사이버전에서의 무기체계에 대한 위협

국방기술품질원 기술기획본부 기술정보센터
책임기술원/공학박사 김 정 국 · 위촉연구원 김 세 영

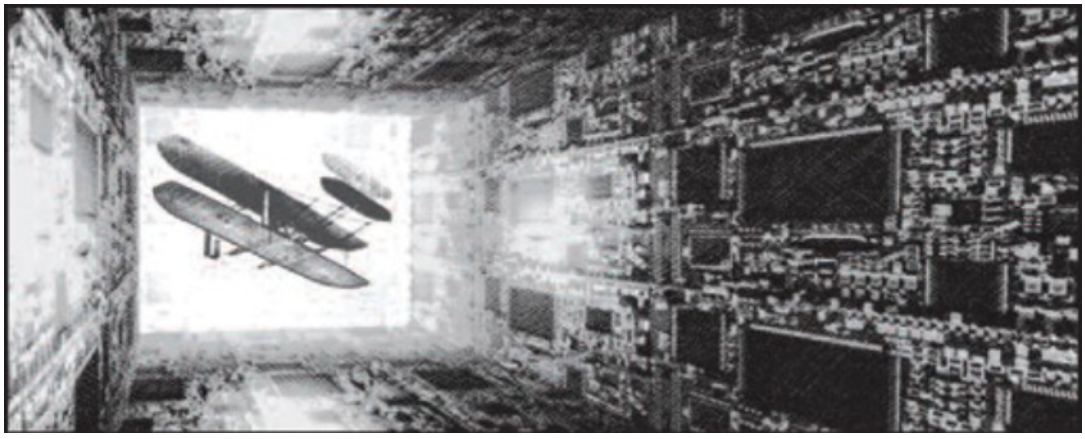

그림 1. 사이버전 이미지

Carl von Clausewitz(프로이센 군인 겸 독일 군사 전문가, 1780~1831)는 전쟁을 "우리의 목표를 달성하기 위해 적에 대응하는 폭력 수단으로서 이를 위해 적은 무장 해제되어야 하고 이것이 바로 전쟁행위의 목적인 것이다."라고 정의했다. 이 정의는 더 이상 현대식 전쟁을 완전하게 정의하지 못한다. 오늘날에는 소프트웨어 중심 체계의 양상에 따라 Carl von Clausewitz의 '적군 무장 해제'를 위한 전쟁 개념처럼 폭력을 쓰지 않고 한 국가를 공격하는 것이 가능해졌다. 사이버전의 개념과 사용은 최근 몇 년간 급격하게 성장했다. 사이버전이 주로 정보체계와 관련 있긴 하지만 여기서는 사이버전의 무기체계에 대한 잠재 영향에 대해 기술하고자 한다.

폭력 없는 전쟁

사이버라는 용어는 인간을 대신해 통제하는 기계 또는 전자체계를 채택하는 체계를 설명하는 데 사용될 수 있다. 여기서는 이 용어에 통제 컴포넌트로 소프트웨어를 통합하는 체계들을 포함했다. 사이버전은 물리적 공격 없이 벌어질 수 있고, 따라서 소프트웨어 중심 체계(사이버 체계) 의존도에 따라 비폭력전에 대한 각 국가의 취약성이 결정될 수 있다. 전통적으로 전쟁에서

진행된 공격은 체계의 물리적 컴포넌트(군인, 무기, 시설, 차량 등)에 집중되어 있었다. 전쟁의 목적은 일반적으로 이런 대상들을 무력화하고 파괴하는 데 있었다. 이런 대상들을 공격하는 것이 '적군 무장 해제'의 주요 수단으로 여겨졌다. 전략적 차원에서 보면 이런 대상들은 아래와 같이 대형 체계의 일환이라는 이유로 표적이 된다.

- 생산 체계(전략적 폭격으로 공격받는)
- 보급 체계(저지 폭격으로 공격받는)
- 지휘통제 체계(전격 전술로 공격받는)

컴포넌트 파괴는 전체에 영향을 주기 위한 것이며, 공격이 프로세스를 붕괴시키지 않더라도 체계 내 전투원의 수를 줄일 수는 있다. 공격은 프로세스 내 부대들에 직접적인 타격을 주지만, 궁극적인 목표는 프로세스 자체를 공격하는 것이다. 이런 프로세스들은 적국이나 군의 잠재적인 '핵심부'이다. 핵심부를 공격해 적의 전쟁 수행능력을 빼앗을 수 있다. 무력을 사용하지 않고 핵심부를 공격할 수 있다면, 한 국가를 폭력 없이 꺾을 수 있고 그 능력은 전쟁에 대변혁을 일으킬 것이다. 예컨대, 기계나 사람에게 해를 끼치지 않고 프로세스를 붕괴시킨다면 모든 컴포넌트를 파괴하는 것과 같은 효과를 볼 것이다. 컴포넌트와 인력은 대체할 수 있기 때문에 체계 자체를 붕괴시키는 것은 더욱 장기간 동안 피해를 입힘으로써 그 효과가 더 클 수 있다. 군 체계를 무력화시킨 공격에 국가가 탐지 및 적합한 위협 대응을 못한다면 국방 임무를 수행하지 못하게 될 것이다. 컴포넌트가 아닌 체계 및 프로세스에 대한 공격이 성공한다면 한 국가는 무력이나 전쟁 선포도 없이 굴복하게 될 것이다.

초기 World Wide Web 사이버전 기간 동안의 정보 및 네트워크 체계 발전은 관련 정보 원칙에 따른 군의 작전 수행으로 정의됐었다. 다시 말해, 이 용어는 군 통신 및 합동 능력, 또는 반대로 정보 및 통신 체계의 효과적인 사용이 방해받는 것을 설명하기 위해 사용되었다. 하지만 이런 설명은 더 이상 사이버전에서 가능한 것들을 모두 규명하지 못한다. 비용효율적인 컴퓨터 프로세서, 메모리, 기타 컴퓨터 하드웨어 기능이 계속 발전함에 따라 소프트웨어는 모든 종류, 목적, 크기의 체계를 통제하는 데 사용되고 있다. 게다가, 컴퓨터 네트워크가 계속해서 전 세계로 퍼져나가면서 문명을 지원하는 기반시설(전자, 석유, 가스, 운송, 수질관리 체계) 등 모든 종류의 체계 들은 글로벌 네트워크를 통해 통합 또는 접속이 가능하다.

사이버전에 대한 무기 플랫폼의 취약성

무기체계들은 소프트웨어, 컴퓨터 하드웨어, 전장 네트워킹에 대한 의존도도 매우 높아져서, 사이버체계를 통해 표적이 될 수 있다. 이들 무기체계에 대한 보안은 사이버 기술의 개발과 실행에 따라 발전하고 있지만 사이버 공격의 영향을 점점 많이 받을 수도 있다. 항공기는 무기체계에 대한 사이버전 변천의 좋은 예다.

과거에 항공기 성능과 기능은 100% 하드웨어(항공기의 물리적 구성 등)로 결정됐었다. 최근 첨단 항공기의 성능과 기능은 80%가 소프트웨어에 의존하고 있다(그림 1 참조).

소프트웨어 없는 항공기는 통제가 불가능하고

Aircraft	Year	Software Percentage of Functions
F-4	1960	8
A-7	1964	10
F-111	1970	20
F-15	1975	35
F-16	1982	45
B-2	1990	65
F-22	2000	80

그림 1. 무기체계의 소프트웨어 의존도

필요한 기능을 발휘하지 못할 것이다. 예컨대, F-16은 Mach 1 미만에서는 불안정하고, 자체 소프트웨어 기반 비행통제체계 없이는 통제 불가능하다. 보잉 777과 에어버스 330은 수동식 백업이 없는 소프트웨어 비행통제체계를 구비하고 있으며, 디지털 비행통제체계에 따라 항공기 성능이 달라진다.

일부의 경우, 항공기 성능은 소프트웨어를 통해 물리적 구성에 대한 의존도를 줄이고 있어서, 소프트웨어 의존도는 높아지고 하드웨어 의존도는 낮아지고 있다.

예를 들어, 고각 공격 비행에서 F-22는 소프트웨어 통제식 진로 추력과 비행 통제로 항공기를 조종한다. 게다가, 현대식 항공기는 전자장치로 조종하고 엔진은 전자장치로 통제되며, 무기는 전자장치로 발사 및 투하된다. 전적으로 하드웨어의 기계적 통제를 받던 과거 체계들은 소프트웨어 통제식 소프트웨어로 대체되고 있다.

소프트웨어는 현대식 무기체계의 내구도와 효용성도 결정할 수 있고, 많은 별개 품목을 네트워킹으로 통합하는 기반을 제공한다. 하지만, 네트워크 소프트웨어 체계들은 사이버 공격에 취약하고, 공격 강도와 취약성이 점점 커지고 있다(그림 2 참조).

아직까지 소프트웨어를 군 전투체계의 주요 컴포넌트로 규정하진 않지만, 위에서 언급된 바와 같이 많은 소프트웨어와 소프트웨어 통제식 체계들이 체계 개발에 활용된다. F-22 무기체계는 소프트웨어 통제식 항공체계의 한 예로서 통합정보체계와 통신기능을 보유하고 있다.

F-22는 폐쇄형이 아니며, 외부정보체계가 비행 중 F-22 전투작전을 갱신하고 통합한다. 외부 연결을 통해, F-22의 정보체계뿐 아니라 기본 소프트웨어와 하드웨어체계도 공격받을 수 있다. 최근 미 합참의장이 공표한 정보전 정책은 주로 F-22 통합용 외부 C4I 체계의 보안을 염두에 두고 있지만, 소프트웨어 중심체계는 F-22 내부체계를 사이버 공격에 취약하게 만든다. 이런 취약성을 고려한 공격 및 방어 수단을 마련해야 한다. 미 국방부 공개 문서와 규정에는 적절한 사이버전 정의가 없지만 희망은 있다. 사이버공간 작전을 위한 2006 국가 군사

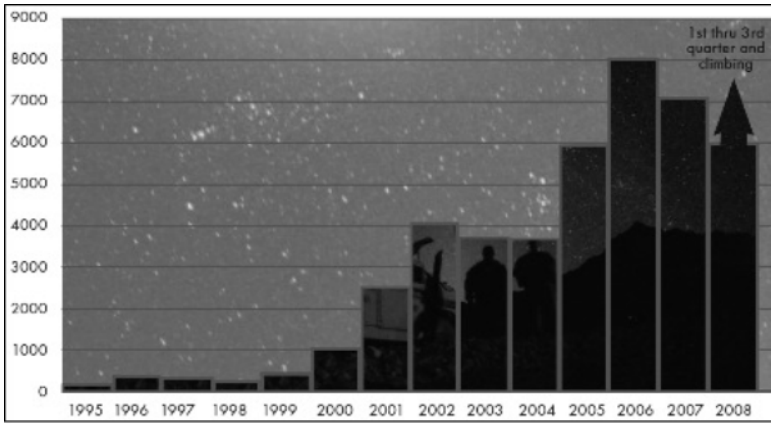

그림 2. 카네기멜론 소프트웨어 체계공학연구소의 취약성 발생 목록

전략(NMS)은 사이버전을 정확하게 정의하고 관련 정책을 명시했다. 불행히도, 이 정책은 미 국방부 정책에 포함되지 못했다.

사이버전 표적

일반적으로 사이버전 표적에는 네트워크, 디지털체계, 기반시설, 그리고 정보·통신·통제체계 기능을 하는 컴포넌트 모두가 포함된다. 따라서 미 국방부의 소프트웨어 통제식 군 체계는 특히 사이버 공격에 취약하다. 모든 공격의 첫 단계는 사이버 침투(CyI)다. 소프트웨어를 통합하고 있는 체계는 모두 사이버 침투에 취약하다. 사이버 침투 후 활동은 전송, 파괴, 기록 조작(사이버 급습(CyR))을 통해 기관에 영향을 줄 수 있다. 체계 내 소프트웨어는 조작될 수 있고 소프트웨어의 통제를 받는 체계는 오작동되거나 통제(사이버 조작(CyM))받을 수 있다. 소프트웨어 자체는 복사, 오작동, 재구성(사이버 공격(CyA))될 수도 있다.

데이터베이스 등의 군 체계는 계속해서 사이버전의 표적이 될 것이다. 무기체계에 대한 사이버 공격의 가능성은 평시보다는 전시에 높다.

군 표적(군 C4I)

현대식 군 체계는 C4I에 의존하고 있다. 군부대는 이 체계들을 통해 제공되는 합동 및 통신 기능이 없으면 전투할 수 없다. 군 C4I 체계는 특히 취약하며, 미 국방부 사이버 관련 정책의 주요 과제다. JP 3-13과 JP 3-13.1은 정보전에 정책을 제공한다. C4I 체계는 무선통신기부터 레이더, 대형 컴퓨터부터 개인 컴퓨터까지 매우 복잡하게 구성되어 있다. 군 C4I는 다양한 주파수 범위의 인터넷, 기지 및 기관 LAN, 민군 통신체계, 항법체계, 무선통신기를 통해 인터페이스한다. 군 C4I 체계는 상호연결성 때문에 특히 취약하다. 사이버 침투는 많은 지점에서 발생할 수 있으며 무수한 체계에 영향을 줄 수 있다. 한 예로, 사이버전은 레이더, 미사일, 통신 통제에 영향을 줄 수 있다. 미사일을 불능화하거나 발사지점으로 다시 방향을 바꿀 수도 있다. 지휘통제 네트워크, GPS, 이동통신체계를 중단 및 붕괴시킬 수도 있다.

이 체계들과 그 상호작용은 너무 복잡해서 아무리 현대화된 군 기관이라도 사이버 침투의 근원을 추적하기는 어려울 것이다. 모든 종류의 사이버 공격이 가능하며 그 결과는 참담할 것이다. 예를 들어, 핵무기 통제체계가 군 C4I에 통합되는 것이다. 국방부 네트워크, 데이터 베이스, 웹사이트 침입 사례에서 보았듯이 거의 모든 적이 마음만 먹으면 군 컴퓨터체계에 사이버 공격을 가할 수 있다. 군 컴퓨터는 국가 C4I의 핵심이기 때문에 이를 표적으로 삼는 IA(의도적 사이버전 공격) 및 UA(비의도적 사이버전 공격)가 성공하면 국가 보안을 위험에 빠트릴 것이다.

미국이 현재 연합군과 진행하고 있는 프로그램들은 첨단 기술이나 최신 보안 표준을 적용하지 않는 장비 및 체계를 일부 사용하는 것으로 보인다. 부대 간 통합이나 통신 모두 또 다른 보안 취약성을 야기할 수 있다.

무기체계

미 국방부의 현 정책은 운용 시 소프트웨어가

필요한 항공기 및 차량 등의 군 하드웨어체계에 대한 사이버 공격을 제대로 다루지 못하고 있다. 위에서 언급한 바와 같이 F-22는 사이버통제식 항공기다(그림 3 참조).

그림 3. 항공기 내장 소프트웨어

항공기체계를 직접 또는 C4I 연결을 통해 침투 및 방해하면 공중에서 항공기를 격추하는 것처럼 타격을 줄 수 있다. 현대식 항공기에 데이터를 제공하는 C4I 체계에 대한 사이버 침투는 사이버 급습, 조작, 공격의 단초가 된다. 민간 글로벌 항공 교통 관리(GATM)와 군의 전술 타깃팅 네트워킹 기술(TTNT) 및 F-22 내부 비행 데이터 링크(IFDL) 등 많은 체계가 자동으로 항공기 정보를 갱신하며, 이로 인해 항공기 침투를 탐지하지 못할 수도 있다. 정보, 항법, 통신체계는 서로 통합되어 있으며 자동조종장치를 통한 비행통제체계, 자동스로틀을 통한 추진체계, 레이더체계, 마스터경고체계, 환경통제체계 등 수많은 항공기체계에 입출력된다. 정확한 통제 순서, 입력 또는 재프로그래밍으로 침투자는 항공기 경로이탈 유도부터 비행 통제 소프트웨어 조작까지 다양한 체계 붕괴를 야기할 수 있다. UAV는 수천마일 거리에서 통제되기 때문에 제어기능을 빼앗길 수 있다. 다른 많은 무기체계도 유사한 장비와 조종장치를 이용하기 때문에 취약하다고 볼 수 있다.

새로운 정책

종합해 보면, 국방부와 정부는 무기체계에 대한 공격을 포함해 가능한 모든 형태의 사이버전을 다룰 강력한 정책이 필요하다. 보안 위협 분류는 이 정책을 수립하는 데 유용하다. 이는 현재와 미래의 모든 사이버전 위협을 포함하는 정책 개발에 우선한다. 관건은 모든 소프트웨어 통제식 체계의 보안 수준을 강화하기 위해 필요한 노력과 자금을 대는 것이다.

참고자료
The WSTIAC 분기간행물(2010.4.28)

※ 사이버 관련 용어

사이버공간

정보환경 내 글로벌 영역으로 인터넷, 원격 통신 네트워크, 컴퓨터체계, 내장 프로세서 및 제어기 등 정보기술 기반시설의 상호의존 네트워크로 구성.

사이버공간 작전

사이버공간에서 목표 달성을 위해 사이버기능을 활용. 이 작전은 글로벌 정보망 운영 및 방어를 위해 컴퓨터 네트워크와 그 활동을 포함.

사이버전(CyW: Cyber warfare)

적이 자국 의도에 따라 적의 체계 내 소프트웨어 통제

프로세스를 공격하도록 하는 행동. CyW는 사이버 침투, 사이버 조작, 사이버 공격, 사이버 급습방식을 포함한다.

사이버 침투(CyI: Cyber infiltration)

소프트웨어 통제식 국방체계에 침투해 체계를 조작, 공격, 급습.

사이버 조작(CyM: Cyber manipulation)

침투에 이어 소프트웨어로 체계를 통제해 체계의 작동을 마비시키고, 피해를 주기 위해 체계기능을 사용. 체계 소프트웨어를 사용해 전원 끄기 등.

사이버 공격(CyA: Cyber assault)

침투에 이어 체계 소프트웨어 및 데이터를 파괴하거나 체계를 공격해 기능을 손상. 바이러스 및 과도한 데이터 전송으로 체계 과부하 유도.

사이버 급습(CyR: Cyber raid)

침투에 이어 체계 내 데이터를 조작 또는 습득해서 체계의 작동을 마비시키고 데이터를 전송, 파괴, 조작.

사이버 범죄(CyC: Cyber crime)

국가 보안에 영향을 주거나 국가 보안에 반하는 작전 진행 의도 없이 하는 사이버 공격. 사이버전 개념도 사이버 범죄에 적용됨. 사이버 범죄는 비판적 시각을 반영한 용어. 국가 간 재앙을 막기 위해 국가는 사이버 범죄와 사이버전을 구분해야 함. 사이버 범죄에 대한 정의는 사이버전과 비슷하지만 두가지 다른 점이 있음. 첫째, 사이버 범죄는 공식적으로 알려진 정치 인물 간에 벌어지는 게 아니지만, 사이버전은 전쟁 법규를 따르는 독립체 간에 벌어짐. 둘째, 사이버 범죄 목적은 사이버전처럼 적을 국가 의도대로 조종하는 것이 아님. 사이버 범죄는 사이버전처럼 엄청난 파급효과를 낼 수 있음. 하지만, 국가 정책의 주요 임무는 범죄자의 행동으로 인한 국가 간 보복을 막기 위해 두 가지를 구분하는 것임. 사이버 작전에서 중요한 것은 사이버전과 범죄를 구별하는 것과 병사들이 투입된 총격전이 아니라는 것임. 국가는 정치적인 실수를 범하지 않도록 주의해야 함.

의도적인 사이버전 공격
(IA: Intentional cyber warfare attack)

의도적으로 국가 보안에 영향(사이버전)을 미치거나 국가 보안에 반하는 작전을 수행하기 위해 사이버 수단으로 하는 모든 공격. 의도를 갖고 있는 행위자의 설득으로 우연히 저지르는 사이버 공격 포함.

비의도적 사이버전 공격
(UA: Unintentional cyber warfare attack)

국가 보안에 영향(사이버 범죄)을 줄 의도 없이 사이버 수단을 통해 저지르는 모든 공격. IA는 전쟁과 거의 동급으로 전쟁 등급 분류 시 국가 정책에 해당. UA는 범죄로 볼 수 있음. UA는 빌딩 해커나 전문 사이버 범죄자가 저지를 수 있지만, 그 의도는 개인적 이고 특별한 국가 위협 목표가 없음. 하지만 비의도적 공격도 정책에 영향을 줄 수 있고 의도적 공격만큼 파괴 효과도 가질 수 있음.

의도적 사이버 행위자
(I-actors: Intentional cyber actors)

의도적으로 사이버전을 수행하는 개인(사이버 운영자, 사이버 병력, 사이버 병사, 사이버군).

비의도적 사이버 행위자
(U-actors: Unintentional cyber actors)

국가 보안에 영향을 줄 수 있는 사이버 공격을 행하는 개인으로 주로 자신의 행위로 인한 세계적인 파급효과를 인식하지 못함. 비의도적 행위자는 의도적 행위자의 영향을 받을 수 있는데, 자신이 속아서 사이버 작전에 관여된다는 것을 인식하지 못함. 비의도적 행위자는 국가 보안에 영향을 주거나 국가 보안에 반하는 작전을 수행할 의도 없이 CyI, CyM, CyA, CyR를 저지르는 모든 사람. CyC에 관련된 개인, 언론인, 산업 스파이도 포함. 언론인과 산업 스파이, 그리고 이들 CyI 노력의 영향을 받는 UA의 체계에 대한 위협은 매우 크다고 볼 수 있음.