사이버전(Cyber War) 교전규칙

문봉교 (동국대학교 컴퓨터공학과 UCS연구실)

(1) 사이버전장

총알과 포탄이 빗발치는 전쟁터에도 '룰'은 있다. 교전(交戰)을 아무 때나 할 수 없고 국제법이 정한 일정 조건에서만 가능하다. 민간인을 고의로 살상하면 안 되고 병원과 교회, 문화재 등도 공격목표로 삼아선 안 된다. 포로와 부상자는 '인도적 대우'를 해야 한다. 무력충돌의 극한상황 속에서도 서로 지켜야 할 최소한의 약속, 바로 '교전수칙'이 존재한다. 유엔 헌장(7장)과 제네바·헤이그 협약이 그것이다. 그러나 국제사회는 지금 전혀 다른 차원의 전쟁을 목도하고 있다. 무기는 총탄과 미사일에서 '악성코드'(malware)로 바뀌었고 전장(戰場)은 인터넷으로 무대를 옮겼다. 출처불명의 해킹공격으로 방송국과 금융기관 서비스가 순식간에 마비되고 댐과 고속철도 등 국가 기간시스템이 교란되는 충격적 상황이 빈발하고 있다. 바로 '사이버 전쟁'이다.

사이버전은 사이버 첩보전, 사이버 테러전, 사이버 심리전, 물리적 연계전 등을 포괄하고 있는 개념으로 매우 다양하게 정의될 수 있다. 따라서, 사이버전 위협은 보이지 않는 적과 가상공간에서의 전장, 그리고 핵무기에 버금가는 엄청난 피해를 초래할 수 있다는 점에서 국가안보에 직접적인 영향을 미친다고 볼 수 있다. 본 연구의 목적은 바이러스 유포, 해킹 등 사이버 테러가 각종 행정정보를 위협하고, 경제활동을 위축시켜 경제적 손실을 야기하는 등 국방뿐 아니라 정치, 경제, 사회 등 전 분야에 걸쳐 큰 위협이 되고 있는 상황에서 사이버전을 효율적으로 대처하는데 있다.

그림1. 컴퓨터와 인터넷을 통해 이루어지는 사이버전

(2) 사이버전 교전규칙

북대서양조약기구(NATO)의 탈린 매뉴얼이 규정한 '사이버 전쟁'은 국가와 국가가 사이버 공간에서 적대적 군사행위를 하는 '무력충돌'의 한 형태다. 일반적 사이버 범죄나 사이버 스파이

행위와는 차별화된 개념이다. 일반적으로 분초를 다투는 사이버공격의 특성상 국가 주요 시스템이 공격받는 경우 여러 단계를 거쳐 대통령이나 국방부장관에 보고하고 답변을 기다리는 사이에 심각한 피해를 입을 수 있기 때문에 문제를 해결할 수 있는 군 내 사이버 전문가의 권한을 확대하는 것이 필요하다. 탈린 매뉴얼은 구속력 있는 문서가 아닌 사이버 전쟁을 둘러싼 국제법적 유권해석과 국제사회의 컨센서스를 반영한 일종의 '가이드라인'이다. 하지만 향후 국제법을 입안하는데 결정적 기준이 될 것으로 보인다. 본 연구에서는 군에 고용된 사이버부문 전문가가 유사시 비군사 컴퓨터 시스템에 대해서도 즉각적으로 조치를 취할 수 있는 권한을 어떤식으로 부여하도록 하는 것이 적절한지 탈린 매뉴얼 분석을 통해 심도 있는 방안을 도출하고자 한다.

(3) 주요 연구내용

가. 사이버전 진행과정

사이버전의 목적은 공격자가 목표시스템에 접근하여 자신이 원하는 형태의 공격을 시도하여 해당 시스템에 피해를 입히는 것이라 요약할 수 있다. 이와같은 공격은 다양한 공격과정과 공격기술을 기반으로 진행된다. 아래 그림은 사이버전 진행 순서를 5단계로 구분하여 나타낸 것이다.

그림 2. 사이버전의 진행순서

1) 정보수집

정보수집 단계는 해커들이 사이버전을 진행할 때 가장 먼저 하는 행위로 공격을 진행할 시스템에 관한 정보를 수집한다. 자동화된 네트워크 스캔도구를 이용하여 불특정 다수의 시스템의 네트워크 구조, 운영체제의 비전, 취약점 등과 같은 정보를 수집할 수 있다. 공격시스템이 사전에 정해져 있을 경우, 미리 사전정보를 획득하기 위해 주로 다음과 같은 도구들을 사용한다.

- 특정 취약점 스캔 공격 도구 : Cgiscan, winscan, rpcscan
- 다중 취약점 스캔 공격 도구 : SAINT, sscan2k, mscan, vetescan
- 은닉 스캔도구 : stealthscan, Nmap
- 네트워크 구조 스캔도구 : Nmap. firewalk

2) 공격시스템 접근

공격시스템 접근단계는 두 개의 과정으로 구성된다. 첫 번째 과정에서는 정보수집단계에서 수집한 정보를 바탕으로 공격할 시스템의 유효사용자의 계정정보 및 취약한 시스템 공유자원을 수집하여 공격시스템에 접근한다. 이때 수집한 정보는 대개 사용자 및 그룹명, 라우팅 테이블 정보, SNMP 정보등이 있다. 이러한 정보수집에 사용되는 도구의 종류는 다음과 같다.

- 사용자 계정 목록화 : null sessions, dumpACL
- 시스템 목록화 : net use/view, nbtscan, nbstat

- 파일공유 목록화 : shownmount, NAT, Legion
- SNMP 목록화 : solarwinds

두 번째 과정에서는 공격대상에 접근하여 권한을 획득한다. 여기에서 특정사용자의 비밀번호를 수집하는 것이 가능한데, 주로 스니퍼를 이용하여 아이디와 비밀번호를 찾아낸 후 시스템에 바로 접근하는 방법, 웹서버 등 네트워크 서버의 취약점을 이용하여 접근하는 방법, 비밀번호 정보가 기록된 파일을 취득하는 방법등 다양한 방법으로 공격시스템에 접근할 수 있다. 이 과정에서 사용가능한 도구를 이용하면 다음과 같다.

- 패스워드 도청 : tcpdump, L0phtcrack
- 파일 공유 무작위 공격 : NetBIOS Audit Tool, Legion
- 패스워드 파일취득 : pwddump7

3) 권한 변경

공격시스템에 접근한 해커들은 시스템의 취약점을 이용하여 관리자(root) 권한을 획득하려고 시도하게 된다. 일반적으로 시스템에서는 사용자별로 접근할 수 있는 서비스의 종류를 제한하고 있기 때문에, 해커들은 모든 서비스에 접근이 가능한 관리자 권한을 얻으려고 시도한다. 주로 시스템 취약점이나, 트로이목마 같은 악성 프로그램 그리고 버퍼 오버플로우(buffer overflow) 기술을 통해서 관리자 권한을 획득하게 되는데, 이때 사용할 수 있는 도구를 요약하면 다음과 같다.

- 패스워드 크랙 : John, L0phtcrack
- Exploit : lc_message, getadmin, sechole

4) 프로그램 설치

시스템에 접근한 해커들은 자신이 필요한 정보를 얻기 위해 추가적인 프로그램들을 설치할 수 있다. 예를들어, 일반 사용자의 홈 디렉토리에 스니퍼를 설치하여 관련 아이디와 비밀번호를 알아내어 해커의 이메일로 보내도록 할 수 있고, 웜 바이러스를 설치하여 주변시스템에 악성코드를 전파할 수도 있으며, 시스템내의 일부 환경을 변경할 수도 있다. 또한, 공격 대상에 관한 모든 접근권한을 획득한 후에, 해커가 침입한 사실을 은폐하기 위해 로그 및 감시기록을 삭제하고 설치된 프로그램들을 숨길 수도 있다. 이와 관련된 도구들은 다음과 같다.

- 로그 삭제 : Zap, Event Log GUI
- 도구 숨기기 : rootkit, file streaming
- 감사 방해 : AuditPol, /disable

5) 불법행위 실시

앞 단계에서 설치된 프로그램을 통해 해커는 원하는 정보를 얻을 수 잇게 되며, 경우에 따라서 구체적인 시스템 파괴를 할 수도 있다. 예를들어, rm -rf.* 등의 명령어를 이용하여 하드디스크내의 모든 디렉토리 정보와 파일정보를 삭제하거나 변경할 수 있다. 또한 사용자들의

이메일 정보나 디렉토리에 존재하는 자료들을 들여다 볼 수도 있으며, 공격시스템내에 있는 개인 사용자의 사적인 정보들을 허가없이 획득할 수도 있다.

나. 기존의 사이버공격 주요 사례

1) 스턱스넷 (Stuxnet)

최초의 사이버 무기로 알려져 있는 스턱스넷(Stuxnet)은 독일 지멘스사의 산업자동화제어시스템을 공격 목표로 제작된 악성코드로, 원자력, 전기, 철강, 반도체 등 주요 산업 기반 시설의 제어시스템(SCADA: Supervisory Control and Data Acquisition)에 침투해 오작동을 일으키는 멀웨어(malware)이다.

Stuxnet 공격 과정

- 1단계 (PC 감염) : 인터넷에 연결된 windows 기반 PC 감염 (자각증상 없음)
- 2단계 (내부망 침투) : USB 저장장치를 통해 내부망 침투 (외부 인터넷 망 연결없이 가능)
- 3단계 (제어시스템 교란) : 기반시설제어시스템 감염후 제어 명령 조작을 통한 이상 동작발생 (예, 냉각장치 교란, 특정 임계치 조작 등)

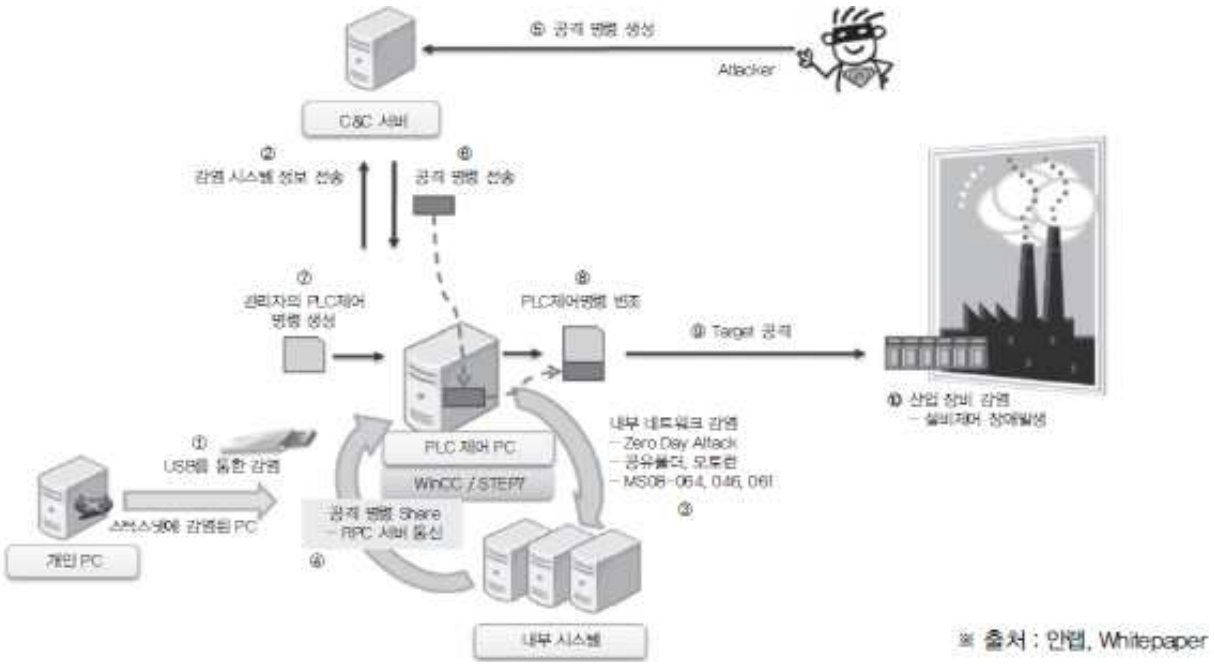

그림 3. 스턱스넷 (Stuxnet) 공격과정

2) GPS 교란 공격

2011년 3월4일, 북한측 지역에서 강한 GPS(Gloabl Positioning System) 교란 전파가 발사되어 경기도를 포함하여 서울 북부, 인천, 파주 등 수도권 일대에서 이동통신 서비스 등에 문제가 발생하였다. 이로 인해, 인공위성 자동위치측정시스템(GPS)을 활용한 휴대전화의 시계가 오작동하고, 이동전화의 수/발신에 장애가 발생하였으며, GPS 신호 수신에 문제가 발생하였다.

그림 4. 북한의 GPS 교란 개념도

3) DDoS (분산서비스거부) 공격

2009년 7월7일부터 10일까지 국내외 주요 웹사이트를 대상으로 동시 다발적인 DDoS 공격이 발생하여 인터넷서비스 장애 및 지연 발생하였으며, 3차에 걸친 DDoS 공격으로 청와대를 포함한 국내 22개 사이트와 백악관을 포함한 14개 미국 웹사이트가 접속장애 발생 (7.7 DDoS 공격). 또한, 2011년 3월3일부터 5일까지 국내 주요 웹사이트를 대상으로 동시다발적 DDoS 공격이 발생하여 인터넷 서비스 장애 및 지연 발생 (3.4 DDoS 공격)

〈표 1〉 2009년 7.7 DDoS 공격 및 2011년 3.4 DDoS 공격의 특징 비교

항 목		7.7 DDoS	3.4 DDoS
공격 대상		한국, 미국의 23개 사이트	한국 40개 사이트
공격 방법	시스템 손상	특정 조건 완료시 좀비 PC 하드디스크 파괴	모든 좀비 PC 하드디스크 파괴
	악성코드	동일한 악성코드	6개 이상의 변종 악성코드
	지령서버	없음	있음
공격 주체		–	–
치료 방해		없음	백신 업데이트 및 홈페이지 접근 방해
좀비 PC 규모		총 115,044대 (최대 공격 좀비 PC : 47,123대)	총 77,207대 (최대 공격 좀비 PC : 51,434대)
피해액		363억~544억원 (산출: 현대경제연구원)	–

4) 금융전산망 해킹

사이버전으로 금융전산망을 마비시켜 국가적인 혼란을 초래할 수 있음을 보여준 극명한 사례

- 1단계 (웹서버 해킹, 악성코드 삽입, 이용자 감염) : 불특정 다수를 대상으로 무차별적인 감염 시도 중 NH 외주업체 직원의 노트북이 감염
- 2단계 (공격대상 정보수집) : 네트워크(중계서버) 접속 감시 및 키로깅(Keylogging)을 통한 접속암호를 수집 (Stuxnet과 같이 폐쇄망에서도 인터넷PC와 USB 혼용시 정보수집 가능)
- 3단계 (공격 실행) : 수집된 중계서버 접속정보(IP주소, ID, 패스워드) 이용, 데이터 삭제 스크립트 작성, 스크립트 파일을 사고 노트북PC에 설치, 충분한 시간이 경과후 의도적 실행

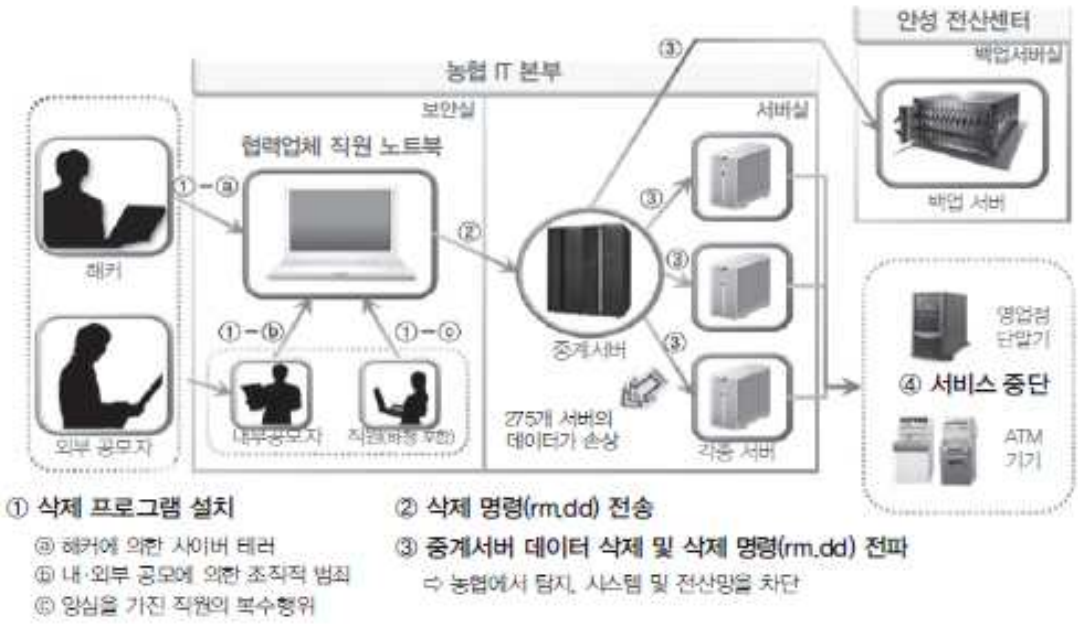

그림 5. NH 전산망의 장애 발생 과정

라. 국내외 사이버전 사례와 탈린 교전규칙

지난 2013년 3월 20일 우리나라 3개 방송사와 2개 금융회사 전산망이 마비되면서 충격을 줬지만, 최근까지도 세계 각지에서 사이버 테러가 잇따랐다. 지난달 북대서양조약기구(NATO)와 체코, 벨기에, 포르투갈 등 유럽 정부 기관 컴퓨터가 일제히 악성코드 공격을 받았다. 미국은 기업과 정부 기관, 언론사 등이 파상적인 해킹 피해를 입으면서 공격 당사국으로 지목된 중국과는 외교전까지 벌이는 단계다. 각국 정부는 사이버 전쟁에 대비한 군부대를 조직하고, NATO는 '사이버 전쟁 교본'까지 내놨다.

1) 사이버전 교전 사례

- 사이버전 대책 및 안내서

NATO의 협력기구인 사이버방어센터(CCDCOE)는 '사이버 전쟁 안내서'를 출간했다. 에스

토니아의 탈린에 있는 CCDCOE는 2008년부터 각종 사이버 공격과 관련한 연구를 진행해 온 NATO 협력기구다. 3년에 걸친 작업으로 완성된 안내서는 사이버 공격을 '사상자를 내거나 시설을 파괴·손상시키려는 의도로 행한 행위'로 정의하면서 "핵 시설이나 병원, 댐 시설 등은 절대로 목표물로 삼지 않는다"는 수칙을 제시했다. 또 '핵티비스트(hacktivist·컴퓨터 해킹을 투쟁 수단으로 사용하는 행동주의자)'가 사이버 공격에 가담할 경우엔, 민간인이더라도 합법적인 군대의 공격 목표물이 될 수 있다고도 했다.

각국 정부도 사이버 공격 대응에 나서고 있다. 미국은 단순 방어에서 벗어나 공격도 불사한다는 방침을 세웠다. 미국 국방부 국가안전국(NSA)의 키스 알렉산더 사이버사령관은 상원 군사위원회 청문회에서 "2015년까지 미국의 주요 기반시설 해킹을 막기 위한 40개의 지원팀을 만들고, 만약 공격을 당할 경우 해당 국가에 사이버 공격을 할 수 있는 13개 부대를 창설하겠다"고 밝혔다고 워싱턴타임스가 전했다. 독일도 국가 주도로 사이버 전쟁에 대비한 군부대를 둔 상태다. 독일 정부는 2012년 6월 의회 보고서를 통해 극비리에 사이버 전쟁에 대비한 군부대가 있다는 사실을 밝혔다고 DPA통신이 보도했다. 러시아도 정부 주도로 사이버 보안 대책을 마련하고 있다. 모스크바타임스는 올해 초 블라디미르 푸틴 대통령이 "러시아 본국과 외교 거점에 대한 사이버 공격을 추적·예방하는 것은 물론, 아예 무력화시킬 수 있는 시스템을 개발하라"고 주문했다고 전했다.

- 해킹에 노출된 각국 정부기관 및 은행

구글 등 글로벌 대기업을 겨냥해 왔던 사이버 공격은 최근 각국 정부 기관과 금융회사, 언론사로 번지는 양상이다. 올해 사이버 공격 문제로 가장 시끄러운 국가는 단연 미국이다. 뉴욕타임스(NYT)의 폭로로 알려진 미국 주요 언론 해킹 사태는 컴퓨터 보안업체 맨디언트가 "중국 군대가 해킹을 주도했다"는 보고서를 내놓은 후 외교전으로까지 번졌다. 그 외에 주요 은행 중 하나인 JP모건체이스가 해킹을 당했다. 또 버락 오바마 미국 대통령의 부인인 미셸 오바마를 포함한 여러 미국 정부 인사도 해킹 피해를 입었다고 ABC가 보도했다. 유럽도 해킹 문제로 시끄럽다. 먼저 체코가 해킹으로 몸살을 앓았다. 주요 언론사 웹사이트가 공격을 당한 데 이어, 체코 중앙은행과 체코 주요 은행, 프라하 증권거래소가 사이버 공격을 받았다. 앞서서 NATO 컴퓨터와 체코, 아일랜드, 루마니아의 유럽 정부 기관 컴퓨터가 어도비(Adobe)의 소프트웨어로 퍼진 악성코드 때문에 마비됐다.

- 각국에 등장한 사이버 민족주의

각국이 사이버 전쟁 대비 태세를 갖추는 모습을 '사이버 민족주의(cyber nationalism)'로 묘사하기도 한다. 사이버 보안 전문가인 브루스 슈나이더는 "세계 각국이 사이버전쟁에 대비한 무장 경쟁을 벌이고 있다"면서 "인터넷 상에서 민족주의가 나타나고 있다"고 지적했다. 사이버 민족주의가 발전하면 소프트웨어의 국적이 문제될 수 있다. 특정 국가의 소프트웨어가 일괄적으로 기피 대상이 될 수 있다는 얘기다. 그럴 경우 보안업체들은 미국과 중국처럼 사이버 보안 문제가 민감한 곳에 기반을 두지 않고, 그 대신 아예 사이버 공격 혐의가 없는 국가로 이전하게 될 것이라는 전망도 나온다. 실제로 핀란드의 에프 세큐어(F-secure)라는 보안업체에는 최근 아시아·태평양 지역 고객의 문의가 늘어나고 있다.

2) 사이버전 교전규칙의 필요성

- 사이버전이 전면전으로 확전가능

반드시 국가만이 전쟁의 당사자는 아니다. 테러단체와 같은 비국가 행위자도 해당된다. 사이버전의 핵심 요소인 사이버 공격(cyber attack)은 인명 살상이나 목표물의 손상 등 물리적 타격으로 이어질 수 있는 사이버 작전을 뜻한다. 상대국의 중요 인프라나 명령·통제시스템을 겨냥한 해킹공격이 대표적이다. 사이버 공격을 당했을 경우 피해국은 비례성의 원칙에 따라 가해국에 대해 대응조치(countermeasures)를 취할 수 있다. 이 경우 공격의 강도와 피해규모에 비례해 적절한 대응을 꾀해야 한다.

국제사회가 주목하는 대목은 사이버 전쟁이 반드시 사이버 공간에만 한정되지 않는다는 점이다. 상황에 따라 물리적 대응이 가능하고 이는 온·오프라인을 포괄하는 전면전으로 '확전'될 수 있다는 관망이 나오고 있다. 탈린 매뉴얼은 국제법상 허용되는 '무력 사용'(use of force)'이 사이버 공간에서도 가능하다고 해석하고 있다. 관건은 과연 언제, 어떤 조건 하에서 무력 사용이 가능하느냐 하는 점이다. 합법적 무력사용이 인정되는 경우는 유엔 헌장 7장을 원용한 두 가지 경우다. 국제평화 유지를 목적으로 안보리 승인에 따라 군사적 강제조치를 취하는 경우(42조), 그리고 '무력 공격'을 당해 자위권을 행사하는 경우(51조)다. 사이버전쟁과 연계된 무력사용은 바로 자위권 행사에 근거할 가능성이 높다는 분석이다.

문제는 사이버 공간에서 자위권 발동 요건인 '무력 공격'이 발생한 경우를 어떻게 상정할 것이냐이다. 탈린 매뉴얼은 사이버 공격으로 인해 인명피해가 발생하거나 국가자산이 손상 또는 파괴되는 경우, 즉 '치명적이고 파괴적인' 물리적 피해가 발생한 경우 무력사용이 가능하다고 보고 있다. 이는 앞으로 사이버 전쟁이 재래식 전쟁과 맞물리며 매우 복잡다기한 양상으로 발전할 것임을 보여주고 있다는 분석이다. 리언 패네타 전 국방장관은 올해 초 "적의 사이버 공격 징후가 있으면 선제공격도 가능하다"고 밝힌 바 있다. 탈린 매뉴얼 논의에 참여한 학자들도 만장일치로 "사이버 공격으로 전면전이 일어날 가능성이 있다"는 견해를 보이고 있다.

- 사이버전에서 공격가능 대상범위의 애매함

탈린 매뉴얼은 핵티비스티의 개념을 "이념적·정치적·종교적·애국적 목적으로 해킹에 가담한 민간인으로 규정하고 있다. 그러면 사이버 전쟁에서 공격이 가능한 대상은 어디까지로 해야 하는지 어려움이 있다. 제네바 협약과 마찬가지로 시민들의 생존에 필수불가결한 목표물들은 공격을 삼가도록 하고 있다. 광범위한 인명의 손실을 가져올 잠재적 위험성이 있기 때문이다. 농업과 식품, 가축, 식수, 관개시설 등이 그것이다. 또 댐과 제방, 원자력 발전소와 같은 시설에도 특별한 주의를 기울이라고 주문하고 있다. 병원과 의료시설, 문화재도 보호대상이다. 그러나 시민들의 일상생활이나 삶의 질과 관련된 목표물들은 탈린 매뉴얼상 사이버 공격으로부터 보호를 받는 대상이 아니다. 방송사와 금융기관, 인터넷, 통신망 등이 그것이다.

- 사이버전에서는 보이지 않는 적들과의 교전

사이버 공간의 복잡하고 불가측한 속성을 감안할 때 탈린 매뉴얼의 적용기준이 모호하고 허점도 적지 않다는 지적이 나온다. 무엇보다도 적이 보이지 않는다는 게 최대 난제다. 사이버 공격의 진원지를 찾기 어렵다는 얘기다. 갈수록 정교해지는 해킹수법으로 볼 때 '공격의 흔적'을 얼마든지 은폐·위장할 수 있고, 이 경우 사이버 대응의 전제조건인 '책임규명' 자체가 어려워질 수 있다는 것이다. 미 컴퓨터 보안업체 맨디언트는 지난 2월 보고서에서 지난 10년간 미국 내 140개 민간기업과 연방정부 등이 상하이 거점의 인민해방군 부대에 의해 해킹을 당했다고 밝혔지만 이를 실제로 '입증'하지는 못하고 있다.

특히 사이버 공격이 특정국가의 사이버 인프라에서 시작됐거나 경유됐다는 것만으로 공격의 책임이 있다고 단정하기 어렵다는 게 탈린 매뉴얼의 설명이다. 다만 해당 국가가 사이버 작전에 연관돼 있음을 보여주는 지표에 불과하다는 얘기다. 지난 3·20 사이버 테러와 관련해 공격에 사용된 북한 내부 IP 주소에서 나왔더라도 북한에 공격의 책임이 있다고 확정하기는 어려울 수도 있다는 분석이 나온다. '무력사용'의 발동요건도 모호하다는 지적이 있다. 눈에 보이는 물리적 피해가 없더라도 경제적·무형적 손실이 크고 지속적일 경우 무력수단을 사용해야 한다는 주장이 나온다.

- 국제법 질서와 사이버전 적용시 어려움

탈린 매뉴얼 발간을 계기로 사이버전쟁 교전수칙을 어떤 방향으로 만들 것이냐를 놓고 미·영과 중·러 간 줄다리기가 이어지고 있다. 미국과 영국은 제네바·헤이그 협약 등의 국제법을 사이버 공간에도 그대로 원용하자는 입장이다. 그러나 중국과 러시아는 사이버 공간은 완전히 별개의 '공간'이어서 새로운 차원의 조약을 만들자고 주장하고 있다. 미·영 중심의 현 국제법 질서를 바꿔보려는 의도다. 탈린 매뉴얼은 기본적으로 미·영의 입장을 반영하고 있다. 지난해부터 사이버전쟁 교전규칙을 독자 준비 중인 미국은 탈린 매뉴얼을 가장 중요한 준거 자료로 삼을 가능성이 커 보인다. 영국도 탈린 매뉴얼을 기초로 한 교전수칙 논의에 찬성하고 있다.

그러나 미·영의 이니셔티브에 중·러가 선뜻 동의할 가능성은 커 보이지 않는다. 다만 국제법적 논의를 서둘러야 한다는 공감대가 커지고 있어 양대 그룹으로서는 어떤 식으로든 '접점'을 마련해야 한다는 압박을 느낄 것으로 예상된다. 탈린 매뉴얼을 기초한 미국 해군 전쟁대학 마이클 슈미트 교수는 "사람들은 사이버 공간을 무법천지의 '와일드 웨스트'라고 하지만 적용할 법들은 매우 많다"고 말했다.

3) NATO의 탈린 매뉴얼

북대서양조약기구(NATO) 산하 사이버방위센터 (CCDCOE)는 해킹 같은 무형의 공격이라도 유형의 물리력으로 대응할 수 있는 교전규칙을 제정했다. 사이버방어 협력센터가 있는 에스토니아의 수도 이름인 탈린을 제목으로 사용한 사이버 교전규칙 ('탈린 매뉴얼'의 95개 조항) 은 40여 명의 군사 및 국제법 전문가가 3년에 걸쳐 연구한 결과물로 현대의 전면전이 단순 컴퓨

터 해킹으로부터 촉발될 수 있으며, 사이버전을 통해 인명이 살상될 수 있다는 점을 연구의 모티브로 삼고 있다. 이 매뉴얼은 사이버작전을 물리적 수단을 사용하는 비사이버작전과 동일하게 보고 있다. 다음은 '탈린 매뉴얼(tallinn manual)'로 불리는 NATO가 발표한 사이버 전쟁 교전수칙의 주요 내용이다.

▲ 1조 = 국가는 영토 안의 사이버 인프라와 사이버 활동을 통제할 수 있다.
▲ 5조 = 국가는 영토 안의 사이버 인프라가 다른 국가에 불법적으로 악영향을 미치도록 쓰이게 둬서는 안 된다.
▲ 6조 = 국가는 스스로 유발해 국제적 의무를 위반한 사이버 활동에 법적 책임이 있다.
▲ 7조 = 한 정부의 사이버 인프라에서 사이버 공격이 비롯됐다는 사실만으로 이 국가가 공격을 일으켰다고 단정할 수는 없다. 하지만, 이는 이 국가가 사이버 작전에 관련 있다는 것을 암시한다.
▲ 8조 = 사이버 공격이 어느 국가의 사이버 인프라를 거쳐 이뤄졌다는 것만으로 이 국가에 책임을 돌릴 수는 없다.
▲ 9조 = 국제적으로 잘못된 행동으로 피해를 본 국가는 이에 비례해 사이버 작전으로 상대국에 대응할 수 있다.
▲ 10조 = 다른 국가의 영토 주권이나 정치적 독립을 위협하거나 이를 상대로 무력을 사용하는 사이버 작전은 불법적이다. 유엔의 목적에 어긋난 사이버 작전도 마찬가지로 불법적이다.
▲ 11조 = 사이버 작전은 규모와 영향이 무력을 쓴 정도의 비(非)사이버 작전에 버금갈 정도로 클 때 무력 사용으로 여겨진다.
▲ 13조 = 무력공격 수준의 사이버 작전의 대상이 된 국가는 고유한 자위권을 행사할 수 있다. 피해국의 인명이 살상되거나 주요 자산이 파괴된 경우 무력공격 수준의 사이버 작전으로 간주한다.
▲ 22조 = 국제적 무력 충돌은 2개 이상의 국가 사이에 사이버 작전을 포함한 적대행위가 있을 때 존재한다. 사이버 작전만으로도 국제적 무력 충돌로 번질 위험성이 있다.
▲ 30조 = 사이버 공격은 인명을 살상하거나 기물을 파손할 것으로 합리적으로 예상할 수 있는 사이버 작전을 뜻한다.
▲ 32조 = 민간인은 사이버 공격의 대상이 돼서는 안 된다.
▲ 35조 = 민간인은 적대행위에 직접 가담하지 않는 한 공격에서 보호받아야 한다.
▲ 36조 = 민간인에 공포심을 퍼뜨리는 것이 주목적인 사이버공격과 그 위협은 금지된다.
▲ 58조 = 상황이 여의치 않은 경우가 아니라면 민간인에 영향을 끼칠 수 있는 사이버 공격을 할 때 미리 경고해야 한다.
▲ 75조 = 전쟁 포로와 다른 수감자들은 사이버 작전의 악영향으로부터 보호받아야 한다.
▲ 80조 = 댐과 제방, 핵 발전소를 공격하면 민간인이 큰 피해를 보거나 위험 물질이 방출될 수 있으므로 특별히 주의해야 한다.
▲ 81조 = 사이버 작전으로 민간인의 생존에 필수적인 시설을 공격·파괴· 제거하거나 쓸모없게 만드는 행위는 금지된다.
▲ 82조 = 무력 충돌 당사자들은 사이버 작전으로 영향받을 수 있는 문화재를 존중하고 보

호해야 한다. 특히 디지털 문화재를 군사 용도로 사용하는 것을 금한다.

▲ 92조 = 중립지역에서 사이버 수단으로 공격권을 행사하는 것은 금지된다.

4) 미국의 사이버전 교전규칙 승인

지난 2012년 11월 미국은 자국의 컴퓨터 네트워크를 보호하기 위하여 2004년의 지침을 개정한 새로운 가이드라인을 마련했다. 이 지침에서 미 정부의 국가안보와 사이버 방책들이 서로 잘 결합할 수 있도록 작전 원칙과 절차를 규정한 것으로 알려졌다. 이 지침은 최초로 사이버 분야에 있어 방어 행위와 공격 행위를 그리고 네트워크 방호와 사이버작전을 명확하게 분리하여 규정하였다. 또한, 사이버 안보 거버넌스를 확립하여 각 기관의 사이버 작전 관련 업무를 부여하였으며, 군이 미국의 공공·민간 네트워크 위협에 대응하며 나아가 사이버 공격을 수행할 수 있는 근거를 마련하였다. 이러한 점에서 미국 언론을 비롯한 주요 언론들은 이번 지침을 사이버 교전규칙, 사이버전 전략, 사이버 작전 가이드라인의 마련 등으로 표현하고 있다.

이번 지침에 따라 미 국방부가 마련하고 있는 사이버전 교전 규칙 역시 중요한 변화와 함께 진전이 있을 것으로 예상된다. 2012년 3월, 미 국방부는 사이버전 교전 규칙을 개발하고 있다고 발표한 바 있으며, 현재 사이버전 교전규칙이 완성 단계이며, 미 국방부는 국방 네트워크뿐만 아니라 미국 공공과 민간 네트워크 전반에 대하여 책임이 있다고 밝혔다. 이번 지침에 대하여 국제 교전규칙 및 사이버전 관련 규범이 마련되지 않은 상황에서 독자적인 규칙 마련이라는 한계 역시 지적되고 있다. 하지만, 이는 미국 정부의 현실적인 대응방안의 마련과 적극적인 의지를 표명했다는 점에서 의미를 갖는다는 평가를 받고 있다. 이번 지침으로 인하여 효율적인 의사결정이 가능하다는 점에서 큰 진전이라 평가받고 있다.

마. 국내 사이버전 교전규칙의 필요성

사이버 위협이 국가 안보에 대한 위험 요소로 다가옴에 따라 사이버 영역에서 군의 역할이 확대되고 있는 상황이다. 한국군 역시 2010년 사이버사령부를 창설하고 위상을 강화하였으며, 2012년 국방부 연두 업무보고에서 국가 통합방위영역에 사이버공간을 포괄하여 방어를 규정한 바 있다. 하지만 아직까지 사이버사령부의 역할이 명확하지 않으며, 역량이 부족하다는 평가를 받고 있다. 현재 사이버 전투준비태세와 사이버 교전규칙이 마련되고 있지 않아 사이버전 대응 정책도 미비하다고 볼 수 있다. 사이버안보 거버넌스 문제 역시 2011년 국가사이버안보마스터플랜이 제정되었음에도 명확하게 해결되지 않았다는 지적이 나오고 있다.

최근 북한의 GPS 신호교란은 비(非) 물리적 수단을 쓴 새로운 형태의 도발행위다. 전자전의 일종으로 간주되는 GPS 신호교란은 유해한 전파의 혼신을 금지하는 국제전기통신연합(ITU) 헌장 45조와 국제민간항공조약 부속서 17에 명시된 불법침해 행위에 해당하는 명백한 국제법 위반이다. 고의로 자행하는 전자적 교란을 통해 비행 중인 여객기와 국민의 안전이 위협받는다는 측면에서도 분명한 적대행위다. 그러나 이러한 북한의 GPS 신호교란에 대해 무력공격으로 즉각 대응하는 것은 유엔헌장 51조에 명시된 자위권 발동 기준에 의거 제약될 수 있다. 즉, 실질적인

무력을 기반한 자위권을 발동하기 위해서는 우선 적의 무력공격이 발생해야 하며, 공격받은 수준에 비례하고 다른 수단으로 대체할 수 없을 때만 국제법상 정당화된다는 뜻이다. 결국 현재 국제법을 법리적 측면에서만 보면 적의 전자전이 무력공격에 해당한다고 간주하더라도 전자전은 동일 수준의 전자전으로 대응할 수밖에 없는 어려움이 있다.

탈린 매뉴얼은 현대의 전면전이 단순 컴퓨터 해킹으로부터 촉발될 수 있으며, 사이버전을 통해 인명이 살상될 수 있다는 점을 연구의 모티브로 삼고 있다. 이 매뉴얼은 사이버작전을 물리적 수단을 사용하는 비사이버 작전과 동일하게 본다. 즉, 사이버 공격을 사이버 피해나 파괴뿐만 아니라 인명이 살상될 수 있는 무력분쟁으로 간주(30조)하고, 물리적 공격에 상응하는 사이버 공격의 대상이 된 국가는 고유의 자위권을 사용할 수 있으며(13조), 사이버 공격과 물리적 공격이 상호 비례한다면 맞대응 수단이 될 수 있다는 원칙을 제시(14조)했다. 아직은 탈린 매뉴얼을 나토가 공식적으로 채택하지 않고 자문 성격으로 활용하는 단계지만, 앞으로 사이버전을 통해 발생한 피해에 실제 물리적 공격으로 대응하는 형태로 전쟁이 확대될 가능성이 커졌기 때문에 국제법 학자들을 동원해 선행연구를 한 셈으로 볼 수 있다.

예를 들어 이란의 나탄즈 핵발전소를 중지시킨 스턱스넷 공격이 냉각시스템의 마비와 폭발을 조장하거나, 북한의 GPS 신호교란 공격이 인천공항에 접근하는 여객기의 항로이탈과 추락사고를 조장할 수 있다면 비물리적 공격행위가 현실의 전쟁행태임을 인식해야 한다. 유엔헌장 제정 당시인 1945년에는 전혀 예상하지 못했던 공격유형에 대해 당시 기준을 계속 적용하는 것은 합당치 못하다. 오히려 사이버공간을 포함한 비물리적 영역을 하나의 작전영역으로 간주하고 있는 현실을 고려할 때 피해가 자명하고, 더더욱 인명 살상으로 확대될 수 있다고 판단된다면 사후적 자위권은 운용돼야 하는 것이 타당하다.

최근 미국의 사이버안보 해결 의지와 사이버 공격을 포함한 사이버 교전규칙 마련을 위한 노력은 많은 시사점을 준다. 정부에서도 사이버 안보 분야 역시 해결에 대한 의지와 효과적인 거버넌스 체계의 마련과 사이버 교전수칙의 마련 등의 노력을 기대한다. 또한 올해 서울에서 개최되는 '2013 서울 사이버스페이스 총회'와 서울안보대화 등의 국제회의에서 국제 사이버전 규범 및 사이버 교전규칙 등에 대한 논의가 이루어질 것으로 보인다. 이제 우리 군도 한반도 실정에 적합한 전자전 및 사이버교전 교전규칙을 마련해야 한다.