情 報 保 護 學 會 誌
第 14 卷 第 6 號, 2004. 12

사이버전에 관한 주요국의 견해

박 상 서, 박 춘 식*

요 약

사이버전의 위협과 발생 가능성에 대한 찬반 양론이 있기는 하지만, 분명한 것은 향후 사이버공간에서의 또는 사이버공간을 매개체로 한 분쟁은 분명히 커다란 위협으로 대두될 것이라는 것이다. 이에 따라, 주요국들은 각국이 처한 상황과 국가 정책 등에 따라 각각 사이버전의 개념을 정립해 나아가고 있다. 또한, 사이버전을 군사적인 측면뿐 아니라 경제적인 측면과 범죄의 관점에서 바라보고 있기도 하다. 본 고에서는 사이버전에 관련된 주요국가의 기본적인 견해를 정리한다.

Ⅰ. 서 론

사이버전은 기본적으로 사이버공간을 대상으로 하는 전쟁으로서, 정보 및 컴퓨터를 방어(defend)하고, 정보에 대한 공격을 억지(deter)하며, 적이 이러한 능력을 가지지 못하도록 거부(deny)하는 것을 의미한다[1]. 또한, 적에 대한 공격적인(offensive) 정보작전 또는 전장에 대한 정보를 지배(dominate)하는 것까지 포함한다. 예를 들면, 컴퓨터 또는 네트워크에 대한 침입, 컴퓨터와 네트워크에 대한 서비스거부 공격, 사이버공간을 통한 시설에 대한 방해, 센서 재밍, 그리고 의사결정을 위하여 믿을 수 있는 정보를 조작하거나 적의 사고를 통제하는 것 등을 포함한다.

2001년 11월, 부시대통령과 럼스펠드(Rumsfeld) 국방장관은 모두 사이버전이 미국 국가 안보에 위협으로 대두되고 있다는 것을 인정하였다[2]. 몇 년 전, 중앙정보국(Central Intelligence Agency: CIA)은 단지 러시아와 중국만이 특별히 사이버위협을 가할 수 있다고 언급하였지만, 지금에 와서는 20개 이상의 국가가 미국을 대상으로 하는 다양한 종류의 정보작전(Information Operations : IO)을 구사하고 있다고 지적한다[1]. 더 최근에, CIA는 적들이 사이버전을 군사 교리의 새로운 한 부분으로 편입시키고 있다고 증언하기도 하였다. 기밀 해제된 해군 위협 평가 보고서에서는 사이버전을 준비하기 위한 정책을 가지고 있고 그 능력을 신속히 개발하고 있는 국가로 러시아, 중국, 인도, 그리고 쿠바를 지목하고 있다. 이 보고서에 따르면, 북한, 리비아, 이란, 이라크, 그리고 시리아는 어느 정도 사이버전 능력을 가지고 있는 것으로 알려지고 있으며, 프랑스, 일본, 그리고 중국은 이 분야에 대해 적극적인 것으로 알려지고 있다[3].

하지만, 각국은 자국의 상황이나 정서, 국가 시책에 따라 사이버전에 대한 입장이 조금씩 차이가 있다. 따라서, 본 논문에서는 미국 의회조사국에서 의회에 보고한 보고서[1]를 중심으로 최근 이슈로 등장하고 있는 사이버전에 관한 주요국의 시각을 소개함으로써 우리의 개념 개발을 위한 화두를 제공하고자 한다.

Ⅱ. 미 국

미국 정부가 사이버전 문제를 과거보다 더 많이 고려·정리하고 있는 것으로 보이지만, 사이버위협이 심각한 국가 안보 위협이 되기 때문에 국가적 안보 차원의 명확한 대응이 필요하다는 것에 대한 국가적인 합의가 이루어져 있거나 앞으로 이루어질 것인지는 명확하지 않은 것으로 알려져 있다.

미국 정부는 사이버전 대응에 관하여 두 가지 관점을 가지고 있는 것으로 알려져 있다. 하나는 사이버위협은 근본적으로 국가 안보 문제이기 때문에 미국의 주요 국가 이익과 주요 기반이 위협을 받는다는 것이다. 역사적으로, 미국은 미국의 이익을 보호하기 위해 군사력과 외교

* 국가보안기술연구소 (csp@etri.re.kr)

력을 동시에 사용해왔다. 미국에 대한 사이버위협이 미국의 국가 이익을 위협하는 또 하나의 유사 사례가 되는 것이다. 또 다른 관점은, 사이버위협은 민간 또는 국내 당국자가 해결해야 한다는 것이다. 여기서는 미국 국경 내에서의 강력한 군사적 역할에 관심이 모아진다. 게다가, 다양한 사생활 및 민간의 자유에 대한 관심이 높다. 과거에는 미국에 대한 외국으로부터의 위협은 거의 외국으로 반격을 하였다. 그러나, 오늘날 우리는 지리적 국경이 의미가 없어지고 심지어 사이버공간에서는 존재하지도 않는 시대에 살고 있다. 따라서 의사결정권자들이 새로운 도전을 받고 있는 것이다.

미군은 합동 비전 2010(Joint Vision 2010 : JV-2010)[4]에서 합동참모본부가 발표하는 합동 군사 전략을 위한 광범위한 장기적 전략 및 계획의 개념을 소개하였다. JV-2010은 전통적 전투력을 변화시키기 위한 방편으로 정보 우위(information superiority)와 기술우세(technological advantages)를 채택하였다. 그 후, 2000년 5월 30일 발표된 JV-2020[5]에서는 미 군사력의 지속적인 변화를 유도하기 위하여 JV-2010에서 확립한 개념적 틀(conceptual template)을 확대하고 있다. JV-2020에서는 다음과 같이 기술하고 있다.

> *정보 환경의 변화에 따라 정보 우위는 합동군의 작전 능력의 변화와 합동 지휘통제의 발전을 가능케 하고 있다.*

또한, 4년주기 국방 논평(Quadrennial Defense Review: QDR)[6]에서는 전세계적으로 사이버전과 같은 비대칭전이 점차 늘어날 것이라고 언급하면서, 다음과 같이 덧붙이고 있다.

> *미군의 전통적 전투력이 압도적으로 우세하여, 미래의 잠재적인 적이 비대칭전 능력을 보급하고 있고, 이러한 수단에 의존할 가능성이 증가하고 있기 때문에, 미군은 이러한 조건에서 주요 전구 전투에서 싸우고 승리하기 위한 계획을 세우고 준비해야 한다.*

Ⅲ. 러시아

많은 러시아인들은 사이버전의 위협성이 핵전쟁에 못 미친다고 주장한다. 여러 러시아군 고위 장교는 다음과 같은 주장을 제기하였다[7].

> *군사적 관점에서 볼 때, 러시아 또는 러시아군에 대하여 사이버전을 사용한다면 사상자의 유무에 관계없이 군사적 분쟁으로 여길 것이다. … 적이 러시아의 경제나 국가 지휘통제 체계, 또는 군의 전투 잠재력에 대하여 전략적 사이버전 수단을 사용할 가능성을 고려한다면 … 러시아는 우선적으로 사이버전 수단 및 군사력, 그 다음으로는 적국에 대하여 핵무기를 사용할 권한을 가지고 있다.*

다른 러시아인들은 사이버전은 군사적 측면이며, 사이버전의 목표는 분쟁중에 한 편이 다른 편에 대한 정보를 입수하고 그 정보를 이용하여 유리한 고지를 점령하는 것이라고 여기고 있다. 이는 적의 정보 시스템, 의사결정 과정, 지휘통제체계, 그리고 국민에게 영향을 미칠 수 있는 특별한 정보기술력을 이용할 때 가능하다[8]. 몇몇 러시아인들은 분쟁이 발발하면 "전투 바이러스와 여타 정보에 관련된 무기들이 전력을 배가시키는 요소"가 될 것이라고 믿는다.

2000년 9월 12일, 러시아 푸틴 대통령은 6월 23일 러시아안보위원회(Russian Security Council)에서 승인된 러시아정보보안독트린(Russian Information Security Doctrine)[9]을 선포하였다. 새 독트린은 정부가 컴퓨터 범죄를 다루고 사이버공간의 보안을 확고히 하기 위한 법적 토대를 제공하기 위한 것이다. 이는 러시아가 직면하고 있는 외국과 국내로부터의 사이버 위협을 다루기 위한 노력의 일부이기도 하다.

Ⅳ. 중 국

중국은 사이버전을 군사적 용어, 조직, 훈련 및 교리에 편입시키는데 적극적이다. 만일 군사혁신(Revolution in Military Affairs: RMA)이라는 것이 기술적 변화를 통한 군사 훈련, 조직 및 교리의 변화를 의미한다면, 중국은 사이버공간에서 전정한 RMA를 경험하고 있는 나라가 될 것이다. 게다가 중국이 개념을 발전시키는 것을 보며 미군 지도자들은 우려를 나타내게 되었다. 예를 들어, 미군우주사령부의 사령관인 Eberhart 장군은 미군이 중국의 의도에 관심을 가지고 있으며 중국이 컴퓨터 네트워크 공격 수행 능력을 개발하는 것에 대하여 우려하고 있다고 언급한다[10].

중국의 사이버전 개념은 현대의 인민전쟁 개념과 과거의 36계에 기반을 두고 있다. 이 두 개념은 각각 전략적, 전술적, 작전적 수준에서 어떻게 전쟁을 수행할 것인지에 대한 중국식 시각을 나타내고 있다. 또한 중국은 전쟁에 대해서는 마르크스-레닌주의의 영향을 강하게 받았다. 따

라서, 중국식 전쟁 방법은 기만, 지식전(knowledge-style war), 적에 대한 비대칭 우위를 강조하고 있다. 중국에게 있어서 사이버전은 "산업사회의 기계화 전쟁에서 결심·통제 전쟁(a war of decisions and control), 지식전쟁(a war of knowledge), 그리고 지성전쟁(a war of intellect)으로 변화하고 있는 것이다.[11]"

중국은 Net Force(대대 규모)의 개념을 추구하고 있는데, 이 부대는 수많은 대학교, 사관학교 및 훈련 센터에서 훈련된 컴퓨터 전문가들로 구성된다. 중국은 이러한 임무 수행을 위하여 젊은 사람을 훈련시키도록 강조하고 있으며, 1997년 이후 여러 대규모 연례 훈련을 실시하고 있다[12].

V. 영 국

영국은 사이버전에 대하여 미국과 유사한 관점을 가지고 있다. 영국은 사이버전을 국가 목표 달성을 위하여 자신의 정보 시스템을 보호하면서 적군의 정보 시스템에 영향을 주는 행위라고 인식하고 있다[1]. 더구나, 영국은 사이버공간의 활동에 적용될 수 있는 여러 현존 법률을 기반으로 하는 합법적 체계를 이용한다[2]. 이를 통해, 영국이 개인과 기업에 대한 사이버공격을 사회·범죄적 문제로 인식하고 있음을 알 수 있다. 최근 들어서는, 조사권 제한법(Regulation of Investigatory Powers Act 2000)에서 영국 정부가 전자우편을 감청 및 해독할 수 있도록 하고 있으며, 필요한 경우 개인의 파일을 복호화할 수 있도록 하고 있다. 영국 정부는 이 법이 "최초로 적극적인 조사 기술을 법률에 포함시켰고, 강력한 암호를 범죄에 사용함으로 인해 발생하는 위협과 싸우는데 필요한 새로운 권한을 부여하였으며, 권한에 대한 독립적인 감독을 보장한다"고 주장하고 있다[13].

VI. 독 일

사이버전에 대한 독일의 시각은 대체로 미국과 영국에 비교된다[14]. 독일은 국가 목표를 추구함에 있어서 공격적·방어적 사이버전의 합법적 역할을 인지하고 있다. 하지만 미국보다 더 체계적인 측면도 있다. 사이버 위협과 사이버 대응(cyber responses)에 대하여, 국가 부분을 비국가 부분(예: 정치가, 국제 기구, 언론 등), 범죄(예: 조직범죄, 해커 등), 그리고 개인(종교가 및 전문집단 등)과 분리시켜 고려하고 있다.

하지만 다음 두 가지 측면에서 사이버전에 대한 독일의 관점은 다르다. 독일은 언론 관리를 사이버전의 한 요소로 여긴다. 또한, 프랑스처럼 경제적 사이버전 이론에 무게를 두고 있는데 그 이유는 다음과 같다. (1) 독일 기업 및 경제에 영향을 미칠 수 있는 경제적 피해 가능성을 평가하였다. (2) 사이버공간에서의 산업 첩보활동 때문에 프랑스로부터 심각한 경제적 손실을 입은 바 있다. (3) 잠재적 사이버 공격의 결과를 경감시키기 위한 방안을 찾고 있다.

VII. 프랑스

프랑스는 사이버전이 군사적 측면과 경제적(또는 사회적) 측면을 가지고 있는 것으로 인지하고 있다[15]. 먼저, 군사적 측면에서는 다소 제한된 역할을 수행하는 것으로 구상하고 있다. 즉, 사이버전이 대부분 저강도(low intensity conflict) 분쟁 또는 전쟁 이외의 작전에서 발발한다고 판단하고 있으며, 일반적으로 나토나 (종종 미국의 통제하에) UN의 체제안에서 수행되는 것으로 인지하고 있다. 이런 맥락에서 볼 때, 동맹국은 적대적이지 않다고 판단하고 있다.

한편, 경제적 또는 사회적 측면에서는 잠재적으로 사이버전을 보다 광범위하게 적용할 수 있다고 보고 있다. 즉, 사이버전은 경제 영역에서의 분쟁에 대하여 보다 넓고 깊이 관계되어 있으며, 경쟁국들이 시장에서의 이익을 zero-sum으로 추구하는 환경에서는 경제적 평화가 존재하지 않는 것으로 가정하고 있는 것으로 보인다. 그리고 이에 관련된 사이버전에 대해서는 나토, UN 또는 미국의 승인을 받지 않아도 된다고 보고 있다. 특히, 경제적인 관점에서는 동맹국이 곧 적이 될 수도 있다고 여기고 있다. 프랑스는 사이버전을 염두에 둔 경제학교를 운영하

1) 2000년 6월, 영국은 사이버전을 "자신의 정보와 정보 시스템을 보호함과 동시에 이를 활용하여 적의 정보, 정보를 기반으로 하는 프로세스, 지휘통제, 시스템 및 주요기반에 영향을 줌으로써 정치적·군사적 목표 달성에 있어서 의사결정자들에게 영향력을 행사하는 전체 활동"라고 정의하였다.

2) 관련된 법률로는 컴퓨터오용법(Computer Misuse Act, 1990), 통신법(Telecommunications Act, 1984), 통신(부정행위)법(Telecommunications (Fraud) Act, 1987), 음란물간행법(Obscene Publications Act, 1959 및 1964), 아동보호법(Protection of Children Act, 1978), 범죄재판법(Criminal Justice Act, 1988), 범죄재판과공중질서법(Criminal Justice and Public Order Act, 1994), 자료보호법(Data Protection Act, 1984 및 1998), 절도법(Theft Act, 1968 및 1978), 위조와모조법(Forgery and Counterfeiting Act, 1981), 저작권및특허법(Copyright Design and Patents Act, 1988), 통신감청법(Interception of Communications Act, 1985) 등이 있다.

고 있기도 하다[16].

프랑스는 또한 사이버공간에서 자국민을 감시하는 것에 대해서도 다른 시각을 가지고 있다. 보고서에 따르면, 프랑스는 독자적인 Echelon을 운영하고 있는 것으로 알려져 있다. Frechelon으로 알려진 이 체계는 프랑스의 통신 특히 파리 지역의 통신을 감시 및 분석하고 있는 것으로 알려져 있다[17].

Ⅷ. 결 론

사이버전에 대하여 비판적인 시각을 가지고 있는 일부 전문가들은 사이버전이 전통적인 전쟁이나 분쟁에 비해 직접적인 분쟁으로 발전할 가능성이 낮다고 지적한다. 하지만, 언론 등에서는 사이버테러리스트들이 미국의 전력, 운송 또는 통신망을 마비시킬 적당한 시기를 기다리고 있다고 경고하고 있기도 하다. CIA를 참여시켜 2000년 2월 23일 개최된 사이버테러에 관한 하원 합동 경제 위원회 청문회에서 Bob Bennett 상원의원은 "미국의 국방 및 산업 시설에 관한 사이버공간의 공격은 경제 번영과 국가 안보에 대한 전통적인 위협만큼이나 실제적이고 위험하다."라고 언급한 바 있다[1].

현재까지 사이버전 위협을 가까이 느껴질 정도의 사례는 아직 발표되고 있지 않다. 하지만 무엇보다도 중요한 것은 사이버위협은 분명히 존재하고 있고, 미래의 커다란 위협으로 다가올 것이라는 점이다[18,19].

미국 의회 청문회에서 과학기술 분야의 국가 정보 담당관인 로렌스 거쉰(Lawrence Gershwin)이 서비스 거부 공격을 포함한 대량 피해 무기가 10년 뒤에는 확산될 것이라고 지적한 CIA 보고서[20]를 인용한 것은 시사하는 바가 크다.

전쟁과 평화의 전통적인 경계는 희미해지고 있다. 이러한 상황은 냉전시대에 이미 예견된 것이었으나, 911 세계무역센터와 펜타곤에 대한 공격 발생후 수행된 테러와의 전쟁 이후 더욱 모호해지고 있다.

정보 기반의 무력화나 파괴는 한 국가의 국방 및 경제 안보를 위협하게 된다. 미래 사이버위협 및 사이버전에 대비하기 위해서는 전략 개발과 함께, 인식제고·교육훈련·제도·체계의 정비 등이 뒤따라야 할 것이다. 그리고 무엇보다도 우선적으로 한국 실정에 적합한 개념을 개발하고 공감대를 형성해야 할 것이다.

참 고 문 헌

[1] Steven A. Hildreth, Cyberwarfare, CRS Report for Congress, *Congressional Research Service*, The Library of Congress, June 2001.

[2] "Remarks by the President and Secretary of Defense Donald Rumsfeld Swearing-In Ceremony," *The Oval Office*, Office of the Press Secretary, Jan. 26, 2001; President Bush, "Remarks to Central Intelligence Agency Employees in Langley, Virginia," Weekly Compilation of Presidential Documents, Washington, DC, March 26, 2001; and "Secretary of Defense Donald Rumsfeld Interview on Fox News Sunday," Feb. 11, 2001, News Transcript, U.S. Department of Defense.

[3] *Navy Names Nations Posing Cyber Threats*. Defense Week. Sept. 5, 2000, p. 1. The Office of Naval Intelligence prepared the report.

[4] http://www.dtic.mil/jv2010/jvpub.htm

[5] http://www.dtic.mil/jointvision/jvpub2.htm

[6] Department of Defense. *Report of the Quadrennial Defense Review*. May 1997.

[7] V.I.Tsymbal, "Kontseptsiya 'Informatsionnoy voyny'", (Concept of Information Warfare), speech given at the Russian-U.S. conference on "Evolving post Cold War National Security Issues," Moscow 12-14 Sep., 1995 p 7. Cited in Col. Timothy Thomas, "Russian Views on Information-Based Warfare." Paper published in a special issue of Airpower Journal, July 1996.

[8] Lester W. Grau and Timothy L. Thomas. "A Russian View of Future War: Theory and Direction," *The Journal of Slavic Military Studies*. Issue 9.3 (Sept. 1996), pp. 501-518.

[9] http://www.dcaf.ch/publications/e-publications/Rusian_law_comments_engl/05A_LEIGH.pdf

[10] "U.S. Military Concerned about China's Cyberwarfare Capabilities: General," *Agence France Presse*, March 28, 2001.

[11] Military Strategic Research Center, Beijing, May 1996.
[12] Timothy Lee Thomas, *Chinese IW 101*, Inforwarcon 2000.
[13] http://www.homeoffice.gov.uk/ripa/ripact.htm
[14] Andy Jones, *The European Perspective*, InfoWarCon 2000, Sep. 2000.
[15] http://www.infoguerre.com
[16] http://www.ege.eslsca.fr
[17] http://www.zdnet.fr/actu/tech/secu/a0014768.html
[18] 박상서, 박춘식, "정보전 위협과 사례," *한국 정보보호학회지*, 제 12권 6호, 2002. 12.
[19] 박상서, 박춘식, "정보전 개념과 주요 동향," 한 국 *정보처리학회지*, 제 10권 2호, 2003. 3.
[20] Gershwin, Lawrence K, *National Intelligence Officer for Science and Technology*, Statement for the Record for the Joint Economic Committee Cyber Threat Trends and US Network Security (as prepared for delivery) 21 June, 2001, http://www.cia.gov/cia/public_affairs/speeches/gershwin_speech_ 06222001.html

〈著 者 紹 介〉

박 상 서(Sangseo Park)

1991년 : 중앙대학교 전자계산학과 공학사
1993년 : 중앙대학교대학원 전자계산학과 공학석사
1996년 : 중앙대학교대학원 컴퓨터공학과 공학박사
1996년~1998년 : 국방정보체계연구소 선임연구원
1998년~1999년 : 국방과학연구소 선임연구원
2000년~현재 : 국가보안기술연구소 선임연구원
2001년~현재 : 한국사이버테러정보전학회 이사

박 춘 식(Chunsik Park)

1981년 : 광운대학교 전자통신공학과 공학사
1983년 : 한양대학교 전자통신공학과 공학석사
1995년 : 일본 동경공업대학교 전기전자공학과 공학박사
1989~1990 : 일본 동경공업대학 객원연구원
1982~1999 : 한국전자통신연구원 책임연구원
2000~현재 : 국가보안기술연구소 책임연구원