군의 사이버전 대응체계 현재와 미래

국방대학교 남길현

1. IT 강군건설과 사이버 위협

현대전은 고도로 발달된 C4I시스템(Command Control Communication Computer and Intelligence System)을 운용하면서 최고지휘관으로부터 말단 병사들에 이르기까지 관련정보를 공유함으로써 전투력을 극대화할 수 있도록 하고 있으며, 무기체계와 연동된 실시간 정밀타격시스템은 정보통신기술과 밀접하게 연관되어 있다. 이제 선진국들은 모두가 국방력의 핵심요소는 정보기술력이라는 판단하에 IT 강군을 육성할 수 있는 중장기 전략을 수립하고 예산확보와 전문인력양성에 힘을 기울이고 있다.

특히 정보전의 개념이 네트워크중심전(Network-centric War)으로 진행하면서 지휘체계의 중추신경역할을 담당하고 있는 컴퓨터와 유무선통신망의 중요성은 더욱 비중이 높아지고 있다. C4I시스템은 유무선통신망을 통하여 연결된 정보시스템의 결집된 형태를 기반으로 하고 있으므로 중요 네트워크를 마비시키고 컴퓨터시스템을 공격하여 C4I시스템의 기능을 파괴하는 사이버 공격은 IT 강군건설을 지향하는 군 전략에 심대한 위협요소로 평가된다.

사이버 위협은 크게 군 정보통신망에 대한 공격과 내부 컴퓨터시스템에 대한 공격으로 구분할 수 있다. 다시 정보통신망에 대한 공격은 도청(수동적 도청과 능동적 도청)과 네트워크 마비공격으로 나눌 수 있다. 군은 통상적으로 전용선 기반의 네트워크를 운용하기 때문에 상용의 인터넷망보다는 비교적 안전하다고 할 수 있으나 군의 네트워크 규모가 크기 때문에 공중망과 대등한 위협을 대비하여야 하며, 최근에는 다양한 필요성 때문에 대부분의 부대에서 인터넷망을 운용하고 있기 때문에 더욱 도청과 서비스 거부공격과 같은 네트워크 공격에 만반의 준비를 해야 할 것이다.

또한 내부 컴퓨터시스템에 대한 사이버공격은 해킹과 바이러스를 비롯하여 트로이 목마와 같은 악성코드를 이용한 공격으로서 주요정보를 변조 또는 유출하거나 정보와 컴퓨터시스템 자체를 손상시켜 기능을 무력화시킴으로서 군사력을 약화시키는 것을 일컫는다. 이와같은 내부 컴퓨터시스템에 대한 공격도 전용선을 사용하는 군 전산환경에서는 공중망과는 분리되어 있기 때문에 비교적 안전하다고 할 수는 있지만 내부 불순자의 위협을 무시할 수 없고 전용선이라도 민간회사의 회선을 임대하여 사용하기 때문에 보안의 중요성을 강조하고 있는 군에서는 더욱 치밀한 대비책을 강구하여야 한다.

최근의 정보화 역기능 동향을 살펴보면 해킹과 바이러스 기술은 더욱 급속도로 지능화·광대역화되고 있으며, 대상도 특정 개인, 회사, 기관 등을 가리지 않고 무차별적으로 확산되고 있다. 이들의 목적도 개인의 이익추구 뿐만 아니라 특정 집단이나 정치적 의도를 관철시키거나 국가적 목적을 갖고 수행하고 있다고 볼 수 있다.

우리 군도 지식정보화시대에 부응할 수 있는 IT 강군을 건설하기위해 중장기 국방정보화계획을 수립하여 단계적으로 진행하고 있다고 본다. 그러나 사이버전의 개념은 비교적 최근에 형성되었기 때문에 아직까지는 군 정보시스템을 안전하게 운영하기 위한 대응체계가 완전하게 정착되었다고 보기는 어려운 실정이다. 재래식 전쟁에서는 전시와 평시가 확연히 구분할 수 있으며 군의 역할도 명확하게 구분되어 있으나 사이버전은 전시와 평시를 구분하기 어려우며 전쟁영역도 불분명하다고 볼 수 있다. 따라서 군의 사이버전 대응체계는 평시에 민관군의 협력체계를 굳건히 하고 전시에는 아측의 정보시스템을 보호할 뿐만 아니라 상대방의 정보시스템을 무력화시킬 수 있는 역량을 구비하여야 한다. 아무리 군 정보시스템이 확산되었다고 하더라도 정보화 역기능에 대한 대비책이 완전하지 못하면 정보화는 사상누각이 되거나 유사시에 오히려 군 전력을 약화시키는 악영향을 초래할 수 있을 것이다.

본고에서는 사이버전에 대한 개념과 외국의 동향을 간단히 살펴보고 현재 우리 군의 사이버전 대응체계를 고찰해봄으로써 정책 및 제도적인 측면에서 IT 강군을

지향하는 군 정보시스템의 정보보호분야와 사이버전 대응체계 발전방향을 모색해 보고자 한다.

2. 사이버전의 범위와 외국군 동향

2.1 정보전과 사이버전

미 국방대 교수인 Libiki는 1996년 그의 저서인 "정보전이란 무엇인가(What is information warfare?)"에서 정보전을 지휘통제전, 심리전, 전자전, 경제정보전, 사이버전(Cyber Warfare), 해커전, 군사정보전 등으로 분류하여 사이버전을 정보전(Information Warfare)의 한 형태로 분류하였고, 다시 사이버전을 정보테러리즘, 시뮬라전, 깁슨전, 시멘틱 공격의 4가지 형태로 나누어 해커전과는 다른 개념으로 구분하였다. 그러나 한국군과 미군에서 사용하고 있는 개념이 보다 현실적이기 때문에 여기에서는 정보전과 사이버전의 개념을 함께 살펴본다.

2.1.1 한국군과 미군의 정보전 정의

미군은 1995년에 합동교범에 정보전의 정의를 다음과 같이 공식적으로 기술하였다. "정보전이란 아군의 정보체계를 적의 파괴, 조작, 탈취행위로부터 무결성을 보존하고 정보우위를 확보하며 동시에 적의 정보 체계와 절차를 파괴, 조작, 탈취하기위해 취해지는 행위를 말한다." 즉, 정보전을 정보우위 달성을 위한 정보체계 및 절차에 대한 보호 및 공격 행위로 정의하였다. 이후 미군은 1998년 합동교범 3-13 〔정보작전〕을 발간하면서 새롭게 정보전을 아래와 같이 정의하였다. "정보전이란 특정 적 또는 적들을 대상으로 특정 목적을 달성하거나 달성을 지원하기 위해 위기시나 분쟁시에 수행되는 정보작전이다." 여기서는 정보전을 정보작전에 포함시키면서 그 범위를 한정하였다. 그러나 동 교범에서는 정보작전의 부분집합으로의 정보전에 대한 보다 자세한 설명과 기타 정보작전의 요소작전들과의 관계는 추가적으로 명시하지 않았다. 따라서 미군의 정보전에 대한 정의는 정보를 기반으로 하는 폭 넓은 의미의 전쟁(광의의 정보전)을 의미하는 정보전과는 큰 차이점이 있음을 알 수 있다.

이에 반해 우리 합참은 광의적 의미의 정보전을 그대로 수용한 것으로 보이며 다음과 같이 기술하였다. "정보전은 정보우위를 달성하기 위해 수행되는 포괄적이고 전반적인 국가총력전 차원의 개념으로서 군사 및 비군사 분야의 정보 및 정보체계의 영역을 포함하고 있으며 정보우위를 달성하기 위해 자국의 정보 및 정보체계는 보호하고, 상대국의 정보 및 정보체계를 교란, 파괴시키기 위해 실시하는 광범위한 제반 활동으로서 정보전의 범주에는 정보작전, 경제정보전, 해커전, 사이버전 등이 광범위하게 포함된다." 그러나 2002년 2월 국방부에서 발행한 국방 정보보호 발전 기본계획에서의 정보전 정의는 98년도의 미 합참의 정의를 그대로 수용하고 있어 우리 군의 정보전에 대한 통일된 용어 정의가 아직 미흡한 실정이다〔1〕.

2.1.2 한국군과 미군의 사이버전 정의

우리나라 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 정보마비전을 추구하는 전쟁수행방식을 의미한다."라고 정의하였고, 국방부는 사이버전을 "사이버 공간에서 일어나는 새로운 형태의 전쟁수단으로서, 컴퓨터시스템 및 데이터 통신망 등을 교란, 마비 및 무력화함으로써 적의 사이버체계를 파괴하고 아군의 사이버 체계를 보호하는 것"으로 정의하였다. 본고에서는 우리나라 국방부에서 정의한 사이버전 개념이 가장 현실에 근접된 내용으로 판단하고자 한다.

한편, 미군의 공식문서상에 등장한 다양한 사이버전 유사 용어를 정리하면 표 1과 같다. 사이버전의 개념은 사이버전 유사용어로 복잡하게 표현되는 듯 하나 정보작전 범주내의 컴퓨터 네트워크 공격(CNA) 및 방어(CND) 그리고 정보보증(IA)으로 정리될 수 있다. 상기 3가지 형태의 작전은 모두 정보작전의 한 부분이다.

표 1 미군의 사이버전 유사용어 정의

- 컴퓨터 네트워크 공격(Computer Network Attack)
  적의 컴퓨터 및 컴 퓨터 네트워크 그 자체나 또는 내재하는 정보를 파괴, 거부, 감퇴, 방해 하는 작전
- 컴퓨터 네트워크 방어(Computer Network Defense)
  적의 아군에 대한 파괴, 감퇴, 거부, 방해로부터 정보와 네트워크, 컴퓨터를 방어하고 보호하는 방어적 수단
- 정보보증(Information Assurance)
  가용성, 무결성, 인증, 기밀성, 부인봉쇄를 보장함으로써 정보와 정보시스템을 방어하고 보호하는 정보작전

이와 같이, 미군의 사이버전은 정보작전의 일부로서 공격은 컴퓨터 네트워크 공격 형태로, 방어는 컴퓨터 네트워크 방어와 정보보증의 형태로 수행된다. 단, 현재 미국에서 제공되는 대부분의 자료는 방어적 측면의 정보보증에 관한 것이며 공격에 대한 자료가 극히 부족하여 미군의 사이버전 수행 개념을 충분히 논의하기에는 어려우며 방어측면에서도 정보보증과 컴퓨터 네트워크 방어와의 차이점 식별이 곤란한 실정이다.

또한 사이버전과 평시의 사이버테러를 비교하면 표 2와 같다. 미 FBI에서는 사이버테러를 "준 정부 집단이나 비밀기관에 의한 비 전투 목표물에 대한 폭력을 통해 데이터와 컴퓨터 프로그램, 컴퓨터 시스템, 정보를 대상으로 사전 계획적이고 정치적 동기를 가진 공격"으로 정의하고 있으며, 우리나라 국가정보원에서는 "인터넷 등의 컴퓨터 네트워크 상에서 일어나는 파괴활동, 정부나 주요정보통신기반시설의 컴퓨터 시스템에 대하여 해킹을 시도하거나, 시스템 파괴나 정지를 통하여 사회기능의 혼란을 목적으로 시도되는 행위, 특히 그 피해가 심각하고 악질적이며 사회적인 영향이 큰 경우"를 가리키며 그 주요 대상으로는 국방·치안 관련시스템, 전력·수도, 항공관제 등의 시스템이 해당되며, 주요 사이버테러 방법으로는 중요정보의 파괴, 위·변조, 기밀 정보유출, 중요 서비스·기기·회선 등의 정지 등이 있다[1].

표 2 사이버전과 사이버테러 비교

구 분	사이버전	사이버테러
유사점	대상(컴퓨터시스템, 정보, 네트워크)	
차이점	주체(국가) 목적(군사작전)	주체(집단 및 단체, 비밀조직) 목적(이익추구, 사회혼란)

2.2 외국군의 사이버전 대응 동향

2.2.1 미 국

2001년 9.11테러 이후 미국은 사이버 공격의 위력을 핵무기에 비유하는 등 사이버 테러 대응의 중요성을 인식하고, 대통령 사이버 안보담당 특별보좌관 신설에 이어 테러의 위협으로부터 자국의 안전을 보장하기 위해 중앙 부(Department)수준의 조직인 국토안보부(Department of Homeland Security)를 2003년 3월에 설립하였다.

미국 국토안보부에서는 2003년 9월 국가사이버 보안부(National Cyber Security Division) 산하기관으로 US_CERT를 창설하였다. US_CERT는 미국정부의 사이버 공격 대응 능력을 하나의 단일 조직으로 집중화시킨 조직으로 미국 전역의 사고방지, 경고, 대응을 지휘하는 역할을 수행한다.

또한 미국 정보전 대응체계의 핵심조직인 미군 전략사령부 산하의 JTF-GNO(Joint Task Force-Global Network Operation)는 기존의 JTF-CNO를 확대개편한 조직이다. JTF-GNO는 사이버전 대응에 주력하는 부서로 2005년에는 최첨단 사령센터의 설치를 계획하고 있으며, 미군의 군사력 발휘시 컴퓨터 네트워크에 대한 공격과 방어능력을 활용할 수 있도록 전략사령관을 보좌한다.

JTF-GNO는 CND(Computer Network Defense)와 CNA(Computer Network Attack)로 구성된다. CND는 허가받지 않은 모든 탐색, 스캔, 바이러스사고, 또는 침입으로부터 DoD의 컴퓨터 네트워크와 시스템을 보호하는 임무를 맡고 있으며 CNA는 대통령의 명령에 의해 분쟁 지역과 국가 목표 달성을 목적으로 컴퓨터 네트워크에 대한 공격을 조정, 지원, 수행한다[2][3].

대부분 미군에서 준비하고 있는 사이버전 내용은 비밀로 분류되고 있으나, 방어의 개념에서 한 걸음 발전하여 컴퓨터 바이러스, 논리 폭탄 프로그램과 같은 공격무기도 이미 개발한 것으로 알려지고 있다. 이와 함께, 컴퓨터 해커들을 양성하고, 직접 물리적인 공격 없이 적의 지휘통제체계를 무력화시키며, 주요 도시의 전화망을 마비시키거나, 부대의 위치, 병력 배치, 지형 등에 대한 허위 정보를 입력하여 적을 교란시키는 전술 등도 개발중인 것으로 보인다.

기술적인 측면에서 미 국방부는 최근 사이버 공격의 유형을 표 3과 같이 크게 5가지로 분류하고, IATF(Information Assurance Technical Framework) 및 종심방어전략을 통해 이를 방어해 낼 수 있다고 판단하였다[6].

표 3 사이버 공격유형

공 격	기 술
수동적 공격 (Passive)	- 시스템에서 처리되거나 네트워크를 통해 전송되는 데이터 및 데이터를 통해 추출할 수 있는 정보를 수동적으로 감시하는 유형의 공격 (예) 평문 정보의 모니터링, 스니핑, 낮은 수준의 암호문의 분석 등
능동적 공격 (Active)	- 일반적으로 알려진 대표적인 공격 유형으로, 보호수단의 우회/파괴, 악성코드 삽입, 정보의 탈취/변조/삭제 등과 같이 정보나 정보시스템의 기밀성, 가용성, 무결성에 직접적인 영향을 미치는 공격 유형 (예) 정보 변조/위조, 사용자 가장, 서비스거부공격 등
근접 공격 (Close-in)	- 인가되지 않은 자가 정보를 변조, 수집하거나 정보자산에 대한 정상적인 접근을 방해하기 위한 목적으로 네트워크, 시스템 또는 시설에 물리적으로 접근하여 수행하는 공격 (예) 데이터 변경/정보수집, 시스템 변경, 물리적 파괴 등
내부자 공격 (Insider)	- 정보보호 처리 시스템의 물리적 경계 내에 있거나 직접적인 접근 권한을 갖고있는 인가된 사람에 의해 수행되는 공격 (예) 데이터 및 보안매커니즘 변경, 비밀채널 설정, 물리적 파괴 등
배포 공격 (Distribution)	- 생산에서부터 설치까지의 과정 중이나 사이트 간 이동 중에 악의적인 목적으로 하드웨어나 소프트웨어를 수정, 변경하는 공격 유형 (예) S/W, H/W의 악의적 수정, 백도어 설치 등

1990년대 중반부터 미 국방부는 정보통신 환경 변화와 미래 군사 임무 환경 변화에 따른 새로운 위협에 대응하기 위해 정보보호 개념을 "정보보증(IA, Information Assurance)"이라는 용어로서 재정립하고, 관련 체제의 정비 및 활동을 추진하고 있다. 정보보증은 "정보 및 정보체계의 무결성, 기밀성, 인증, 가용성, 부인봉쇄를 보장하기 위한 제반 활동으로, 정보체계에 대한 공격 및 침입을 방어, 탐지, 대응, 복구하는 것을 포함한다."고 정의하였으며 군 임무준비태세의 일환으로 모든 국방 임무 수행에 있어 정보보증의 완벽한 대응을 강조한다. 이러한 정보보증 달성을 위해 미 국방부가 제시한 방안이 IATF 및 종심방어전략이다.

먼저, 종심방어전략(Defense-in-depth strategy)은 정보기술 및 네트워크 기술 발전에 따라 고도화, 지능화, 전문화되어가고 있는 정보보호 위협에 효율적으로 대응하며, 정보 및 정보체계를 안전하게 보호하여, 궁극적으로 임무의 성공적인 수행을 지원하는 정보보증의 목표 달성을 위해 미 국방부에서 공식적으로 채택한 추진 전략이다. 종심방어는 다중계층, 다중차원의 보호수단을 구축하는 접근 방법으로, 하나의 방어 장벽이 공격자에 의해 침투되거나 돌파되어도, 연속적인 또 다른 방어수단을 통해 이에 대응한다는 개념이다. 이는 현재 알려져 있는 다양한 형태의 정보보호 위협 및 공격을 단일 보호체계를 통해 모두 방어할 수 없다는 현실적인 인식을 기반으로 한다.

이와 같은 종심방어 전략의 구현 영역은 단순히 기술적인 측면으로만 제한되지 않는다. 인력(People), 운영(Operation), 기술(Technology)을 주요 핵심 영역으로 설정하고, 모든 영역의 균형적인 발전을 강조하고 있다. 또한 종심방어 전략은 다양한 위협 및 취약점이 산재하여 있는 복잡한 정보통신 기반구조 환경에서 기술적 보호수단을 효율적으로 구현하기 위한 방법으로 계층적 접근방법을 채택하고 있다. 계층적 접근방법은 정보보호 요구사항이 도출되고 처리되어야할 핵심영역을 설정하고, 핵심영역에 높은 보증 수준의 보호 수단 구축을 집중하는 접근 방법이다. 4가지 핵심영역은 다음과 같다.

- 지역 컴퓨팅 환경(Local computing environment)
- 지역영역 경계(Enclave boundary)
- 네트워크 및 기반구조(Network and Infrastructure)
- 지원 기반구조(Supporting Infrastructure)[7]

한편 IATF(정보보증기술프레임워크)는 미 국가 및 국방 사용자들이 종심방어 전략의 기술적 구현을 위해 공통적으로 참조하여야할 정보 및 지침을 제공하고자 개발, 관리되는 기술 참조 문서이다. IATF는 미 국가안보국(NSA, National Security Agency)의 주도하에 다양한 기관 및 전문가들이 참여하여 작성되었다. IATF는 네트워크 보안에 대한 기술적인 지침을 제공하기 위해 1998년 개발된 NSF(Network Security Framework)를 기반으로 1999년 IATF로 명칭을 바꿔 지속적으로 보완 발전되어, 2002년 9월 버전 3.1이 공표되었다.

IATF는 종심방어 전략의 기본 원칙 하에 정보보증 기술과 체계를 분류 하고 있다. IATF는 전문가들에게 참고가 될 정보보호 기술의 세부적인 기능 및 특성을 기술하고 있다기보다는 다양한 유형의 국방 사용자들이 상위적 수준에서 정보보호 요구사항을 식별하고 적절한 솔루션을 선택하는데 참조가 될 수준의 정보를 포함하고 있다.

2.2.2 중 국

중국은 1985년부터 「정보전」을 중시하기 시작해 이미 실제 연구, 실험, 증명단계에 진입했다. 그리고 국방과학기술정보센터라는 기구의 설립 외에도 남경, 북경, 난주 군구에서 여러 차례에 걸쳐 모의 정보전 훈련을 실시하였으며, 국가안전과 방호의 측면에서 중국 과학원 첩보안전기술공정연구센터에 안전응용, 비밀번호이론, 안전관리 등의 연구 분과를 설치했다[1].

또한 중국중앙군사위원회는 낙후된 정보체계를 극복하기 위해 '컴퓨터 바이러스 침투가 원자탄보다 효율적이라는' 개념으로 S/W의 중요성을 강조하였다. 97년 6월에 100명 규모의 컴퓨터 바이러스 부대를 창설하였고, 1999년에는 해커부대를 창설하였으며, 2000년 하반기부터 사이버공격 및 정보교란 모의훈련을 수행하는 'NET Force' 부대를 운영하고 있다[4]. 그리고 중국에는 홍커(Red Hacker)라고 하는 100만명 정도의 회원을 갖는 해커집단을 비롯하여 다양한 3-8만명 수준의 해커집단들이 존재하고 있다.

중국의 정보전 및 사이버테러의 최근 공격사례 및 준비사항을 살펴보면 유고전시 미국에 대한 해킹 감행 및 대만과의 사이버전을 수행하였고, 대만에 7,200건의 공격('00.8)을 감행하였으며, 공개되지 않은 바이러스 약 1000여개를 보유하고 있으며, 논리폭탄, EMP 등도 개발하였다고 보도된 바 있다. 2004년에는 우리나라 10여개 국가공공기관이 중국으로부터 해킹을 당하기도 했다.

2.2.3 일 본

일본에서는 2000년 2월부터는 정부 차원의 대응체제를 강화하기 위해 전 성·청의 국장급 회의로서 "정보보안

대책 추진회의"를 설치하고, 정부와 민간사이의 정책협의를 긴밀하게 하기위해 학자, 보안전문가, 중요 민간시설의 대표자 등으로 구성된 "정보보안부회"를 설치하였다.

2000년 12월에는 "사이버테러 대책에 관한 특별 행동계획"을 발표했는데 일본 정부는 내각관방을 중심으로 민·관의 긴밀한 협력 하에 이 계획을 실시할 것을 천명하였으며, 2005년 4월에는 내각관방의 IT 전략본부 산하에 일본정보보호센터(NISC)를 설립하여 중장기 정보보호 기본전략수립과 정보보호 종합대책을 추진하고 있다. 이외에도 NISC는 법제도 정비와 연구개발추진과 전문인력 양성을 중점사업으로 하고 있다.

한편, 방위청은 2000년 10월 시험용 바이러스와 해킹기술을 독자적으로 개발한다는 방침을 발표하고 육·해·공 자위대가 통합하는 "사이버부대"를 창설하였다. 2001년도에는 사상 처음으로 방위예산에 사이버테러 공격을 방어하기 위한 첨단 전자장비 및 관련기술 개발비용을 포함하는 등 미래전 대비에 주력하고 있다[1].

2.2.4 러시아

러시아는 KGB 후신인 FSB 내에 사이버전 전담부서를 설치하고, 컴퓨터 바이러스 등 사이버 무기 및 물리적 마비 무기를 개발하여 실전 배치하였다고 전한다[4]. 또한 2000년 9월 12일 푸틴 러시아 대통령은 러시아 안전보장위원회의에서 의결한 러시아 정보보호정책을 승인하였다. 이 새로운 정책은 표면적으로는 컴퓨터 범죄를 처리하고 사이버 공간상에서의 보안을 보증하기 위한 강화된 법적 기반을 정부에 제공하는데, 다른 측면으로는 러시아가 외부 및 내부로부터 직면하고 있는 사이버 위협에 대처하기 위한 적극적인 시도라고 할 수 있다[1].

3. 우리 군의 사이버전 대응체계

3.1 군의 CERT 운영

CERT(Computer Emergency Response Team : 침해사고대응팀)란 해킹과 바이러스에 대항하는 보안기술을 개발하고 서비스하는 컴퓨터응급대응센터이며, 군의 CERT는 군내에서 운영되고 있는 전산망의 침해사고 대응활동을 지원하고, 전산망 운용기관 등에 대해 통일된 협조체제를 구축하기 위한 것으로, 군내의 CERT에는 국방CERT, 육군CERT, 해군CERT, 공군CERT 등이 각각 운영되고 있다. 이들은 국방통합보안관제센터를 중심으로 통합보안관제, 안전성 평가, 침해사고예방, 탐지 및 분석, 긴급대응/복구, 취약점 분석 등의 업무를 수행하며 대응팀들간의 협조체제를 유지하고 있다.

또한 일반적인 국방 사이버테러 대응절차는 방어단계를 5단계로 구분하여 적용하며 세부내용은 표 4와 같다[1].

표 4 국방 사이버 테러 대응 절차

단 계	기 준	조 치 사 항
예방단계	보안활동이 보장되는 평시상황	· 대응절차 숙지, 정보보호시스템 운영 · 기타 통상적인 정보보호 업무수행
공격감지 단계	특정 정보체계에 대한 공격징후 발견	· 특정 시스템 및 네트워크 집중감시 · 사용자 최소화, 공격 경보 발령
공격분석 단계	공격 받은 대상과 공격유형 분석	· 로그분석, 세부공격방법과 유형분석 · 피해 시스템 파악, 침입경로 추적
대응방안 수립 및 조치단계	대응방안 수립과 조치	· 손상된 시스템 운영중지 및 전산망에서 분리 · 대체 정보체계 지정 및 운영, 역공격
복구단계	공격으로 인한 피해 복구	· 업무 중요도에 따른 시스템 복구 · 공격 잔재 요소 파악, 제한적 정보체계 운용

3.2 INFOCON 운영

INFOCON(Information Operations Condition: 정보작전방호태세)이란 아군의 정보 및 정보체계에 대한 적의 침투가 예상 또는 공격 받을때 이에 효율적으로 대처하기 위한 단계별 방호태세로써, 2001년 4월부터 시행되고 있으며, 국방정보통신기반체계와 전장관리정보체계 및 자원관리정보체계를 이루는 국방전산망, 지휘소자동화망, 위성망 및 전술통신체계, 합동 C4I체계, 각군 C4I체계, 기능별 자원관리체계, 대외 전산망 등을 그 대상으로 하고 있다.

INFOCON 운영의 조직으로는 INFOCON 위원회가 있으며 INFOCON 위원회에서는 종합된 정보사항에 대한 정보작전방호태세 설정 필요성을 검토하고 실제 위협에 대한 작전적 영향 및 기술적 평가를 하며, 적절한 정보작전방호태세 등급의 결정 및 대응책을 수립하고, 정보체계에 대한 통합보안관제체계 점검 및 운영을 강화하며, INFOCON 발령, 해제 및 등급변경을 건의하고, 합동정보작전 수행기구에 상황을 통보하는 기능을 가지고 있다. INFOCON 발령절차는 INFOCON 위원회의 건의를 합동참모의장이 승인함으로써 이루어진다.

INFOCON의 단계는 정상, 알파, 브라보, 찰리, 델타 등 총 5단계로 구성되어 있으며, 각 단계별 대응조치

사항을 세부적으로 규정하여 정보시스템의 침해 위협에 적절하게 조치할 수 있도록 하고 있다.

3.3 국방정보전대응센터와 민관군 협력체계

"국방정보전대응센터"는 사이버 위협으로부터 군 정보체계를 보호할 목적으로 군 정보통신 시스템의 취약성 진단·조치와 침해사고에 대한 사고조사를 위해 2003년 11월에 설립되었다[8].

그 임무는 국방부, 국방부 직할부대 및 기관, 합참, 육·해·공군 각급부대 정보보호 관련 업무를 지원하는 것이며, 수사체계 운영팀, 침해사고 조사팀, 취약성 분석팀, 사이버전 대응훈련팀을 운영하고 있다.

또한 국방정보전대응센터는 1·25 인터넷 대란을 계기로 국가정보원이 사이버 테러로부터 국가정보통신망을 보호하기위해 2004년 2월에 설립한 "국가사이버안전센터"를 중심으로 한국정보보호진흥원에 설립한 "인터넷침해사고대응지원센터"와 함께 정보협력 및 공조체제를 구축하여 사이버테러에 대응하고 있다.

그림 1은 2005년 1월 31일에 대통령훈령 제141호로 제정된 "국가사이버안전관리규정"에 명시된 국가사이버안전센터를 중심으로 민·관·군 사이버테러 대응 기구간 업무 계통을 도식한 것이다[9].

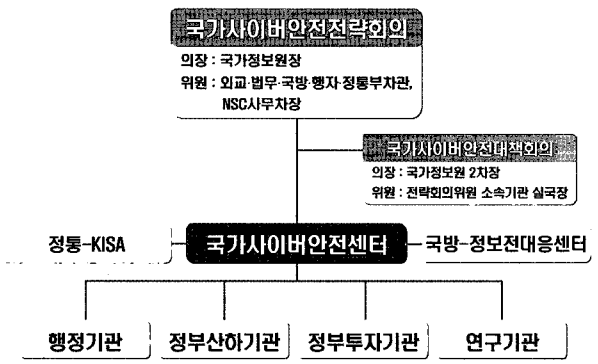

그림 1 국가 사이버테러 대응체계

"국가사이버안전센터"는 공공분야 사이버테러 전담 기구로서, 자체 전문인력과 함께 재정경제부, 국방부, 행정자치부, 정보통신부, 대검찰청, 경찰청 등 유관부처와 KISA, 국가보안기술연구소 등의 전문인력이 동시 근무하고 있다. 국가사이버안전센터의 역할은 한마디로 국가사이버 안전을 위한 컨트롤 타워다. 즉 국가기관의 정보통신망을 직접 모니터링하는 동시에 "인터넷침해사고대응지원센터", "국방정보전대응센터", "보안관제센터", "정보공유분석센터(ISAC)", "컴퓨터침해사고대응팀" 등 국내·외 사이버보안 또는 침해사고 대응기구들과 협력해 각종 위협정보를 종합적으로 분석하고 공격징후를 탐지해 각 기관에 안전대책을 제공하게 된다. 또 긴급상황 발생시 예·경보 발령과 함께 보안권고문을 작성·배포하고 피해발생시 사고원인 규명 및 긴급복구를 지원하는 등 사이버테러 예방 및 대응 활동도 국가사이버안전센터 임무의 하나다. 이를 위해 기본적인 사이버테러 대응조치 등을 규정한 "국가사이버안전메뉴얼"을 제작하여 각급 기관에 배포함으로써 사전 예방활동을 전개하고 있다[9].

4. 사이버전 대응체계 발전방향

본고에서는 사이버전의 개념과 외국군 동향을 살펴보았으며 현재 우리 군의 사이버전 대응체계에 대해서 알아보았다. 미래 정보전에서 승리할 수 있는 IT 강군을 건설하기 위해서는 군의 정보화가 체계적으로 이루어져야함은 당연하지만 정보시스템을 안전하게 유지할 수 있는 정보보호체계가 굳건하게 구축되어야 하며 사이버전에 효율적으로 대응할 수 있는 시스템을 갖추는것이 무엇보다도 중요한 핵심사항이라고 할 수 있다. 발빠른 정보기술의 발전과 함께 정보화 역기능 기술들도 더욱 지능화되고 있는 현실에서 첨단기술을 쫓아갈 수 있는 사이버전 대응체계를 구축하기위한 몇 가지를 제시해 보고자 한다. 여기에서는 구체적이고 세부적인 사항은 피하고 정책 및 제도적인 측면에서 우선 시급하다고 판단되는 사항만을 간추려 본다.

4.1 정보보호 조직 및 인력 확대

현재 국내외적으로 인식되고 있는 사이버 위협의 심각성에 비추어 우리 군의 정보보호 조직은 매우 약하다고 할 수 있다. 국방부와 각군의 정보보호 조직과 인력을 강화하여 체계적인 정보보호정책과 중장기계획을 수립하고 예산을 확보할 수 있는 역량을 확보하여야 한다.

4.2 정보보호 교육강화 및 전문인력 획득

개개인의 정보보호의식 강화와 임무와 수준에 맞는 교육이 필수적이라고 할 수 있으며 교육과 연구에 전념할 수 있는 전문인력이 확보되어야 한다. 새로운 첨단기술을 습득하고 응용할 수 있어야만 효율적인 사이버전 대응능력을 구비할 수 있다.

4.3 민관군 협력체계 구축과 국방정보전대응센터 조직 강화

현재 운용되고 있는 국방정보전대응센터는 임무와 기능의 중요성에 비추어 볼때 너무 미약하다고 본다. 국가적 사이버테러대응 조직에서 국방분야의 창구역할을 수행하고 사이버전에 대비하는 핵심조직으로서의 위상에 걸맞는 조직이 되기 위해서는 현 센터조직을 대폭적으로 강화해야 한다.

4.4 정보전 전략과 연계된 사이버전 대응체계 운용

실질적으로 사이버전 대응체계는 국가 방위전략의 정보전략과 연계되어 운용되어야 하지만 현 실정은 그렇지 못하다. 미국의 사이버전 대응을 위한 종심방어전략과 같은 기본개념을 정립하고 합참이 주도적인 역할을 수행할 수 있는 지휘체계가 갖추어져야 하며 이를 위해서는 좀더 심도있는 연구와 지원이 선행되어야 한다.

지금까지 우리 군이 IT 강군을 건설하기 위하여 기초가되는 사이버전 대응체계를 구축하기위한 정책 및 제도적인 측면에서의 발전방향을 제시해 보았다. 그러나 첨단 정보통신기술과 함께 발전되어야 할 사이버전 대응체계는 군 독자적으로만은 제기능을 완벽하게 갖출 수 없으므로 민간분야와 협력하여 학문적 연구와 실제적인 기술개발이 동시에 이루어져야 한다.

마지막으로 어느 조직이거나 새롭게 조직을 정비하고 인력을 확충하며 추진에 필요한 예산을 확보하기 위해서는 최고 경영자의 의지와 전체 조직원의 공감대 확산이 가장 중요하다는 점을 다짐하고 싶다.

참고문헌

[1] 장재규 · 남길현, "사이버전의 개념과 체계구축에 관한 연구", 국방대학교, 2002.12.

[2] http://www.fcw.com/fcw/articles/2005/0221/web-jtfg-02-25-05.asp.

[3] http://www.fcw.com/fcw/articles/2003/221/web-net-02-07-03.asp.

[4] 김세헌, 선진 각국 국방 정보보호 동향, 국방정보보호 컨퍼런스, 2004.

[5] 합동참모본부, "정보작전방호태세 규정(INFOCON)", 2003.4.

[6] 한국국방연구원, "국방정보보호 기술구조 연구", 2004.12.

[7] NSA, "Information Assurance Technical Framework release 3.1", 2002.

[8] IWRC, "정보전 대응센터 소개", http://www.iwrc.mil(국방인트라넷), 2004.

[9] 국가정보원, "국가사이버안전관리규정(대통령훈령 제141호)", 2005.1.

남 길 현

1965. 2~1969. 3 육군사관학교(이학사)
1971. 3~1973. 2 서울대 공과대학 토목공학과(학사)
1977. 8~1979. 6 미 해군대학원 전산학(석사)
1981. 9~1983. 6 미 위스콘신-메디슨 주립대 전산학(석사)
1983. 8~1985. 12 미 루이지애나 주립대 전산학(박사)

관심분야 : 정보보호, 암호학, 정보시스템 보안, 알고리즘, 개인정보보호

E-mail : khnam@kndu.ac.kr