情 報 保 護 學 會 誌
第21卷 第6號, 2011. 10

사이버전을 위한 보안기술 현황과 전망

서 동 일*, 조 현 숙**

요 약

전장의 양상이 물리적인 대량살상을 중심으로 한 전통적인 재래전에서 눈에 보이지 않는 사이버전으로 변화되고 있는 시점에서 이에 대비하기 위한 사이버전 공격 및 방어기술은 매우 중차대한 문제이다. 사이버전을 위한 보안 기술로는 암호·인증·인식·감시와 같은 정보보안 핵심원천 기술, 분산서비스거부공격 대응기술, 스마트 아이디 기술, 영상보안 및 바이오인식 기술, 부채널 공격 방지 기술 등이 있다. 이러한 기술들은 사이버전을 위해 사용될 수 있는 매우 명확한 분야라 할 것이다. 또한, 사이버전 기술로는 암호·인증·인식·감시와 같은 핵심 원천 기술 및 기존 보안 기술 분야를 포함하고 초경량 고비도 암호화 기술, 밀리터리 포렌식 기술, 사이버공격 근원지 역추적 기술, 사이버 공격 정보공유 협업관제 기술, 사이버 공격 무기 제작 기술 등이 있다. 특히, 사이버전은 작은 비용으로 최대 효과를 거둘 수 있는 비대칭 전력의 매우 중요한 분야이며, 주요 선진국들은 사이버 공격에 대한 자위권 확보 차원에서 사이버전에 대한 기술적·제도적 준비를 서두르고 있는 상황이다. 본 기고문에서는 이와 같은 사이버전을 위한 보안 기술 현황과 전망을 살펴보고자 한다.

Ⅰ. 서 론

사이버 무기화된 최초의 악성코드로 알려진 스턱스넷(Stuxnet) 공격은 사이버전쟁이 생각보다 우리들의 일상 생활 속에 더욱더 깊숙이 들어와 있음을 보여준 단적인 일예로 볼 수 있다. 사실 최초의 전면적 사이버전으로 알려진 2007년 에스토니아전을 시발점으로 하여 인터넷을 중심으로 한 사이버 냉전시대의 도래는 정보통신 기술의 발전과 함께 더욱 더 기승을 부리고 있는 사이버테러(사이버 침해사고)를 중심으로 급격히 확산되고 있으며 그 위험성이 급격히 높아지고 있는 상황이다.

사이버 냉전의 기운이 확산되면서 미국의 오바마 정부는 사이버 침해사고(해킹 등)를 국가 안보의 제1위협으로 규정하는 등 전통적인 전쟁양상에서 눈에 보이지 않는 사이버전으로 전장의 양상이 변화되고 있는 것이다. 특히 모든 전력 요소들이 유기적인 연결을 통하여 통합 작전체계를 구성하는 네트워크 중심전 (NCW: Network-Centric Warfare)으로 작전 수행이 변화되고 있는 국방 분야는 그 영향력이 더욱 더 커지고 있는 상황이다. 즉, 기존 재래전에서는 물리적인 파괴를 중심으로 전쟁이 수행되었다면 현재는 전쟁 수행체계를 마비시키는 사이버 전쟁으로 발전되고 있는 것이다.

이러한 사이버전은 현재 매우 다양하게 정의되고 있으며, 사이버 첩보전, 사이버 테러전, 사이버 심리전, 물리적 연계전 등을 포괄하고 있는 총괄 개념으로 볼 수 있다. 예를 들어, 전쟁으로서 사이버전(Cyber War)은 컴퓨터 시스템, 네트워크 통신망 등을 교란, 마비 및 무력화시킴으로써 적의 사이버 체계를 파괴하고 아군의 사이버 체계를 보호하는 것으로 규정할 수 있으며, 현대는 지상전, 해상전, 공중전, 우주전과 함께 이러한 사이버전을 5차원 전쟁의 한 분류로 나누고 실질적인 작전을 수행하는 하나의 전쟁으로 인식하고 있는 것이다. 이러한 사이버전은 앞서 본 바와 같이 인터넷에 연결된 PC 및 네트워크를 불능화하는 행위라든지 해킹 기술을 이용하여 개인, 경쟁자, 정부 등이 보유한 정보를 허락없이 획득하는 행위와 같은 사이버테러(CyberTerror) 행위를 포함하고 있다.

사이버전의 특징은 저비용의 전쟁수행이 가능하고, 적군과 아군의 식별이 곤란하며, 조기 경보 및 공격징후 포착이나 공격대응 시간의 확보가 곤란하며, 전투피해 평가의 곤란, 법적 제재 근거 미흡 등 매우 다양하게 나

* 한국전자통신연구원 인프라보호연구팀(bluesea@etri.re.kr)
** 한국전자통신연구원 지식정보보안연구부(hscho@etri.re.kr)

타나고 있다. 따라서, 이러한 사이버전은 방어자 보다는 공격자에게만 매우 유리한 전쟁 양상이며, 이를 수행하는 수행자 역시 국가 단위뿐만 아니라 누구나 소프트웨어 개발 능력만 있으면 사이버 전쟁무기를 제작, 구매, 대여하여 전쟁을 수행할 수 있다는 특징을 가지고 있다. 또한, 사이버전의 무기는 일부 물리적인 피해를 동반하기도 하지만 대부분의 경우에는 물리적 피해와는 관련이 없어 전통적인 무기 개념에 포함되지도 않고 있다. 사이버 공격은 좀비PC의 이용, 타국 서버 경유 등을 통해 이루어져 공격자 식별 및 확인이 어렵고, 이를 방어하기 위해서는 매우 높은 수준의 부담을 지우고 있으며, 공격자 역추적 및 식별의 어려움으로 정당한 보복과 처벌을 통한 전쟁 억제를 힘들게 하는 특징도 가지고 있다. 반대로 네트워크 통신망은 전세계 국가가 인터넷으로 연결됨에 따라 사이버 공격은 공격자에게도 전파되어 피해를 당할 가능성도 존재하고 있다[1].

이와 같은 국제 평화와 안보를 위협하는 사이버전을 피하기 위해 국제 협력을 논의하는 기구로는 EWI (EastWest Institute)가 있다. EWI에서는 사이버 충돌 관련하여 제네바 협약과 헤이그 협약을 사이버 공간에서 어떻게 해석하고 적용할 것인지에 대한 논의를 구체적으로 진행하고 있다. 여기에서는 제네바 협약과 같은 기존 국제 전쟁 규약을 사이버전 환경으로 확장하기 위해 사이버전을 4가지 체계로 카테고리화 하였으며, 기존 전쟁법에 대한 분석을 통하여 10가지 공동 발견점(Joint Observations)을 제시하였고, 사이버 환경 하에서 제네바 협약 등이 명시하고 있는 인도주의 관련 핵심 기반시설을 보호하기 위하여 5가지 공동제안을 제시하였다[2].

10가지 공동 발견점은 다음과 같다. 사이버 공간에서는 보호해야 할 핵심기반시설과 보호하지 않아도 될 핵심기반시설이 혼재되어 있고, 보호되어야 할 인도주의적 핵심기반시설의 보호 여부에 대한 표시가 부족하며, 사이버 공간에서는 군사적 목표와 민간 목표에 대한 구별이 어렵다. 정보통신기술은 각종 협약이 요구하고 있는 인도주의적 요구 사항을 이행하는 데 있어 도움이 될 수 있고, 사이버 공간에서는 비국가 주체와 네티즌은 높은 권력을 행사하고 있으며, 사이버 무기는 기존 재래식 무기와는 다른 양상을 보일 뿐만 아니라, 전쟁법을 만들 때 고려되지 않은 성격을 갖고 있다. 군은 사이버 무기를 기밀로 하기를 원할 것이며, 정보통신과 사이버 공간의 복잡성은 이들의 특성과 한계에 대한 미신을 증폭시킬 것이고, 사이버 군사작전은 발각되지 않고 수행될 것이며, 이러한 특성은 문제를 발생시킬 것이다. 마지막으로 사이버전에 관한 모호한 성질들은 서로 다른 접근법을 제안하도록 할 것이다.

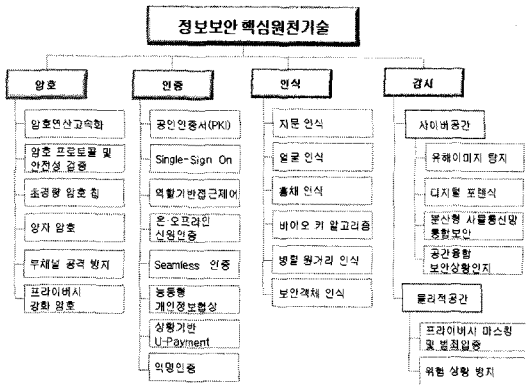
다섯가지 공동제안은 아래와 같다. 첫째, 제네바 협약에서 인도주의적(Humanitarian Focused) 주체들과 인원에 대하여 특정 조건하에서 보호 수단을 제공하는 조항을 사이버 공간에서 적용하기 위한 노력이 필요하다는 점. 둘째, 국제 협약에서 명시하고 있는 보호되어야 할 주체를 사이버 공간에서 어떻게 식별 표시(Distinctive Emblem)할 것인지를 제정하여야 한다는 점. 셋째, 물리적인 전쟁은 국가 단위의 세력에 의해 수행되지만, 사이버 공간에서는 비 국가주체와 네티즌(Netizen)에 의하여 이루어질 수 있다는 사실을 인식할 필요가 있다는 점. 넷째, 물리적 전쟁에서 금지하고 있는 생화학 무기 같은 것들이 사이버 무기상에 존재한다면 이들의 영향 등을 논의하고 이를 사이버 공간에서 금지할 필요가 있다는 점. 다섯째, 각종 재래식 전쟁에 대비한 국제 협약은 이를 적용할 시기가 대부분 명확하지만, 사이버전쟁은 사이버전의 특징상 전쟁 혹은 평화의 이분법적 분류가 아닌 '전쟁과 다른 형태'를 고려할 필요가 있다는 점 등이다[3].

지난 5월 월스트리트 저널은, 미 국방부가 국가 기간망을 흔들 수 있는 중대한 사이버 공격에 대하여 이를 전쟁 행위로 간주하고 무력 대응할 방침을 세웠다고 보도한 바가 있다. 즉, 사이버전은 또 다른 물리적인 재래식 전쟁을 유발할 수도 있는 것이다.

본 기고문에서는 이와 같은 사이버전에 대응 할 수 있는 기존 보안기술 개발 현황을 제2장에서 알아보고, 제3장에서 사이버전 공격과 방어기술을 살펴본 후 제4장에서 결언 및 향후 우리가 해야 될 일들에 대해 살펴보고자 한다.

Ⅱ. 사이버전을 위한 보안기술 현황

여기서는 현재까지 개발되었거나 개발이 진행 중인 여러 가지 사이버 보안 기술을 알아본다. 여기에는 암호·인증·인식·감시와 같은 정보보안 핵심원천 기술, 분산서비스거부공격 대응기술, 스마트 아이디 기술, 영상보안 및 바이오인식 기술, 부채널 공격 방지 기술 등이 있다. 이러한 기술들은 사이버전을 위해 사용될 수 있는 매우 명확한 분야라 할 것이다.



〔그림 1〕 정보보안 핵심 원천 기술 리스트

1) 핵심 원천 기술 리스트

정보보안 기술은 암호, 인증, 인식, 감시 기술을 기반으로 하여 많은 응용 기술, 융합 기술 들이 발전되고 개발되어지고 있다. 이러한 기술들의 리스트는 [그림 1]과 같다. 이러한 핵심 원천기술 들은 사이버전을 위한 공격과 방어기술에서도 기반기술로써 사용되고 있으며, 이를 지속적으로 발전시켜나가야 함은 당연하다 할 것이다.

2) 분산서비스거부공격(DDoS) 대응기술

분산서비스거부공격은 시스템 혹은 네트워크의 가용성을 떨어뜨리기 위한 공격기술이다. 이러한 공격을 방어하기 위한 기술 개발은 최근의 7.7 DDoS 공격이나 3.4 DDoS 공격 사례에서 알 수 있는 것처럼 사이버전뿐만 아니라 일반적인 인터넷 사용을 안전하게 하기 위해서도 그 필요성은 매우 높은 것이다.

특히, 최근에는 인터넷과 같은 네트워크 통신망의 매우 빠른 발전과 함께 40기가급 이상의 DDoS 공격 탐지를 위한 하드웨어 플랫폼이나, 단위 서버에서 활용될 수 있는 Secure NIC(Network Interface Card) 기술 개발이 활발히 진행되고 있다.

또한, 인터넷 서버를 이용하는 많은 응용계층 서비스는 웹기술을 기반으로 하는 경우가 많아지고 있어 이를 방어할 수 있는 DDoS 방어기술 및 모든 인터넷 구간에서 통합적인 대응을 수행할 수 있는 통합보안기술을 포함하여 개발되고 있다.

3) 스마트 아이디(Smart ID) 기술

인터넷과 같은 통신망을 안전하게 사용하기 위해서는 본인을 증명할 수 있는 아이디 기술이 매우 중요한 원천기술 중 하나이다. 특히 최근 급속히 진행되고 있는 모바일 환경은 스마트폰과 같은 통신 수단을 활용하여 언제 어디서나 수행 가능한 지불, 인증, 구매 등 다양한 실생활을 모바일 환경에서 구현하고 있으며, 이러한 환경에서 개인의 중요 정보를 보호하고 프라이버시를 보장하기 위해서는 더욱더 안전하고 편리한 스마트 아이디 기술이 필요한 것이다.

또한, 디지털 정보의 급격한 증가에 반해 관리되지 않은 사용자 특정(Identity) 정보가 급속히 증가하고 있으며, 개인별 가치 창출이 가능한 개인화된 서비스들을 위해서는 프라이버시가 보호되면서 개인정보를 활용할 수 있는 안전한 정보 공유 체계 또한 필요하다.

이러한 스마트 아이디 기술 분야로서 최근 자기통제 강화형 전자아이디지갑 기술, 스마트 지갑 기술, 바이오 인식 기술, 자가 인증(Self-Certifying) 기술, 모바일 클라우드 통합 인증 기술 등이 연구 개발되고 있다. 미국에서는 신뢰할 수 있는 사이버 공간에서의 아이디 정책을 수립하여 추진하고 있는 중이다[5].

4) 영상보안과 바이오 인식 기술

개인 신변안전 보장을 위해 신뢰성과 이기종 영상 보안 장비간 상호 호환성이 보장되는 영상보안기술은 최근 CCTV(Closed-Circuit Television)를 이용한 범죄자 추적 등과 같은 적극적인 활용이 증가하면서 그 중요성이 더욱더 커지고 있는 상황이다. 또한 이러한 영상 화면을 통하여 특정 개인을 찾아 낼 수 있는 바이오 인식 기술 또한 연구 개발 활동이 활발한 분야중 하나이다. 특히 CCTV 환경에서 얼굴, 귀모양, 걸음걸이, 행동패턴, 외형 등과 같은 사람정보를 추출하여 실시간으로 사람을 식별·추적·검색할 수 있는 원거리 사람 식별기술이 개발되고 있는 중이다. 여기에는 환경 변화에 민감한 영상인식기술의 성능 특성에 따라 더욱 더 효율적인 영상인식이 가능하도록 하는 기술도 포함되어 있다. 최근에는 장애인과 청소년들을 대상으로 한 성적 범죄의 증가, 묻지마 범죄와 같은 무차별적인 강력사건의 증가 등에 따라 이들을 추적할 수 있는 보안 기술도 많은 분야에서 개발되고 있다.

그러나 이러한 기술들은 영상 정보를 오·남용할 수 있는 역기능이 함께하고 있으며, 이를 방지하기 위한 개인 프라이버시 보장 기술이 동시에 발전되어야 할 분야일 것이다.

5) 부채널 공격 방지 기술

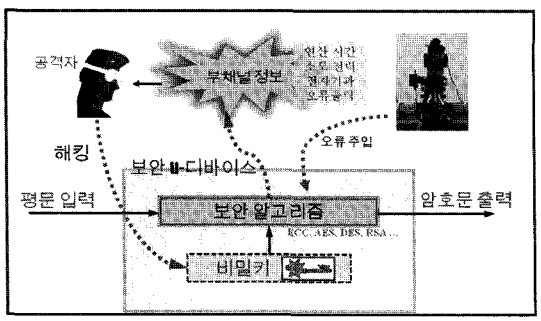
부채널 공격(Side-Channel Attack)이란 [그림 2]와 같이 암호 모듈이 다양한 디바이스에 탑재되어 구동되는 동안 발생하는 각종 부가적인 정보(예를 들어, 구동 시간, 발열, 소리, 전력소모량, 전자기파, 오류주입결과 등)를 이용하여 암호 모듈의 비밀 정보를 크랙킹 하는 공격 기술을 말한다.

최근 스마트폰과 같은 모바일 환경 구축이 급속히 진행됨에 따라 보안토큰, 전자태그, 스마트기기, IC카드 등 보안 기능을 내장하고 있는 소형 정보기기의 사용이 급증하고 있는 상황이다. 이에 따라 이러한 소형 전자기기에 대한 부채널 공격에 의한 복제 위협도 점차 증가하고 있으며, 전자 금융 서비스에 사용하는 금융 IC카드나 전자여권 등의 복제 가능성은 심각한 사회적 비용과 국가 사회적인 위협을 초래할 수 도 있는 매우 중대한 위협인 것이다.

Ⅲ. 사이버전 공격과 방어기술

여기서는 사이버전 공격과 방어기술의 핵심 분야를 살펴보고자 한다. 사이버전을 위한 기반기술은 앞서 제2장에서 살펴본 바와 같은 암호·인증·인식·감시와 같은 핵심 원천 기술 및 기존 보안 기술 분야를 포함하여 초경량 고비도 암호화 기술, 밀리터리 포렌식 기술, 사이버공격 근원지 역추적 기술, 사이버 공격 통합대응 기술, 사이버 공격 무기 제작 기술 등이 있다.

특히, 사이버전은 작은 비용으로 최대 효과를 거둘 수 있는 비대칭 전력의 매우 중요한 분야이며, 주요 선진국들은 사이버전에 대한 기술적·제도적 준비를 서두르고 있는 상황이다.



〔그림 2〕 부채널 공격 개념도

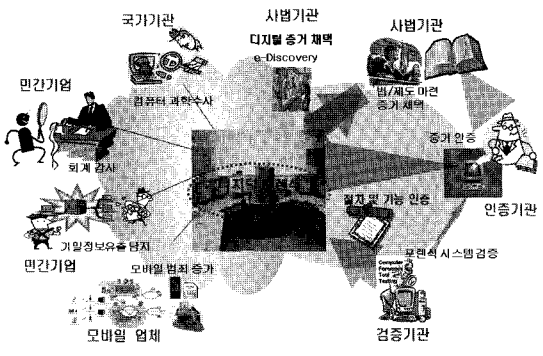
1) 초경량 고비도 암호화 기술

차세대 군 전술정보통신 체계에서는 이동 중에도 활용 가능한 다양한 전자기기가 있으며 이를 통한 정보의 교환에는 고비도 암호화 기술이 필수적으로 소요될 것이다. 따라서 최신 암호해독 기술을 분석하고 이를 바탕으로 최근의 복합 통신 환경에서 동작할 수 있는 암호 논리 및 최적화된 모듈을 개발하고, 이에 대한 안전성을 입증하는 등 초경량 고비도 암호화 기술은 사이버전 공격과 방어 기술의 기반이 되는 분야이다.

2) 밀리터리 포렌식 기술

일반적인 디지털 포렌식(Digital Forensic) 기술은 컴퓨터와 같은 정보기기 장치에 내장된 디지털 자료를 근거로 삼아 그 장치를 매개체로 발생한 어떤 행위의 사실 관계를 규명하고 증명하는 기술을 말한다. 이러한 디지털 포렌식의 적용 개념은 [그림 3]과 같다.

여기에는 컴퓨터를 매체로 한 증거 수집 및 분석을 위한 컴퓨터 포렌식 기술, 핸드폰, 스마트폰 등과 같은 이동형 정보기기에 대한 모바일 포렌식 기술, 네트워크의 사용자 추적 및 로그 분석을 위한 네트워크 포렌식 기술, 이진코드나 소스코드를 분석하여 복제하거나 재활용 여부를 판단하는 소프트웨어 포렌식 기술, 디지털



〔그림 3〕 디지털 포렌식의 적용 개념도

포렌식을 어렵게 하는 기술에 대응하는 항포렌식 기술, 휘발성 데이터에 대한 증거 수집 및 분석을 위한 활성 데이터 포렌식 기술, 기업내부 전자 증거 확보 및 법적 자료 제출을 위한 e-Discovery 기술, 카메라나 CCTV 등에서 증거를 수집하고 분석하는 비디오 포렌식 기술 등이 포함된다.

일반적인 디지털 포렌식 기술에 있어서 핵심 기술 영역은 디지털 증거를 확보하는 기술과 디지털 증거를 조사 분석하는 기술이 있다. 디지털 증거 확보 기술에는 저장매체 복제 및 이미지 인식 기술, 활성 데이터 수집 및 분석 기술, 디지털 증거 무결성 확보 기술, 모바일 포렌식 기술 등이 있다. 디지털 증거 조사분석 기술에는 삭제·손상 데이터 복구 기술, 데이터 고속 검색·분석 기술, 패스워드 검색 및 암호 해독 기술, 정보은닉 탐색 및 추출 기술 등이 있다.

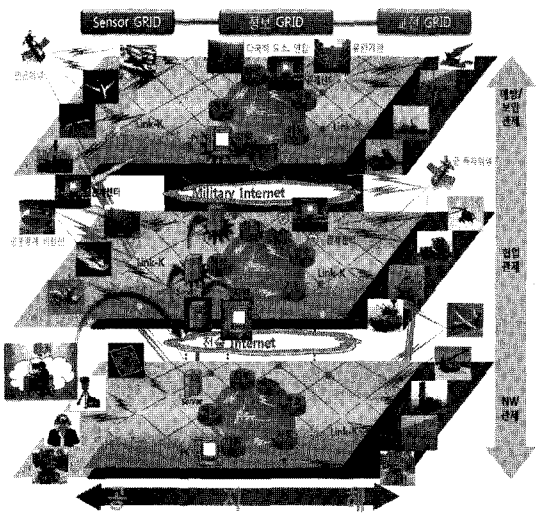
밀리터리 포렌식(Military Forensic)이란 차세대 군 전술정보통신 체계를 비롯한 국가 기간망에 대한 사이버 공격 시, 관련 정보기기 장치에 내장된 디지털 자료를 근거로 삼아 그 장치를 매개체로 발생한 어떠한 행위의 사실 관계(예를 들어, 공격방법, 공격자 위치, 공격자 등)를 규명하고 증명하는 기술을 말한다.

특히, 밀리터리 포렌식 기술을 통해 공격 근원지에 대한 대응 공격의 국제적 명분 확보가 가능하여야 한다. 이는 최근의 사이버 공격(침해사고 등)을 자국에 대한 물리적 공격과 동일시 여기는 국제적인 사이버전 개념 추세에 따라 매우 중요한 목적 중 하나일 것이다.

이를 위해서는 다양한 군 환경에 적합한 디지털 증거를 수집하는 기술, 공격자의 근원지 역추적 기술, 코드 역분석 방지 기술, 모바일 포렌식 기술, 영상 포렌식 기술 등을 필요로 한다.

3) 근원지 역추적 및 정보공유 협업 기술

공격자의 근원지를 역추적하는 기술은 사이버전을 예방하고 방어하기 위한 매우 효율적인 수단을 제공한다. 이를 위해서는 밀리터리 포렌식 기술을 기반으로 하여 사이버 공격의 근원지를 역추적 할 수 있는 기술 개발이 필요하며, 사례기반추론 및 유사도 측정기법 등을 통한 제로데이(zero-day) 공격 탐지 기술, PC와 개인용 모바일 기기 등을 포함하는 복합 경로에 대한 공격 관련 정보 도출 및 예측 기술 등의 연구 개발이 필수적으로 필요할 것이다.



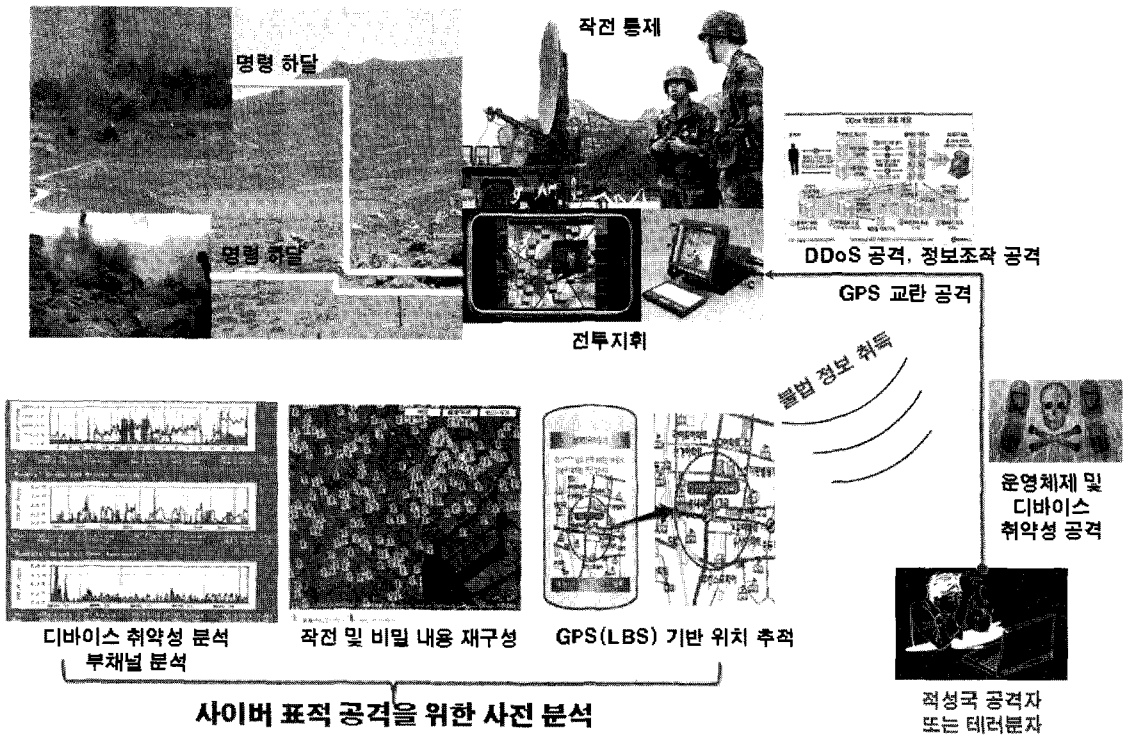
〔그림 4〕 정보공유 협업 기술 적용 개념도

사이버전은 그 특성상 민·관·군을 구분하지 않고 이루어질 가능성이 매우 높다. 예를 들어 인터넷과 같은 네트워크는 전방위적으로 구성되어 있으며, 어느 한 통신망을 통해서 또 다른 통신망으로 공격의 파급효과가 연속적으로 전파될 가능성이 매우 높은 것이다. 따라서, 이러한 사이버전의 특성에 따라 사이버전을 방어하기 위해서는 육·해·공군의 사이버 상황 정보 뿐만 아니라 민간 영역에서의 사이버 상황 정보도 공유할 수 있는 [그림 4]와 같은 협업 관제기술이 필수적으로 소요될 것으로 보인다. 이러한 협업 관제기술은 앞서 살펴본 밀리터리 포렌식 기술과 연동되어 사이버 공격자의 근원지를 역추적 할 수 있는 효율적인 방법을 제공할 것이다.

4) 사이버 공격 무기 제작 기술

공격과 방어 기술의 적절한 균형은 사이버 전쟁 억지력을 보유하는 효과적인 방법중 하나이다. 따라서, 사이버전에 있어서 공격 진원지를 역추적한 이후 사이버 대응 공격을 위한 사이버 공격 무기 제작 기술은 매우 중요한 분야중 하나이다.

이러한 기술 영역에는 최근의 분산서비스거부공격에 활용되고 있는 봇(Bot) 기술, 스턱스넷과 같은 산업기반 시설용 제어시스템(SCADA: Supervisory Control and Data Acquisition)에 대한 악성코드 제작기술, EMP(Electromagnetic Pulse) 폭탄 기술, 논리 폭탄 기술, AMCW (Automatic Mobile Cyber Weapon) 기술 등이 있다.



〔그림 5〕 사이버공격의 일예: 사이버 이동 표적 공격 기술 개념도〔1〕

[그림 5]는 이러한 사이버 공격의 일예로서 사이버 이동표적 공격 기술의 개념도이다.

Ⅳ. 결 론

전장의 양상이 물리적인 대량살상을 중심으로 한 전통적인 재래전에서 눈에 보이지 않는 사이버전으로 변화되고 있는 시점에서 이에 대비하기 위한 사이버전 공격 및 방어기술은 매우 중차대한 문제일 것이다.

미국 오바마 정부는 국가 핵심 아젠더로 지정한 사이버보안과 관련된 국가정책, 체계 등을 전반적으로 검토하여, 향후 미국의 신뢰할 수 있는 영속적인 디지털 인프라 구축을 위한 구체적인 검토의견 및 실행계획 등을 발표한 바 있다. 여기에는 상위 수준에서의 리더쉽 발휘와 디지털 국가로서의 역량 구축, 효과적인 정보공유 및 사고대응체계 구축, 사이버보안을 위한 연구 활동 강화 등을 제시하고 있다[4].

또한 미국은 중대한 사이버 공격에 대해 이를 전쟁행위로 규정하고 이에 대한 사이버 공격의 자위권(Right of Self-Defense)을 가질 수 있음을 천명하고 있다[6].

이러한 사이버전의 특징은 모든 전력 요소들이 유기적인 연결을 통하여 통합 작전체계를 구성하는 네트워크 중심전(NCW: Network-Centric Warfare)이며, 사이버전 기술을 활용할 수 있는 우수한 기술적 인력을 중심으로 한 인간중심전 (Human-Centric Warfare)이고, 동시에 사이버 공격 및 방어 기술을 확보하여 전쟁 억지력을 제공 하는 기술중심전(Technology Warfare)이며, 지금 현 시점에 사이버 공간을 중심으로 하여 이미 전쟁이 진행되고 있는 현재전(Present Warfare)이라는 점을 들 수 있다.

향후에는 EWI 국제 공동연구를 통해 나타난 바와 같은 여러 가지 사이버 전쟁 관련 국제 조약 수립과 사이버 무기 이용 규제 협약 등을 마련하기 위한 활동이 더욱더 많아질 것이며, 국제적으로 사이버 전쟁 억지력(Deterrence)을 확보하기 여러 가지 방안들이 심화 발전될 것으로 보인다. 이러한 활동들은 물리적 공격 능력을 보유 하므로써 전쟁을 억제하는 것처럼 사이버전을 억

제하기 위한 방편일 것이다.

따라서 앞서 살펴본 바와 같은 사이버 보안 기술을 활용하여 사이버 공격 기술 및 무기를 연구개발하고 사이버 전쟁을 수행할 수 있는 인력을 양성하여야 하며, 국가 안보 차원에서의 대응책 마련과 국민들의 사이버 보안 인식 제고를 위한 홍보·교육 강화가 매우 중요할 것으로 판단된다.

참고문헌

[1] 조현숙, "사이버 냉전시대: 현황과 미래과제", KOFST Issue Paper 2011-3호, 2011.8월

[2] EastWest Institute (EWI), http://www.ewi.info

[3] EWI, "Working Towards Rules for Governing Cyber Conflict" 2011. January

[4] U.S. White House, "Cyberspace Policy Review" 2009. May

[5] U.S. NIST, "National Strategy for Trusted Identities in Cyberspace", 2010. June

[6] U.S. White House, "International Strategy for Cyberspace", U.S. White House, 2011 May

[7] 문종식, 이임영, "사이버테러 동향과 대응방안", 정보보호학회지 제20권 제4호, pp.21-27, 2010년 8월

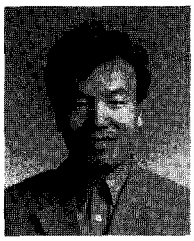
[8] 김지훈, 조시행, "사이버 환경에서의 보안위협", 정보보호학회지 제20권 제4호, pp.11-20, 2010년 8월

[9] 이상호, "군사전략차원에서 정보·사이버전의 효용성", 세종정책연구 제6권 1호, pp.41-72, 2010년

[10] James A. Lewis, "Cyberwar Thresholds and Effects", IEEE Security and Privacy, pp.23-29, Sep./Oct. 2011

[11] Ralph Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon", IEEE Security and Privacy, Vol.9 No.3, pp.49-51, May/June 2011

〈著者紹介〉



서 동 일 (Seo, Dong-il)
정회원
1989년 2월 : 경북대 전자공학과 졸업
1994년 2월 : 포항공대 정보통신과 석사
2004년 8월 : 충북대 전산학과 박사
1994년 3월~현재 : 한국전자통신연구원 팀장(책임연구원)
<관심분야> 인터넷정보보호, 미래인터넷 보안 등

조 현 숙 (Cho, Hyun Sook)
정회원
1979년 2월 : 전남대 수학교육 졸업
2001년 2월 : 충북대학교 박사
1982년 3월~현재 : 한국전자통신연구원 부장(책임연구원)
<관심분야> 인터넷정보보호, 물리보안, 융합보안 등