사이버기술 연구현황 소개 및 역량강화를 위한 제언

2018. 7. 24.

ADD

사이버전 정의

❑ 컴퓨터/네트워크를 통해 디지털화된 정보가 유통되는 가상적인 공간에서 **다양한 사이버 공격수단**을 사용해 **적의 정보체계를** 교란, 거부, 통제, 파괴하는 등의 공격과 이를 방어하는 활동"

❑ 보이지 않는 전쟁 "사이버戰"

"제3차 세계대전이 일어난다면 그것은 사이버戰이 될 것이다. 어떤 국가도 성역으로 남을 수 없다." (UN, 2009. 10.)

"사이버戰은 핵전쟁과 비슷할 것이다." (영국 국제전략연구소, 2010. 2.)

사진출처: http://i-hls.com/2013/02/cyber-warfare-and-deterrence-trends-and-challenges-in-research

주요 군사작전 연계 사이버작전 사례

❑ 미국 등 주요 선진국은 사이버작전을 군사적 목표 달성을 위한 방안으로 활용 중

러시아-그루지아 ('08)

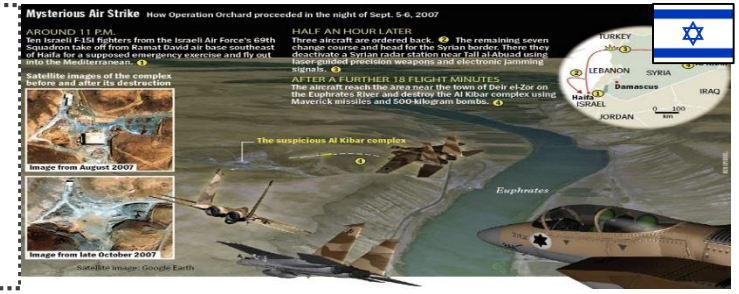
✓ 러시아의 물리적 침공 이전에 그루지아 정부기관, 군사 기반시설등에 대한 사이버 공격 시행 (DDoS, 홈페이지 변조, 네트워크 장애 등)

전면전과 연계한 최초의 사이버 작전

이스라엘-시리아 ('07, Orchard Operation)

✓ 시리아 핵시설에 대한 이스라엘군의 전투기 공습
✓ 공습시, 시리아 방공시스템 무력화
※ 전자전 공격과 사전에 준비된 사이버공격이 병행

공중작전 + 사이버 작전 + 전자전

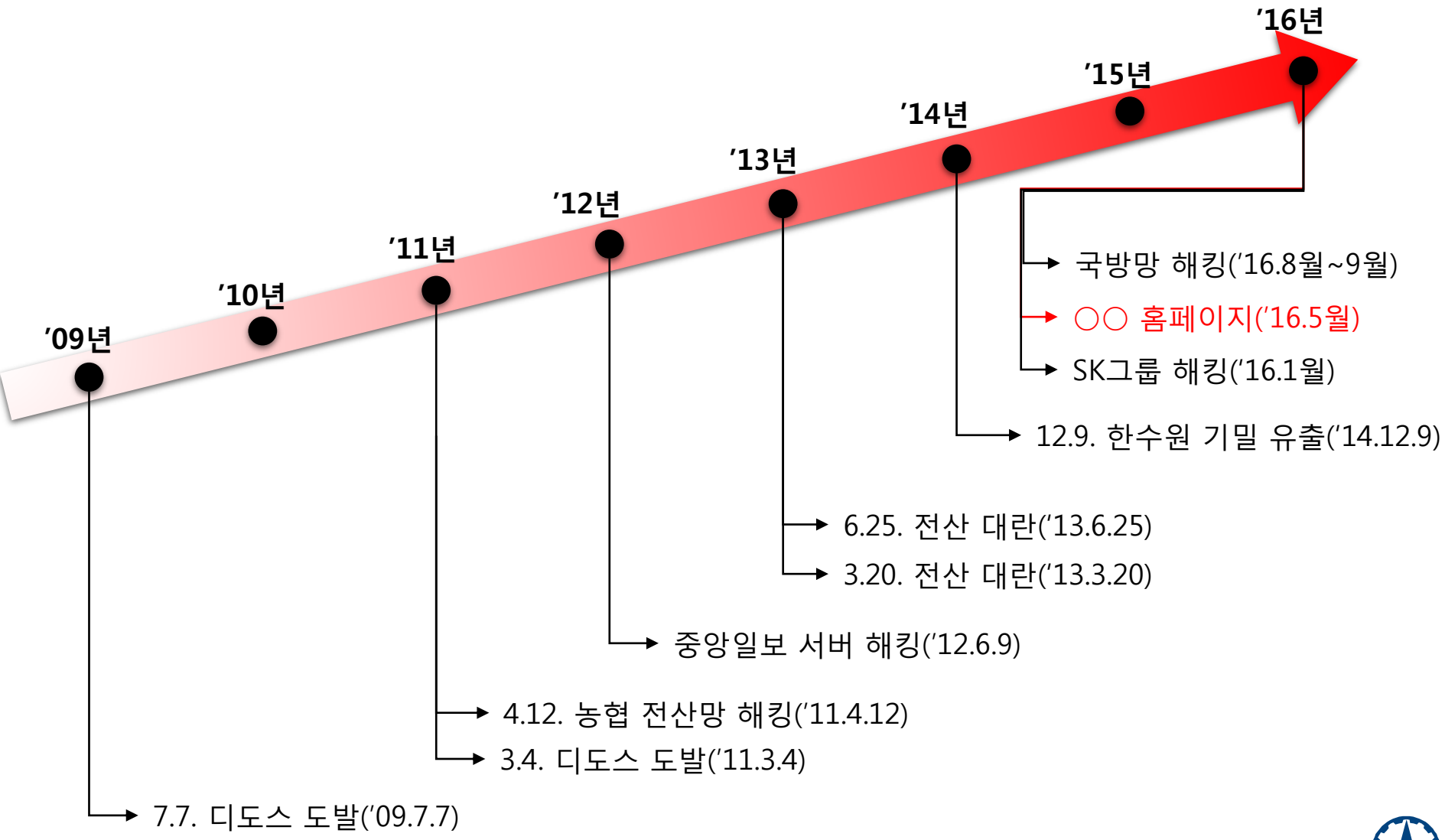


미국-이라크 반군 ('07~'08)

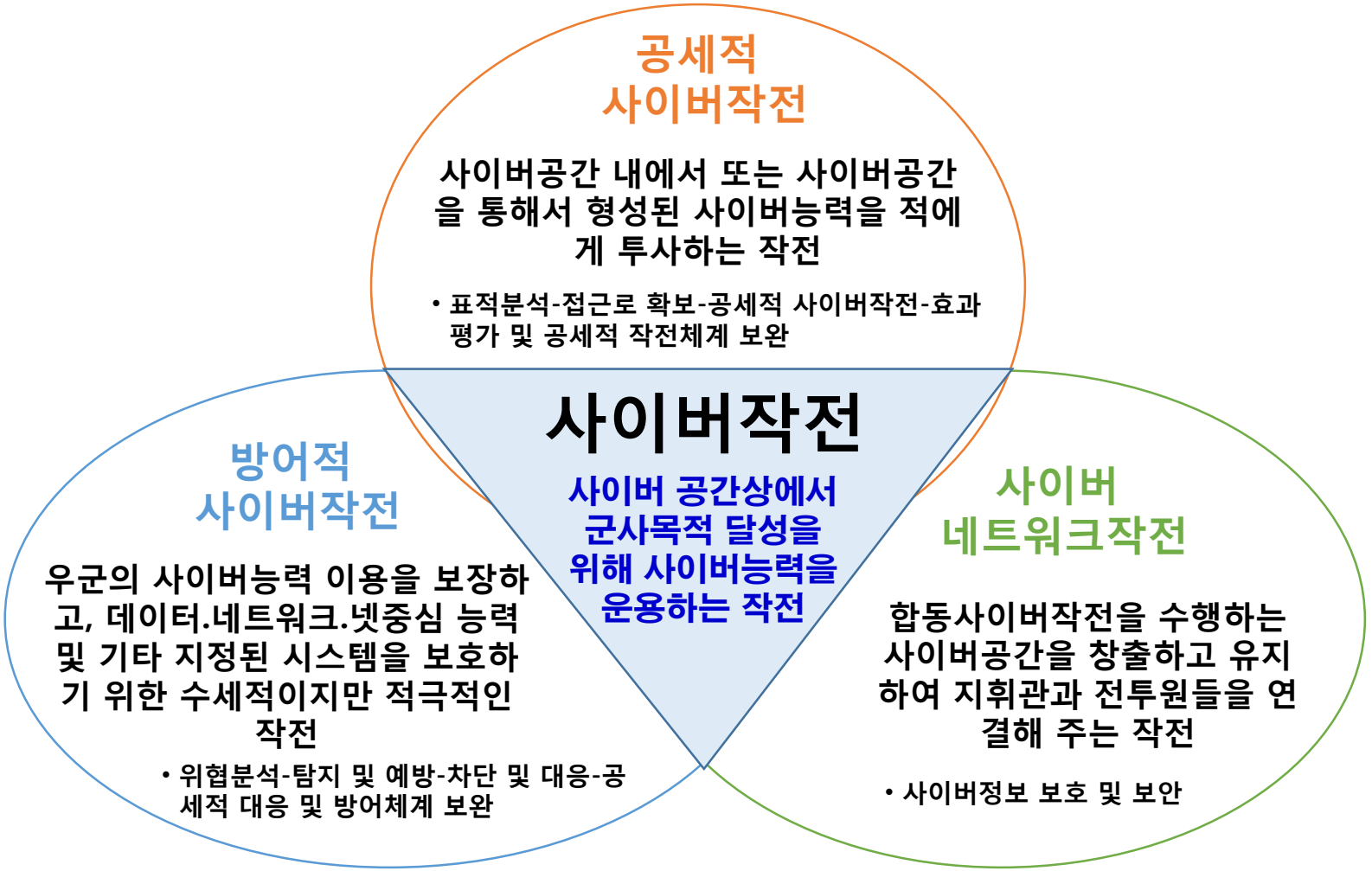
✓ IED을 이용한 이라크 반군 공격으로 인한 피해 증가
✓ 정보기관 DB, 해킹 활용, 반군 커뮤니케이션 네트워크 분석/ 추적하는 사이버 작전 수행, 관련 정보를 지상군 전투와 통합
✓ 사이버 작전과 연계한 지상군 작전 후,
IED 공격 90% 감소

지상군작전 + 사이버 작전 + 정보(INT)

북한의 사이버공격 사례


'09년
'10년
'11년
'12년
'13년
'14년
'15년
'16년
7.7. 디도스 도발('09.7.7)
4.12. 농협 전산망 해킹('11.4.12)
3.4. 디도스 도발('11.3.4)
중앙일보 서버 해킹('12.6.9)
6.25. 전산 대란('13.6.25)
3.20. 전산 대란('13.3.20)
12.9. 한수원 기밀 유출('14.12.9)
국방망 해킹('16.8월~9월)
○○ 홈페이지('16.5월)
SK그룹 해킹('16.1월)

사이버작전 형태



* 출처 : 합동교범 3-24, 합동사이버작전, 합동참모본부, 16.6"

현 연구소 추진 주요과제

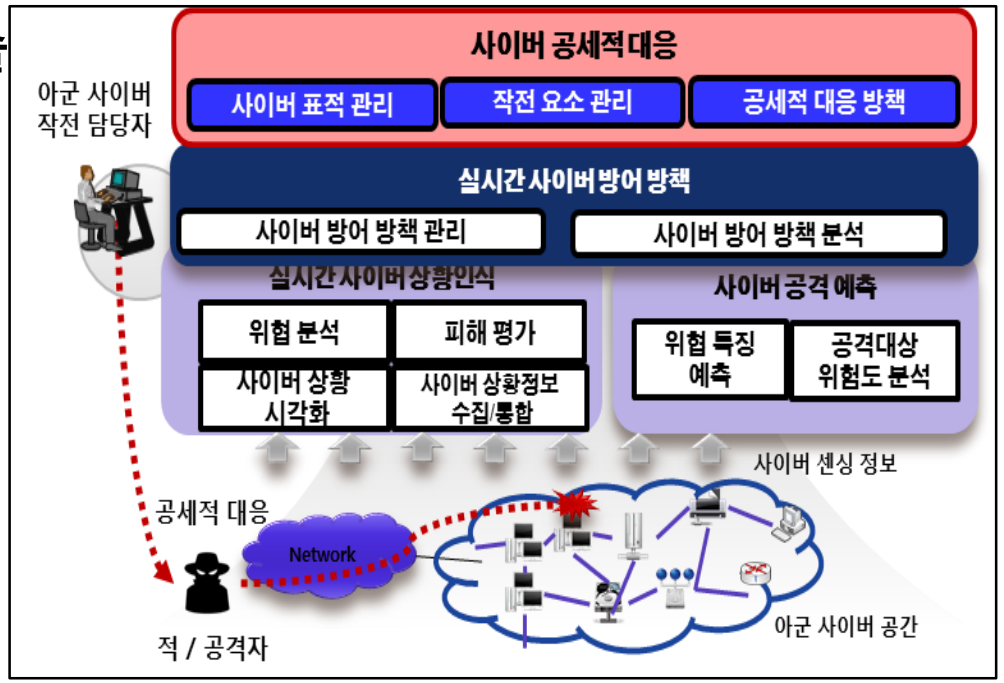
사이버 지휘통제 실시간 의사결정지원 기술(응용)

❑개요

- 사이버 상황인식기반의 공격자 행동예측 기술 및 즉각적인 사이버 방어를 위한 최적을 정보를 제공하는 의사결정지원 기술임.

❑주요내용

- 실시간 사이버 상황인식 기술
- 공격자 행동 예측 기술
- 사이버 방어방책 기술
- 사이버 표적 및 작전요소 관리 기술
- 공세적 대응 판단 기술



❑적용

- 사이버 작전체계

사이버전 모의전투 기술(응용)

❑개요

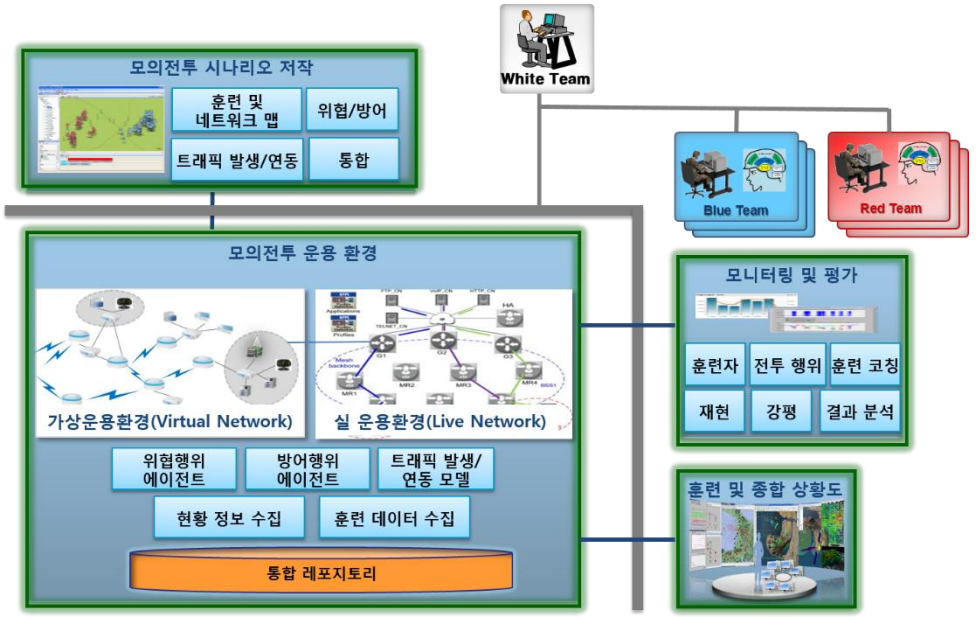
- 사이버 전투 운용 환경과 시나리오 저작 기술을 개발하고, 전투과정의 관찰 및 분석을 통해 전투성과를 평가하는 기술 개발

❑주요내용

- 모의전투 운용 환경 구축
- 모의전투 시나리오 저작
- 모의전투 모니터링 및 평가

❑적용

- 사이버 훈련체계



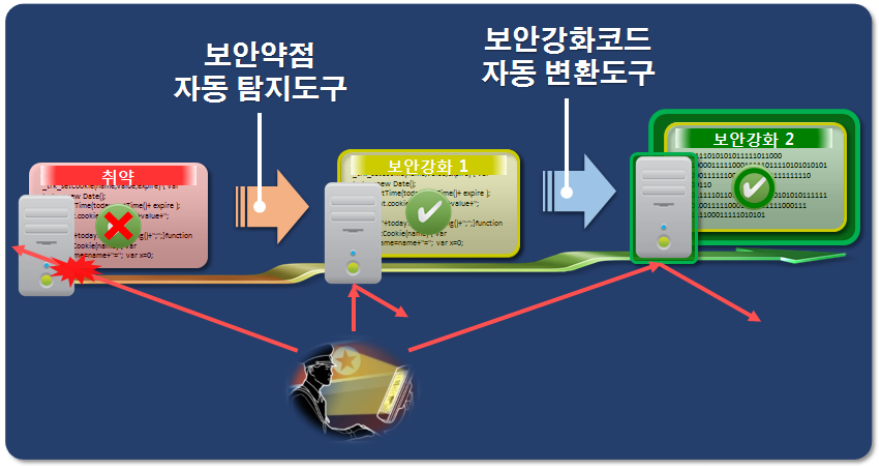
무기체계 내장형 SW 보안강화코드 기술 개발(핵심SW)

❑개요

- SW 구현단계에서 소스코드에 존재하는 보안약점을 탐지하는 기술과 보안이 강화된 실행코드로 변환하는 기술 및 SW 확보

❑주요내용

- 무기체계 내장형 SW 보안약점 분석
- 보안약점 자동 탐지도구 개발
- 보안강화코드 자동 변환도구 개발



❑적용

- C/C++ 언어로 개발된 내장형 SW를 포함하는 무기체계

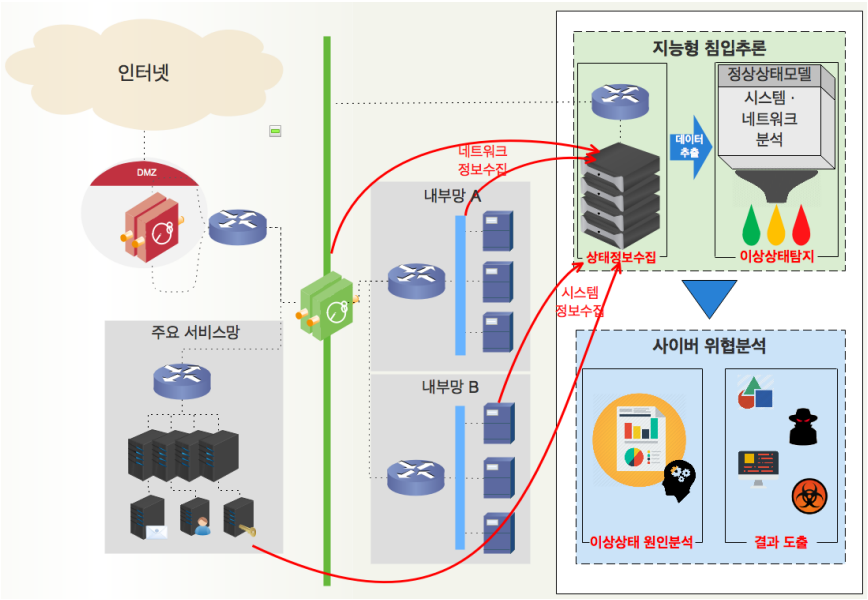
지능형 침입추론 및 사이버위협 분석기술(응용)

❑개요

- 시스템/네트워크의 정상상태 모델링 기술을 개발하고 지능형 기법을 적용한 정상상태 모델 기반의 탐지기법으로 침입위협 여부를 추론하며, 침입탐지 시 이상상태 증상에 대한 관련 정보 식별 및 이상상태 분석을 통해 사이버위협을 분석하는 기술을 연구 개발함

❑주요내용

- 침입추론을 위한 시스템/네트워크 상태정보 수집 기술
- 침입추론을 위한 이상상태 탐지 기술
- 사이버위협 분석 기술

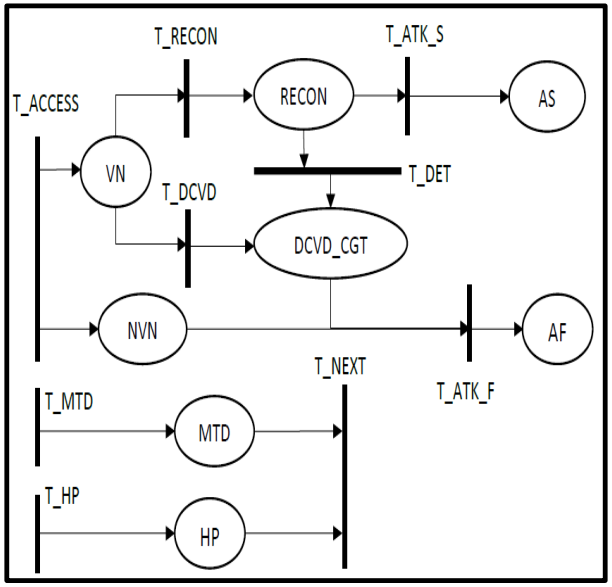


❑적용

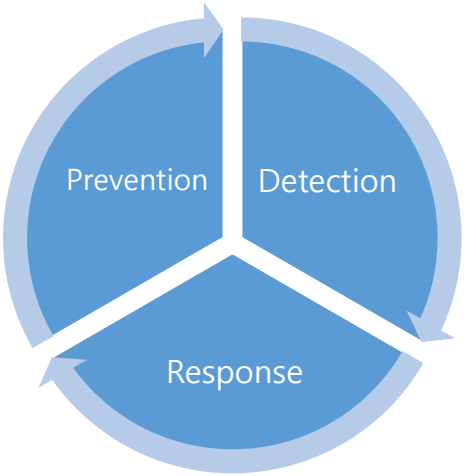
- 사이버 작전체계

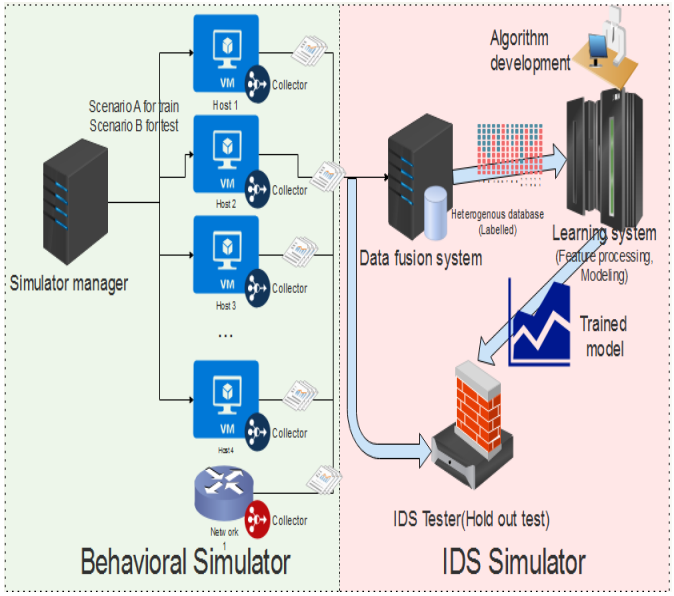
Integrated Proactive and Adaptive Defense System(IPADS)

IPADS



Moving Target Defense(MTD)

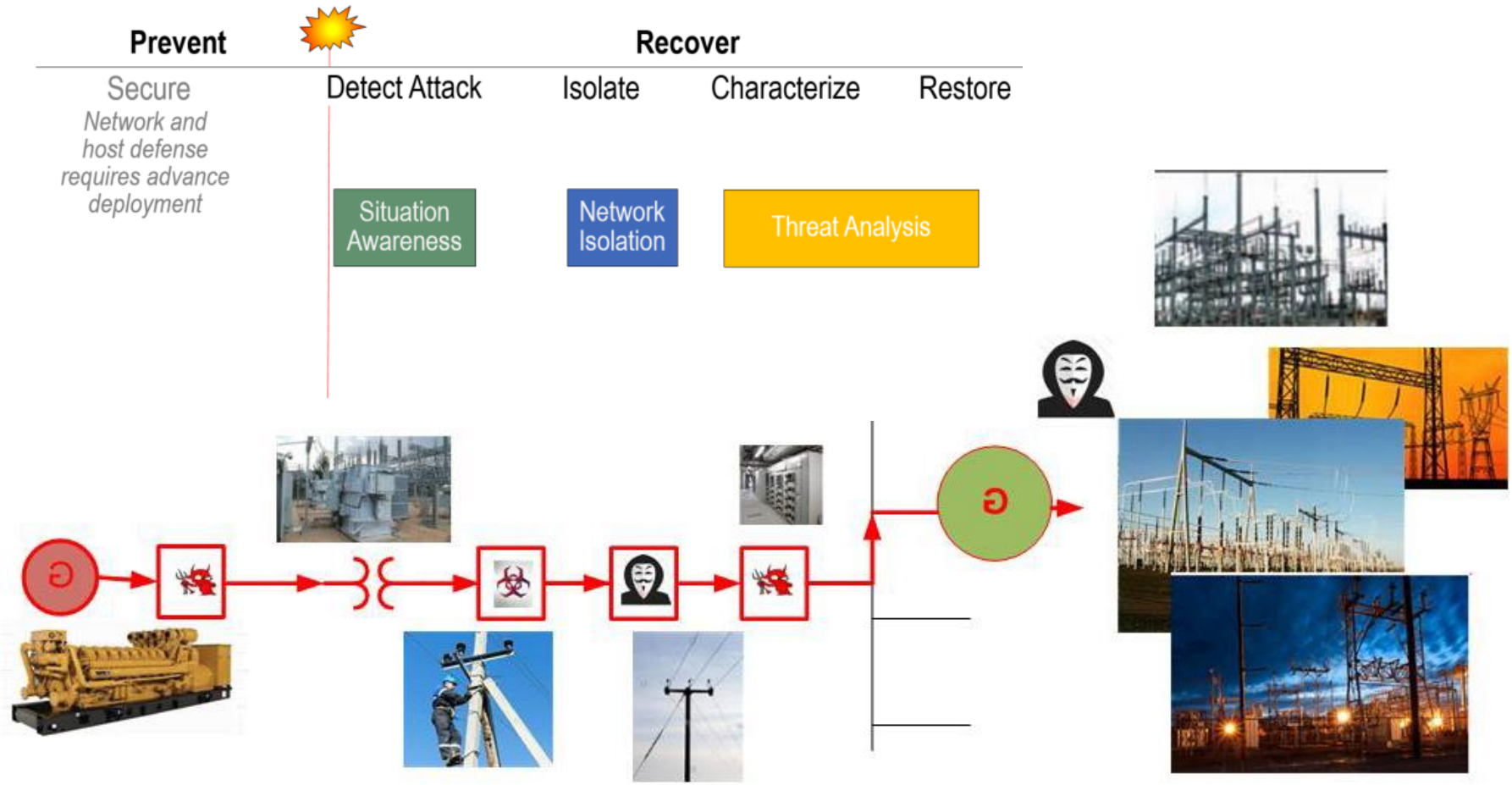




AI based IDS simulator

프로세스 실행 중지, 네트워크 격리	Signature/Policy 업데이트	침입통계 / 패턴분석 / 식별

RADICS (Rapid Attack Detection, Isolation and Characterization Systems) – '16~'20



Goal: Seven Days to Isolate, Characterize & Restore Crank Pathways

AFRL Cyberspace S&T Strategy

Tenets

ALIGN, LEVERAGE AND GROW

INVENT THE FUTURE

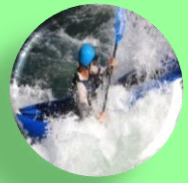
STREAMLINE

Assure and Empower the Mission

- Mission Awareness
- Integrated Full Spectrum Operations
- Command, Control (C2) and Decision Support

Enhance Agility and Resilience

- Cyber Maneuver and Response
- Resilient Architectures
- Military-Grade Hardware and Software



Create Next-Gen Cyber Warrior

- Visualization
- Augmentation of the Cyber Warrior
- Cyber Workforce (Select, Educate and Train)

Invent Foundations of Trust and Assurance

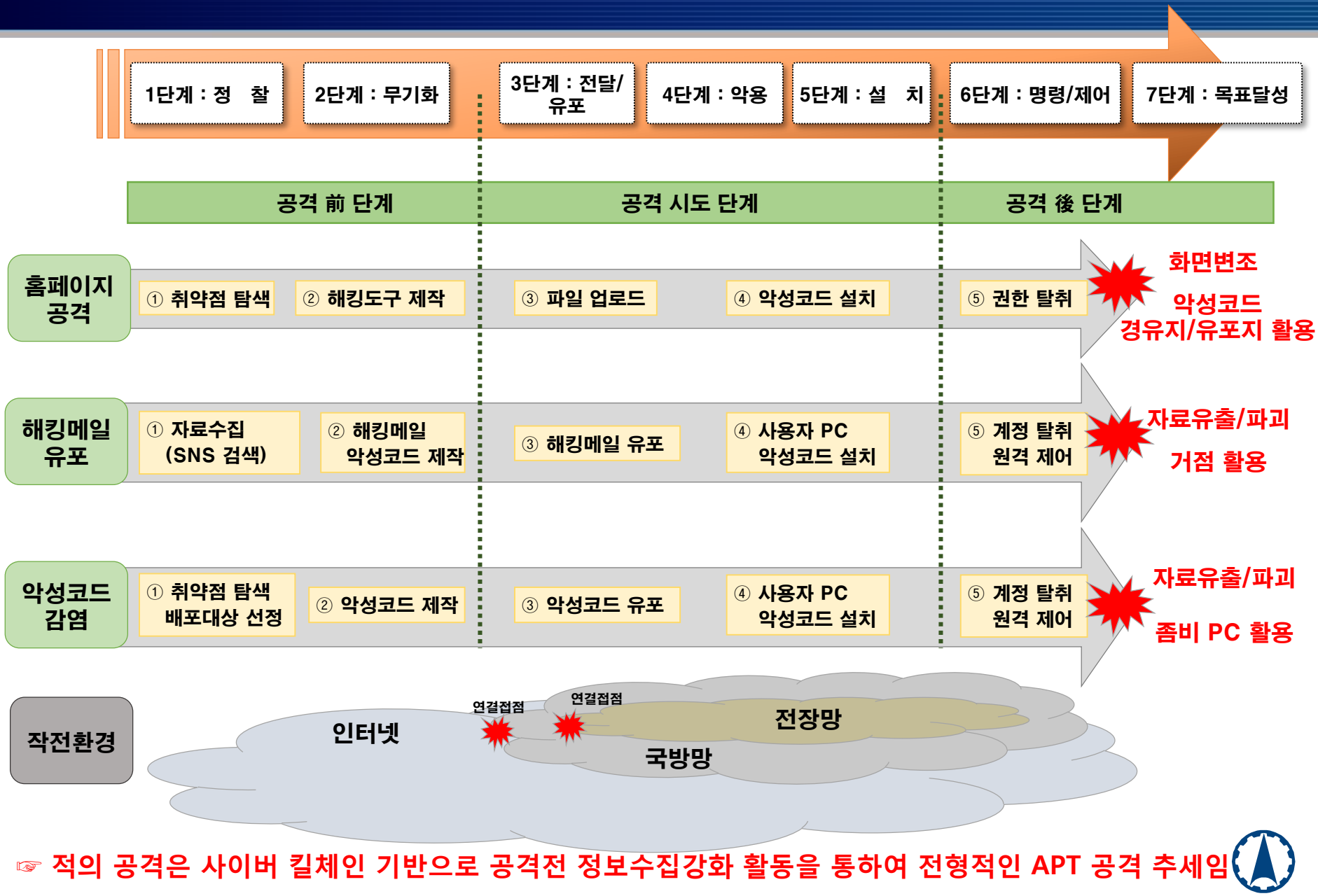
- Scientific Foundations of Mission Assurance
- Scientific Foundations of Trust
- Supply Chain Trust

Establish a firm foundation in cyberspace to build mission capability upon

DCO 관점 제언 :

방어역량 강화 포인트 1

사이버 킬체인 기반 적 공격전술



☞ 적의 공격은 사이버 킬체인 기반으로 공격전 정보수집강화 활동을 통하여 전형적인 APT 공격 추세임

사이버 킬체인 기반 공격 특징

- ❑ 대부분의 백신 100% 탐지 불가능
  - 공격자는 공격전에 다양한 백신 제품에 대하여 공격무기를 시험검증함
  - 다양한 멀웨어 탐지를 회피하기 위한 위장기법을 보유함
- ❑ 탐지를 회피하기 위하여 합법적으로 시스템을 사용할 권리를 취득함
  - 많은 방어도구는 이러한 종류의 악의적인 사용을 탐지할 만큼 충분한 자료를 수집하지 않음
- ❑ APT 공격은 합법적인 SSL로 암호화
- ❑ 적은 빠르게 방어자보다 공격기법을 개발

☞ 완벽한 방어체계 구축은 어려움, 다계층 방어체계를 구축하여, 공격자로 하여금 공격에 성공할 수 있는 시간을 지연시키는 전략이 필요함

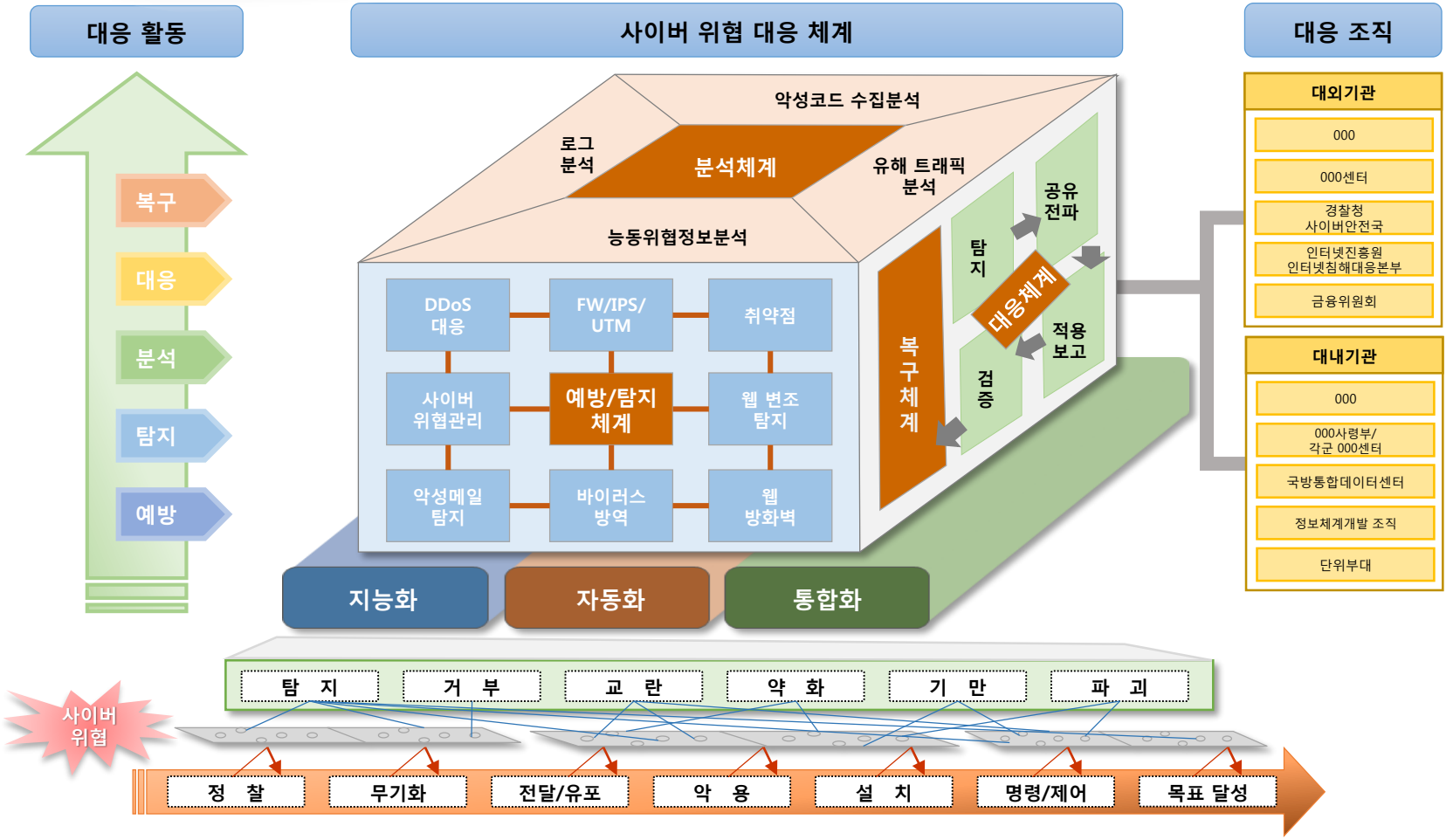
☞ 지속적인 사이버 공방훈련을 통하여 방어 TTP(전술, 기술, 절차) 개발과 검증, 부족 능력 식별과 투자요소 도출/보강이 필요함

* 출처 : MITRE, Finding Cyber Threats with ATT&CK-Based Analytics, June 2017

국방 사이버위협 대응체계

❑ 비 전

사이버킬체인 기반으로 능동대응 할 수 있는
국방 사이버위협 대응체계 구축



- 경계선 방어에 중점
- 知彼知己에 보다 신경을 써야 함

NetOps 관점 :

우리가 신경써야 할 또 한가지...

무기체계 사이버 위협

전자신문

2018년 06월 20일 수요일 001면 종합

실전 배치된 軍 무기체계 SW '보안 무방비'

정보보호인증센터, 무기체계 SW 보안 검증…"기본도 안지켜"
소스코드 내 암호키 노출돼 해커가 계정획득 후 정보 탈취 우려
악성코드 발견돼도 오작동 일으킬라 치료 못하고 그대로 운영

김인순 insoon@
보안 전문기자

군이 사용하고 있는 무기 체계 소프트웨어(SW) 보안이 위험 수준인 것으로 드러났다. 무기 체계 SW 소스 코드와 주석문, 설정 파일 내 관리자 계정 다. 전체 기능 90%가 SW로 구현되는 등 무기 체계 내 SW 비중과 중요성은 높다.

기무사 정보보호인증센터 관계자는 "두 번에 걸친 시범 검증에서 무기 체계에 쓰인 소스 코드 내 암호키가 그대로 들어있고, 취약한 암호 알고리즘이 사용된 사례를 발견했다"면서 "해코드에 감염되는 사례가 많다"고 설명했다. 이 관계자는 "무기 체계에서 악성코드가 발견돼도 치료할 수 없는 구조"라면서 "악성코드 치료로 무기 체계가 오작동을 일으킬 수 있다"고 덧붙였다.

군은 무기 체계 전용 백신을 개발·배포하는 1차 조치만 취했다. 전용 백신은 PC나 무기 체계에 설치하지 않고 USB나 CD에서 실행하는 휴대형이다. 무기 체계 내 악성코드 감염 여부만 탐지하고 치료는 하지 않는다. 사이버 위협을 안고 무기 체계를 운영하는 상황이다.

무기체계 사이버 위협

❑운영단계의 취약점 제거 비용은 개발단계에서 보다 60~80배의 비용 소요(IBM)

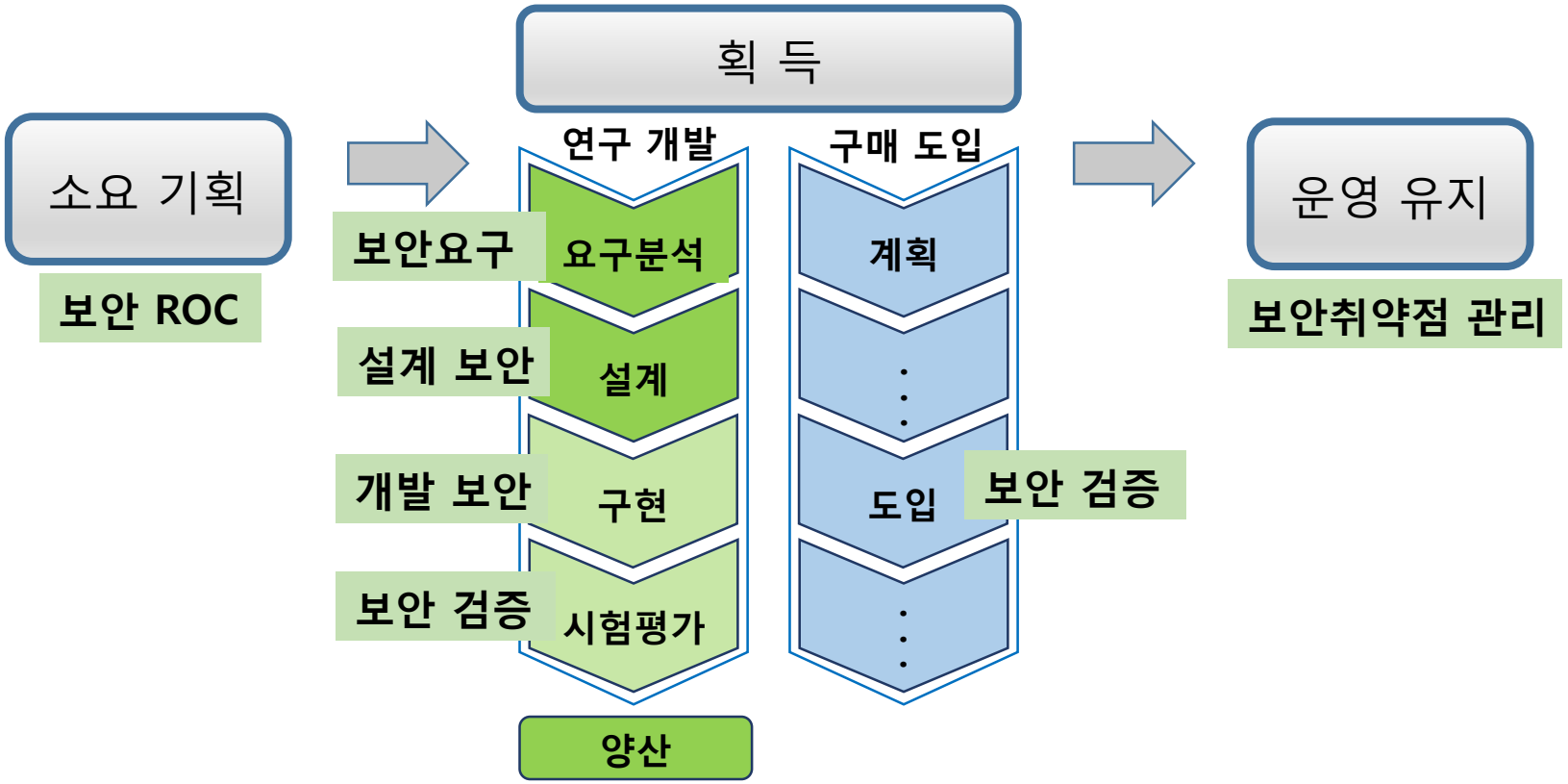
※ 출처: 국방SW발전 포럼 및 동계워크샵, 2015.2.

❑안전한 무기체계 SW를 확보하기 위하여 공급사슬 전체에 대한 위험 관리 방안 필요

무기체계 SW를 잘 만들자!!!

무기체계 획득 전 단계에서
보안성 강화 노력 필요

무기체계 획득 단계 보안성 강화




기동무기체계


유도무기체계


감시정찰무기체계

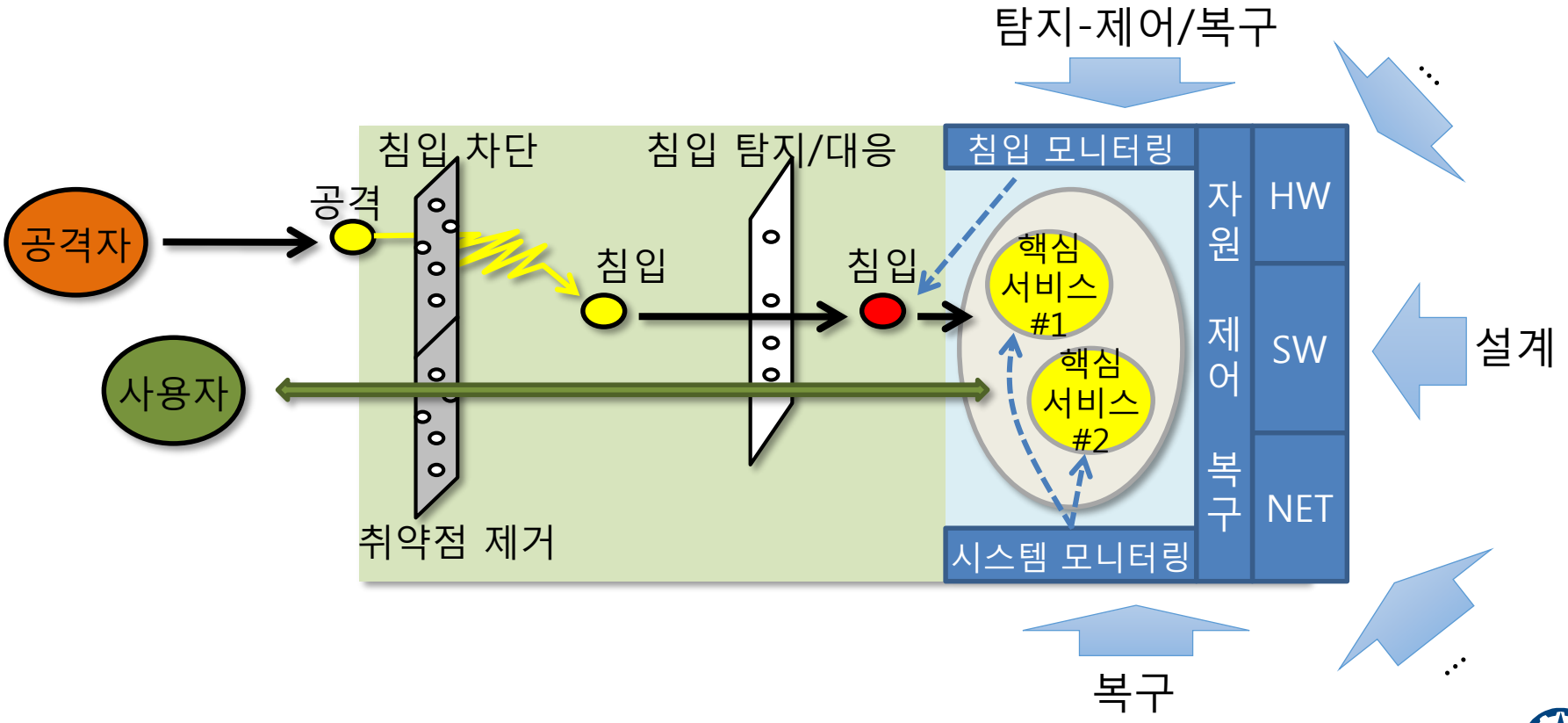

함정전투체계


항공무기체계

사이버 방어 : 침입감내

❑기술개요

- **알려지지 않은 적의 사이버 공격에도 아군 시스템의 정보서비스를 지속적으로 제공할 수 있도록, 정보 시스템, 통신 네트워크, 무기체계 내장형 시스템의 자원을 제어·복구·재구성하여 보호하는 기술**



전력증강 관점 :

사이버전 무기체계

- 사이버작전체계, 사이버훈련체계만 구축되면 사이버전력이 완성되는 것은 아님
- 감시정찰 무기, 능동방어 무기, 공세대응 무기 등이 작전체계의 프레임 위에서 퍼즐처럼 끼워져야 하며, 이는 진화적으로 발전되어야 함
- 사이버 특성에 맞는 획득 프로세스 개선이 요구됨

결 론

- ❑ 방어적 측면에서 면밀한 피아식별이 중요하며, 이는 실시간으로 인식되어야 함
- ❑ 모든 무기체계는 사이버 대응 능력이 요구됨
- ❑ 사이버전 무기체계 개발은 큰 프레임 속에서 지속적/진화적으로 발전되어야 함
- ❑ 사이버전 전승의 요인은 스마트한 인재 뿐만 아님
  - Machine Speed Intelligence Sharing
  - Automation for Defensive & Offensive Operation

감사합니다

Q&A