한국경호경비학회 – 제39호(2014): 319–353
투고일 2014. 04. 21, 심사일 2014. 05. 27, 게재확정일 2014. 06. 18

사이버 안보에 대한 국가정보기구의 책무와 방향성에 대한 고찰

한 희 원

사이버 안보에 대한 국가정보기구의 책무와 방향성에 대한 고찰

한 희 원*

〈요 약〉

2001년 9/11 테러공격 이후에 미국은 사이버 안보를 가장 위중한 국가안보 문제로 인식한다. 미국 국방부는 2013년 처음으로 사이버 전쟁이 물리적인 테러보다 더 큰 국가안보 위협임을 확인했다. 단적으로 윌리암 린(William J. Lynn) 국방부 차관의 지적처럼 오늘날 사이버 공간은 육지, 바다, 하늘, 우주 다음의 '제5의 전장(the fifth domain of warfare)'이라고 함에 의문이 없다. 인터넷의 활용과 급속한 보급은 사이버 공간에서의 상상하지 못했던 역기능을 창출한 것이다.

이에 사이버 정보와 사이버 네트워크 보호까지를 포괄하지 않으면 국가안보 수호의 목표를 달성할 수 없게 되었다. 그런데 이러한 위험성에도 불구하고 각국은 운영상의 효율성과 편리성, 국제교류 등 외부세계와의 교류확대를 위해 국가기간망의 네트워크화를 더욱 확대해 가고 있고 인터넷에의 의존도는 심화되고 있다. 하지만 그 실천적인 위험성에도 불구하고 우리의 법제도적 장치와 사이버 안전에 대한 인식수준은 현실을 제대로 반영하지 못하고 있는 것으로 판단된다.

오늘날 가장 실천적이고 현실적인 위협을 제기하는 사이버 안보의 핵심은 하나도 둘도 계획의 구체성과 실천력의 배양이다. 대책회의나 교육 등은 부차적이다. 실전적인 사이버 사령부와 사이버 정보기구 그리고 사이버 전사의 창설과 육성에 더 커다란 노력을 경주해야 하고, 우리의 경우에는 가장 많은 경험을 가지고 인력과 장비를 가진 국가정보원의 사이버 수호 역량을 고양하고 더 많은 책무를 부담시키고 합리적인 업무 감독을 다하는 것에 있다고 할 것이다.

이에 본고는 법규범적으로 치안질서와 별개 개념으로서의 국가안보에 대한 무한책임기구인 국가정보기구의 사이버 안보에 대한 책무와 그에 더하여 필요한 사이버 정보활동과 유관활동의 범위를 검토하고자 한다. 사이버 테러와 사이버 공격을 포괄한 사이버 공격

* 동국대학교 법과대학 정교수

(Cyber Attack)에 대한 이해와 전자기장을 물리적으로 장악하는 전자전에 대한 연구도 포함한다.

주제어 : 사이버 안보, 사이버 테러, 사이버전쟁, 전자전, 제5의 전장

목 차

Ⅰ. 새로운 국가안보 환경

2009. 7. 7과 2011. 3. 4 대한민국 주요기관 홈페이지가 사이버 공격을 받았다('해럴드 경제', 2013. 8. 9: 21). 2013년 3월에는 신한은행, 우리은행, 농협의 금융전산망이 뚫려 개인정보가 유출되었고 KBS, YTN, MBC가 해킹을 당했고 3만대 이상의 컴퓨터가 악성 바이러스에 오염되는 대형 사이버 사고가 발생했다('머니투데이', 2014. 3. 11: 23). 현재까지도 주동자가 밝혀지지 않은 가운데 북한 또는 북한 연계조직과의 의심에 무게를 둔다. 그 무렵 북한은 북핵에 대한 비난과 한미 연합훈련의 강행 등을 이유로 대한민국 국책은행과 주요 언론사에 대한 강도 높은 보복 경고를 해 오던 터이기 때문이다. 오늘날 북한의 사이버 전쟁 능력은 대단한 것으로 추정된다. 북한은 약 4,000명의 훈련된 해커를 국가가 직접 관리하는 것으로 알려져 있다(Kim, Eun-jung, Yonhap News Agency. 2013. 4. 6).

이에 2013. 7. 4일 박근혜 정부는 '선진 사이버안보 강국 실현'을 목표로 하는 사이버안보 강화를 위한 4대 전략(PCRC)을 발표했다. 4대 전략 내용은 다음과 같다. 첫째, 사이버 위협에 대한 즉응성 강화를 위해 사이버안보 컨트롤 타워는 청와대가 맡고, 실무총괄은 국정원이 담당하며 미래부·국방부 등 관계 중앙행정기관이 소관 분야를 각각 담당토록 하는 대응 체계와 동시 상황전파 체계를 구축하며 중요 사고에 대해서는 '民·官·軍 합동대응팀'을 중심으로 상호협력 및 공조를 강화한다. 둘째,

국가차원의 ‘사이버위협정보 공유시스템’을 2014년까지 구축하고 민간 부문과의 정보제공·협력을 강화해 나간다. 셋째, 2017년까지 집적정보통신시설(IDC)·의료기관 등을 포함한 주요정보통신기반시설을 확대(209→400개)하고 국가기반시설에 대해 인터넷 망과 분리·운영하는 테마별로 특화된 위기대응훈련을 실시한다. 주요 민간기업에 대해서는 정보보호 관리체계 인증 대상을 확대(150→500개)하고 중소기업을 대상으로 보안취약 점검 및 교육지원도 한다. 넷째, 최정예 정보보호 전문가 양성사업 확대 및 영재교육원 설립 등 다양한 인력양성 프로그램을 추진하여 2017년까지 사이버 전문 인력 5,000명을 양성하고 10대 정보보호 핵심기술 선정과 연구개발의 집중적 추진으로 기술 경쟁력을 강화해 나간다.

이처럼 대규모 해킹 사건과 금융사 개인 정보 유출 등 초대형 정보 보안 사고가 빈발하자 대한민국 사이버 시장의 잠재력이 매우 크다고 판단하고 카스퍼스키랩, 래피드7, 인베이테크놀로지스 등 글로벌 보안업체들이 '코리아러시'를 이룬다고 한다(‘조선비즈’, 2014. 2. 17: 18). 사이버 보안사고가 빈발하는 한국이 일종의 테스트 베드(test bed) 역할을 하는 우울한 모습인 것이다.

한편 미국 국방부는 2013년 처음으로 사이버전이 알카에다 등 테러보다 더 커다란 국가안보 위협임을 공식적으로 확인했다. Mike Rogers(2013) 하원 정보위원회 의장은 “대부분의 미 국민들은 미국이 현재 “사이버 전쟁” 중 인줄을 모른다고 지적했다. William J. Lynn(2013) 국방부 차관은 “펜타곤은 사이버 공간을 육지, 바다, 하늘, 우주처럼 군사작전에 결정적으로 중요한 새로운 전장, 즉 ‘제5의 전장(the fifth domain of warfare)으로 공식적으로 인식하고 있다”고 밝혔다.

사이버 공간의 위험성에 대해서는 일찍이 국제테러조직과 미국의 경고 공방이 있었다. 2001년 9월 11일 테러공격에 대한 보복이자 주동자인 오사마 빈 라덴을 포획하기 위한 작전일환으로 미국과 북대서양조약기구(NATO) 연합국은 알카에다를 지원하는 것으로 의심되는 아프가니스탄을 상대로 전쟁을 개시했다. 이에 알카에다 테러조직 및 아랍권 일부에서는 “사이버 지하드(cyber jihad)”를 조직하여 미국에 대해 사이버 테러를 감행할 것이라고 선포했다(Robert Lemos, 2007: 1). 미국의 반응은 단호했다. 미국은 만약 그들이 사이버 공격을 가해 올 경우에는 이를 실제 물리적 공간에서의 선전포고로 간주하여 군사적으로도 보복할 것이라고 선언했다(James Middleton 2001: 1). 사이버 테러의 실전성과 엄중성을 잘 말해준다.

오늘날 누구에게나 간단한 장치와 조작으로 개방되어 있는 인터넷의 활용과 급속

한 보급은 사이버 공간에서의 상상하지 못하였던 역기능을 창출한 것이다. 인터넷은 전 세계를 사이버 공간이라는 하나의 가상적인 공간으로 묶어 놓고 그 속에서 지식의 정보교류는 물론이고 통신, 경제거래, 문화와 이념교류가 가능한 새로운 공동체 공간을 창출했다. 물론 거기에서도 각종 범죄활동이 전개되고 국가안보를 위태롭게 할 수도 있는 상황이 되었다. 따라서 사이버 공간은 21세기 미래형 전쟁인 사이버 전쟁의 위협을 제시하고 있다(박준석. 2014: 177-202).

국민과 영토와 주권을 보호한다는 전통적 의미에서의 국가안보는 이제 사이버 정보와 사이버 네트워크 보호까지를 포괄하지 않으면 국가안보 수호의 목표를 달성할 수 없게 그 영역이 새로운 과학기술 문명의 발전에 따른 신대륙으로 확대된 것이다. 이러한 과학기술 문화 그리고 정보혁명의 결과로 군사안보는 단순한 화력의 세기가 아니라 사이버 전쟁수행 역량이 결정적인 요소가 되었다. 그런데 이러한 위험성에도 불구하고 운영상의 효율성과 편리성, 국제교류 확대를 위해 국가기간망의 전산화·네트워크화는 확대되고 인터넷에의 의존도는 심화되고 있다.

특히 전 세계에서 가장 빠른 속도의 인터넷 기반시설을 구축하고 기술을 선도하는 우리의 경우에는 사이버 안보를 포괄한 사이버 안전의 문제는 그 어떤 나라보다도 절실하고도 중요하다고 하지 않을 수 없다(김두현, 안광호. 2010: 37-64).

그러나 우리의 법제도적 장치와 사이버 안전에 대한 인식의 수준은 현실을 잘 반영하지 못하고 있는 것으로 판단된다. 이에 본고는 변모하는 안보 환경에서 국가안보에 대한 무한책임기구인 국가정보기구의 사이버 안보에 대한 책무의 현실을 사이버 안전의 엄중성을 통해 성찰되도록 하는 우회적 분석과 더 나아가 필요한 사이버 정보활동과 유관활동의 필요범위를 검토하고자 한다. 당연한 전제로 사이버 테러와 전쟁을 포괄한 사이버 공격(Cyber Attack)에 대한 내용을 분석한다. 또한 사이버 세계의 전자기장을 물리적으로 장악하는 전자전도 사이버 안보와 연동되어야만 그 실전적 위험성을 더욱 알 수 있을 것이기 때문에 전자전에 대한 내용도 포함한다.

Ⅱ. 사이버 위협자

1. 사이버 위협의 실전성과 각국의 인식

1) 개관

오늘날 대부분의 주권국가들은 각종 사이버 공격으로부터 국가 핵심기반시설(Critical infrastructure: CI)을 보호하는 노력을 국가경영의 핵심 과제 가운데 하나로 설정하고 있다. 그에 대한 입법노력은 아무래도 미국 의회가 대표적이다(박노형, 2014. 4. 17). 국가 핵심기반시설(CI)은 국민생활에 불가피한 전기, 통신, 가스, 석유 및 석유 제품, 물 공급, 연료 등의 생산, 수송 및 유통시설, 공중보건 시설, 교통시스템(연료공급, 철도 네트워크, 공항, 항만, 내륙 운송), 금융 서비스, 보안 서비스(경찰, 군인)등을 지칭하는 것으로, 그들의 불작동 등 무능력화나 시설파괴는 공중의 건강과 안전 그리고 경제문제를 포함한 국가안보에 치명적인 위험성을 초래할 수 있는 시설 등의 실체를 말한다.

지면 제약상 본고의 본격적인 논의 범위는 아니지만 국가안보에 핵심적 위협을 초래할 수 있는 핵심 인프라와 관련된 사이버 안전의 취약성에 대한 논의와 사이버 위협으로부터 국가 네트워크를 보호하려는 노력, 민간영역과 공적 영역 사이의 사이버 위협정보의 공유를 비롯한 협력증진의 문제가 적지 않은 법적인 쟁점을 형성한다. 또한 국방 정책적으로는 사이버 안보는 궁극적으로 사이버전쟁을 대비하는 것으로서, 미 국방부 표준이론은 일정한 수준의 사이버 공격은 전통적인 물리적 전쟁개시를 가능하게 하는 정당전쟁론(*Casus belli*)을 합리화 하는 것으로 설정하고 있다(James Middleton 2001: 2).

2) 사이버 안전문제에 대한 각국의 현실적 전개

대표적으로 미국의 버락 오바마 행정부는 2009년에 국가 디지털 인프라는 국가가 반드시 지켜야할 전략적 국가자산(strategic national asset)이라고 확언했고, 2010년 5월 미국 사이버 사령부(U.S. Cyber Command: USCYBERCOM)를 창설했다(U.S. Department of Defense, Cyber Command Fact Sheet, 2010. 5. 21; 1). 초대 사령관은 알렉산더(Keith B. Alexander) 국가안보국(NSA) 국장을 겸임하도록 하여 사이버 전쟁

의 핵심이 정보 전쟁임을 보여주었다. 사령부의 목표는 미군의 네트워크는 철저하게 보호하고 침투국가의 그것을 강력하게 공격하는 것에 있다. 미국 정부 사이버 보안 전문가인 제임스 고슬러(James Gosler)는 현실적으로는 2만-3만 명이 필요한데 현재 약 1,000명의 유자격 사이버 전문가가 있을 뿐이라고 말했다. 2012년 1월 마이크 맥코넬 전 국가정보국장(DNI)은 그동안 많은 사이버 공격을 받기만 했지만 이제 다른 나라 컴퓨터 네트워크에 대한 공격을 시작했다고 밝혔다. 그는 나라를 특정하지는 않았지만 로이터 통신은 이란일 것으로 추측했고 2012년 6월 뉴욕 타임스는 버락 오바마 대통령이 이란 핵농축 시설에 대한 사이버 공격을 명령했다고 보도했다(Lynn, William J. III. 2010: 97).

한편 유럽연합(EU)은 유럽의 사이버 안전을 수호하기 위해 2004년 '유럽네트워크 및 정보보안청(ENISA: European Network and Information Security Agency)'을 창설했다. 미국 정보공동체는 러시아, 이스라엘, 북한이 최강의 사이버 전사를 목표로 하고 있고 이란은 현재도 세계 2위 규모의 사이버 군대를 보유하고 있는 것으로 파악한다(Clarke, Richard. Wall Street Journal. 2011).

그러나 사이버 공간에서의 가장 강력한 위협자는 사이버 무법자로 평가받는 중국이다. 이코노미스트는 중국은 21세기 정보전쟁의 최강자로의 등극을 목표로 하고 있는 나라라고 보도했다(The Economist. 2013). 2010년 8월 미국 정보공동체(IC)는 공개적으로 중국이 미국 회사와 행정부를 상대로 사이버 군사요원을 동원하여 공격하고 있음을 경고했고 펜타곤은 이를 확인했다. 밝혀진 바에 의하면 중국은 GhostNet(幽靈網, 유령망)이라는 전 세계 컴퓨터 스파이 네트워크를 설치하여 사이버 스파이 활동을 해왔다. 미국은 이를 2009년 3월 적발했다. 유령망 통제부는 중국에 위치했고 전 세계 약 103개 국가의 최고 보안이 설치된 정치적, 경제적, 언론 컴퓨터 네트워크에 지속적으로 침투했다. 각국 대사관, 총리, 대통령 관저, 인도, 런던, 뉴욕의 달라이 라마 센터도 침투 대상이었다고 한다. 한편 펜타곤은 중국 인민해방군(The People's Liberation Army)의 정보전 부대(Information warfare units)는 경쟁세력 컴퓨터와 네트워크에 침투하기 위한 바이러스를 끊임없이 개발하고 있다고 확인했다.

이러한 상황에서 오늘날 사이버 세계에서의 공격이 바로 사이버 전쟁으로 이어질 수 있는 것은 시간문제이다. 이에 미 국방부는 사이버 공격을 결정적인 국가안보위협으로 판단한다. 2010년 국방부 합동사령부의 다음 표현이 잘 말해준다;

"사이버 공간에의 기술이 제반 힘의 원천이자 수단이 되고 있다. 또한 적대세력도

손쉽게 획득할 수 있는 힘이 되어 그들은 통신과 정보의 흐름을 공격하고, 저감시키며, 교란시킨다. 낮은 진입장벽과 어렵지 않은 기술적 조작으로 인해서 오늘날 사이버 세계에서의 적대세력은 매우 다양하고 방대하다. 게다가 사이버 영역의 무한성과 국경의 부존재는 기존 법률체계를 무의미하게 하고 그 대응에 매우 어려움을 초래한다."(United States Joint Forces Command: USJFCOM).

이처럼 인터넷에 의해 제기되는 안보위협은 생각보다 가깝고 훨씬 위중하다. 적은 투자와 익명성은 국가이익을 위협하는 끊임없는 적대세력을 양산한다. 이에 상대세력과의 충돌이 발생하면 사이버 공간이 정규·비정규 전쟁의 주요 전장터가 될 것임은 명백하다. 사이버 세계에서의 적대세력은 국가와 비국가 주체를 망라하고 아마추어 수준의 해커와 고도의 훈련된 해커를 포함한다. 그들은 산업, 연구소, 정부 그리고 육·해·공과 우주의 영역을 망라하여 활동한다. 제2차 세계대전에서 공군력이 전장을 압도했던 것처럼, 사이버 세계는 물리적인 공격의 한계를 간단히 제거해 주었다. 그들은 흉포한 테러를 손쉽게 자행할 수 있을 뿐만이 아니라 주권국가의 일반시민과 정책당국의 인식과 의지에도 직접적인 영향을 미친다. 이 같은 사이버 위협(Cyberthreats)을 초래하는 대표적인 활동유형을 가장 권위 있는 자료로 인정받는 의회 보고서는 다음과 같이 구분한다(CRS Report R41927: 3).

2. 사이버 위협 행위자의 분류

1) 사이버 해커(Cyberhacktivists)

해킹(hacking)은 전자회로나 컴퓨터 하드웨어, 소프트웨어, 네트워크, 웹사이트 등의 정보체계가 설계자, 관리자, 운영자가 의도하지 않은 동작을 일으키도록 하거나 주어진 권한 이상으로 정보를 열람, 복제, 변경하는 행위를 광범위하게 이르는 말로 해킹을 하는 사람을 해커라고 한다. 사이버 위협인자로 분류하는 사이버 해커는 오락이나 성취감 등 개인적 욕구, 철학적 동기 등 비금전적인 이유로 사이버 공격을 실행해 보는 개인이나 단체를 의미한다. 정보통신망 이용촉진 및 정보보호 등에 관한 법률은 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 "침해사고"라고 개념 정의하여 해킹을 침해사고의 한 가지 원인으로 나열하고 있다(정보통신망 이용촉진 및 정보보호 등에 관한 법률, 제2조 7호).

2) 사이버 절도(Cyberthieves)

사이버 절도는 금전적인 목적으로 불법적인 사이버 공격을 하는 개인이나 조직을 말한다. 일반인을 상대로 전화로 유인하여 송금하게 하는 금융사기를 포함하여 신용카드 정보를 악용하여 금융계좌에 접근하여 1회적 금원탈취나 지속적으로 예금을 인출하는 행위 등이 대표적인 사이버 절도이다. 사이버 절도는 상대적으로 낮은 위험부담으로 매우 높은 이득을 얻을 수 있는 활동으로 글로벌 사이버 절도 피해는 매년 수백억 달러에 달할 것으로 추산된다(CRS Report 97-1025, Charles Doyle; CRS Report R41927, Kristin Finklea).

3) 사이버 스파이(Cyberspies)

사이버 스파이는 사이버 영역에서 경쟁전략, 보안정보, 재정과 금융정보 또는 정치적 이익을 목적으로 정부나 사기업체가 보유하거나 사용하는 비밀정보와 독점정보를 수집하는 사람이나 행위를 말한다. 사이버 스파이는 사기업체 뿐만이 아니라 외국정부를 위하여 일하기도 한다. 2011년 FBI 보고서는 미국의 어떤 기업은 하룻밤만에 그 회사가 10년 동안 연구개발한 약 10억 달러의 가치가 있는 기술정보를 침탈당했다"고 지적했다(Shawn Henry, 2011). 미국 정보공동체(IC)는 미국은 많은 나라 산업 사이버 스파이들의 목표로 그들의 활동은 미국의 경제 경쟁력을 위협한다고 밝혔다(Ellen Nakashima, 2013). 그들 나라에는 러시아, 이스라엘, 프랑스도 있는데 그들 나라의 사이버 산업스파이 활동은 중국의 저돌적인 대쉬에 비하면 초라하다고 지적한다.

4) 사이버 테러리스트(Cyberterrorists)

국가나 비국가 후원의 행위자로 전쟁 유사의 양식으로 사이버 공격을 감행하는 세력을 의미한다. 오늘날 기왕의 국제테러조직이나, 반란세력 그리고 이슬람 근본원리를 주창하는 지하디스트(jihadists)들은 인터넷을 공격기획, 과격 선동, 테러리스트 충원, 선전과 선동의 창구 그리고 통신의 통로로 활용한다(CRS Report RL 33123, John W. Rollins & Clay Wilson). 물론 이론적으로는 후술하는 바와 같이 사이버 테러는 정책변경이 목적이고 사이버 전쟁은 국가전복 목적으로 양자가 구분되기는 한다(한희원, 2011: 791).

5) 사이버 전사(Cyberwarriors)

사이버 전사 또는 사이버 군인은 특정한 국가의 군사전략 목적을 수행하거나 지원하기 위한 주권국가의 행위자 또는 준행위자(대리인)를 의미한다(CRS Report RL31787, Catherine A. Theohary). 금전적 이득이나 정책변경 목적이 아니라 파괴나 괴멸 목적으로 진행된다. 예컨대 2012년 8월 정체불명의 세력으로부터 전 세계 최대 원유와 가스 생산업체인 사우디 아마코사(Saudi Aramco)에 대한 사이버 공격이 자행되었다. 사이버 공격은 회사의 3만대 컴퓨터에 대해 일제히 진행되었고 목적은 시설파괴와 원유생산을 중단시키는 것이었다. 사이버 안보 전문가들은 이란이 자행한 것으로 추정했다(Wael Mahdi, 2012). 물론 회사 내부자 소행일 수도 있다는 반론도 있다(Michael Riley & Eric Engleman, 2012). 이러한 모든 것을 포함한 사이버 안보에 대한 국가정보기구의 임무와 책무범위를 설정하는 것은 대단히 실천적인 문제로 매우 중요하다고 하지 않을 수 없다.

그 목적과 방향성은 국가안보 전문가인 클레이 윌슨(Clay Wilson)이 의회에 제출한 2006년 보고서에 잘 나타나 있다. 미 국방부가 보고서를 의회에 제출한 목적은 의회로 하여금 ① 사이버 무기를 국제회의에서 무기통제, 즉 군축대상으로 설정할 것인지에 대한 입법정책 판단, ② 사이버 공격자의 추적과 처벌을 용이하게 하기 위한 사이버 관련 형사처벌 법안에 대한 입법자료 제공, ③ 국내에도 영향을 끼칠 수 있는 사이버 심리공작 활동에 대한 불가피성과 영향력을 국민의 대표인 의회에 설명하여 사전이해 구하기, ④ 개개인이 보유하고 있는 국가적으로 중대한 사적 컴퓨터 인프라에 대한 컴퓨터 보안을 촉진하기 위한 규제 장치의 준비 등과 같은 현안 문제에 대한 대책을 강구하도록 하는 데 있었다(Clay Wilson, 2006).

3. 소결어 – 사이버 위협의 복합적 효과

사이버 위협의 개념만 이해해도 2013년 대한민국을 질곡 시켰던 소위 국정원이나 사이버 사령부의 댓글 사건 논란이 얼마나 허망한 것인지를 잘 알게 해 준다. 한편 개념적으로는 구분되는 다양한 사이버 위협세력들은 당연히 고립된 절연체가 아니고 복합성을 가질 수 있다. 현실적인 위협은 대개 복합적이다. 예컨대 어떤 기업의 지적재산권을 목표로 하는 사이버 해커는 사이버 절도범이나 사이버 스파이로 개념정의될 수 있다. 또한 만약 그 행위가 군 관련 조직이나 단체에서 이루어진 것이라면 사이버 전사의 활동에도 포섭될 수 있다(Mandiant. 2013: 7).

Ⅲ. 사이버 정보와 사이버 공격(Cyber Attack)

1. 사이버 정보와 사이버 공격

사이버 정보는 사이버 공간(cyber space)에서 생성되고 수집되는 정보를 말한다. 사이버 정보는 통상 두 가지 방법으로 수집된다. 첫 번째는 사이버 공간상에서 발생하는 각종 현상적인 데이터에서 자동적으로 무한정의 자료축적을 하고 그중에서 가치 있고 의미 있는 내용을 정보로 추출하는 것이다. 두 번째는 광범위하게 축적된 자료를 슈퍼컴퓨터 등 별도의 분류장치를 통해서 활용방안과 방향을 특정한 지시를 전자적으로 시달하면, 기왕의 다른 정보들과 함께 종합적으로 체계화되어 해석과 분석을 통해 원하는 방향과 내용으로의 새로운 정보가 자동적으로 생성되게 하는 것으로 소위 데이터 마이닝(data mining)이다(한희원, 2011: 791). 그런데 사이버 정보는 사이버 공간에서 획득한 단순한 지식이라는 이상의 커다란 가치를 가진다. 사이버 정보는 일반정보들과 조화하여 일반정보의 능률을 극대화할 수 있으며, 상대세력에 대해 자동적으로 정보우위를 점할 수 있게 해주기도 한다. 이러한 연유 등으로 각국은 사이버상의 정보는 그 자체가 별도의 특별한 고유 가치를 창출하는 국익의 새로운 영역이라고 인정하는 데 주저하지 않는다. 그러므로 사이버 정보는 매우 중요한 국가자산이면서 전쟁무기이다.

사이버 공간에서의 위협과 위해(危害)를 야기하는 각종 범죄나 테러위협 그리고 국가 간의 전쟁을 표현하는 용어는 다양하다. 현재 사이버 공간에서의 여러 가지 공격을 표현하는 용어로는 사이버 테러(Cyber terrorism)라는 용어가 역설적으로 그 친근감으로 인하여 가장 널리 사용되고 있다. 한편 국가안보적인 면을 강조하는 군사적 측면과 입법부 등 전문 영역 부문에서는 정보공작 또는 정보작전(Information Operation)과 사이버 전쟁(Cyberwar 또는 Cyber warfare)이라는 용어를 사용한다(Clay Wilson, 2006. 9. 14: 6). 또한 정보전쟁, 네트워크 전쟁, 인공두뇌전쟁(Cybernetic war) 등으로도 불린다. 이들은 주로 인터넷 등 전자적 통신망을 활용하고 전자기장을 이용하는 공격행위라는 점에서 공통점이 있다. 사이버 공간에서의 이러한 행위들은 결국 상대방 컴퓨터 네트워크를 무력화 또는 파괴시키고 기능을 마비시키며, 추적 등 정보활동을 저해하는 행위로서 이들은 포괄적으로 모두 사이버 공격(Cyber Attack)이라고 할 수 있다(Clay Wilson, 2006: 7).

한편 사이버 공간은 물론이고 현실의 물리적인 세계에서 전자장치를 사용하여 전자기장에 대한 공격으로 감행되는 전자전쟁도, 사이버 공격의 범주에서 함께 이해하는 것이 보통이다. 그러므로 용어의 혼선을 피하고 통일을 위해 사이버 테러와 사이버 공작활동을 포함한 사이버 전쟁 그리고 전자전쟁의 3가지를 포괄하는 용어로 사이버 공격(Cyber Attack)이라는 용어를 상정한다.

단순한 개념 구분으로 사이버 테러는 사이버 공간에서의 물리적 테러공격, 사이버 전쟁은 정부 전복이나 국가소멸을 목적으로 사이버 공간에서 전개하는 전쟁을 말한다. 사이버 진주만 공습, 사이버 제3차 세계대전 등을 예상할 수 있으며 실전적인 전쟁에 못지않은 규모와 피해로 전개될 수 있다. 한편 사이버 공간이 아닌 일상생활 공간에서 사용되는 전자장비에 대한 공격은 이를 전자전쟁(Electronic Warfare : EW)이라고 지칭한다. 한편 사이버 전쟁은 필연적으로 사이버 공간상에서의 제반 정보활동을 요구한다. 그것이 사이버 정보활동 또는 사이버 정보공작(Information Operation)이다. 그러므로 사이버 공격에서 살펴볼 내용은 사이버 테러와 정보공작 그리고 전자전쟁의 3가지가 된다(한희원, 2011: 801).

2. 사이버 테러(Cyber Terror)

1) 사이버 테러의 의의

테러는 일반인에게 공포심을 조성해 어느 나라나 국제기구로 하여금 부당하게 어떤 행동을 하게 하거나 또는 어떤 행동을 하지 못하게 하려는 의도에서 자행되는 불법적인 공격행위이다. 사이버 테러는 상대방의 정책목표를 수정하게 하고 그들의 정치적 목적을 달성하기 위해 사이버 공간을 통해서 목표시설과 정보기술에 영향을 미쳐 물리적으로 대규모 손해나 붕괴를 야기함으로써 공포심을 조성하는 것이 주된 목적이다. 오늘날 인터넷이 공동체 생활의 거의 모든 영역에서 활용됨으로 인하여 개인·단체 등은 사이버 공간에서 익명과 간단한 클릭의 손동작만으로 시민들, 특정 소수그룹이나 신념을 가진 단체, 공동체 그리고 많은 나라를 위협할 수 있게 되었다. 약 3,000명의 목숨을 앗아간 2001년 미국의 9/11 테러 공격에서 보았듯이 현실적인 물리적 테러공격의 수법은 상상을 초월하며 피해는 또한 엄청나다(Park, Dong-Kyun, 2010, 65-90). 그러나 현실세계에서의 물리적인 테러공격은 공격수단의 밀행성에 따른 공격규모의 제약과 목표물의 한정성이라는 성격, 즉 공격에 있어서의 규모의 경

제라는 원칙에 따라서 어느 한 국가를 전복하거나 괴멸시키는 데에는 한계가 있다(한희원, 2011: 678). 그러나 사이버 테러공격은 그러한 물리적 테러의 한정성의 제약을 받지 않고 정치적 목적 달성 이상의 국가소멸·국가전복 목적으로도 자행될 수도 있고, 실제로 재래식 무기 등에 의한 전쟁을 넘어서는 국가기간망 전체에 대한 손해를 야기해 국가의 존망을 위협하고, 심리적 선동 등으로 정부전복을 도모할 수 있는 충분한 위험수준까지 올라가 있다. 물론 이 단계는 이미 사이버 전쟁단계라고 할 수 있는 것으로, 공포심 유발을 통해 정책변경을 유도할 목적인 사이버 테러와, 국가소멸과 정부전복 목적의 사이버 전쟁(Cyberwar)을 구분해야 한다는 견해도 있고, 또한 국제법적인 제반 규율의 관점에서는 그렇게 사용할 필요는 있다(Clay Wilson, 2006: 11). 그러나 이해의 편의를 위한 구분에도 불구하고 사이버 공간상에서의 공격방법에 있어서는 사이버 테러와 사이버 전쟁에 명확한 차이를 두기가 현실적으로 곤란한 것도 사실이다.

오늘날 사이버 테러는 그 잠재적 대량 피해의 가능성만으로도 그리고 사이버 전쟁으로 비화될 수 있다는 위험성으로 가장 쉽게 접할 수 있으면서도 중요한 사이버 공격의 대표적 내용이 되었다. 현재 미국은 2001년 알카에다 조직에 의한 9/11 테러공격 이후 또 다른 잠재적 가능성이 높은 테러공격 방법으로 사이버 테러공격을 손꼽는 데 주저하지 않는다. 미국은 미국에 적대적인 국제테러조직이 컴퓨터 네트워크를 이용해 국가기간 시설망에 대한 사이버 공격을 감행해 원자력 발전소 등의 오작동으로 방사선 누출을 야기하거나, 또는 원자력 발전소 자체의 폭발을 야기한다거나, 가스유출, 발전장치 손상, 열차선로의 충돌 야기, 항공제어 시스템의 오작동으로 국가기간 시설 망에 엄청난 손상과 파괴를 초래하거나, 컴퓨터 시스템의 오작동을 야기하여 국가경제에 대혼란을 초래하는 등으로 미국에 크나큰 위해(危害)를 가할 개연성을 가장 위험스러운 테러공격에 의한 피해로 예측하고 있다(Michael A Vatis, 2001: 9).

2) 사이버 테러의 유형

(1) 사이버 테러 개관

사이버 공간에서의 공격수법과 기술은 실제 대응기술보다 항상 한발 앞서서 발달해 간다. 그만큼 기술진보가 빠르고 실시간적 대응이 어렵다는 것을 뜻한다. 사이버 공격에 사용되는 무기를 사이버 무기(Cyberweapons)라고 한다. 현재 사이버 무기는

상당한 정도로 개발되어 있고, 지속적으로 개발될 것으로 예상된다. 사이버 무기들은 적극적 공격 무기로는 각종 컴퓨터 바이러스 외에 시스템 하드웨어 설계 시에 칩 속에 고의로 특정한 코드를 입력시켜 시스템을 공격하게 하는 치핑(Chipping), 컴퓨터에 은밀하게 침투시켜 시한폭탄처럼 때가 되면 시스템을 공격하여 파괴시키는 논리폭탄(Logic Bomb), 프로그램 속에 숨어 있다가 프로그램이 실행될 때 활성화되어 데이터를 공격하는 트로이 목마(Trojan Horse), 컴퓨터가 도저히 감당할 수 없는 양의 메일을 지속적이고 대량으로 발송하여 상대방 컴퓨터를 다운시키거나 완전히 파괴시키는 악성 프로그램 등이 있다. 공격과 방어 겸용의 장치로는 네트워크 감시 장치나 특수 스캐너가 있다. 방어무기로는 방화벽과 암호장치 등이 있다. 한편 사이버 전쟁은 다양한 사이버 무기와 전자전쟁 무기를 사용해 상대방의 컴퓨터와 컴퓨터 네트워크 및 전자기장에 타격을 가하는 일련의 행위들이다. 사이버 무기를 이용한 사이버 테러 공격에는 다양한 방법이 있는바 대표적으로 다음의 6가지 방법이 있다. 물론 이들 방법들은 사이버 전쟁에서도 동일하게 사용될 수도 있고, 역으로 사이버 전쟁에서의 조직적이고 체계적인 방법이 사이버 테러에서도 응용될 수 있음은 물론이다. 그러므로 어떠한 것이 정치적 목적 등을 달성하기 위한 사이버 테러이고 어떠한 공격이 국가전복과 파멸을 목적으로 하는 사이버 전쟁이 될 것인지에 대한 전개과정을 국가정보기구가 주목해야 하는 이유이다. 사이버 공간에서는 상상의 한계가 없음을 말해 주는 것이다.

(2) **사이버 테러의 수법**

① 웹 반달리즘(Web vandalism)

초보적 공격 유형으로 웹 페이지를 손상하거나 속도를 저감하는 등의 방법으로 실제 컴퓨터 네트워크에 대한 운용상의 손해로까지는 연결시키지 않는 공격을 말한다. 추후에 강도 높은 공격을 예상할 수 있는 암시가 되기도 한다. 컴퓨터 바이러스(Virus)와 웜(Worm) 등이 사용되는데 컴퓨터 바이러스는 자기 복제능력과 함께 전산 프로그램에 변형물을 감염시켜 기생하는 자가 번식능력을 가지는 수법이 동원된다. 한편 웜은 네트워크를 통하여 자동적으로 자가 복제하여 전파하면서 네트워크의 속도를 저감시킨다(Hicks, Jesse. 2014).

② 사이버 선전(Cyber Propaganda)

사이버 공간에서의 여론조작 또는 새로운 허위 여론을 형성하는 것으로 인터넷을

통한 심리공작이다. 상대국의 정책결정권자로 하여금 강경한 노선을 포기하게 하거나 외국과의 동맹관계에 균열을 초래하게 하는 등 사이버 선전 효과는 상상 외로 지대하다. 예컨대 이라크 전쟁에서 미군은 인터넷을 통하여 후세인의 사망설을 끊임없이 유포하여 이라크 군의 사기를 꺾는 심리전 공격을 지속적으로 실행해 큰 효과를 보았던 것으로서 사이버 심리전은 첨단무기보다 더욱 무서운 힘을 발휘할 수 있다. 사이버 선전은 상대방에 대한 심리적 와해뿐만 아니라 전쟁의 정당성을 옹호하기도 하고, 우호자 등 지원세력의 지지를 위해 적국은 물론 자국민의 여론과 제3국의 지지를 얻기 위한 심리전으로 확대시킬 수도 있다(The World. 2013: 21).

③ 비인가 접근과 데이터 수집(Gathering data)

사이버 공간에서의 스파이 활동으로 보안장치가 취약한 곳에 침투하여 정보를 수집하거나 상대방의 정보를 새롭게 각색하여 몰래 가공해 놓는 것이다. 비인가 접근과 데이터 수집은 네트워크, 전산시스템, 전산자료 등에 인가를 받지 않은 채, 또는 인가권한을 초과하여 논리적 또는 물리적으로 불법 접근해 자료를 획득하는 제반 행위를 말한다. 불법접근 행위를 전문용어로 크래킹(cracking)이라 칭하는데 해킹의 한 유형이라고 할 수 있다. 비인가 접근은 패스워드를 불법으로 알아내어 접속하거나 보안 취약점을 찾아내어 접속하는 방식으로 이루어지기도 하지만 개발업체의 협조를 받거나 개발업체 스스로가 프로그램 자체에 비밀 접근 코드를 설치한 후 사후에 자동적으로 접근하는 방식이 많이 이루어진다. 그것을 백 도어(backdoor) 또는 트랩도어라고 한다(Sterling, Bruce. 1993: 61).

실례는 미국을 상대로 한 사이버 상에서의 정보획득을 시도하고 미국의 방위 능력 시험을 위해 2003년 이래 미국항공우주국(NASA), 록히드 마틴, 국립 연구소 등의 미국 컴퓨터 망에 지속적으로 침투하려는 조직적·대규모 시도가 있었다. 미국 당국은 그에 대한 방첩공작 활동을 타이탄 레인(Titan Rain)이라고 명명하여 일단은 효과적으로 제어했던 것으로 알려지고 있다(Graham, B. 2005). 미국은 이것을 조직적인 중국 해커부대의 소행으로 보고 있다. 한편 1999년 러시아의 컴퓨터 망으로 추정되는 곳으로부터의 미국 보안 컴퓨터 시스템에의 지속적 침투시도인 소위 "달빛 미로(Moonlight Maze)"도 대표적인 사이버 비인가 접근 중의 하나였다(Bob Drogin, 1999).

④ 서비스 거부공격(Denial-of-Service Attacks : DoS)

서비스 정지공격(停止攻擊), 불능공격(不能攻擊) 또는 방해공격(妨害攻擊) 등으로

도 지칭된다. 컴퓨터 시스템을 파괴하지 않고 소비자가 컴퓨터를 이용할 수 없게 만드는 공격을 말한다. 예를 들어 네트워크 또는 전산 시스템에 과도한 부하가 걸리게 하여 정상적인 정보통신 서비스를 제공할 수 없게 하거나 서비스 제공 성능을 급격하게 저감시키는 것을 말한다. 공격 팀이 대규모의 원격조정 컴퓨터 망을 사전에 구축하여 특정기관 특정 서비스 네트워크에 동시에 접속함으로써 타깃이 된 컴퓨터 서비스를 마비시키는 수법이다. 2000년 2월 세계 컴퓨터 마니아들이 인터넷 서비스 업체인 야후(Yahoo)와 온라인 쇼핑 업체인 이베이(E-Bay)에 대한 분산공격으로 서비스가 중단된 사례가 대표적인 서비스 거부공격이다(Kumar, S. 2010: 88-80).

⑤ 시스템 파괴(Equipment disruption)

악성코드 등을 사용하여 목표 전산시스템 자체를 아예 파괴하는 것을 말한다. 시스템 파괴 테러는 대상국가 국가핵심기간시설(CI) 공격으로 전개될 수도 있다. 이것은 대상 컴퓨터나 컴퓨터 시스템 침투를 넘어선 사이버 파괴 공격으로 대상국가의 발전소 운용체계, 물과 전력 공급체계, 행정 서비스 공급망, 통신시스템, 운송시스템, 금융시스템 등 국가 기간시설에 대한 운용상의 장애를 초래하여 국가의 제반 서비스 활동을 마비시키는 컴퓨터 공격을 말한다. 병행하여 후술하는 전자전쟁에서 보는 바와 같이 전자폭탄, 전자총 등을 사용해 컴퓨터와 컴퓨터 통신망을 직접 대상으로 파괴공격을 감행할 수도 있다(Clay Wilson, 2006: 7).

3) 사이버 테러의 실례와 대책

가장 최근의 국가에 대한 의도적인 컴퓨터 공격은 에스토니아(Estonia) 공화국에 대한 사이버 공격이 있었다. 그것은 2007년 4월 27일부터 시작하여 5월 17일까지 에스토니아 국회, 수상 관저, 은행 그리고 언론사의 컴퓨터 망을 대상으로 한 광범위한 공격이었다(Ian Traynor, 2007: Russia accused of unleashing cyberwar to disable E). 사이버 공격에는 일반시민들이 자동차 렌탈 등 각종 서비스 이용을 못하게 하는 서비스 거부 공격과 정치적 목적의 선전활동도 병행되었다. 당시 에스토니아 정부가 할 수 있었던 것은 더 커다란 네트워크상의 피해를 방지하기 위해 컴퓨터 시스템을 다운시켜 놓는 것뿐이었다(Larry Greenemeier, 2007). 사이버 공격은 러시아가 직접 실행했던 것으로 알려졌다. 2007년 6월 25일 에스토니아 대통령 헨드릭 일베스(Toomas Hendrik Ilves)는 부시 대통령과 만나 에스토니아 국가기간시설 망에 대한

복구와, 컴퓨터 공격에 대비한 보안 지원을 요청했고, 자국의 문제를 국제사회의 의제로 삼아 줄 것을 요청했다(White House. 2007; The Economist. 2010). 에스토니아 공화국에 대한 사이버 공격은 군 관계자들에게는 커다란 심각성을 안겨 주었다. 이에 2007년 6월 14일 북대서양조약기구(NATO) 회원국 정상들이 브뤼셀에서 만나 대책회의를 가졌고 사이버 안보 국제기구를 창설했다.

3. 사이버 전쟁(cyberwarfare)

1) 사이버 테러와의 개념 구분

사이버 전쟁은 사이버 공간에서 벌이는 일련의 전쟁을 말한다. 국가안보 전문가 클락은 "사이버전이란 어떤 국가가 손상이나 파괴를 목적으로 다른 국가의 컴퓨터나 네트워크에 침투하는 행위라고 정의했다(Richard A. Clarke. 2010). 정치적 의도를 관철하기 위해 공포와 혼란을 초래하려는 사이버 테러의 범위를 넘어서서 실제로 정부를 전복하려고 하거나 어느 한 국가를 궤멸시키려는 의도 아래에서 시도되는 사이버 전쟁은 그 심각성이 사이버 테러와 또 다르다. 그러므로 그러한 사이버 전쟁에 대응하기 위한 사이버 정보활동은 단순하게 사이버 공간이라는 공개출처자료에서의 정보를 수집하는 공개출처 정보수집 활동의 문제가 아니라 사이버 전쟁에 대비한 실전적인 정보활동이 되어야 한다. 이에 미국 국방부는 그것을 정보공작과 사이버 전쟁(Information Operation & Cyberwar)이라고 불가분적으로 호칭하기도 한다(Clay Wilson, 2006: 7). 사이버 전쟁은 직접적으로 국가 전복을 목적으로 한 전쟁수행이라는 관점에서 그에 대한 명백한 개념정립과 전쟁수행 능력에 대한 체계적인 이해는 21세기 사이버 전쟁을 대비하는 국가입장에서는 순수한 사이버 치안의 역량만으로는 달성할 수 없는 새로운 과제를 제시한다.

사실 사이버 전쟁은 재래식 무기에 의한 전쟁이나 테러에 비해 매우 저렴한 비용으로 큰 효과를 거둘 수 있다. 현재 이란, 북한, 중국, 러시아 등은 상당한 수준의 사이버 전쟁 부대를 운용중인 것으로 알려지고 있다. 미국은 세계 최강의 신호정보 전담기구인 국가안보국(NSA) 등 각종 기술정보 수집 정보기구를 병유하고 있는 국방부가 사이버 전쟁에 대한 책임을 담당하고 있다. 그에 따라서 미국 국방부는 "글로벌 네트워크 공작을 위한 합동특별대책본부(Joint Task Force-Global Network Operations : JTF-GNO)"를 운용하고 있다(Peter Brookes, 2005).

현재의 정보혁명의 추세는 국제관계의 역학 결정이 어느 나라가 정보의 우위를 점하느냐에 따라서 좌우될 것이라고 함에 이론이 없다. 즉 정보혁명은 정보 그 자체를 새로운 왕국으로 만들어 국제관계의 중요한 상품이자 무기가 되게 한 것이다(Clay Wilson, 2006: 1). 사이버 전쟁은 마치 과거에 군사력의 사용과 위협이 국제체제에서 중심적인 힘의 원천이었던 것과 마찬가지이다. 전통적으로 군사력의 비교 기준이었던 병력 수와, 화력의 크기와 양의 비교가 무의미해진다. 정보화에 힘입은 군사혁명은 단순한 미사일 수의 비교보다는 누가 우수한 전자적인 정보작전 수행능력을 가졌는가가 더 중요해졌다는 점을 의미한다. 고도의 사이버 공작 기술과 능력만 갖춘다면 미래의 전쟁은 더 이상 화력이 우세한 현재의 강대국들의 전유물이 절대로 아니고, 기술적으로 우위를 갖춘 나라가 얼마든지 세계 역학질서의 중심역할을 할 수 있다는 것을 의미하는 것이다(Clay Wilson, 2006: 3).

2) 사이버 전쟁의 핵심 능력

(1) 사이버 심리공작(Psychological Operations : PSYOP)

사이버 심리공작은 상대방 국민들의 감정 등 여론과 궁극적으로는 상대방 정부, 조직 그리고 개인의 행동에 영향을 끼칠 목적으로 의도된 정보를 사이버 공간을 통해서 다양한 방법으로 상대방에 전달하는 것을 말한다. 예를 들면 미국은 2003년 이라크 전쟁에서 공군과 걸프 만에 정박 중이던 해군 함정에서 이메일, 팩스, 휴대전화 등을 통해 이라크 정치·종교 지도자·군 지휘관을 포함한 이라크의 수많은 정책결정자들과 오피니언 리더들에게, 더 이상 정상적이지 아니한 사담 후세인 대통령을 지지하지 말라는 정치 메시지를 지속적으로 대량 발송하여 이라크 정부 내에 심각한 내부동요를 야기했다. 사이버 심리전은 원칙적으로 상대방이 대상이다. 원칙적이라는 의미는 사이버 심리전은 일단 방송을 함과 동시에 전파적 통제가 불가능하기 때문에 정보소비자를 제한할 방법이 없다는 의미에서이다. 소위 역류 현상이다. 군사전문가들은 미래의 전쟁은 정부 등 공식적인 조직의 의지가 아니라 대중의 심리에 의해 좌우될 것이라고 한다. 이러한 관점에서 사이버 심리전은 더욱 활용될 것이 명백하다. 사이버 심리전 능력은 사이버 전쟁 역량 중에서 해외정보를 직접 취급함으로써 현지 사정에 능통한 국가정보기구가 직접 수행해야 할 부분이다(Joint Chiefs of Staff. 2007: 2).

(2) **군사기망작전**(Military Deception : MILDEC)

군사기망작전(MILDEC)은 상대세력으로 하여금 그들의 군사능력과 의도를 포함하여 군 정책을 수행함에 있어서 오판을 하게 해, 특정한 행동을 하거나 또는 필요한 대책을 강구하지 못하게 함으로써 아국의 군사작전을 성공적으로 수행하기 위한 제반 행위를 말한다. 잘못된 정보와 허위영상, 허위·과장연설 등 사이버 영역에서의 가상적인 기망작전으로 적국으로 하여금 결정적인 오판을 유도해 군사작전을 성공적으로 수행하는 것이다. 예를 들면 2003년 이라크 전쟁에서 미국은 실제 전투현장에 대한 이라크의 방어와 공격을 방해하기 위해 이라크의 레이더에 포착되게 가상의 비행공격편대 공습을 만들어, 즉 허위영상을 유도하여 이라크 군이 그곳에 집중하도록, 즉 오판공격하게 만듦으로써 실제 미국의 전투 현장에는 아무런 피해 없이 성공적으로 작전을 수행할 수 있었다(Latimer. 2001: 6-14).

(3) **작전보안**(Operational Security : OPSEC)

작전보안은 통상적으로는 비밀정보는 아니지만 상대방으로 하여금 아국의 작전상 취약점을 유추할 수 있는 좋은 자료가 될 사이버 상에서의 공개정보를 유사시에는 이용하지 못하도록 삭제하는 등의 통제를 말한다. 그러므로 역으로 작전보안은 상대세력이 평소 무엇에 관심을 가지고 있는지에 대한 평상시의 끊임없는 정보파악 활동이 긴요함을 일깨워 주는 것이다. 예를 들면 2003년 이라크 전쟁에서 미군은 이라크 군 당국의 군사적 사용을 방지하기 위해 국방부 웹사이트의 정보자료 중에서 평상시에는 공개되어 누구나 일반적으로 이용하던 민감한 내용의 정보를 모두 삭제했다. 이라크 정보당국 등이 실제 전투에서 활용하면 미군 측에 타격을 줄 수 있는 것으로 판단한 내용들이었다(Clay Wilson, 2006: 1-2).

(4) **컴퓨터 네트워크 공작**(Computer Network Operations: CNO)

컴퓨터 네트워크 공작은 상대세력의 컴퓨터 네트워크를 공격하거나 붕괴하는 것, 아국의 군사정보 시스템을 보호하는 것, 일반적 정보수집 활동을 포함한 제반 정보수집기법을 동원하여 상대세력 컴퓨터 네트워크를 역(逆) 이용하는 것을 모두 포함한다. 그것은 첫째, 컴퓨터 네트워크 방위(Computer Network Defense: CND), 둘째, 컴퓨터 네트워크 착취(Computer Network Exploitation: CNE), 셋째, 컴퓨터 네트워크 공격(Computer Network Attack : CNA)의 3가지로 나뉜다.

미 국방부 보고서에 따르면 미국은 21세기 최첨단 특수부대로 “네트워크 전쟁을 위한 기능적 합동부대(Joint Functional Component Command for Network Warfare : JFCCNW)”를 창설하여 운용 중이라고 한다(Clay Wilson: 4). 동 부대는 정규군 조직으로 사이버 전쟁을 목적으로 창설되었지만 구체적인 임무는 비밀 분류되어 있다. 군 관계자들에 따르면 막강한 사이버 전쟁을 수행할 능력을 갖추고 있음은 틀림없지만 어떤 경우에도 선제적 사이버 공격을 하지는 않는다고 한다. 많은 컴퓨터 보안전문가들도 미국의 네트워크 전쟁을 위한 기능적 합동부대는 상대세력의 네트워크를 궤멸할 수도 있고 적국의 컴퓨터와 네트워크에 침입해 정보를 절취하거나 조작해 정보를 새롭게 임의적으로 배치하거나 지휘통제 시스템을 붕괴시킬 수 있는 역량이 있다고 판단한다(U.S Joint Publication. 2013: 3-13).

3. 전자전쟁(Electronic Warfare : EW)

1) 전자전쟁의 의의

전자전쟁은 상대방의 컴퓨터와 컴퓨터 네트워크 그리고 반도체 등의 전자부품에 대해 전자기장 에너지(electromagnetic spectrum energy)를 방출하는 전자폭탄과 전자총 등의 전자무기를 사용하여 전개하는 공격행위이다. 통상 광의의 사이버 전쟁의 일환으로 일컬어지기도 하지만 사이버 전쟁이 사이버 공간에서의 전쟁을 말한다면 전자전쟁은 사이버 공간 이외의 실제 사회생활 공간에서도 전개된다는 점에서 차이가 있다.

전자전쟁은 전자기기를 사용하는 모든 물체를 상대로 전자무기를 사용해 전자회로에 오작동을 초래함으로써 재래식 전쟁과 같은 대량 살상은 피하면서도 국가의 기능마비 등 더욱 커다란 손해를 초래하는 신개념의 전쟁이다. 예컨대 고준위 전자기 에너지를 사용하여 상대세력의 컴퓨터, 라디오, 전화 등 통신장치 그리고 트랜지스터나 반도체 등을 사용하는 각종 전자장치에 과부하가 걸리게 하거나 회로장치에 고장을 유발시켜 작동불능 또는 오류를 야기함으로써 통신, 교통, 발전, 수도, 군사지휘통제 등에 결정적 타격을 가하는 방법이 동원될 수 있다(Joint Publication. 2013: 3-13). 오늘날 미국은 전 세계에서 유일하게 실전적 전자전쟁을 경험한 국가이다. 미국은 2차례에 걸친 걸프전쟁과 2001년 아프가니스탄 전쟁, 2003년의 이라크 전쟁에서 전자전쟁의 능력을 유감없이 발휘했다. 단 3주 만에 종료된 2003년의 이라크 전쟁은 전자

전쟁의 서막이었다. 전방과 후방이 따로 없이 지휘부로부터 말단 전투부대에 이르기까지 목표물을 동시에 타격하여 무력화시키는 "동시 병렬전쟁(Parallel War)"을 수행하여 막강하다던 이라크 혁명수비대는 힘 한번 써보지도 못하고 초토화되었다.

전자기장을 지배하여 전자회로에 마비를 초래하는 전자폭탄 등 사이버 무기는 최첨단 전력도 일순간에 무력화 시킨다. 전자적으로 무력화된다는 것은 토마호크 미사일, 스텔스 전폭기, 항공모함, 최첨단 전차들이 아무런 기능을 발휘할 수 없는 고철이 된다는 것을 의미한다. 이라크 전쟁에 동원된 미·영국군 약 35만 명 중 전사자는 불과 136명이었다. 현대적 전자전쟁은 전자무기를 포함한 최첨단 무기를 전략표적과 전술표적들에 대해 동시, 다량, 집중적으로 사용하여 정확한 목표 타격을 함으로써 민간피해와 전투원의 손실을 최소화하며 필요한 표적만 무력화시킴으로써 단기간 내에 전쟁을 종료해 인명살상을 최소화하고 전쟁비용도 경감하며 전후 복구도 손쉽게 처리할 수 있는 부수적이지만 중요한 효과도 있다.

2) 전자전쟁 능력: 전자기장의 지배와 전자무기

전자전쟁은 전자기장의 우월적 지배에 성패가 달려 있다. 통신과 원격 조종장치 및 각종 무기에 장착되어 있는 전자적 회로에 장애를 유발하는 것이 전자전쟁의 요체이기 때문이다. 미국이 전자전쟁 목표로 설정한 영역은 상상을 초월한다. 미 국방부는 상대세력의 인공위성의 붕괴를 포함하는 소위 "항법전쟁(navigation warfare)"을 비롯해 라디오 등 상대방의 언론에 대한 전자적 장악으로, 예컨대 상대방의 정상방송 중에서 아국에 불리한 내용은 방송되지 않게 하는 등으로 방송내용이 자동적으로 변형되게 전자적으로 여론의 우위를 점하는 것, 상대방의 레이더 시스템, 전자전쟁 무기, 무인 정찰 장비나 로봇 등을 파괴하거나 오작동을 유발하는 내용을 모두 포함하고 있다.

오늘날 반도체 등 전자부품이 거의 모든 일상 제품에 사용되고 있음을 감안하면 전자전쟁을 감행한다는 것은 전자부품을 장착한 전화, 라디오, TV, 컴퓨터, 자동차, 기차, 항공기, 선박, 무선통신기기, 레이더장치, 탱크, 미사일 등 전쟁무기는 물론이고 생활필수품도 일순간에 무용지물로 만들 수 있다는 것을 의미한다. 전자전쟁은 인명살상 없이 전자적·기계적 장치에 장애를 초래하여 기계장치를 고철화 함으로써 그 기능을 마비시키는 것으로 전쟁의 성격을 극적으로 변환시키는 것이라고 할 수 있다. 그 결과 방위와 자위의 개념에 대하여 근본적인 수정을 요구하는 것이라고 할

수 있다(Joint Publication. 2013: 3-13).

전자전쟁은 사이버 영역에서 컴퓨터 네트워크 이용(CNE)을 통하여도 전개될 수도 있다. 최근의 사이버상의 군사정보작전 결과를 보면 상대방의 컴퓨터 네트워크에 비밀리에 침투하여 그들의 레이더망이 과연 무엇을 탐지하고 있는지를 모니터링할 수도 있다고 한다. 실험은 더 진행되어 현재 미국은 상대방의 컴퓨터와 네트워크를 상대방이 인지하지 못하도록 한 채 비밀리에 접수하여 상대방의 레이더가 오히려 상대방에게 허위의 영상을 제공하도록 외부에서 조종할 수 있는 능력도 갖추었다(David Fulghum, 2004). 데이비드에 따르면 작전은 네일 공군 비행기지에서 2000년과 2003년에 시연되었다. Suter 1과 Suter 2라고 불렸다고 한다. 이것은 즉 상대방이 허상을 보고 자국의 시설이나 자국민을 대상으로 또는 동맹국을 향해 미사일 발사 등 오류 공격을 하게 만들 수도 있음을 뜻하는 것이다. 이처럼 전반적인 전자기장을 제압하고 전자기장에서 우위를 확보하는 것이 상상을 초월한 위력을 가지는 것이다.

전자무기를 비역학성 또는 비폭발성 무기라고 한다. 그것은 목표물에 대한 외형상의 타격을 가함이 없이, 따라서 인명살상이나 물체의 외형적 손상 없이 전자파장에 대한 강력한 충격을 가해 목표물의 회로장치 등에 손상을 초래함으로써 전자기계를 사용 불가능하게 하거나 오작동 되게 하는 무기로 극초단파(high power microwave: HPM)나 강력한 단파 전자기장(Electromagnetic Pulses : EMP)을 사용하는 전자폭탄과 전자총이 있다. 전자무기는 전자 회로장치를 연소시킬 수 있는 고출력의 마이크로웨이브(HPM)로 지휘체계를 무력화시키거나, 직접적으로는 발사한 미사일에 집중되게 하여 미사일 공격을 좌절시키거나 또는 허위의 영상을 전송해 목표를 오인하게 만들어 결국 오폭하게 유도할 수도 있다. 예를 들어 2003년 이라크와의 전쟁에서 이라크 지휘부 벙커는 재래식 무기로는 도저히 폭파할 수 없는 지하 깊숙한 곳에 위치했다. 그러나 미국은 지휘부 벙커와 연결된 전자장치의 통신망을 통해 고출력의 마이크로웨이브를 집중시켜, 즉 전자전쟁 병기를 사용하여 벙커 내부의 컴퓨터와 네트워크를 간단히 붕괴시켰고 결국 이라크 사령탑을 무용지물 화했다(Will Dunham, Reuters, 2003).

Ⅳ. 사이버 안보와 국가정보기구

1. 개관

오늘날 사이버 영역은 국제법적 규율대상에서 벗어나 있는 개별국가의 노력과 전력 경주에 의한 무한 경쟁의 영역이다. 그러나 정책적인 관점에서만 본다면 사이버 정보경쟁에 대한 각국의 지혜로운 국제적 공조 노력은 중요하다고 하지 않을 수 없다. 사이버 무기에 대한 실질적인 국제 군축협상, 각국의 서버를 경유하며 자행되어 특정국가의 노력만으로는 추적이 어려운 사이버 테러조직에 대한 국제적 공조노력, 민간영역에 있어서의 컴퓨터 보안의식의 제고, 비군사적 목적의 컴퓨터 네트워크에 대한 사이버 공격에 대한 제재를 규율하는 국제조약 등의 합의 도출은 유엔 헌장에 바탕을 둔 세계평화와 안전을 위한 초석이 된다고 할 것이다.

따라서 각국은 미래전쟁 능력고양과 예방책 확보에 진력하는 한편 과거 국제법상의 군축경험을 이 새로운 전쟁 영역에도 도입하여 소모적으로 벌이고 있는 노력과 비용을 줄이자는 논의가 진행되고 있다(Clay Wilson, 2006: 5). 그러나 그것은 아직 논의 단계이고 설령 그러한 국제법적인 논의가 성사된다고 하더라도 협약 위반 사실을 적발하기가 재래식 무기에 대한 감시보다 더욱 어려울 뿐만 아니라, 사이버 정보전쟁의 성격상 단기간에 국가기간망 및 군사시설에 결정적인 손해를 초래하는 것이기에 사후적 제재와 보상은 이미 야기된 손해를 회복할 수도 없는 것이므로, 결국 각국은 저마다 할 수 있는 최선의 노력으로 사이버 안전망을 구축하고 사이버 역량을 증가시키는 것이 현실적인 대안이라고 할 수 있다.

원래 국가정보는 국가안보와 국가이익을 수호하려는 일국의 결집된 노력이다. 그런데 사이버 환경은 테러공격의 모습과 미래전쟁의 새로운 모습을 선보임으로써 국가안보의 양상을 근본적으로 바꾸고 있다. 따라서 국가정보에 대하여도 전혀 다른 새로운 접근과 모습을 요구하고 있다. 그러나 사이버 공격이 요구하는 국가정보의 새로운 모습과 역량은 그 절실한 필요성에도 불구하고 대다수의 국가가 경험해 보지 않은 내용으로서 국가정보기구의 창조적인 노력을 전제로 한 국가 간 무한정의 경쟁이 진행 중인 정보영역이다(Clay Wilson, 2006: 3).

2. 사이버 안보에 대한 국가정보기구의 책무

1) 사이버전쟁 능력 구비와 사이버 공격 의도와 능력의 실시간적 파악

먼저 국가정보기구는 사이버 전쟁수행에 필요한 5대 역량, 즉 사이버 심리전(PSYOP), 군사기망작전(MILDEC), 작전보안(OPSEC), 컴퓨터 네트워크 작전(CNO), 전자전쟁(EW)에 대한 이해와 함께 능력을 구비하는 것이 필요하다. 또한 국가정보기구는 그 연장선상에서 현재의 적국, 잠재적 적국 그리고 경쟁국들과 단체 등 적대세력의 사이버 테러 역량은 물론이고 그들의 사이버 전쟁수행 5대 역량을 면밀히 파악할 수 있는 능력을 구축하고 모니터링 해야 할 것이다. 상대국들이 사이버 전쟁 능력을 갖추고 그를 주된 전쟁 방법으로 상정하고 있는 마당에는 아무리 우수한 최첨단의 물리적·재래식 무기를 갖추었다고 하더라도 아국의 전자장이 상대세력에 의해 지배당하는 순간 재래식 무기는 고철에 지나지 않았음을 이라크 전쟁은 이미 잘 보여 주었기 때문이다(Clay Wilson, 2006: 4).

2) 사이버 공격과 전자전쟁 신병기의 추적 및 방어

국가정보기구는 또한 사이버 무기와 전자전쟁 무기의 세계적 발전과 개발 추이를 누구보다 잘 추적·파악하고 있어야 한다. 이것은 상대세력의 공식적인 사이버 국방무기 체계에 대한 파악만을 뜻하는 것은 아니다. 사적 영역에서 개발되는 상업적 전자장비 등은 하시라도 첨단 전자무기로 변모할 수 있는 것으로, 민간 영역의 기술개발 수준을 포함한 상대국의 전반적인 사이버 역량을 파악해야 한다는 것을 의미한다. 사이버 전쟁이 국가의 존망을 좌우할 중요한 국가안보의 문제임에는 재론이 필요 없고, 국가안보의 문제는 국가정보기구 제1의 존재 이유인 것이므로 상대방의 사이버 역량이 아국에 위협요소로 작용될 위험이 있는 한 국가정보기구의 노력은 뒤따라야 한다(Clay Wilson, 2006: 5).

3) 사이버 국제규범의 파악과 분석

국가정보기구는 사이버 전쟁 등 사이버 영역에 대한 국제법적 논의과정과 각국의 제도적·법적 내용도 추적하고 파악하여 이를 정책담당자들이 올바르게 정책에 반영하도록 제공해야 한다. 1998년과 1999년 러시아는 유엔에서 사이버 무기 군축제안을 한 바가 있다. 2002년 G-8 정상들은 하이테크 범죄대책 회의를 개최하여 악성 컴퓨

터 코드를 분류하고 통제하는 국제적 합의를 도출한 바가 있다(Andrew Rathmell, 2002). 또한 2001년 11월 23일 유럽연합 이사회(EU Council)는 헝가리 부다페스트에서, 사이버 영역에 있어서 각국의 관련법을 통일하고 각국의 조사방법의 체계화를 이루어 조사능력을 고양하며, 사이버 영역에서의 국제적 협력을 도모하기 위해 총 48개조로 구성된 사이버 범죄에 대한 유럽협약(Council of Europe Convention on Cybercrime)을 마련한 바가 있다(Kristin Archick, 2004). 그러나 각국의 정치적 고려 및 외교·국방정책과의 연관성 등 제반 사정으로 유럽연합의 사이버 범죄협약은 2004년 7월 1일 단지 5개국이 비준하는 데 그쳤다. 미국은 많은 논쟁 끝에 2006년 8월 3일 다수의 조항에 대한 유보 후에 일단 동 협약을 비준하였다(Clay Wilson: 13).

그러나 이러한 모든 국제적 노력은 그 목적의 정당성에도 불구하고, 이미 어느 정도 사이버 무기에 대한 개발과 기술 발전을 이룬 나라와 이제 사이버 전쟁 역량 고양의 문제에 대한 심각성을 깨닫고 개발을 시도하는 후발국가 모두를 현 상태 기술수준에서 동결을 가져올 수도 있는 것으로써, 극단적으로 말한다면 제2의 핵무기 개발에서도 기존의 핵무기 개발과 동일한 국가장벽, 즉 전자무기 블록을 형성하여 일국을 영원히 전자전쟁에서의 종속국가로 영락시킬 수도 있다는 현실적 이해관계에 부딪치게 만든다. 이러한 제반 노력에 대한 정보수집과 분석 판단은 국가정보기구가 아니면 수행하기 어려운 분야이다(Clay Wilson, 2006: 7).

4) 사이버 방첩공작(Cyber Counterintelligence)

사이버 방첩은 해외세력 정보기구를 포함한 사이버 위협자들의 사이버 활동을 확인하고, 침투하며 또는 무력화시키는 제반 활동을 말한다. 2009년 4월 7일 펜타곤은 사이버 공격에 대응하고 피해를 복구하기 위해서 지난 6개월 동안에만 1억 달러를 지출했다고 발표했다. 국제적인 사이버 방첩활동의 노력은 기구창설로도 나타난다. 2007년에 자행되었던 주권국가 에스토니아(Estonia)에 대한 사이버 전쟁을 고려하여 북대서양조약기구(NATO)는 사이버 방어능력의 획기적인 증대를 위하여 에스토니아의 수도 탈린(Tallinn)에 최고합동사이버국방센터Cooperative Cyber Defence Centre of Excellence (CCD CoE)를 창설했다. 동 기구는 NATO로부터 2008년 10월 28일 국제군사기구의 자격을 취득했다. 한편 에스토니아 공화국의 사이버 대란을 수사하고 지원했던 FBI는 컴퓨터 범죄 전문 인력을 상주시킨다고 발표했다(Clay Wilson, 2006: 7).

우리의 국가정보원도 마땅히 사이버 방첩수요가 상존하는 대한민국 안보현실에서 사이버 방첩의 주무부서로서의 실천적인 역할을 다해야 할 것이다. 그런데 사이버 방첩에서 가자 어려운 문제는 행위자 속성(Attribution), 즉 책임귀속의 문제이다. 전통적인 전쟁과 달리 실질적인 배후 공격자가 누구인지를 밝히는 것은 현실적인 활동을 위한 핵심적인 사항이지만 매우 어려운 일이다. 그런데 미국의 자신감은 국가정보원의 역량에 지침을 제공한다. 단적으로 미 국방부 장관 레온 파넷(Leon Panetta)은 미국은 그 어떤 사이버 무법자나 배후자라도 그를 추적하여 책임을 귀속시킬 능력을 확보하고 있다고 밝혔다(Carroll, Chris.11. 2012. 10).

5) 민간영역에 대한 보안과 교육

마지막으로 민간영역에서의 컴퓨터 보안에 대한 역량강화 및 대책 강구이다. 오늘날 컴퓨터 네트워크의 발달은 민간영역이 국가 주요기간시설의 운용에 참여하는 기회를 넓혀 주고 있다. 시설구축에서뿐만 아니라 유지 보수 등이 민간영역에 의해서 이루어지고 있는 것이 적지 않다. 국가기간시설 네트워크에 대한 보수와 유지가 불가피하게 민간영역에서 이루어진다는 것은 국가기간시설에 대한 정보가 자연스럽게 외국 업체를 통해서 상대세력으로 흘러 들어갈 수도 있음을 뜻한다. 왜냐하면 오늘날 다국적 기업의 활성화는 기업의 국적을 불투명하게 했고, 또한 기술적으로도 하청, 재하청 공정은 기업의 영역에서 무수히 발생하고 있기 때문에 민간영역에서의 컴퓨터와 네트워크 보안은 국가안보와 직결되어 있다고 할 수 있다. 따라서 국가정보기구는 특히 핵심국가기간시설망과 연결되어 있는 민간영역에 대한 보안활동과 상대세력의 침투에 대한 방첩활동 및 실질적인 보안교육을 통한 최선의 보안체계 확립에 민간영역과 상호 협조하는 노력을 경주해야 한다. 그런데 본고에서는 지면 제약으로 상술하지만 핵심 문제는 법적 근거이고, 미국 의회와 오바마 행정부의 힘겨루기가 보여준 바와 같은 입법론적 접근방법이다(최진혁, 2010, 197-230; 이창무, 2010, 91-111).

Ⅴ. 마무리

앨빈 토플로는 제1의 물결시대인 농업사회에서의 전쟁은 칼, 창, 활, 방패 등을 사용한 원시적 백병전으로 전개되었고, 제2의 물결시대의 산업사회에서의 전쟁은 화

약발명과 더불어 대포, 전차 등이 개발된 데 이어서, 원자폭탄 등 대량 화력으로 무차별 대량파괴 및 살육전이 전개되었으나, 제3의 물결시대의 지식정보화 시대에서는 하이테크 전쟁으로서 정밀 유도무기로 주문파괴를 하고, 실시간의 정보획득 처리 및 타격이 가능하고 그 범위도 우주전쟁으로 확대됨으로써, 대량파괴와 대량살상 없이 전장에서의 우위를 점함으로써 승리하게 될 것이라고 예견했었다. 그의 예언대로 컴퓨터 과학기술과 정보기술의 획기적인 발전은 군사력 운용에도 혁신적인 변화를 요청하여 1990년대에 이르러 선진 각국은 소위 "군사혁신(Revolution in Military Affairs : RMA 또는 Military Technical Revolution : MTR)"을 단행하여 전자전쟁 등에 대비한 새로운 전쟁 패러다임을 추진해 왔다.

2003년 부시 행정부는 의회의 정식 입법조치 전에 국가안보 대통령 명령 제16호(National Security Presidential Directive 16)를 발령했다(대통령 명령 제16호(To Develop Guidelines for Offensive Cyber-Warfare). 동 대통령 명령은 미국이 언제, 그리고 어떻게 상대국의 컴퓨터와 네트워크에 공격을 할 수 있는지의 기준을 제시한 국가차원의 가이드라인을 설정했다. 그 내용이 비밀 분류되어 있지만 상대국의 사이버 공간에서의 어떠한 행위를 사이버 전쟁에 따른 공격으로 간주하고, 따라서 어떠한 조건에서 상대방에 대해 정당한 대응 공격을 할 수 있는지와, 그것을 누가 결정할 것인지 법적인 기준을 제시하고 있다고 한다(Kristin Adair, 2006). 쉽게 말하면 촌각을 다투는 사이버 전쟁의 선포 가이드라인을 준비한 것이라고 할 수 있다. 이러한 노력은, 국가업무의 명백성과 책임성을 확보할 수 있으며 비상시에 사이버 전쟁 발동의 국제법적 정당성을 뒷받침할 수 있다는 점에서도 우리가 본받아야 할 내용이라고 할 것이다(조재현, 2009, 18-31).

결론적으로 무정형의 그러나 가공(可恐)할 내용으로 이해되는 사이버 전쟁을 포함한 사이버 환경에 대한 구체적 현실화와 대책은 법집행기구의 사이버 치안역량 강화만으로는 이루어질 수 없다. 궁극적으로 국가정보기구의 몫이라고 할 것이다. 유능한 국가정보기구의 4대 임무는 정보수집·정보분석·(해외에서의) 비밀공작 그리고 방첩공작활동이다. 그런데 많은 경우에 대책회의, 연구조사, 보안, 해외연수와 협조 등 감시 감독을 위한 일을 만들어 놓고 감독하는 입법 방식에 따르는 경우가 적지 않다. 하지만 오늘날 초국가적 안보위협세력의 대표인 국제테러조직은 우리에게 테러 진압 부대나 5개년 국가대책이 있다고 하여 무서워서 계획한 테러를 안 하는 것이 아니고, 국가 사이버 대책이나 센터가 있다고 하여 북한이나 해외세력이 사이버

공격을 안 할 것도 아님을 직시하여야 한다. 적대세력보다 한발 앞선 테러 정보획득과 사전분쇄, 사이버 공격에 맞대응할 실전적인 사이버 부대의 역량 구축이 결여된 대책은 모두 공허한 것이다. 결국 기본은 하나도 둘도 해당 분야의 "정보" 생산이고 두 번째는 생산한 정보의 취합과 정밀한 분석이고, 세 번째는 신속한 정보수집과 전파 그리고 정보공유를 통한 법집행기구에 의한 치밀한 수사와 처벌로 연결되도록 통로를 구축하는 것이라고 할 것이다.

결론적으로 자칫 방심하는 사이에 사이버 세계의 안전성 확보에서 2류 국가로 전락하는 사이버 남북분단의 참상을 겪을 수도 있는 것이 현실이다. 지적 창조의 결과로 수단과 방책을 가리지 않고 사이버 안보를 확보하는 것은 결코 사이버 중상주의나 사이버 제국주의가 아니다. 사이버 전장에서의 2등은 무의미한 것이기 때문이다. 오늘날 세계 최강의 미국 사이버 안보전략과 실천력은 그 실천성과 위중함을 잘 말해준다. 미국의 사이버 안보전략을 요약한다면 단적으로, 전 세계 어떤 사이버 공간이나 사이버 자료도, 첫째, 원하면 침투한다, 둘째, 원하면 절취한다, 셋째, 원하면 파괴한다고 파악되는 그 엄중성에 대한 이해가 절실해 보인다.

오늘날 사이버 세계의 안전은 가장 실천적이고 현실적인 위협세계의 쟁점이다. 따라서 핵심은 하나도 둘도 계획의 구체성과 실천력의 배양이다. 대책회의나 교육 등은 부차적이다. 실전의 사이버 사령부와 사이버 정보기구 그리고 사이버 전사의 창설과 육성에 더 커다란 노력을 경주해야 하고, 우리의 경우에는 가장 많은 경험을 가지고 인력과 장비를 가진 국가정보원의 사이버 수호 역량을 고양하고 더 많은 책무를 부담시키고 합리적인 업무 감독을 다하는 것에 있다고 할 것이다. 물론 어느 경우에도 사이버 안보를 포함한 국가안보 그리고 국가정보기구의 철학적 이념은 사회계약 사수를 위한 국가 체제 그 자체의 사수와 더 커다란 자유의 수호에 있음을 바로 알아야 할 것이다.

참고문헌

1. 국내문헌

박노형 (2014). 국내외 사이버안보 법제정 동향과 시사점: 미국을 중심으로. 국가안보전략연구소 학술회의 초록집. (4. 17). 은행회관 2층 국제회의실.

박준석 (2014). 국가안보 위기관리 대테러론. 서울: 백산출판사.

한희원 (2011). 국가정보(법의 지배와 국가정보). 서울: 법률출판사.

김두현, 안광호(2010), 다중이용시설의 대테러 안전대책, 한국경호경비학회지, 제22호, pp. 37-64.

최진혁(2010), 산업보안의 제도적 발전방안 연구: 미국 사례를 중심으로, 한국경호경비학회지, 제22호, pp. 197-230.

이창무(2010), 우리나라 보안산업의 역사적 기원에 관한 연구, 한국경호경비학회지, 제22호, pp. 91-111.

Park, Dong-Kyun(2010) The Counter-Terrorism Measures for International Sports Events in Korea (한국의 국제스포츠 행사에 대한 대테러 전략), 한국경호경비학회지, 제22호, pp. 65-90.

박준석(2006), "한국민간보안·시큐리티Security) 산업의 발전방안" 龍仁大學校 논문집 제24집.

조재현(2009), "테러방지법의 제정방향", 「테러방지법의 제정의 필요성과 방향」, 한국테러학회 춘계학술세미나자료집, pp. 18-31.

2. 외국문헌

Andrew Rathmell. (2001). Controlling Computer and Network Operations. Information and Security. Vol(7).

Bob Drogin. (1999). Russians Seem To Be Hacking Into Pentagon: Sensitive information taken but nothing top secret. Los Angeles Times. (10. 7).

Charles Doyle. (2010). Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws. CRS Report 97-1025.

Carroll, Chris. (2012). US can trace cyberattacks, mount pre-emptive strikes, Panetta says. Stars and Stripes. (10.11).

Catherine A. Theohary. (2013). Information Operations, Cyberwarfare, and Cybersecurity:

Capabilities and Related Policy Issues. CRS Report RL31787.

Clarke, Richard. (2011). "China's Cyberassault on America", Wall Street Journal.

Clay Wilson. (2006). Information Operation and Cyberwar: Capabilities and Related Policy Issues. Congressional Research Service-The Library of Congress. (9.14).

David Fulghum. (2004). Sneak Attack. Aviation Week & Space Technology.

Ellen Nakashima. (2013). U.S. Said to Be Target of Massive Cyber-Espionage Campaign. Washington Post. (2. 10).

Graham, B. (2005). Hackers Attack Via Chinese Web Sites: U.S. Agencies' Networks Are Among Targets. Washington Post. (8. 25).

Hicks, Jesse. (2014). This machine kills trolls. The Verge.

Ian Traynor. (2007). Russia accused of unleashing cyberwar to disable E., The Guardian. (5. 17).

James Middleton. (2001). Hackers launch 'cyber jihad' on US: Pakistani group defaces government website .Maura Conway-DORAS. (10.18)

John W. Rollins and Clay Wilson. (2007). Terrorist Capabilities for Cyberattack: Overview and Policy Issues. CRS Report RL33123,

Joint Chiefs of Staff. (2007). Joint Publication. Department of Defense Dictionary of Military and Associated Terms. 1(2).

Kristin Adair. (2006). Rumsfeld's Roadmap to Propaganda. National Security Archive Electronic Briefing Book. No(177). (1.26).

Kristin Archick. (2004). The Council of Europe Convention. Foreign Affairs. Defense, and Trade Division. (7.22).

Kristin Finklea. (2011). The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement. CRS Report R41927.

Kumar, S. (2010). "Denial of Service Due to Direct and Indirect ARP Storm Attacks in LAN Environment*". Journal of Information Security 01(2).

Larry Greenemeier. (2007). Estonian Attacks Raise Concern Over Cyber 'Nuclear Winter". Information Week. (5. 24).

Latimer, Jon. (2001). Deception in War. New York: Overlook Press.

Lynn, William J. III. (2010). "Defending a New Domain: The Pentagon's Cyberstrategy", Foreign Affairs.

Mandiant Intelligence Center Repor. (2014). APT1: Exposing One of China"s Cyber Espionage Units. DC Headquarters.

Michael A Vatis. (2001). Cyber Attacks during the War on Terrorism: A Predictive Analysis, Institute for Security Technology Studies. Dartmouth College. (9. 22).

Michael Riley & Eric Engleman. (2012). Code in Aramco Cyber Attack Indicates Lone Perpetrator. Bloomberg Businessweek. (10. 25).

Peter Brookes. (2005). The Art of (Cyber) War. The Heritage Foundation.

Robert Lemos. (2007). Electronic Jihad' fails to threaten, again. SecurityFocus. Shawn Henry. (2011). Responding to the Cyber Threat. Federal Bureau of Investigation, Baltimore, MD.

Sterling, Bruce. (1993). "Part 2(d)". The Hacker Crackdown. McLean, Virginia: IndyPublish.

The World. (2013). US hands China cyber propaganda weapon, David Pilling. U.S. Department of Defense. (2010). Cyber Command Fact Sheet. (5. 21).

Wael Mahdi. (2012). Saudi Arabia Says Aramco Cyberattack Came from Foreign States. Bloomberg News. (12. 9).

White House. (2007). President Bush to Welcome President Toomas Ilves of Estonia. (5. 4).

Will Dunham. (2003). U.S. May Debut Secret Microwave Weapons versus Iraq. Reuters. (2.2).

William J. Lynn III. (2010). Defending a New Domain. Foreign Affairs.

3. 인터넷 자료 등

보안뉴스. 2014. 3. 31. http://www.boannews.com/media/view.asp?idx=40381&kind=3.

조선비즈. 2014. 2. 17, http://biz.chosun.com/site/data/html_dir/2014/02/16/2014021602442.html

Kim, Eun-jung. (2013). Korean military to prepare with U.S. for cyber warfare scenarios". Yonhap News Agency. (4. 6).

http://www.newswire.co.kr/newsRead.php?no=703568.

CIA. https://www.cia.gov/index.html.

FBI. http://www.fbi.gov/.

NSA. http://www.nsa.gov/.

【Abstract】

A Study about the Direction and Responsibility of the National Intelligence Agency to the Cyber Security Issues

Han, Hee-Won

Cyber-based technologies are now ubiquitous around the glob and are emerging as an "instrument of power" in societies, and are becoming more available to a country's opponents, who may use it to attack, degrade, and disrupt communications and the flow of information. The globe-spanning range of cyberspace and no national borders will challenge legal systems and complicate a nation's ability to deter threats and respond to contingencies. Through cyberspace, competitive powers will target industry, academia, government, as well as the military in the air, land, maritime, and space domains of our nations. Enemies in cyberspace will include both states and non-states and will range from the unsophisticated amateur to highly trained professional hackers. In much the same way that airpower transformed the battlefield of World War II, cyberspace has fractured the physical barriers that shield a nation from attacks on its commerce and communication. Cyberthreats to the infrastructure and other assets are a growing concern to policymakers.

In 2013 Cyberwarfare was, for the first time, considered a larger threat than Al Qaeda or terrorism, by many U.S. intelligence officials. The new United States military strategy makes explicit that a cyberattack is casus belli just as a traditional act of war. The Economist describes cyberspace as "the fifth domain of warfare and writes that China, Russia, Israel and North Korea. Iran are boasting of having the world's second-largest cyber-army. Entities posing a significant threat to the cybersecurity of critical infrastructure assets include cyberterrorists, cyberspies, cyberthieves, cyberwarriors, and cyberhacktivists.

These malefactors may access cyber-based technologies in order to deny service, steal or manipulate data, or use a device to launch an attack against itself or another piece of equipment. However because the Internet offers near-total anonymity, it is difficult to discern

the identity, the motives, and the location of an intruder. The scope and enormity of the threats are not just focused to private industry but also to the country's heavily networked critical infrastructure.

There are many ongoing efforts in government and industry that focus on making computers, the Internet, and related technologies more secure. As the national intelligence institution's effort, cyber counter-intelligence is measures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligence service collection efforts that use traditional methods to gauge cyber capabilities and intentions. However one of the hardest issues in cyber counterintelligence is the problem of "Attribution". Unlike conventional warfare, figuring out who is behind an attack can be very difficult, even though the Defense Secretary Leon Panetta has claimed that the United States has the capability to trace attacks back to their sources and hold the attackers "accountable".

Considering all these cyber security problems, this paper examines closely cyber security issues through the lessons from that of U.S experience. For that purpose I review the arising cyber security issues considering changing global security environments in the 21st century and their implications to the reshaping the government system.

For that purpose this study mainly deals with and emphasis the cyber security issues as one of the growing national security threats. This article also reviews what our intelligence and security Agencies should do among the transforming cyber space. At any rate, despite of all hot debates about the various legality and human rights issues derived from the cyber space and intelligence service activity, the national security should be secured. Therefore, this paper suggests that one of the most important and immediate step is to understanding the legal ideology of national security and national intelligence.

Key words : Cyber security, Cyber terrorism, Cyberwarfare, Electronic warfare, The fifth domain of warfare