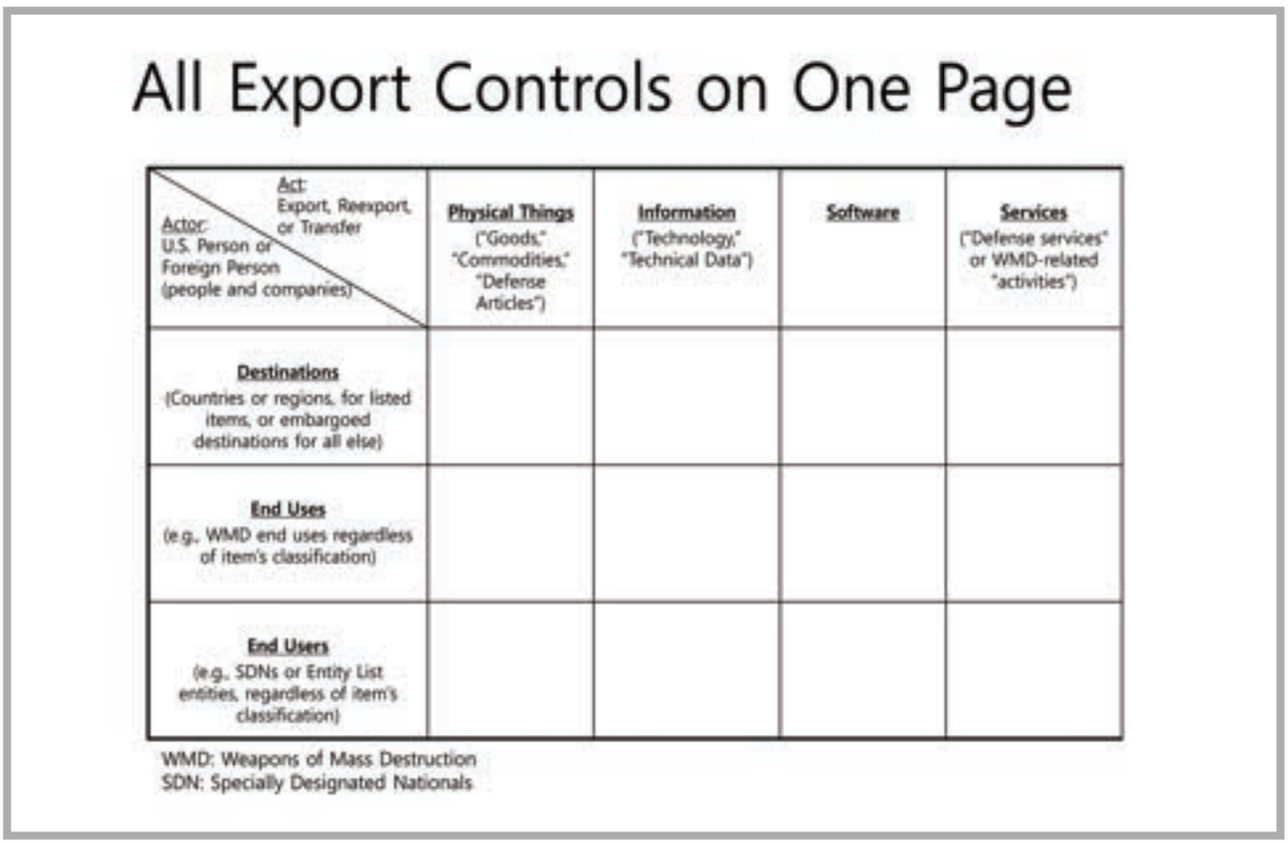
History of the International Export Control Regime

Classification	International Export Control Regime				Non-Proliferation Treaty	
	Wassenaar Arrangement	Nuclear Suppliers Group	Missile Technology Control Regime	Australia Group	Chemical Weapons Convention	Biological Weapons Convention
Established	1996	1978	1987	1985	1997	1975
Member States	42	48	35	43	193	174
Korea's Join	1996	1995	2001	1996	1997	1987
Subjects of Control	Conventional arms (firearms, gunpowder) and dual-use items (materials, machines, electrons, chemicals)	Nuclear dedicated items and dual-use items (centrifuge, etc.)	Missile-related items (missiles, rockets, navigation equipment, etc.)	Raw materials and manufacturing equipment for biochemical weapons (virus, toxins, etc.)	Schedule 1, 2, 3 toxic chemicals and raw materials	No internationally stipulated items; but 67 biotic agents are stipulated in the domestic Chemical Weapons Prohibition Act

Concept of Strategic Goods Export Control


Concept of Strategic Goods Export Control
WA
42 countries
NSG
48 countries
MTCR
35 countries
Republic of South Africa, Russia (2 countries)
Brazil (1 country)
India (1 country)
Greece, the Netherlands, Norway, New Zealand, the Republic of Korea, Denmark, Germany, Luxembourg, the U.S., Belgium, Bulgaria, Sweden, Switzerland, Spain, Argentina, Ireland, the UK, Austria, Ukraine, Italy, Japan, the Czech Republic, Canada, Turkey, Portugal, Poland, France, Finland, Hungary, Australia (30 countries)
Iceland (1 country)
Belarus, Serbia, China, Kazakhstan (4 countries)
Latvia, Romania, Lithuania, Mexico, Malta, Slovakia, Slovenia, Estonia, Croatia (9 countries)
Cyprus (1 country)
The Australia Group
42 countries+EU
EU

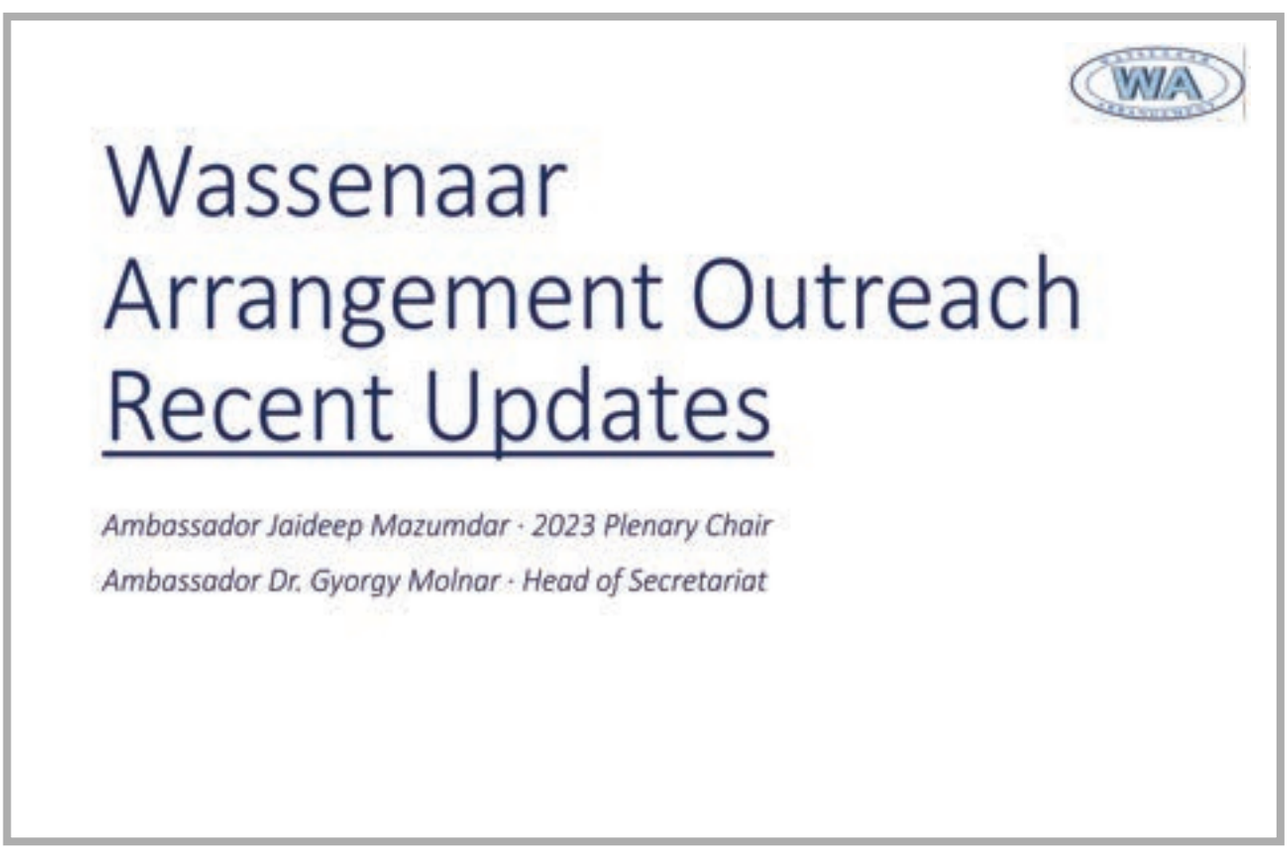

Basics of Export Control
- By US Kevin Wolf (kwolf@akingump.com)
• Export control refers to norms that regulate the following:
• 1. Exports, re-exports, and transfers by citizens and foreign ers
• 2. to destinations, end uses, end users
• 3. of goods, technologies, software, and services
• 4. to achieve diverse national security and foreign policy objectives



All Export Controls on One Page

Act: Export, Reexport, or Transfer / Actor: U.S. Person or Foreign Person (people and companies)	**Physical Things** ("Goods," "Commodities," "Defense Articles")	**Information** ("Technology," "Technical Data")	**Software**	**Services** ("Defense services" or WMD-related "activities")
Destinations (Countries or regions, for listed items, or embargoed destinations for all else)				
End Uses (e.g., WMD end uses regardless of item's classification)				
End Users (e.g., SDNs or Entity List entities, regardless of item's classification)				

WMD: Weapons of Mass Destruction
SDN: Specially Designated Nationals



Wassenaar Arrangement Outreach
Recent Updates

Ambassador Jaideep Mazumdar · 2023 Plenary Chair

Ambassador Dr. Gyorgy Molnar · Head of Secretariat

Purposes

Participating States seek to contribute to regional and international security and stability by promoting:

- transparency and
- greater responsibility

in transfers of **Conventional Arms** and **Dual-Use Goods & Technologies**, thus preventing:

- destabilising accumulations and
- acquisition by terrorists


WA Control Lists
Munitions List
• 22 Categories
• 300 entries
Dual-Use List
• 9 Categories
• Over 1,000 entries
• Sensitive List


List Review Process
Market Trends
Developments in International Security
List Review
Advances in Technology

The Munitions List

Only one criterion:
the military characteristics.

Concept of
"Specially designed or modified for military use"

The Dual-Use List

Dual Use Goods and Technologies are intended for
Civil-use applications
They can also be used for military applications

Because WA does not seek to impede bona fide civil transactions, by using generic parameters which would capture civil market goods

Criteria are **multiple and complex**

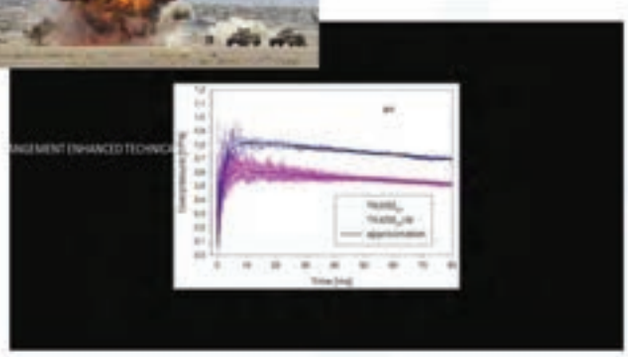
Annex E

LIST CHANGES 2018-2022
Categories 1, 2, 7, 8, 9.

Enhanced Technical Briefing 19 June 2023

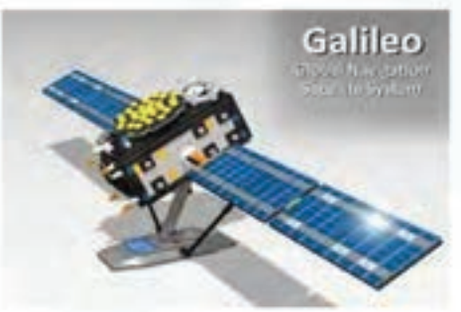
Changes to Categories 1, 2, 7, 8, 9.

CAT 1 List "EXPLOSIVES". EDNA and TKX-50 added to the list.



Changes to Categories 1, 2, 7, 8, 9.

7.A. *Satellite Navigation Systems* replace *Global Navigation Satellite Systems*



Changes to Categories 1, 2, 7, 8, 9.

8.A.2.o.4. Permanent Magnet, including Rim-Driven, propulsion

Changes to Categories 1, 2, 7, 8, 9.

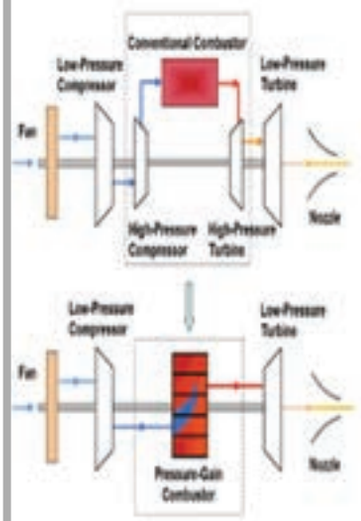
9.A.4.h. Sub-orbital craft.

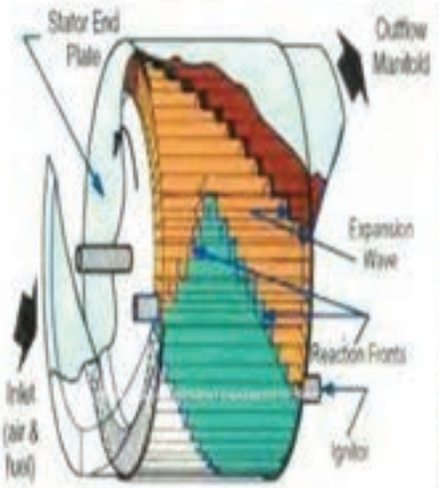
Changes to Categories 1, 2, 7, 8, 9.

9.A.4.g. Aircraft specially designed or modified to be Air-launch Platforms for space launch vehicles or sub-orbital craft.

Changes to Categories 1, 2, 7, 8, 9.

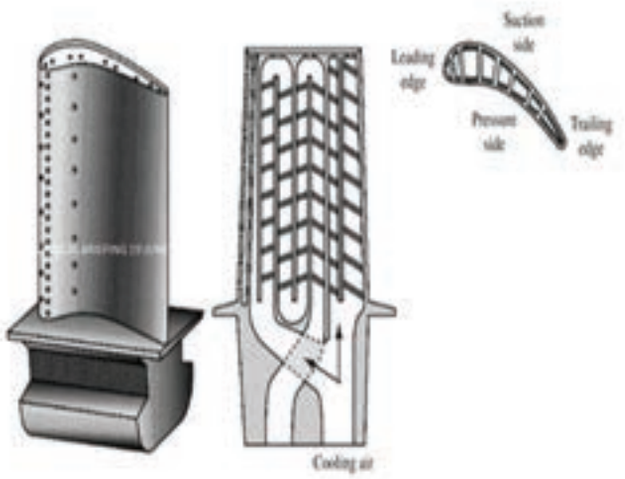
9.E.3.a.2.e. Pressure Gain Combustion





Changes to Categories 1, 2, 7, 8, 9.

9.E.3.k. Supersonic Enabling Technology.



Annex F

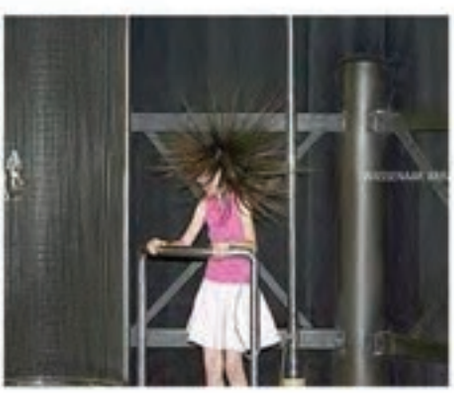
LIST CHANGES 2018-2022

Categories 3, 4, 5 Part 1, 5 Part 2, 6.

Enhanced Technical Briefing 19 June 2023

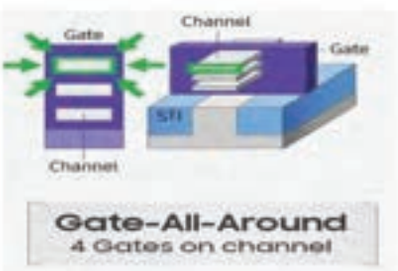
Changes to Categories 3, 4, 5 Part 1, 5 Part 2, 6.

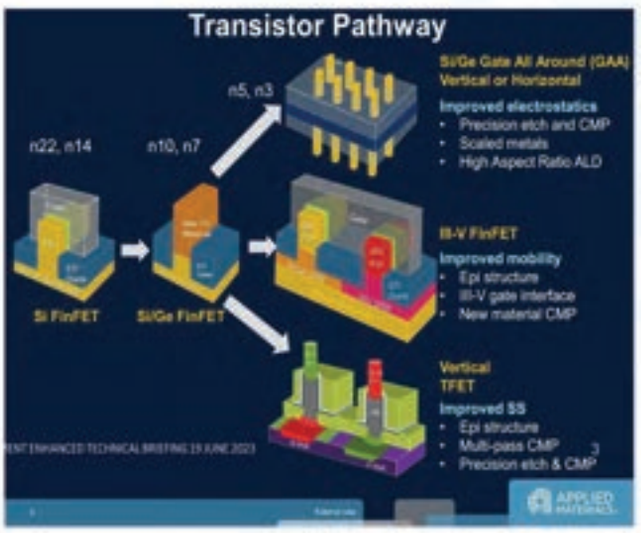
3.D.5. Software for restoring operation of microcircuits or computers after Electromagnetic Pulse (EMP) or Electrostatic Discharge (ESD)



Changes to Categories 3, 4, 5 Part 1, 5 Part 2, 6.

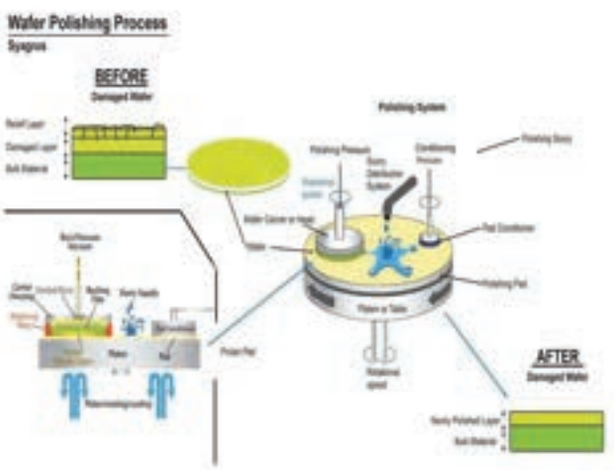
3.D.6. Electronic Computer-Aided Design (ECAD) Software for the development of Gate All-Around Field-Effect Transistor (GAAFET) circuits.

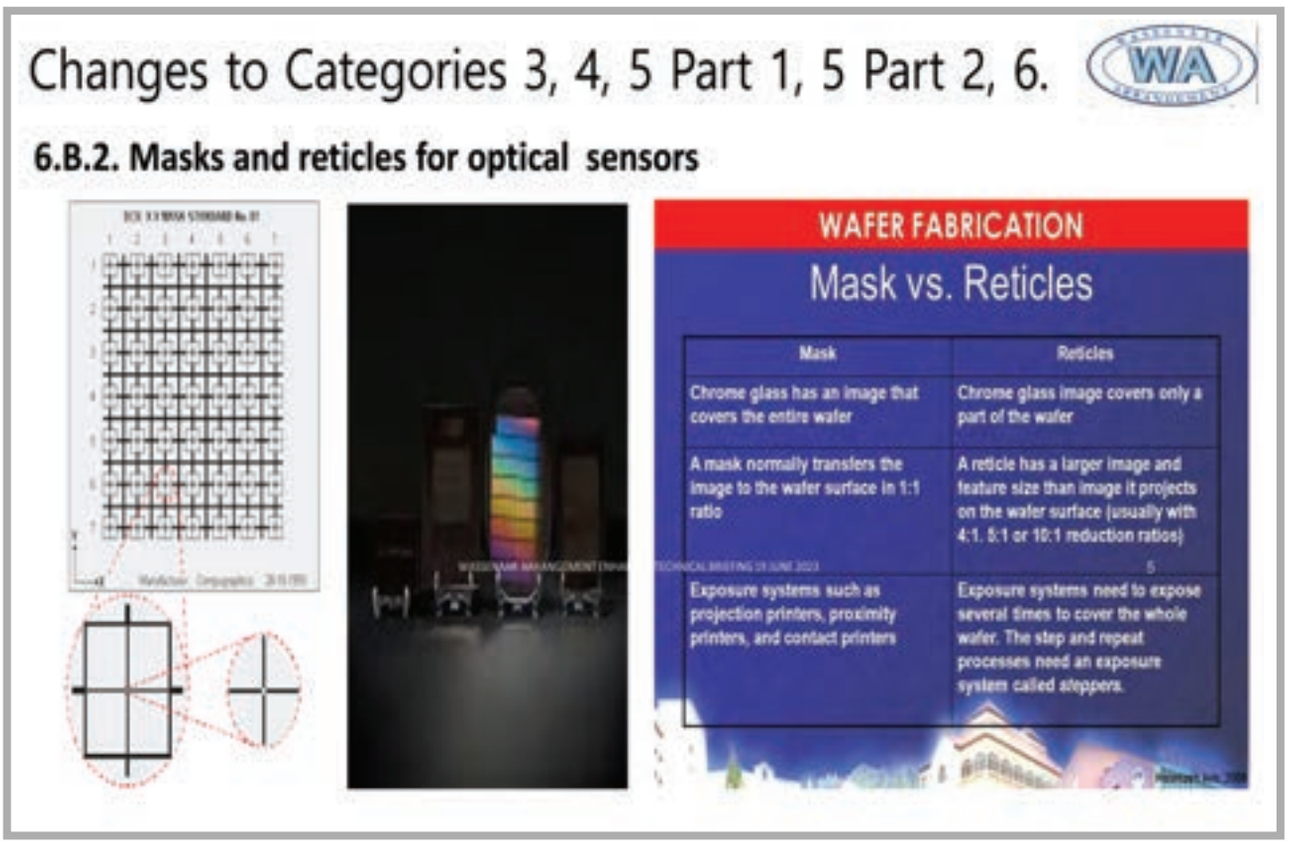


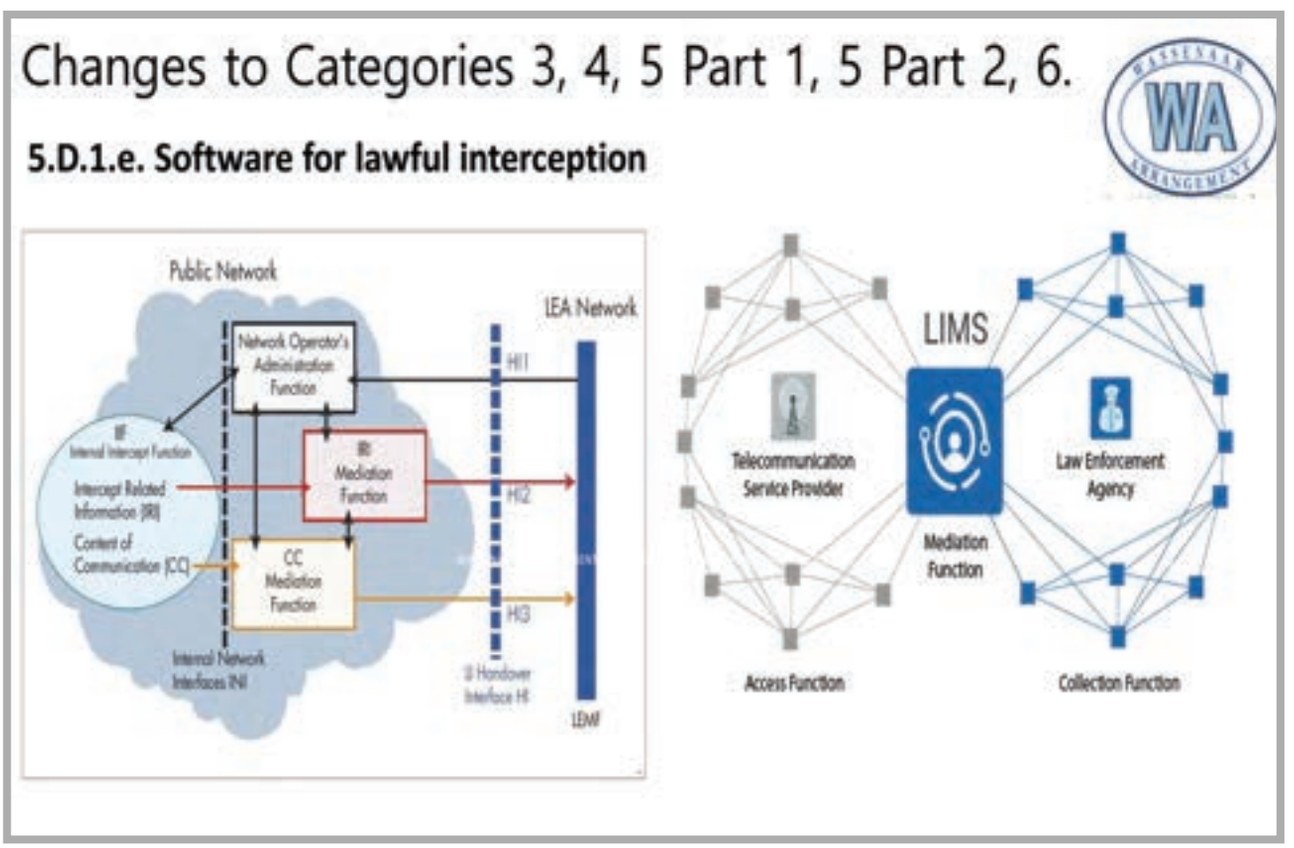


Changes to Categories 3, 4, 5 Part 1, 5 Part 2, 6.

3.E.4. Technology for high-surface quality slicing, grinding or polishing of 300 mm silicon wafers.




Changes to Categories 3, 4, 5 Part 1, 5 Part 2, 6.
6.B.2. Masks and reticles for optical sensors
WAFER FABRICATION
Mask vs. Reticles
Mask
Reticles
Chrome glass has an image that covers the entire wafer
Chrome glass image covers only a part of the wafer
A mask normally transfers the image to the wafer surface in 1:1 ratio
A reticle has a larger image and feature size than image it projects on the wafer surface (usually with 4:1, 5:1 or 10:1 reduction ratios)
Exposure systems such as projection printers, proximity printers, and contact printers
Exposure systems need to expose several times to cover the whole wafer. The step and repeat processes need an exposure system called steppers.


Changes to Categories 3, 4, 5 Part 1, 5 Part 2, 6.
5.D.1.e. Software for lawful interception
Public Network
LEA Network
Network Operator's Administration Function
Internal Intercept Function
Intercept Related Information (IRI)
Content of Communication (CC)
IRI Mediation Function
CC Mediation Function
HI1
HI2
HI3
Internal Network Interfaces INI
X Handover Interface HI
LEMF
LIMS
Telecommunication Service Provider
Mediation Function
Law Enforcement Agency
Access Function
Collection Function

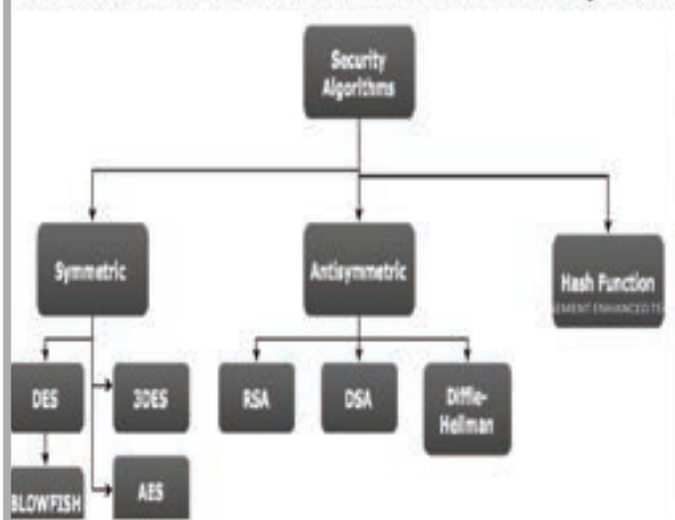
Changes to Categories 3, 4, 5 Part 1, 5 Part 2, 6.

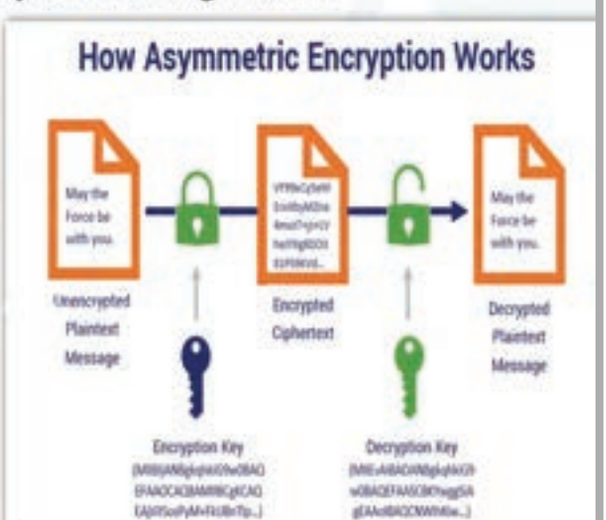
5.A.4.b. Digital Investigation (Forensic) tools

Changes to Categories 3, 4, 5 Part 1, 5 Part 2, 6.

5.A.2.a. *Described security algorithm* replaces *In excess of 56 Bits*

5.A.2.a. Technical Note 2.c. new entry for *asymmetric algorithm*





Changes to Categories 3, 4, 5 Part 1, 5 Part 2, 6.

In addition to these significant new entries, many control threshold values throughout the List have been updated to keep pace with the constant evolution of technology. This is in particular the case for :

- **Digital Computers**
- **Lasers**
- **Signal analysers, Signal generators or Frequency synthesisers**

These updates are intended to exclude from the controls items having increasing legitimate civil use and ensure that only items of strategic concern remain controlled.

Annex G

LIST CHANGES 2018-2022
Munitions List

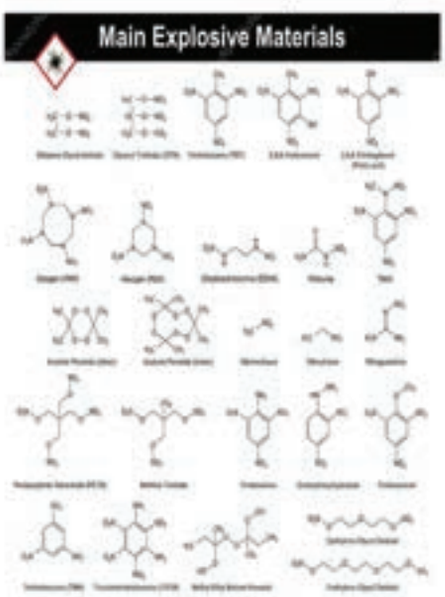
Enhanced Technical Briefing · 19 June 2023

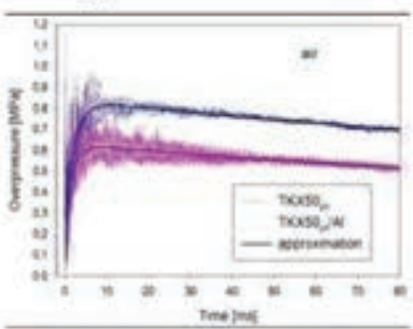
Changes to the Munitions List

The criteria for the Munitions List are more binary (specially designed/not specially designed) than the DU List. Therefore, most of the newest or most advanced weapons are already controlled under an existing item. Changes are mostly intended to clarify the list, improve its readability for exporters and licensing officers, or exclude obsolete items having no military significance.

Changes to the Munitions List

ML 8.a.43. TKX-50 explosive (new entry)





Explosives of military concern are normally added to the DU List and to the ML

ML8.a.33. "Explosives" not listed elsewhere in ML8.a. and having any of the following:
a.Detonation velocity exceeding 8,700 m/s, at maximum density, or
b.Detonation pressure exceeding 34 GPa (340 kbar);

Changes to the Munitions List

ML9.h. Nuclear power generating equipment or propulsion equipment (new entry)

The new entry completes and clarifies existing entry ML 17.g.

Changes to the Munitions List

ML13.c. Helmets and specially designed components and accessories

~~c. Helmets manufactured according to military standards or specifications, or comparable national standards, and specially designed helmet shells, liners, or comfort pads, therefor;~~

~~Note 2 ML13.c. does not apply to **conventional steel helmets**, neither modified or designed to accept, nor equipped with any type of accessory device.~~

c. Helmets and specially designed components and accessories therefor, as follows:

1.Helmets manufactured according to military standards or specifications, or comparable national standards;

2.Shells, liners, or comfort pads, specially designed for helmets specified in ML13.c.1.;

3.Add-on ballistic protection elements, specially designed for helmets specified in ML13.c.1.

The new text clarifies the status of components and accessories sometimes exported separately.

Changes to the Munitions List

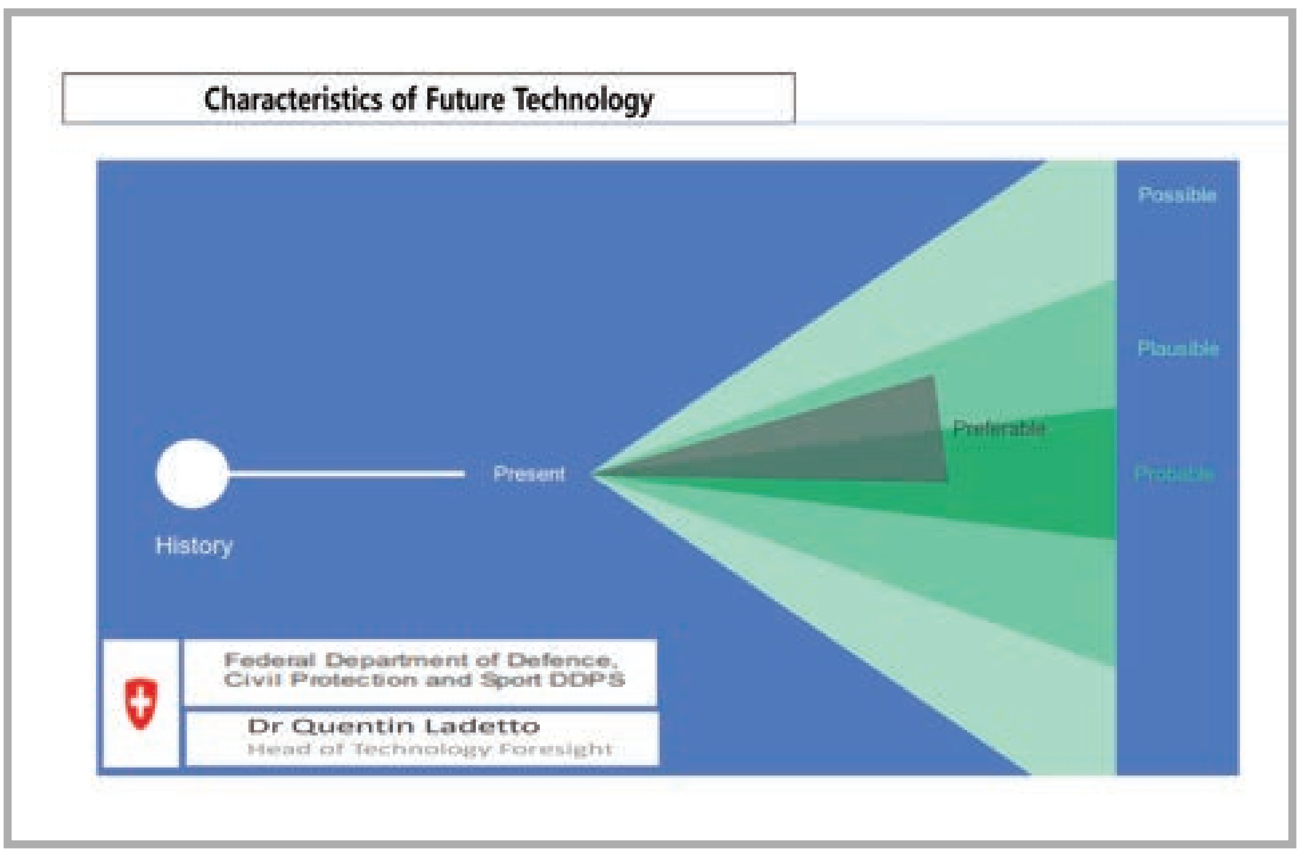
ML 10. Note 6. decontrol of vintage aero-engines

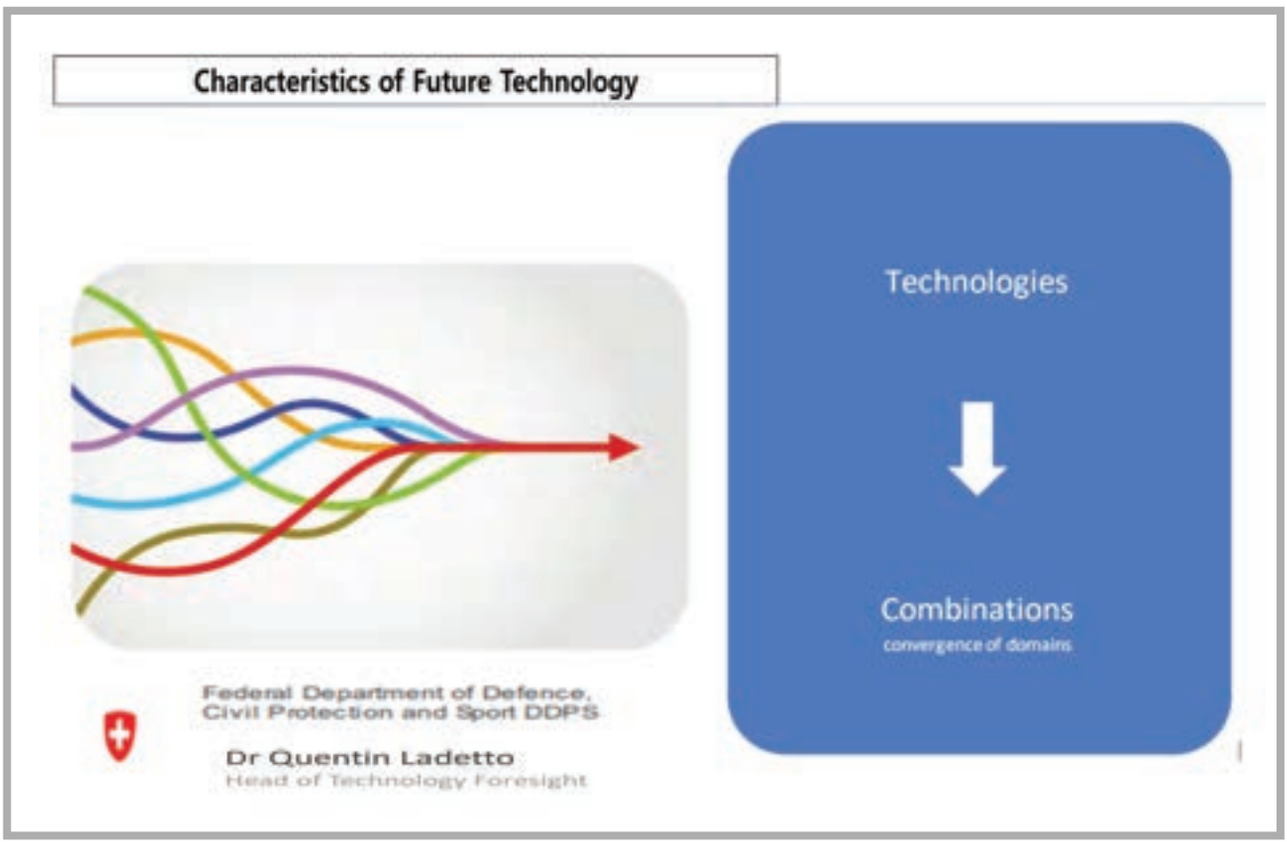
Messerschmidt 262 (Seattle Museum) and its 1942 JUMO Axial compressor Turbojet Engine.

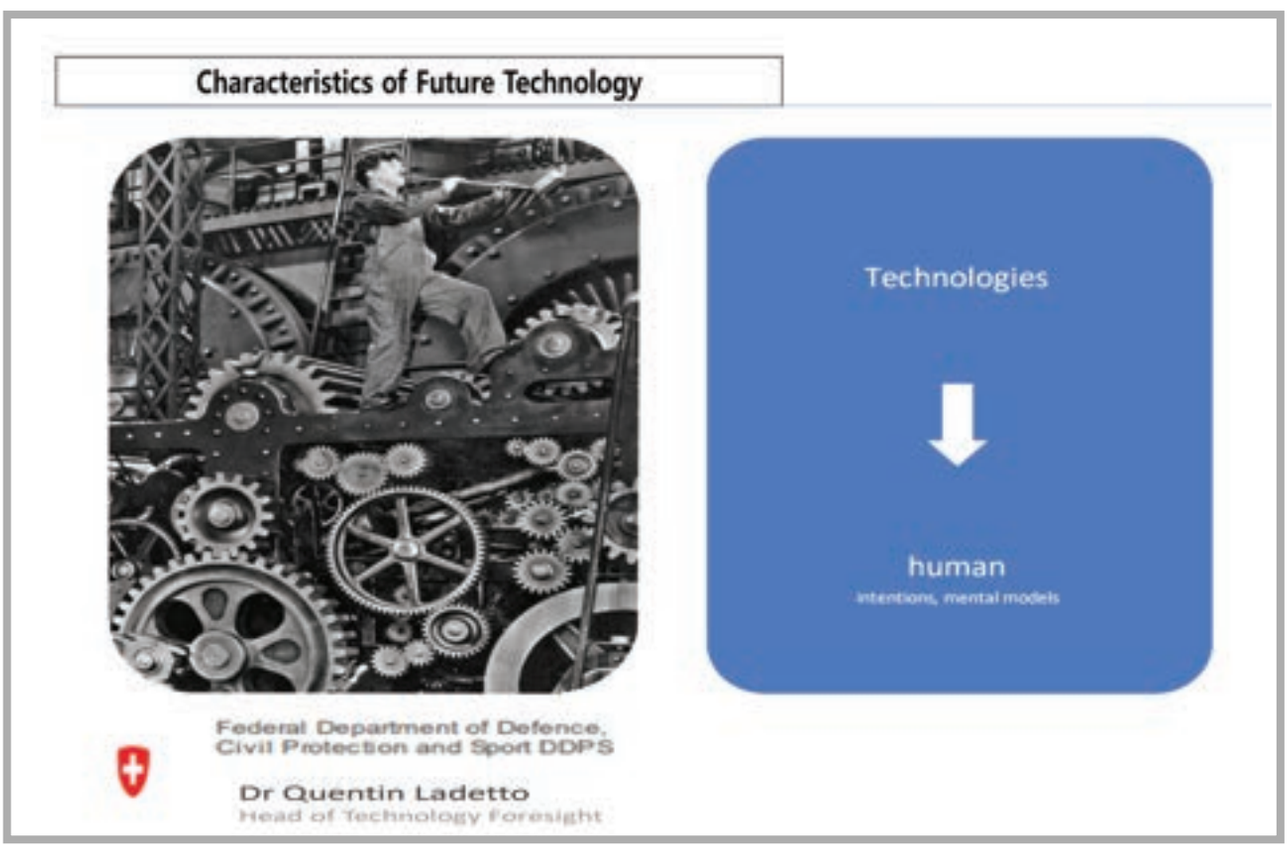
Changes to the Munitions List

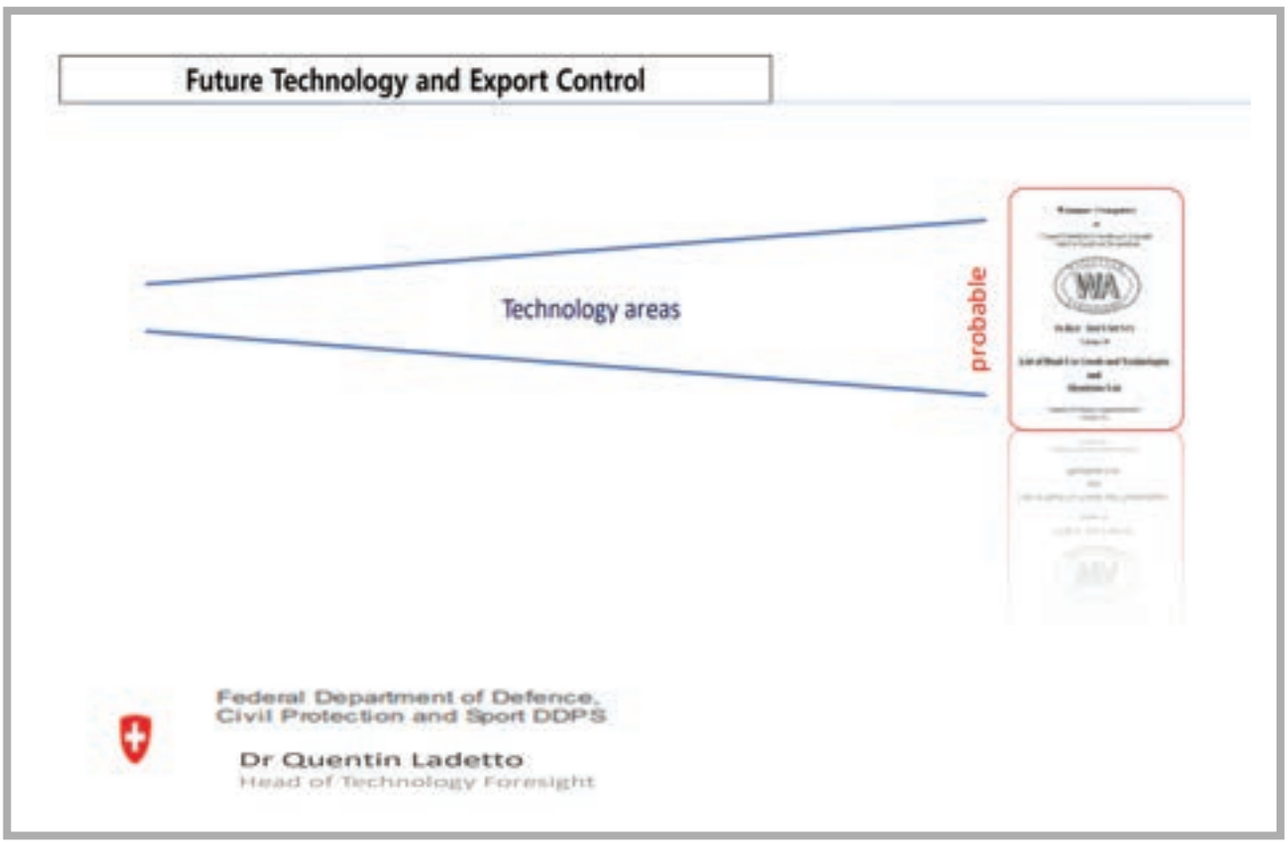
ML 21.b.5 Software specially designed or modified for the conduct of military offensive cyber operations (new entry)


Changes to the Munitions List
WA
MORE CLARIFICATIONS...
•Comparable national standards replaced with equivalent standards;
•Non-sensitive ground equipment excluded from ML 10 controls;
•Gun-mountings clarified;
•Cyphering processes replaced with cryptographic functionality;
•Protective goggles clarified.


Characteristics of Future Technology
Possible
Plausible
Preferable
Probable
Present
History
Federal Department of Defence, Civil Protection and Sport DDPS
Dr Quentin Ladetto
Head of Technology Foresight


Characteristics of Future Technology
Technologies
Combinations
convergence of domains
Federal Department of Defence,
Civil Protection and Sport DDPS
Dr Quentin Ladetto
Head of Technology Foresight


Characteristics of Future Technology
Technologies
human
intentions, mental models
Federal Department of Defence,
Civil Protection and Sport DDPS
Dr Quentin Ladetto
Head of Technology Foresight


Future Technology and Export Control
Technology areas
probable
Federal Department of Defence,
Civil Protection and Sport DDPS
Dr Quentin Ladetto
Head of Technology Foresight


Expansion of Export Control Objects
o New Technology
Supercomputing,
quantum computing
Analysis of "big data"
Artificial intelligence
Robotic engineering
Supersonic
Bioengineering

2018 U.S. ECRA (Export Control Reform Act)

o **Identifying Emerging & Foundational Technologies in the U.S.**

1. Technology that is critical to U.S. national security
2. And which is not stipulated in the Defense Production Act

• Notified on 2018. 11. 19 and collected feedback

o **Selection criteria and characteristics**

1. Technology that is speedily developed and applied
2. Goods that can be used in the military are produced through the same supply chain as related private sector goods
3. Technology that needs to be controlled in a timely manner

(1) Development probability or observations by foreign military and producers of concern should be shared

(2) Assessment of advanced technology by foreign competitors can help determine which controls need to be agreed on

(3) Goods and participants within the supply chain can logically be subject to temporary control before multilateral control

List of 14 New Technologies in U.S. ECRA in 2018

(1) Biotechnology, such as: (i) Nanobiology; (ii) Synthetic biology; (iii) Genomic and genetic engineering; (iv) Neurotech. **(2) Artificial intelligence (AI) and machine learning technology,** such as: (i) Neural networks and deep learning (e.g., brain modelling, time series prediction, classification); (ii) Evolution and genetic computation(e.g., genetic algorithms, genetic programming); (iii) Reinforcement learning; (iv) Computer vision (e.g., object recognition, image understanding); (v) Expert systems (e.g., decision support systems, teaching systems); (vi) Speech and audio processing (e.g., speech recognition and production); (vii) Natural language processing (e.g., machine translation); (viii) Planning (e.g., scheduling, game playing);	(ix) Audio and video manipulation technologies (e.g., voice cloning, deep fakes); (x) AI cloud technologies; (xi) AI chipsets. **(3) Position, Navigation, and Timing(PNT) technology.** **(4) Microprocessor technology,** such as: (i) Systems-on-Chip (SoC); (ii) Stacked Memory on Chip. **(5) Advanced computing technology,** such as: (i) Memory-centric logic. **(6) Data analytics technology,** such as: (i) Visualization; (ii) Automated analysis algorithms; (iii) Context-aware computing **(7) Quantum information and sensing technology, such as** (i) Quantum computing; (ii) Quantum encryption; (iii) Quantum sensing.

List of 14 New Technologies in U.S. ECRA in 2018

(8) Logistics technology, such as: (i) Mobile electric power; (ii) Modeling and simulation; (iii) Total asset visibility; (iv) Distribution-based Logistics Systems (DBLS).

(9) Additive manufacturing (e.g., 3D printing);

(10) Robotics such as: (i) Micro-drone and micro-robotic systems; (ii) Swarming technology; (iii) Self-assembling robots; (iv) Molecular robotics; (v) Robot compliers; (vi) Smart Dust.

(11) Brain-computer interfaces, such as

(i) Neural-controlled interfaces; (ii) Mind-machine interfaces; (iii) Direct neural interfaces; (iv) Brain-machine interfaces.

(12) Hypersonics, such as:

(i) Flight control algorithms;

(ii) Propulsion technologies;

(iii) Thermal protection systems;

(iv) Specialized materials (for structures, sensors, etc.).

(13) Advanced Materials, such as:

(i) Adaptive camouflage;

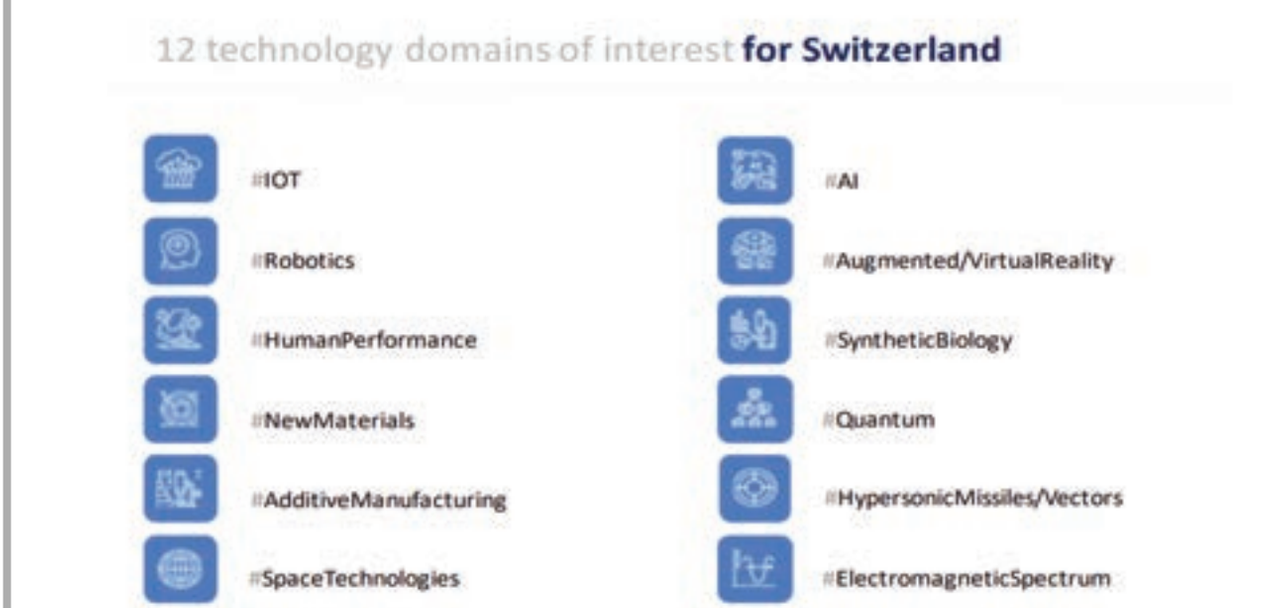
(ii) Functional textiles (e.g., advanced fiber and fabric technology);

(iii) Biomaterials.

(14) Advanced surveillance technologies, such as:

Faceprint and voiceprint

Future Technology of Interest for Switzerland

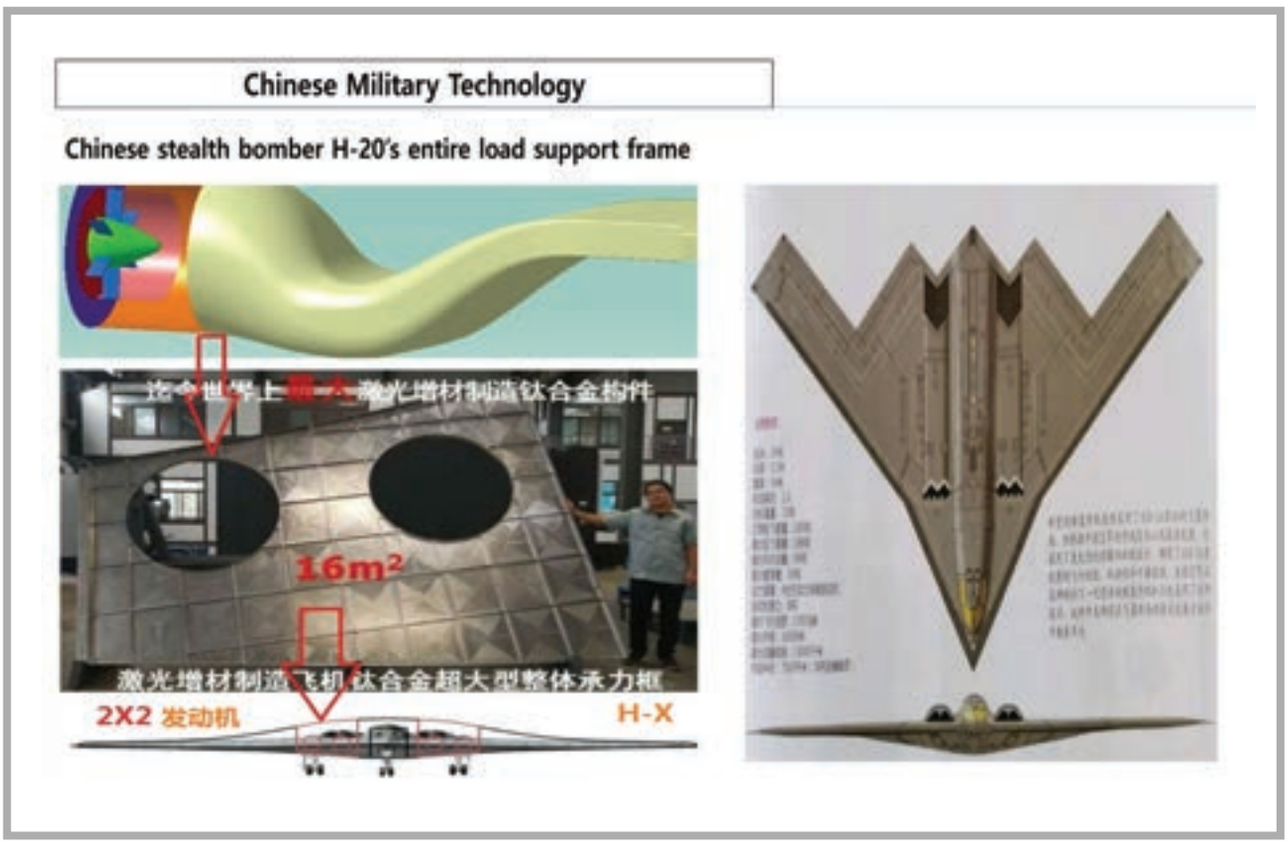


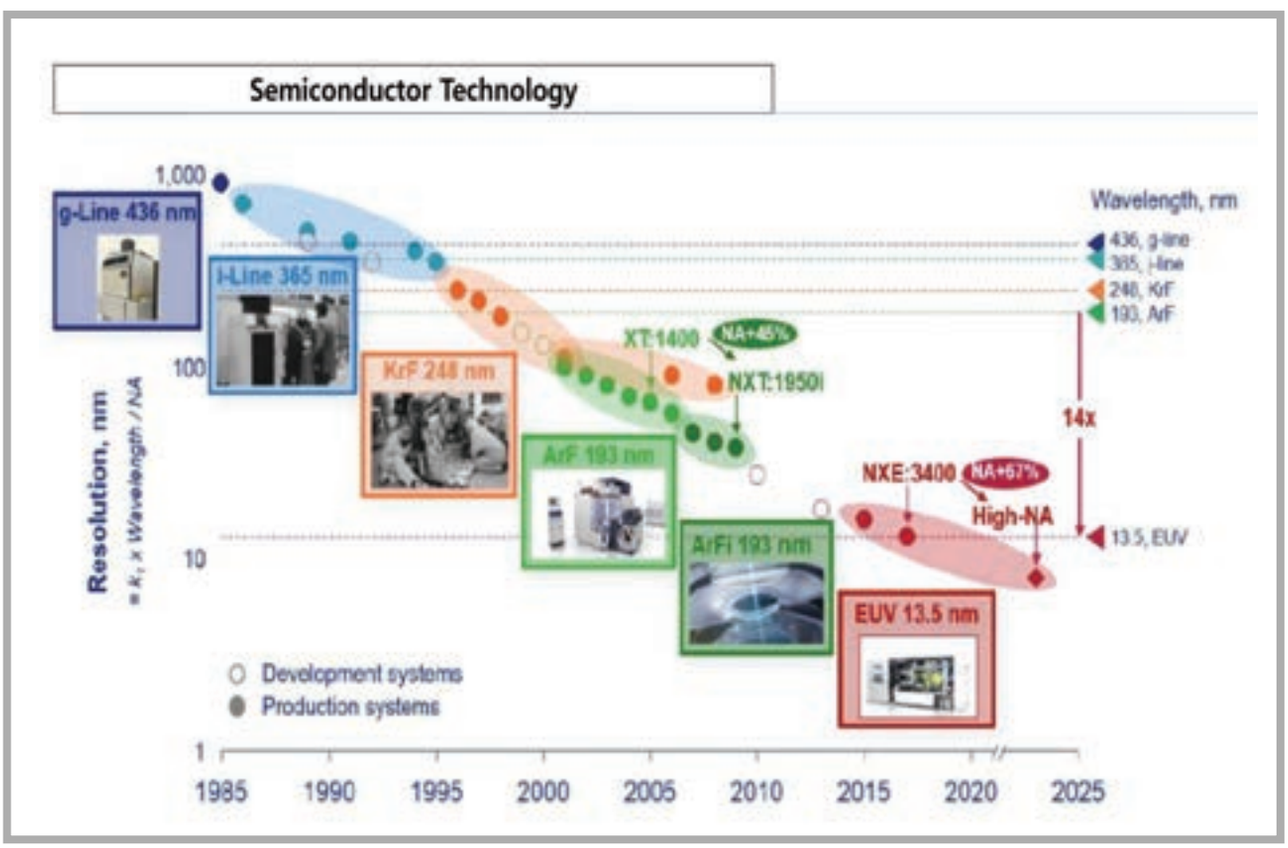
Chinese Military Technology

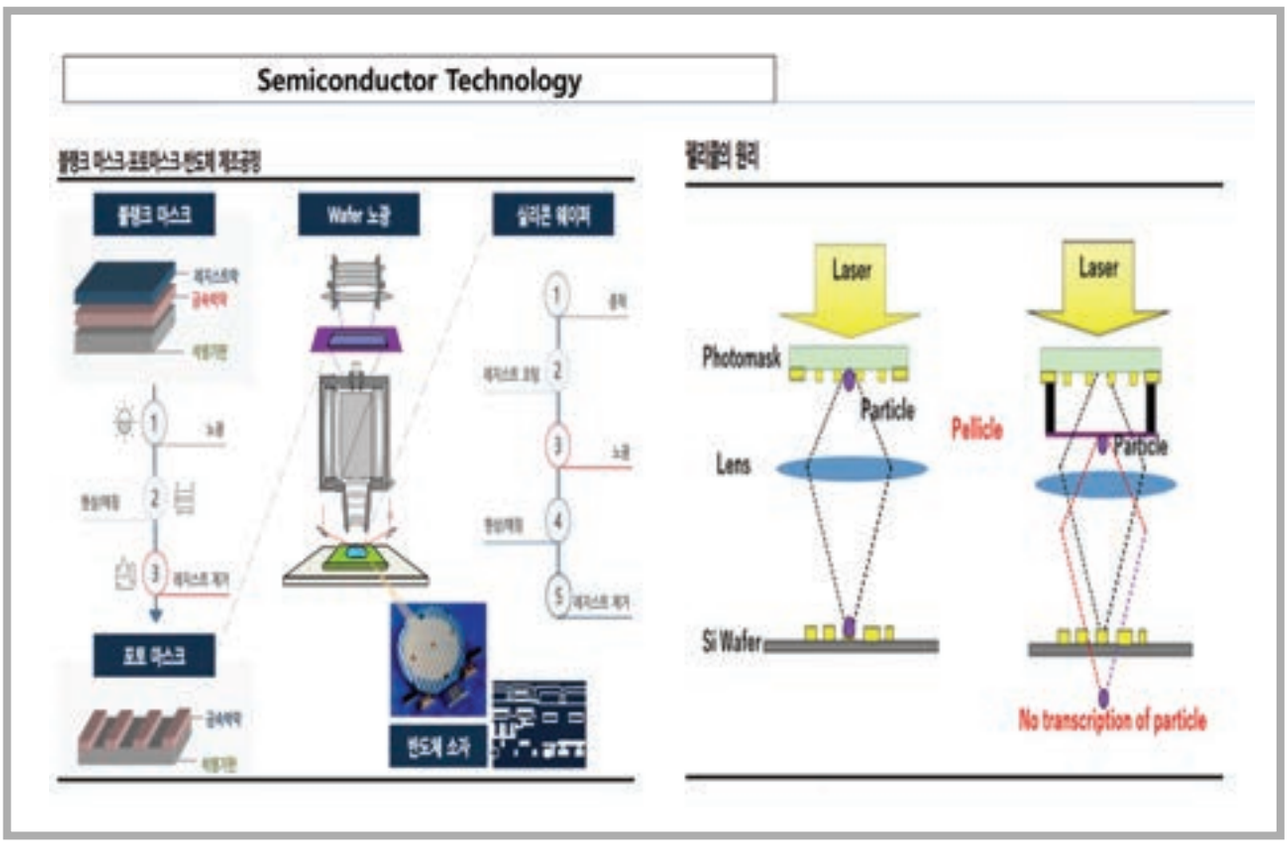
< Electronic war equipment of China's Electronic Technology Group and Weapon Engineering Group >

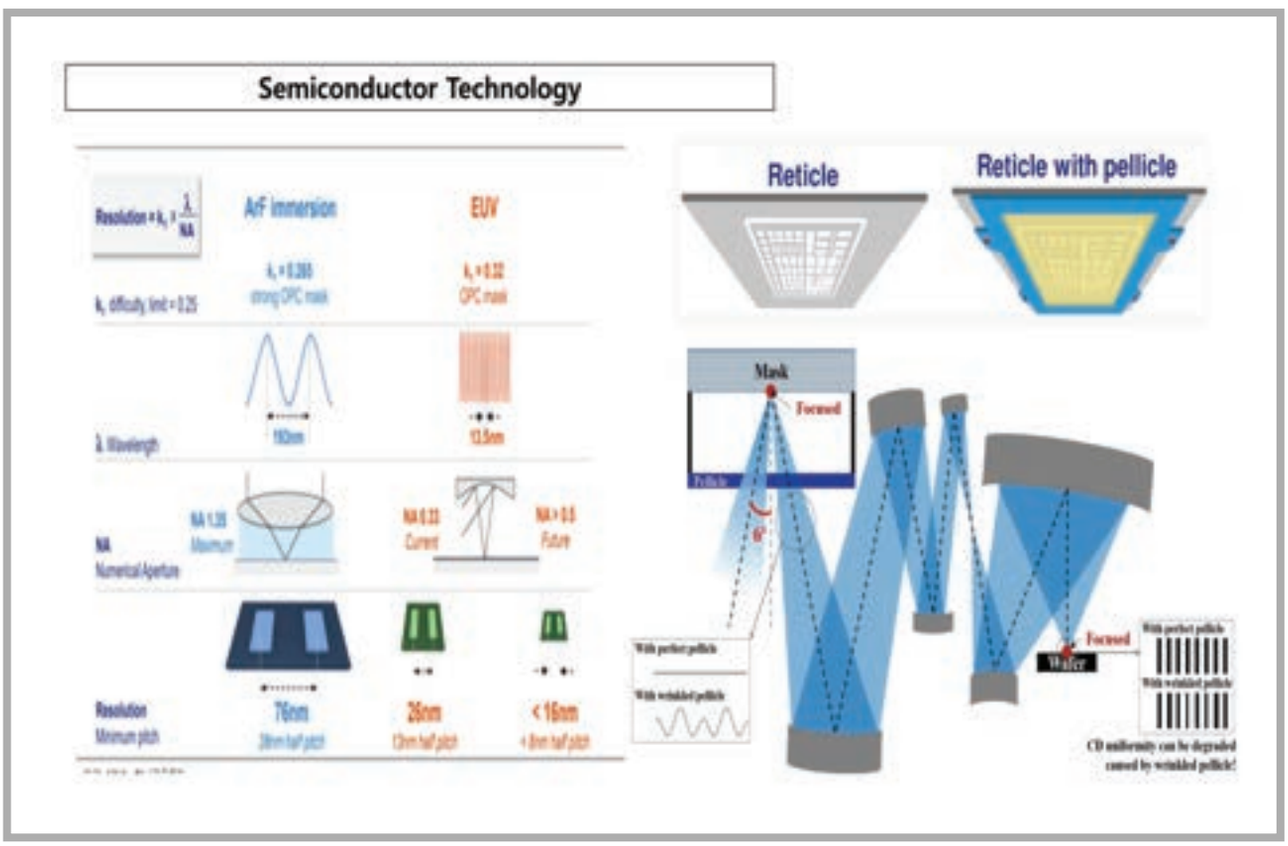
Chinese Military Technology

Chinese stealth jet J-31 and related engine rear support frame


Chinese Military Technology
Chinese stealth bomber H-20's entire load support frame
16m²
2X2 发动机
H-X


Semiconductor Technology
1,000
100
10
1
g-Line 436 nm
i-Line 365 nm
KrF 248 nm
ArF 193 nm
ArFi 193 nm
EUV 13.5 nm
XT:1400
NA+45%
NXT:1950i
NXE:3400
NA+67%
High-NA
14x
Wavelength, nm
436, g-line
365, i-line
248, KrF
193, ArF
13.5, EUV
Resolution, nm
Development systems
Production systems
1985
1990
1995
2000
2005
2010
2015
2020
2025


Semiconductor Technology
Wafer 노광
Laser
Photomask
Particle
Lens
Si Wafer
Pellicle
Laser
Particle
No transcription of particle


Semiconductor Technology
ArF immersion
EUV
Reticle
Reticle with pellicle
Mask
Focused
Wafer
Resolution
Minimum pitch
76nm
26nm
< 16nm

Agendas on Export Control

3B001.f Lithography equipment as follows:
1. a. A light source wavelength equal to or shorter than 193 nm; or b. Capable of ... a pattern with ...MRF of 45 nm or ...;

Technical Note:
The 'Minimum Resolvable Feature size' (MRF) is calculated by the following formula:
MRF = {(light source wavelength in nm) × (K factor)} / maximum numerical aperture, where K factor = ~~0.35~~ 0.25

3B001.g Masks and reticles, designed for integrated circuits specified in 3A001; 'EUV' masks and reticles, 'pellicles'

3B001.k Inspection equipment ,,, for EUV mask blanks ...

3C002.a Resists designed for semiconductor lithography as follows: 1. Positive resists adjusted (optimised) for use at wavelengths less than 193 nm but equal to or greater than 15 nm; ...

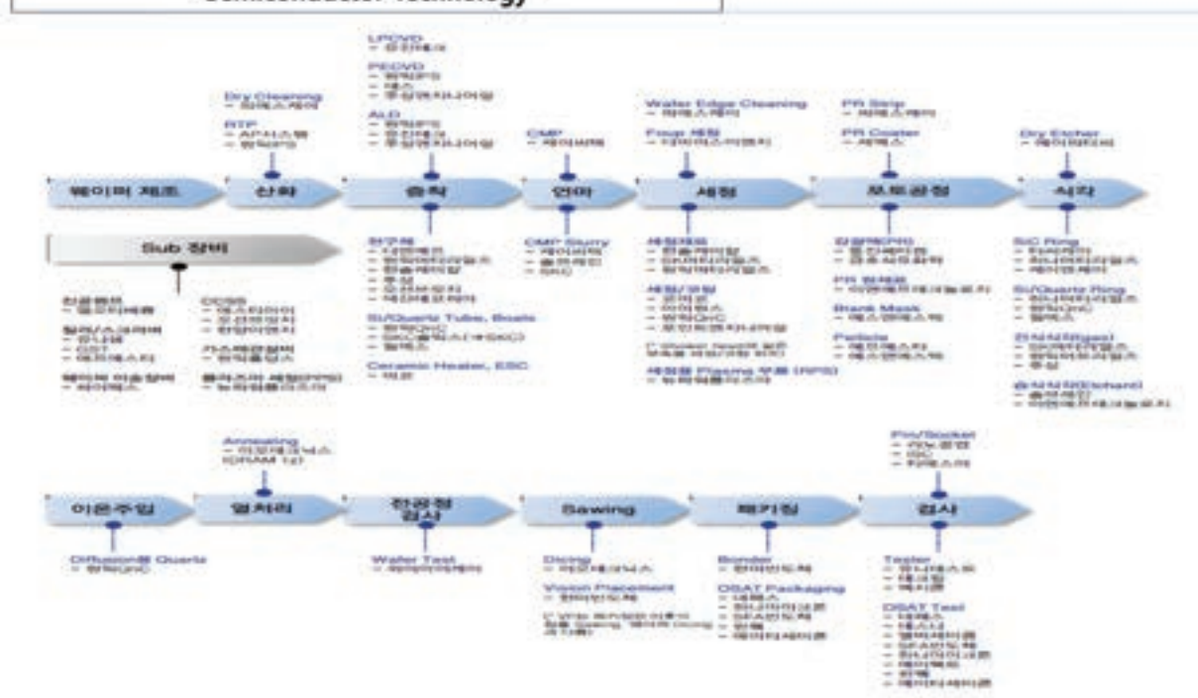
3B001.f 리소그래피(lithography) 장비로서 ...
1. a. 광원의 파장이 193 nm 미만인 것; 또는
b. '최소 분해 선폭'(MRF)이 45 nm 이하인 패턴을 생성할 수 있는 것;

기술해설:
'최소 분해 선폭'(MRF)은 다음 공식에 의해 계산된다.
MRF = {(노출광원파장(nm)) × (K factor)} / 개구수(numerical aperture(NA)) 여기에서, K factor = 0.35

3B001.g 3A001에 해당하는 집적회로를 위해 설계된 마스크 또는 망선(reticles)

3C002.a 반도체 리소그래피를 위해 설계된 레지스트로써 다음 중 하나의 것:
1. 15 nm 이상 193 nm 보다 작은 파장에서 사용할 수 있도록 최적화된 양성 레지스트 ...

Semiconductor Technology



Exclusive Export Control of the U.S.

- **Control Standards Unique to the U.S.**

3B991 Equipment not controlled by 3B001 for the manufacture of electronic "parts," "components" and materials, and "specially designed" "parts," "components" and "accessories" therefor.

License Requirements, Reason for Control: AT

b. Equipment "specially designed" for the manufacture of semiconductor devices, integrated circuits and "electronic assemblies", as follows, and systems incorporating or having the characteristics of such equipment:

Exclusive Export Control of the U.S.

- **Control Standards Unique to the U.S.**

b.1.h. "Stored program controlled" equipment for the selective removal (etching) by means of anisotropic dry methods (e.g., plasma), as follows:

b.1.h.1. Batch types having either of the following:

b.1.h.1.a. End-point detection, other than optical emission spectroscopy types; or

b.1.h.1.b. Reactor operational (etching) pressure of 26.66 Pa or less;

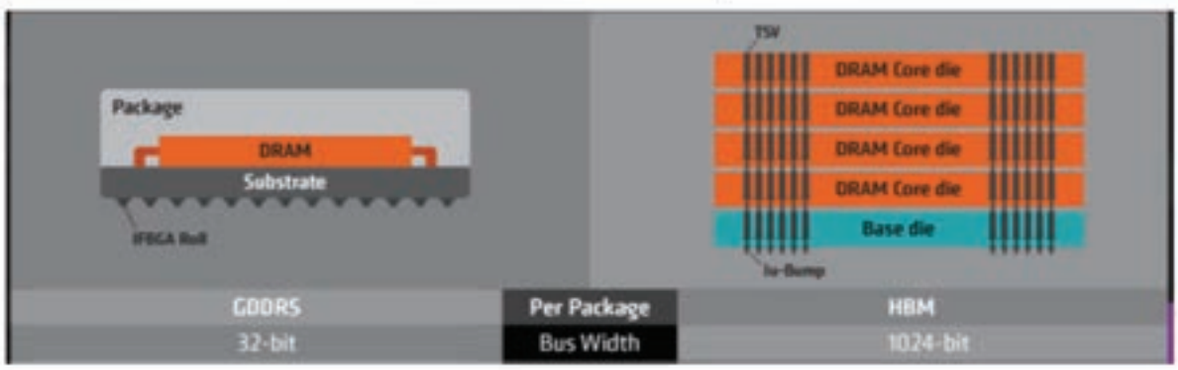

Exclusive Export Control of the U.S.
Revision of the BIS EAR on October 7
❶ Semiconductors ※ Took effect on October 21
• Advanced computing chips of certain specifications (300TFLOPS of computing power and data input and output speed of over 600GB/S)
- High-specification GPUs produced in third countries cannot be exported to China without authorization
• All products for end use in supercomputers of certain specifications (computing power of over 100PFLOPS)
- Products produced in third countries also need authorization if they are intended to develop and produce supercomputers
• All products to be exported to China's 28 semiconductor and supercomputer companies listed on the U.S. Entity List
- Products made with technology, software, and equipment of certain specifications in third countries also need authorization
※ The above three items have a low likelihood of being authorized, as they are subject to a "presumption of denial" policy


Exclusive Export Control of the U.S.
Revision of the BIS EAR on October 7
❷ Semiconductor Equipment ※ Took effect on October 7
• All U.S. export control items cannot be exported to China without authorization, including equipment, provided they are intended to produce semiconductors fulfilling the following requirements:
- Logic chips: FinFET structure or under 16/14nm
- DRAM: under 18nm
- NAND: over 128 layers
• High-specification deposition equipment that are newly included in control targets are also limited from exports
• Presumption of denial theoretically applies to Chinese companies, while multinational companies in China, such as Korean companies, are authorized through a case-by-case review

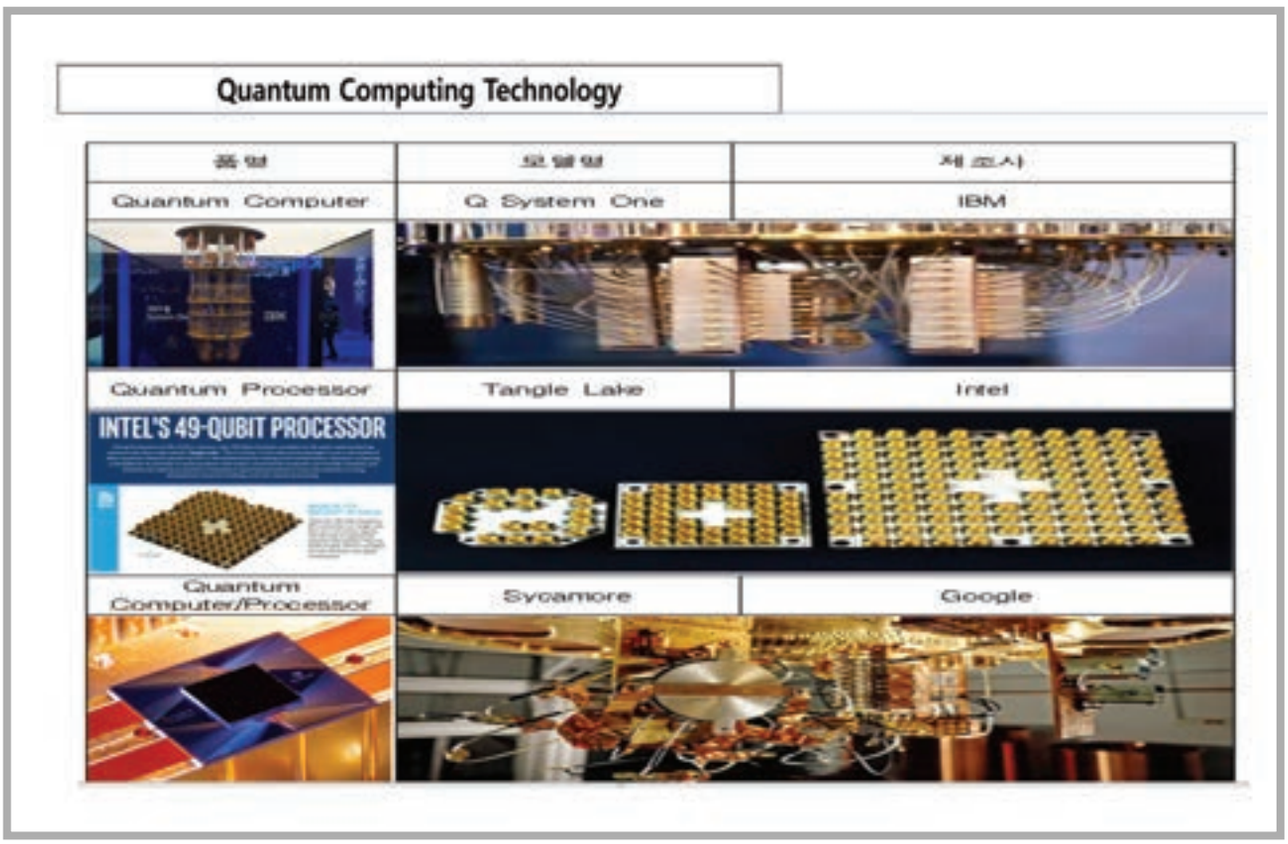
Exclusive Export Control of the U.S.

< Samsung Electronics PIM (Processing-in-Memory) >

Exclusive Export Control of the U.S.



< Hynix HBM3 (High Bandwidth Memory, HBM) >


Quantum Computing Technology
품 명
모 델 명
제 조 사
Quantum Computer
Q System One
IBM
Quantum Processor
Tangle Lake
Intel
INTEL'S 49-QUBIT PROCESSOR
Quantum Computer/Processor
Sycamore
Google


Quantum Computers
양자, 나노와 디지털을 넘어
양자물리학:
물질의 궁극적 원리 → 궁극적 기술
20세기 정보통신기술
양자물리학
정보이론
하드웨어원리
→작게
(나노기술)
→원리적 한계
소프트웨어/운영체제
양자정보과학
21세기 정보통신기술
양자물리학→하드웨어, 소프트웨어, 운영체제에 적극적으로 이용
→ 양자컴퓨터 / 양자암호 / 양자센서, 양자계측, 양자이미징
* Reference: KIAS Vice President Kim Jaewan
2022 노벨물리학상
Alain Aspect
John F. Clauser
Anton Zeilinger
위헌 광자 실험으로 벨 부등식이 위배됨을 보이고,
양자정보과학을 개척한 공로
2012 노벨물리학상
Haroche
Wineland
단일 양자계를 조작하고 측정한 공로 → 양자정보연구에 공헌

Quantum Computers

○ The U.S. is proposing to designate as strategic goods computers over 34 qubits now*, from the previous over 200 qubits The average error occurring in the Controlled Not Gate of the two physical qubits closest to the international level is currently defined as a "CNOT error." What does this mean?

* The requirements for strategic goods designation are not simply determined by qubit numbers, but must be over 34 qubits while meeting multiple conditions at the same time, such as fully controlled, connected, working, and physical

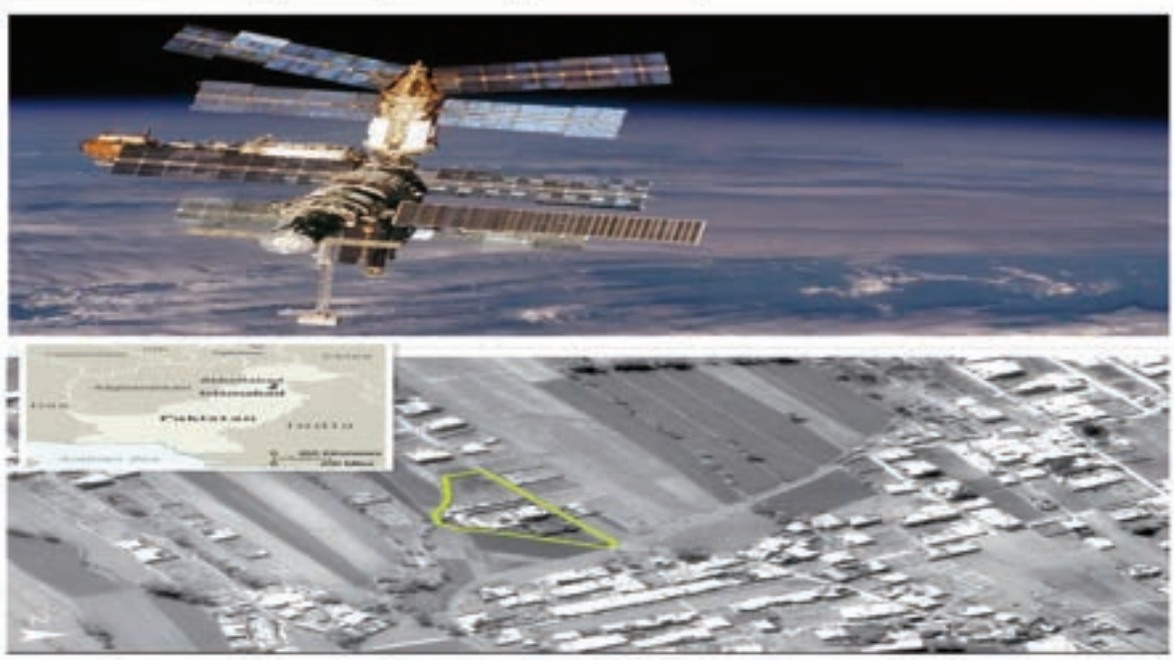
- Quantum computers calculate by manipulating qubits. In addition to the several kinds of single-qubit gates, at least one two-qubit gate is essential

※ CNOT gate is the representative among the two-qubit gates. Just this one two-qubit gate is enough. One of the qubits to be manipulated by a two-qubit gate is called the control qubit, and the other is called the target qubit.

- When the control qubit is at 0, the target qubit is left as it is; when the control qubit is at 1, NOT calculations are done on the target qubit. This is called the Controlled-NOT gate, or the CNOT gate. However, two-qubit gates are typically more difficult and error-prone compared to single-qubit gates

※ The U.S. company IBM has introduced quantum computing at Yonsei University's Songdo campus, but there is a principle that services for technology development is not to be disclosed. Germany has IBM quantum computing as well, but access by outsiders for purposes other than use is strictly prohibited.

AI Deep Learning Technology



Agendas on Export Control

"Software" specially designed or modified for training a deep learning model to automate ...

a. Providing a graphical user interface ...

b. Performing ...

c. Training a deep learning model to detect ...

Research Contents

MQ-9 Reaper (Predator B)

➢ **<Example of a Recent Trend> Discussions related to Category I and II under MTCR**

□ **Cat I: Completed missile products and parts with a range of over 300km and a payload of over 500kg**

- ㅇ Rocket systems (such as ballistic missiles, space launch vehicles, and sounding rockets) and unmanned air vehicle systems (such as cruise missiles, target drones, reconnaissance drones)
- ㅇ Rocket parts (such as stages, reentry bodies, and engines), production facilities → equipment and technology directly related to WMD transport

* Authorization guidelines: prohibited from renovating, copying, and re-exporting without prior agreement from the export country (strong presumption of denial)
  - Exceptional export is possible if it is not used for purposes other than those reported and if it is guaranteed by the import country's government (not to be transferred to a third party without authorization)
  (Category I item production facilities cannot be transferred; Category II items to be used in transporting WMDs are the same as Category I items)

□ **Cat II: aforementioned missile parts and technology, missiles with a range of over 300km and a payload of under 500kg**

- ㅇ Dual-use parts, equipment and technology used in Category I items, such as propellants, composites, navigation equipment, flight control equipment, aviation electronics equipment, launch support equipment and facilities, test equipment, stealth technology
- ㅇ Missile, rockets, UAV → equipment and technology not directly related to WMD transport

Research Contents

- **<Example of a Recent Trend> Discussions on NSG, WA Additive Manufacturing Machines**

1.B.8 Additive Manufacturing Machines with all the following characteristics:

a. having a controlled atmosphere (vacuum or inert gas) process environment with two dimensions greater than 200mm; and

b. using a selective fusion process with laser or electrons beam on powder bed.

Oak Ridge National Laboratory, the U.S.
R&D project on nuclear reactor core design (launched a prototype reactor core)

The University of Sheffield Advanced Manufacturing Research Centre (AMRC), the UK
Production technology for key parts of SMR (shortened the time needed to produce pressure vessels from 3 years to 6 months)

Conclusion

o **The scope of the international export control regime is expected to expand to include general items as well as military items**

- Semiconductors, AI, and other information technology will be applied to almost every kind of weapons and general products
- Complex negotiations are anticipated in the form of multilateral, minilateral, and bilateral consultations for each agenda item
- Responding to the international regime, national R&D, and strategies to foster the industry need to be interconnected

o **Acquisition and security of advanced technology will determine economic and security sustainability in the future**

- Intensifying export rivalry all over the world, and heightened issues in the supply chain
- Innovative advances and fusion in military and commercial technology are expected
- Acquisition and management of source technology will determine national security in the future

Q & A

2023 Defense Technology Security Conference 2023 방산기술보호 컨퍼런스

SESSION 3

기술의 발전과 앞으로의 과제

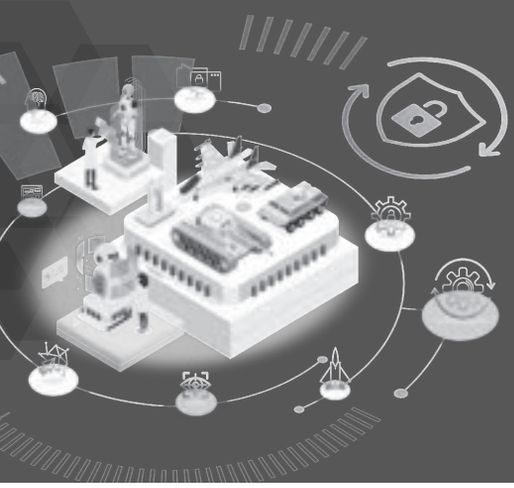
Technological Advancements and Future Challenges

K-국방을 위한 미래도전기술
Future Challenges Technology for K-Defense

방산기술보호 등급분류 및 조치를 위한 평가방법
Assessment Method for Classification and Measures in Defense Technology Security

Post K-방산을 위한 방산기술보호 정책 방향
Defense Technology Protection Direction For Post K-Defense

양자암호통신 기술 및 동향
Quantum Key Distribution Technology and Trends



2023 Defense Technology Security Conference 2023 방산기술보호 컨퍼런스

주제발표 1.

K-국방을 위한 미래도전기술

Future Challenges Technology for K-Defense

동국대학교 국방안전연구센터장 I **박진호**

Director, Defense Security Research Center, Dongguk University

Prof. Jinho Park

2023 Defense Technology Security Conference

Future Challenges Technology for K-Defense

August 4, 2023

Defense Security Research Center / Division of AI Software Convergence,
Dongguk University

Director / Prof. Jin-ho Park
gomalove@hanmail.net

방위사업청

국방안전연구센터

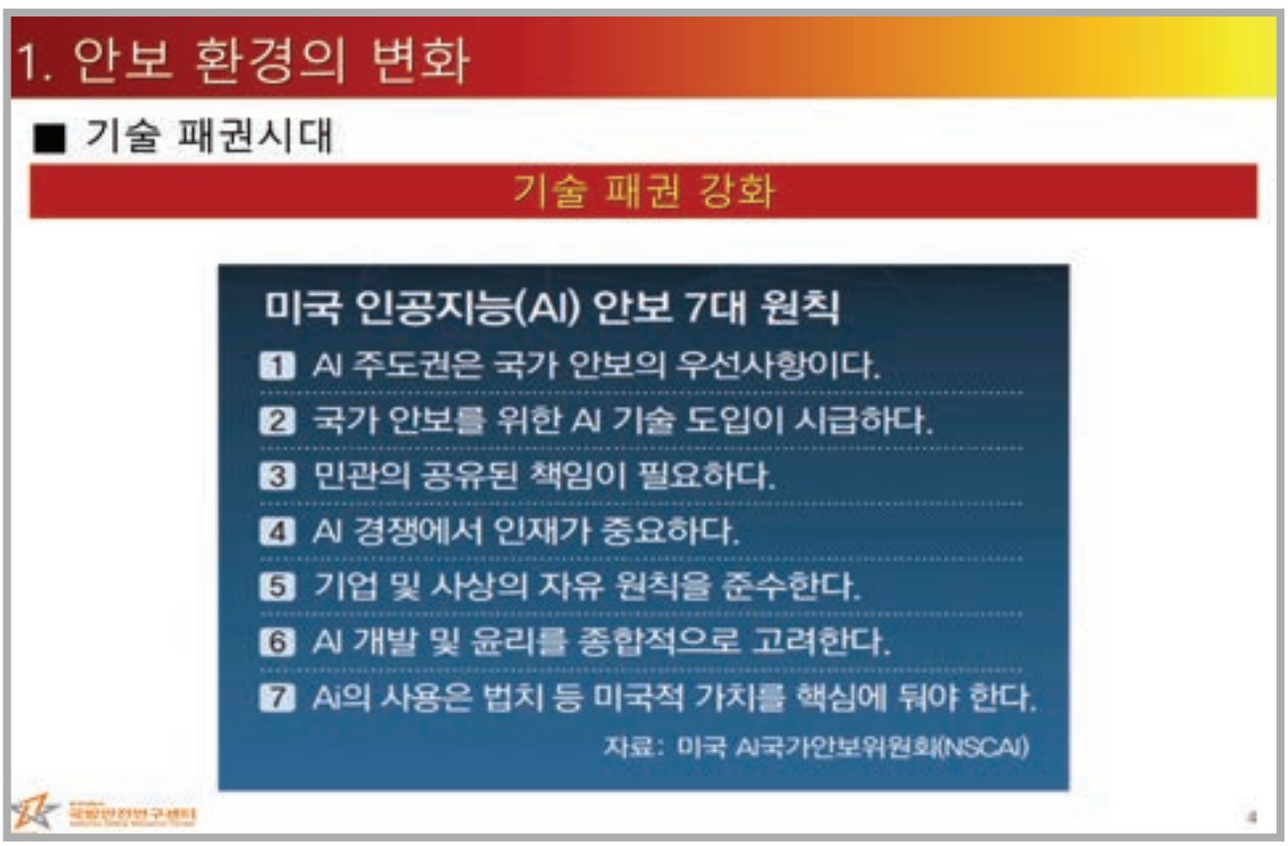
목 차

1. 안보 환경의 변화
2. 국방기술 환경의 변화
3. 첨단기술 적용 사례
4. 미래도전기술
5. 결론

국방안전연구센터

2


1. 안보 환경의 변화
3


1. 안보 환경의 변화
■ 기술 패권시대
기술 패권 강화
미국 인공지능(AI) 안보 7대 원칙
1 AI 주도권은 국가 안보의 우선사항이다.
2 국가 안보를 위한 AI 기술 도입이 시급하다.
3 민관의 공유된 책임이 필요하다.
4 AI 경쟁에서 인재가 중요하다.
5 기업 및 사상의 자유 원칙을 준수한다.
6 AI 개발 및 윤리를 종합적으로 고려한다.
7 Ai의 사용은 법치 등 미국적 가치를 핵심에 둬야 한다.
자료: 미국 AI국가안보위원회(NSCAI)
4

1. 안보 환경의 변화

■ 안보개념의 변화

전쟁 발생 전조증상

- 기존 전쟁 : 국경지역 전차 집결, 미사일 포문 개방 등
- 현대전 : 야전병원 천막 설치/헌혈차량 배치, 거짓 문자 유포/사이버 공격 등

5

1. 안보 환경의 변화

■ 첨단기술의 중요성

첨단장비와 전투력

- 모스크바함 레이더 수 : 7개
- 이지스함 레이더 수 : 2개

(출처 : 사틀의 군사연구소)

6

1. 안보 환경의 변화

■ 첨단기술의 중요성(계속)

첨단기술과 가성비?

- 터키제 : 바이락타르
- 이번 전쟁에서 최고의 스타 : 첨단기술 + 가성비?

(출처 : 샤를의 군사연구소)

7

1. 안보 환경의 변화

■ 첨단기술의 중요성(계속)

첨단기술과 전술통신망

- 러시아 : S-108
- 광대역이긴 하지만 데이터 전송 용량이 매우 적은 시스템
- 여러 기종에 대한 동시통제 임무에 제한이 큼

(출처 : 샤를의 군사연구소)

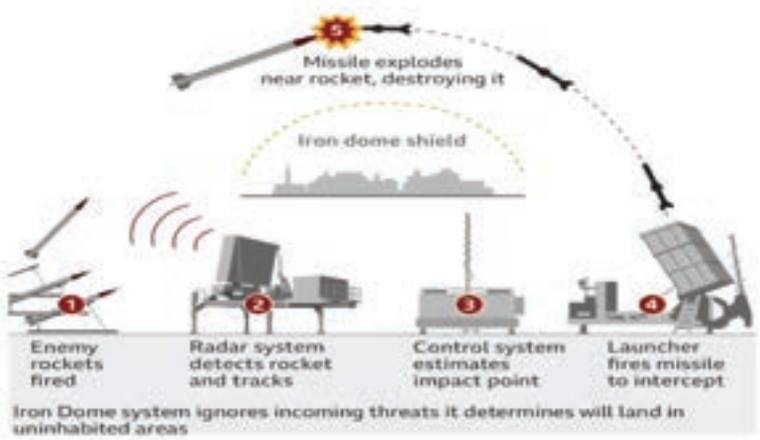
8

1. 안보 환경의 변화

■ 첨단기술의 중요성(계속)

이스라엘 미사일 방어 시스템

- 이스라엘 : Iron Dom



9

1. 안보 환경의 변화

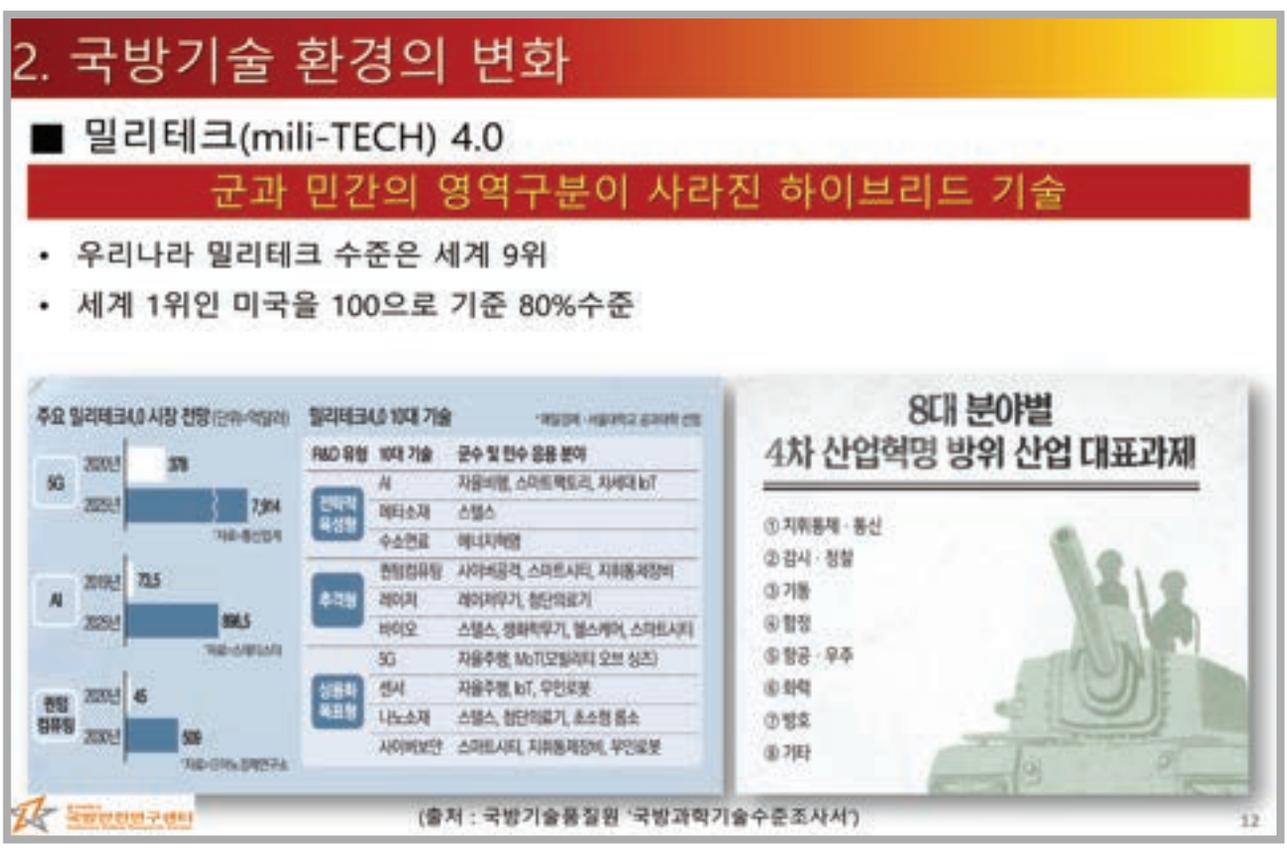
■ 첨단기술의 중요성(계속)

첨단전쟁의 핵심은 Software

- F-35
- Software 비중 : 95%?

10


2. 국방기술 환경의 변화
11


2. 국방기술 환경의 변화
■ 밀리테크(mili-TECH) 4.0
군과 민간의 영역구분이 사라진 하이브리드 기술
• 우리나라 밀리테크 수준은 세계 9위
• 세계 1위인 미국을 100으로 기준 80%수준
주요 밀리테크4.0 시장 전망
5G
AI
밀리테크4.0 10대 기술
R&D 유형
10대 기술
운수 및 한수 응용 분야
AI
자율비행, 스마트팩토리, 자세대 IoT
메타소재
스텔스
수소연료
에너지저장
양자컴퓨팅
사이버공격, 스마트시티, 지휘통제장비
레이저
레이저무기, 첨단의료기
바이오
스텔스, 생화학무기, 헬스케어, 스마트시티
5G
자율주행, MoT(모빌리티 오브 싱즈)
센서
자율주행, IoT, 무인로봇
나노소재
스텔스, 첨단의료기, 초소형 통소
사이버보안
스마트시티, 지휘통제장비, 무인로봇
8대 분야별
4차 산업혁명 방위 산업 대표과제
① 지휘통제 · 통신
② 감시 · 정찰
③ 기동
④ 합정
⑤ 항공 · 우주
⑥ 화력
⑦ 방호
⑧ 기타
(출처 : 국방기술품질원 '국방과학기술수준조사서')
12

2. 국방기술 환경의 변화

■ 미래도전기술개발 환경개선

국방과학기술혁신 촉진법

- 국방과학기술혁신 촉진법 통과
- 기술혁신속도 가속화 : 국방미래도전기술개발 사업 추진

13

2. 국방기술 환경의 변화

■ 주요 선진국의 국방혁신(2'43")

14


3. 첨단기술 적용 사례
15


3. 첨단기술 적용 사례
■ 美 해병대(United States Marine Corps)
美 해병대는 신기술을 적용 새로운 전술 변화 진행 중
무게 1lb 미만, 1km 이상 비행 가능
M134미니건 장착, 분당 최대 6천발 사격 가능
모듈식 첨단 로봇 무기 시스템
400발 탄환 실고 이동 가능, 40mm 폭탄 투척기 설치 가능
(출처 : DMA 등)
16

3. 첨단기술 적용 사례

■ IOT 기반 첨단 무인경계 시스템

소수인원으로 철통경계! 기존경계인원은 전투병으로

17

3. 첨단기술 적용 사례

■ 중국 무인 상륙전투 수상함

빠르게 상륙하고 인원피해를 줄인다!

18

3. 첨단기술 적용 사례

■ 자율군집주행 시스템

소수의 병력으로 자율군집 무인 무장 및 수송차량 운용

19

3. 첨단기술 적용 사례

■ 미군 무인 헬기(MQ-8 파이어 스카우트)

인원 피해 없이 화력지원 및 정보수집 수행!

20

3. 첨단기술 적용 사례

■ UAM

공간에 구애 받지 않는 작전 수행!

21

3. 첨단기술 적용 사례

■ 드론 킬러

드론을 이용한 적들의 감시 및 활용을 무력화!

22


3. 첨단기술 적용 사례
■ 스텔스 장갑차
보이지 않게 침투하고 막강한 화력으로 적들을 제압!
NEWSIS
PL-01
23


3. 첨단기술 적용 사례
■ 위성 무기
우주에서 지구를 지킨다!
ODIN
ODIN
24

3. 첨단기술 적용 사례

■ 스타링크

우주에서 전 지구를 이어주는 전술망 구축!

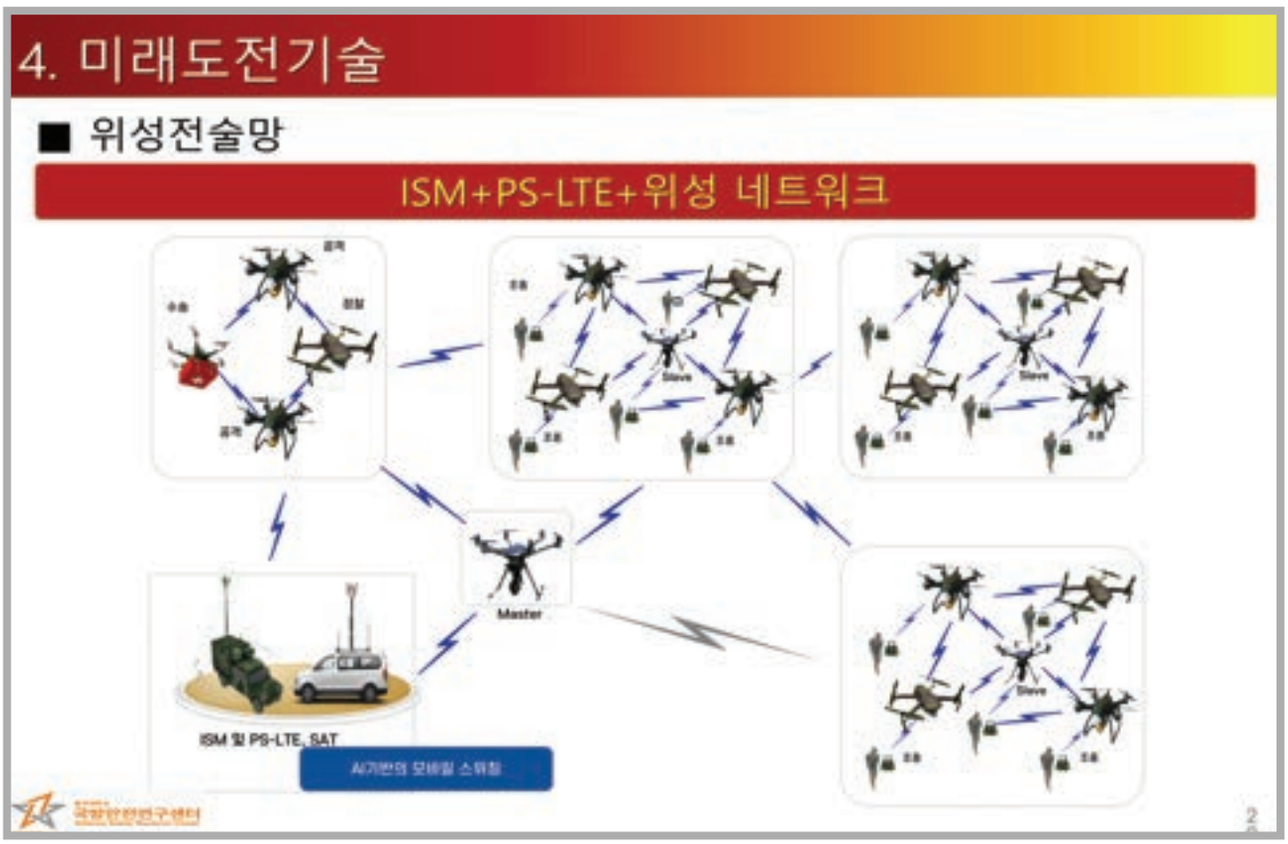
25

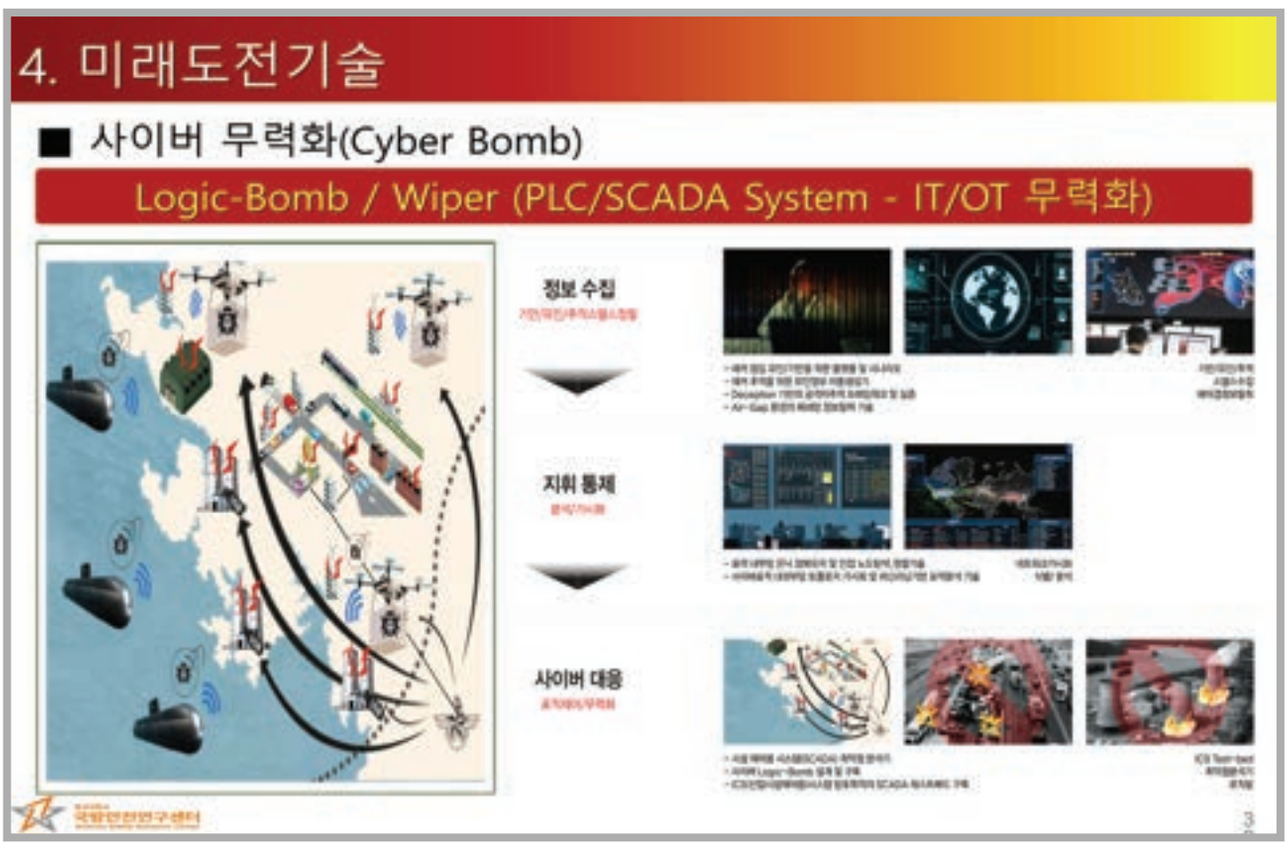
4. 미래도전기술

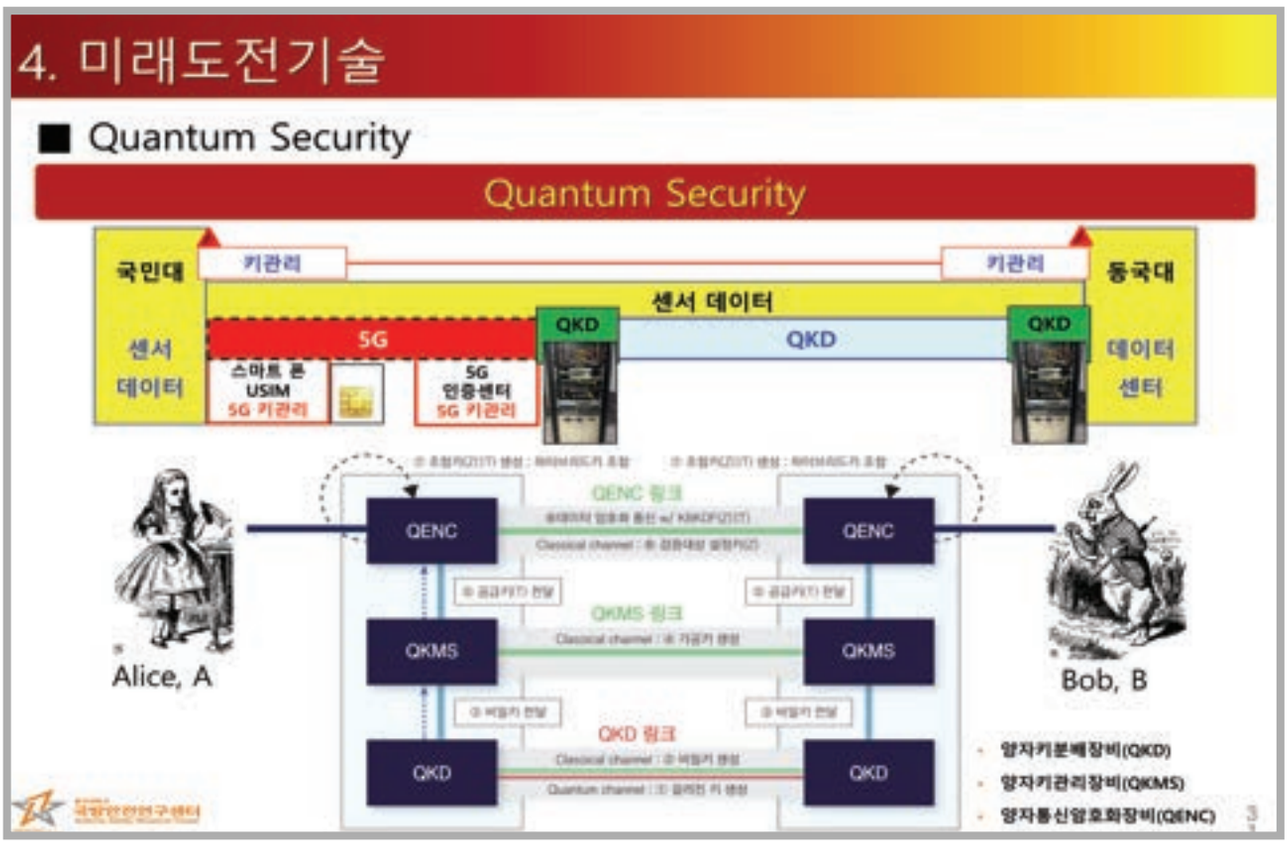
26


4. 미래도전기술
■ 3D 프린터
식량 보급은 전쟁 승리의 키! 식품 3D 프린팅으로 해결!
먹을 수 없으면 싸워 이길수 없다!
3D 식품 프린팅 장점
✓ 소규모 및 이동성
✓ 식량 부피 최소화
✓ 식품재료 카트리지화
✓ 보급지 이동중/정착후 제조
야전시 이동 및 전투력 상승영양식 보급
장병들의 건강상태 보강에 의한 전투력 증대
원격지 식량 보급력 원활화
식품 3D 프린팅
이동하면서 식품 공급
식량 보급이 어려운 고립지 전투 적용
현대전
남한산성 (식량부족)
나폴레옹 (통조림 개발)
고립지 전투 (3D 식품 프린팅)
승리
승리
(출처 : 네덜란드 New Scientist)
27


4. 미래도전기술
■ 3D 프린터
안전한 식품 섬유 필터 !!!
보호되지 않으면 싸워 이길수 없다!
• 통상 섭취로 인체안전성 검증 식품소재 이용
• 생화학 테러 대응형 바이오 소재 탑재 가능
• 장병 전투력 고취 및 트라우마 치유용 아로마테라피
• 필터소재의 카트리지화
• 유사시 필터 자체 재생에 의한 전투력 지속
현재
• 착용 불편함
• 정화통 교체
• 호흡 불편
• 전투수행 불편
미래
필터 재생기 내장형 개인보호구
• 착용 용이
• 필터 교체 필요 없음
• 호흡 용이
• 전투수행 용이
• 유사 시 상처 도포제로 이용 가능
부착형 필터장치
산소공급 팬
교체형 필터부
필터 카트리지(교체형)
내장 필터 재
원리: 접촉식 정복
28

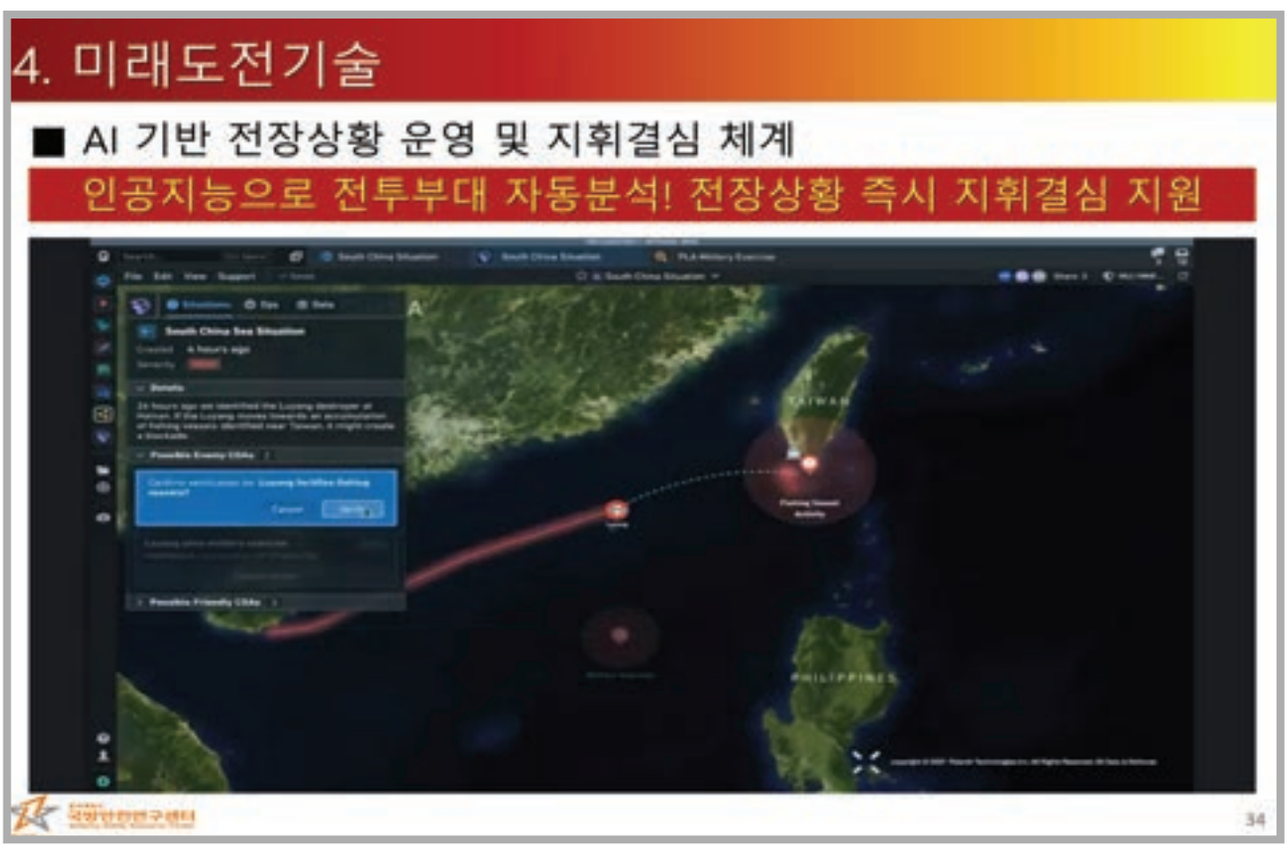

4. 미래도전기술
■ 위성전술망
ISM+PS-LTE+위성 네트워크
Master
ISM 및 PS-LTE, SAT
AI기반의 모바일 스워칭


4. 미래도전기술
■ 사이버 무력화(Cyber Bomb)
Logic-Bomb / Wiper (PLC/SCADA System - IT/OT 무력화)
정보 수집
지휘 통제
사이버 대응


4. 미래도전기술
Quantum Security
Quantum Security
국민대
키관리
키관리
동국대
센서 데이터
센서
데이터
5G
QKD
QKD
QKD
데이터
센터
스마트 폰
USIM
5G 키관리
5G
인증센터
5G 키관리
QENC 링크
QENC
QENC
QKMS 링크
QKMS
QKMS
QKD 링크
QKD
QKD
Alice, A
Bob, B
양자키분배장비(QKD)
양자키관리장비(QKMS)
양자통신암호화장비(QENC)


4. 미래도전기술
Quantum Security
양자암호통신장비 - 사전보안확인
사업계획
개발 / 구매
전력화
현재
보안제도
보안대책 검토
* 제품 유형별 사전 인증요건
확인 등 보안대책 검토
① 보안기능 확인서
② cc인증서
③ 성능평가인증서
④ 암호모듈검증서
기기 보안적합성 검증
"예" 정보보호제품및네트워크장비
암호 보안적합성 검증
"예" 검증필암호모듈,
양자암호통신장비
SW 보안성 검증
"예" 클라우드 보안적합성 검증
보안측정
사전 보안
확인
보안대책 검토
간소화(무결성 체크)
보안측정
업체에서 개발한 양자암호통신장비의 軍 도입을 위해 " 군 보안요구사항의 구현" 여부를
사전에 확인하여 목록을 공개, 보안성 및 상호운용성이 내재된 양자암호통신장비 군 활용 촉진


4. 미래도전기술
■ Quantum Security
양자암호통신장비 - 사전보안확인
업체
국방부
방첨사
1. 제품 개발
2. 보안 확인 의뢰
3. 의뢰 접수
4. 보안 확인 지시
5. 보안요구사항 확인
6. 결과 보고
7. 사전 보안확인
양자암호통신장비 등재
※ 핵심 관건은 군의 보안요구사항을 국방 표준 규격화 필요
→ 신속한 도입이 가능
국방표준종합정보시스템
3


4. 미래도전기술
■ AI 기반 전장상황 운영 및 지휘결심 체계
인공지능으로 전투부대 자동분석! 전장상황 즉시 지휘결심 지원
TAIWAN
PHILIPPINES
34

5. 결론

35

5. 결론

■ 안보범위 확장으로 인한 국군의 임무 변화

우주와 사이버까지 전장의 확대!!

- 지정학적 위치로 한국은 영원한 안보위기 국가
- 지속적인 병력감소와 주변국들의 군사력강화
- 주변국은 공군 및 해군력 집중강화
  → 글로벌 강국은 우주와 사이버 전력 강화
- 현대전에서는 첨단무기의 발전에 따라 대규모 위협이 증대
  → 새로운 유형의 전투가 발생

미래에는 육, 해, 공 이외에도 우주, 사이버 공간 등으로 전장이 확대,
신속하게 대응 작전 및 전투를 수행하는 최첨단 미래군이 필요!
AI-ICBM, Cyber-Bomb, Quantum Security 등 첨단기술이 적용된
"미래도전기술" 개발이 한반도 안보를 지키는 최우선 과제!


Thank you!
Defense Security Research Center / Division of AI Software Convergence,
Dongguk University
Director / Prof. Jin-ho Park
gomalove@hanmail.net
37

2023 Defense Technology Security Conference

Future Challenges Technology for K-Defense

August 4, 2023

Defense Security Research Center / Division of AI Software Convergence,
Dongguk University

Director / Prof. Jin-ho Park
gomalove@hanmail.net

방위사업청

국방안전연구센터

Table of Contents

국방안전연구센터

2


1. Changes in the Security Landscape
3


1. Changes in the Security Landscape
Period of Technology Rivalry
Strengthening technology rivalry
미국 인공지능(AI) 안보 7대 원칙
1 AI 주도권은 국가 안보의 우선사항이다.
2 국가 안보를 위한 AI 기술 도입이 시급하다.
3 민관의 공유된 책임이 필요하다.
4 AI 경쟁에서 인재가 중요하다.
5 기업 및 사상의 자유 원칙을 준수한다.
6 AI 개발 및 윤리를 종합적으로 고려한다.
7 Ai의 사용은 법치 등 미국적 가치를 핵심에 둬야 한다.
자료: 미국 AI국가안보위원회(NSCAI)
4

1. Changes in the Security Landscape

■ Changes in the Concept of Security

Signs of a war breakout

- Wars in the past: Assembly of tanks in border areas, opening missile gunports, etc.
- Modern warfare: Setting up tents and blood donation vehicles at field hospitals, disseminating false messages, cyberattacks, etc.

5

1. Changes in the Security Landscape

■ Importance of Advanced Technology

Advanced equipment and combat power

- Number of radars on the Moskva: 7
- Number of radars on the Aegis: 2

(Source: @charlesmililab)

6

1. Changes in the Security Landscape

■ Importance of Advanced Technology (cont'd)

Advanced technology and cost-efficiency?

- Turkish: Bayraktar
- The biggest star in this war: advanced technology + cost-efficiency?

(Source: @charlesmililab)

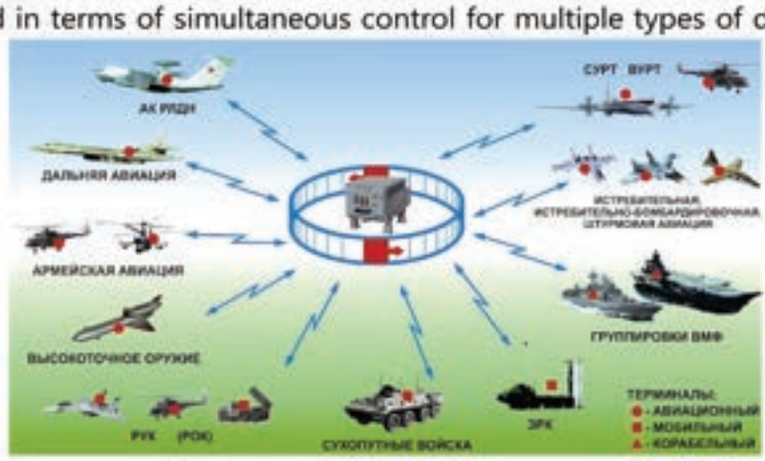
7

1. Changes in the Security Landscape

■ Importance of Advanced Technology (cont'd)

Advanced technology and tactical nets

- Russia: S-108 Russia:
- Broadband system, but with very low data transmission capacity
- Highly limited in terms of simultaneous control for multiple types of devices



(Source: @charlesmililab)

8

1. Changes in the Security Landscape

■ Importance of Advanced Technology (cont'd)

Israeli missile defense system

- Israel: Iron Dom

9

1. Changes in the Security Landscape

■ Importance of Advanced Technology (cont'd)

Software is the essence of advanced warfare

- F-35
- Proportion of software: 95%?

10

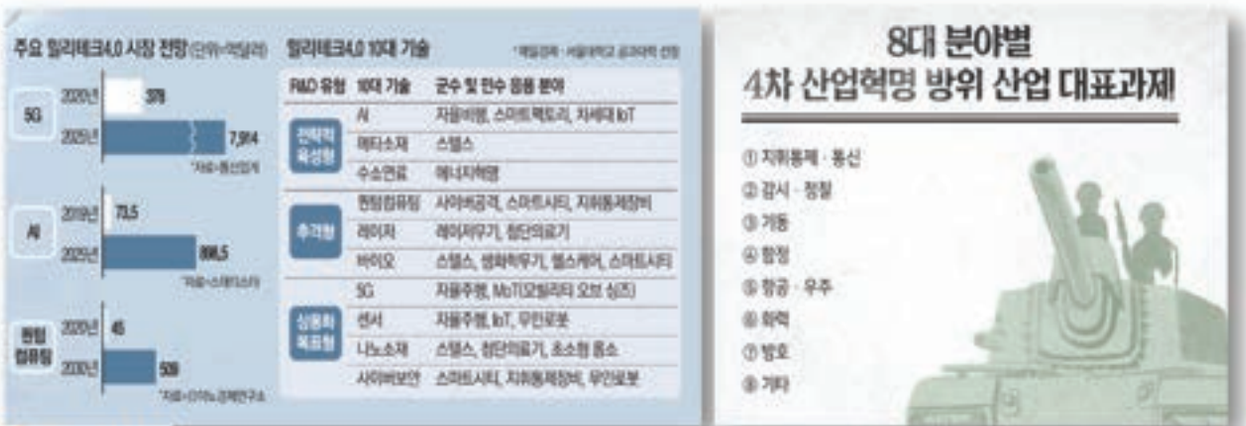
2. Changes in the Defense Technology Landscape

2. Changes in the Defense Technology Landscape

■ mili-TECH 4.0

Hybrid technology with blurred borders between military and civilian sectors

- ROK's militech ranking is 9th in the world
- 80% with the U.S., which comes 1st in the world, as 100



(Source: DTaQ's 'Report on Defense Science and Technology Level ')

2. Changes in the Defense Technology Landscape

■ Improvements in the Future Challenges Technology Development Landscape

Defense Science and Technology Innovation Promotion Act

- The Defense Science and Technology Innovation Promotion Act was passed
- Accelerated pace of technology innovation: initiating the Future Challenges Defense Technology Project

13

2. Changes in the Defense Technology Landscape

■ Defense Innovation by Major Advanced Countries (2'43")

14

3. Examples of Advanced Technology Application

15

3. Examples of Advanced Technology Application

■ The United States Marine Corps

The U.S. Marine Corps is developing new strategies by applying new technology

무게 1lb 미만, 1km 이상 비행 가능

M134미니건 장착, 분당 최대 6천발 사격 가능

모듈식 점단 로봇 무기 시스템
400발 탄환 실고 이동 가능, 40mm 폭탄 투척기 설치 가능

(Source: DMA, etc.)

16


3. Examples of Advanced Technology Application
Advanced IoT-Based Unmanned Guard System
Iron-clad defense with just a few people!
Previous guard personnel can be redeployed as combat troops
17


3. Examples of Advanced Technology Application
China's Unmanned Amphibious Combat Vehicle
Speedy landings reduce casualties!
18

3. Examples of Advanced Technology Application

■ Autonomous Platooning System

Arming unmanned autonomous platooning systems and operating transport vehicles with just a few people

19

3. Examples of Advanced Technology Application

■ The U.S. Unmanned Helicopter (MQ-8 Fire Scout)

Provided firepower support and collected information without any casualties!

20

3. Examples of Advanced Technology Application

■ UAM

Performed operations without any spatial constraints!

21

3. Examples of Advanced Technology Application

■ Drone Killers

Incapacitates adversaries' surveillance and use of drones!

22

3. Examples of Advanced Technology Application

■ Stealth Armored Vehicles

Infiltrates without being detected and overpowers adversaries with immense firepower!

23

3. Examples of Advanced Technology Application

■ Satellite Weapons

Save Earth in space!

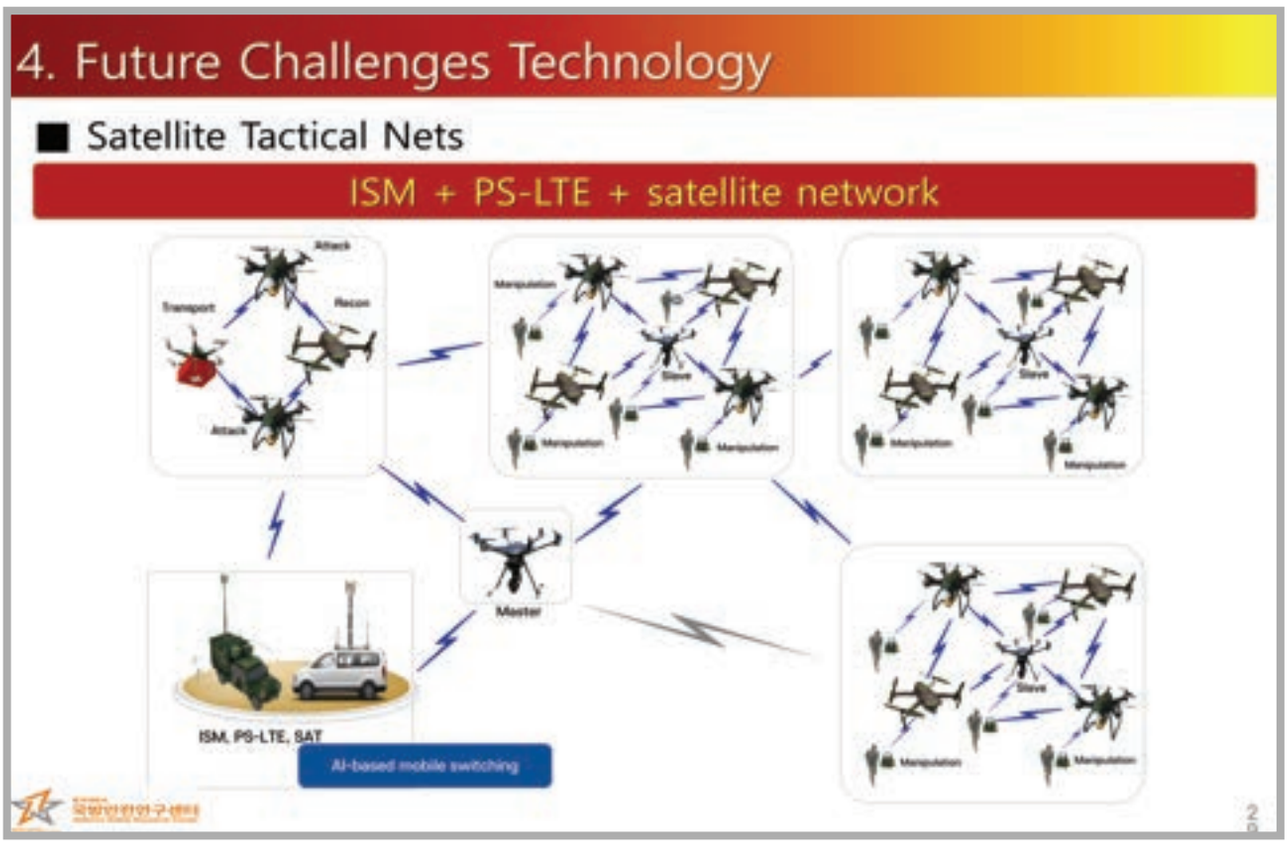
24

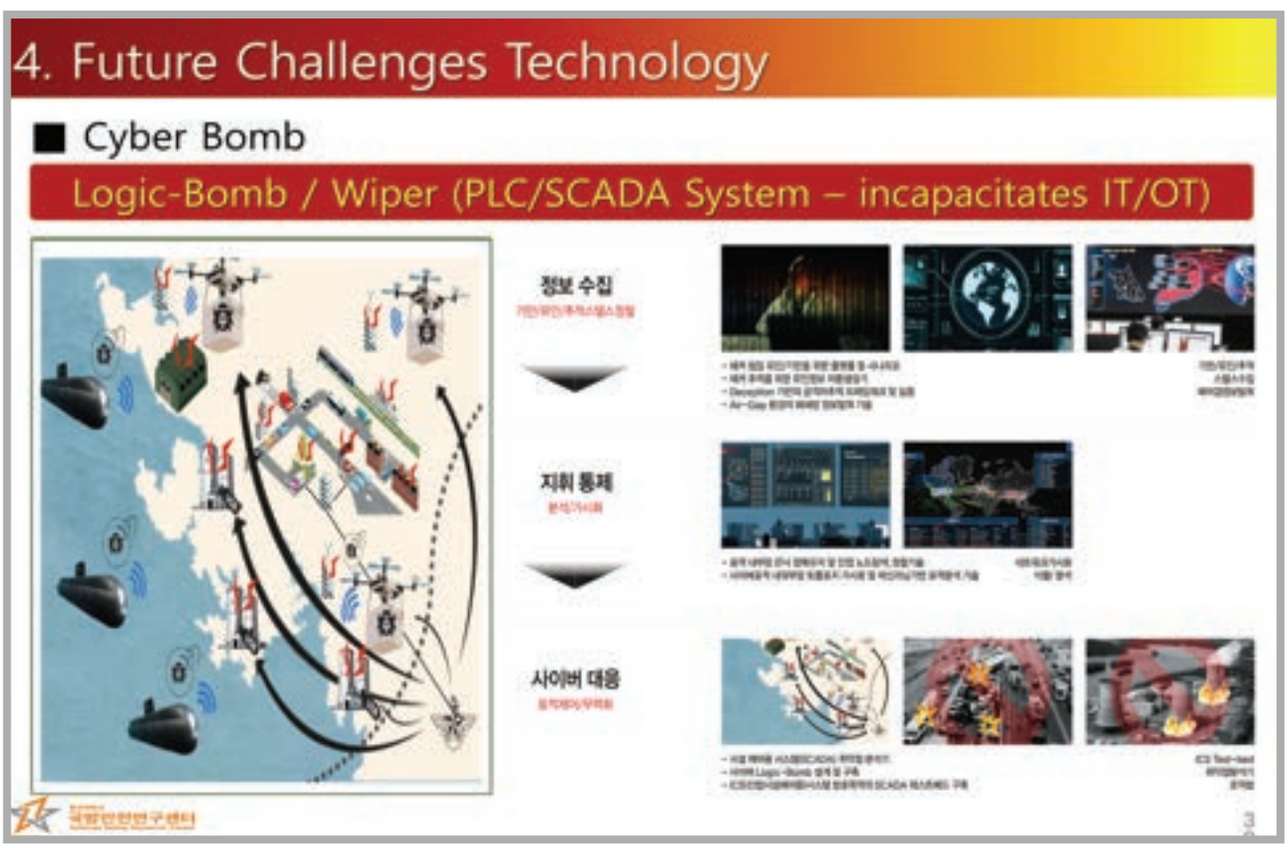

3. Examples of Advanced Technology Application
Starlink
Construction of a tactical net in space that connects the whole world!
25

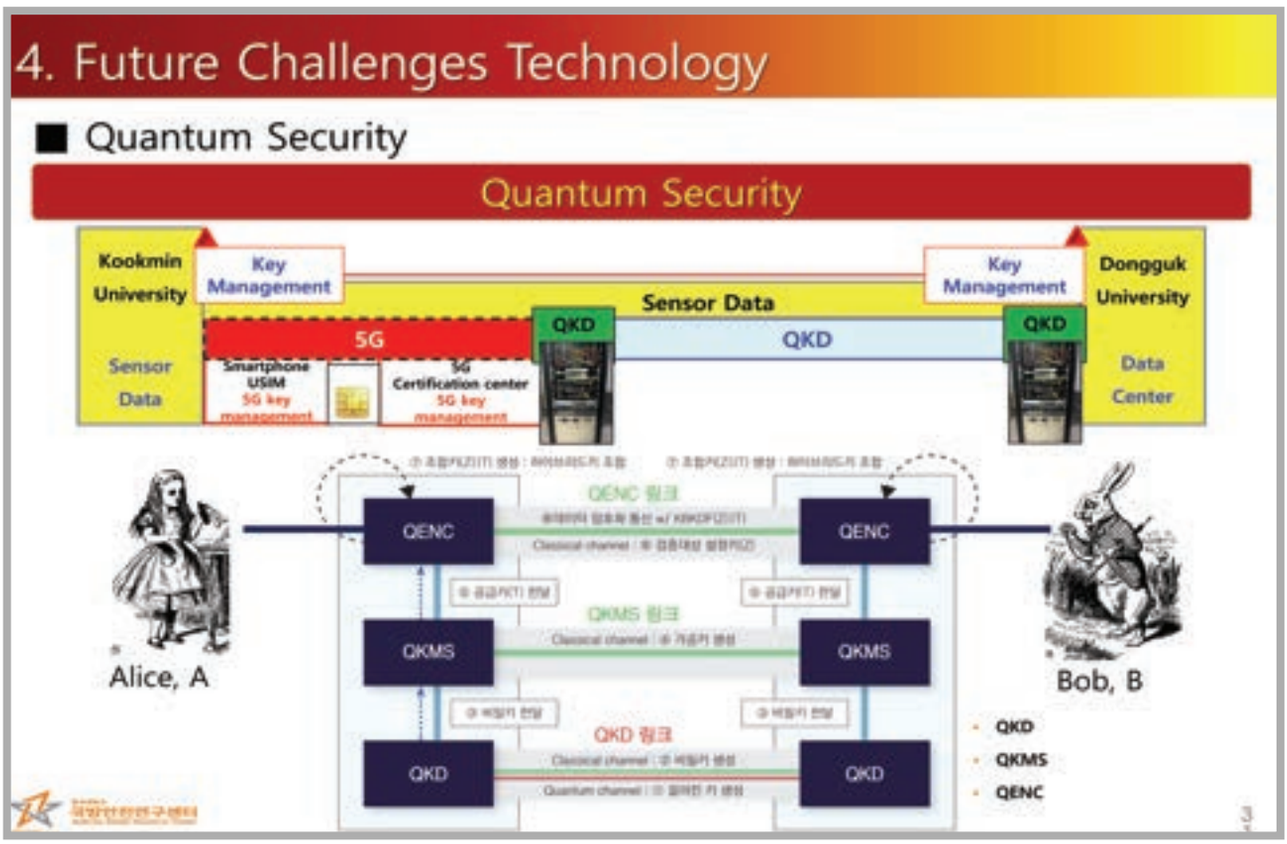

4. Future Challenges
Technology
26

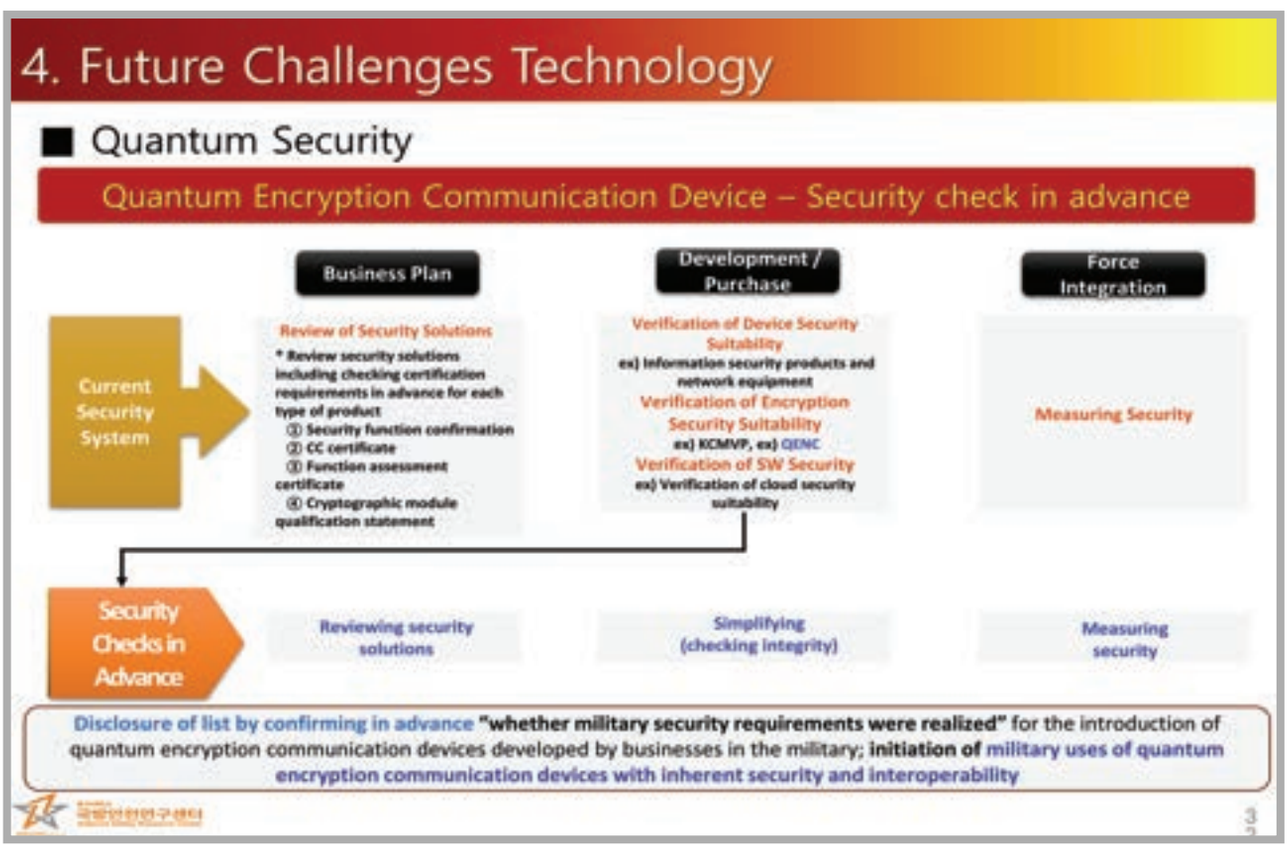

4. Future Challenges Technology
3D Printers
Food supply is key to winning wars! Resolved through 3D food printing!
Winning a war is impossible without food!
Advantages in 3D food printing
Small size and portable
Minimizes the volume of food
Food ingredients can be made into cartridges
Can be printed while traveling to and after settling in the supply location
Can be moved at night and provide nutritious food to boost combat power
Boosts combat power by reinforcing soldiers' health
Streamlines food supply capacity in remote places
3D food printing
Supplies food on the move
(Source: New Scientist, The Netherlands)
Can be used in isolated locations where food supply is difficult
Modern warfare
Namhansan seong Fortress (lack of food)
Napoleon (Invention of canned food)
War in isolated areas (3D food Printing)
Defeat
Victory
Victory
27

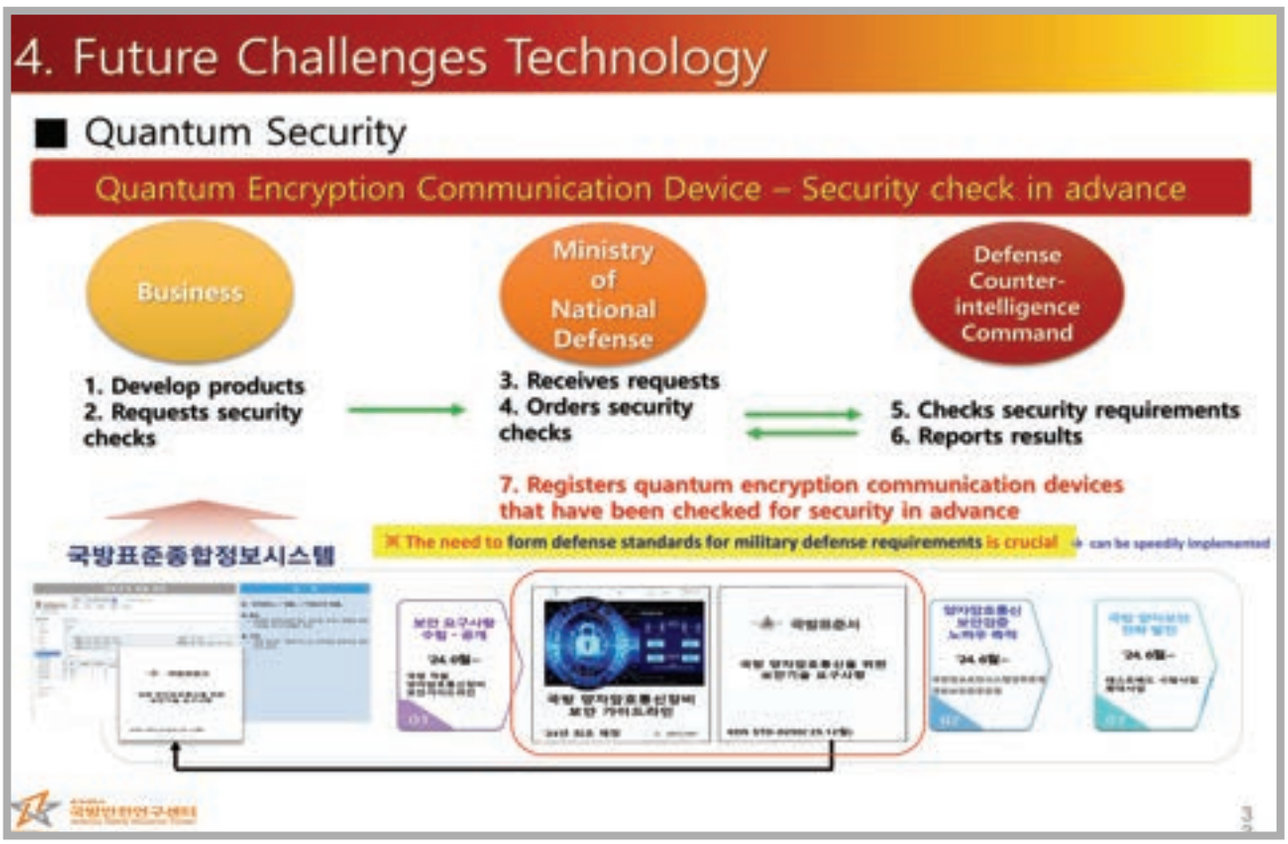

4. Future Challenges Technology
3D Printers
Safe food fiber filters!!!
Winning a war is impossible without protection!
Uses food materials proven safe for the human body to consume
Can utilize bio-materials to respond to biochemical terrorism
Aromatherapy to elevate troops' combat power and treat trauma
Filter materials can be made into cartridges
Combat power can be maintained in emergencies through filters' self-restoration functions
Present
Uncomfortable to wear
Canisters need to be replaced
Difficult to breathe
Uncomfortable in combat
Future
Personal protective equipment with built-in filter regenerator
Easy to wear
Filters don't need to be replaced
Easy to breathe
Comfortable in combat
Can be used as liniment for wounds in emergencies
Replaceable filter cartridges
Attachable filter equipment
Built-in filter
Fans to supply oxygen
Replaceable filters
Principle: contact reciprocating
28


4. Future Challenges Technology
Satellite Tactical Nets
ISM + PS-LTE + satellite network
Attack
Transport
Recon
Attack
Manipulation
Manipulation
Manipulation
Slave
Slave
Manipulation
Manipulation
Master
Slave
Manipulation
Manipulation
ISM, PS-LTE, SAT
AI-based mobile switching


4. Future Challenges Technology
Cyber Bomb
Logic-Bomb / Wiper (PLC/SCADA System – incapacitates IT/OT)
정보 수집
지휘 통제
사이버 대응


4. Future Challenges Technology
Quantum Security
Quantum Security
Kookmin University
Key Management
Sensor Data
5G
Smartphone USIM 5G key management
5G Certification center 5G key management
QKD
Sensor Data
QKD
Key Management
Dongguk University
Data Center
QENC
QKMS
QKD
Alice, A
Bob, B
QKD
QKMS
QENC


4. Future Challenges Technology
Quantum Security
Quantum Encryption Communication Device – Security check in advance
Business Plan
Development / Purchase
Force Integration
Current Security System
Review of Security Solutions
* Review security solutions including checking certification requirements in advance for each type of product
① Security function confirmation
② CC certificate
③ Function assessment certificate
④ Cryptographic module qualification statement
Verification of Device Security Suitability
ex) Information security products and network equipment
Verification of Encryption Security Suitability
ex) KCMVP, ex) QENC
Verification of SW Security
ex) Verification of cloud security suitability
Measuring Security
Security Checks in Advance
Reviewing security solutions
Simplifying (checking integrity)
Measuring security
Disclosure of list by confirming in advance "whether military security requirements were realized" for the introduction of quantum encryption communication devices developed by businesses in the military; initiation of military uses of quantum encryption communication devices with inherent security and interoperability


4. Future Challenges Technology
Quantum Security
Quantum Encryption Communication Device – Security check in advance
Business
Ministry of National Defense
Defense Counter-intelligence Command
1. Develop products
2. Requests security checks
3. Receives requests
4. Orders security checks
5. Checks security requirements
6. Reports results
7. Registers quantum encryption communication devices that have been checked for security in advance
※ The need to form defense standards for military defense requirements is crucial
국방표준종합정보시스템


4. Future Challenges Technology
AI-based System for Operating Battlefield Situations and Command Decisions
Automated analysis of combat forces with AI!
Provides immediate command decision support in battlefield situations
TAIWAN
PHILIPPINES

5. Conclusion

35

5. Conclusion

■ Changes in the duties of national armed forces due to expanded scope of security

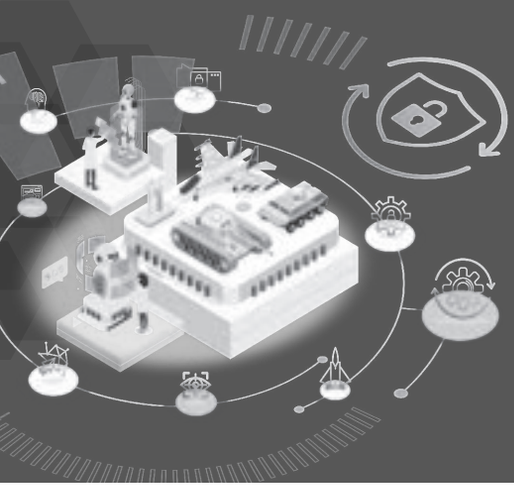
Battlefields are expanded to include space and cyberspaces!!

- ROK is perpetually at a security crisis due to its geopolitical position
- Consistent decline in number of troops and improved military powers in neighbor countries
- Neighbor countries are intensively boosting their air force and navy
  → Major countries are boosting their space and cyber combat powers
- In modern warfare, large-scale threats increase as a result of developments in advanced weapons
  → New types of wars occur

In the future battlefields will be expanded to space and cyberspace as well as land, sea, and air; high-tech future forces are necessary to operate response strategies and combat!

Developing "Future Challenges Technology," with advanced technology such as AI-ICBM, Cyber-Bombs, and Quantum Security is the top priority to defend the Korean peninsula!


Thank you!
Defense Security Research Center / Division of AI Software Convergence,
Dongguk University
Director / Prof. Jin-ho Park
gomalove@hanmail.net
37



주제발표 2.

방산기술보호 등급분류 및 조치를 위한 평가방법

Assessment Method for Classification and Measures in Defense Technology Security

광운대학교 방위사업학과 교수 I **정석재**
Professor, Department of Defense Acquisition Program, KwangWoon University
Prof. Sukjae Jeong

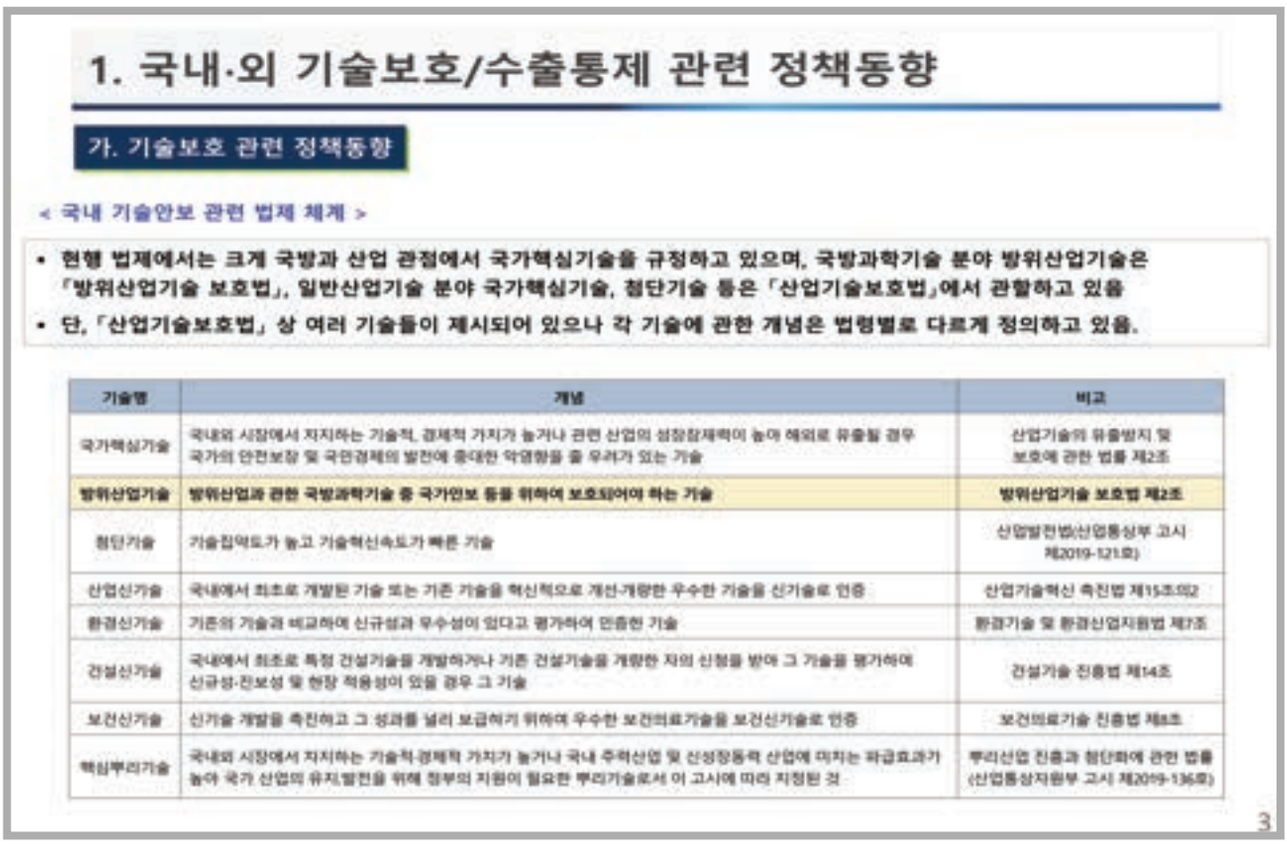
방산기술보호 컨퍼런스

방산기술보호 등급분류 및 조치를 위한 평가방법

2023. 08. 04

광운대학교 정 석 재

목 차



1. 국내·외 기술보호/수출통제 관련 정책동향

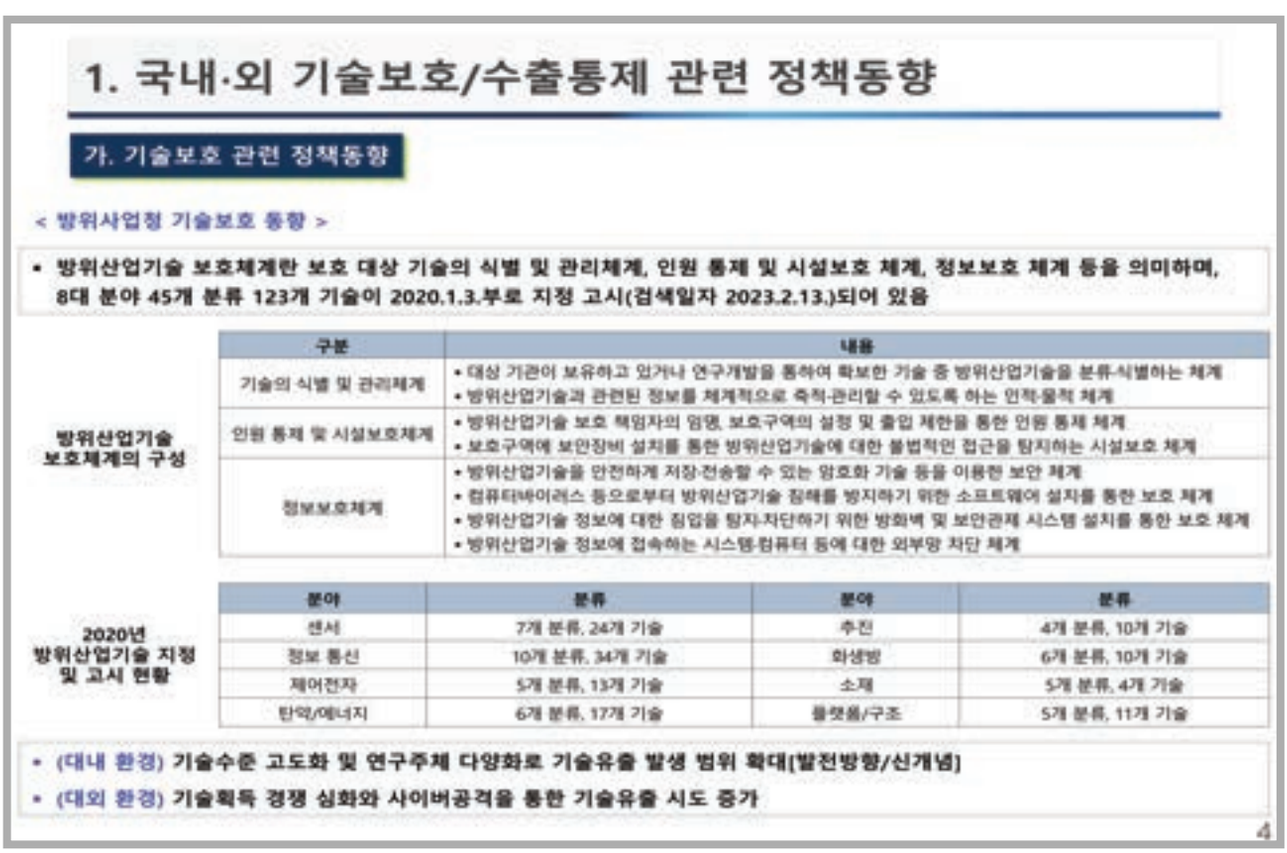
가. 기술보호 관련 정책동향

< 국내 기술안보 관련 법제 체계 >

- 현행 법제에서는 크게 국방과 산업 관점에서 국가핵심기술을 규정하고 있으며, 국방과학기술 분야 방위산업기술은 「방위산업기술 보호법」, 일반산업기술 분야 국가핵심기술, 첨단기술 등은 「산업기술보호법」에서 관할하고 있음
- 단, 「산업기술보호법」 상 여러 기술들이 제시되어 있으나 각 기술에 관한 개념은 법령별로 다르게 정의하고 있음.

기술명	개념	비고
국가핵심기술	국내외 시장에서 지지하는 기술적, 경제적 가치가 높거나 관련 산업의 성장잠재력이 높아 해외로 유출될 경우 국가의 안전보장 및 국민경제의 발전에 중대한 악영향을 줄 우려가 있는 기술	산업기술의 유출방지 및 보호에 관한 법률 제2조
방위산업기술	방위산업과 관한 국방과학기술 중 국가안보 등을 위하여 보호되어야 하는 기술	방위산업기술 보호법 제2조
첨단기술	기술집약도가 높고 기술혁신속도가 빠른 기술	산업발전법(산업통상부 고시 제2019-121호)
산업신기술	국내에서 최초로 개발된 기술 또는 기존 기술을 혁신적으로 개선·개량한 우수한 기술을 신기술로 인증	산업기술혁신 촉진법 제15조의2
환경신기술	기존의 기술과 비교하여 신규성과 우수성이 있다고 평가하여 인증한 기술	환경기술 및 환경산업지원법 제7조
건설신기술	국내에서 최초로 특정 건설기술을 개발하거나 기존 건설기술을 개량한 자의 신청을 받아 그 기술을 평가하여 신규성·진보성 및 현장 적용성이 있을 경우 그 기술	건설기술 진흥법 제14조
보건신기술	신기술 개발을 촉진하고 그 성과를 널리 보급하기 위하여 우수한 보건의료기술을 보건신기술로 인증	보건의료기술 진흥법 제8조
핵심뿌리기술	국내외 시장에서 지지하는 기술적·경제적 가치가 높거나 국내 주력산업 및 신성장동력 산업에 미치는 파급효과가 높아 국가 산업의 유지·발전을 위해 정부의 지원이 필요한 뿌리기술로서 이 고시에 따라 지정된 것	뿌리산업 진흥과 첨단화에 관한 법률 (산업통상자원부 고시 제2019-136호)

3



1. 국내·외 기술보호/수출통제 관련 정책동향

가. 기술보호 관련 정책동향

< 방위사업청 기술보호 동향 >

- 방위산업기술 보호체계란 보호 대상 기술의 식별 및 관리체계, 인원 통제 및 시설보호 체계, 정보보호 체계 등을 의미하며, 8대 분야 45개 분류 123개 기술이 2020.1.3.부로 지정 고시(검색일자 2023.2.13.)되어 있음

방위산업기술 보호체계의 구성

구분	내용
기술의 식별 및 관리체계	• 대상 기관이 보유하고 있거나 연구개발을 통하여 확보한 기술 중 방위산업기술을 분류·식별하는 체계 • 방위산업기술과 관련된 정보를 체계적으로 축적·관리할 수 있도록 하는 인적·물적 체계
인원 통제 및 시설보호체계	• 방위산업기술 보호 책임자의 임명, 보호구역의 설정 및 출입 제한을 통한 인원 통제 체계 • 보호구역에 보안장비 설치를 통한 방위산업기술에 대한 불법적인 접근을 탐지하는 시설보호 체계
정보보호체계	• 방위산업기술을 안전하게 저장·전송할 수 있는 암호화 기술 등을 이용한 보안 체계 • 컴퓨터바이러스 등으로부터 방위산업기술 정책을 방지하기 위한 소프트웨어 설치를 통한 보호 체계 • 방위산업기술 정보에 대한 침입을 탐지·차단하기 위한 방화벽 및 보안관제 시스템 설치를 통한 보호 체계 • 방위산업기술 정보에 접속하는 시스템·컴퓨터 등에 대한 외부망 차단 체계

2020년 방위산업기술 지정 및 고시 현황

분야	분류	분야	분류
센서	7개 분류, 24개 기술	추진	4개 분류, 10개 기술
정보 통신	10개 분류, 34개 기술	화생방	6개 분류, 10개 기술
제어전자	5개 분류, 13개 기술	소재	5개 분류, 4개 기술
탄약/에너지	6개 분류, 17개 기술	플랫폼/구조	5개 분류, 11개 기술

- (대내 환경) 기술수준 고도화 및 연구주체 다양화로 기술유출 발생 범위 확대[발전방향/신개념]
- (대외 환경) 기술획득 경쟁 심화와 사이버공격을 통한 기술유출 시도 증가

4

1. 국내·외 기술보호/수출통제 관련 정책동향

가. 기술보호 관련 정책동향

< 산업통상자원부 기술보호 동향 >

- 산업기술 유출로 인한 국가적인 손실을 직시하고 대상기관이 보유한 산업기술의 부정한 유출을 방지하고 산업기술을 보호함으로써 국내산업의 경쟁력을 강화하고 국가의 안전보장과 국민경제의 발전을 제고하기 위하여 산업기술보호지침 마련
- 국가핵심기술 종합관리시스템(www.nct.or.kr) 운영

국가핵심기술 보호현황

구분	반도체	디스플레이	전기·전자	자동차·철도	철강	조선
지정 현황	10개	2개	3개	9개	9개	8개
구분	원자력	정보·통신	우주	생명공학	기계	로봇
지정 현황	5개	7개	4개	4개	7개	3개
합계	총 12개 분야, 71개 기술이 '국가핵심기술'로 지정·관리됨					

국가핵심기술의 보호 및 관리를 위한 제공서비스

구분		내용
진단/컨설팅/인증	산업기술 확인제도	산업기술보호법에 따른 산업기술에 해당되는지 여부를 확인해주는 제도
	보안컨설팅	보안전문가가 현장을 방문하여 보안영역별 취약점을 점검함으로 써 보호대책과 개선방안을 제시
	보안 원터치 지원	국가핵심기술 보유 중견·중소기업 대상 보안진단 컨설팅, 모의해킹 등 사후지원
워크숍/세미나	산업기술 분쟁조정 세미나	기업의 기술유출·침해 분쟁에 대한 심각성을 알리고, 분쟁에 대한 대응방안으로서 조정제도 안내
	보안담당자 워크숍	보안담당자 간 기업보안 실무 정보교류 및 인적네트워크 구축 산진기업 벤치마킹 기회 제공 (국가핵심기술 보유기관 우대)
교육	CSO(Chief Security Officer) 양성교육	산업보안 전문 직무역량 강화를 위해 기업, 연구기관 보안 책임 자, 담당자를 대상으로 맞춤형 실무 심화교육 운영 (국가핵심기술 보유기관 우대)
	보안전담인력 대상 보안교육	국가핵심기술 보안전담인력의 직무능력 향상을 위한 맞춤형 교육과정 지원
기타	보안역량강화 지원사업	국가핵심기술 보유 중견기업 대상 보안설비 구축자금 지원 및 산업보안 컴플라이언스 구축 지원
	보안닥터 지원사업	국가핵심기술 보유기업 대상 보안역량 강화 및 인식전환을 위한 종합적인 지원

5

1. 국내·외 기술보호/수출통제 관련 정책동향

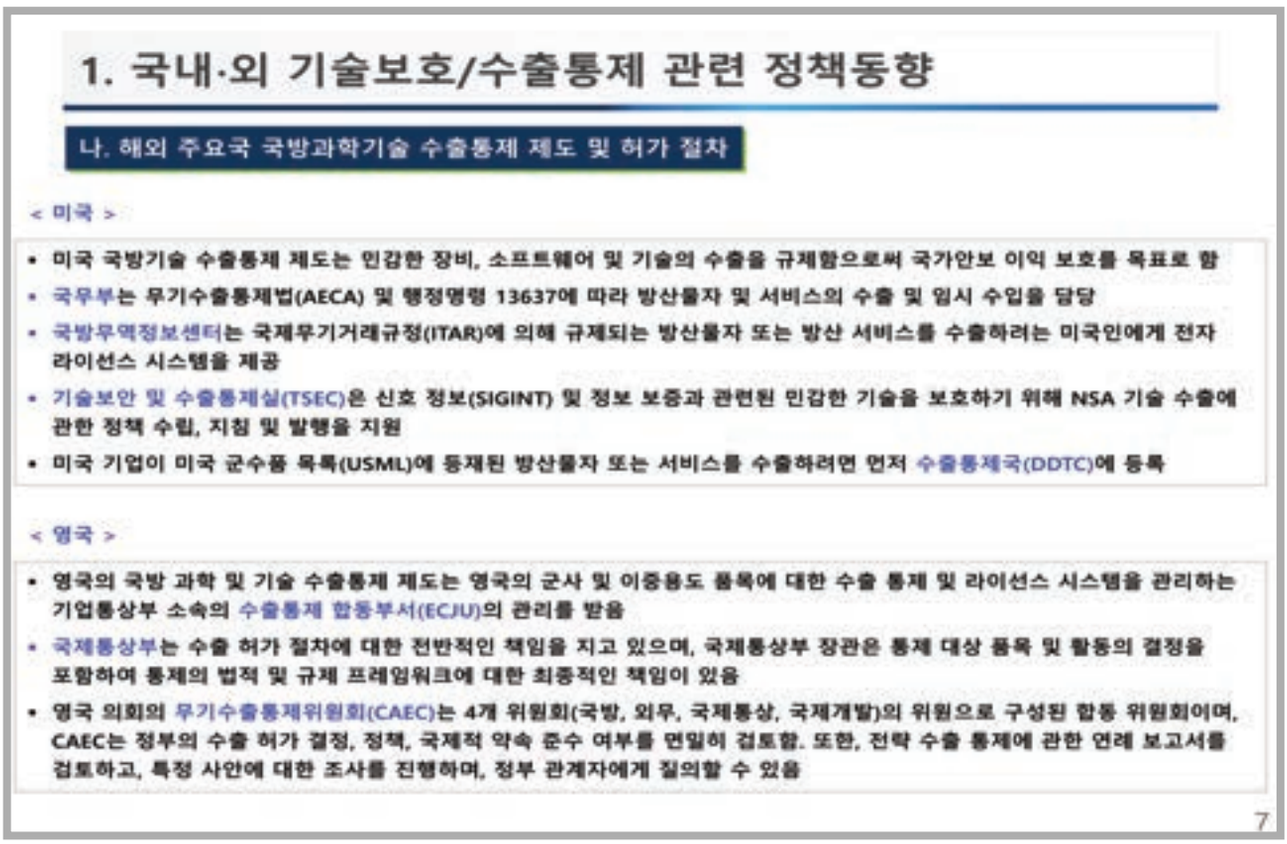
가. 기술보호 관련 정책동향

< 국외 기술보호 관련 정책동향 >

- 미국, 중국, 일본, 유럽 등 자국 기술보호를 위한 법령을 마련하고 있으며, 자체 조직을 신설하여 규제를 강화하고 있음

구분	내용
미국	• 미 국방부 안티탬퍼 정책 - 안티탬퍼 여부를 결정하는 프로세스는 프로그램 보호 계획(PPP)의 핵심기술(CPI) 식별부터 보호조치의 결정까지의 절차에 의해 진행되며, 핵심기술(CPI) 보호를 위해 안티탬퍼 적용 여부가 결정 • 방위산업기술 보호 관련 법령 · 제도 및 관련 조직 강화 - **(관련 법령)** 산업스파이 처벌 강화 및 기술경쟁국 대상 방위산업기술 유출 방지 - **(제도 강화)** 방위산업분야 국방조달 법령체계인 'DOD 5000 Series'를 통해 기술보호를 제도화하고, 국방 공급망내 방산업체 정보시스템에 있는 국방기밀 정보 침해에 대처하기 위해 '사이버보안 성숙도 모델인증(CMMC)' 제도 추진('20.1월) - **(조직 강화)** 국방안보서비스국(DSS)의 사이버위협 대응 대상을 기존 국방 관련 기관 이외 방산업체까지 확장하여 수행하기 위한 국방방첩보안국(DCSA) 창설('19.10월)
중국	• 인재 우대 정책으로 기술유출 방지 조치 - **(관련 법령)** 기존 외자 3법(외자기업법, 중외합자경영 기업법, 중외합작경영기업법)을 통합한 외국인투자법 전면시행('20.1월) - **(관련 정책)** 중국 내 고급인재 발탁 및 지원을 목표로 과학기술 분야의 국가적 인재 선발 및 양성 목표로 차세대 과학기술인재 육성
일본	• 해외 기술유출 방지 관련 제도 및 조직 강화 - **(관련 제도)** 기술유출방지를 위한 해외 연구자와의 공동연구 및 외국기업과의 연계에 대한 지침 및 가이드라인 마련을 위한 「제6기 과학기술혁신 기본계획」 수립('21.3월) - **(조직 강화)** '통합혁신전략 추진회의'(관방장관이 의장)에서 경제안보의 관점에서 중요 기술개발을 진행하면서 첨단기술 유출을 막기 위한 조사·분석 업무를 수행하는 싱크탱크 조직 신설('21.4월)
유럽	• "기술이전 통제 및 외국인 투자 심사제도 강화" - **(관련 규정)** 유럽에 외국에 대한 개방적인 투자체제를 유지하면서도 각국의 핵심기술 및 인프라 보호를 목적으로 'EU 외국인 심사 규정(EU FISR)을 제정('19.4월) • 국가별 업무 - **(영국)** 방위산업기술 보호 및 관리를 위해 수출 통제 방안으로 암호화, 보안장치 및 기타 보호기법의 사용을 통한 기술의 이전을 명시 - **(독일)** 대외경제법과 전쟁무기관리법 기반의 방위산업기술 보호 및 관리를 수행, 기존 부정경쟁방지법에서 분리하여 영업비밀보호법 제정('19.4월)

6



1. 국내·외 기술보호/수출통제 관련 정책동향

나. 해외 주요국 국방과학기술 수출통제 제도 및 허가 절차

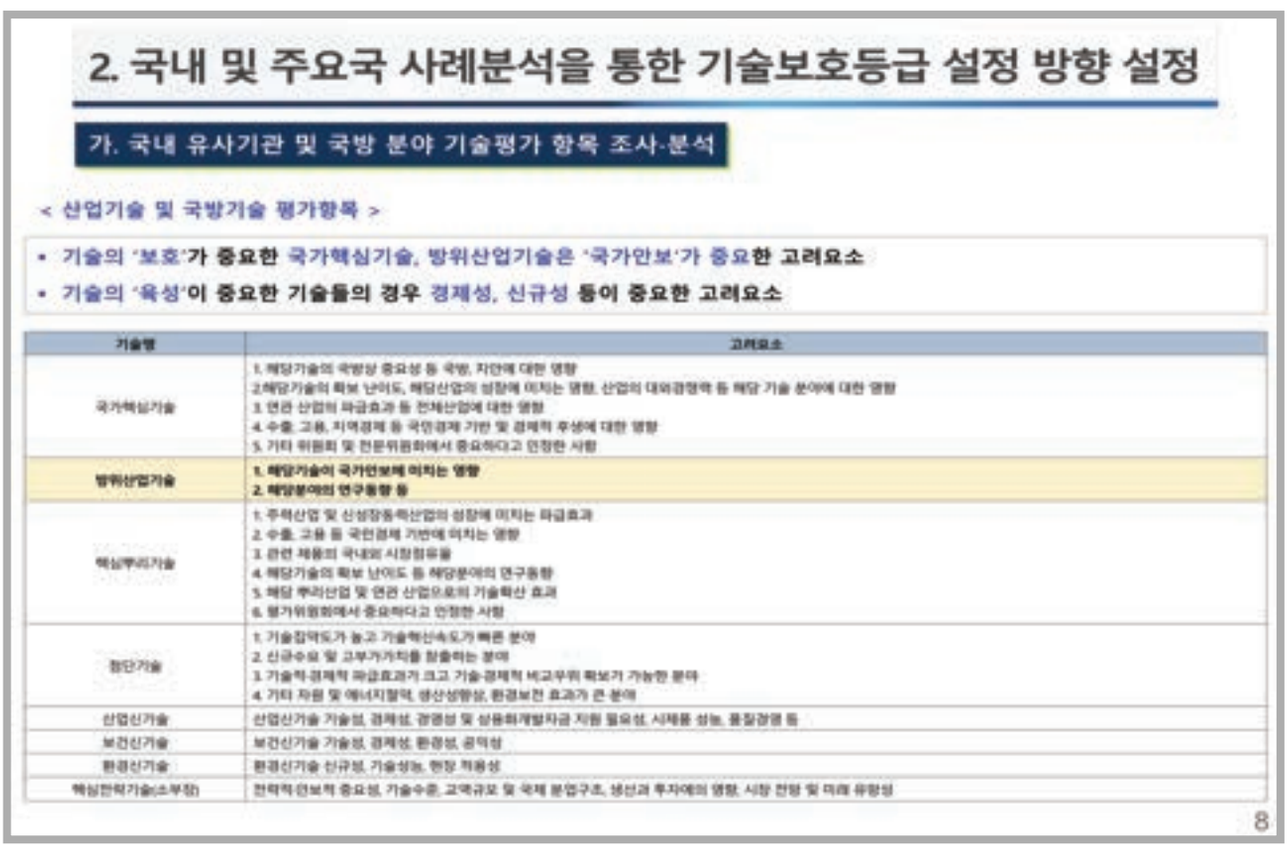
< 미국 >

- 미국 국방기술 수출통제 제도는 민감한 장비, 소프트웨어 및 기술의 수출을 규제함으로써 국가안보 이익 보호를 목표로 함
- 국무부는 무기수출통제법(AECA) 및 행정명령 13637에 따라 방산물자 및 서비스의 수출 및 임시 수입을 담당
- 국방무역정보센터는 국제무기거래규정(ITAR)에 의해 규제되는 방산물자 또는 방산 서비스를 수출하려는 미국인에게 전자 라이선스 시스템을 제공
- 기술보안 및 수출통제실(TSEC)은 신호 정보(SIGINT) 및 정보 보증과 관련된 민감한 기술을 보호하기 위해 NSA 기술 수출에 관한 정책 수립, 지침 및 발행을 지원
- 미국 기업이 미국 군수품 목록(USML)에 등재된 방산물자 또는 서비스를 수출하려면 먼저 수출통제국(DDTC)에 등록

< 영국 >

- 영국의 국방 과학 및 기술 수출통제 제도는 영국의 군사 및 이중용도 품목에 대한 수출 통제 및 라이선스 시스템을 관리하는 기업통상부 소속의 수출통제 합동부서(ECJU)의 관리를 받음
- 국제통상부는 수출 허가 절차에 대한 전반적인 책임을 지고 있으며, 국제통상부 장관은 통제 대상 품목 및 활동의 결정을 포함하여 통제의 법적 및 규제 프레임워크에 대한 최종적인 책임이 있음
- 영국 의회의 무기수출통제위원회(CAEC)는 4개 위원회(국방, 외무, 국제통상, 국제개발)의 위원으로 구성된 합동 위원회이며, CAEC는 정부의 수출 허가 결정, 정책, 국제적 약속 준수 여부를 면밀히 검토함. 또한, 전략 수출 통제에 관한 연례 보고서를 검토하고, 특정 사안에 대한 조사를 진행하며, 정부 관계자에게 질의할 수 있음

7



2. 국내 및 주요국 사례분석을 통한 기술보호등급 설정 방향 설정

가. 국내 유사기관 및 국방 분야 기술평가 항목 조사·분석

< 산업기술 및 국방기술 평가항목 >

- 기술의 '보호'가 중요한 국가핵심기술, 방위산업기술은 '국가안보'가 중요한 고려요소
- 기술의 '육성'이 중요한 기술들의 경우 경제성, 신규성 등이 중요한 고려요소

기술명	고려요소
국가핵심기술	1. 해당기술의 국방상 중요성 등 국방, 치안에 대한 영향 2.해당기술의 확보 난이도, 해당산업의 성장에 미치는 영향, 산업의 대외경쟁력 등 해당 기술 분야에 대한 영향 3. 연관 산업의 파급효과 등 전체산업에 대한 영향 4. 수출, 고용, 지역경제 등 국민경제 기반 및 경제적 주생에 대한 영향 5. 기타 위원회 및 전문위원회에서 중요하다고 인정한 사항
방위산업기술	1. 해당기술이 국가안보에 미치는 영향 2. 해당분야의 연구동향 등
핵심부리기술	1. 주력산업 및 신성장동력산업의 성장에 미치는 파급효과 2. 수출, 고용 등 국민경제 기반에 미치는 영향 3. 관련 제품의 국내외 시장점유율 4. 해당기술의 확보 난이도 등 해당분야의 연구동향 5. 해당 뿌리산업 및 연관 산업으로의 기술확산 효과 6. 평가위원회에서 중요하다고 인정한 사항
첨단기술	1. 기술집약도가 높고 기술혁신속도가 빠른 분야 2. 신규수요 및 고부가가치를 창출하는 분야 3. 기술적·경제적 파급효과가 크고 기술·경제적 비교우위 확보가 가능한 분야 4. 기타 자원 및 에너지절약, 생산성향상, 환경보전 효과가 큰 분야
산업신기술	산업신기술 기술성, 경제성, 경영성 및 상용화개발자금 지원 필요성, 시제품 성능, 품질경쟁 등
보건신기술	보건신기술 기술성, 경제성, 환경성, 공익성
환경신기술	환경신기술 신규성, 기술성능, 현장 적용성
핵심전략기술(소부장)	전략적·안보적 중요성, 기술수준, 고객규모 및 국제 분업구조, 생산과 투자에의 영향, 시장 전망 및 미래 유망성

8

2. 국내 및 주요국 사례분석을 통한 기술보호등급 설정 방향 설정

가. 국내 유사기관 및 국방 분야 기술평가 항목 조사·분석

< 핵심전략품목 평가항목 및 법제체계 및 정부정책상 선정기준 방향성 >

- 韓-日 무역갈등 이후 핵심전략품목 선정을 위한 분석기준으로 대체가능성, 기술수준, 특정국가 의존도 등 추가
- 법제체계 및 정부정책 고찰 결과를 통해, 국가 산업기술안보와 직결될 수 있는 기술 분야를 선정하기 위한 기준을 도출

100대 핵심전략품목 주요 분석기준

구분	분석 기준
안보/산업측면	외부 수급충격에 따른 국내 산업생산에 미치는 영향
대체가능성	국내외 대체생산 기업의 존재여부
기술수준	국내기업의 기술수준과 기술력 확보 가능성
특정국가 의존도	수입규모와 비중이 높은 품목
주력·신산업 연관	반도체, 자동차, 이차전지 등 주력·신산업 생산 연관성

법제체계 및 정부정책상 산업기술 관련 주요 선정기준

구분		주요 선정기준
법제체계	기술 보호	기술확보 난이도, 파급효과, 국가안보에 미치는 영향 등
	기술 육성 및 기술개발 장려·촉진	신규성, 경제성, 기술성, 현장적용성 등
정부정책	소재·부품·장비 경쟁력 강화 대책	대체가능성, 기술수준(기술확보 가능성), 특정국가 의존도, 주력·신산업 연관(파급효과) 등
산업기술안보 관련 기술 분야		기술적난이도, 대체가능성 및 기술확보 가능성, 산업적 가치

9

2. 국내 및 주요국 사례분석을 통한 기술보호등급 설정 방향 설정

나. 해외 주요국 국방분야 기술확보 및 관리 현황

- 미국, 영국, 프랑스 등 국방부에서는 무기체계 확보를 위해 필요한 핵심 기술 개발 전략 수립 및 제반 활동 수행
- 이를 위하여 국방과학기술 및 핵심기술에 대한 평가 전담 기관을 두고 있음

국가 및 기관		기술평가 항목
미국	국방기술정보센터 (DTIC)	• 미 국방부는 과학기술정보의 관리를 위해 '국방기술정보센터(DTIC)를 운영 - DTIC는 과학기술정보의 획득, 저장, 검색 및 배포를 위한 중앙집중식 국방 서비스로써 국방부의 연구, 개발, 공학 및 연구 과제를 지원하고 있으며, 국방관련 획득 기능을 지원
	국방부 (DARPA)	• 국방과학기술 조사방법/분석 프로세스 - QFD(Quality Function Deployment)를 활용하여 국방검토보고서(QDR : Quadrennial Defense Review) 또는 국방전략서(NDS : National Defense Strategy)의 우선순위항목과 과학기술 매칭
	공군 (USAF)	• 미 국방성 및 공군의 군사력 비전에 맞는 무기체계 및 과학기술 분야를 분류 - QFD(Quality Function Deployment)를 활용하여 미 공군의 무기체계의 우선순위항목 과학기술분야 매칭
영국	국방부 (DCDC 센터)	• 2015년에 'The Future Operating Environment 2035'가 발간되었으며, 해당 보고서에서는 미래 국방 과학기술예측을 위해 트렌드 분석을 위한 지표를 활용하고 있음. - 과거 데이터 분석, 차이점 확인, 주제 선정, 분류 및 분석과 맵핑, 초안 작업에 대한 컨설팅 등의 과정을 거침 - DCDC 미래 예측 분석의 특징은 트렌드 위주의 분석과 국외 전문가 및 기관 등의 다양한 견해 포함
프랑스	국방부 (병기본부(DGA)	• 병기본부(DGA)는 합참과 동등한 위상으로 독립적인 무기체계 획득 계획 및 추진과 미래 방위체계 구축을 준비 - 전문기술국(DET)에서 주관하여 추진하는 기술 조사는 통상 요구능력이나 새롭게 추구하고자 하는 기술 분야 방향과 연관하여 전문가 주도로 진행되며, 기술조사결과는 TRL 수준으로 분류하여 국방기술조사 전략계획에 포함

10

2. 국내 및 주요국 사례분석을 통한 기술보호등급 설정 방향 설정

나. 해외 주요국 국방분야 기술확보 및 관리 현황

< 미국의 국방과학기술 정보 분류 >

- DoDI 3200.12에 의하면 연구개발을 통해 획득한 과학기술 정보를 STI(Scientific Technical Information)로 정의
- 국방부 내부 및 외부에서 수행된 과학기술 사업(기초연구, 응용연구, 고급 기술개발, 조사 분석 등)에서 생산되는 모든 문서와 데이터는 반드시 국방기술정보센터(Defense Technical Information Center, DTIC)에 저장
- STI는 기밀 정보, 통제 기술 정보, 일반 정보로 분류하는데, 기밀 정보는 ① Top Secret, ② Secret, ③ Confidential로 구분
- 기밀이 아닌 정보는 배포등급 A~X 중 하나를 표시해야 함

STI의 배포등급 분류

배포 등급	배포 범위
A	일반 공개
B	미국정부기관
C	미국정부기관 및 그 계약자에 배포
D	미 국방부 및 그 계약자에 배포
E	미 국방부 기관에만 배포
F	미 국방부 또는 상위 기관의 지시에 의해서만 배포
X	수출통제 기술자료, 미국 정부기관과 승인 받은 개인 또는 업체에게 배포

배포등급 예시 (DoDI 5230.24)

구분	정의	배포등급
핵심 기술 (Critical Technology)	미국을 포함한 어떤 국가의 군사 잠재력에 중요한 기여를 할 수 있는 제품 또는 서비스의 설계, 개발, 생산, 운용, 응용 또는 유지 관리에 필수적인 기술 정보	- 배포등급 B~F - 수출 통제
직접 군사 지원 (Direct Military Support)	미국, 다른 국가 또는 미국-외국 공동 프로그램의 기술적 또는 군사적 이익에 피해를 줄 수 있는 수출 통제 기술 정보	- 배포등급 E, F
시험 평가 (Test and Evaluation)	유출 시 제품의 업체에 불이익을 줄 수 있는, 상업용 제품 또는 군사용 하드웨어의 시험 평가 결과	- 배포등급 B, E, F

11

3. 기술보호등급 설정을 위한 평가항목 설계

[1단계] 타 기관 조사항목 검토

(평가항목 설계 1단계) 타 기관 조사항목 문헌 조사 및 분석

평가항목 그룹	시사점	부서/기관
기술수준	• 기술수준평가 사례의 주 목적이 되는 평가항목 • 국방 분야에서는 기술수준을 5단계로 구분하고 있으나 민간 분야에서는 4단계(선도, 추격, 후발, 낙후)로 구분하는 것이 일반적 (단, 단계별 기준은 상이) • ICT 기술수준조사(IITP)는 다른 사례와 다르게 1차 설문에서 기술수준 등급만 평가하고, 2차 설문에서 1차 결과를 토대로 기술수준(%)을 부여	국가핵심기술(산자부) 핵심전략기술(산자부) 7개 기술수준평가 사례
기술격차	• 기술수준평가 사례에서만 활용된 평가항목 • 해당기술의 최고기술 보유국과 그 국가와의 시간적 기술격차를 조사	6개 기술수준평가 사례 (KIAT 제외)
최고기술		7개 기술수준평가 사례
기술동향	• 국가지정기술, 기술수준평가 사례 모두 활용 • 기술수준평가 사례에서는 해당기술의 수준이 시간적으로 혹은 타 국가와 비교할 때 경향성이 어떠한지 조사	범위산업기술(기술동향) 국가첨단전략기술(산자부) 핵심부리기술(산자부) ICT 기술수준조사(IITP) 산업기술 수준조사(KEIT)
중요도	• 국가지정기술, 기술수준평가 사례 모두 활용 • 해당기술이 산업적으로 혹은 무기체계의 기능/성능이나 상위기술을 수행하는데 있어서 차지하는 중요성을 조사	국가첨단전략기술(산자부) 해양수산 기술수준평가(KIMST) ICT 기술수준조사(IITP) 산업기술 수준조사(KEIT) 국방과학기술조사(KRIT)
난이도	• 국가지정기술 사례에서 추로 평가되었으며, 기술수준평가에서는 국방과학기술조사만 활용 • 해당기술을 확보 혹은 연구하는데 난이도를 조사	국가핵심기술(산자부) 국가첨단전략기술(산자부) 핵심부리기술(산자부) 국방과학기술조사(KRIT)

12

3. 기술보호등급 설정을 위한 평가항목 설계

[1단계] 타 기관 조사항목 검토

(평가항목 설계 1단계) 타 기관 조사항목 문헌 조사 및 분석

평가항목 그룹	시사점	부서/기관
안보 영향도	• 국가지정기술 사례에서만 활용된 평가항목 • 해당기술이 국가·산업·경제의 안보에 미치는 영향, 국방상 중요성 등을 조사	국가핵심기술(산자부) 핵심전략기술(산자부) 국가첨단전략기술(산자부) 국가전략기술(과기부) 방위산업기술(국방부)
연관기술(산업) 영향도	• 국가지정기술, 기술수준평가 사례 모두 활용 • 국가지정기술의 경우 해당기술이 해당산업 혹은 연관산업으로 미치는 파급·확산효과를 조사 • 기술수준평가 사례의 경우 해당기술이 타 기술의 개발 및 활용에 미치는 영향도를 조사	국가핵심기술(산자부) 핵심전략기술(산자부) 핵심뿌리기술(산자부) 국가전략기술(과기부) 국토교통 기술수준 분석(KAIA) 산업기술 수준조사(KEIT)
시장 현황	• 국가지정기술 사례에서만 활용된 평가항목 • 해당기술이 속한 시장의 미래 유망성과 국내외 시장점유율을 조사	핵심전략기술(산자부) 핵심뿌리기술(산자부) 국가전략기술(과기부)
경제 영향도	• 국가지정기술 사례에서만 활용된 평가항목 • 해당기술이 수출·고용·지역경제 등 국민경제에 미치는 영향을 조사	국가핵심기술(산자부) 국가첨단전략기술(산자부) 핵심뿌리기술(산자부)
국제관계	• 국가지정기술 사례에서만 활용된 평가항목 • 해당기술의 고액규모, 국제 분업구조, 외교상황 등을 조사	핵심전략기술(산자부) 국가전략기술(과기부)

13

3. 기술보호등급 설정을 위한 평가항목 설계

[2단계] 델파이 기법을 통한 검토 가능한 추가 항목 도출

- **델파이 기법은 미국 RAND 연구소에서 개발된 기법으로 전문가 집단의 의견을 하나의 의견으로 수렴하는 과정**
- **타 기관으로부터 출처된 조사항목의 변경 및 삭제, 신규 평가항목 추가 등을 검토하기 위해 전문가들에게 개방형 설문과**
  폐쇄형 설문을 반복하여 합의를 도출하는 과정을 진행할 계획
  - 연구의 안정성 및 설문 횟수를 객관적으로 판단하기 위해 표준편차를 산출평균으로 나눈 값인 변이계수(CV, Coefficient of Variance)가 사용되며 일반적으로 CV가 0.5이하인 경우에 라운드를 종료하고 추가 설문을 하지 않음
  - 0.5~0.8인 경우 비교적 안정적으로 전문가 합의가 이루어진 것으로 판단하며, 0.8이상인 경우 추가 설문조사를 수행할 필요가 있다고 판단함

[3단계] 요인분석을 통한 유사평가항목 군집화 및 항목별 계층구조 확정

- **요인분석은 다변량 자료의 통계적 분석의 가장 대표적인 방법으로 평가항목(변수)간의 상호관련성을 분석하고 공통적으로 내재된 요인을 새로이 추출하는 통계적 방법**
  - 여러 변수들 사이에 내재된 특성을 최대한 활용하여 전체자료를 대표하면서도 적은 수의 요인으로 요약 및 구조화하는 것이 요인분석의 가장 큰 목적
- **델파이 기법으로 도출된 평가지표 간 내재된 공통요인의 특성 및 수가 명확하지 않고, 평가지표들을 동일한 요인으로 분류 및 구조화하기 위해 탐색적 요인분석(Exploratory Factor Analysis)을 적용**
- **요인분석을 통해 구조화 및 계층화된 평가지표는 향후 각 기술보호등급 평가지표별 가중치를 도출하는데 활용**

14

4. 보호등급 설정을 위한 전문가 평가

가. 기술분야별 전문가 평가를 반영한 요소기술별 기술보호등급 설정

< 기술분야별 전문가 평가 시 신뢰성 확보 >

- **전문가 설문 응답 시 "응답의 확신도" 반영**
  - 확신도 응답은 5점 척도의 등간척도로 입력
  - 확신도가 3미만은 삭제, 확신도가 3이상 응답에 대해서는 확신도를 반영한 가중평균값을 반영

15

5. 기술보호등급 분류(세분화) 방법

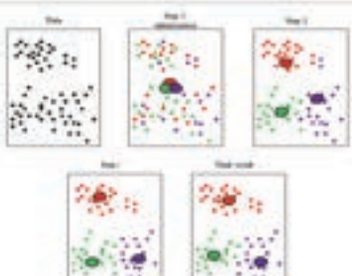
가. 기술보호등급 분류(세분화) 방안

< K-NN 알고리즘 >

- K-NN 알고리즘은 데이터를 가장 가까운 속성에 따라 분류하여 레이블링하는 알고리즘
- 거리에 기반하여 속성의 가까움을 측정하며, 상대적으로 거리가 더 짧은 이웃이 더 가까운 이웃으로 취급
- 즉, 어떤 새로운 데이터로부터 거리가 가까운 K개의 다른 레이블을 참고하여 빈도가 높게 나오는 레이블로 분류
- 주로 사용되는 거리 측정 방법은 다음과 같음
  - 유클리드 거리 : $d(A,B)=\sqrt{(x_2-x_1)^2+(y_2-y_1)^2}$
  - 맨해튼 거리 : $d(A,B)=|x_1-x_2|+|y_1-y_2|$

< K-Means 알고리즘 >

- K-Means 알고리즘은 비슷한 특성을 지닌 데이터들끼리 묶어 K개의 군집으로 구성하는 알고리즘
- 즉, 목표된 클러스터의 개수(K)에 도달할 때까지, 클러스터 중심을 계속 이동시키며 주어진 데이터를 군집화



16

5. 기술보호등급 분류(세분화) 방법

가. 기술보호등급 분류(세분화) 방안

< K-NN / K-Means 알고리즘의 비교 및 기술보호등급 분류 활용방안 >

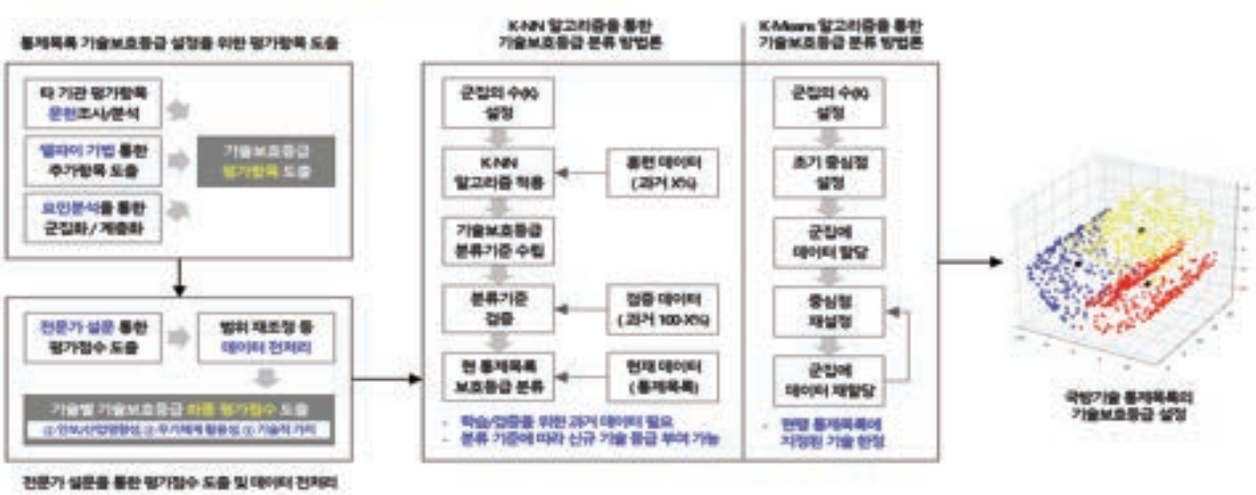
구분	K-NN 알고리즘	K-Means 알고리즘
공통점	• 데이터를 K개의 그룹으로 분류/클러스터링하는 것을 목표로 함. • 거리를 기반으로 구현되는 거리기반 분석 알고리즘	
학습데이터 필요 여부	• 입력 데이터(x)와 연관된 결과(y)가 존재하는 학습데이터가 필요함.	• 입력 데이터(x)만 필요하므로 학습데이터가 요구되지 않음.
과거데이터 필요 여부	• 과거 통제목록으로 지정된 기술의 입력 데이터(x)와 연관된 결과(y)가 요구되며, 이 중 일부는 학습데이터로 나머지는 검증데이터로 활용될 예정임.	• 학습데이터가 요구되지 않으므로 필요 없음.
기술보호등급 선지정 여부	• 과거데이터를 학습데이터로 활용하기 때문에 과거 분류된 기술보호등급을 유지할 필요가 있음. • 새로운 등급분류 필요시 과거데이터에 새롭게 지정할 등급을 부여하는 과정이 요구됨.	• 학습데이터가 요구되지 않으므로 필요 없음.
주요 목표	**• 과거 기술보호등급 데이터를 활용하여 등급분류 기준을 확립 • 분류 기준에 따라 신규 기술의 등급을 부여**	**• 현행 통제목록으로 지정된 기술 Pool에 한정하여 K-Means 알고리즘에 따라 등급을 분류**

17

5. 기술보호등급 분류(세분화) 방법

나. 기술보호등급 분류(세분화) 수행 절차

< K-NN/K-Means 방법론을 활용한 기술보호등급 세분화 절차>



18

Defense Technology Security Conference

Assessment Method for Classification and Measures in Defense Technology Security

2023. 08. 04

Sukjae Jeong, KwangWoon University

Table of Contents

1. Domestic and foreign policy trends regarding technology security and export control

A) Technology Security Policy Trends

< Domestic Technology Security Legal System >

- **Current law regulates national core tech. largely in terms of national security and industry**
- **Defense industry tech. in the field of national science tech. is under the jurisdiction of the "Defense Technology Security Act,"**
- **National core technology in the field of the general industry and advanced tech. are under the jurisdiction of the "Act on Prevention of Divulgence and Protection of Industrial Technology"**
- **The concept pertaining to each technology is defined differently in each ordinance.**

Type	Concept	Notes
National Core Technology	Technology that has high technological and economic values in the Korean and overseas markets or brings high growth potential to its related industries and which may exert a significantly adverse effect on national security and the development of the national economy in the event that it is divulged abroad	Article 2 of the Act on Prevention of Divulgence and Protection of Industrial Technology
Defense Technology	**Technology requiring protection for national security, etc., among the defense science and technologies related to the defense industry**	**Article 2 of the Defense Technology Security Act**
Advanced Technology	Technology with a high level of technological intensity and high-speed technological innovation	Industrial Development Act (Announced by MOTIE, 2019-121)
New Excellent Technology	New technology domestically developed for the first time or an excellent technology developed by innovatively improving or ameliorating existing technologies	Article 15-2 of the Industrial Technology Innovation Promotion Act
New Environmental Technology	Technology that has been certified as having novelty and excellence compared with the existing technology	Article 7 of the Environmental Technology and Industry Support Act
New Construction Technology	Where the Minister of Land, Infrastructure and Transport, upon receipt of an application for evaluation from a person who has first developed any construction technology in Korea or who has improved any existing construction technology, evaluates the relevant construction technology and then finds that it has novelty, progressiveness, and field applicability, he or she may designate it as a new construction technology	Article 14 of the Construction Technology Promotion Act
New Excellent Technology in Health	certify superior technology in health and medical services as new excellent technology in order to promote development of new technology and to widely disseminate the achievement	Article 8 of the Health and Medical Service Technology Act
Core Ppuri Technology	A ppuri technology certified by this promulgation that requires government support for the maintenance and development of national industries due to its high technical and economic value in domestic and foreign markets or its great ripple effect on major domestic industries and new growth engine industries	Act on Promotion and Sophistication of Ppuri Industries (Announced by MOTIE, 2019-136)

5

1. Domestic and foreign policy trends regarding technology security and export control

A) Technology Security Policy Trends

< Technology Security Trends of DAPA >

- **A defense technology protection system refers to the identification and management system of protected technologies, personnel control and facility protection system.**
- **123 technologies of 45 classifications and 8 sectors are designated as such (search date 2023.2.13.).**

Organization of defense technology protection system

Classification	Description
Technology Identification and Management System	• A system of classifying and identifying defense technology among the technologies that a target organization holds or has secured through R&D • A system of human and material resources that allows information related to data technology be systematically accumulated and managed
Personnel Control and Facility Protection System	• A personnel control system through the appointment of a defense technology protection officer, designating protected areas and restricting access • A facility protection system that detects illegal access to defense technology by installing security equipment in protected areas
Data Protection System	• A security system using encryption technology to safely store and transmit defense technology • A security system with software that prevents infringement of defense technology from computer viruses • A security system with firewalls and security control systems to detect and block invasion of defense technology • A system that blocks external networks of systems or computers accessing defense technology information

Status of defense technology designation and announcement in 2020

Sector	Classification	Sector	Classification
Sensor	7 classifications, 24 technologies	Propulsion	4 classifications, 10 technologies
Information and Communications	10 classifications, 34 technologies	CBR	6 classifications, 10 technologies
Control Electronics	5 classifications, 13 technologies	Material	5 classifications, 4 technologies
Ammunition/Energy	6 classifications, 17 technologies	Platform/Structure	5 classifications, 11 technologies

- (Domestic Environment) **Expansion of technology leakage range due to advanced technology and diverse research agents [Direction of development/new concept]**
- (External Environment) **Increase in technology leakage attempts through intensified competition over technology acquisition and cyberattacks**

4

1. Domestic and foreign policy trends regarding technology security and export control

A) Technology Security Policy Trends

< Technology Security Trends of MOTIE >

- **Established industrial technology protection guidelines to strengthen domestic industries' competition and enhance national security and economy by recognizing national losses from industrial technology leakage, preventing unauthorized leakage of industrial technology held by target organizations, and protecting industrial technology**
- **Runs the National Core Technology Comprehensive Management System (www.nct.or.kr)**

Protection Status of National Core Technology

Classification	Semiconductor	Display	Electricity/Electronic	Automobile/Railway	Steel	Shipbuilding
Designation Status	10	2	3	9	9	8
Classification	**Nuclear**	**ICT**	**Space**	**Bioengineering**	**Mechanics**	**Robotics**
Designation Status	5	7	4	4	7	3
Sum	71 technologies in 12 sectors are designated and managed as "National Core Technology"					

Provided Services for the Protection and Management of National Core Technology

Classification		Description
Diagnosis/ Consulting/ Certification	Industrial Technology Verification	An institution that identifies whether a technology is an industrial technology according to the Industrial Technology Protection Act
	Security Consulting	A security expert visits the site to examine vulnerabilities in each security aspect and suggests solutions
	One-Touch Security Support	Subsequent support such as security diagnosis consulting and mock hacking for SMEs possessing NCT
Workshops/ Seminars	Industrial Technology Dispute Mediation Seminar	A mediation system that informs of the severity of companies' technology leakage and infringement disputes, and which acts as a method of response to said disputes
	Security Officer Workshops	Provides opportunities to share practical information on corporate security among security officers, network, and benchmark leading companies (preferential treatment to NCT-holding organizations)
Training	CSO(Chief Security Officer) Training	Customized practical advanced training for security officers at companies and research institutions to enhance job competency of industrial security (preferential treatment to NCT-holding organizations)
	Security Training for Security Personnel	Customized training curriculum to enhance job competency of NCT security personnel
Etc.	Support to Enhance Security Capacity	Financial support to build security equipment and industrial security compliance for NCT-holding SMEs
	Security Doctor Support	Comprehensive support to enhance security capacity and raise awareness for NCT-holding companies

5

1. Domestic and foreign policy trends regarding technology security and export control

A) Technology Security Policy Trends

< Overseas Technology Security Policy Trends >

- **The U.S., China, Japan, and Europe are establishing laws to protect their technology, and enforcing regulations by newly establishing their own organizations**

Region	Description
U.S.	• DOD's Anti-Tamper Policies - Anti-tamper decision process is carried out under a procedure from identifying CPI in the PPP to determining protection measures, and whether or not anti-tamper will be applied is decided to protect CPI • Enhancement of Laws, Institutions, and Relevant Organizations regarding Defense Technology Protection - **(Relevant Laws)** Reinforcement of punishment for industrial espionage and prevention of defense technology leakage to technology competitors - **(Reinforcing Institutions)** Institutionalizing technology protection through "DOD 5000 Series," a defense industry national defense procurement legal system, and promoting "CMMC" system to respond to infringement of classified national defense information within the national defense supply chain's defense company data system (Jan. 2020) - **(Reinforcing Organizations)** Establishment of DCSA to expand DSS's cyber threat response targets to defense companies in addition to defense agencies (Oct. 2019)
China	• Technology Leakage Prevention Measures with Preferential Policies for Talented Personnel - **(Relevant Laws)** Full implementation of the Foreigner Investment Act, an integration of the existing 3 Foreign Capital Acts (Jan. 2020) - **(Relevant Policies)** Fostering next-generation science and technology talent with the goal of selecting, supporting, and training talented individuals in China
Japan	• Reinforcement of Overseas Technology Leakage Prevention Institutions and Organizations - **(Relevant Institutions)** Establishment of the "6th Basic Plan for Science and Technology Innovation" to prepare guidelines regarding technology leakage prevention in joint research with overseas researchers and foreign companies (Mar. 2021) - **(Reinforcing Organizations)** Establishment by the "Integrated Innovation Strategy Promotion Meeting" (chaired by The chief cabinet secretary) of a think tank to conduct research and analysis to prevent advanced technology leakage while developing critical technologies for economic security (Apr. 2021)
Europe	• "Controlling Technology Transfers and Reinforcing Foreigner Investment Evaluations" - **(Relevant Regulations)** Enactment of the EU FISR to protect core technologies and infrastructure while maintaining Europe's open investment system for foreigners (Apr. 2019) • In Each Country - **(UK)** Specifying technology transfer through the use of encryption, security devices, and other protective techniques as export control measures to protect and manage defense technology - **(Germany)** Protection and management of defense technology based on the Foreign Trade and Payments Act and the War Weapons Control Act, enactment of the Trade Secret Protection Act separately from the existing Unfair Competition Prevention Act (Apr. 2019)

6

1. Domestic and foreign policy trends regarding technology security and export control

B) Defense Science and Technology Export Control Systems and Licensing Procedures in Major Overseas Countries

< U.S. >

- The U.S. Defense Technology Export Control System aims to protect national security interests by regulating exports of sensitive equipment, software, and technology
- The Department of State is responsible for the export and temporary import of defense goods and services governed by the AECA and Executive Order 13637
- The Defense Trade Information Center provides an electronic licensing system to Americans seeking to export defense goods or services regulated by the ITAR
- TSEC supports policymaking, guidance, and issuance of NSA technology exports to protect sensitive technologies related to SIGINT and information assurance
- If a U.S. company wants to export defense goods or services listed on the USML, they must first register with the DDTC

< UK >

- The UK's Defence Science and Technology Export Control System is governed by the ECJU under the Department for Business and Trade, which manages the UK's export control and licensing system for military and dual-use items
- The Department for International Trade has overall responsibility over export licensing procedures, and the Minister of International Trade has final responsibility for the legal and regulatory framework of controls, including the determination of items and activities subject to control
- The British Parliament's CAEC is a joint committee comprised of members from four committees (defence, foreign affairs, international trade, and international development), which closely examines government export licensing decisions, policies, and compliance with international commitments. It also reviews annual reports on strategic export controls, conduct investigations on specific issues, and make inquiries to government officials.

7

2. Setting technology security levels and directions through a case analysis of Korea and other major countries

A) Research and Analysis of Technology Assessment Categories in Similar Korean Institutions and Defense Sectors

< Industrial and Defense Technology Assessment Categories >

- For NCT, "protection" is key, while for defense technology, "national security" is key
- For technologies where fostering is important, economic feasibility and novelty are important factors

Technology	Factors for Consideration
National Core Technology	1. Impact on national defense and security, such as the technology's importance for national defense 2. Impact on relevant technology sectors, such as the difficulty of technology procurement, the impact on the development of its industry, and the industry's external competitiveness 3. Impact on the entire industry, such as a ripple effect on related industries 4. Impact on the national economic base and welfare, such as exports, employment, and the local economy 5. Other matters recognized as important by the committee and the professional committee
Defense Technology	**1. The impact of the technology on national security** **2. Research trends in relevant fields, etc.**
Core Ppuri Technology	1. Ripple effect on the growth of major industries and new growth engine industries 2. Impact on the national economic base, such as exports and employment 3. Domestic and foreign market share of related products 4. Research trends in relevant fields, such as the difficulty of securing relevant technology 5. Technology diffusion effect on the relevant ppuri industry and other relevant industries 6. Matters recognized as important by the evaluation committee
Advanced Technology	1. Fields with high technological intensity and high speed of technological innovation 2. Fields that create new demand and high added value 3. Fields that have great technological and economic ripple effects and can secure comparative advantages in technology and economy 4. Other fields with great effect on resource and energy conservation, productivity improvement, and environmental conservation
New Excellent Technology	Level of technology, economic feasibility, business feasibility, need for commercialization development fund support, prototype performance, quality management, etc.
New Excellent Technology in Health	Level of technology, economic feasibility, environmental and public interest
New Excellent Technology in Environment	Novelty of technology, technological performance, field applicability
Core Strategic Technology (Material, Parts, Equipment)	Strategic and security significance, level of technology, size of trade and international division of labor, impact on production and investment, market prospects and future promise

8

2. Setting technology security levels and directions through a case analysis of Korea and other major countries

A) Research and Analysis of Technology Assessment Categories in Similar Korean Institutions and Defense Sectors

< Directions for evaluating criteria regarding key strategic item assessment categories, legal systems, and government policies>

- Replaceability, technology level, and reliance on certain countries **were added as** analysis criteria for selecting key strategic goods after the trade conflicts between Korea and Japan
- **Derive standards for selecting technology fields directly relatable to national industrial technology security through** reviewing the legal system and government policies

Major analysis criteria for 100 key strategic items

Classification	Analysis Criteria
Security/Industry	Impact of external supply and demand shocks on domestic industrial production
Replaceability	Presence of a domestic or foreign alternative producer
Technology Level	Technology level and acquisition possibility of domestic companies
Reliance on Certain Countries	Items of high import volumes and proportions
Relevance to Major and New Industries	Relevance to major and new industry production such as semiconductors, automobiles, and secondary batteries

Major analysis criteria for industrial technology in terms of legal system and government policies

Classification		Major Analysis Criteria
Legal System	Technology security	Difficulty in securing technology, ripple effect, impact on national security, etc.
	Promotion of fostering and developing technology	Novelty, economic feasibility, technicality, field applicability, etc.
Government Policies	Measures to strengthen competitiveness of materials, parts, and equipment	Replaceability, technology level (technology acquisition possibility), reliance on certain countries, relevance to major and new industries (ripple effects), etc.
Technology Sectors related to Industrial Technology Security		Technical difficulty, replaceability and technology acquisition possibility, industrial value

9

2. Setting technology security levels and directions through a case analysis of Korea and other major countries

B) Defense technology acquisition and management in major countries

- **Ministries of Defense in the U.S., UK, and France are establishing strategies to develop critical technology and working to secure weapon systems**
- **These countries have dedicated organizations for evaluating defense science technology and core technology**

Country and Organization		Technology Evaluation Standards
U.S.	DTIC	• The U.S. Department of Defense runs the DTIC to manage scientific technology information - The DTIC is a centralized defense service for the acquisition, storage, search and distribution of scientific technology information, and supports the DOD's research, development, and engineering tasks, as well as defense acquisition capacities
	DARPA	• Process of examining and analyzing defense scientific technology - Uses Quality Function Deployment to match scientific technology and priorities in the Quadrennial Defense Review or the National Defense Strategy
	USAF	• Classifies weapon systems and technology areas that fit the military visions of DOD and the Air Force - Matches priority items in the Air Force's weapon systems and scientific technology areas using Quality Function Deployment
UK	DCDC Center	• Released "The Future Operating Environment 2035" in 2015, which utilizes trend analysis indexes to predict future defense technology - Goes through a process of analyzing past data, identifying differences, selecting topics, classifying, analyzing, and mapping, and consulting on draft work - The DCDC's future prediction analysis includes a trend analysis and diverse opinions from international experts and organizations
France	Ministry of the Armed Forces (DGA)	• The Directorate General of Armaments (DGA) initiates and plans independent weapon system acquisition and prepares for constructing future defense systems, as an organization of equal rank as the Joint Chiefs of Staff - Technological surveys conducted by the DET are usually led by experts in relation to required capabilities or the direction of new technology fields to be pursued, and the survey results are classified on a TRL level and included in the defense technology investigation strategy plan

10

2. Setting technology security levels and directions through a case analysis of Korea and other major countries

B) Defense technology acquisition and management in major countries

< U.S. classification of defense scientific technology >

- **According to the DoDI 3200.12, scientific technology information acquired through R&D is defined as STI (Scientific Technical Information)**
- **All documents and data produced from scientific technology businesses in and outside the DoD (basic research, applied research, advanced technology development, investigation analysis, etc.) are always stored in the DTIC**
- **STI is categorized into classified information, information on controlled technology, and general information. Classified information is divided into ① Top Secret, ② Secret, ③ Confidential**
- **Non-classified information must be marked as one distribution level from A to X**

Categorization of STI distribution levels

Distribution Level	Distribution Range
A	General disclosure
B	U.S. government agencies
C	U.S. government agencies and their contractors
D	U.S. DoD and its contractors
E	Only U.S. DoD agencies
F	Distributed only on orders by DoD or upper organizations
X	Export controlled technology information, distributed to authorized individuals or businesses and U.S. government agencies

Examples of distribution levels (DoDI 5230.24)

Type	Definition	Distribution Level
Critical Technology	Technical information critical to the design, development, production, operation, application, or maintenance of products or services that could be of great contribution to the military potential of any country, including the U.S.	- Levels B~F - Export controlled
Direct Military Support	Export controlled technology information that could be damaging to the technical or military interests of the U.S., other countries, or joint programs between the U.S. and other countries	- Levels E, F
Test and Evaluation	Test and evaluation results of commercial products or military hardware that could be damaging to their producers if leaked	- Levels B, E, F

3. Designing evaluation categories to set technology security levels

[Step 1] Reviewing investigation categories of other organizations

(Step 1 of designing evaluation categories) Examining and analyzing literature of investigation categories from other organizations

Evaluation Category Group	Implications	Department/Organization
Technology Level	• The main purpose of technology level evaluation cases • The defense sector distinguishes 5 technology levels, but private sectors generally distinguish 4 levels (leading, chasing, late, and behind; although standards for each level are different) • The ICT IITP only evaluates technology levels from a primary survey and confers a percentage level based on the primary results on a secondary survey	• 7 technology level evaluation cases • National Core Technology (MOTIE) • Key Strategic Technology (MOTIE)
Technological Divide	• Only utilized in technology level evaluation cases • Investigates the country that has the best prowess in the technology, and the technological divide in time from that country	• 6 technology level evaluation cases (excepting KRIT)
Best Technology		• 7 technology level evaluation cases
Technological Trends	• Utilized in both nationally designated technology and technology level evaluation cases • In technology level evaluation, tendencies regarding time or compared to other countries are investigated	• Defense Industrial Technology (Technological Trends) • National Advanced Strategic Technology (MOTIE) • Core Ppuri Technology (MOTIE) • ICT Technology Level Investigation (IITP) • Industrial Technology Level Investigation (KEIT)
Importance	• Utilized in both nationally designated technology and technology level evaluation cases • Investigates the importance the technology holds commercially or in performing weapon system functions or upper technology	• National Advanced Strategic Technology (MOTIE) • Maritime and Fisheries Technology Level Evaluation (KIMST) • ICT Technology Level Investigation (IITP) • Industrial Technology Level Investigation (KEIT) • Defense Scientific Technology Investigation (KRIT)
Difficulty	• Mainly evaluated in nationally designated technology cases; only defense scientific technology investigations make use of this category in technology level evaluations • Investigates the difficulty of acquiring or researching the technology	• National Core Technology (MOTIE) • National Advanced Strategic Technology (MOTIE) • Core Ppuri Technology (MOTIE) • Defense Scientific Technology Investigation (KRIT)

12

3. Designing evaluation categories to set technology security levels

[Step 1] Reviewing investigation categories of other organizations

(Step 1 of designing evaluation categories) Examining and analyzing literature of investigation categories from other organizations

Evaluation Category Group	Implications	Department/Organization
Impact on Security	• Utilized only in nationally designated technology cases • Investigates the technology's impact on national, industrial, and economic security, as well as importance in defense	• National Core Technology (MOTIE) • Key Strategic Technology (MOTIE) • National Advanced Strategic Technology (MOTIE) • National Strategic Technology (MSIT) • Defense Industrial Technology (MND)
Influence on Relevant Technology (Industry)	• Utilized in both nationally designated technology and technology level evaluation cases • Investigates the ripple effect or diffusion effect on its industry or relevant industries for nationally designated technology • Investigates the influence on the development and utilization of other technologies for technology level evaluation cases	• National Core Technology (MOTIE) • Key Strategic Technology (MOTIE) • Core Ppuri Technology (MOTIE) • National Strategic Technology (MSIT) • Land and Transport Technology Level Analysis (KAIA) • Industrial Technology Level Analysis (KEIT)
Market Trends	• Only utilized in nationally designated technology cases • Investigates future promise of the relevant market and domestic/overseas market shares	• Key Strategic Technology (MOTIE) • Core Ppuri Technology (MOTIE) • National Strategic Technology (MSIT)
Influence on Economy	• Only utilized in nationally designated technology cases • Investigates influence on economy such as exports, employment, and local economy	• National Core Technology (MOTIE) • National Advanced Strategic Technology (MOTIE) • Core Ppuri Technology (MOTIE)
International Relations	• Only utilized in nationally designated technology cases • Investigates volume of trade, international division of labor, diplomatic situation, etc.	• Key Strategic Technology (MOTIE) • National Strategic Technology (MSIT)

13

3. Designing evaluation categories to set technology security levels

[Step 2] Deriving additional categories for review through the Delphi method

- **The Delphi method, developed by the RAND Institute of the U.S., is a process of collecting expert opinions into one opinion**
- **Plans to reach a consensus by repeating open and closed surveys to experts in order to review changes and deletions of investigation categories from other organizations and additions of new evaluation categories**
  - Uses Coefficient of Variance (CV) in order to objectively judge research stability and number of surveys; when the CV is below 0.5, the round is closed without any further surveys
  - When the CV is 0.5~0.8, a relatively stable expert consensus has been reached; when the CV is 0.8 or over, there is a need to conduct further surveys

[Step 3] Grouping similar evaluation categories and deciding on a class structure for each category through factor analysis

- **Factor analysis is a representative statistical method for multivariate data that analyzes the correlations between evaluation categories (variables) and newly extracts factors in common**
  - The greatest purpose of factor analysis is representing the entire data by utilizing characteristics of many variables to the fullest, while at the same time summarizing and structuralizing with only a few factors
- **Applies Exploratory Factor Analysis in order to classify and structuralize evaluation indexes by the same factor when the characteristics and number of common factors in evaluation indexes derived by the Delphi method are unclear**
- **Evaluation indexes that have been structuralized and classified through factor analysis are later used to derive weight factors for each technology security level evaluation index**

14

4. Expert evaluation to set security levels

A) Setting technology security levels for each factor technology, reflecting expert evaluation for each technology sector

< Securing reliability by getting expert evaluations for each technology sector >

- **A "confidence level for responses" is reflected when responding to expert surveys**
  - Confidence levels are input on an interval scale of 5 points
  - Responses of below level 3 confidence are deleted; a weighted average is calculated for those of level 3 and above

15

5. Classification methods of technology security levels

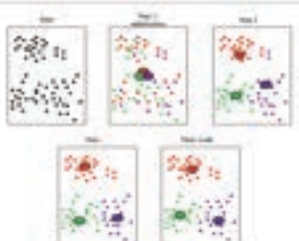
A) Classification methods of technology security levels

< K-NN Algorithm >

- The K-NN algorithm labels and classifies data according to its closest properties
- Measures closeness of properties based on distance, and neighbors at a shorter distance are treated as closer neighbors
- In other words, it refers to a K number of other labels close to certain new data to classify them as frequent
- Often used methods to measure distance
  - Euclidean distance: $d(A,B) = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$
  - Manhattan distance: $d(A,B) = |x_1 - x_2| + |y_1 - y_2|$

< K-Means Algorithm >

- The K-Means algorithm groups data of similar characteristics into a K number of clusters
  In other words, it groups together given data while mobilizing the cluster's core until it reaches the targeted number of clusters (K)



16

5. Classification methods of technology security levels

A) Classification methods of technology security levels

< A comparison of K-NN and K-Means algorithms and ways to use technology security level classification methods >

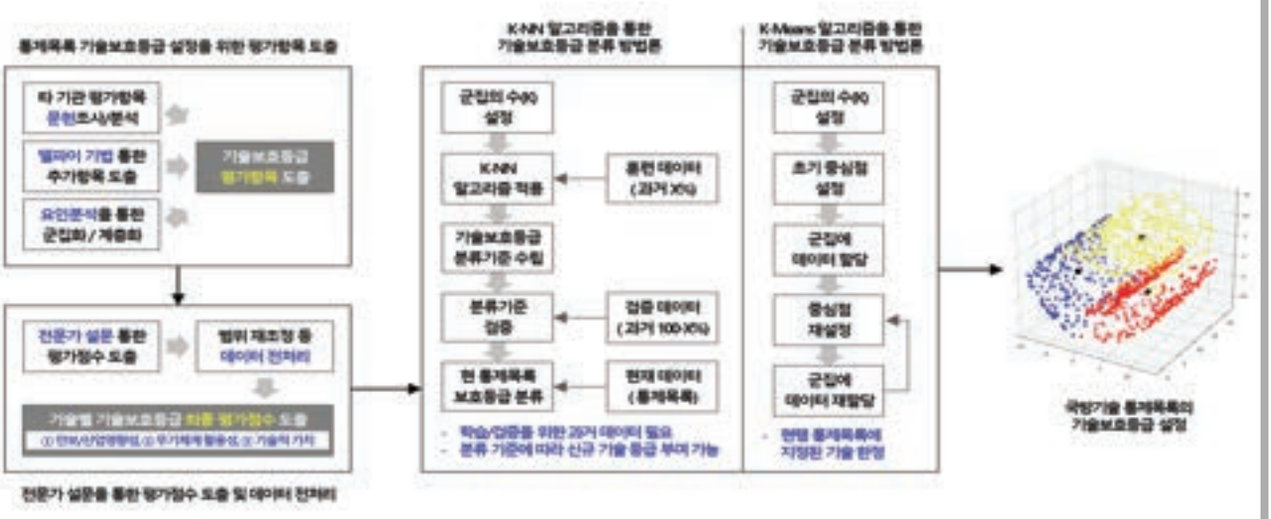
Type	K-NN Algorithm	K-Means Algorithm
Similarities	• Purpose of classifying/clustering data into a K number of groups • A distance-based analysis algorithm that is realized on a basis of distance	
Need for learning data	• Needs learning data with a result (y) related to input data (x)	• Does not need learning data, just input data (x)
Need for past data	• Needs results (y) related to input data (x) of technology designated as past control lists; part of the results will be used as learning data, and others as verification data	• Does not need past data because there it does not require learning data
Pre-designation of technology security level	• Needs to maintain the past technology security level because past data is utilized as learning data • A process of designating new levels to past data is required if new levels are needed	• Does not need past data because there it does not require learning data
Key objectives	• **Establishes level classification standards using past technology security level data** • **Designates new technology levels according to classification standards**	• **Classifies levels according to the K-Means algorithm, limited to a pool of technologies designated as current control lists**

17

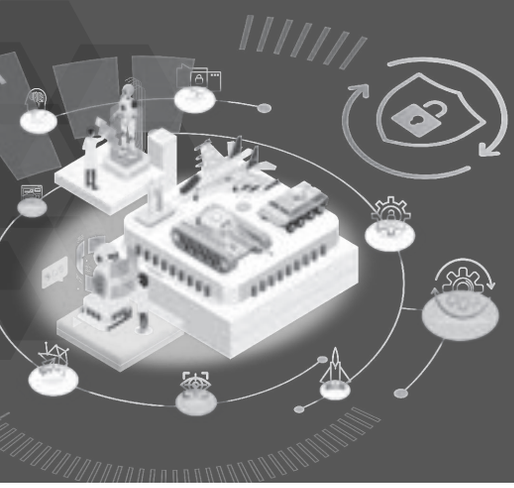
5. Classification methods of technology security levels

B) Classification procedures of technology security levels

< Technology security level classification procedures using K-NN and K-Means methodologies >



18



2023 Defense
Technology Security
Conference 2023 방산기술보호 컨퍼런스

주제발표 3.

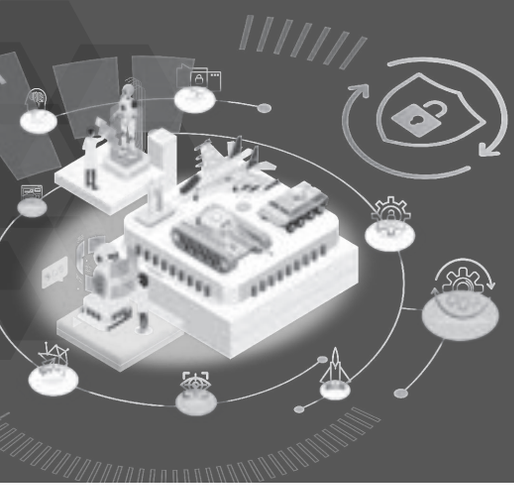
Post K-방산을 위한 방산기술보호 정책 방향

Defense Technology Protection Direction For Post K-Defense

한화에어로스페이스 경영지원실보안팀 차장 I **심의칠**

Deputy Senior Manager, Hanwha Aerospace Co., Ltd

Mr. Euichil Sim



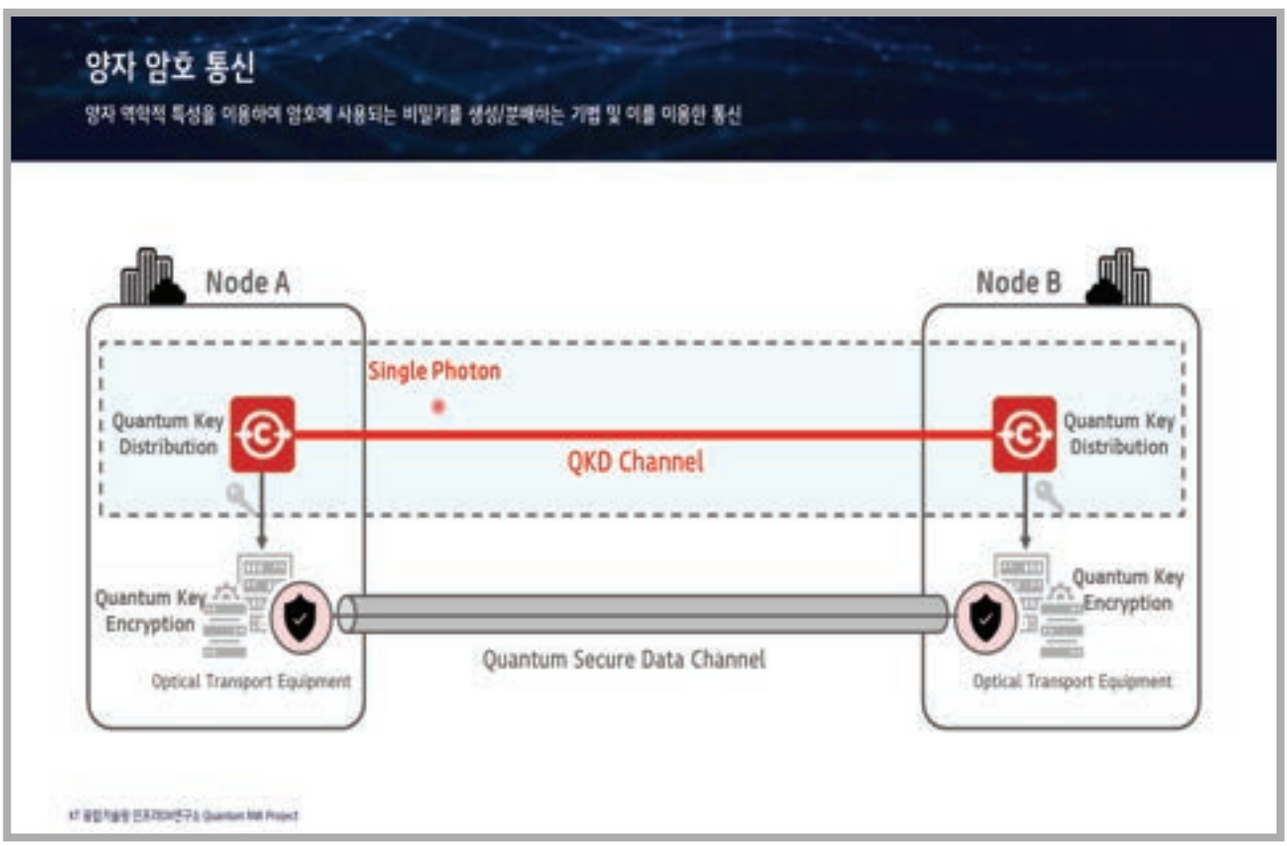
주제발표 4.

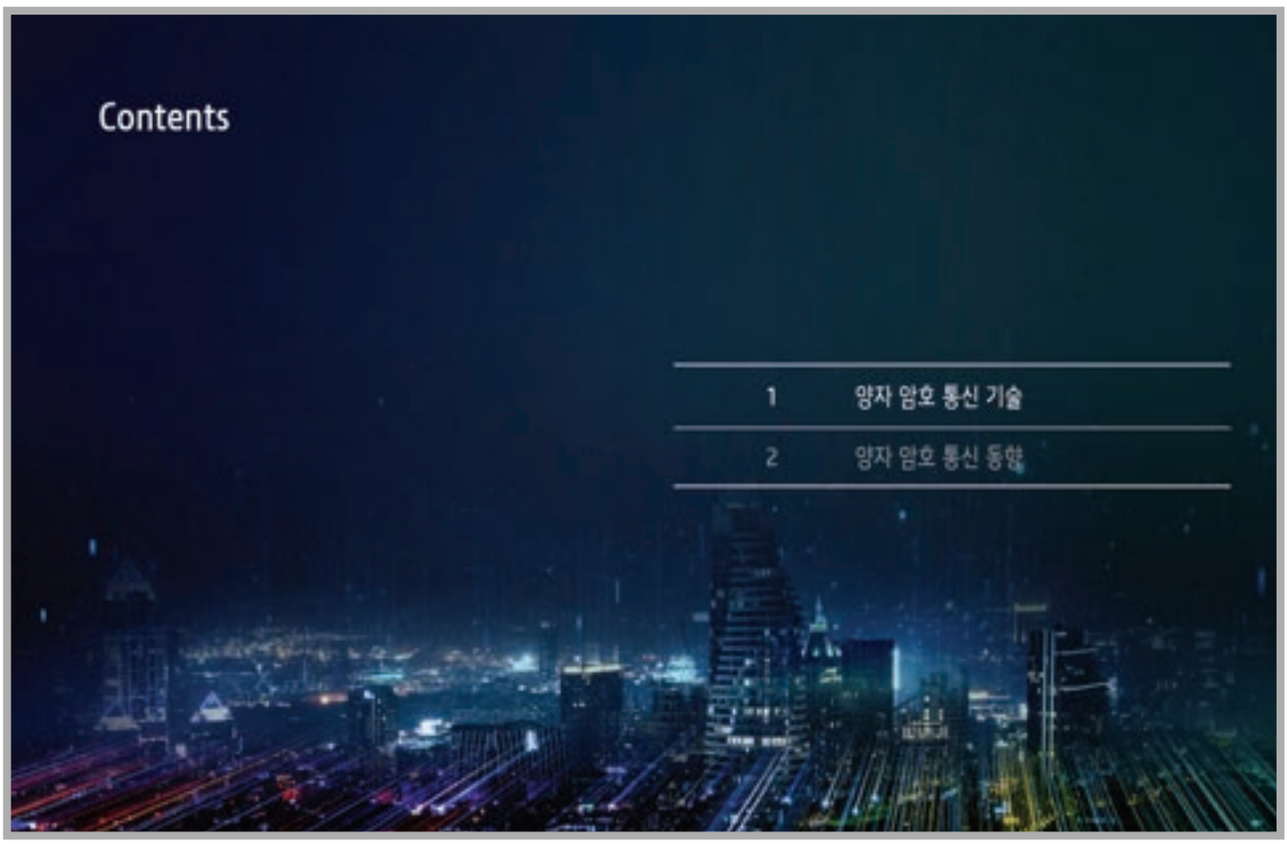
양자암호통신 기술 및 동향

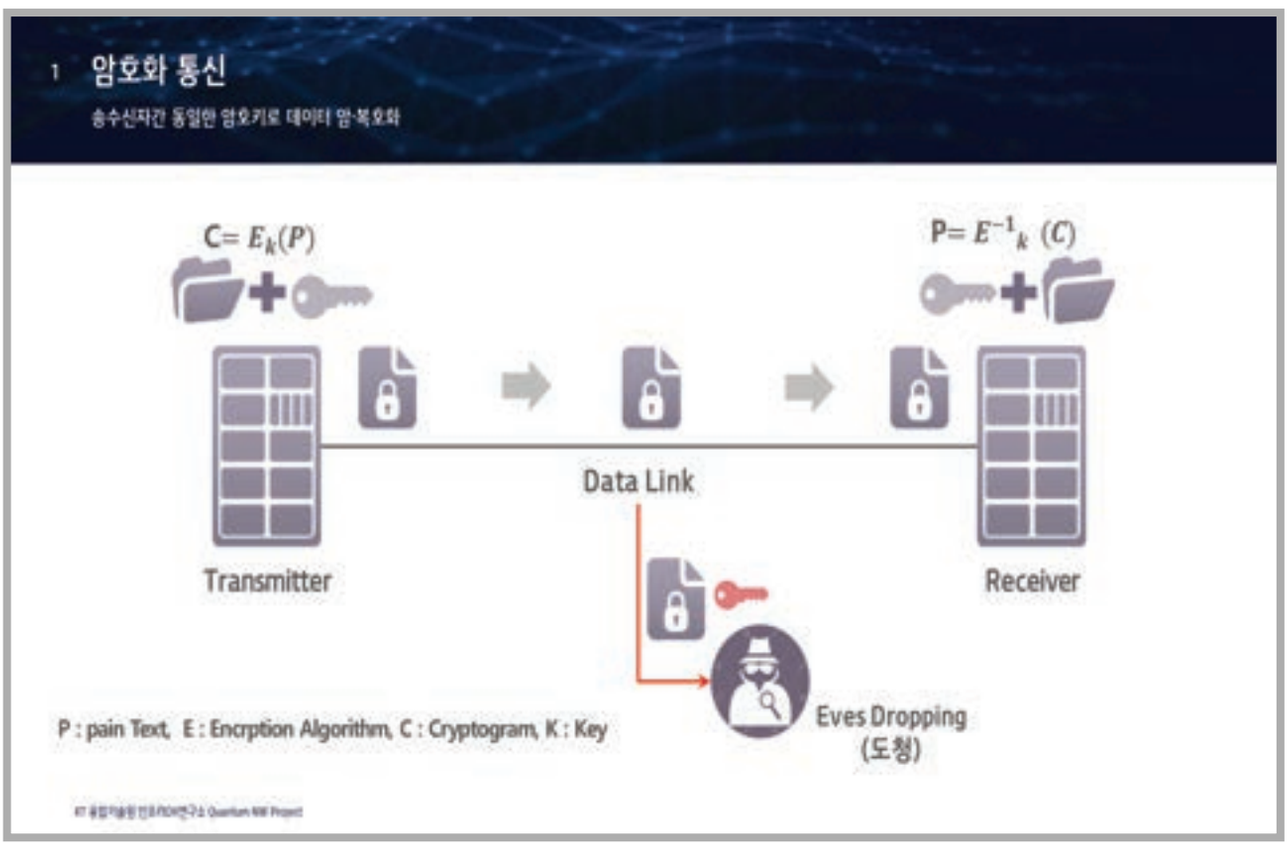
Quantum Key Distribution Technology and Trends

KT 인프라DX연구소 융합기술원 팀장 I **신정환**
Team Leader, Infra DX Lab, Institute of Convergence Technology,
KT Coporation
Mr. Jeonghwan Shin


양자암호통신 기술 및 동향
Digital
Transformation
Partner
kt


양자 암호 통신
양자 역학적 특성을 이용하여 암호에 사용되는 비밀키를 생성/분배하는 기법 및 이를 이용한 통신
Node A
Node B
Single Photon
Quantum Key
Distribution
QKD Channel
Quantum Key
Distribution
Quantum Key
Encryption
Quantum Secure Data Channel
Quantum Key
Encryption
Optical Transport Equipment
Optical Transport Equipment


Contents
1 양자 암호 통신 기술
2 양자 암호 통신 동향


1 암호화 통신
송수신자간 동일한 암호키로 데이터 암·복호화
C= $E_k(P)$
P= $E^{-1}{}_k$ (C)
Data Link
Transmitter
Receiver
Eves Dropping
(도청)
P : pain Text, E : Encrption Algorithm, C : Cryptogram, K : Key

2 암호 시스템의 안전성

- **Kerckhoff의 원리**
  - 암호시스템은 키를 제외한 모두가 공개되어도 안전해야 함
  - 암호시스템의 안전성은 암호키의 안전성에 의존함을 의미
    - 안전한 암호시스템 구축 → 안전한 암호키 생성

- 암호키 생성 방법
  - 난수발생기 (Random number generator)
    - ✓ 암호키 생성에 사용되는 장치 혹은 알고리즘
    - ✓ 의사난수발생기 (Pseudo random number generator, PRNG)와 진난수발생기 (True random number generator, TRNG)로 분류
  - 진난수 (True random)로 암호키를 생성하여 암호통신 하고 싶지만… → 진난수 생성 및 키 공유의 어려움

보안이슈	암호키 (Secret key)를 안전하게 나누어 갖는 문제

3 암호통신 시스템 - 하이브리드 방식의 안전성

현 암호키 공유: 수학적 난제를 이용한 보안성 확보

- **RSA(Rivest-Shamir-Adleman) 암호시스템**
  - 공개키와 개인키로 구성 ($N = pq$)
    송신부 암호화: $c_i = m_i^e \bmod N$
    수신부 암호화: $m_i' = c_i^d \bmod N$
  - 소인수 분해의 어려움(수학적 난제)에 기반하여 보안성 확보
    - 매우 큰 수의 소인수분해는 현재의 컴퓨터로 매우 오랜 계산 시간이 걸림
  - 현재 기술로는 암호키 해독 어려움

보안 이슈	• 키 공유 알고리즘 → 수학적 난제 (풀기가 매우 어렵거나 시간이 오래 걸림)에 의존

4 양자 컴퓨터의 위협

양자컴퓨터, 공개키 암호시스템 안전성 위협

768 비트 RSA 알고리즘 공격: 약 3,300 년 (기존) → 1초 (양자컴퓨터)

"A Blueprint for Building a Quantum Computer" By Rodney Van Meter, Clare Horsman
Communications of the ACM, Vol. 56 No. 10, Pages 84-93 10.1145/2494568

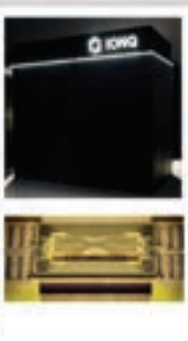
수학적 난제* 기반의 기존
공개키 기반 암호시스템
* 소인수 분해/이산 대수 문제의 어려움

양자컴퓨터 등장
(기존 난제를 빠르게 해결)

양자컴퓨터 위협 대응 위한
새로운 암호체계 필요

5 양자 컴퓨터 산업 동향

대표적 양자 컴퓨팅 업체 기술 현황

구분	IBM	Google	Intel	ionQ	Microsoft	AWS
외형						rigetti OQC IONQ QuEra COMPUTING INC.
큐비트	433	53	12	32	-	-
방식	초전도	초전도	실리콘 스핀	이온트랩	위상 큐비트	-
서비스 (SDK)	Qiskit	-	Intel Quantum SDK 1.0	-	Azure quantum	Amazon Braket
개발년도	2022	2019	2023	2020	-	-

6 양자 암호 통신 (Quantum key distribution, QKD)

기존 암호 키 분배가 가지고 있는 수학적 알고리즘 기반의 문제 해결 (양자 컴퓨터로 부터도 안전)

알고리즘에 의존하지 않는 물리적 특성으로 완벽한 보안 제공 (보안이 증명된 유일한 기법)

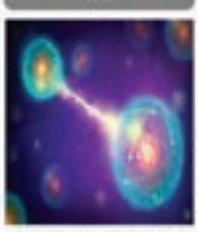
C. H. Bennett and G. Brassard. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 1984.
Bennett, C.H., Bessette, F., Brassard, G. et al. Experimental quantum cryptography. J. Cryptology 5, 3–28 (1992).

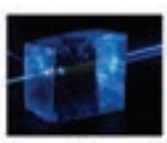
KT 융합기술원 인프라DX연구소 Quantum Mill Project

7 양자 (Quantum)

더 이상 나눌 수 없는, 물질이 가질 수 있는 최소 에너지 또는 최소 에너지를 가지고 있는 상태

• 양자(Quantum)의 주요 특징

Uncertainty (불확정성)	Indeterminism (중첩)	Entanglement (얽힘)	Irreversibility (복원 불가)
			
Commute 하지 않은 두 개의 물리량을 동시에 측정 할 수 없음 $[x, P_x] = i\hbar$	다수의 고유 양자 상태가 중첩된 상태 $\|\Psi'_1\rangle + \|\Psi'_2\rangle + \|\Psi'_3\rangle$	모든 계의 양자 상태는 상호 의존적임 $\|\Psi'_1\rangle + \|\Psi'_2\rangle + \|\Psi'_3\rangle$ ⊗ $\|\Psi'_1\rangle + \|\Psi'_2\rangle + \|\Psi'_3\rangle$	측정 후 양자 상태 변화 측정 전 상태로 복원불가 $\|\Psi'_1\rangle + \|\Psi'_2\rangle + \|\Psi'_3\rangle$ measurement $\|\Psi'_1\rangle$



광자

KT 융합기술원 인프라DX연구소 Quantum Mill Project

8 양자암호통신 - 양자 키 분배

암호통신에 사용되는 암호키를 양자의 특성을 이용하여 생성/분배하여 암호화를 수행하는 통신

양자암호통신 = 양자 키 분배 + 암호통신

- 양자역학의 원리를 이용하여 물리적으로 완벽한 도청 불가능한 암호키 분배
  - 양자 정보의 특성: 복사 불가, 중첩, 얽힘, 비가역성
- 진난수 기반 암호키 사용
- 지속적/실시간 암호키 분배를 통해 안전성 향상

9 양자 암호 통신 상용 시스템

- Encryptor

- KMS

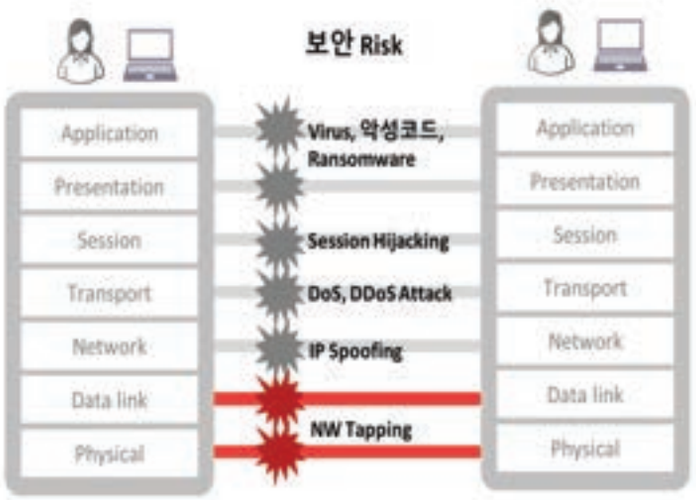
- QKD

Toshiba Long Distance QKD system

- Typical key rate = 300 kb/s for 10dB loss
- Range of up to 120km

10 보안 Risk

모든 계층 단계에서 다양한 해킹 위협의 존재
양자암호통신은 Data Link/Physical 회선 단에서의 해킹 위협(도감청) 방어



11 장거리 양자 암호키 분배 - 신뢰 노드

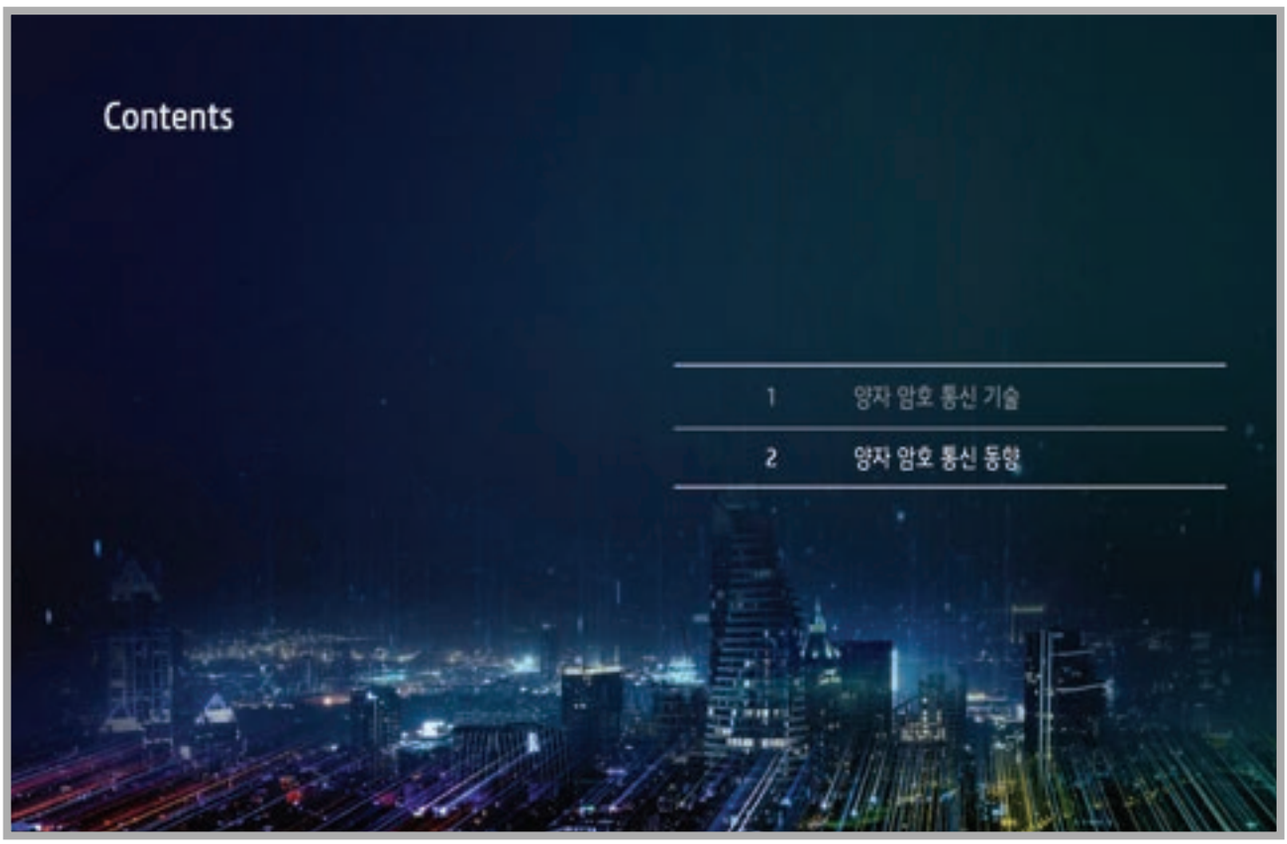
양자 키 분배 장치는 전송 거리에 한계 있음 → 이를 극복하기 위해 신뢰노드를 구성하여 장거리 전송 수행

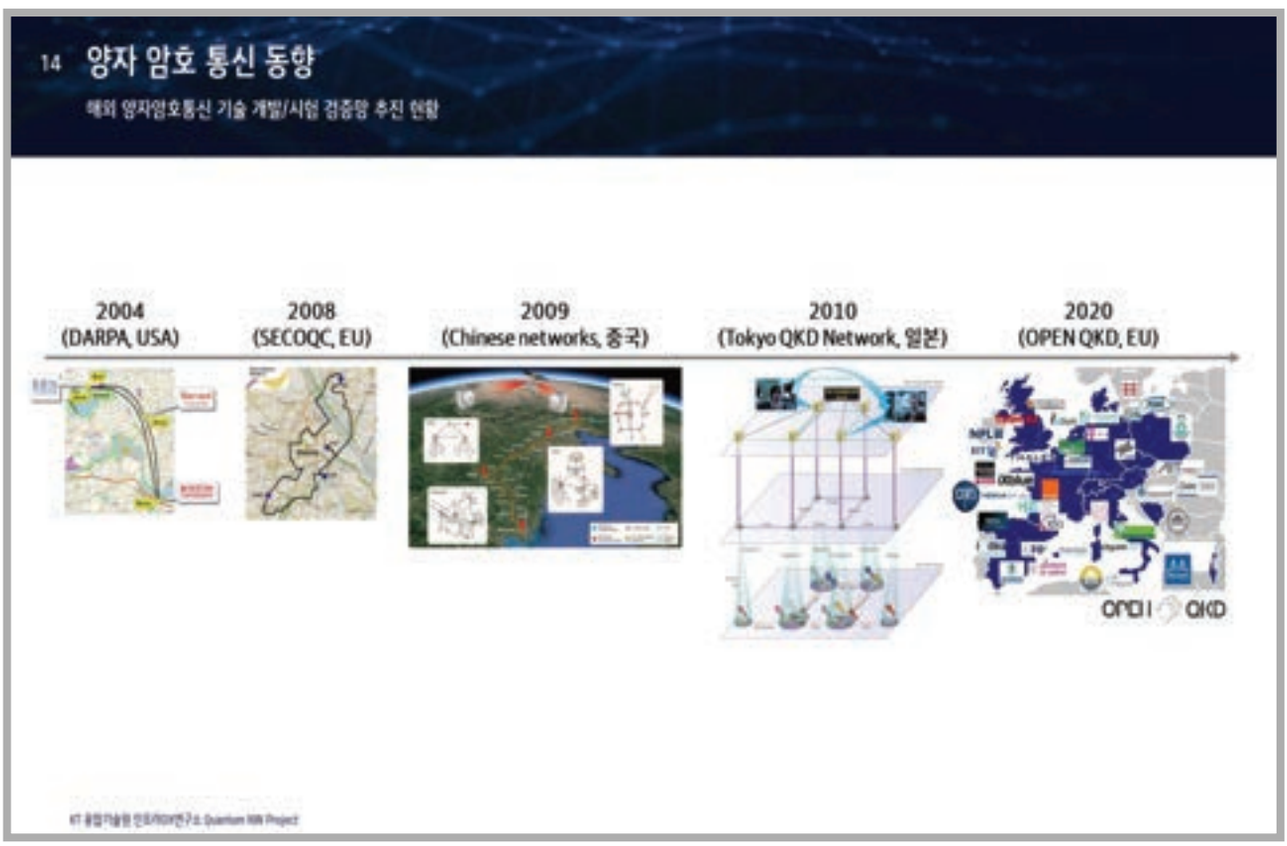
- **QKD, 전송 거리에 따른 광 손실로 전송 거리 한계**
  - 일반적인 광 회선의 경우 0.2dB/km의 광 손실율을 가지고 있음
  - QKD 시스템은 일반적으로 약 18dB (90km~120km 내외) 정도의 광 손실까지 전송 가능
  - QKD 시스템은 일반적인 증폭기나 중계기의 사용이 불가능

- **장거리 전송을 위한 신뢰노드 구성**
  - QKD의 전송 거리 한계 이상으로 암호키를 전달하기 위해 신뢰노드(Trusted node)를 구성하여 암호키 전달


12 양자 암호 통신 네트워크
Adaptive-
Encryptor
Key Manager
QKDN manager
QKD module

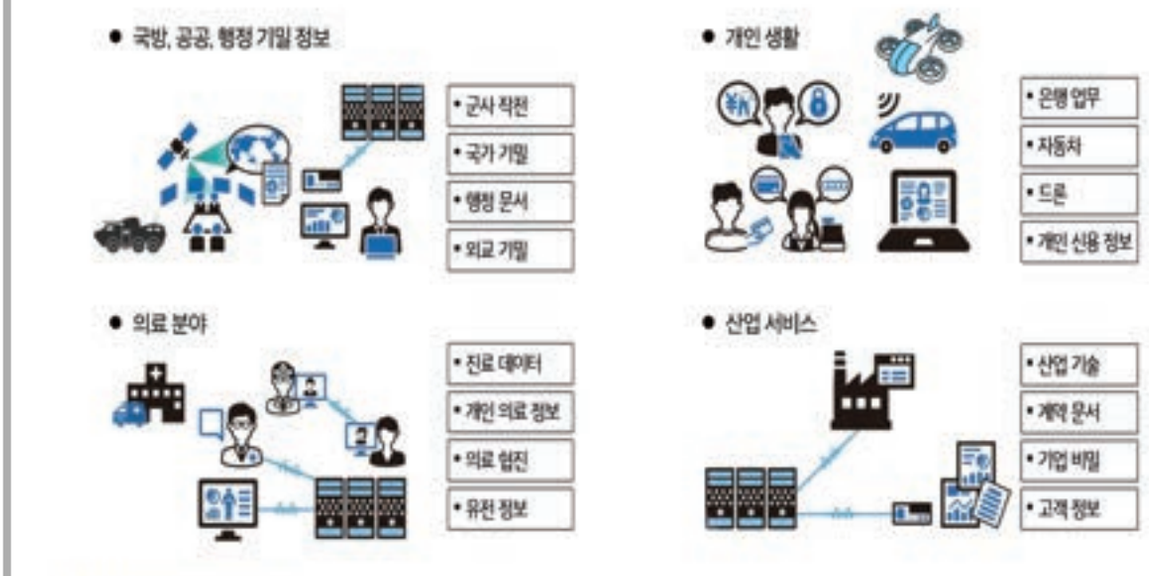

13 무선 양자암호통신
국내 최초/최장 상용 무선 양자 암호 통신 시스템 개발 추진
'22년 1km (동작대교)
무선 QKD 기술 확보
'23년 2km (가평)
무선 QKD 기술 확보
'24년 10km
국내 무선 QKD 기술 추진
'22년 300m (제주)
무선 QKD 시범 적용


Contents
1 양자 암호 통신 기술
2 양자 암호 통신 동향


14 양자 암호 통신 동향
해외 양자암호통신 기술 개발/시험 검증망 추진 현황
2004 (DARPA, USA)
2008 (SECOQC, EU)
2009 (Chinese networks, 중국)
2010 (Tokyo QKD Network, 일본)
2020 (OPEN QKD, EU)

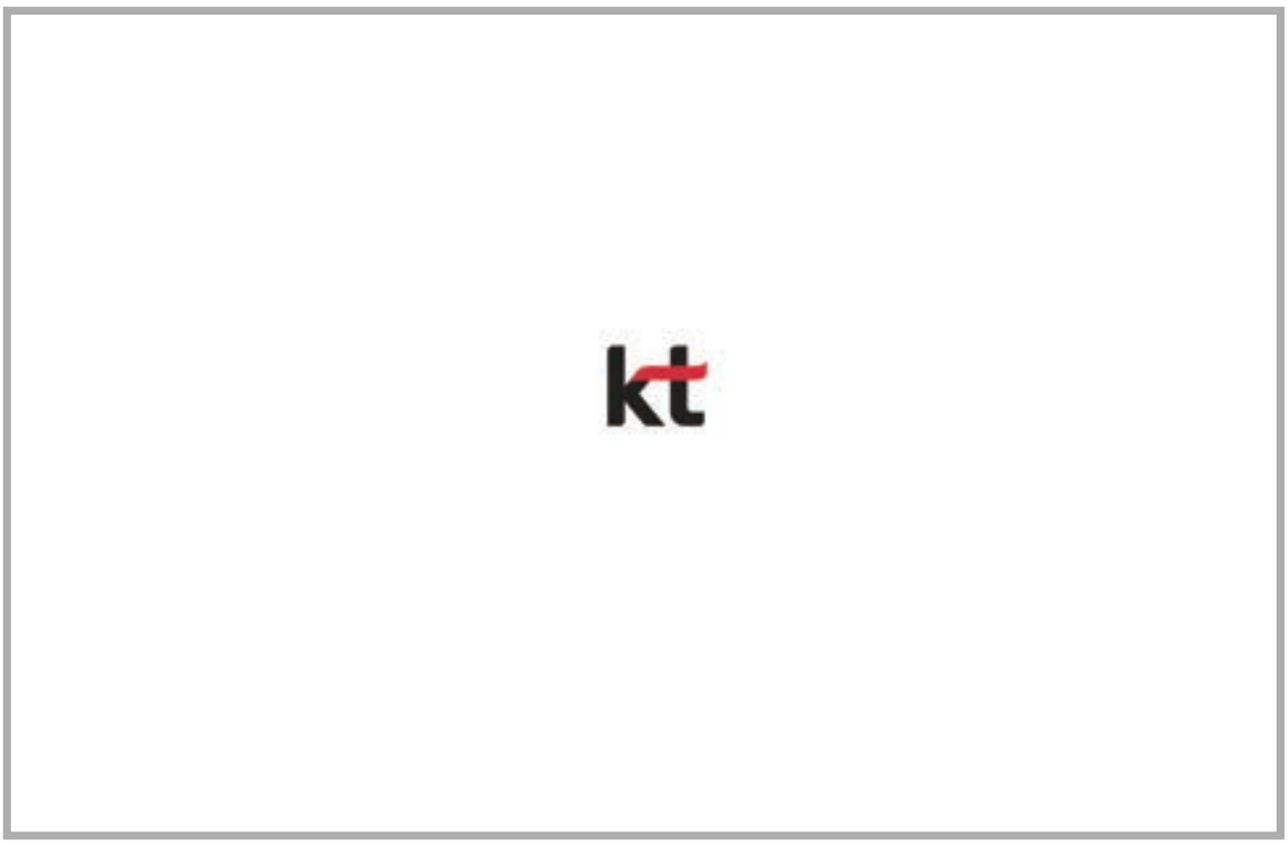
15 양자 암호 통신 시장 동향

세계는 국방, 행정, 민간 전 분야 양자암호통신 적용을 추진

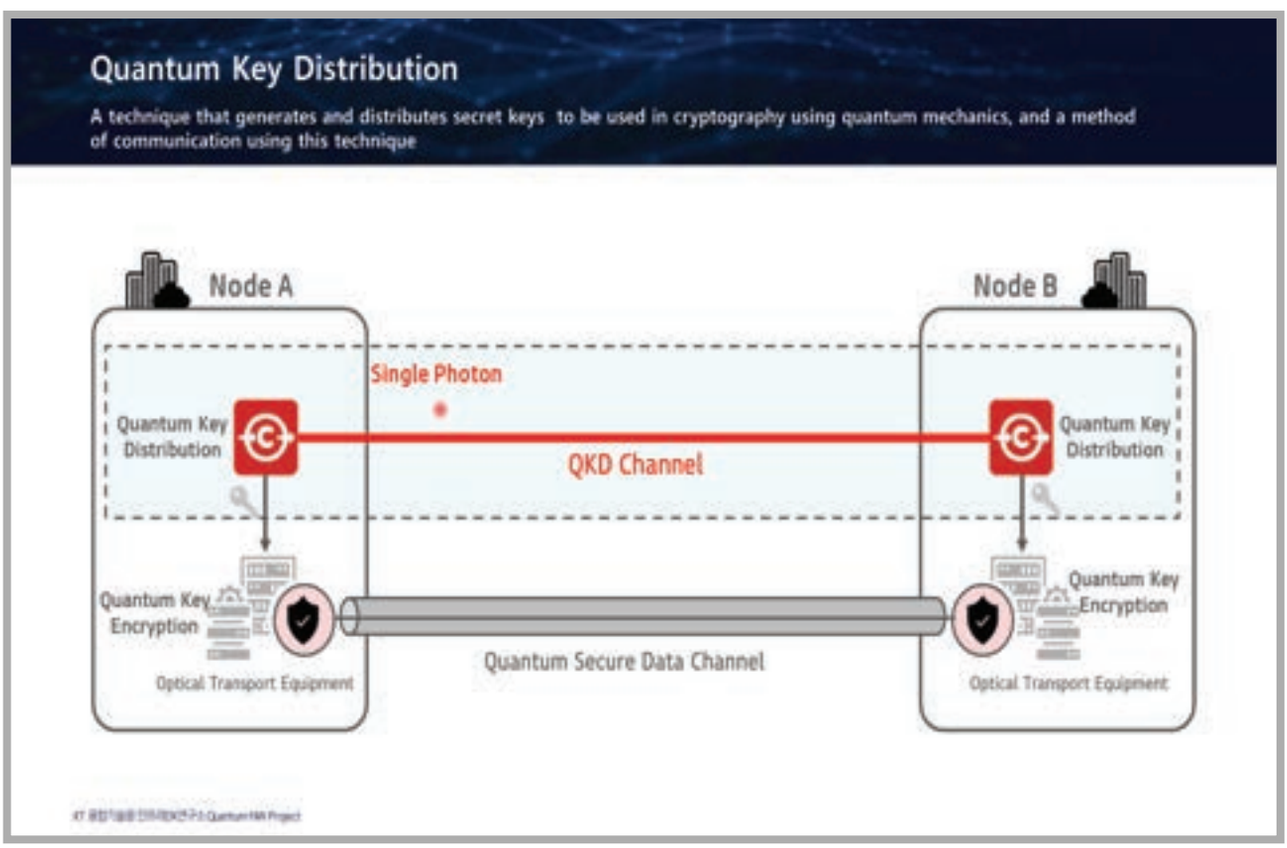


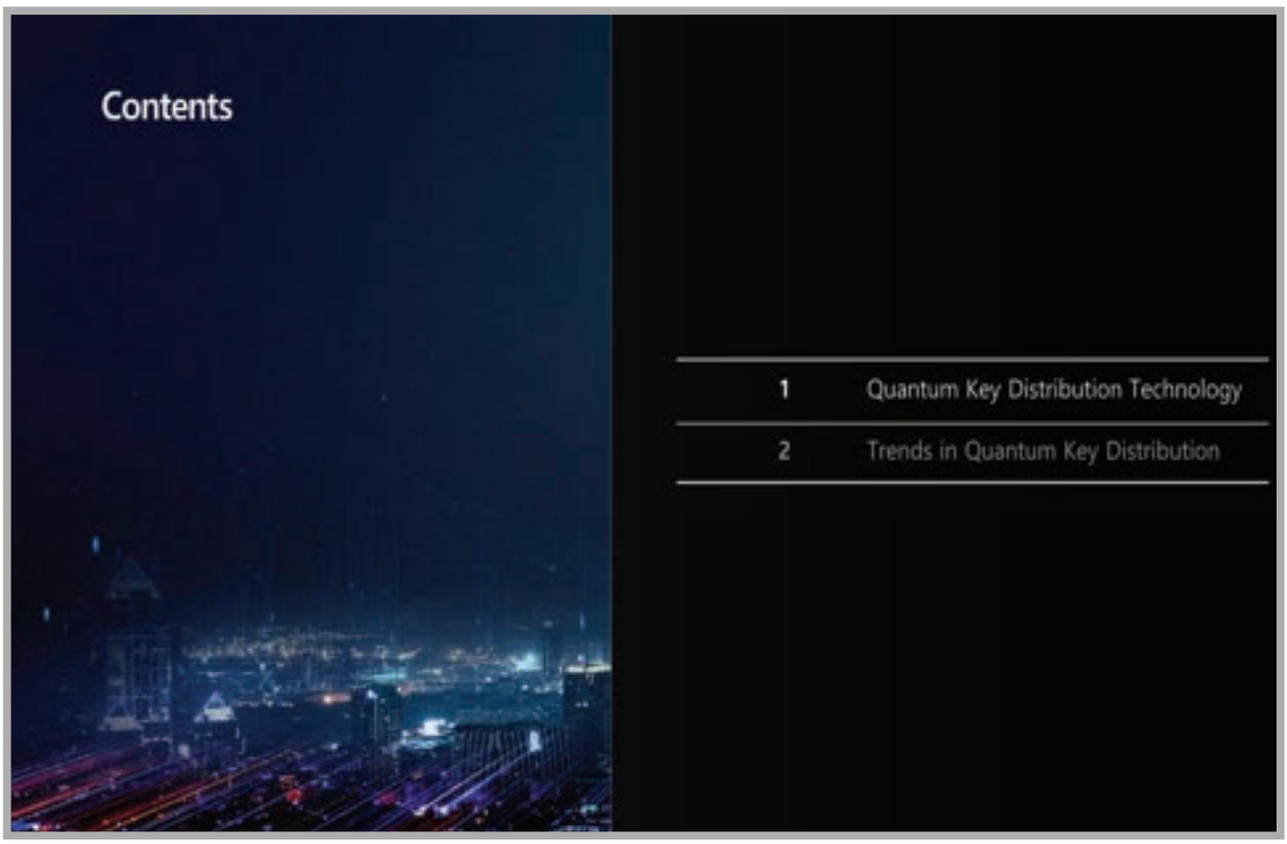
16 국내 양자암호통신 사업

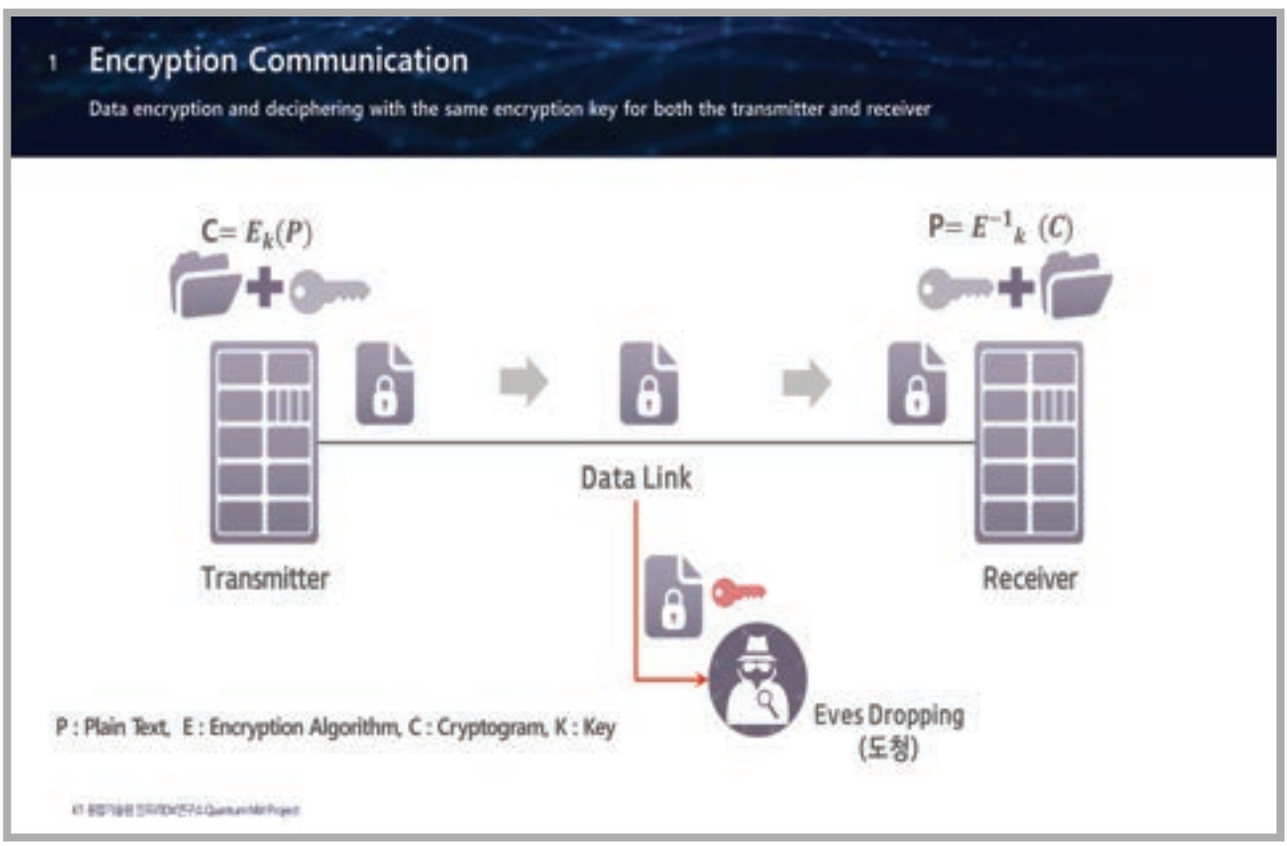
국내 양자암호통신 시범망/사업 추진, 다양한 양자암호통신 서비스 연계/발굴




Quantum Key Distribution
Technology and Trends
Digital
Transformation
Partner
kt


Quantum Key Distribution
A technique that generates and distributes secret keys to be used in cryptography using quantum mechanics, and a method of communication using this technique
Node A
Node B
Single Photon
Quantum Key Distribution
QKD Channel
Quantum Key Distribution
Quantum Key Encryption
Optical Transport Equipment
Quantum Secure Data Channel
Quantum Key Encryption
Optical Transport Equipment


Contents
1 Quantum Key Distribution Technology
2 Trends in Quantum Key Distribution


1 Encryption Communication
Data encryption and deciphering with the same encryption key for both the transmitter and receiver
C= $E_k(P)$
P= $E^{-1}{}_k$ (C)
Data Link
Transmitter
Receiver
Eves Dropping
(도청)
P : Plain Text, E : Encryption Algorithm, C : Cryptogram, K : Key

2 Encryption System Safety

- **Kerckhoff's Principle**
  - An encryption system should be secure, even if all its details, except for the key, are publicly known
  - An encryption system's security is dependent on the security of the key
    - ➢ Constructing a secure encryption system → Generating a secure encryption key
  - Generating encryption keys
    - ➢ Random number generator
      - ✓ Device or algorithm used in generating encryption keys
      - ✓ Classified into Pseudo random number generator (PRNG) and True random number generator (TRNG)

➢ **Generating encryption keys with TRNG and engaging in encrypted communication is the wish, but it is difficult to generate true random and share keys**

Security Issue	Issue of securely distributing secret keys

3 Encrypted Communication System: Safety of the Hybrid Method

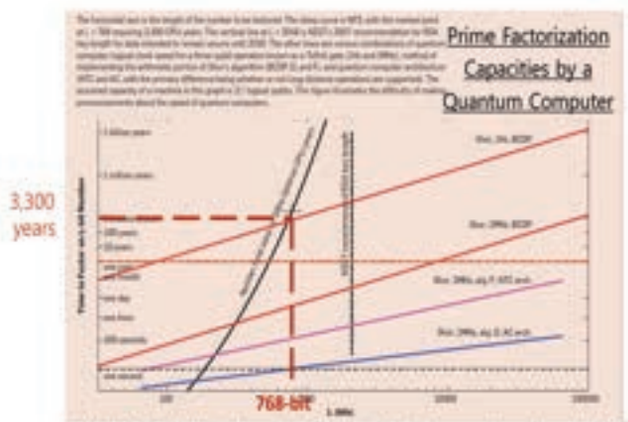
Sharing current secret keys: security by using a mathematical conundrum

- **RSA (Rivest-Shamir-Adleman) Encryption System**
  - Comprised of public/private keys $(N = pq)$
    Encrypting transmiter: $c_i = m_i^e \bmod N$
    Encrypting receiver: $m_i = c_i^d \bmod N$
  - Security from the difficulty of prime factorization (a mathematical conundrum)
    - ➢ Prime factorization of very big numbers takes a very long time to calculate with current computers
  - Difficult to decipher the encryption key with current technology

Security Issue	• Key-sharing algorithms → dependent on a mathematical conundrum (very hard or time-consuming to solve)

4 Threats of Quantum Computing

Security threats in quantum computers and public-key encryption systems



768-bit RSA algorithm attack: about 3,300 years (previously) → 1 second (quantum computers)

"A Blueprint for Building a Quantum Computer" By Rodney Van Meter, Clare Horsman Communications of the ACM, Vol. 56 No. 10., Pages 84-93 10.1145/2494568

Existing public-key encryption system based on a mathematical conundrum*

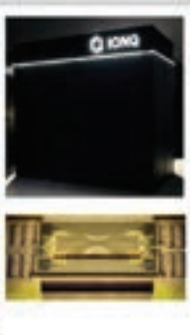
* Difficulty of prime factorization and discrete logarithm

Advent of quantum computers (able to speedily solve the conundrum)

Need for a new encryption system in the face of quantum computers' threats

5 Trends in Quantum Computer Industry

Major quantum computing businesses' technology status quo

구분	IBM	Google	Intel	IonQ	Microsoft	AWS
외형						rigetti OQC IONQ IQuEra COMPUTING INC.
큐비트	433	53	12	32	-	-
방식	초전도	초전도	실리콘 스핀	이온트랩	위상 큐비트	-
서비스 (SDK)	Qiskit	-	Intel Quantum SDK 1.0	-	Azure quantum	Amazon Braket
개발년도	2022	2019	2023	2020	-	-

6 Quantum key distribution (QKD)

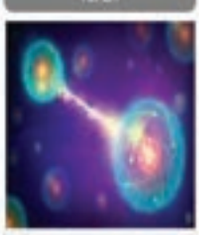
Solves the mathematical algorithm issue of existing encryption key distribution (secure from quantum computers)
Provides perfect security with physical characteristics that don't rely on algorithms (the only technique that's been proven to be secure)

C.H. Bennett and G. Brassard. In Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, 1984.
Bennett, C.H., Bessette, F., Brassard, G. et al. Experimental quantum cryptography. J. Cryptology 5, 3–28 (1992).

7 Quantum

The minimal and indivisible amount of energy an entity can have, or the state of possessing such a minimal amount of energy

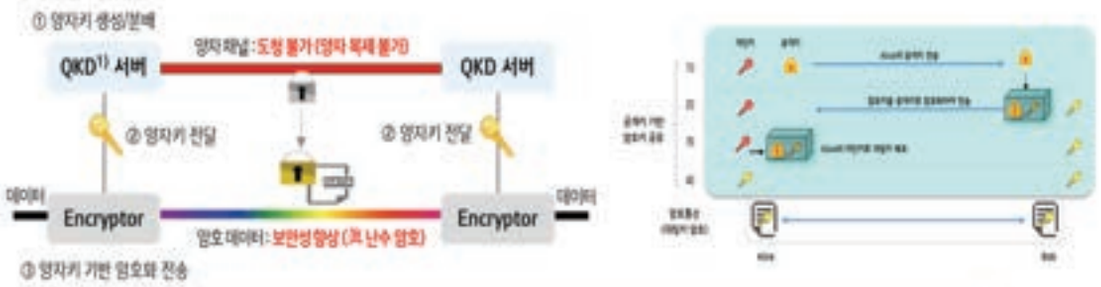
• **Main characteristics of quantum**

Uncertainty (불확정성)	Indeterminism (중첩)	Entanglement (얽힘)	Irreversibility (복원 불가)
			
Commute 하지 않은 두 개의 물리량을 동시에 측정 할 수 없음 $[x, P_x] = i\hbar$	다수의 고유 양자 상태가 중첩된 상태 $\|\Psi'_a\rangle + \|\Psi'_b\rangle + \|\Psi'_c\rangle$	모든 계의 양자 상태는 상호 의존적임 $\|\Psi'_a\rangle + \|\Psi'_b\rangle + \|\Psi'_c\rangle$ ⊗ $\|\Psi'_a\rangle + \|\Psi'_b\rangle + \|\Psi'_c\rangle$	측정 후 양자 상태 변화 측정 전 상태로 복원불가 $\|\Psi'_a\rangle + \|\Psi'_b\rangle + \|\Psi'_c\rangle$ measurement $\|\Psi'_a\rangle$

광자

8 Quantum Cryptography: Distributing Quantum Keys

Encrypted communication through generating and distributing secret keys, using the characteristics of quantum



Quantum Cryptography = Quantum Key Distribution + Encrypted Communication

- Physically perfect, tap-proof secrety key distribution by using quantum mechanics
  - Characteristics of quantum data: cannot be copied, overlaps, entangled, Irreversible
- Uses secret keys based on true random numbers
- Improved security through continuous and real-time secret key distribution

9 Commercial QKD Systems

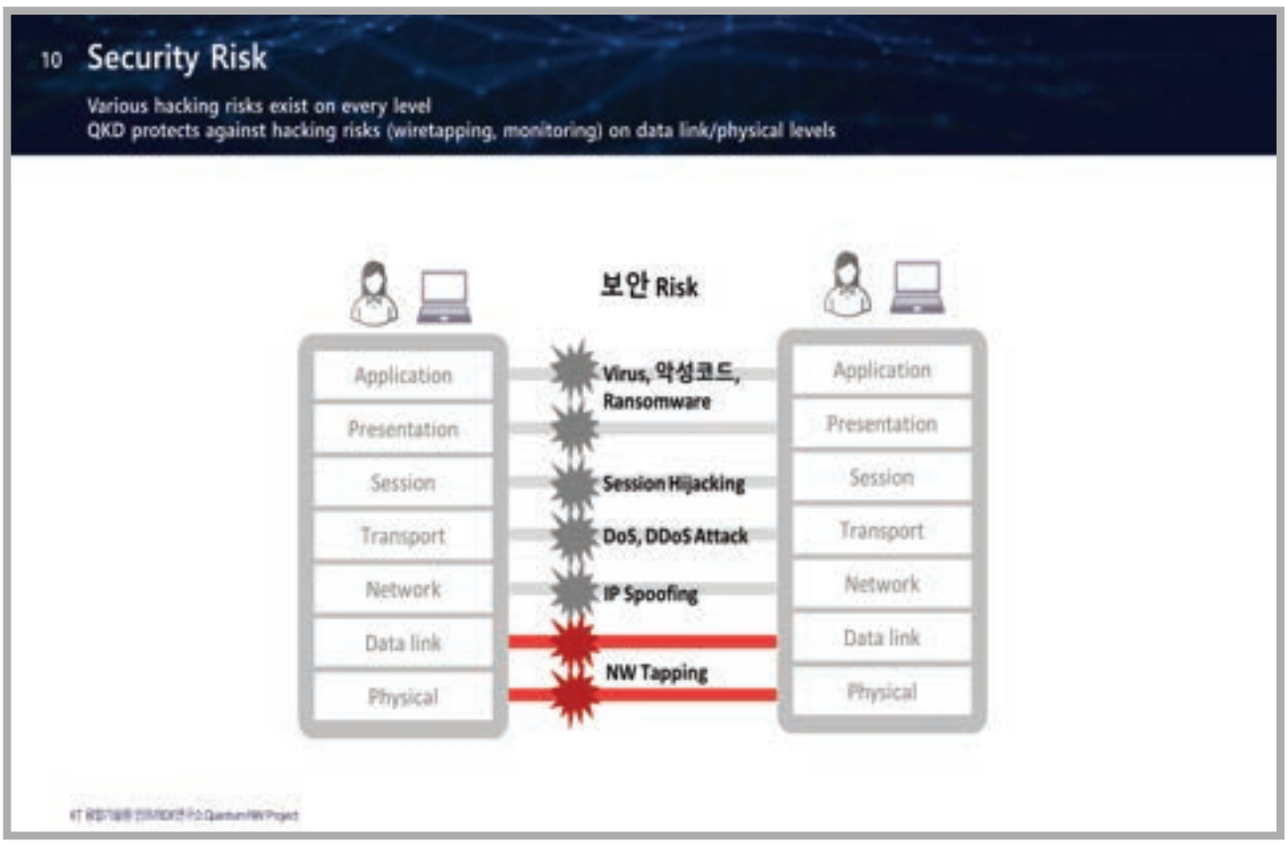
- Boxptor

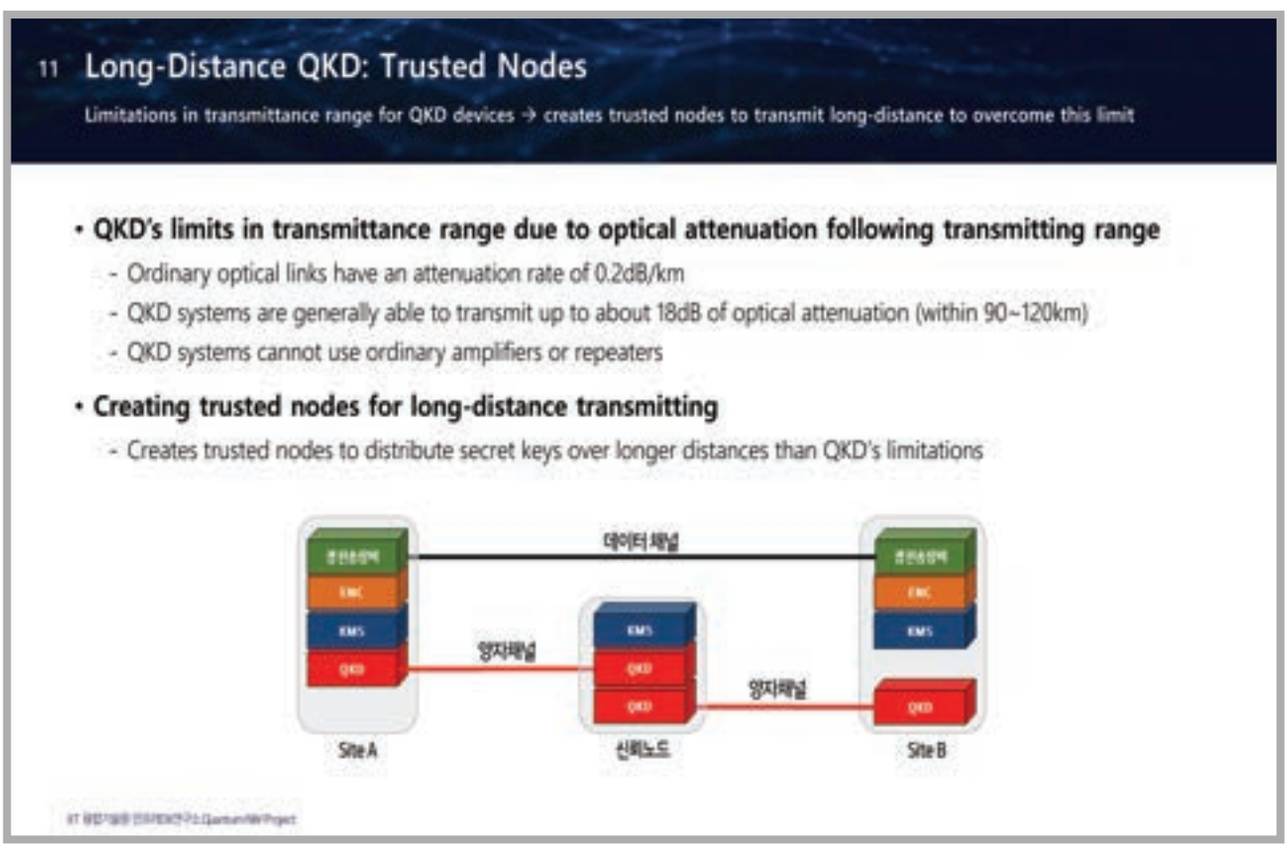
- KMS

- QKD

Toshiba Long Distance QKD system

- Typical key rate = 300 kb/s for 10dB loss
- Range of up to 120km

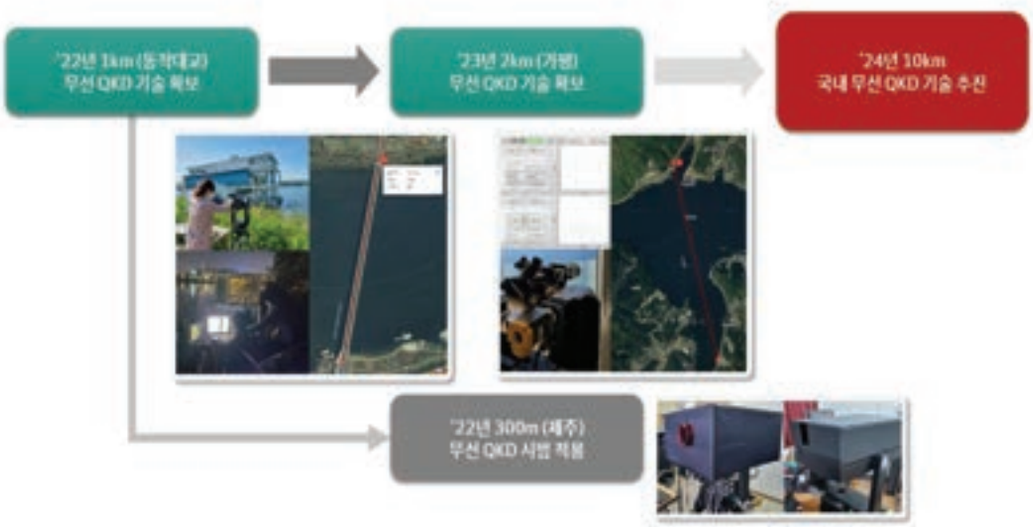

10 Security Risk
Various hacking risks exist on every level
QKD protects against hacking risks (wiretapping, monitoring) on data link/physical levels
보안 Risk
Application
Presentation
Session
Transport
Network
Data link
Physical
Virus, 악성코드, Ransomware
Session Hijacking
DoS, DDoS Attack
IP Spoofing
NW Tapping
Application
Presentation
Session
Transport
Network
Data link
Physical

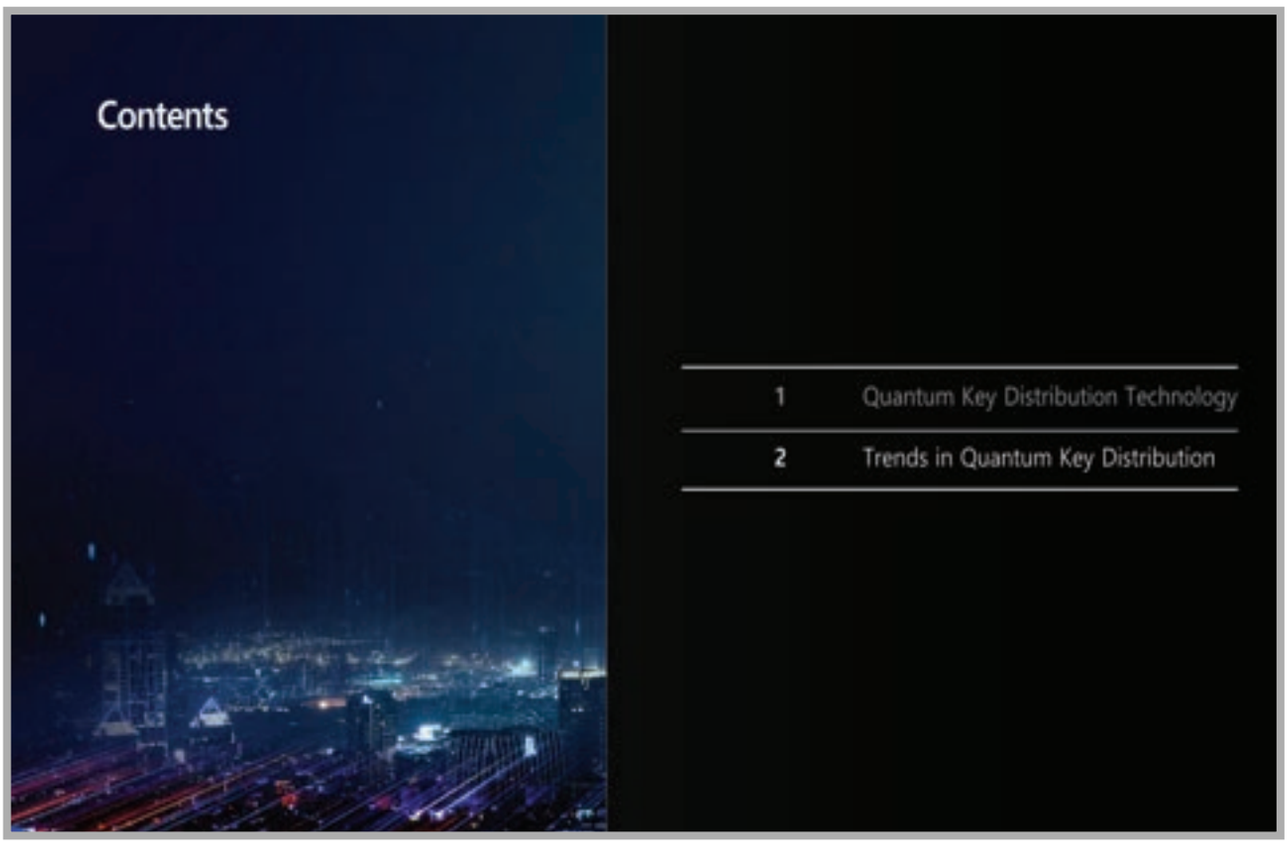

11 Long-Distance QKD: Trusted Nodes
Limitations in transmittance range for QKD devices → creates trusted nodes to transmit long-distance to overcome this limit
• QKD's limits in transmittance range due to optical attenuation following transmitting range
- Ordinary optical links have an attenuation rate of 0.2dB/km
- QKD systems are generally able to transmit up to about 18dB of optical attenuation (within 90~120km)
- QKD systems cannot use ordinary amplifiers or repeaters
• Creating trusted nodes for long-distance transmitting
- Creates trusted nodes to distribute secret keys over longer distances than QKD's limitations
데이터 채널
양자채널
양자채널
KMS
QKD
Site A
신뢰노드
Site B

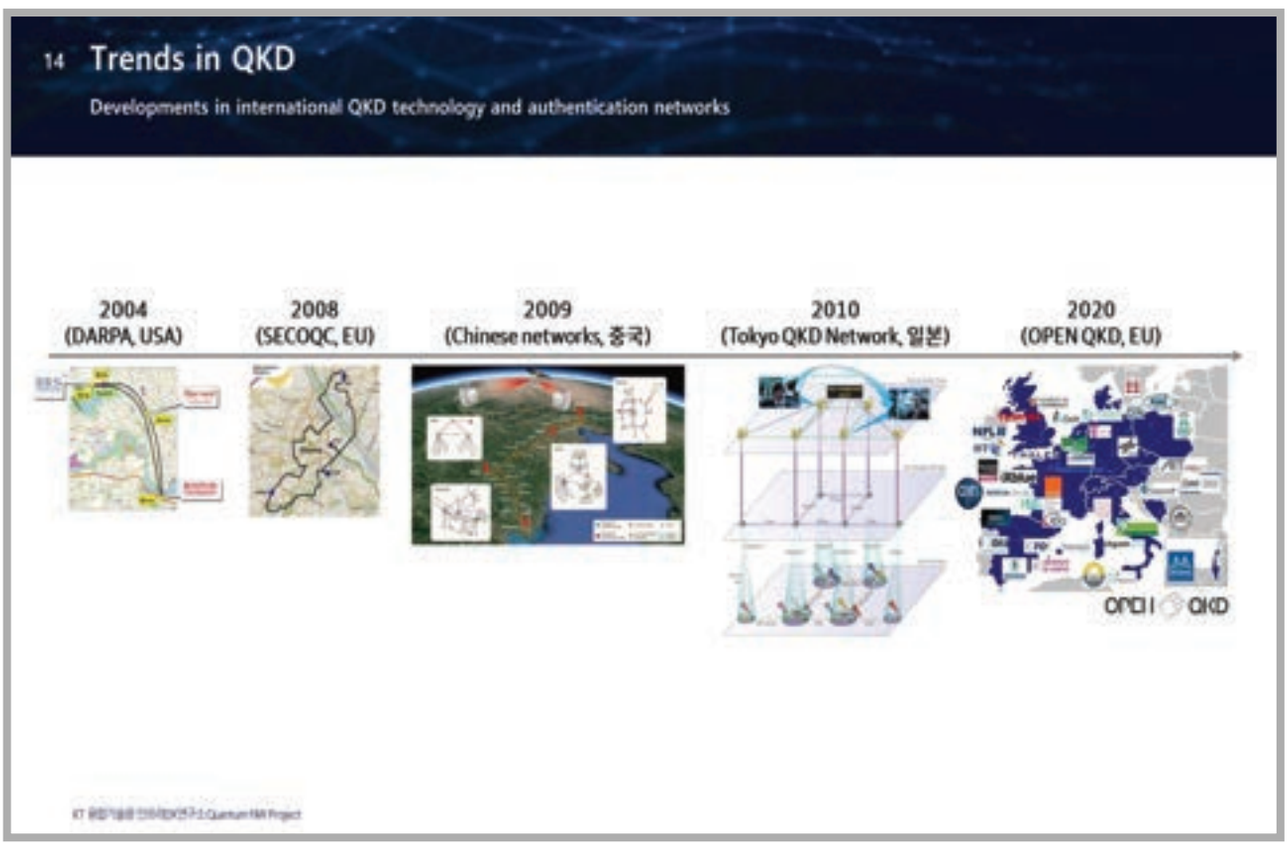
12 QKD Network

13 Wireless QKD

Plans to develop the first and longest commercial wireless QKD system in Korea

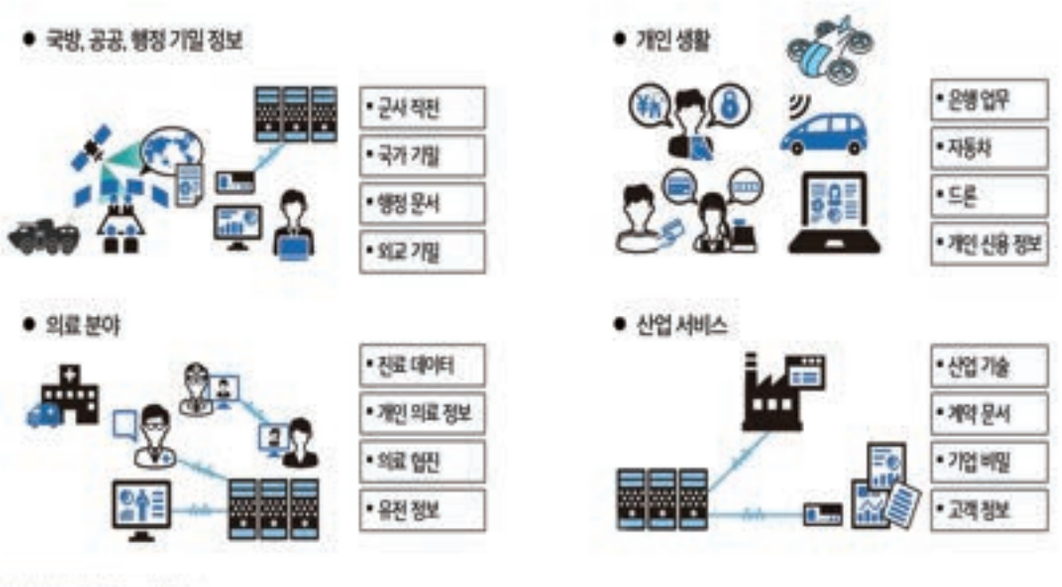



Contents
1 Quantum Key Distribution Technology
2 Trends in Quantum Key Distribution


14 Trends in QKD
Developments in international QKD technology and authentication networks
2004
(DARPA, USA)
2008
(SECOQC, EU)
2009
(Chinese networks, 중국)
2010
(Tokyo QKD Network, 일본)
2020
(OPEN QKD, EU)

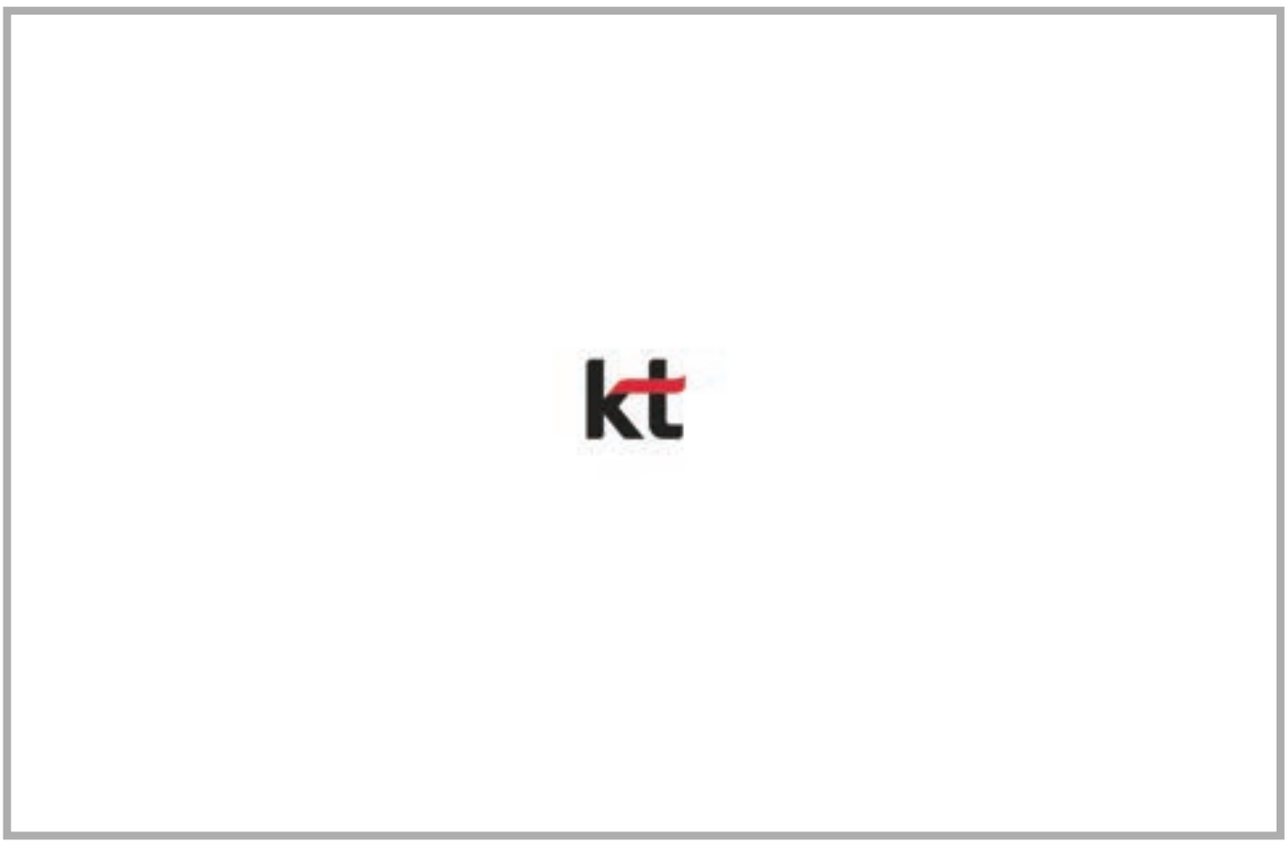
15 Trends in the QKD Market

Global developments in QKD application to all parts of national defense, administration, and private sectors



16 Domestic QKD Businesses

Developments in domestic QKD pilot networks and businesses, and connecting/forging diverse QKD services



Memo

Memo

Memo