The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 14, No. 2, pp.1-10, Apr. 30, 2014. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2014.14.2.1
JIIBC 2014-2-1

북한의 사이버전 위협분석과 대응방안 고찰

North Korean Cyber Warfare Threat and South Korean Action

김두현*

Doo-Hyun Kim*

요 약 본 연구에서는 위협이 증가되고 있는 사이버전의 위협과 사이버전에 전장 환경의 위협이 무엇인가에 대해 현재 일어나고 있는 실상을 중심으로 분석하였다. 그리고 주요 선진 국가들이 사이버전에 어떻게 대응하고 있는가에 대한 현 실상을 제시하였다. 그리고 세계 3위권의 사이버전 수행능력을 구비하고 있는 북한의 사이버전 위협과 북한의 사이버전 전략이 한국의 국가안보에 미치는 영향을 제시하였으며, 현존하는 북한의 사이버전 위협과 미래에 예상되는 북한의 사이버전 위협에 한국이 어떻게 대비하고 대응할 것인가에 대해서 연구하였다.

Abstract In this study, I analyzed the increased threat of cyber warfare and the threat of reality about what is happening around the currently. And to prepare for it, I proposed the fact how main developed countries deal with cyber warfare. Also, I presented North Korea's cyber warfare threat which is equipped with world's top 3 cyber warfare performance and the way how their strategy influence to South Korea's national security. Moreever, I studied the existing North Korea's cyber warfare threat and the way how, how South Korea deal with it and prepare to against expected threat of cyber warfare in future.

Key words : Information Warfare, Network Centric Warfare, Cyber Terror, Cyber Warfare, Internet, Information Communication System, Cyber Attack, Cyber Defence, Cyber Battlefield, Cyber Warfare Threat, Cyber Space, Cyber Warfare strategy

Ⅰ. 서 론

남한과 북한은 60년 동안 정전상태로 대치하고 있으며 북한은 지상과 해상을 이용한 침투와 무력충돌을 지속적으로 자행해 왔다. 그리고 최근에는 북한이 사이버 테러를 자행함으로써 한국을 혼란에 빠트리고 정부기관의 전산 시스템을 마비시키려는 북한의 사이버 테러가 핵 위협에 버금가는 위협으로 대두되고 있다., 그리고 북한은 핵·미사일과 함께 사이버전을 3대 전쟁수단이라 칭하며 만능의 보검으로 중요시하고 있다.

특히, 북한은 사이버 공간을 이용한 대남공작 활동으로 한국의 국가안보를 크게 위협하고 있다. 이러한 사이버전 위협이 증대되는 이유는 컴퓨터를 중심으로 하는 네트워크가 절대적인 사회기반 체계가 되었기 때문이다. 그리고 정보전(information warfare), 네트워크 중심전(network-centric warfare, network centric operation net-centric warfare, NCW), 사이버테러, 사이버전 등의 용어가 등장하였는데 정보전이란 적국에 배치된 컴퓨

*정회원, 국민대학교 정치외교학과
접수일자 2014년 2월 19일, 수정완료 2014년 3월 19일
게재확정일자 2014년 4월 11일

Received: 19 February, 2014/ Reviced: 19 March, 2014 /
Accepted: 11 April, 2014
*Corresponding Author: kimdh0024@hanmail.net
Dept. of Political Science & International Relations, Kookmin University, Korea

터와 이에 침투시킨 바이러스로 적국의 전산망 등을 공격하는 것이다. 현대적인 정보전의 개념 및 주요 대상은 적군의 첨단장비 내부에서, 컴퓨터 바이러스나 소프트웨어 해킹을 통한 적 컴퓨터의 기능마비나 파괴, 정보획득 등으로 범위가 확대되었다.

이러한 정보전의 핵심은 정보기술을 통한 군사적 지휘, 통제, 통신체계의 효과적인 통합과 운영이라 할 수 있다. 네트워크 중심전이란 네트워크를 활용한 작전수행 방식을 일컫는다. 이는 군사작전을 구성하는 탐지체계, 지휘체계, 타격체계 등의 여러 요소를 통신체계를 이용해서 효율적인 작전을 수행한다는 개념이다. 사이버테러의 개념은 개인 또는 특정집단이 자신의 정치적 목적이나 이념을 관철시킬 의도로 대중, 정부요인 또는 정부기관이나 공공기반시설 등에 대해 위협을 가할 수 있는 무기로써 컴퓨터의 사용과 이를 기반하는 사회 주요시설에 대한 물리적 공격을 의미한다고 볼 수 있다. 이와 같은 용어가 등장하게 된 배경은 컴퓨터가 전쟁지휘의 주 수단이 되어가면서 정보전 수행을 위한 네트워크 거점, 중요시설 및 무기체계에 컴퓨터 바이러스 등을 유포하거나 정보를 조작하여 적의 공격을 무력화시키는 사이버전의 위협이 등장하면서 이와 같은 용어가 등장하였다..

이러한 의미의 사이버전은 인터넷을 포함한 사이버공간에서 일어나는 전쟁으로 컴퓨터를 중심으로 연결된 네트워크 및 관련된 모든 소프트웨어와 데이터베이스를 포함하는 개념으로 누구나 수시로 활용할 수 있으며, 수많은 정보가 아무런 제약 없이 순간적으로 이동할 수 있다는 장점이 있으나 적으로 하여금 그것을 공격으로 활용하도록 함으로써 결정적인 취약점을 형성시키기도 한다.

즉 사이버전은 나의 사이버 공간을 자유로운 사용을 보장하는 동시에 상대방의 사이버 공간을 자유롭게 사용하지 못하도록 하기 위한 모든 군사적 활동을 지칭하는 용어로서 사이버전의 개념을 정리해 보면 일반적인 개념은 사이버공간에서 총성 없이 수행되는 개념으로 적군의 정보통신 체계 및 국가기간 전산 시스템을 공격해서 기능을 발휘하지 못하게 하거나 그 가치를 떨어뜨림으로써 정보우위와 특정 목적을 달성하는 동시에 아군의 정보통신체계를 보존하기 위해 수행하는 사이버상의 전쟁을 의미하며, 지금까지 정보작전 또는 컴퓨터 네트워크 작전을 더욱 확장시킨 것이다.

미군에 의하면 사이버전은 정보작전 범주 내의 컴퓨터네트워크 공격(CNA) 및 방어(CND) 그리고 정보보증(IA)으로 컴퓨터 네트워크 작전과 범세계적 정보망을 작동 및 방호하는 활동을 포함한다.

한국군의 정의를 보면 합참은 사이버전을 “컴퓨터가 합성한 가상현실의 세계(Cyber Space)와 가상인간의 영역과 같이 인공지능체계가 운용되는 공간에서의 전쟁으로서 이는 정보화 사회의 과학기술 발전을 역이용하여 취약점을 공격함으로써 물리적인 군사시스템 파괴보다 훨씬 결정적인 손실을 강요할 수 있는 총체적인 가상공간에서의 정보 마비전을 추구하는 전쟁수행방식을 의미한다”라고 정의한다. 그리고 사이버테러나 사이버전은 더 이상 가상적 상황이 아닌 현실적이며 실체적인 안보상황으로 상대국의 군사지휘체계는 물론 통신, 금융체계 등 국가의 주요기능을 무력화시키는 전쟁개념의 확대로 인식되고 있다. 따라서 사이버전이 국가방위 및 안보에 지대한 영향을 미침에 따라 세계 주요 국가들은 미래형 첨단 사이버 전쟁에 대비하여 전문인력의 양성, 사이버부대 창설 등 다양한 노력을 통해 사이버전 역량을 강화하고 있으나, 이러한 주요 선진 국가에 비해 한국의 사이버전 대비는 매우 미흡한 것이 현실이다.

본 연구에서는 북한의 사이버전의 위협분석과 대응방안을 중점적으로 제시하고자 한다. 따라서 본 연구의 구성은 제1장 서론, 제2장 사이버전 위협의 실체와 분쟁사례, 북한의 사이버전 공격양상을 제시하였고 제3장 에서는 주요 국가의 사이버전 대비실태와 전략을 알아보았다. 제4장은 북한의 사이버전 위협과 전략해 대하여 현재 실상을 중심으로 제시하였으며, 제5장은 북한의 사이버전 위협에 대비하여 한국이 어떻게 대응할 것인가에 대한 방안을 제시하였고 제6장은 결론으로 구성하였다.

Ⅱ. 사이버전 위협의 실체와 분쟁사례

1. 사이버전 전장 환경

사이버전장은 컴퓨터, 센서, 유·무선 네트워크로 구성된 국방 주요체계를 기반으로 정보수집체계, 지휘통제체계, 타격체계 등을 상호 연결하여 모든 사이버 전투수단과 체계가 포함되고 공격과 방어 등 사이버전이 수행되는 공간이라 할 수 있다. 한국군이 사이버전을 수행해야 할 사이버전장은 다음과 같은 특징이 있다.

첫째, 사이버전장은 물리적 전쟁처럼 지역적인 전·후방의 개념이 없으며 사이버공격을 감행한 나라나 단체들

과 대치하는 전선을 형성하지 않는다. 사이버공격은 전 세계에 걸쳐서 네트워크에 연결된 PC를 좀비PC로 만들어 일제히 공격대상을 공격하고 피해국 역시 공격받은 네트워크에 연결된 모든 시스템이 동시 공격을 받을 수 있다. 즉, 사이버전장에서는 적과 직접적으로 직면하는 경우가 없으며, 공격이나 방어가 거의 동시 다발적으로 이루어지기 때문에 별도의 전·후방의 개념이 없다. 또한 사이버전장에서는 공격 주체국과 피해국간의 1:1 상황에서 발생하는 것이 아니라 범세계적으로 연결된 네트워크를 통해서 공격이 진행되기 때문에 특정한 전선이 별도로 있지 않다. 최근 사이버공격에서 공격 주체자가 북한이라고 추정되는 경우에 북한과 연결된 네트워크로부터 직접 들어온 것이 아니라 중국, 아랍, 미주 등을 통해서 침투하였다. 그리고 사이버공격은 공격 근원지를 노출시키지 않기 위해서 여러 국가를 경유하여 공격하기 때문에 네트워크 연결된 모든 국가가 전장이라 볼 수 있다.

둘째, 사이버전장에서는 적·아 식별이 곤란하다. 2011년 9월 공군 작전사령부의 일부 전산망이 '웜 P2P 팔레보' 바이러스에 감염된 바 있다. 바이러스가 공군 작전사령부 전산망으로 침투한 경위는 외부업체 직원이나 내부 근무요원이 무단 반입한 장비 사용으로 감염된 것으로 예측된다. 이 사건은 사용자의 부주의로 발생한 것이기 때문에 적의 소행이라고 단정할 수 없다.

셋째, 사이버전장은 시·공간적 제한이 없다. 물리적 전쟁에서는 대륙 간 전쟁이 발발할 경우 당사국들이 무장을 탑재하고 이동하고 공격효과를 증대시키기 위해서 연합군이나 합동군의 공격시점을 조율하기도 한다. 그러나 사이버전장에서는 사이버공격자가 네트워크로 연결되어 있는 공격대상 시스템을 선정한다면 좀비 PC를 이용하여 사이버공격 수단으로 공격대상이 어디에 있던지 거리에 상관없이 공격할 수 있다. 그리고 공격자가 좀비 PC에 공격시점을 입력하거나 공격수단에 공격개시와 종료 시간을 설정할 수 있기 때문에 특정한 시간에 구애받지도 않는다.

넷째, 사이버전의 특징은 소수인원과 적은 비용으로 지구촌 어디서든 공격할 수 있으며 초보적인 공격기술로도 핵무기 못지 않은 치명적 손상을 줄 수 있다. 이러한 사이버전의 위협은 기술의 발달과 컴퓨터 네트워크에 대한 인류의 의존도가 더 커질수록 증대되고 사이버전의 범위가 과거에는 정보통신기술을 사용하는 무기 시스템이나 군사시설 등이 공격목표였다면 최근에는 금융, 전력, 수도, 항만 등 국가 기반시설을 포함한 민간분야도 사이버전의 목표가 되고 있다.

다섯째, 사이버전장은 군사정보나 안보, 전략, 작전 등 군 관련 기관들 간에 정보를 주고받는 공간으로 사용된다.

2. 사이버전 위협과 분쟁사례

사이버전은 기존에는 컴퓨터 네트워크 상에만 한정되어 존재하는 것으로 간주되었으나, 최근에는 국가 단위에서 다른 국가의 사이버 공간을 공격하는 사례가 발생하는 등 대규모화된 사이버 범죄 및 사이버전의 형태로 발전하고 있다. 특히 이러한 변화는 사이버 공격이 정치적, 군사적 목적을 가지면서 더욱 위험해지고 있고 국가안보의 결정적 요소로 격상되고 있다. 특히 미래전에서 첫 번째 전투인 "물리적 전투"가 발생하기 이전에 사이버 공간에서 일어날 것이라고 예상해 볼 수 있다. 그리고 미래에는 사이버전이 군사작전을 위한 여건조성에 적극적으로 활용될 것으로 예상되는데 주요 국가들의 사이버전 분쟁사례와 북한의 사이버전 위협의 실체를 제시하면 다음과 같다.

1. 사이버전 위협의 실체와 분쟁사례

Table 1. Cyber Warfare Threat of reality and warwatch

피해 시기	발생국가	피해내역	피해분야
1999년	NATO	NATO의 유고 코소보 사태 공중폭격 반발로 악성코드 유입, 군사작전 교란 시도	군사시설
2007년 5월	에스토니아	러시아가 에스토니아 수도 탈린 사이버 공격으로 정부기관, 은행, 통신망, 방송망 등 3주간 마비	사회기반 전반
2008년 8월	그루지아	러시아가 그루지아 전쟁간 그루지아군 작전통신 시스템 해킹으로 전쟁수행 능력 마비, 사회기반 시설 마비로 개전 5일만에 항복,	군사지휘 통제, 사회기반 전반
2009년 8월	러시아	수력발전댐 터빈 제어 시스템 장애 발전기 터빈 폭발로 75명의 인명 피해 발생	수력 발전 시설
2010년 7월	이란	스턱스넷을 통한 원자력 발전소 제어 시스템 침투, 원자력 발전소 원심분리기 기능 일부 마비	원자력 발전 시설
2011년 11월	미국	일리노이 상수도 시설 시스템 침투로 상수도 펌프 25동 시스템 파괴	수자원 시설

한국의 경우에는 아직 사이버전 차원의 위협으로 보기는 어렵지만 사이버 공간에 대한 다수의 의도적 공격 행위가 발생하였다. 2003년 1월 "슬레계 웜 바이러스"에 의한 인터넷 대란이 발생하였고, 2004년 4월 국회 · 해양경찰청 · 원자력연구소 등 24개 주요 국가 · 공공기관 PC가 마비되어 복구에 2개월이 소요되기도 하였다. 2007년 7월 에느 Daum 회원 7,000명과 2008년 2월 옥션 해킹으로 수백만의 개인정보가 유출되는 일이 있었다.

2009년 7월 7일부터 발생한 주요 국가기관과 공공기관에 대한 3차에 걸친 "분산 서비스 거부(DDos) 공격"은 좀비 PC를 쓰는 등 사이버 공격 방법이 진화하였다.

그리고 2011년 4월 12일 농협 전산망이 수일 동안 마비 되었으며 이는 북한의 소행으로 발표되기도 하였다.

2013년 3월 20일에는 KBS, MBC, YTN 방송사와 신한은행, 농협, 제주은행 등 방송•금융기관 6곳이 사이버테러로 전산망이 마비되었으며, 미래창조과학부는 3.20 사이버테러 주체자로 북한 정찰총국을 지명하였다.

그리고 2013년 6월 25일 청와대 홈페이지 및 주요 정부기관에 사이버 공격으로 피해 발생, 웹 사이트 변조 및 분산 서비스 거부(DDos) 공격, 신상정보 유출 등 악성행위가 발견되었다.

3. 사이버공격의 양상

사이버전 위협의 실체와 분쟁사례를 보면 사이버 공간만이 갖고 있는 취약점을 공격함으로써 물리적인 파괴보다 더욱 심대한 손실을 강요하고 있다. 그리고 사이버 공격은 매우 정교하고 지능적으로 진화하고 있으며 최근의 사이버 공격의 사례를 분석해 본 결과 특징은 다음과 같다.

첫째, 정밀유도무기체계 기능을 갖는 사이버 무기체계를 활용한다. 2010년 이란의 부셰르 원자력 발전소에서 발견된 스턱스 넷은 국가 및 산업의 중요 공정 프로세스에 많이 사용되는 독일 지멘스사의 PCS7 시스템을 목표로 프로그램이 가능한 논리제어장치의 코드를 변경함으로써 시스템 제어권을 획득하여 국가 및 산업의 중요 기반시설을 파괴하는 매우 정교한 군사적 수준의 사이버 무기체계이다. 스턱스 넷이 오랜 시간동안 활동하면서도 발견되지 않았던 이유는 공격대상, 공격경로, 공격절차, 기능 등에서 기존의 웜과 전혀 다른 양상으로 진화했기 때문이다.

둘째, DDos 공격의 진화이다. 3.20 사이버테러 양상은 기존의 DDos 공격 기법보다 한 차원 진화된 공격 양상을 보여준다. 3.20 사이버테러 공격과정은 웹서버 해킹, 웹서버 접속 및 악성코드 감염, 1차 C&C 서버 접속 및 정보유출, 추가 악성코드 다운로드, 2차 C&C서버 접속, 업데이트 파일 변조 및 배포 등으로 진행되었다. 즉, 사전에 공격목적과 공격대상을 선정하는 등 치밀하게 준비하였으며, 공격 종료 후에는 감염된 자료를 삭제하도록 함으로써 역 추적을 피할 수 있게 하였다.

셋째, 침입경로의 다양화이다. 현재 네트워크와 시스템에 관련된 다양한 디바이스가 개발되고 있으며 대중화되고 있다. 이에 따라 디바이스로 인해 악성코드가 유포되는 경우가 지속적으로 발생하고 있고, 유포된 악성코드는 사이버공격의 시작점이 된다. 또한, 다양한 어플리케이션을 통해 악성코드가 유포되고 있다. 그리고유포된 악성코드 기능에 따라 개인정보를 유출하거나 DDos 공격을 위한 좀비PC가 되어 사이버공격을 수행하기도 한다.

넷째, 사이버공격 기술의 융합이다. 융합은 이전부터 진행되어 왔으나 최근에 들어서는 융합된 사이버공격 기술의 장점만 추려내어 변종이 발생한다. 이러한 변종은 또 다른 형태의 사이버공격 원천기술이 되며, 새로운 변종이 개발되어 보안시스템으로부터의 탐지를 어렵게 만든다.

Ⅲ. 주요국가의 사이버전 전략

주요 선진국들은 적은 비용으로 최대 효과를 거둘 수 있는 비대칭 전력의 중요성을 인식하여 사이버전에 대한 기술적·제도적 준비를 하고 있다. 그리고 사이버전을 수행하는 사이버부대와 해커부대를 공식화하고 있으며 사이버무기들도 개발하고 있다. 사이버전에 대비한 미국, 영국, 중국 등 세계 주요국가의 대응태세를 보면 다음과 같다.

1. 미국

미군은 2009년 6월 23일 미 전략사령부(U.S. Strategic Command) 예하에 사이버사령부(Cyber Command)를 창설하여 2010년 5월 21일부터 기능을 수행하고 있다.

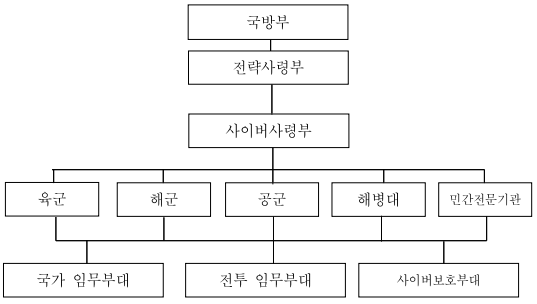
미군의 사이버사령부는 기존의 "지구네트워크작전 합동임무부대"(The Joint Task Force for Global Network Operations: JTF-GNO)와 네트워크전의 합동기능구성군

사령부(Joint Functional Component Command for Network Warfare: JFCC-NW)를 통합하였다., 그 예하에는 육군 사이버사령부(Army Forces Cyber Command, ARFORCYBER), 제 24공군(24 Air Force, 24th USAF), 함대 사이버사령부(Feet Cyber Command, FLTCYBERCOM), 해병대 사이버사령부(Marine Corps Forces Cyber Command, MARFORCYBER)가 편성되어 있다.

미국의 사이버전 임무를 수행하는 부대의 조직은 다음 그림과 같이 요약 할 수 있다.

2. 미국의 사이버전 부대 조직도

Table 2. American Cyber Warfare unit organization chart



국방부 예하 전략사령부가 사이버사령부를 지휘・통제하며, 사이버사령부는 지시에 따라 사이버작전을 수행하고 각 군의 사이버작전을 조정하며, 국방부의 정보통신 체계 운영과 방어를 지휘한다. 그리고 각 군의 사이버사령부는 각 군의 정보네트워크를 운영・유지・방어하며, 지시에 따라 사이버전을 수행한다.

전략사령부 예하 사이버사령부는 국방부가 운영하는 정보통신체계의 운영과 방어를 담당하며, 상위부서의 지시에 따라 전 사이버영역에 대한 군 사이버작전을 수행하고 미국 및 동맹국의 사이버영역에서의 작전 활동의 자유를 보장하고 적의 활동은 억제하는 역할을 수행한다. 국가 임무부대는 국가 주요기반시설(전력통제시설, 수자원 공급 시설 등)을 운영하는 정보통신 시스템을 보호한다. 전투 임무부대는 사이버작전 임무를 수행하며, 자국에 대한 잠재적인 위협을 내포한 단체나 나라에 대해서 실제 전쟁이 발발하기 전에 적의 지휘통제시스템을 사전에 무력화 한다. 사이버 보호부대는 국방부가 운영하는 정보통신체계 보호 및 보안성 강화 임무를 수행하고 국방부 정보네트워크에 관한 작전과 방어를 지도하고, 지시에 의하여 모든 영역에서의 활동을 보장하면서 미국과 동맹국이 사이버공간에 자유롭게 접근하도록 보장한 상태에서 적에게는 그러한 것을 거부하기 위한 모든 형태의 군사적 사이버공간작전을 수행할 준비를 하기 위한 활동들을 계획, 조정, 통합, 동시화 및 시행"하는 임무를 수행하고 다른 국가의 암호화된 통신을 분석하고, 자국 통신을 암호화하여 보호하는 기능을 수행한다.

미국 오바마 정부는 국가의 핵심정책으로 지정한 사이버 보안과 관련하여 전반적으로 검토하였는데 주 내용은 사이버 보안을 위한 연구활동 강화와 사이버전을 위한 조직, 훈련, 준비, 방어 개념 등을 제시하고 있다. 또한 미국은 사이버공격을 전쟁행위로 규정하고 있고 이에 대한 사이버 공격의 자위권(Right of Self-Defence)을 가질 수 있음을 천명하고 있다.

2. 영국

2013년 초에는 정보기관과 민간 보안 전문가로 구성된 사이버 보안통제센터인 퓨전 셀(Fusion Cell)을 설립하였다. 이 조직은 금융, 국방, 에너지, 통신, 제약 등 5개 분야에서 160개 업체가 참여하여 사이버위협에 기업과 정보기관이 공동으로 대응한다.

영국 정부와 영국군을 위하여 사이버공간작전을 담당하고 있는 부서는 정부통신사령부(GCHQ: Government Communications Headquarters)이다. 이 사령부는 1919년부터 창설되어 영국 정부와 영국군에게 통신정보와 그에 대한 보안대책을 강구하는 기관으로서 예하에 통신전자보안단(CESG : Communications-Electronics Security Group)을 보유하고 있는데, 이 조직에서 암호해독과 함께 사이버공간작전에 관한 사항을 처리하고 있다. 영국의 사이버공간작전을 담당하고 있는 또 다른 부서는 "사이버보안 및 정보 보증실"(OCSIA: Office of Cyber Security & Information Assurance)로서, 영국의 모든 사이버안보 및 정보보호에 관한 지침을 하달하며, 관련된 활동을 조정하는 역할을 수행한다. 그리고 영국군은 2010년 10월 국방 사이버 작전단(Defence Cyber Operations Group)을 설치하였고, 사이버보안 시험장(cyber security test range)을 설치하여 사이버전에 관한 다양한 시험을 실시하고 있다.

그리고 주요 국가기반시설과 정부기관을 대상으로 사이버위협을 가하는 공격자들에게 대응하기 위해 방어 위주가 아닌 공격 위주의 방어수단으로 사이버 무기체계를

개발하고 있다. 아울러 사이버공격 관련 국가 위기상황이 발생할 경우에 영국군을 지원하기 위한 사이버예비군을 창설하겠다고 발표하였다.

3. 중국

중국은 최첨단 무기체계 및 핵무기, 테러와 함께 사이버전 능력을 현대전의 3대 요소라고 판단하여 정보전 역량확대에 막대한 투자를 하고 있다. 중국은 전자전대응책을 담당하는 중국군 총참모부의 제4국이 사이버공간에 대한 공격임무를 수행하고 있는 것으로 파악되고 있다. 이 부서에서 사이버공간에 관한 모든 작전부대와 연구기관을 통제하고 있고, 그 인원이 130,000명 이상으로 다양한 민간 해커단체들과도 유기적으로 협조하고 있는 것으로 분석되고 있다.

그리고 최근에는 사이버공간에 대한 중국의 활동이 급격하게 증대되고 있으며, 2010년 4월 8일 중국 국영 "China Telecom"17분 동안 대규모 오류 정보를 유통시켜 미 상원, 미 국방부 및 각 군, 그리고 미국의 500대 기업 관련 사이트에 영향을 준바 있다고 폭로된 바도 있다.(BBC News March 11, 2011). 한국에 대한 다수의 인터넷 해킹 활동도 중국에 의하여 행해지고 있다고 믿어지고 있다. 특히 중국군이 적국의 컴퓨터 시스템과 네트워크를 공격할 수 있는 바이러스나 우군 컴퓨터를 보호할 수 있는 전술과 수단을 개발할 수 있는 정보전 부대도 설립한 것으로 식별되었다. 2005년 이후에는 공세적 컴퓨터 네트워크 작전 훈련도 실시하고 있는 것으로 확인되었다

Ⅳ. 북한의 사이버전 위협과 전략

1. 북한의 사이버전 위협

북한은 유사시 모든 첨단정보기술 및 장비들을 총동원하여 적의 1차적 전자정보공격으로부터 아군의 지휘자동화 능력 및 명령지휘 통신체계를 보존하고 이에 상응한 적의 능력을 파괴하며, 아울러 전쟁수행에 있어 모든 목표들을 성과적으로 달성하기 위해 정보전 수행능력을 배가하고 있다.

특히, 북한의 국방위원회가 직접 지휘하는 정찰총국이 북한의 사이버전의 핵심 부서이며 그 휘하에 해킹과 사이버전 전담부대인 전자경찰국 사이버전지도국(121국)이 편성되어 있다. 북한은 노동당 산하에 7개의 해킹조직 1700여명과 4200여명의 대규모 사이버전 지원조직을 갖추고 있으며, 현재 세계 3위권의 사이버전 대국으로 평가받고 있다. 북한은 80년대 중반 이후 김일성 군사대학에서 해킹 전문인력을 매년 수 백명씩 배출하여 정찰총국, 지휘 자동화국 등의 예하부대에 배치하고 있다.

북한은 1990년대 초반부터 사이버전사를 양성함과 동시에 다수의 고성능 컴퓨터를 중국과 해외에서 대량으로 구입하였고, 인민무력성 정찰국 예하로 있던 사이버부대 121소를 별도의 사이버전국으로 격상시켜 정찰총국에 직속시켰다. 이 정찰총국의 사이버전국이 바로 한국의 기관들에 대한 사이버 테러와 공격, 민간기관과 단체들에 대한 해킹 및 인터넷 대란을 일으키는 작전을 총괄하는 총본산 역할을 수행하고 있다고 판단된다. 그 외에도 "중앙당 35실 기초자료실", "총참모부 적공국 204소" 등이 설립되고 있고, 김일성 종합대학, 김책 공업종합대학, 평양컴퓨터 대학교 이과대학, 미림대학 등에서 최고의 사이버 전사들을 육성하고 있다.

그리고 2013년 3월 20일에 주요언론사와 농협 등 금융기관 전산망을 마비시켰으며, 2014년에는 북한의 사이버 공격이 정교화 되고 가속화 될 것이고 사이버 공간을 이용한 대남공작 활동은 한국의 군사안보를 크게 위협할 것으로 예상된다.

2. 북한의 사이버전 전략

북한의 사이버 위협에는 사이버 심리전, 사이버 정보수집, DD_{OS} 공격을 포함한 사이버 테러, 사이버 통일전선 등이 있으며 이를 활용한 전략은 다음과 같다.

첫째, 사이버 심리전이다. 북한은 사이버 공간을 통해 자유민주주의 체제를 뿌리 채 흔들기 위해 각종 악성 루머와 유언비어를 퍼트리는 등 여론 조작을 통해 한국의 국론을 분열시키려는 것이다. 북한은 우리 국민의 마음을 공략해 나라 전체를 분열과 혼란으로 몰아넣으려 하고 있으며 친북 인터넷사이트 100여개의 망을 구축해 놓고 대남심리전을 펼치고 있다.

둘째, 사이버 정보수집이다. 과거에는 북한이 간첩을 통해 얻을 수 있었던 정보를 평양이나 해외 거점의 책상에 앉아서 한국의 주요국가 기관망, 공공망, 포털망 등을 해킹함으로서 신속하고 손쉽게 수집할 수 있게 되었다. 특히, 우리 군에 대한 해킹 건수는 2008년 2,800만 건, 2009년 3,400만 건, 2010년 상반기에만 7,600만 건이 넘었

고 해킹을 통해 유출된 군사기밀도 1,700여 건에 달하는 등 군에 대한 사이버 위협은 날로 높아가고 있다.

셋째, DDos 공격 등 사이버 테러 문제는 북한은 2009년 국내 35개 주요 전산망을 공격한 이른바 '7.7 사이버 대란'을 일으켰고, 2011년 3월 국내 40여개 공공전산망에 대해 DDos 공격을 감행한 바 있다. 2011년 4월에는 농협 전산망을 마비시킴으로써 그것을 복구시키는데 18일이나 소요된 적도 있다. 현재까지 발생한 사이버 테러는 공격진원지의 IP주소를 파악한 결과 북한군 해킹요원들이 한 짓으로 판명이 났지만 중국내 주소를 사용했기 때문에 북한의 소행이라고 단정 짓기가 어렵다. 북한은 사이버 테러와 동시에 위성위치 정보시스템 교란을 통한 전자전도 감행했다. 그들은 2008년 8월 을지훈련동안 GPS 신호교란을 시도했고, 2011년 키 리졸브 훈련 동안에도 교란신호를 송출했다. 2010년 11월 연평도 포격당시 우리군의 대포병 레이더가 제대로 작동하지 않은 것도 그들의 GPS 교란 때문인 것으로 알려지고 있다.

Ⅴ. 북한의 사이버전 위협대비 대응방안

1. 한국의 실태

주요 선진국들은 사이버공격에 대비하여 새로운 개념의 국가사이버 안보 전략을 강화하고 있으나 한국의 사이버 안보 정책은 매우 미흡한 것이 현실이다. 한국은 2003년 1월 25일 인터넷 대란이 발생하자 "국가사이버테러 대응체계구축 기본계획"을 수립하여 국가정보원에 국가사이버안전센터(국가, 공공분야), 국방부에 국방정보전대응센터(국방분야), 정보통신부에 인터넷 침해사고대응센터(민간분야)를 설치하였고, 국가정보원이 총괄 기능을 수행하도록 체계를 갖추었다. 국가정보원은 국가사이버위기 경보체계를 관심(Blue), 주의(Yellow), 경계(Orange), 심각(Red) 등 4단계로 구분하고 각 수준별로 적절한 수준에서 대응하도록 하고 있다. 그러나 국가정보원 자체가 실행력을 보유하고 있는 것이 아니기 때문에 경고나 조정 정도에 그칠 수밖에 없다.

그 외에도 한국에서는 한국인터넷진흥원(KISA: Korea Internet & Security Agency), 금융 결재원 금융정보 보호센터(FISC:Financial Information Security Center) 등에서 사이버공간에 대한 업무를 수행하고 있으나 담당분야에 대한 정보보호 활동에 국한되고 있다. 국방부의 경우에도 군 전산망의 안전을 보장하거나 분산서비스방해(DDos) 공격과 같은 국가 사이버위기 발생 시 민 · 관 · 군 공동 대응을 보장하기 위한 수준을 벗어나지 못하였다. 2000년 1월 국방부 및 각군 본부에 사이버전 침해사고 대응팀(CERT: Computer Emergency Response Team)을 설치하였고, 2003년 인터넷 대란 이후에 국군기무사령부 내에 국방정보전 대응센터를 설치하였다., 2005년에는 작전사령부 및 군단급까지 CERT를 구축하여 사이버위협에 대응하고 있다. 2010년 1월에 사이버사령부를 창설하였으나 이 사령부는 국군기무사령부에서 수행하던 보안관제 및 침해사고 조사업무를 이관받아서 출범을 하였으나 정보본부 예하에 창설됨으로써 인터넷을 통한 정보수집이나 정보보호에 국한될 수밖에 없었다.

한국은 7.7 DDos 사건을 계기로 군차원의 사이버 안전의 중요성을 감안하여 사이버사령부를 창설하였고 2011년 7월 1일부로 국방부 직속으로 사이버사령부를 격상한 것은 사이버공간이나 사이버 공간작전과 관련한 긍정적인 조치라고 할 수 있다. 그러나 아직은 역량이 부족한 것으로 평가하고 있다. 그러나 전문성을 구비한 군 사이버요원을 양성하기 위해 2012년부터 고려대학교 정보보호대학원에 30명 규모의 사이버국방학과를 신설하여 사이버전사들을 육성하고 있으며 학교 졸업후에 소위로 임관하여 7년간 복무 뒤 장기복무를 하거나 대기업, 밴처기업, 국정원, 검찰, 청와대 등 국가기관에 특별채용 하고자 하는 정책과 국방부와 미래부가 한국형 탈피오드 제도(이스라엘 과학기술 엘리트 장교 육성 프로그램)을 도입해서 올해부터 매년 20명씩 과학기술 전문사관을 모집하여 사이버정보보호 인력 육성을 추진하는 계획과 사이버위협에 대비해서 한미공동 대응을 위해 2014년 2월 7일에 실시한 제 1차 한미 국방 사이버정책 실무협의회 개최 등은 미래의 사이버전 위협에 대응 할 수 있는 효율적인 정책으로 평가 할 수 있으나 사이버전에 대비한 범국가적 정책마련과 군 차원의 대책이 시급한 현실이다.

2. 한국의 대응 방안

현재 북한의 사이버전 위협에 대비한 한국의 대응태세는 매우 미흡하다. 특히, 군 관련 사이버전 대비태세의 문제점은 국방 정부보호정책수립 집행의 일관성 부족 및 최신 정보보호기술과 해킹, 바이러스 등 사이버전 위협에 대응하기 위한 실무적인 내용이 극히 미흡한 상황이

다. 따라서 이에 대응하기 위해서는 국가 수준에서 사이버전과 관련된 제반 문제점을 정확하게 식별해서 그것을 구현하기 위한 정부차원의 체제와 역할분담을 제도화할 필요가 있고, 사이버전을 예방 및 억제시키기 위한 대비책을 강구해야 하고 어떠한 상황이 발생하더라도 효과적으로 대응할 수 있는 체제를 구비할 필요가 있다. 현 시점에서 필자가 생각하는 사이버위협에 대비한 한국의 대응방안을 제시하면 다음과 같다.

가. 사이버 공격 및 방어능력 향상

사이버전 공격 및 방어기술은 매우 중차대한 문제이다. 왜냐하면 사이버 공간에 대한 방호나 안전의 확보에만 사고를 국한시켜서는 곤란하다. 어느 경우도 방어로는 승리를 보장할 수 없기 때문이다. 공격이 최상의 방어라는 말처럼 공격을 시도하는 적의 사이버공간을 사전에 무력화시킬 수 있는 능력을 구비하고 있어야 한다. 사이버공간에서의 방어와 함께 공격작전에 관한 사항도 충분히 분석하고, 그에 필요한 수단과 방법을 개발해 나가야 한다. 그리고 사전에 예방 및 억제할 수 있는 수단으로 사이버공격 수단을 확보할 필요가 있다. 따라서 사이버전의 중심인 합참의 합동지휘통제 시스템을 중심으로 각군의 C4I체계 및 연합사 C4I체계가 연동될 수 있는 기반체계 구축을 위해 합참에 사이버전 공격부대를 창설 또는 사이버사령부에 기능을 수행할 수 있도록 사이버공격을 위한 인력을 확보하는 방안도 검토가 필요하다.

나. 사이버작전사령부의 영역 확대 및 실행부대 창설

사이버사령부는 사이버전, 특히 공격작전에 관한 제반 사항을 연구 및 적용할 수 있도록 그 기능을 확대할 필요가 있고 사이버전을 수행할 수 있는 전문부대 및 요원들을 조직, 충원, 훈련할 수 있어야 한다.

그리고 합참에 사이버위기에 대한 전·평시 사이버전을 지휘, 통제할 수 있는 사이버 지휘통제소를 구축해서 평시에 국방 CERT를 지휘통제하고 군내 사이버테러 발생시에 대응 업무를 총괄하고, 전시에는 정부작전 상황하에서 공세적·수세적 사이버전 지휘통제업무를 수행하면서 사이버전 종합상황실을 운영하는 임무를 수행할 수 있는 체계를 갖추어야 한다. 또한, 사이버전을 전담 대응하는 사이버군을 창설해서 공세적 사이버전 업무를 담당하는 컴퓨터 네트워크 공격부대와 수세적 사이버전 업무를 담당하는 컴퓨터네트워크 방어부대를 신설하는 방안도 검토가 필요하다.

그리고 사이버전의 원할한 수행을 위해 미군과도 긴밀한 협조체제를 구축할 필요가 있으며 사이버전에 대한 교리를 정립하고, 필요한 사항들을 작전계획에 반영하여 통상적인 군사작전과 조화를 이루도록 조치를 해야 한다.

다. 국방 사이버전 연습체계 발전

현재 군 사이버전 대응 연습체계를 분석해 보면 몇 가지 문제점이 있다. 첫째, 사이버전 대응연습이 단편적으로 1년에 한번 합동참모본부 주관하에 실시하기 때문에 훈련시 기본목표인 “숙달”이 미흡하고, 합동참모본부 주관하에 인포콘(INFOCON) 연습이든 국정원 주관하에 실시하는 정부통합훈련이든 다양한 상황에서의 연습이 진행되지 않고 전군적 규모 또는 범정부적으로 실시하기 때문에 연습 및 훈련의 기본목표인 “숙달”에 이르는 실질적인 성과를 달성하지 못하는 것이 현실이다. 따라서 이러한 문제점을 고려하여 체계적인 사이버전 연습체계에 대한 개선방안 보완이 필요하다.

둘째. 사이버전 연습을 효과적으로 수행하기 위해서는 연습기획 및 통제단을 구성해서 계획수립이 잘 되어야하고 연습통제가 잘 이루어지도록 해야 한다.

사이버전 대비연습을 위해서는 계획수립 과정에서 연습계획을 수립하여 연습시나리오와 실제 연습시 수행하는 여러 가지 조치사항을 사전에 계획해야 한다.

셋째. 사이버전 훈련연습 유형은 실제 침해 상황부여 없이 페이퍼워크(paper work)만 실시하는 탁상연습과 실제상황을 혼합해서 연습하는 방법으로 페이퍼워크 및 각본에 의한 가상 상황을 부여해서 연습하는 방안과 전군 실제상황 연습시 사전협의 없이 실제 긴급 상황을 부여해서 실질적인 대비태세가 이루어질 수 있도록 검증해야 한다.

넷째. 사이버전 연습 실시는 연습 통제단에 의해 주관되고 통제 되어야 한다. 모든 연습 진행은 철저히 연습계획에 나와 있는 시나리오대로 통제단에서 주관하여 진행한다. 평가관은 참가부대가 사이버 공격에 어떻게 대응하는가 에 대한 과정을 관찰하여 평가를 해야 한다.

라. 전문 인력과 기술 발전

사이버공간작전을 위한 인력의 확보에 있어서 중요한 사항은 최고 전문가를 양성하고자 노력해야 한다는 것이다.

사이버전 기술개발을 위한 정보통신 기반시설을 관장

하는 기관을 중심으로 기금을 조성하는 방안과 국방부의 사이버전 기술연구개발을 위한 국방투자비의 일부를 활용하기 위한 제도를 정립하는 방안도 검토가 필요하다.

그리고 민·관·군 소요 인력충원 방안으로 "사이버전문대학원" 개설, 고려대에 설치되어 있는 사이버국방학과를 확대하여 4년제 및 2년제 대학과 전문계 고등학교에 국비로 교육할 수 있는 사이버 국방학과를 점차적으로 확대하는 방안과 군 인력 충원방안으로 정보보호 분야의 전공자 특채를 통해 국방부 및 각군 CERT 조직을 강화하고 각 군 대학 및 국방대 사이버전문 인력 양성과정 개설과 전산 특기 간부 및 병사를 정부기관 및 각 군 부대에 활용하는 방안도 검토하고 조속한 시일 내에 추진해야 한다.

마. 기타 조치사항

사이버전의 성공을 위해서는 국제적인 협력도 중요하다. 왜냐하면 국경에 의하여 구속받지 않는 사이버공간을 특정 국가가 단독으로 방어한다는 것은 불가능하기 때문이며 동맹 및 우방국과 긴밀하게 협력함으로써 노력과 비용을 절약할 수 있기 때문이다. 그리고 사이버전과 관련된 다양한 법률들을 단일법으로 통합하는 것도 중요하고 국가적 통제기구를 설치하여 사이버전의 효과적 수행을 위한 관련 부서 간의 협조체계, 정보의 공유, 사이버 테러 위험수준 및 단계별 대응 요령, 국제협력 및 공조체제 등을 총괄할 수 있도록 정부 차원의 컨트롤 타워를 설치할 필요가 있다.

Ⅵ. 결 론

사이버전은 기존의 전쟁양상과 전혀 다른 차원의 전쟁 개념으로 지금 이 순간에도 사이버전과 사이버테러와 같은 '보이지 않는 조용한 전쟁'은 하루도 쉬지 않고 계속 전개되고 있다. 그러나 지금까지와 같은 사이버공간의 보안이나 정보보호 활동만으로는 그러한 위협에 제대로 대응하기가 어려운 것이 현실이다. 따라서 지상, 해양, 공중, 우주에 이은 다섯 번째의 공간으로 간주될 정도로 사이버공간의 비중이 커지고 있는 현 시점에서 사이버전과 사이버테러에서 패배할 경우 많은 것을 잃을 수 있다는 사실을 명심해야 할 것이다.

미국의 경우 국방부 차원에서 사이버전 수행과 대비에 대하여 장기적이면서 체계적인 비전을 정립하였을 뿐만 아니라, 군 전략사령부 예하에 사이버사령부를 설치함으로써 이미 군사작전차원에서 접근하고 있다. 중국과 북한도 전력의 열세를 사이버공격과 같은 비대칭적 수단으로 만회하고자 노력하고 있다. 이에 비해 한국은 아직도 정보보호 차원으로만 사이버공간을 인식하고 있는 상태로서, 근본적인 인식의 전환과 정책적 발전이 요구되는 상황이다.

특히, 북한으로부터 국방네트워크가 사이버 공격을 받아 전쟁수행 능력을 상실하게 되는 경우를 가정하여 이에 대한 대비도 철저히 해야 하고 더 큰 위협이 가시화되기 이전에 국가차원에서 필요한 사항을 심도 있게 분석해서, 사이버전에 대한 정책 및 억제전략을 심층적이고 실효성 있게 마련해야 한다.

References

[1] Hwi Rak Park, North Korea Nuclear Threat and Action, 2013
[2] Jin Seok Kang, Losig and Philosophy of Modern warfare, 2012
[3] Jin Seok Kang, Clausewitz and Korea, Arms and Gown, 2013
[4] Kil Hyun Nam, Cyber Terror, National Security, 2002
[5] Security Engineering thesis, 2013
[6] No Hoon, Je Wook Lee, Emergence of Cyber Warfare, Effect and Direction of reaction, 2001
[7] Sang Ho Lee, Utility of Cyber, information Warfare in Military Strategy, 2010
[8] Hong Kook Park, Ki Cheong Jeon, Decision Making Supporti System, 1999
[9] The Headquarter of the Army, Field Manual, Cyber Warfare, 2002
[10] Ecward Watz Information Warfare Principles and Opewrations, 1998
[11] Jung Ho Eom Sung Su choi, Tai-Myoung chung, An Introdction of cyber warfare Honghrohers, 2012
[12] NSHC. 6.25 Cyber terror Analysis Cyber terror

Analysis Reports, 2013.
[13] Jung Ho Eom. Sung Su Ohoi, Tai-Myung, An Introduction of cyber warfare, Hang Publishers, 2012
[14] Ssang kul Lee. US DoD, Cyber Command published an increase of Cyber Secuntiy Experts , Internet & Security Weekly, 2013.
[15] Michael N. Schmitt et al, Tallinn Manual on the international law applicable to cyber warfare, NATO CCDEOE, 2013.

소개

두 현(정회원)

- 1986년 2월 : 건국대학교 경영학과 석사
- 2002년 2월 : 전남대학교 행정학 석사
- 2012년 3월~현재 : 국민대학교 정치외교학과
- 주관심분야 : 안보전략, 사이버전