정보전대응을 위한 컴퓨터 포렌식스 기반 모의실험1)

최용락* · 고병수** · 박명찬

목 차

1. 서론

오늘날 비즈니스 커뮤니케이션의 70%가 전기, 전자적으로 이루어지고 있으며, 이에 따른 모든 순기능과 역기능에 대하여 결정적인

* 대전대학교 컴퓨터공학전공 교수
** 대전대학교 컴퓨터공학 박사과정
1) 본 결과물은 산업자원부의 출연금 등으로 수행한 지역전략산업 석박사 연구인력 양성사업의 연구결과입니다.

거래증거는 컴퓨터와 네트워크 안에 있다. 불과 2-3년 사이에 급격히 증가한 사이버테러가 범국가적으로 이루어지고 있고, 인터넷의 활용성 증가와 함께 컴퓨터 범죄의 수법이 보다 지능적이고 다양화되어 가고 있다.

컴퓨터 통신기술을 기반으로 하는 정보전은 최근 미국에 의한 이라크 및 아프가니스탄의 전쟁에서도 보았듯이 현대 전투의 핵심적 요소이다. 하늘의 위성에 의한 정보와 땅 위의 다양한 계측 정보 및 바다에서의 전략적 지휘 통제는 컴퓨터와 통신을 기반으로 하는 첨단기술이 아니고서는 불가능한 일이다.

미래에는 정보전을 대비하여 무기체계를 외국에 판매하기 전에 미리 소프트웨어적으로 정해진 특정조건이 충족되면 그 무기체계의 소프트웨어 체계가 자동으로 작동되어 그 무기체계가 스스로 자폭하거나 혹은 그 체계의 조종이 불가능한 상태 등이 되도록 치핑(chipping)장치를 구매국이 알지 못하도록 설치하여 둘 수 있다. 이것은 향후 국제정세의 변화로 인하여 자국이 판매한 무기체계에 의하여 자국이 공격을 받지 않도록 하기 때문에, 타국으로부터 믿고 구매할 할만한 무기체계가 없을 것이라고 주장한다[5].

정보통신 네트워크를 이용한 원격접속 기술은 비대면성, 익명성, 광역성, 접근 용이성 등의 장점을 가짐으로 현대 정보전에서 매력적인 도구이며, 발전된 전자기술들은 경험하지 못한 첨단 사이버무기들을 출현시키고 있다. 현대전에서는 과거의 농경사회나 산업사회에서 볼 수 없었던 새로운 전쟁의 특성을 갖는다. 이제 한 나라의 군사력은 단순히 용감한 군인들의 수효와 전술에 의해 산출하기보다는 해당 조직이 갖는 전체적 경제능력과 보유하고 있는 첨단기술력을 함께 고려해서 평가되어야 한다.

미래 전쟁에서 정보작전의 전체 범위에 걸쳐 정보우세를 성취하기 위하여, 실시간 가시화 전장, 실시간 지휘관 결심, 실시간 전투

원의 공격 혹은 방어적인 조치를 가능하게 하기 위하여 실시간 탐지/타격 체계의 국방 정보통신체계가 필요하다. 이러한 아군의 국방 정보통신체계를 적의 공격으로부터 보호할 수 있는 능력을 구비하여야 하며, 반면에 유사시에 적의 국방 정보통신체계를 마비시킬 수 있는 해커, 바이러스, EMP(ElectroMagnetic Pulse)폭탄, 기타 사이버 무기 등이 중요한 전쟁도구가 되었다[6].

정보는 역사적으로 과거나 현대의 전쟁에서 전술 전략적 우위를 점유하기 위하여 공통적으로 필요한 핵심적 요소이었다. 그러나, 사이버 무기들을 기반으로 한 전쟁도구들은 과거의 단순한 정보획득과 보호와는 근본적으로 차원이 다른 공격적 정보전이 가능해진 점이다. 따라서 적의 정보자원을 효과적으로 획득하고 자신의 의지대로 교란시킬 수 있으며, 아군의 정보를 보호할 수 있는 능력은 미래 전쟁에서 승리를 담보할 수 있는 핵심적 요소로 부각되었다. 그러한 능력을 확보할 수 있는 국가적 전략을 수립해야함은 전쟁을 승리로 이끌고 국가의 생존문제를 보장해야 하는 국가적 사명이라고 할 수 있다.

이러한 국가적 전략 차원에서 미국, 일본, 이스라엘, 중국, 대만, 러시아, 북한 등에서 사이버군의 창설, 전문적 해커양성, 바이러스, 치핑, EMP 등을 위시한 전자 사이버 무기들의 개발이 추진되고 있다. 우리나라도 이와 관련된 다양한 대응책들이 준비되고 있으며, 그 내용은 첨단 사이버 무기개발, 안전한 국방 정보통신체계 확립과 이러한 일들을 가능하게 하는 인력양성 대책을 포함한 법과 제도적 정비일 것이다. 이와 같은 소요 제기에 의한 대전대학교의 군사학과와 같은 신설은 미래 정보전에서 민간대학이 갖는 장점을 최대한 부각 시킬 수 있도록 특성화 방향을 모색하여 운영해야 할 것이다.

본 논문에서는 미래의 정보전 형태이해를 도모하기 위하여 정보

전의 개념적 특성을 분석하고, 정보전에서 예상되는 위협요소 및 국내외 기술동향을 조사하며, 실용적으로 사용할 수 있는 정보전 핵심기술의 일부로써 대학에서 가능한 기술개발을 제안하고자 한다.

2. 정보전의 특징

1992년 미 국방부가 발표한 DoD Directive TS3600.1에서 정보전이란 용어를 처음 사용하면서 일반에 알려진 정보전은 현재 널리 사용되고 있는 용어지만, 관점에 따라 정의가 약간씩 차이가 나며 또한 전쟁의 개념으로 군사적 차원과 민간차원에서 보는 시각에 따라 약간씩 다르다[7]. Thomas Rona는 초기의 정보전의 개념을 "평시, 위기시, 경계시, 분쟁발생시, 전시, 전쟁 종료시, 복구시에 정보기술(수단)을 이용한 모든 전략/전술과 작전"이라고 포괄적으로 정의하였으며[15], Winn Schwartau는 정보전의 개념을 "컴퓨터 네트워크에 대한 공격"이라고 협의로 정의하였다[18]. 또한 미 합참은 " 정보 우위를 달성하기 위하여 아군의 정보, 정보 프로세스, 정보시스템, 컴퓨터 네트워크를 보호하고, 적군의 정보, 정보 프로세스, 정보시스템, 컴퓨터 네트워크를 공격하는 일체의 행위"라 정의한바 있다.

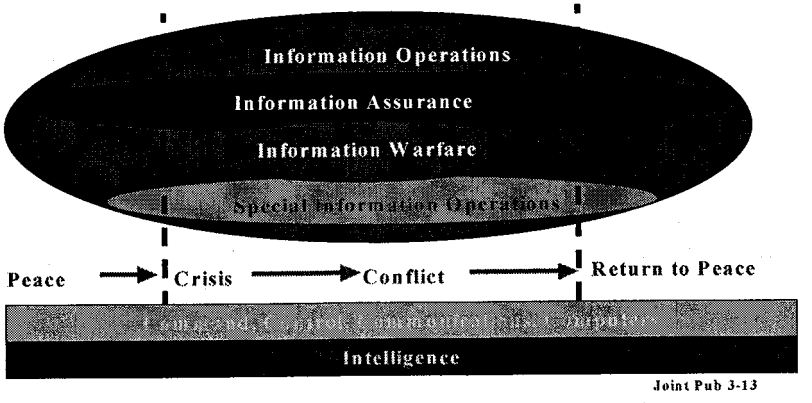
모두가 새로운 사이버 위협에 대한 견해에는 일치하지만 Winn Schwartau는 정치·경제·사회적 차원에서 설명을 하고 있으며, Thomas Rona와 미 합참은 군사적 차원에서 정의를 내리고 있다. 엘빈 토플러는 "제 3의 물결 정보시대에서 전쟁은 대량파괴가 아닌 중요 데이터를 지우거나 손상시켜 적에게 피해를 가하는 정보전으

로 변천하고 있으며, 정보전은 인명피해를 최소화시키면서 목적을 달성할 수 있다는 것이 특징이다"라고 하였듯이 정보전은 과거의 전쟁개념과는 달리 물리적인 파괴가 아닌 국가의 신경조직인 정보통신망, 주요기반구조의 컴퓨터 등을 파괴 또는 무력화시켜 목적을 달성하는 새로운 개념의 전쟁으로 볼 수 있다.

이와 같은 정보전의 개념은 1996년 12월 미 국방차관 White 가 미 국방부 지침 S-3600.1 정보작전(DoD Directive S-3600.1 Information Operations)에 서명함으로써 기존의 정보전에 대한 미 국방부의 인식을 갱신하면서 변화를 갖게 된다. 정보작전은 국방부 단독으로 사이버공간을 통한 국가의 안전을 위협하는 사이버위협을 대처할 수 없음을 인식하고 국방부, 연방정부부처, 공공기관 및 산업체와의 협력체제를 강화시켜 주는 기틀을 제공하기 위한 것이다. 이와 같은 정책변경의 내면에는 미국의 국가방위기술이 국가의 주요 IT 기반구조에 의존한다는 사실에 기인하며, 해킹, 사이버테러 등 주요 기반구조 침해위협을 방지하기 위해서는 주요 기반구조를 소유·운영 및 관리하는 국방부를 비롯한 연방정부, 공공기관 및 산업체의 보호노력을 통합하고 조정하는데 그 성공의 열쇠가 있다고 인식한 결과로 판단된다. 정보작전에서의 정보전은 [그림 1]과 같이 전시 혹은 위기시에 적국에 대하여 특별한 목적을 달성하기 위하여 행하는 행위로 국한하였으며 평시준비태세를 위하여 "정보보증"이라는 개념을 도입하고 연방부처 및 민간기관과의 상호 협력을 강조하였다.

군사관련 분야에서 일반적으로 사용하는 정보전은 사용하는 단체 및 개인들에 따라서 사이버전 및 사이버테러, 네트전, 해커전 등으로 인용되고[2] 있으나 그 출현 배경과 목적에 따라 약간씩의 개념 차이가 있다. 그러나 본 논문에서는 군사부문의 지휘통제전, 전자전, 군사정보전, 민군 중첩부문의 심리전, 사이버 테러전, 네트전, 해

커전, 사이버전, 그리고 민간부문의 경제산업전 등을 통칭하여 정보전으로 사용한다.



[그림 1] C4I 정보보증

정보전은 과거의 농업시대와 산업시대에서의 전쟁이 병력, 화력과 기동중심의 전쟁으로서 소모전, 대량살상 및 파괴의 성격을 가지고 있었던 것과는 상당히 다르다. 정보사회에서의 전쟁은 정보와 지식이 중심이 되고, 첨단과학기술이 바탕이 된 정밀무기와 정보자산으로써 파괴와 살상을 최소화하면서 승리를 추구하는 방향으로 전개된다. 정보시대의 전쟁특징을 주요 부문별 요약하면 <표 1>과 같다.

전 세계를 대상으로 하는 수평적 네트워크 구조에서 정보 전사들이 수행하는 사이버 공격은 이래와 같은 새로운 경향을 갖는다.

■ 범행의 광역화: 정보전 대상에 접근해야 할 필요가 없고 통신망(전화선)이 깔려 있는 곳이면 지구촌 어디에서나 분산된 다발적 공격이 가능하며, 통신망 전체를 24시간동안 전면적으로 차단하지 않는 한 완전한 예방이 불가능하다.

■ 범행의 익명성: IP 스푸핑과 같이 일반적으로 이용 가능한 도구 또는 여러 대의 중간 매개체 컴퓨터를 이용하고, 어떤 조직이나 정부에 의존하지 않고 개별적으로 행동이 가능하므로 특정 공격자와 공격 장소의 추적이 매우 곤란하다.

<표 1> 시대별 전쟁 주요특징

사회 특징 / 전쟁 특징	농업시대	산업 시대	정보 시대
전쟁수행 주체	무사 용병	직업 군인	정보 전사
전쟁지휘 구조	계층 구조의 소리/신호 체계	계층 다자간의 전화/통신 체계	수평 네트워크 구조의 C4I 체계
전쟁수행 범위	특정 부족중심의 지역 기반 대리전	전/후방의 대규모 군대 동원	전/후방, 가상공간, 우주의 원거리 3차원 공격
인명피해 특징	지역적 인명 살상	다수의 사상자 발생	소수의 사상자
중요 전쟁도구	칼, 창, 활 등의 물리적 도구를 사용	총, 핵, 화학물질 등의 대량파괴 무기를 사용	해킹, 전자기파 등의 사이버 정보기술을 이용
핵심 경제가치	노동과 토지의 부족/지역 기반경제	물질과 에너지의 자본/기술 기반경제	컴퓨터와 통신의 지식/정보 기반경제
전쟁 인력가치	단순 노동적 능력 용감한 응집력의 수준	기술적 도구의 활용능력 기술개발 습득의 수준	지식정보의 활용능력 창조적 두뇌집단의 수준
정보 원천가치의 사용	O	O	O
정보 가공기술의 사용	X	O	O
공격적 정보기술 사용	X	X	O

■ 사건예측 불가: 작고 은밀한 공간에서 컴퓨터 조작으로 공격이 가능할 뿐 아니라 신속한 처리속도로 삽시간에 범행이 가능하므

로 공격받은 전산망이나 기간시설이 완전 무력화되거나 정보유출·조작 등이 이루어진 후에야 공격받은 사실을 감지할 수 있다.

■ 피해 규모의 대형화: 최소의 노력과 금전적 투자로 테러효과를 극대화할 수 있는 수법으로 전력·통신·금융망 마비, 컴퓨터망 이용 상거래 중단 철도·항공·군사장비 시스템 파괴, 군·경 비상연락망 교란 등 국가 안보를 위협할 수 있는 엄청난 피해와 혼란이 초래될 수 있다.

■ 미래형 첨단폭격: 정보전은 정보시대의 산물로서 정보통신망의 급속한 발달과 비례하여 그 위협이 증대되고 있으며, 현재로서는 예측하기 어려운 인간의 상상력이 극대화 된 미지 형태의 정보전 공격이 더욱 부각될 것으로 전망된다.

3. 정보전 위협요소

정보시대의 전쟁특징은 정보전을 수행하려는 조직이나 국가들에게는 대단히 매력적으로 비칠 것이다. 특히 직접 기술을 습득하지 않아도 이 같은 지식에 뛰어난 해커를 고용하거나 익명성을 이용한 공격을 통해서도 피해를 광역적으로 입힐 수 있고, 범행의 일체를 증명하기가 어려워서 혐의를 부정하기도 쉽기 때문이다. 그리고 첨단의 정보기술을 확보하지 못한 기술적 후진국으로서는 그 내용을 파악 분석하고 대응할 힘을 갖추기가 단순한 노력과 의지만으로 불가능하다.

한편, 정보전에서 사이버 공격을 감행하는 이유는 대단히 심리적 효과가 크기 때문이기도 하다. 지난해 말 우리나라의 대통령 선거에서 인터넷을 이용한 사이버 기술 선거전략은 매우 주효함이 입증되었고, 이라크 전쟁에서도 주요 간부들에게 조직적인 회유를 권유

하는 사이버 접속은 널리 알려진 바 있다. 사이버 공격의 용이성과 인명 안전성에 비하여 범국가적 산업의 타격을 주기가 쉽고, 공격자의 신원증명을 회피하면서 다발적이고 지속적인 공격이 가능하다.

오늘날과 같은 정보시대의 사회구조는 대부분이 컴퓨터와 통신기술이 연합된 기반시설을 이용하여 이루어지고 있다. 정보전의 위협은 이러한 기반시설에 대한 직간접적인 공격(infrastructure attack)을 감행하는 사이버 테러 형태와 일반적 컴퓨터 시스템 및 통신망에 전문적 악성 소프트웨어(malicious software)를 이용한 해킹 공격, 그리고 자동제어, 전자 및 전파의 첨단기술을 이용한 전자무기체계에 의한 전자적인 공격(electronic attack) 등 3가지 측면으로 구분할 수 있다.

기반시설 공격의 대상이 되는 사회의 기반시설로는 국내의 금융, 국방, 치안, 교육연구, 행정 등의 부문별 기간 전산망체계를 포함하여 철도, 전력, 가스, 항공 등의 제어시스템과 기타 지리정보시스템(GPS) 및 다양한 형태의 응용서비스들이 될 수 있다. 이러한 서비스들은 정보사회의 일상 활동에 필수적이며, 국방관련 원활한 운영과 서비스 제공은 정보전에서 또한 결정적 요소가 된다. 이에 대한 공격의 일반적인 형태는 다음과 같다.

◉ 컴퓨터, 통신 소프트웨어, 데이터, 케이블 또는 제어장비 등의 기반시설에 대한 물리적(전자적 또는 기타의 방법을 사용한) 직접적인 공격

◉ 건물, 전력, 환경적 통제설비 등과 같은 주요 기반구조 지원설비에 대한 물리적 공격

◉ 해당 기반시설의 핵심적 운영요원 또는 지원요원에 대한 물리적 공격 또는 살상

◉ 주요 기반구조의 모든 시스템 구성요소에 대한 논리적(소프트

웨어적) 공격

◉ 컴퓨터 및 통신기술로 제어되는 환경적 통제 지원설비에 대한 논리적 공격

◉ 정당한 시스템 서비스를 무력화시키는 합법적 형태의 논리적 가용성 공격

◉ 내부인의 오용 및 남용을 유인하여 유효 정보의 논리적 파괴 또는 혼란

◉ 기타 적군에게 타격을 가할 수 있는 다양한 형태의 물리적 공격과 논리적 공격의 통합 공격

현재 일반적으로 사용되고 있는 컴퓨터통신 기술 소프트웨어는 대부분 이론적으로 완전하지 않으며, 각각의 취약점과 보안 허점들을 가지고 있다. 이러한 취약점들이 널리 사용하고 있는 컴퓨터 운영체제, 데이터베이스 및 인터넷 서비스 시스템 소프트웨어들에서 계속하여 발견되고 있으며, 이것은 트로이 목마나 트랩도어 등의 악성 소프트웨어의 이식을 위한 창구로 이용될 수 있다. 악성 소프트웨어의 이식에 성공하면 상대방의 정보시설은 원격지에서 은밀하게 자신의 의지대로 제어할 수 있음은 물론 상대방은 이러한 사실조차 인식하지 못하게 할 수도 있다. 악성 소프트웨어의 기술은 적군의 정보획득만이 아니라 반대의 정보를 의도적으로 가공하여 삽입할 수도 있으며, 최소한 상대의 정보통신체계를 원하는 목적대로 교란시키는데 성공이 가능하다. 예를 들어 내가 보통 때 사용하고 있는 컴퓨터가 나도 모르게 내 컴퓨터에 비밀 보관된 정보를 알 수 없는 제3자에게 전송하고 있거나 내 컴퓨터의 스크린에 디스플레이 되고 있는 모든 내용이 원격지의 다른 사람의 컴퓨터에도 그대로 디스플레이 되고 있다면 어떠하겠는가?

현대 첨단무기의 핵심적 부품들은 대부분 전자적으로 제어된다.

전자적으로 제어할 수 있다는 의미는 무기나 장비들의 주요 기능들을 전자적으로 공격하여 무력화 시킬 수 있다는 가정이 성립된다고 본다. 정보통신체계를 마비시키는 비살상 무기로써 전자기 펄스 탄, 고출력 마이크로웨이브 총, 고출력 섬광 탄, 흑연 섬유 탄, 등의 새로운 형태의 군사무기들이 소개되고 있다. DEW(Directed Energy Weapon)는 정보통신 체계의 물리적 구성품에 대하여 치명적인 손상 및 마비를 유발시킬 수 있는 잠재력을 제공한다. DEW 무기는 RF(Radio Frequency), 레이저, 입자 에너지 등의 무기로 공격거리 및 용도에 따라서 무기운용에 대한 새로운 작전개념의 수립이 필요하다. 단거리의 법 집행용 HERF(High Energy Radio Frequency)총으로 헌병이 도주하는 차량을 쏘면 도주차량이 엔진이 꺼지고 정지하며, 중거리의 전자기적 공격용 EMP(Electro Magnetic Pulse) 탄은 전투기, 포 등으로 공격이 가능하며, 장거리의 EMP 탄, 레이저 빔을 조사하는 무기는 우주선 대 우주선, 우주로 올라오는 탄도탄 공격에 운용할 수 있을 것이다.

이와 같이 정보전은 국가적 주요 기반시설에 대한 테러행위, 컴퓨터 소프트웨어에 의한 지능적 정보획득이나 다양한 형태의 방해 및 사이버 심리전, 그리고 첨단 전자기술을 이용한 미래전의 전자무기 개발 등 정보시대에 등장하는 모든 분야에서 응용 가능한 새로운 형태의 공격 위협요소를 갖는다. 이와 같은 사실은 오늘날의 국방이 일부 군인들에 의해서만 보장이 되는 것이 아니라 선진화된 산업기술과 더불어 국민들 전체의 역량이 총체적으로 결집되어야 함을 시사한다. 다양한 개성의 집단이 국가적 안보라는 하나의 목표를 위하여 총화 단결해야 할 때는 그 만큼 통찰력 있는 위협요소의 분석과 시대적 변화를 확실히 인식하면서 장기적인 지휘전략이 필요하다고 판단된다.

일반적으로 널리 알려진 전쟁무기는 크게 살상(hard-kill) 무기와

비살상(soft-kill) 무기로 구분할 수 있다. 정보전에서는 주로 비살상 무기들이 사용되는데, 정보전사(infowarrior)들에 의해 이용될 수 있는 비살상 무기들은 <표 2>와 같이 크게 14가지 유형으로 제시할 수 있다[3].

4. 정보전 기술동향

9. 11테러 이후 미국은 사이버보안에 대해서 특별한 관심을 표명하며, 미국의 국가 및 군을 대상으로 한 사이버테러와 정보전 위협에 대비를 강화하고 있다[4]. 특히, 정보전 공격·방어를 수행하기 위한 전담 군사 조직을 공개적으로 발족한 이래, 국가 전략으로서 사이버보안 국가 전략(The National Strategy to Secure Cyber-space)[16]과 주요 기반시설 및 주요 자산의 물리적 보호를 위한 국가 전략(National Strategy for the Physical Protection of Critical Infrastructures and Key Assets)[17]을 발표하였으며, 관련 법제와 조직체계를 정비하는 등 다각적으로 노력하고 있다. 그리고 연방차원에서 중심기관 설치의 필요성을 인식하고, 이를 위한 각종 제안들을 고려하여 2001년 10월 8일 대통령 명령(Executive Order) 13228 발표와 함께 국토안보국(Office of Homeland Security)을 설립하였고[10], 사이버안보담당 대통령특별보좌관, 국토안보회의, 대통령 주요기반보호위원회 등을 새로이 신설하였다.

이러한 조직들은 물리적 테러뿐 아니라 사이버테러의 대응 및 복구에 관한 활동의 임무를 갖고 정보시스템 보안을 위한 각 부처, 연방, 지방정부의 활동을 조정하고, 침해사고 복구를 총괄지휘하며, 주요 정보통신기반시설을 운용하고 있는 민간 분야와의 업무를 협

의 조정하는 역할을 부여하였다.

미군 정보전 대응체계의 핵심은 미군 전략사령부(U.S. Strategic Command) 산하의 JTF-CNO(Joint Task Force-Computer Network Operations)이다. JTF-CNO는 미군 전략사령부의 컴퓨터 네트워크 작전수행을 위한 작전 부서이다. JTF-CNO의 컴퓨터 네트워크 작전은 두 개의 특별한 상호보완적 임무인 컴퓨터 네트워크 방어(CND)와 컴퓨터 네트워크 공격(CNA)으로 구성되어 있다. CND 임무는 모든 허가받지 않은 탐색, 스캔, 바이러스 사고, 또는 침입으로부터 국방부의 컴퓨터 네트워크와 시스템을 보호하는 것이다. CNA 임무는 대통령의 명령에 의해 분쟁 지역과 국가 목표 달성을 목적으로 컴퓨터 네트워크에 대한 공격을 조정, 지원 및 수행하는 것이다. 미공군정보전센터는 1993년 창설된 이래, 미공군의 정보전 개념과 정보작전 능력을 개발해오고 있다[14]. 미공군정보전센터(Air Force Information Warfare Center)는 우주항공 및 합동군의 정보전 요구를 만족시키기 위한 능력 즉, 작전 수행, 목표 식별 및 포착을 위한 정보전 분석 및 자료 생산을담당하는 임무를 맡고 있다.

일본은 총리가 주재하는 생화학, 핵에 대한 대응책 마련과 함께 사이버테러 대책강화 등을 중점 추진사항으로 의결하여 사이버테러에 관심을 촉구하고 있다.

<표 2> 정보전 무기의 유형

무기 유형	주요기능
해킹 기술	해커들은 시스템의 정상적인 동작을 방해하여 시스템이 사용자가 요구하는 서비스를 처리하지 못하도록 하는 서비스 거부 공격을 감행하거나, 웹 서버 및 홈 페이지를 공격하는 등 다양한 기법과 도구를 이용한다.
컴퓨터 바이러스	바이러스들은 인터넷의 영향으로 인해 점차 그 확산 속도가 빨라지고 있다. 불과 5년 전만 해도 컴퓨터 바이러스가 전세계적으로 퍼지는데 2년이 걸렸으나 최근의 조사에 따르면 불과 몇 시간밖에 걸리지 않고 있다.
웜	웜은 스스로 전파되는 악성 코드로서, 전파를 위하여 사람이 개입하여야 하는 바이러스와 달리 웜은 스스로 전파될 수 있다.
트로이 목마	트로이 목마는 정상적으로 보이는 프로그램 내부에 숨어서 시스템이나 네트워크에 해를 끼치는 코드이다. 트로이 목마는 시스템의 보안 취약성 점검도구와 같은 형태로 위장될 수 있으며, E-mail을 통해 전달될 수도 있다.
논리 폭탄	만약에 소프트웨어 제작국가가 트로이 목마나 트랩도어 및 논리폭탄 등을 은폐한 소프트웨어를 적국이 수입하도록 한다면 자신들의 의지대로 정보를 획득 가공이 가능하고 적군은 그 사실조차도 파악하기 어려우며, 적기에 대처할 수 없게 된다.
전자우편 폭탄/스팸메일	적대국에 악의적 또는 별 의미없는 내용을 담은 전자우편을 대량으로 발송하여 컴퓨터나 네트워크를 마비시킬 수 있다. 분초를 다투는 사이버 전쟁에서 상대방을 혼란시키고 시간을 소모하게 만들어 정보우위를 점유할 수 있다.
지뢰	특정 조건을 만족하면 동작하는 기능이나 회로를 칩(chip)의 일부분에 하드웨어적으로 삽입하는 공격방법이다. 자신이 가지고 있는 방안의 전자장비가 취약한 임의의 시간에 다른 사람에 의하여 나 자신을 공격하도록 제어될 수 있다면 심각한 일이 아닐 수 없다.
나노머신	나노 머신은 적의 정보센터 등에 살포되는 컴퓨터 하드웨어를 파괴하는 작은 크기의 로봇이다. 나노 머신들은 컴퓨터를 찾아 사무실 등을 돌아다니다가 슬롯 등의 틈을 통해 컴퓨터에 잠입한 뒤, 기판이나 회로 등을 파괴한다.
미생물	컴퓨터 기판을 부식시키는 미생물이 있다. 미 육군에서는 컴퓨터 칩에 대하여 공격을 하는 실리콘 박테리아에 대하여 언급하고 있다.
재밍	예전에는 재밍이 적 통신장비간의 통신 채널을 방해하는데 사용되었지만, 앞으로 정보통신망을 통해 전달되는 패킷들의 유통을 전자적으로 방해하거나 내용을 변경하는 무기로 사용될 것으로 예측된다.
HERF	이 무기는 수백개의 라디오 기지국에서 수백만 와트의 전파를 한 곳으로 집중시켜 동시에 발사하는 것과 동일한 출력을 발생시키는 무기로서 컴퓨터를 포함하여 전자회로로 구성된 모든 장비를 shutdown시킬 수 있다.
EMP	EMP 폭탄은 핵폭발이 발생하는 것과 동일한 수준의 전자기파를 발생시킴으로써 이 전파에 노출된 컴퓨터나 통신 시스템의 모든 전자회로들이 파괴 된다.
AMCW	자신이 외부의 조종이나 도움없이 스스로 네트워크를 따라 목표를 찾아 돌아다니며 바이러스 기술 등을 이용하여 적의 컴퓨터나 네트워크 시스템을 파괴, 정보를 조작하는 무기로서, 마치 지능을 갖춘 순항 미사일에 비교할 수 있다.
Dos	적이 고의적으로 합법적인 사용자가 목표대상이 되는 시스템을 이용하지 못하게 다양한 수법을 이용하여 서비스 불능상태가 되도록 공격할 수 있다.

2001년 10월 2일 사이버테러 특별 행동계획에 대한 후속조치를 통하여 행정부 및 전력, 교통 등 중요 인프라의 사이버테러 대응 연락과 협력체계를 구축하였으며, 보호 대상이 되는 정보시스템을 지정한 바 있다. 특히 이 후속 조치에서는 긴급 상황의 발생시 정보연락이 필요한 경우로 아래와 같은 상황에 따른 사안별 연락체계를 정립하였다.

- 조직적인 예비행위들에 대한 징후
- 중요 시스템의 경미한 장애
- 중요 시스템의 중대한 장애
- 사이버 공격의 확인

그리고, 전자정부 및 민간 주요 인프라에 대한 사이버테러 대책을 원활히 수행하기 위하여 2002년 4월 1일 내각관방 정보보안대책추진실에 국가 긴급 대응팀(National Incident Response Team)을 설치하고 정부부처 정보보안 상담 대응 및 사이버테러 관련정보의 수집과 분석, 사이버테러 피해 확산방지 및 복구에 대한 기술적 지원 등의 임무를 부여하였다.

북한은 사이버전 능력을 태평양사령부 지휘통제소 마비 및 미 본토 전력망에 피해를 줄 수 있는 정도로 상당한 수준인 것으로 추측되고 있다. 미국은 사이버전을 수행할 수 있는 북한과 중국의 해킹 능력을 미 CIA 수준으로 평가하고 있다. 러시아는 KGB 후신인 FSB내에 사이버 전담부서를 설치하고 컴퓨터 바이러스 사이버 무기 및 물리적 마비 기구를 개발하여 실전배치하고 있는 것으로 알려져 있다.

이외의 많은 국가들이 정보전에 대비하여 사이버군의 창설과 정보통신체계를 공격하기 위한 해킹, 바이러스 유포, 각종 에이전트 설치 등의 기술과 첨단 전자무기체계를 개발하고 있다. 외국의 정보전 관련 주요동향을 요약하면 <표 3>과 같다[6,11].

<표 3> 외국의 정보전 주요동향

국가	현 황
미국	- 미공군 사이버전쟁 총책임부대: 미공군우주사령부(콜로라도 위치) - 사이버 무기개발: 해킹기법, 바이러스, 트로이목마, 논리폭탄, 치핑, 자동이동 사이버 무기(AMCW), 비살상 공격무기인 전자기파폭탄(EMP), 전자기 총, 레이저, 입자무기 등 - 전세계 전자우편, 팩스 및 유무선 통신 감청기관(Enchelon) 운영 - 육해공군에 사이버 전 전담부대 - 사이버전시 해킹을 공격수단으로 전술개발 중
일본	- 일본정부 해킹, 바이러스, 전자기파폭탄 등에 대처할 국가기관 필요(2000.1) - 일본 방위청 2000년 백서에 사이버전 부대 창설 - 2001년 방위 예산에 사이버테러 공격대비 1398억엔 예산책정
싱가포르	- 공세적 사이버전 작전요구 충족위한 국방부 내에 사이버 전 전담부대 창설 - 군용정보통신체계 보호 위한 연구조직 창설
북한	- 평양자동화대학(옛미림대학)해커 100여명 양성중이며, 해커 능력은 미국 CIA나 국가 보안국(NSA) 수준으로 판단함 - 사이버 무기개발: 해킹 기법, 바이러스 등
중국	- 사이버군 창설: 해킹/바이러스 부대 창설 전국에 배치 - 사이버 무기개발: 해킹기법, 바이러스, 트로이목마, 논리폭탄, 치핑, AMCW, 저주파음파, 전자기파폭탄, 레이저 등 - 사이버 공격 및 정보교란모의훈련의 "Net Force" 부대를 운영
러시아	- 비살상 공격무기 연구: 바이러스, 전자기파폭탄, 전자기 총, 레이저 등 - 사이버 무기개발: 치핑 AMCW, 음파무기, 심령술 등
대만	- 대만 국방부 사이버 전 수행 부대 창설 결정(2000.11) - 해커로부터 군용 정보통신체계 보호용 관제체계 구축 등

5. 정보전 대응 컴퓨터 포렌식스 전략

인간의 신경망처럼 유무선 네트워크로 연결된 컴퓨터 통신망은 오늘날 정보시대에 우리 인간들의 교육, 금융, 레저 등의 사회생활과 전문적 업무활동은 물론 국가적 차원의 정보인프라와 국방기술의 주요 근간이 되었다. 인체의 신경망에 원활한 영양 공급이 되고 정상적인 활동이 보장될 때 우리는 건강할 수 있으나 신경조직의 파괴, 바이러스의 침투 또는 비정상적인 어떤 기능이 있다면 우리는 느낌이나 여러 가지의 검사를 통하여 그 진단과 처방을 하게 된다. 인체의 경우처럼 컴퓨터 통신망의 시스템 자원에 대한 파괴, 악성 바이러스의 침투 또는 비정상적인 동작이 감지된다면 어떻게 해야 할까? 우선 감지된 증상들이 특정 자원의 파괴, 해킹, 트로이 목마나 바이러스 등의 악성 소프트웨어 공격, 또는 하드웨어 장비와 소프트웨어의 오동작인지 그 원인을 알기 위하여 컴퓨터 시스템과 정보통신기기에 남아 있는 여러 가지의 전자적 흔적들을 진단해야 할 것이다.

정보보안 침해사고로부터 전자적인 현상에 의하여 과학적으로 그 원인을 진단하고 분석하여 법의학적인 증거를 제시하고 대응할 수 있는 기법이 바로 컴퓨터 포렌식스(Computer Forensics)이다. 미국을 중심으로 한 기술 선진국들은 정보시스템에 대한 보안침해사고에 대하여 디지털 전자적 증거를 분석하고 대응하는 기술들을 개발하고 있다. 정보전에서 다양한 전자적 침해사고에 대하여 현장을 검증하고 사건의 원인과 공격루트를 밝혀내어 법적으로 보장되는 정확한 증거를 확보하는 것을 출발점으로 하여 진정한 정보의 주인이 될 수 있다. 즉, 자국의 컴퓨터 포렌식스 기술이 확보되지 않는다면 국내외에서 일어나는 모든 보안침해사고에 대하여 국가 자존적 해석이나 사실증명이 불가능하고 외국에 의뢰하여 결과를 통보

받아야 하는 안타까운 현실을 초래할 수밖에 없을 것이다.

현재, 우리나라는 항공기 사고의 블랙박스 분석이나 고공 정찰에 따른 다양한 정보분석 등 대부분의 분야에서 선진국에 의존하고 있는 실정이다. IT산업 강국을 목표로 하는 관점에서 보안침해사고의 경우 다른 분야와 마찬가지로 선진국에만 의존한다면 본래의 국가적 목표달성이 한계에 부딪칠 수밖에 없다. 무한 경쟁의 국제 산업질서 속에서 자국의 이익과 자존심을 확보하기 위해서도 보안침해사고를 자주적 기술력으로 분석파악하고 정확한 법적인 입장과 대응전략을 모색하는 정책은 매우 중요하다. 특히, 사회 전반적인 인터넷 활용증가와 더불어 각종 음란 사이트 개설, 내부인의 불법적 계좌이체, 위협 편지, 지능적 사기, 지적재산 도난, 적성국의 의도적 접속 등의 위협요소 속에서 전자정부의 실현, 전자상거래의 활성화, 원격교육의 정착, 사이버 홈의 건설, 무선 인터넷의 인프라 구축 등 사이버 세계가 현실화 되어가고 있다. 그러나, 정보전송 기반시설에 대한 사이버 테러 및 보안침해사고로 인한 서비스 불능과 중요정보의 유출이 산업경제와 사회적 큰 피해로 나타나고 있으며, 이러한 위협요소와 연합하여 유사시에 국가간의 전략적 정보전 형태는 더욱 심각한 상황을 몰고 올 위험성이 있다.

따라서, 우리나라도 정보시대의 산업기반시설 동맥이 되는 주요설비의 보호, 정보기술 강국으로써의 자국 정보보호 및 상대국 정보의 획득, 첨단 전자무기체계 개발을 통한 공격 및 보호 기술에 대한 개발 등이 필요하다. 컴퓨터 포렌식스는 정보시스템 자원에 대한 각종 보안침해사고에 대하여 증거의 확보, 원인의 분석, 절차에 따른 단계적 대응 및 문제점 개선을 통한 향후 대응책 보완수립 등 정보전에 대비하여 반드시 필요한 원천 기술이다.

5.1 컴퓨터 포렌식스 방법론

일반적으로 컴퓨터 범죄 관련 증거자료를 대상으로 한 컴퓨터 포렌식스 분석 방법론은 크게 역추적을 통한 방법과 증거물 복원을 통한 컴퓨터 포렌식스로 구분할 수 있다[1].

역추적을 통한 컴퓨터 포렌식스 방법에서는 이벤트가 발생한 근원지 또는 위치를 찾아가는 방법에 관한 사항을 제공한다. 컴퓨터 범죄와 관련된 증거를 수집하고 이를 분석하여 근원지에 해당하는 IP 주소 등을 역추적한다. 그리고 근원지가 파악되면 이를 문서화하여 최종적인 증거물로 채택한다. 증거물 복원을 중심으로 한 컴퓨터 포렌식스 방법은 관련 증거자료를 수집하여 데이터 복구 과정을 수행하고, 필요로 할 경우 암호화된 데이터에 대한 복호과정을 수행하여 증거물에 해당하는 데이터의 특성에 따라 수사하는 방식이다.<표 4>는 단계별로 수행되는 주요 과정을 나타내고 있다.

<표 4> 목적에 따른 포렌식스 방법

단계	역추적을 통한 방법	증거물 복원방법
1 단계	관련된 증거 자료 수집	관련된 증거 자료 수집
2 단계	키워드 분석	데이터 복구 및 암호 제거
3 단계	위치,저장장소 및 근원지 파악	포맷 분류 및 은닉 자료 검색
4 단계	증거물에 대한 문서화	증거물 정리 및 문서화

차세대 정보전에서 보안의 개념은 방어적이기보다는 공격적이게 되었다. 컴퓨터 침해 사고 방지를 목적으로 침입방지기술에 관한 연구가 많이 수행되고 있지만 방어 수단만으로는 충분한 목적을 달

성할 수 없다. 그러므로 부정행위자의 신분을 확인하여 증거를 확보하거나 상대 시스템을 위협하는 적극적인 형태의 공격형 기술이 요구된다. 그러나 대부분의 부정행위자는 추적하고자 하는 사람이 미칠 수 없는 원격 컴퓨터를 거쳐서 침입하므로 단기간 내에 신원 파악이 거의 불가능하다. 즉, 침입을 탐지함과 동시에 침입자의 접속을 차단시킴으로써 침입자가 탐지된 사실을 인지하고 차후의 접속을 중단하기 때문이다. 사용자의 시스템을 중간 거점을 삼아 이동하는 경우 역추적과 같은 기존의 기술을 이용한다면 역추적 소프트웨어가 설치되어 있지 않은 상태에서 부정행위자를 추적하는 것은 불가능하다. 부정행위자에 대한 정확한 신분확인을 위해서는 이러한 문제점을 해결해야 한다. 또한 부정행위자를 추적할 수 있는 영역에 대한 제약이 최소화되어야 한다. 이러한 요구조건을 만족하는 진보된 해킹 방지기술이 요구된다. 이러한 기술을 통해 사용자의 시스템을 보호함은 물론 부정행위에 대한 시나리오 데이터베이스를 구축할 수 있다. 또한 부정행위자가 이동한 경로상의 원격 컴퓨터 관리자와 연락하여 공동조사가 가능하고 부정행위자의 습관을 분석함으로써 직접 신원 파악이 가능하다.

유사시의 정보전에서 아군의 정보시스템에 침해가 일어났을 경우, 그 원인분석을 위하여 어느 나라에 믿고 의뢰할 수 있겠는가? 침입경로를 분석하고, 누가, 언제, 어떠한 방식으로, 무엇에 침입했는지 스스로 분석 판단할 수 있는 기술이 없다면 대단히 심각한 일이 아닐 수 없다. 누가 타격했는지 모르면 대응할 수도 없으며, 재차 동일한 형태의 공격을 계속 받을 여지가 남아있게 된다. 그리고 피해를 복구하는 기술 또한 대단히 중요하다. 불의의 사고나 보안침해 공격으로 인하여 손상된 중요한 정보와 시스템을 복구해내는 기술은 정보전 상황에서 부상당한 사람을 치료하는 이상으로 중요한 업무일 수도 있다.

5.2 보안 침해사고 대응

완벽하게 안전한 보안시스템이란 있을 수 없으며 정보시스템에 대한 침해위협은 항상 존재한다. 침해사고 발생시 피해확산의 방지, 서비스의 신속 안전한 복구, 공격자의 위치와 동기 파악, 재범 발생의 방지를 위하여 발생 가능한 위협에 대하여 미리 조치절차를 수립해 두는 것은 침해사고 대응에 매우 효과적일 것이다.

지금까지 우리는 침해사고대응 단계에서 정형화되지 않은 방법과 절차들을 사고분석 절차에 적용하여왔다. 그러나 최근에는 침해분석 대응에 컴퓨터 포렌식스 기법을 적용함으로써 좀더 구체화되고 정형화된 방법론을 가지고 해킹사고에 접근할 수 있게 되었다. 침해사고대응을 할 때 일반적인 접근 방법은 "Incident Response"의 저자 Kevin Mandia과 Chris Prosise는 침해사고 대응의 일반적인 절차와 기능을 사전 준비단계, 사고 탐지단계, 초기 대응단계, 대응전략 수립단계, 포렌식스를 위한 자료 이중화 단계, 조사 단계, 보안평가 수행단계, 네트워크 모니터링 단계, 복구, 보고, 사후조치 단계 등 11단계로 구분한다[13].

컴퓨터 포렌식스는 법적인 문제를 해결하기 위한 컴퓨터 범죄 수사과학이다. 전통적으로 컴퓨터 포렌식스는 하드 디스크의 원본을 완전히 복제하여 분석하는 것으로, 컴퓨터의 부검이라고도 한다. 조사는 복제된 하드디스크나 운영중인 시스템의 로그파일에 대한 검사를 포함하여 최초 사고 발견자, 보안담당자에 대한 면접조사 등 세부적인 사고조사 과정을 말한다. 일반적으로 이 단계는 다른 단계에 비해 가장 긴 시간이 소요되는 것이 보통이다. 보안평가는 앞의 과정에서 조사된 결과물을 토대로 보안상의 문제점을 평가하는 과정으로, 향후 사고방지를 위한 작업을 뜻한다. 사고의 형태와 원인에 따라 시스템이나 네트워크 차원에서 어떠한 문제가 있었는지

또는 관리상의 실수가 있지는 않았는지, 또는 전반적인 보안정책에 문제는 없는지 등의 항목들이 검토되며, 그 수행결과에 따라 정확한 조치를 취하게 된다. 보안평가와 조치 후에 해당 조치의 적절성을 판단하기 위하여 상당기간 네트워크에 대해서 한층 강화된 모니터링이 수행되어야 한다. 안전성이 검증될 때까지 평상시보다 강화된 보안수준을 적용하여야 한다.

이러한 방법론은 각각의 중요한 의미를 지니고 있으나, 작업순서가 반드시 설명된 순서대로 진행되어야 하는 것은 아니다. 응용분야와 침해의 형태에 따라서 조직별로 적합한 방법론을 개발하고 이에 필요한 기술적 도구들과 협력 조정체계가 연구되어야 한다.

5.3 컴퓨터 포렌식스 도구

현재까지 제시된 컴퓨터 포렌식스 도구들은 컴퓨터 포렌식스에 관련된 전반적인 기능을 제공하는 도구와 각 기능별로 포렌식스 과정을 수행하는 부분적인 도구로 구분할 수 있다. 국내에서 공개된 컴퓨터 포렌식스 관련 증거수집 방법 및 도구는 거의 전무하며 또한 상업용 증거수집 도구들 역시 삭제된 파일에 대해 복원 및 복구 기능 등을 주로 제공하기 때문에 상당히 제한적인 분야에만 개발되어 있다.

외국의 포렌식 도구 개발업체로는 유타 주 프로보 소재의 AccessData Development, 캘리포니아 주 파사데나 소재의 Guidance Software, 오리건 주 그레샴 소재의 New Technologies Armor 등이 있으며, 여기에 대학교 연구소의 개발자들과 매사추세츠 주 캠브릿지 소재의 @Stake 같은 보안 컨설턴트 등도 있다. 이들 업체는 대상 컴퓨터내부의 저장장치에 남겨져 있는 수 기가바이

트의 데이터를 분석하는 강력한 도구를 제공한다. 부분적 기능을 제공하는 몇 가지 포렌식스 도구들을 처리내용별로 분류하면 <표 5>와 같다[8,9,12].

5.4 컴퓨터 포렌식스기반 정보전 모의실험

일반적으로 정보전은 정보, 정보기반과정, 정보체계, 컴퓨터 기반 네트워크에 대하여 우군의 것은 보호하면서 적군에게는 영향을 미침으로써 정보우위를 달성하기 위해 취해지는 활동으로 정의되고 있다. 또는, 이러한 정보전은 위기나 분쟁시에 특정 적에 대하여 목적하는 계획을 달성하기 위하여 위기를 조장하고 혼란을 야기 시키기 위한 정보작전의 일환으로 이해되기도 한다. 그러나, 현대의 정보전은 특별히 전쟁수행중이 아닌 평상시에 총괄적 국가이익에 수반되는 모든 정보 자원들을 정보보증의 관점에서 지휘, 통제, 소통, 그리고 컴퓨팅하는 지능정보체계 C4I로 이해하고 준비하는 것이 타당하다고 판단된다.

오늘날의 정보전은 단순히 유사시에만 있는 아군정보의 보호와 적군정보의 획득이나 교란을 포함하여 광의에서 경제정보전 및 사이버테러 등을 포함하여 심리적인 정서나 교묘한 문화의 침투까지도 동일한 대상으로 놓고 장기적으로 필요한 기반 요소기술들을 준비해야 한다. 그러한 종합적인 대응전략에서 각 조직이 가능한 역할을 분담하고 평상시에 법과 제도를 포함하여 기술 및 정책적으로 가능하도록 기획하고 조정해나가는 통찰력이 요구된다. 이제 정보전은 단순히 군부대 내에서만 일어날 수 있는 일부현상이 아니며, 정보시대의 특징을 반영하여 그 나라의 전체 기간산업구조, 정보보호산업과 전문 인력의 수준, 전체 구성원의 보안의식 그리고 법이

나 제도적인 정책지원이 필수적이다.

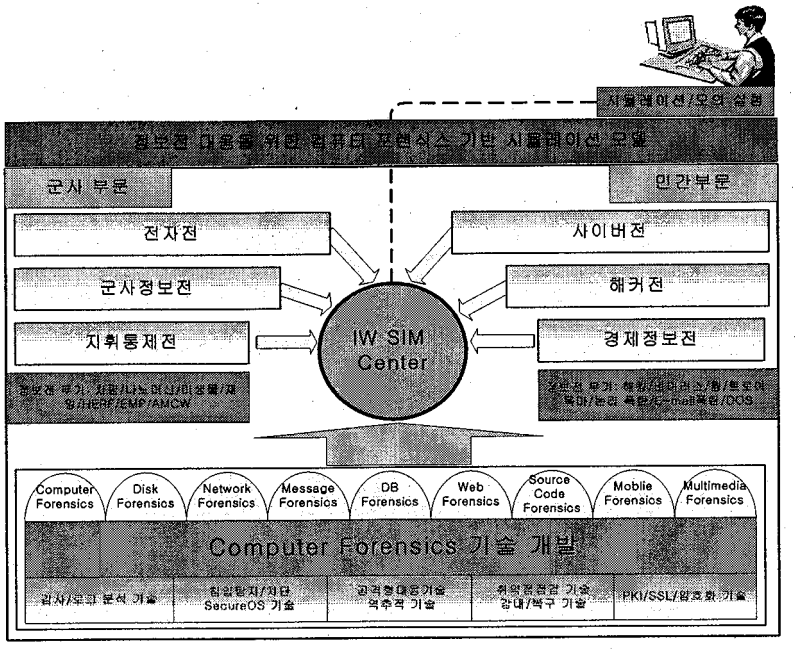
민간학교의 군사학은 일반인들이 접근하기 어려운 국방측면의 군사전문지식과 민간사회측면의 보안전문지식을 함께 교류 융합함으로써 정보전에 대비하여 특정 핵심기술을 집중 연구개발하고 이러한 사례를 기존의 군사학과 차별화하는 전문적 특성화가 추진되어야 한다. 따라서, 핵심기술 개발을 위한 특성화 전략으로 "정보전대응 컴퓨터 포렌식스 모의 실험실"을 구성하고, 군사학 전문가들과 컴퓨터 전문가들이 함께 보안침해사고로부터의 예방, 복구, 증거확보 그리고 역추적을 할 수 있는 실용적 도구들의 연구개발과 인력양성이 필요하다. 특히, 정보전의 위협 속에서 중요 정보시스템에 사용되는 시스템 소프트웨어나 포렌식스 도구들은 궁극적으로 자국의 기술로 개발한 완전한 믿음 속에서만 그 안전성을 담보할 수 있을 것이다.

컴퓨터 포렌식스 관련 기술들은 군사분야의 정보작전이나 민간분야의 경제적 정보전에서 공통적으로 사용할 수 있는 침해사고 대응 핵심기술로 새롭게 부각되고 있는 분야이다.

<표 5> 부분기능을 제공하는 포렌식스 도구들

기능	제품
디스크 조작, 포맷팅, 파티션	-ACARD: SCSI 와 IDE 어댑터 관련 도구, -CPR: Toolsthatwork.com의 도구, -Digital Intelligence: DriveSpy software 와 F.R.E.D 포렌식 하드웨어 도구, -Expert Witness: ASR Data의 포렌식 도구, -FTK: Access Data의 포렌식 툴 킷, -Digital Detective: 데이터 컨버젼 유틸리티., -IMAGE MASTER: 디스크 이미지 도구, -IMAGECAST: 디스크 복제 도구, -Maresware: 디스크, 파일 관련 도구, -Powerquest: 파티션, 디스크 이미지, 디스크 카피 도구, -SnapBack: 이미지 소프트웨어, -Sydex: Safeback 소프트웨어, -WINHEX: 편집기
데이터 복구	-AcoDisk: CD 데이터 복구, -Atlanta Computer Resources: 데이터 복구, -Computer Conversions: 데이터 복구.
Disk /text /hex editing	-Disk: 데이터 분석과 복구 도구. NTFS 디스크 지원, -EditPro: 윈도우 환경의 에디터, -Hex Workshop: Excellent editor, -File Maresware: Maresware 에디터, -VEDIT: text/hex 에디터, -WINHEX: Excellent editor, -NTFS: 디스크 에디터
다양성 있는 소프트웨어	-ASR Data: "SMART" 시리즈 컴퓨터 포렌식 도구, -AccessData: FTK(Forensic Toolkit), -Digital Intelligence: DriveSpy 소프트웨어와 F.R.E.D 포렌식스 하드웨어, -Expert Witness: ASR Data의 컴퓨터 포렌식 도구, -FTK: Access Data의 포렌식 툴킷, -Maresware: 컴퓨터 포렌식과 데이터 분석도구, -NTI: New Technologies의 컴퓨터 포렌식스 도구, -SysInternals: NT와 Windows 계열을 위한 소프트웨어
그래픽 뷰어 및 처리	-CompuPic: 파일 뷰어, -Conversions Plus: DataViz software의 MAC 포맷을 지원하는 데이바 컨버젼 소프트웨어, -DiskJockey: 파일 뷰어, -IrfanView: 그래픽 뷰어. 쉐어웨어, -Quick View: Inso의 파일 뷰어, -Thumbs Plus: 파일 뷰어, -Thumber: 디지털 이미지 처리 소프트웨어, -U.S. Navy: NCIS 소프트웨어
Hashing계산	-AccessData: SHA, -Digital Intelligence: DriveSpy, -Mares: Hash, Crckit, Diskcat, Disk_crc, MD5, -NTI: DiskSig, CRCMD5
Unix /Linux	-ForensiX: 리눅스 포렌식스 도구, -eXaminer: 디지털 증거 분석 도구, -NeoWorx: traceroute 보다 더욱 다양한 기능 제공, -SMART: ASR Data의 리눅스 컴퓨터 포렌식스 도구,
Windows 9X 관리자 툴	-Applog: 히스토리 검사 툴

[그림 2]는 컴퓨터 포렌식스 모의 실험실에서 수행될 수 있는 논리적 기술개발 분야의 개념을 나타내고 있다.



[그림 2] 컴퓨터 포렌식스 기술개발 전략

6. 결론

본 논문에서는 현대의 정보전 개념과 특징을 정의하고 이와 관련된 각종 위협요소들을 분석하였으며, 주요 국가들의 정보전 관련 최근동향을 조사하였다. 그리고, 미국을 중심으로 보안침해사고 대응을 위하여 새롭게 부상하고 있는 컴퓨터 포렌식스 기술을 소개하고, 미래의 정보전 환경에 대응하기 위한 국내의 개발전략과 필요

성을 제시하였다.

정보전 대응은 아군의 정보자원에 대하여 내외부의 공격으로부터 보호하기 위한 방어적 임무의 요소와 적군으로부터 필요한 정보를 획득하거나 교란하기 위한 공격적 형태의 요소로 구분할 수 있다. 현재까지의 국내기술은 대부분 방어적 임무의 침입차단시스템, 침입탐지시스템, 보안관제시스템 및 항바이러스 제품 등의 설치와 유해사이트 차단, 침해사고대응 공조 및 사이버범죄 수사 등의 활동이었다. 그러나, 미래의 정보전 환경은 보다 적극적 의지를 반영하여 특별한 임무를 갖고 있는 트로이목마, 바이러스 및 웜 등의 제작투입과 전문해커의 고용, 정보통신기반설비의 파괴 및 고가의 상용 사이버무기 개발 등 보다 공격적 형태의 양상을 가질 것이다. 이러한 공격은 군 관련 시설만이 아니라 국내의 민생 치안, 행정, 금융, 수도, 에너지, 교통의 정보통신체계를 비롯하여 각 가정의 개인 컴퓨터까지 대상이 될 수 있다.

우리나라는 미래의 정보전 공격에서 분명한 증거확보 및 역추적으로 공격자를 식별하고 실시간으로 대응함과 동시에 중요 정보자원에 대한 최선의 복구를 위하여 컴퓨터 포렌식스 도구를 자국의 기술로 확보할 수 있도록 노력해야 하며, 동시에 상대방을 효과적으로 타격할 수 있는 공격용 사이버 무기의 개발을 서둘러야 한다. 이러한 연구는 단기간 내에 성과를 거두기가 어려우므로 장기적인 계획을 갖고 선진 외국의 기술을 조기에 도입활용하고, 이러한 도입기술의 원초적 분석과 지속적인 연구를 통하여 국산화 해 나가는 전략이 필요하다. 따라서, 미래전장에서 핵심적 정보전 요소가 될 수 있는 다양한 분야중에 효과적 연구개발과 역할 분담이 가능한 컴퓨터 포렌식스 모의실험실을 군사학과가 창설된 대학에 설치하여 필요한 방어와 공격적 무기들을 개발하고 가상적 공격을 통하여 미리 시뮬레이션하면서 필요한 도구들을 지속적으로 업그레이드 준비

해 나가는 정책적 선택이 요망된다.

끝으로 컴퓨터 포렌식스는 전자적 증거를 제공하는 법의학적 측면 및 보안침해사고를 기술적으로 복구하는 산업재해 복구 측면에서도 흥미로운 주제가 될 것이다. 그러나, 이러한 기술들이 필요하고 계속 발전한다는 것은 인간이 범죄심리에 취약하다는 것이므로 보안기술개발에만 진력하기보다는 보안을 침해하지 않도록 의식을 진화시키는 일은 더욱 시급하고 중요한 우리 인간들의 사명일 것이다.

< 참고문헌 >

[1] 고병수, 박영신, 최용락, 2003, "보안침해사고 대응을 위한 컴퓨터 포렌식스 기술동향", 인터넷정보학회지, 4권 1호, pp.37-46, 한국인터넷정보학회.

[2] 권태환, 황호상, 2002, "정보전 개념", 정보보호학회지, 12권 6호, 한국정보보호학회.

[3] 박상서, 박춘식, 2002, "정보전 위협과 사례", 정보보호학회지, 12권 6호, 한국정보보호학회.

[4] 박상서, 김현수, 2003, "미국의 국가 사이버보안 및 국방 정보전 대응체계", 한국사이버테러 정보전학회지, pp.68-77, 한국사이버테러정보전학회.

[5] 엘빈 토플러, 1996, "전쟁과 반전쟁", 한국 경제신문사 번역.

[6] 오제상, 2002, "사이버정보전 즉시 준비해야", 정보보증논문지, 1권 1호, 한국사이버테러정보전학회.

[7] 이철원, 장병화, 이철수, 2002, "주요국 정보전 대응체계와 동향", 정보보호학회지, 12권 6호, 한국정보보호학회.

[8] Eoghan Casey, 2001, *"Handbook of Computer Crime Investigation: Forensic Tools & Technology"*, Academic Press.

[9] Eoghan Casey, 2001, *"Digital Evidence and Computer Crime"*, Academic Press.

[10] Executive Order 13228 of Oct. 8, 2001, *"Establishing the Office of Homeland Security and the Homeland Security Council"*.

[11] Jane's Intelligence Review, 2000.12., pp.32-36.

[12] John R. Vacca, Michael Erbschloe, 2002, *"Computer Forensics: Computer Crime Scene Investigation (With CD-ROM)"*, Charles River Hedia.

[13] Kevin Mandia & Chris Prosise, *"Incident Response - Investigating Computer Crime"*, McGraw-Hill.

[14] Kretzer, 2002, *"Air Force Information Warfare Center: Taking IW Combat Power to the Warfighter"*, InfowarCon.

[15] Martin Libicki, 1995, *"What is Information Warfare?"*.

[16] White House, Feb. 2003, *"The National Strategy to Secure Cyberspace"*.

[17] White House, Feb. 2003, *"The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets"*.

[18] Winn Schwartau, 1996, *"Information Warfare Chaos on the Electronic Superhighway"*, Thunders Mouth Press.

A Simulation Model for the Response of Information-Warfare based on Computer Forensics

Choi, Yong-Rak · Ko, Byung-Soo · Park, Myung-Chan

While the social activities using Internet become generalized, the side effect of the information security violation is increasing steadily and threaten the countries which is not ready to prevent from offensive penetration such as the Information-fighter or Cyber-military. In this paper, we define the concept and characteristics of the modern Information-Warfare and analyze various kinds of threatened elements and also examine the recent trend in other countries. And introducing Computer Forensics raised recently for the confrontation against the security violation in the future, we will show the developing strategies and the necessity in order to response cyber attacks. These developing strategies can be used to ensure and re-trace the technical evidence for the security violation and to achieve the disaster relief effectively. So we hope that can apply them to the actual preparation through developing cyber trial test of the defense and attack for the Information-Warfare.

Keywords : Forensics, information security violation, Cyber-military, Information-Warfare