사이버 안보의 진화:
복합지정학의 시각

제16차 평화학 포럼

서울대학교 통일평화연구원

김 상 배

(서울대학교 정치외교학부 교수)

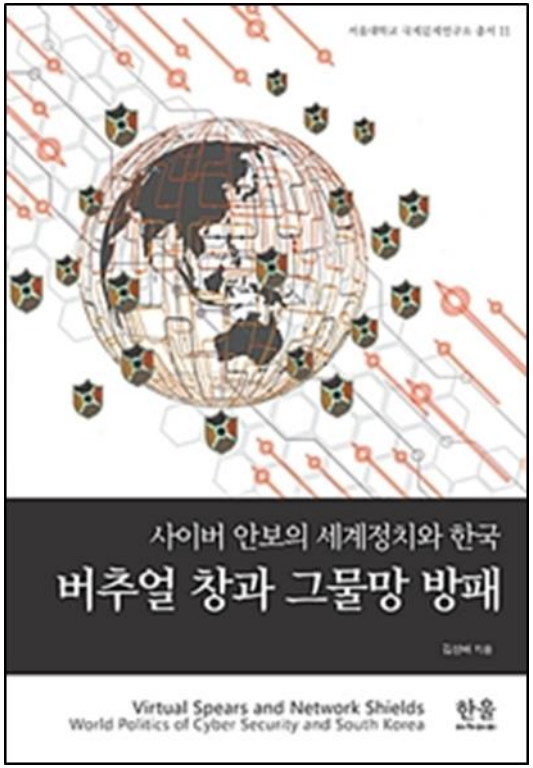
2022년 11월 28일

내 용

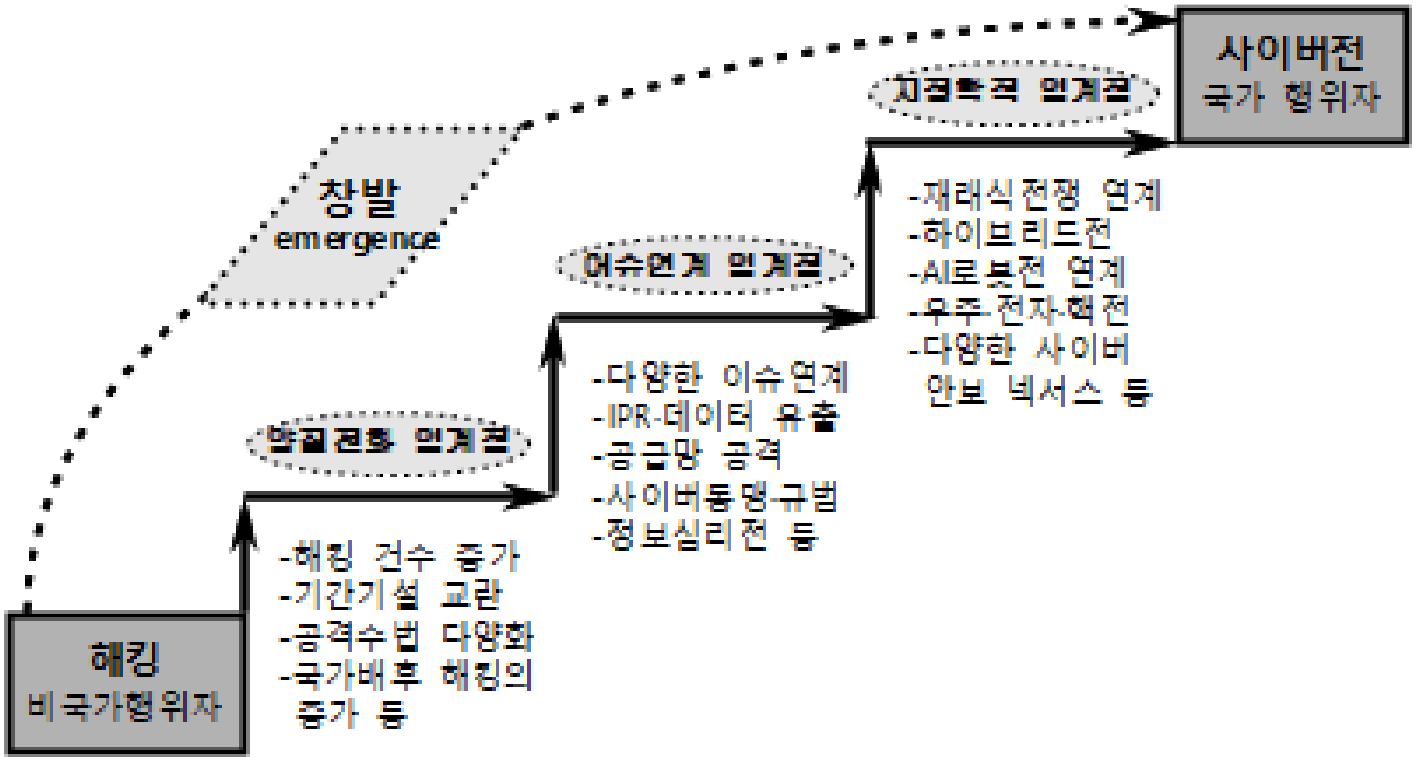
- 사이버 공격의 증가와 변천
  - 사이버 공격의 다변화
  - 국가 배후 사이버 공격의 증가
- 사이버 안보위협의 이슈확장
  - 데이터 유출과 공급망 공격의 위협
  - 사이버 동맹/규범, 정보심리전의 전개
- 사이버전의 부상과 미래전의 전망
  - 재래식 전쟁, 하이브리드전, 우주전자전
  - 사이버 안보의 복합 넥서스

버추얼 창 vs. 그물망 방패

사이버 안보의 복합지정학과 한국



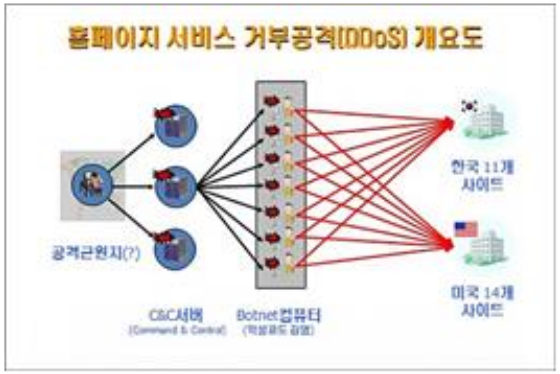
사이버 안보의 진화


해킹
비국가행위자
-해킹 건수 증가
-기간기설 교란
-공격수법 다양화
-국가배후 해킹의
증가 등
창발
emergence
영향력화 임계점
-다양한 이슈연계
-IPR-데이터 유출
-공급망 공격
-사이버동맹-규범
-정보심리전 등
이슈연계 임계점
-재래식전쟁 연계
-하이브리드전
-AI로봇전 연계
-우주-전자-핵전
-다양한 사이버
안보 넥서스 등
지경학적 임계점
사이버전
국가 행위자

사이버 공격의 특성

- **복합 네트워크 구조 속의 안보 문제**
  - 인터넷 자체가 착취혈(exploit)을 안고 있는 취약한 환경 → 그 틈새를 공략
  - 이를 배경으로 "비대칭 전쟁" 발생 → 공격이 방어보다 유리한 게임, 피해대상을 구분하기도 어려움, 공격자에게도 피해 전파 가능성
- **과학기술 변수 그 자체가 위협**
  - 컴퓨터 바이러스, 악성코드, 디도스 공격(좀비 PC), 지능형지속공격(APT), 스턱스넷, 랜섬웨어 등이 비인간(non-human) 행위자로서 행동 (ANT)
- **비국가(non-state) 행위자의 위협**
  - 해커들의 장난 → 테러리스트의 무기
  - 최근에는 국가 배후 사이버 공격이 증가
- **범죄의 재구성과 안보화(securitization)**

2009년 7.7. 디도스 공격



사이버 공격의 개념적 복합성

<table>
<tr><th>공격목적
공격주체</th><th>물리적 파괴</th><th>시스템 교란</th><th>자원의 획득</th></tr>
<tr><td>국가</td><td>사이버 전쟁</td><td rowspan="3">사이버 교란

사보타지
(스턱스넷 공격)

서브버젼
(어노니머스)</td><td>사이버 간첩</td></tr>
<tr><td>집단</td><td rowspan="2">사이버 테러</td><td rowspan="2">사이버 범죄</td></tr>
<tr><td>개인</td></tr>
</table>

사이버 공격 패턴의 변천

- 국가 기간시설에 대한 해킹 공격
  - 공공기관, 금융기관, 언론미디어 등
  - 디지털 인프라, 에너지망, 식량 공급망
- 지식재산권 절취, 기밀 데이터의 절취
  - 군사 분야 무기 데이터, 인사정보 데이터
  - 기업의 첨단 기술, 코로나19 백신 등
- 경제적 이득을 위한 공격
  - 금전을 요구하는 사이버 범죄와의 결합
  - 금융기관 해킹: 방글라데시 중앙은행 SWIFT 해킹
  - 표적형 랜섬웨어 공격, 암호화폐 해킹(비트코인 거래소 공격) 등
- 사이버 공간을 매개로 한 정보심리전과 연계
  - 원자력 발전 시설에 대한 공격위협: ex) 한수원 해킹의 정보심리전 효과
  - 2022년 우크라이나 전쟁의 사례

코로나19와 사이버 안보

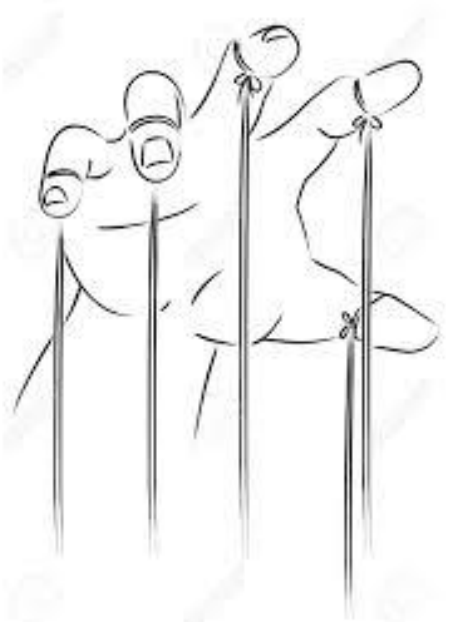
- 최근 코로나19로 인해서 조성된 비대면(untact) 환경을 위협하는 사이버 공격이 늘어나고 있음
  - 디지털 전환(digital transformation)으로 삶의 많은 영역이 사이버 공간으로 들어오면서 이를 겨냥한 범죄와 테러, 스파이 활동도 사이버 공간으로 빠르게 이동하고 있음
- 안전이 검증되지 않은 원격회의 소프트웨어는 시민들의 개인정보와 기업 및 국가 기밀을 노출시켰고,
  - 사람들의 공포심을 이용한 스미싱과 가짜뉴스들도 지속적으로 증가하고 있음
- 백신 연구기관을 대상으로 백신개발 정보를 빼내려는 사이버 간첩 활동도 본격화되고 있음
  - 중국, 2020년부터 코로나19와 관련된 기술과 정보 해킹에 집중
  - 모더나, 아스트라제네카, 화이자(북한 해커), 길어드사이언스(렘데시비르 개발사) 등이 공격 당함
- 그야말로 '코로나 바이러스'를 피해간 비대면 환경을 매개로 하여 '컴퓨터 바이러스'가 급습하는 양상이 펼쳐지고 있음

AI활용 사이버 공격/방어

- 사이버 공격과 방어에 인공지능(AI) 활용
  - AI를 활용하여 무차별적으로 바이러스를 전파 → 속도의 우월성 → 만약에 AI가 개발한 바이러스가 나온다면?
  - 위협정보 분석, 이상징후 감지, 알고리즘 기반 예측 등 사이버 방어에도 AI를 활용
- 사이버 공격의 지능화, 자동화, 자율화
  - 사이버무기도 완전 자율화되는 방향으로 진화
  - 자율적으로 사이버 공방을 주고받는 사이버 로봇 개발
  - 인공지능 알고리즘의 스토리텔링 및 대규모 정보 확산 기술에 기반을 둔 디지털 프로파간다(digital propaganda) 활동
- 스스로 방어하는 자율무기체계 vs. 새로운 취약점을 찾고 공격하는 사이버 자율무기 간의 공방?
  - 조만간 사이버 자율무기는 자체 취약점을 진단하고 자동으로 패치하고 사이버공격에 대응하여 스스로를 방어하는 단계로 갈 뿐만 아니라
  - 더 나아가 선제적 사이버 방어 차원에서 적의 사이버 공격에 대응해 스스로 결정하여 사이버 반격을 수행하는 단계에까지 이르게 될지도

국가 배후 사이버 공격

- 해커들의 영역으로 알려졌던 사이버 공격에 국가 행위자들이 전면에 나서는 추세
  - 직접 사이버 공격의 주체가 되거나 해커그룹, 댓글부대 등을 프록시 병력으로 이용
- 국가의 그림자: 러시아의 사례
  - 2007년 에스토니아에 대한 사이버 공격
  - 2008년 조지아에 대한 사이버 공격
  - 2014년 우크라이나에 대한 공격
- 미국/이스라엘과 이란의 사이버 공방
  - 2010년 이란의 핵 시설에 대한 공격(스턱스넷)
  - 2012년 미국과 사우디 및 카타르에 대한 이란의 사이버 공격
- 2010년대 미국과 중국의 사이버 공방
  - 미국의 안보화: 중국해커위협론
  - 미중 글로벌 패권경쟁의 일환
- 북한의 대남 사이버 공격
  - 2009년 7.7 디도스 공격 이후... 3.20 사이버 공격...
  - 북한의 공격수법과 목적의 진화



사이버 공격과 데이터 유출

- 사이버 공격: 정보-데이터 자원이나 지적재산 절취 목적 → cyber espionage
- 정부/군 차원의 작전
  - 2003 중국의 타이탄 레인 작전: 미군과 미 시스템 겨냥
  - 2012년 Flame: 미국이 이란에 악성코드 침투, 데이터 자원 목표
- 2010년대 중국 해커들의 미국 시스템 해킹
  - 2013년 2월: 중국 61398부대(맨디언트 보고서) → IT, 항공우주, 과학연구, 컨설팅 분야
  - 2015년 미 연방인사관리처(OPM) 해킹→ 미 상원의원, FBI요원 인사정보 누출
  - 2016년 12월 미 연방예금보험공사(FDIC) 해킹
  - 중국 해커, 미 군사 정보-데이터의 절취
- 2010년대 후반 북한 해킹 → 데이터 절취 + 금전적 이득을 노린 해킹 급증
  - 2016년 북한의 방글라데시 중앙은행 SWIFT 시스템 해킹
  - 북한의 외화벌이 작전 → 2017년 12월 국내 비트코인 거래소 유빗 해킹
  - 한국의 국방망, 방산업체의 무기체계 데이터 절취
  - 2017년 5월 라자루스의 워너크라이 랜섬웨어 공격

사이버 안보위협의 증대

- 2021년 전반 → 미국 vs. 러·중 간의 사이버 갈등 유난히 떠들썩
  - 바이든 대통령, 러시아에 대해 "사이버 공격이 실제 전쟁을 초래할 수 있다"고 경고(7월 27일 DNI 방문 시)
  - 미국은 아프간 철군 이후 미국 외교정책의 기조를 중국과 사이버전에 치중하겠다고 발표 (7월초)

- 미국의 대응: 사이버 대응역량 강화의 적극적 행보
  - 사이버 정책 요직에 공세적 성향의 전문가들 기용
  - 러시아 제재 행정명령(2021.4.)
  - 콜로니얼 파이프라인 해킹 이후 사이버 안보 강화 행정명령(2021.5.)
  - 핵심 인프라 시설에 대한 사이버 안보 강화 지시 (2021.7.)
  - EU, 나토 등과 함께 중국의 MS 익스체인지 서버 공격 비난→ 나토가 중국의 사이버 활동을 비난한 최초의 사례(2021.7.)

러시아 배후 사이버 공격

- 2020년 하반기 미 대선 방해 시도
  - 2016 대선, 2018 중간선서 이후 허위조작정보, 가짜뉴스를 통해
- 2020년 12월 미국 최대 보안 솔루션 업체 솔라윈즈 해킹
  - 러시아의 신생 해커조직인 '노벨리움'이 2019년 9월-2020년 6월 여러 단계를 거쳐서 감행
  - 정부와 기업의 네트워크 상황을 모니터링하는 솔루션인 오리온 취약점 공략
- 2021년 5월 7일 미국 최대 송유관업체인 콜로니얼 파이프라인에 대한 랜섬웨어 공격을 가해 시스템이 마비됨
  - 러시아 해킹조직 '다크사이드'의 소행으로 지목
- 2021년 5월 30일 세계 최대 육류 공급업체 JBS가 사이버 공격을 받아, 호주 및 캐나다 공장의 생산라인 가동이 일부 중단됨
  - 송유관 해킹 이후 3주 만에 발생→해커들이 원자재를 주요 타깃으로 삼고 있다는 해석이 나옴
- 2021년 7월 2일 시스템 제어 소프트웨어 업체 카세야에 대한 랜섬웨어 공격 발생
  - 러시아 해킹 그룹 '레빌'이 랜섬웨어 공격을 감행하고 7천만 달러의 대가를 요구

중국 배후 사이버 공격

- 2020년부터 코로나19와 관련된 기술과 정보 해킹에 집중
  - 모더나, 아스트라제네카, 화이자(북한 해커), 길어드사이언스(렘데시비르 개발사) 등이 공격 당함
- 2021년 1월과 3월 마이크로소프트의 이메일·메시지 플랫폼인 익스체인지 서버 해킹
  - 중국 배후 해커 조직 '하프늄'이 개시한 것으로 알려짐
- 2021년 4월 20일 방위산업 관련 소프트웨어 보안 솔루션 업체 펄스시큐어의 VPN 취약점을 이용해 악성코드 심음
  - APT5라 불리는 중국 해커집단 소행으로 추정
  - APT5는 미국, 유럽, 아시아의 항공우주, 방위산업 기관을 주로 공격하는 해커 조직
- 2021년 4월 중국 해커들의 뉴욕 지하철 컴퓨터 시스템 해킹
  - 해커들은 열차 통제 시스템까지는 접근하지 않았고 피해도 적었지만
  - 교통국 컴퓨터 시스템이 뚫렸다는 자체만으로 교통 체계의 보안 취약성이 그대로 드러남
- 2021년 중국 정부 후원의 일명 '키메라' 조직이 대만 반도체 기업 해킹 시도

북한 배후 사이버 공격(1)

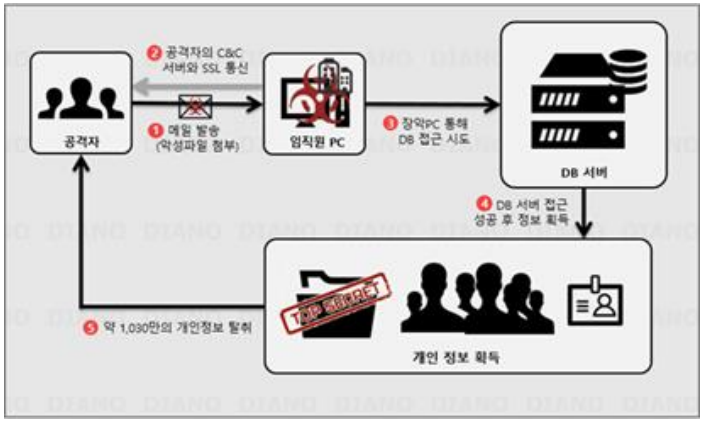
	피해 내용	추정 근거	공격 방법
7.7 디도스 공격 (2009.7.7)	청와대와 국회, 네이버, 미국 재무부와 국토안보부 등 23개 사이트 마비	"테러에 동원된 IP 추적 결과, 북 체신성이 사용해온 것으로 확인" (국정원 국정감사, 2009.10.29)	디도스 공격, 61개국 435개 서버 활용 좀비 PC 27만 여대 동원
3.4. 디도스 공격 (2011.3.4)	청와대, 국가정보원 등 국가기관과 국민은행 등 금융기관 등 주요 웹사이트 마비	"사건 분석 결과 공격 방식이 2009년 7월 발생한 디도스 공격과 일치" (경찰청 발표, 2011.4.6)	디도스 공격, 70개국 746대 서버 활용 좀비 PC 10만 여대 동원
농협전산망해킹 (2011.4.12)	농협 전산망 악성코드 감영으로 장애 발생, 인터넷 뱅킹 등 서비스 중단	"공격 진원지인 노트북에서 발견된 IP가 과거 정찰총국에서 사용된 것" (검찰청 발표, 2011.5.3)	디도스 공격, 13개국 27개의 서버 동원
중앙일보 해킹 (2012.6.9)	내부관리자 PC를 경유하여 중앙일보 전산망 침입으로 홈페이지 변조 및 일부 데이터 삭제	"조선체신회사(체신청 산하)가 중국회사로부터 임대한 IP대역을 통해 접속" (경찰청 발표, 2013.1.16)	APT 공격, 국내 서버(2대) 해외 10개국 서버(17대) 동원
3.20 방송·금융사 침입 (2013.3.20)	KBS, MBC, YTN 등 언론사와 신한은행, 농협 등 금융기관 전산망 마비. 내부망 백신업데이트 서버 및 업무 PC 감염	"공격에 사용된 IP주소 및 해킹 수법 분석 결과 7.7 디도스와 같이 북한 소행으로 추정되는 증거 상당량 확보" (민관군 합동대응팀, 2013.4.10)	APT 공격, 국내외 경유지 49개 동원 악성 코드 76종 사용
6.25 디도스 공격 (2013.6.25)	청와대, 국무조정실 홈페이지 해킹, 11개 언론사, 5개 정부기관 및 정당 등 16개 기관 해킹	"북한이 사용한 IP 발견, 공격방법이 3.20 사이버 테러와 동일" (민관군 합동대응팀, 2013.7.16)	변종 디도스 공격, 악성코드 82종 좀비 PC 활용

소니 영화사 해킹 (2014)

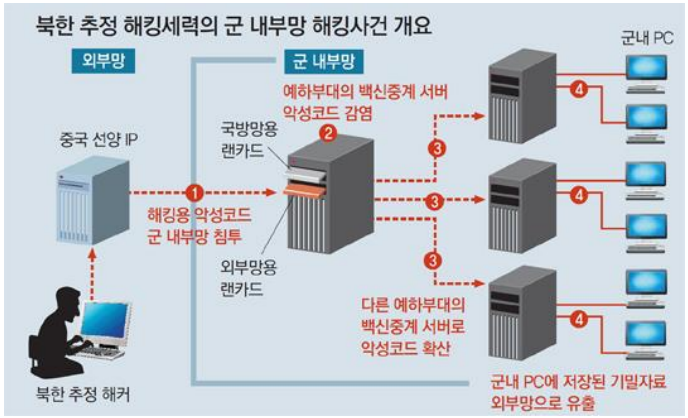
- 북한 김정은 암살을 다룬 영화 '인터뷰' 관련 소니 영화사가 해킹 당함
  - 2014년 12월 19일, FBI는 보도자료를 통해 소니 영화사 해킹 조사 결과 북한이 배후라고 지목
- 북한에 대한 미국의 대응
  - 2014년 12월 21일, 오바마 대통령은 북한의 해킹이 '사이버 반달리즘'이라 규정하고 비례적 대응조치를 취할 것을 천명
- 북미 사이버 전쟁?
  - 2014년 12월 19일 이후 북한의 웹사이트에 접속 장애가 발생했으며, 3G 통신망 역시 마비
  - 2015년 1월, 2015년 4월 오바마 대통령은 행정명령을 통해 북한 정찰총국 등에 대한 경제 제재 …

북한 배후 사이버 공격(2)

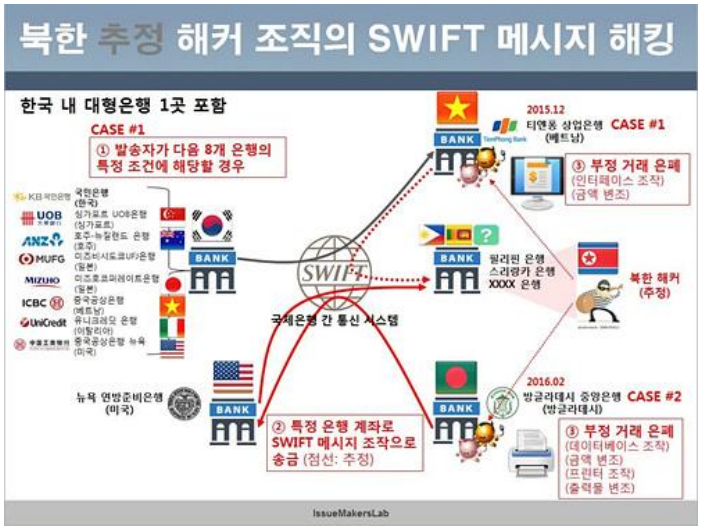
2016년 7월 온라인 쇼핑몰 인터파크 해킹



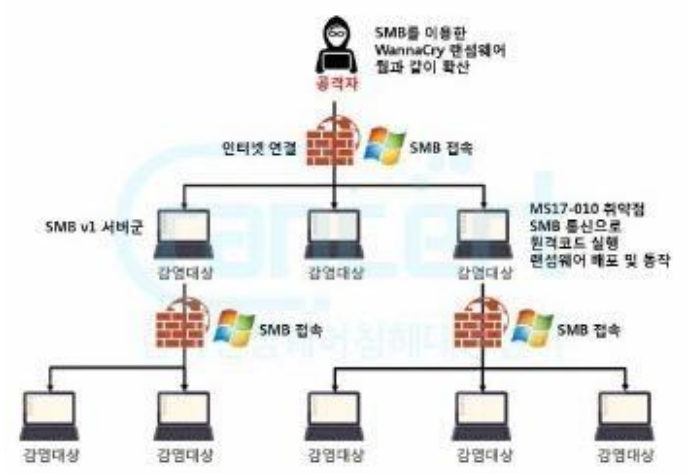
2016년 8월 국방부 내부 전산망 해킹 사건



2016년 2월 방글라데시 중앙은행 SWIFT해킹



2017년 5월 워너크라이의 랜섬웨어 공격



북한 배후 사이버 공격(3)

- 2020년 8월 북한 해커, 뉴욕 및 전세계 금융기관 해킹
  - 2020년 12월 미 법무부는 북한 정찰총국 소속 해커 박진혁, 전창혁, 김일 등을 기소
- 2020년 미국과 서방의 백신과 치료제 절취 사이버 공격 감행
  - 2020년 12월 존슨앤존슨, 노바백스, 신풍제약 등에 대해 사이버 공격 시도
- 2021년 5월 14일 한국원자력연구원(원자력 잠수함용 소형 원자로 개발) 해킹
  - 북한 정찰총국 산하 해커조직인 '킴수키(kimsuky)'로 추정되는 IP를 통해 해킹을 당했다고 알려짐
- 2021년 6월 20일엔 잠수함 건조업체인 대우조선해양 해킹이 뒤늦게 알려짐
  - 2020년 해군 3000t급 신형 잠수함 등 각종 함정을 건조하는 대우조선해양을 해킹해 일부 자료가 유출
- 2021년 6월 16일 한국항공우주산업(KAI) 해킹: 한국형 전투기 KF-21를 제작
  - 북한 해킹조직 '안다리엘'의 소행으로 지목됨: VPN 취약점 공격
- 2020년 우주발사체·위성을 개발하는 한국항공우주연구원(항우연·KARI)도 해킹을 당한 것으로 뒤늦게 확인됨
  - 항우연은 한국형 우주발사체 등 각종 민간 로켓과 아리랑 위성 등 위성 개발

공급망 보안과 수출입규제

- 2010년대 후반 사이버 안보 문제는 중국의 기술추격에 대한 미국의 견제와 만남
  - '안보화'(securitization)를 통해서 수출입 이슈와 연계
  - 공급망 보안: 백도어, 악성코드 삽입의 문제에 대한 우려
- 화웨이 사태 → 수입규제의 문제와 연계
  - 5G이동통신망, 백도어를 통한 데이터 유출 우려
- 민간 드론 시장 규제→ 중국의 DJI를 겨냥
  - DHS CISA, 중국의 드론을 '잠재적 위협'이라고 경고
- 2017년 하이크비전, 다후아 등 CCTV업체 규제 → 소수민족 감시 우려
  - 2019년 안면인식 AI기업, 센스타임, 메그비, 이투 등 규제
- 2018년 CFIUS, 앤트파이낸셜의 머니그램 인수 제지
  - 2019년 5월 중국 게임회사 쿤룬 → 미 SNS 그라인더(성소수자 커뮤니티) 매각 (미국정부의 매각 명령)
- 중국 스타트업인 바이트 댄스의 틱톡(15초 짜리 동영상 서비스) 사용 금지
  - 바이트댄스의 뮤지컬.리 인수에 대한 조사
  - 중국의 지배적 SNS인 위챗도 제재의 대상으로 부각

공급망 공격의 심화

- SW개발업체, 제조업체, IT서비스 관리업체 등 ICT 공급망 타겟 사이버 공격 증가
  - 공급망 공격은 대부분 공급업체 코드에 집중(최근 공급망 공격의 66%가 코드 공격)
  - 2020년 12월 미국 최대 보안 솔루션 업체 솔라윈즈 해킹 (러시아)
  - 2021년 7월 시스템 제어 소프트웨어 업체 카세야에 대한 랜섬웨어 공격 (러시아)
  - 2021년 4월 방산 관련 SW 보안 솔루션 업체 펄스시큐어의 VPN 취약점을 이용해 악성코드 심음 (중국)

사이버 동맹의 전개

- 사이버 안보 이슈는 화웨이 사태를 계기로 동맹이슈로 비화
  - 미국과 파이브 아이즈(Five Eyes): 영국, 캐나다, 호주, 뉴질랜드의 동조
  - 일본, 독일, 프랑스도 가담: 파이브 아이즈+3
  - 그러나 2019년 2월말을 넘어서 사이버 동맹전선의 균열 조짐도 발생
  - 2019-20년 홍콩사태와 코로나 사태를 겪으면서 재결속 경향

- 사이버 안보와 미국의 인도태평양 전략
  - 2019.4. <인도·태평양 국가 사이버 리그(CLIPS)> 법안이 상원에서 발의
  - 2019.6. '인도·태평양 전략보고서'→ 화웨이 사태를 중국이 수행하는 하이브리드전으로 규정

- 중국의 '일대일로' 이니셔티브와 사이버/데이터 안보
  - 해외통신 인프라 확충을 가속화
  - 21세기 디지털 실크로드 건설을 위한 연대외교 추진

- 2020년 美 클린 네트워크 vs. 中 글로벌 데이터 안보 이니셔티브
  - 폼페이오: 중공으로부터 중요한 데이터와 네트워크를 수호 (2020.8.5)
  - 왕이: 각국은 국가안보, 경제, 사회안정과 관련된 데이터 수호 책임과 권리 보유 (2020.9.8)

사이버 안보외교 및 국제규범

- 양자외교 차원의 사이버 안보외교 전개
  - 미중: 2015년 미중 사이버 합의 수준을 기대 → 아직 진전 없음
  - 미러 정상회담: 2021년 러시아 해커의 사이버 공격에 대해 논의 → 카세야 해킹을 가한 러시아 해커조직 레빌에 대해서는 일정한 성과가 있다고...

- 유엔 GGE와 OEWG의 투 트랙 프레임이 출현
  - 유엔정부전문가그룹(GGE): 5차 보고서 채택 실패 이후 회의감
  - 2020년 총회 결의에 따라 5년(2021-25) 회기의 신규 OEWG 출범(2021.3.)

- 미국 등 서방 진영 vs. 중-러, 개도국 등 비서방 진영 대립
  - 기존 국제법 적용, 구속력 있는 규범 필요성, 정례 협의체 등 주요 쟁점별로 진영 간의 근본적 시각 차이가 노정

사이버 공간의 정보심리전

- 허위조작정보와 가짜 뉴스 등을 둘러싼 (국제)정치가 새로운 안보변수로 등장
  - 기존의 선전, 심리전 등에 비해서 사이버 공간의 네트워크(SNS)를 타고서 유통되는 특징
  - '루머 정치' or '괴담 정치'는 '안보화 정치'와 동전의 양면과도 같은 관계

- 러시아 변수: 2016 미 대선 개입설
  - 2016년 6월 민주당 전국위원회와 민주당 지도부, 힐러리 대선캠프 측 인사 100여명의 이메일 해킹
  - 민주당 지도부가 힐러리 측에 유리한 경선 구도를 만들기 위해 노력하였다는 점을 암시하는 이메일의 내용 공개

- 소셜 미디어와 하이브리드전, 내러티브 전쟁
  - 소셜 미디어의 전략적 효과를 노리고 언론매체에 빈번한 역정보/허위정보 유포 → 미래전에 주는 함의

- 현대 초연결 사회의 공개된 온라인 공론장은 이제 정보와 내러티브가 무기화되고
  - 정치적 우위를 점하려는 심리전 전술이 전방위적으로 전개될 수 있는 전장으로 전환; 전쟁 주체가 관객에 대한 전략적 커뮤니케이션을 어떻게 효과적으로 전개하여 이들의 마음과 생각을 획득하는 것이 중요

한수원 해킹 (2014)

- 한수원이 해킹을 당해 각종 기밀정보가 유출
  - 해커는 원자력발전소 가동을 중단하지 않을 경우 파괴하겠다고 협박

- 한수원 해킹 이슈
  - 2014년 12월 9일, HWP 파일 취약점을 이용한 악성코드가 퇴직자 명의 이메일을 통해 한수원 직원들에게 전파
  - 2014년 12월 10일, 악성코드를 통해 기밀정보 탈취 및 PC 파괴 명령 실행됨
  - 2014년 12월 15일 이후, 자칭 '원전반대그룹' 해커는 4차례 기밀 정보 유출
  - 2014년 12월 25일까지 원전 중단하지 않으면 파괴하겠다고 협박했으나 → 이상행위는 발생하지 않음

- 주된 변수로서 사이버 정보심리전의 양상

정보작전

- 정보전(Information Warfare)
  - 정보우위를 달성하기 위한 공격/방어, 또는 이를 위한 정보의 이용과 관리
  - 핵심은 정보의 유통과 연결성을 공격함으로써 결심 과정 자체에 영향

- 정보작전(Information Operations)
  - 적의 정보와 정보체계에 직간접적으로 영향을 주는 작전의 형태
  - 전통적인 정보작전은 상황 인식의 교란과 마비의 효과 추구

- 심리작전(Psychological Operations, PSYOP)
  - 적의 사기나 의지를 꺾고 아군의 사기와 의지를 강화
  - 보통 심리작전과 정보작전과 연계 → 정보심리전

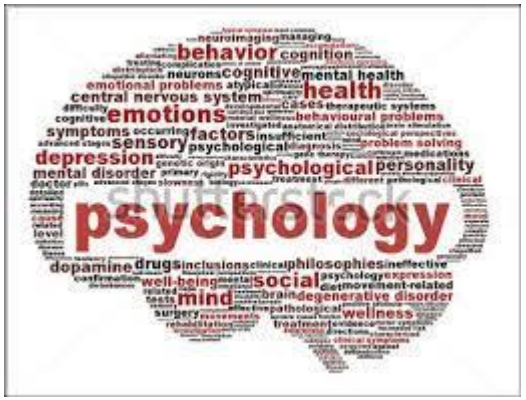
- 4차 산업혁명 시대의 정보전은 전통적인 '정보작전'의 개념을 넘어섬
  - 첨단 무기체계를 통제하는 기술과 전장환경을 관장하는 데이터 등과의 연계를 통해 상대의 인식 체계에 영향

정보심리전의 변환

- 전쟁 수행의 수단이라는 점에서
  - 주로 디지털 미디어를 통해서 자국에 유리한 정보를 유포하여
  - 국내외적으로 정치·외교·군사적 지지를 확보하려는 양상
  - 특히 SNS(Social Network Service) 활용

- 전쟁 수행의 주체라는 점에서
  - 국가 행위자뿐만 아니라 빅테크 기업, 초국적 해커, 일반 시민 등이 중요한 역할
  - '전쟁의 객체'였던 민간 행위자가 '전쟁의 주체'로 부상하는 현상 발생

- 전쟁 수행의 목표라는 점에서
  - 정보심리전 그 자체가 전쟁 수행의 목표
  - 설득력 있고 감동적인 내러티브를 전파하는 측은 '전쟁'에서는 져도 '역사'에서는 이긴다!



인지전(cognitive warfare)

- 개념의 확장과 심화
  - 정보작전 또는 심리작전의 개념을 넘어서
- 공간의 확장→'제6의 공간'으로서 인지공간
  - Cybersphere→Infosphere→Noosphere
- 발신자 모델에서 수신자 모델로
  - 정보의 생산-취합-전달에서 → 대상의 인지체계에 대한 교란과 조작
  - '메시지'가 아니라 '메신저'를 타격하라!
  - 상대방의 급소를 공략하라! 민주주의 or 권위주의 체제의 급소?
  - 인지전 대상의 다양화: 동료층, 지지층, 적대층 등
- 프레임 전쟁과 내러티브 전쟁의 강조
  - 선제공격과 각인효과의 중요성 증대
- 향후 과제
  - 이성(cognition)의 영역을 넘어서 마음(心)과 감성(情)의 영역을 포괄할 과제
  - 한반도 상황에서 인지전? 한국형 인지전 모델?

디지털 007?

- 정보혁명과 첩보
  - 기존의 비밀스런 정보처리작업을 넘어서 정보화시대 무수히 쏟아져 나오는 공개 자료에 대한 분석이 중시됨
  - 안보→산업→지식/사이버 스파이
- 첩보변환?
  - 냉전시대 정립된 조직, 행동양식에서 벗어난 탄력적 대응의 필요성
  - 고정적 조직에서 탄력적 조직으로
- 네트워크 첩보
  - 정보수집의 속도와 질에 있어서 민간 부문의 역량이 크게 증대
  - 다국적 기업의 정보망 vs. 국가정보기관의 정보망
- 소셜 네트워크와 디지털 첩보
  - 빅데이터의 활용
  - HUMINT에서 OSINT로!

우크라이나 전쟁의 사례

- 2022년 2월 24일 러시아의 우크라이나 침공
  - 탈근대 시대에 발생한 (전)근대적 전쟁?
  - 미래전의 사례? 전쟁 수행의 수단과 주체 및 목적의 변화

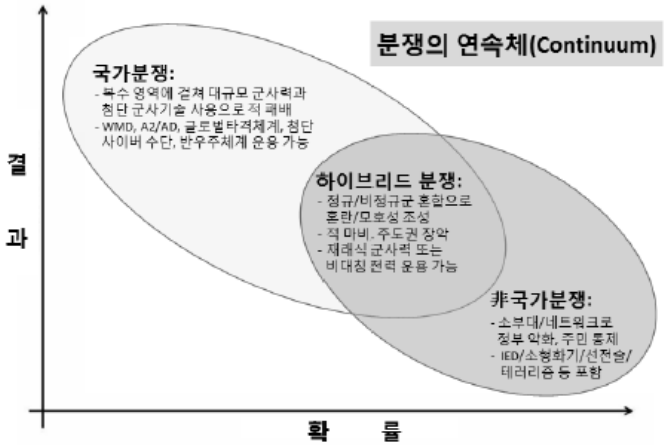
- 사이버전으로서 우크라이나 전쟁
  - 개전 직전의 디도스 공격→그러나 큰 피해를 야기하지는 않은 듯
  - 우크라이나의 사이버전 지원병 모집→ IT Army, 어나니머스의 참전→'사이버 세계대전'?
  - 민간 빅테크 기업들의 기여: 스페이스X, MS

- 정보전으로서 우크라이나 전쟁
  - 드론 공격의 활약: 터키제 '바이락타르', 러시아 드론 '란셋'
  - 우주자산의 활용: 특히 민간 위성사진
  - 오픈소스정보(OSINT)의 시대: 구글맵의 활약, SNS

- 심리전/인지전으로서 우크라이나 전쟁
  - 가짜뉴스, 허위조작정보→하이브리드전, 소셜 미디어 전쟁
  - 러시아발 공세 vs. 우크라이나의 선방: 젤렌스키 대통령
  - 러시아의 가짜뉴스를 차단하는 서방 플랫폼 기업들의 활약도

하이브리드전

- 하이브리드전(hybrid warfare)
  - 고도로 통합된 구상 속에서 노골적 및 은밀한 (overt and covert) 군사, 준군사 및 민간 수단들이 광범위하게 운용되는 전쟁의 양상 (NATO)
- 수단의 복합
  - 재래전, 핵전, 하이테크전, 사이버전의 복합
- 목적의 복합
  - 9.11 이후: 전쟁 목적의 비대칭성
  - 적대국으로부터 군사적 대응을 촉발하기 직전에 그 문턱(threshold)에는 미치지 않는 선에서 교묘하고 신중하게 활동 → 최근 하이브리드전의 양상
- 주체의 복합
  - 전투원과 민간인의 구분이 어려움
  - 인간과 로봇 행위자의 점차적인 복합



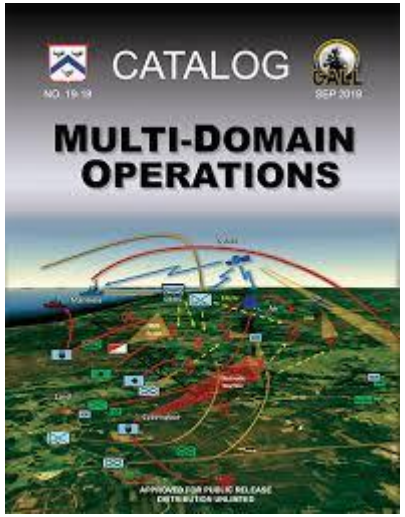
US DoD(2015), p.4; 송승종(2016), p.137에서 재인용

다영역작전(MDO), 전영역작전(ADO)

- 육지
- 바다
- 하늘
- 우주
- 사이버 공간

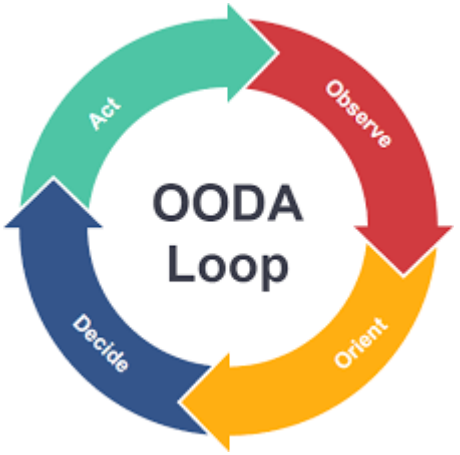
사이버전의 위상과 역할

- 독자적 cyber-warfare냐? Multi-Domain Operation이냐?
  - 육-해-공-우주 + 사이버전의 복합전쟁!
- 사이버전력은 모든 임무를 아울러서 널리 사용될 것으로 전망
  - 전술 임무수행: 무기체계 무력화 및 전투기능 마비
  - 작전 임무수행: 적의 군사 지휘체계 마비 및 군사능력 약화
  - 전략 임무수행: 적의 전쟁의지를 마비시키고 전쟁을 억지
- 미래전에서 사이버전의 효용과 가치는 갈수록 더욱 높아질 것
  - 군과 민간의 주요 전략적 표적들이 디지털화, 네트워크화, 스마트화되면서 사이버무기의 전략적 무기로서의 가능성과 효과도 더욱 커지고 있는 상황
- 미래전에서 사이버 공간을 장악하는 전력의 의미
  - 육·해·공·우주공간의 지배를 보장하고 전쟁의 승패를 좌우할 수 있는 핵심 전력
  - 미래전 환경에서 일국의 국방 전력 수준을 보여주는 핵심 지표



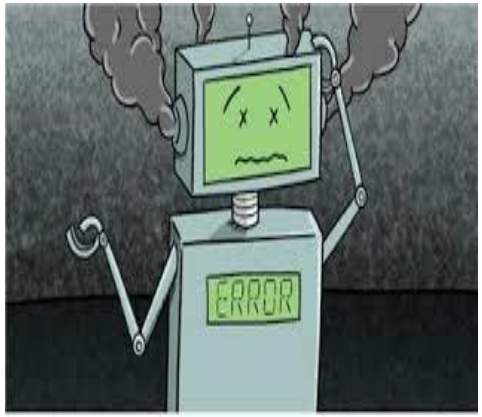
AI기반 미래전 vs. 사이버전

- AI기반 자율무기체계가 사이버 공격을 받는다면?
  - 미래전 무기체계 논의의 핵심은 인공지능(AI) 기반 자율무기체계의 부상
- 자율무기체계와 같은 최첨단 미래전 무기체계가
  - 자신이 가진 취약점으로 인해 적국의 사이버 공격으로 무력화된다면?
  - 그래서 무기의 오작동으로 인해 아군을 공격한다면?
- 인간-기계 통합체계로서의 자율무기체계에 대한 교란과 방해, 침투의 문제
- 특히 OODA 루프에 대한 사이버 공격
  - 탐색(Observation)–발견(Orientation)–교전결심(Decision)–교전(Action)



자율무기체계의 취약점

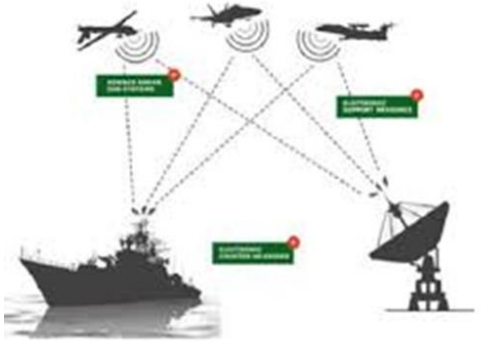
- 기계적 취약점
  - 자율무기체계 자체가 내재한 다양한 버그와 소프트웨어 취약점이 존재
  - 기하급수적으로 증가하고 있는 무기체계 소스코드의 규모와 기술 복잡도 증대 → 정상사고 발생 가능성
  - 의도적 사이버 공격에 의해 무력화되거나 오작동할 가능성(악성코드, USB 등 사용)



- 인간-기계 인터페이스 취약점
  - 인간의 인지적 취약점을 이용하여 경험과 인식을 통제
  - 스크린 이미지 조작, 인공지능 딥페이크 등

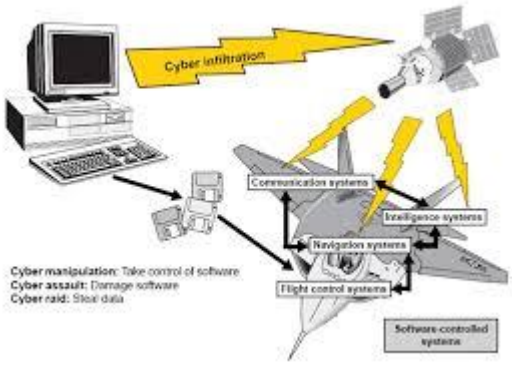
- 인간 자체의 취약점
  - 행동에 이르는 인지 과정에 개입 → 인지적 취약점을 이용하는 방식으로 공격
  - 가짜정보 제공함으로써 원하는 결정을 하도록 만들거나 사기를 떨어뜨리는 사이버 심리전을 통한 공격
  - 미래에는 뇌-컴퓨터간 직접 인터페이스를 통해 인간의 뇌 자체를 직접 조작할 가능성도 거론
  - 인간 병력의 신체 이식물(Body Implants), 예를 들어 심장박동기나 의료장비에 대한 사이버 공격 등의 우려

사이버-전자전



- 미래전은 강대국의 교리가 상정했던 순정 상태의 사이버 공간 또는 '자유로운' 전자파 환경에서 벌어지는 것이 아님
  - 통신망 교란과 무기체계 무력화 및 통통제를 위한 악성코드와 가짜 신호로 넘쳐나는 전장이 미래전의 기본 환경임을 직시해야

- 전자전(Electronic Warfare)=전자기파 공격과 지향성 에너지 무기를 사용한 Warfare의 출현
  - EMP(Electromagnetic Pulse)나 HPM(High Power Microwave) 등과 같은 전자공격용 무기들이 속속 개발
  - EMP탄: 폭발 시 발생하는 엄청난 위력의 전자기파 → 지상의 통신망이나 전자기기장비, 컴퓨터 네트워크 등의 기능을 일시에 마비 → 각종 데이터 및 정보가 일순간 초토화



- 사이버-전자전(CEW: Cyber-Electronic Warfare)
  - 인터넷과 연결된 유무선 네트워크의 침투와 교란을 담당하는 사이버전과 독립망이나 폐쇄망을 방해하고 교란하는 전자전을 결합

'발사의 왼편'

- 발사의 왼편(Left of Launch) = 발사교란작전
  - 오바마 행정부가 2013년 2월 북한의 3차 핵실험 후, 북한의 미사일 발사를 무력화시키는 목적으로 수립한 사이버-전자전 작전
  - 미사일이 발사대에 올려지거나 막 발사됐을 때 사이버 공격이나 전자파 공격을 통해 교란하는 프로그램을 활용

- 북한이 미사일 발사 장소를 계속 옮겨가면서 발사한 것은 이러한 미국의 공격과 무관하지 않다는 분석
  - 실제로 '발사의 왼편' 도입 이후 북한 미사일이 발사 직후 폭발하거나, 궤도를 이탈하는 등의 실패 확률이 이례적으로 높아졌음

- 영국의 일간지 더타임스(The Times)
  - "실패한 북한의 미사일 발사 가운데 일부는 성능 결함 때문이지만 다른 일부는 미 국방부가 첨단 컴퓨터 바이러스를 이용해 발사를 교란시킨 탓으로 보인다"고 보도

우주전과 결합

- 우주공간=4차 산업혁명 시대의 복합공간
  - 냉전 시대의 발상을 넘어서

- 우주분야의 주요국 간 전략경쟁 가속화
  - 기술경쟁, 표준경쟁, 매력경쟁
  - 우주의 군사화와 무기화도 진행 중
- 사이버전과 우주전의 결합
  - 강대국들 간의 최첨단 우주무기체계와 위성체계를 대상으로 한 사이버 공격 증가 가능성
- 인공위성 시스템 해킹, GPS 교란 등
  - 인공위성 궤도를 수정해 의도적으로 서로 충돌하게 하거나 우주 파편과 부딪히게 함으로써 위성체계를 파괴하거나 위성의 작동 자체를 무력화하고 방해하는 방법들이 보고되고 있음
  - GPS 신호나 위성통신대역을 교란 또는 방해하는 전자전 수단인 GPS 재밍(Jamming)

사이버-핵 넥서스

- 사이버 안보와 핵무기의 연계성(Nexus)
  - 핵시설이나 원전에 대한 사이버 공격: 미국/이스라엘 vs. 이란 갈등
- 한반도의 맥락에서 보면, 사이버-핵 넥서스의 의미는?
  - 북한발 사이버 공격과 북핵 시도의 연계성
  - ICBM을 해킹할 수 없을까?
- 국제질서 변화 전반에 미치는 영향?
  - 핵 기반의 기존 강대국 질서의 변화 가능성
  - 사이버 안보 분야의 비국가 행위자들의 도전과 근대국가 중심 질서의 변환
  - 사이버 안보 분야의 국제규범/윤리의 모색: 기존 핵 규범/윤리가 주는 의미
- 사이버-핵 넥서스에 대비하는 국내 법제도와 추진체계의 정비 문제

사이버 안보 복합 넥서스


사이버-키네틱 넥서스 (Cyber-Kinetic Nexus)
사이버-정보전 넥서스 (Cyber-Info Nexus)
사이버-AI무기 넥서스 (Cyber-AI Nexus)
사이버-전자전 넥서스 (Cyber-Electro Nexus)
사이버-핵 넥서스 (Cyber-Nuclear Nexus)
사이버 안보 복합 넥서스

감사합니다

sangkim@snu.ac.kr