사이버전(Cyber Warfare)의 형태와 정보보호 기술
Types and Information Security Technology on Cyber Warfare

박호균(신흥대학교)

차 례

1. 서론

국가 기간산업과 국방 및 안보관련 시스템들이 인터넷과 정보기술에 크게 의존하는 상황에서 사이버공격 또는 사이버테러의 빈도와 피해 규모는 점차 커지고 있다. 다양화·지능화되고 있는 사이버 공격이나 보안 침해사고는 네트워크로 연동된 전체 시스템으로 확산되어 국가 기간망을 위협할 수 있다. 특히, 사이버공격은 군사지휘체계는 물론 국가기밀 정보의 유출 및 위변조, 금융, 통신, 교통시스템 등 국가 기간 시스템을 교란하거나 무력화시킴에 따라 이를 사이버전(Cyber Warfare)의 개념으로 분류하고 있다[5].

사이버전은 적군과 아군의 구분이 모호하고, 국가 간 경계가 없으며, 공격을 위한 전력구축과 유지비용이 저렴할 뿐 아니라 최소인원으로 엄청난 사회적 파장과 경제적 피해를 주는 비대칭·비정형의 군사적 수단으로 운용되어 국가 안보에 심각하게 위협하는 단계에 이르렀다. 사이버전은 모든 전력 요소들이 유기적인 연결을 통하여 통합 작전체계를 구성하는 네트워크 중심전(NCW, Network Centric Warfare)으로 작전 수행이 변화함에 따라 국방 분야에 그 영향력이 더욱 커지고 있다[1][4].

본 고에서는 이러한 사이버전의 정의와 특징을 살펴보고 사이버전의 최근 형태와 사이버전의 대응실태를 알아보고 사이버 침해 및 위협에 따른 보안기술에 대하여 고찰하고자 한다.

2. 사이버전의 개념과 특징

2.1 사이버전의 정의

사이버전은 1990년대 초 미해군 대학원 교수 존 아킬라(John Arquilla)가 처음 제안한 것으로 용어는 명확하게 정의되어 있지 않고 관점에 따라 다양하게 정의되고 있다. 군사용어 사전에서는 “컴퓨터가 합성한 가상현실의 세계와 가상인간의 영역과 같이 인공지능 체계가 운용되는 공간에서의 전쟁으로서, 정보화 사회의 과학기술을 이용하여 취약점을 공격함으로써 물리적 파괴보다 훨씬 경제적 손실을 강요할 수 있는 총체적 가상공간에서의 정보 마비전을 추구하는 전쟁수행 방식”으로 정의되어 있다. 또한, 사이버전의 또 다른 정의로서 “사이버 공간에서 일어나는 새로운 형태의 전쟁으로서 컴퓨터 시스템 및 네트워크, 통신망 등을 교란 및 마비, 무력화함으로써 적의 사이버 체계를 파괴하고, 아군의 사이버 체계를 방호하는 것”이라고 정의하고 있다. 합동참모부 교범인 ‘합동 및 연합작전 군사 용어사전’에서도 “컴퓨터 네트워크를 통해 디지털화된 정보가 유통되는 가상적인 공간에서 다양한 사이버 공격수단을 사용해 적의 정보체계를 교란, 거부, 통제, 파괴하는 등의 공격과 이를 방어하는 활동”으로 규정하고 있다.

미국의 RAND연구소는 “정보의 우선순위에 따른 군사작전으로 상대국의 정보 및 통신 시스템을 파괴 또는 무력화하는 행위”로 규정하고 있으며, 단순히 컴퓨터 시스템을 파괴하는 것뿐만 아니라 이에 의존하는 물리적 체계 및 기반시설까지 영향을 주는 것이라고 정의하고

있다[3].

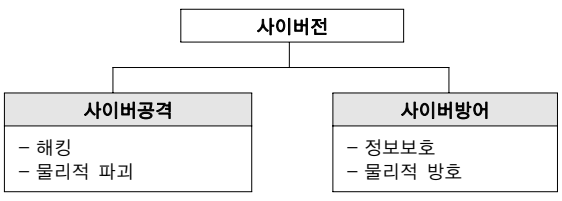
2.2 사이버전의 특징

국가의 정보 기반구조가 잘 갖추어져 있고, 정보기반 처리체계와 사회의 주요 시스템이 컴퓨터에 의존하는 정도가 높은 나라일수록 사이버 공격의 가능성과 피해 정도도 높을 수밖에 없다. 과거의 전쟁형태와 비교할 때 사이버 전쟁은 상대방의 신념과 지식 체계를 공격하기 때문에 전투의 전개 과정을 단계적으로 상상하거나 그 결과를 정확하게 예측하기가 어렵다. 사이버전의 특징을 정리하면 다음과 같다.

- 사이버 전쟁을 준비하고 수행하는데 드는 비용이 저렴하며 높은 파급효과를 얻을 수 있다. 효율적인 전쟁능력을 비교적 낮은 비용으로 구입, 개발하고 널리 쉽게 보급할 수 있기 때문이다.
- 공격대상에 접근할 필요 없이 통신망이 연결된 곳이라면 어디서나 공격이 가능하고 증거를 남기지 않아 공격자와 공격 장소의 추적이 어렵다.
- 국가나 기업의 정보체계가 공격당하고 있을 때 그것이 단순한 범죄행위에 의한 것인지, 전쟁행위로 행해지고 있는 것인지의 경계가 불분명하다.
- 사이버 전쟁을 수행하기 위하여 전통적인 방식을 넘어서는 완전히 새로운 차원의 관심과 정보수집 및 분석 시스템이 요구된다.
- 첩보활동이나 사고 등을 사이버 전쟁과 구분할 수 있는 적절한 조기 경고시스템과 공격감지체계 및 평가방법이 없다.
- 기존 전쟁과는 달리 전선의 구분이 없고 전후방 구분 없이 동일한 공격대상이 된다.

3. 사이버전의 형태

사이버전의 형태에는 사이버 공격과 사이버 방어가 있으며, 유형별 세부 형태는 다음 그림과 같다.



▶▶ 그림 1. 사이버전 세부형태

사이버전의 형태는 행위의 주도권이 어느 편에 있는가에 따라 사이버 공격과 방어로 구분되며, 사이버 공격은 다시 해킹과 물리적 파괴로 나뉜다.

3.1 사이버전의 방어 기술

사이버 방어는 정보보호와 물리적 방호로 세분화 된다.

첫째, 해킹은 컴퓨터 및 프로그램과 데이터를 표적으로 수행된다. 해킹은 특정 시스템의 보안 구조상의 취약점을 통해 침투하여 시스템의 작동을 정지시키나 자료의 파괴 및 도용, 서비스 도용, 악의적인 모니터링, 허위정보 추가행위 등을 함으로써 적의 정보체계를 혼란 및 마비시킬 목적으로 수행된다.

둘째, 정보보호는 정보의 수집, 가공, 저장, 검색, 송신, 수신 과정에서 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적, 기술적 수단 또는 그러한 수단으로 이루어지는 행위를 말한다.

셋째, 물리적 파괴는 사이버 공간을 지배하기 위하여 전자기 펄스 탄, 전자파 공격, 나노머신 및 고출력 전자총 등 물리적 수단을 이용하여 적의 정보체계상의 하드웨어를 파괴 및 마비시키는 행위이다. 사이버전의 물리적 파괴 수단은 재래식 무기를 배제하고 전자적 파괴력을 가진 수단에 한정한다.

넷째, 물리적 방호는 적의 물리적 파괴행위로부터 아군의 정보체계를 방어하는 행위이다. 사이버전은 각종 분쟁, 정규전 및 비정규전, 공격 및 방어 구분 없이 평시부터 은밀하게 진행 할 수 있는 가장 큰 특징을 갖고 있다. 사이버전의 대상도 단순하게 군사작전이나 무기체계, 군사정보통신망, 전장감시체계 등과 같은 군사 분야에만 한정하는 것이 아니라 민간정보체계, 금융체계, 통신체계와 같은 정보인프라 및 철도, 의료, 운송, 산업시설, 항공 등의 국가 인프라를 망라하는 민간분야까지 그 대상에 제한이 없다.

3.2 사이버전의 공격 기술

사이버전의 형태와 관련하여 서이버전의 공격수단도 다양하게 존재하며 계속하여 새로운 기법들이 발전되고 있다. 그 중에서도 최근 개발되고 있거나 치명성 측면에서 대표적이라고 판단되는 몇 가지 사이버전 공격 수단을 예를 들면 다음의 표와 같다.

다음 표에서 제시된 사이버전 공격수단들은 사이버전 전략에 따라 적절하게 사용된다. 일부군사 전략가들은

사이버전 전략을 크게 세 단계로 구분하고 있다. 초기에는 해커 전쟁으로 시작하여 사이버 전쟁, 마지막으로 전면적인 네트워크 전쟁으로 발전된다는 것이다.

표 1. 주요 사이버전 공격 수단

구분	주요내용
코만도 솔로 (Commando solo)	미 공군의 1급 비밀의 전자기기가 장착된 제트기로서 일명 '펠리컨'이라 하며 하늘을 나는 방송국으로 적국 상공에서 허위정보를 유포하여 상대 국민들에게 혼란을 야기
논리폭탄 (Logic-bomb)	평상시에는 컴퓨터 내부에 잠복해 있다가 예정된 시간이나 특정한 명령어가 입력시 작동하는 바이러스 폭탄
컴퓨터 전쟁 바이러스 (Computer war virus)	컴퓨터 바이러스와 세균을 결합해 만드는 생명이 있는 바이러스임. 이것은 쓰레기나 기름찌꺼기에 사는 미생물처럼 전자물질을 먹어 치우며 스스로 번식이 가능함
전자파 총/전자폭탄 (Pulse Gun/E-Bomb)	강력한 전자파를 순간적으로 발생시켜 일정 지역은 마비시킬 수 있음
마이크로웨이브 무기 (Microwave weapon)	미사일, 전투기, 레이더망 등을 무력화시킬 수 있는 것으로써 현재 미국 및 러시아에서 개발 중

4. 사이버전 대응실태와 정보보호기술

세계 주요국의 사이버전 능력과 관련하여 미국의 테크 논리스틱스사는 사이버 무기 개발 프로그램을 바탕으로 세계 160여개 나라의 군 사이버 역량을 평가하였다. 역량목적(목적달성을 위한 목표와 심리 상태), 공격역량(전시 특수목적을 달성하기 위한 능력), 사이버 정보수집 능력(사이버 영역에서의 정보수집 적응력) 등의 3가지 항목에 대하여 각각 5점 만점으로 점수를 부여하였다. 그 결과 중국과 미국이 평균 4점으로 공동 1위에 올랐으며, 북한, 일본, 이스라엘이 평균 3.6점, 한국이 평균 3.2점으로 평가되었다.

또한 다른 분석 결과를 살펴보면, 2010년 미국 정보당국은 중국, 북한의 사이버전 대비 능력에 대하여 유사시 네트워크 단절 계획 및 능력이 매우 우수하다는 평가를 내린 바 있다.

한편 각국은 사이버전 대비 태세 구축 중점을 초기 방어 위주로부터 사이버 공격위주로 급격한 전환을 보이고 있다. 이에 따라 인적자원의 역량이 중요시되는 사이버전에서 승리하기 위하여 각국은 고도로 전문화된 인력을 확보하는 데 국가적 노력을 기울이고 있다.

정보전 또는 사이버 전쟁이란 용어 자체가 미국에서 나왔을 정도로 미국은 사이버 전쟁 분야를 주도하고 있다.

4.1 사이버전의 대응실태

미국은 9.11사태를 계기로 국토안보 및 사이버안보 주무 부처로 국토안보부를 신설하고 사이버 공간에서의 안전을 위한 대책을 추진하고 있으며, 국방부에서도 미국에서 가장 막강한 사이버 공격능력을 갖춘 국가안보국(NSA, National Security Agency) 부서를 가지고 있어 오래 전부터 사이버 전쟁에 대비한 가상훈련을 실시하고 있다. 이외에도 미국은 국가 정보통신기반보호와 악의적 해커들에 의한 사이버공격 대비 및 사이버 전사를 양성하기 위한 주요정책을 실현하고 있다.

또한, 미국은 2012년 국방부 주관으로 전세계 사이버 전장지도를 제작하는 'Plan X' 프로젝트에 착수하였다. 수백억 개의 컴퓨터 도메인, 서버 그리고 그들 간의 연결관계를 분석하는 데 목적이 있으며, 이를 통해 적에 대한 공격 루트를 마련하고, 적의 공격 징후 발생 시 반격 루트를 따라 빠른 속도로 선제공격을 수행하고자 한다. 인력 면에서도 사이버 사령부를 창설하여 '사이버 챌린지 프로젝트'을 통해 우수한 해킹 능력· 해킹 방어 능력을 보유한 사이버보안 전문가를 양성하고 있다.

중국은 '컴퓨터 바이러스' 침투가 원자탄보다 효율적이라는 군사위원회의 개념아래 1997년 6월 컴퓨터바이러스 부대 창설을 모태로 최근에는 사이버 공격과 정보교란의 모의훈련을 임무로 하는 넷 포스(Net Force)부대를 만들어 활동하고 있다.

일본 방위성에서도 방위력정비계획에 따라 사이버 공격을 받는 경우 공격 경로를 역으로 탐지해 공격 컴퓨터를 무력화하는 사이버공격 대항 바이러스를 개발하고 있으며, 자위대 컴퓨터시스템에 침입하는 사이버 테러에 대응하기 위한 전문부대를 신설하고 정보통신 시스템을 강화하고 있다.

현재 우리나라도 국방부에 국방정보전대응센터를 설립하여 정보보호 역량강화와 사이버 위협 대응에 다양한 노력을 기울이고 있다. 과거 통신용 암호장비에서 최근에는 통합 보안 관제 체계, 인증체계, 바이러스 방역체계 등 다양한 정보보호체계의 구축 및 운영을 활발히 추진하고 있다. 특히, 아태지역내 20개국의 국방 고위급회의인 '2013 서울안보대화(Seoul Defence Dialogue)'에서는 사이버안보 이슈를 실질적으로 논의하고 발전시킬 사이버 워킹그룹의 필요성에 공감하여 사이버전 사무국 창설을 제시하기도 하였다.

4.2 정보보호 기술

예견되는 미래전 환경에서는 첨단 IT의 활용이 더욱

증가하고 이에 따라 정보보호의 중요성은 더욱 필수적인 요소로서 대두될 것으로 예상된다. 특히, 사이버 공격이나 보안 침해사고가 쉽게 전체 시스템으로 확산되거나 인가되지 않은 사용자의 컴퓨터 시스템·네트워크 접근, 활용 등 공격이나 침입의 경로가 다양해지고 증가하고 있다.

정보보호 기술 분야는 적의 다양한 사이버 위협 및 공격을 탐지 및 차단하고 실시간으로 대응, 복구하여 정보체계와 이들을 상호 연결하는 네트워크를 효과적으로 보호할 수 있는 기술을 의미한다.

각종 정보보호 센서들이 탐지정보를 통합 추론 판단하여 사이버공격을 효과적으로 탐지하는 침입탐지 기술이 요구되며, 침입이 식별되었을 때 시스템이나 네트워크의 피해를 최소화하고 추가적인 침입을 막기 위하여 초기에 식별 제거하는 침입차단, 침입유도, 침입자 역추적기능이 제공되는 침입대응 기술이 요구된다. 또한, 사이버 침입이 발생하였을 때 국가핵심 시스템과 네트워크가 자기방어 능력을 갖추어 취약점 및 결합에 대해 즉시 인지하여 성능저하를 방지하고 정보체계나 네트워크에 침입이 가해지더라도 핵심기능은 유지되도록 하는 침입 감내 기술이 요구된다.

5. 결론

사이버전은 인력위주의 1세대 전쟁, 화력위주의 2세대 전쟁, 기동위주의 3세대 전쟁과 달리 '4세대 전쟁'이라 하며, 사이버 공격이나 보안 침해사고가 네트워크로 연동된 전체 시스템으로 확산될 경우 국가 기간망을 위협할 수 있다. 사이버공격 기술은 날로 지능화되어 군사지휘체계 및 국가 기간 시스템을 교란하거나 무력화시키는 형태로 발전되어 가고 있다.

이러한 시사점을 바탕으로 본 연구에서는 사이버전의 정의와 특징을 살펴보고, 사이버전의 최근 형태와 사이버전의 대응실태와 사이버 침해 및 위협에 따른 보안기술에 대하여 고찰하였다. 사이버전은 민·관·군이 상호 협력하는 대응체계가 요구되며, 사이버전에 대비한 정보기술은 국가안보를 위한 핵심기술이다. 따라서 사이버전에 대비한 인원, 운영, 기술 등 3대 요소의 균형 잡힌 전략으로 하나의 방어 장벽이 공격자에 의해 침투되거나 돌파되어도 연속적인 또 다른 방어수단을 통해 대응할 수 있는 계층적 전략이 요구된다.

참고문헌

[1] 차현종, 양호경, 신효영, 박호균, 유황빈, "전장 정보의 대량 획득과 처리를 위한 최적화 방안 연구",융합보안논문지, 제13권 제1호, pp.45-50, 2013.

[2] 양호경, 차현종, 신효영, 박호균, 유황빈, "시스템 사고를 이용한 사이버전 보안 정책 레버리지 전략 연구", 융합보안논문지, 제13권 제4호, pp.77-83, 2013.

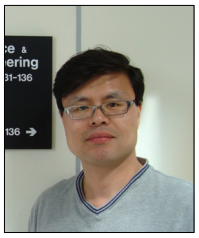
[3] 양호경, "사이버전의 기술적 보안정책 레버리지 전략 연구", 광운대학교 대학원, 2012.

[4] 서동일, 조현숙, "사이버전을 위한 보안기술 현황과 전망", 정보보호학회지, 제21권 제6호, 2011.

[5] 김귀남, "국가 사이버전 대비방안 연구", 정보·보안논문지, 제6권 제4호, 2006.

저자소개

● 박 호 균(Ho-Kyun Park)



- 1987년 2월 : 광운대학교 전자계산학과 (이학사)
- 1989년 8월 : 광운대학교 대학원 전자계산학과 (이학석사)
- 1998년 8월 : 광운대학교 대학원 전자계산학과 (이학박사)
- 1992년 3월 ~ 현재 : 신흥대학교 컴퓨터정보계열 교수
- 2011년 1월 ~ 현재: 경기산업 패밀리 클러스터 협의회장

<관심분야> : 홈네트워크, 정보보호, NFC, VOD