정보전 개념과 대응 기술

국가보안기술연구소 박상서* · 이진석 · 박춘식

1. 서 론

인류가 수행해 온 전쟁의 원인과 사용된 기술, 전략과 전술의 변화 등을 보는 관점은 연구자들에 따라 다양하다. 하지만, 미공군 대령 젠슨(Col. Owen E. Jensen, USAF)은 전쟁을 사회에서 부를 획득하기 위한 방법의 확장으로 보고 시대를 생산 방식(즉 생산 기술)에 따라 농업시대, 산업시대, 정보시대로 분류하고 정보전은 제3의 물결인 정보시대의 전쟁방법이라고 정의한 토플러 부부의 방법이 "정보전이 출현된 배경을 설명하는데 가장 명확하고 정확하다"고 하였다.

해니(Reto E. Haeni)[1]는 토플러 부부가 제시한 시대 구분을 토대로 각 시대별 전쟁의 특징 등을 참조하여 시대별 전쟁 양상의 변화를 표 1과 같이 설명하고 있다.

표 1 시대별 전쟁 양상 변화

구분 \ 시대	농업시대	산업시대	정보시대
전쟁수행주체	무사계급, 용병, 시민군	직업군인, 시민	정보에 능통한 전사
부의 원천	물물 교환	화폐	데이터베이스 등에 저장된 심볼
전쟁 특징	대리전	대량 군대 다수 사상자	정보 공격 소수 사상자
파괴 수단	화약	대량 파괴 (핵, 화학무기 등)	중요 정보 삭제
지휘 구조	계층 구조	하향식 구조	평면 구조
정보기반전쟁	○	○	○
정보기술을 전쟁에 사용	×	○	○
정보에 대한 전쟁	×	×	○

유형의 물질이 부의 원천이었던 앞의 두 시대와 달리, 무형의 정보가 부의 원천이 되는 정보시대에는 정보와 정보기술은 전쟁 수행의 수단뿐 아니라 전쟁의 대상이 된다. 또한, 손자가 주장한 바와 같이 "적을 죽이지 않고 적을 정복하는 것"을 전쟁의 목표로 삼게되어 살상이 수반되는 전쟁은 가능하면 피하고 정보와 정보기술을 이용하여 적을 제압하는 방식의 전쟁을 수행하게 된다. 그리고, 정보시대의 전쟁은 정보가 공격과 방어의 대상이 되므로 적의 정보가 있는 곳은 우주와 사이버 공간을 막론하고 전장이 된다.

걸프전은 흔히 최초의 정보전으로 평가되고 있으며 앞에서 살펴본 정보시대의 전쟁 양상을 잘 보여주고 있다[2]. 즉, 다국적군은 적의 정보 흐름을 마비시키고 적에 대한 정확한 정보를 획득하는데 주력하였고, 이라크는 대량 살상 파괴 무기를 위주로 전쟁을 수행하였다. 다국적군은 이라크의 정보 흐름을 마비시키기 위해서 이라크의 C3I 체계와 통신망을 전쟁 초기에 파괴함으로써 전쟁기간 내내 이라크에 대해서 지휘통제의 우위를 유지하였다. 또한 이라크의 전장 데이터 수집 체계를 전쟁 초기에 10분의 1이상을 파괴하고, 항공 정찰과 상용 위성을 이용한 첩보 수집도 무산시킴으로써 정보 수집 능력을 저하시켰다. 뿐만 아니라, 정확한 정보를 이용하여 적의 미사일 공격에 대항한 것도 방공 효과를 극대화한 것으로 평가되고 있다. 걸프전은 정보시대 전쟁의 특징인 정보의 획득과 처리에서 앞선 다국적군이 승리함으로써 대량 살상 파괴 무기에 대한 정보와 정보기술의 우월성을 입증한 전쟁이었다.

* 종신회원

걸프전에서 정보기술을 작전에 이용하여 승리를 거뒀던 미군은 걸프전에서의 전쟁 양상을 연구한 결과, 정보기술과 정보화 사회의 특성상 미래의 정보전은 과거의 전쟁과 달리 군사 분야뿐만 아니라 민간 분야까지 공격과 방어의 대상이 됨을 인식하기에 이르렀다. 그리고 '93년부터 시작된 다양한 노력과 연구끝에 미국은 올해 1월 CIAO(Critical Infrastructure Assurance Office)를 통해 국가 주요 기반구조 보호(Critical Infrastructure Protection: CIP)를 위한 국가 차원의 계획을 발표하였다[3-6]. 또한, 미국방 정보기반구조를 보호하기 위하여 DARPA(Defense Advanced Research Project Agency)를 통해 정보 보증 및 생존(Information Assurance & Survivability: IA&S) 프로젝트[7-16,5,6,24]를 진행중에 있다. 또한, 미국뿐 아니라 영국, 프랑스, 러시아, 중국 등 많은 국가에서도 미래 정보전에 대비하기 위하여 국가적 차원에서 다각도의 노력을 기울이고 있다[18,19,23].

'00년 8월말 현재 인터넷 사용자가 16,400,000명[1]에 이르는 이제, 정보전은 더 이상 선진국만의 이야기가 아니라 우리 개인과 기업 그리고 국가 안보 차원의 고민거리가 되어 버렸다. 본 고에서는 정보전에 대응하기 위한 각국의 동향과 미국의 국가 계획, 그리고 DARPA를 중심으로 연구되고 있는 IA&S 프로젝트에 대하여 간략히 소개함으로써 정보전과 사이버테러 대응에 관련된 인식을 제고하고 정보전 대응 기술을 개발하기 위한 우리의 노력과 방향을 정립하는데 미력하나마 도움이 되고자 한다.

본 고의 구성은 다음과 같다. 먼저, 2장에서는 정보전의 개념에 대하여 소개하고, 정보전 위협을 고찰하고, 3장에서는 미래 정보전에 대비하기 위한 미국의 국가 계획을 간략히 요약한다. 4장에서는 DARPA에서 정보전 대응 기술 개발을 위하여 추진되고 있는 IA&S 프로젝트에 대하여 소개한 뒤, 5장에서 결론을 맺도록 한다.

2. 정보전 개념

2.1 정보전의 정의와 분류

토마스 로나(Thomas Rona), 슈와르토(Winn Schwartau), 미공군 대령 스자프란스키(Richard Szafranski), 미공군 장관 위드낼과 합동참모인 미공군 대장 포글먼(Sheila E. Widnall and Ronald R. Fogleman), 그리고 미합참(The Joint Chiefs of Staff) 등은 여러 가지 형태로 정보전을 정의하였다[2]. 그 중 미군이 정보전에 대해서 여러 번에 정의한 것 중에서 가장 최신의 것으로 미 각군은 이 정의를 그대로 사용하거나 조금씩 변형하여 자군의 정보전의 정의로 사용하고 있는 것은 미합참의 정의이다.

미합참은 정보전이란 "정보 우위[2]를 확보하기 위하여 적의 정보, 정보에 기반을 둔 처리, 정보체계 그리고 컴퓨터에 기반을 둔 망에 영향을 미치고, 아 측의 정보, 정보에 기반을 둔 처리, 정보체계[3] 그리고 컴퓨터에 기반을 둔 망들을 보호하고 행위"라고 정의하고 있다[2].

정보전의 분류 역시 다양하지만, 현재 가장 많이 참조되고 있는 것은 미국방 대학교의 마틴 리비키(Martin C. Libicki)의 분류이다[17]. 리비키는 정보와 정보기술이 적용될 수 있는 모든 종류의 전쟁 수행 방법을 식별하고, 그림 1과 같이 각각의 특성에 따라 민간 관련 부분과 군사 부분으로 분류하고 있다.

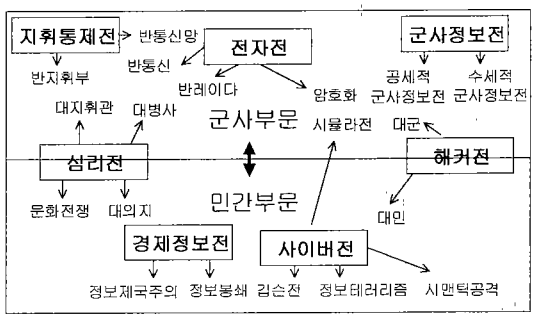


그림 1 리비키의 정보전 분류

2.2 정보전의 특성

그 파급효과가 핵전쟁에 버금가는 것으로 믿어지고 있는 정보전에서는 눈에 보이지 않는 정보

1) 인터넷정보센터 통계

2) 여기서 정보 우위란 "정보의 계속적인 흐름을 수집, 처리, 전파하고, 적이 그렇게 하는 것을 이용하거나 거부하는 능력"을 말한다.

3) 여기서 정보체계란 "정보를 수집, 처리, 저장, 전송, 표시, 유포하고 정보에 작용하는 전체 기반구조, 조직, 인력과 구성요소"를 말한다.

가 공격과 방어의 대상이 되기 때문에 다음과 같은 여러 새로운 특징들이 나타난다[2]. 첫째, 정보전을 준비하고 수행하는데 드는 비용이 저렴하다. 그 이유는, 정보 기술에 대한 전문지식만으로도 정보전 기술과 무기를 개발할 수 있고, 공격 대상 정보 시스템에 연결된 네트워크에 접근할 수만 있으면 정보전 무기를 사용하여 공격할 수 있기 때문이다. 게다가, 인터넷을 통하여 정보전 무기를 제작하는데 필요한 전문지식과 도구를 누구나 손쉽게 습득할 수도 있다.

둘째, 사이버 공간에서는 전통적인 경계가 불분명해진다. 사이버 공간에서는 과거에는 명확하였던 공공과 개인의 이익, 전쟁과 범죄 행위 등을 구분하기가 어려워지고, 국가 사이의 지역적, 정치적 경계가 모호해지기 때문이다. 따라서 정보전 공격 행위가 국내에서 시작된 것인지 외국에서 시작된 것인지 구별하기가 점점 어려워지며, 누가 공격을 수행하고 있는지, 누가 공격을 당하고 있는지, 누가 공격을 준비하고 있는지 구별하기 어려워진다.

셋째, 사이버 공간에서는 사실을 인지하는 지각 능력을 쉽게 조작할 수 있다. 정보기술을 이용하면 영상조작 능력을 크게 증가시킬 수 있으므로 기만이 용이하게 된다.

넷째, 기존 전쟁에서 사용되던 전통적인 첩보 수집 및 분석 방법은 사이버 공간에서는 효과가 없기 때문에 새로운 전략 첩보의 수집 및 분석 방법이 요구된다.

다섯째, 사이버 공간에서는 스파이 활동이나 사고 등을 정보전 공격과 구분할 수 있는 적절한 전술 경고 시스템 및 공격 평가 방법이 명확하지 않다. 정보전에서는 정보전 공격을 사고, 실수, 고장, 범죄 등 다른 사건과 구별하는 것이 매우 어렵기 때문이다.

마지막으로, 전선이 없다. 정보기술은 시간적, 공간적 차이를 무의미하게 하므로 기존 전쟁과 달리 전장과 후방의 구분이 무의미해지고 네트워크를 통해서 접근할 수 있는 곳은 어디든지 잠재적인 전장이 될 수 있다.

3. 미국의 정보전 대응 국가 계획

이 계획서는 클린턴 대통령의 지시에 따라 작성된 것으로서 미국의 주요 기반구조 방어를 위한 국가적 역량을 2003년까지 확보하기 위한 방안이 제시되어 있으며, CIP를 달성하기 위한 목표를 세 가지로 제시하고 있고 각 목표를 구현하기 위한 열 개의 프로그램을 기술하고 있다.

3.1 CIP의 목표

CIP의 첫번째 목표는 준비 및 예방(Prepare and Prevent)으로서 미국의 주요 정보 네트워크에 대한 명백한 공격 가능성을 최소화하고, 공격을 당하더라도 지속적으로 운영될 수 있는(remains effective) 기반구조를 건설하는 것이다. 이 목표를 달성하기 위하여 계획서에는 보호 대상과 상호의존성 파악 및 취약성 평가 프로그램이 제시되어 있다.

두번째 목표는 탐지 및 대응(Detect and Respond)으로서 미국의 주요 기반구조에 대한 공격을 즉각적으로 식별하고 평가하는데 필요한 수단을 개발하고, 피해 복구와 피해 시스템을 재구축하는 것이다. 이 목표를 달성하기 위하여 제시된 프로그램은 공격/침입 탐지, 첩보/법적 대응 능력 확보, 경보 및 정보 공유, 그리고 대응, 재구성 및 복구 능력 확보이다.

세번째 목표는 강력한 기반을 구축(Build String Foundations)으로서 미국의 주요 정보 네트워크에 대한 공격에 대비하기 위한 준비 및 예방과, 탐지 및 대응을 수행하는데 기반이 되는 국가적 차원의 활동을 수행하는 것이다. 계획서는 세 번째 목표를 달성하기 위한 프로그램으로, 연구개발, 전문가 확보, 홍보, 법률적 지원, 그리고 개인의 권리와 사생활 보호를 제시하고 있다.

3.2 프로그램 1: 보호 대상과 상호의존성 파악 및 취약성 평가

첫번째 프로그램은 공격받을 가능성이 있는 정부 및 민간 영역의 주요 정보 네트워크 자산, 이들 간의 상호의존성 및 취약성을 식별하고, 실질적으로 취약성을 제거할 수 있는 프로그램을 개발하는 것으로서, 정보기술의 급격한 발전을 염두에 두고 3-5년 주기로 다음과 같은 과정을 반복한다.

① 국가적 차원에서 볼 때, 명백한 보안이 필요한 연방 기관 및 행정부처의 가장 중요한 정보

자산을 식별한다.

② 이들이 정부 내부에서, 정부기관간에, 또는 정부기관과 민간 영역간에 상호의존성을 갖는지 분석한다.

③ 시스템 관리자, 운영자, 보안 전문가, 그리고 CIO를 통해서 식별된 보호 대상 자산의 취약성을 평가한다.

④ 그 결과를 외부 전문가들이 평가한다.

이를 위하여, '99년 2월, 5월, 그리고 6월에 각각 하나, 두 개 및 여러 연방 행정부처가 자신의 취약성을 평가하고 개선 계획을 작성하였으며, 외부 전문가 그룹 ERT(Expert Review Team)에서 그 결과를 검토하였다. '99년 11월에는 각 부처/기관간에 연방 정보 시스템 보안에 관련된 활동을 식별하고, 조정하여 강화하기 위한 위원회가 출범하여 표준화에 관련된 사항은 NIST (National Institute of Standard and Technology)에 전달하였다. 그리고, 올해 1월에는 연방 정부가 주요 정보 자산을 보호하기 위한 파일럿 프레임워크를 개발하고 데이타베이스를 구축하였다.

3.3 프로그램 2: 공격 및 침입 탐지

두번째 프로그램은 고기능 방화벽(advanced firewalls), 침입탐지 모니터(intrusion detection monitors), 비정상적 행위 식별기(anomalous behavior identifier), 기관차원의 관리 시스템(enterprise-wide management systems), 그리고 악성 코드 스캐너(malicious code scanners) 등의 도구를 활용하여 주요 컴퓨터 시스템을 다중계층(multi-layered)으로 보호하는 것으로서, 각 연방 부서와 기관들에 산재해 있는 침입탐지 모니터들을 중앙 집중 능력이 있는 것과 연결하여 시스템의 비정상적 행위를 분석함으로써 시스템의 보안을 향상시키는 것을 목적으로 하고 있다.

이를 위하여 다음과 같이 세 개의 침입탐지 네트워크를 구성한다.

○ 주요 국방 네트워크를 모니터하고, 침입 또는 공격을 당한 이후에 원래 기능을 복원하기 위한 JTF-CND(DoD Joint Task Force-Computer Network Defense)

○ 정부 및 민간 기관의 침입을 탐지하기 위한 네트워크로서 JTF-CND를 모형으로 하는 FIDNet(Federal Intrusion Detection Network)

○ JTF-CND, FIDNet 및 NIPC(National Infrastructure Protection Center)에 전문가를 지원하여 국가 안보를 위협하는 비인가된 침입과 공격을 격리, 억제 및 해결하며, 이들 기관과 함께 사고 조사와 취약성 평가를 수행하기 위한 NSIRC(National Security Incident Response Center)

미군에서는 '98년에 국방성과 육·해·공·군의 침입탐지 시스템을 연결하였고, '98년 12월에 주요 국방성 시스템에 500개의 침입탐지 모니터를 설치하였다. '99년 봄에는 국방 사이트의 네트워크 감시를 위하여 JTF-CND를 구축하였고, NSIRC는 '98년에 설립되었다. FIDNet 구축을 위해서는 2001년에 1000만 달러를 투자하여 중앙 집중형 침입 탐지 및 대응 시스템을 GSA (General Service Administration)에 갖추게 한다.

FIDNet을 구축하기 위하여, 먼저 각 기관에는 ① 인가된 사용자의 접근 및 행동 규칙과, 인가된 사용자의 비정상적 행동을 식별할 수 있는 스캐닝 프로그램을 보유하고, ② 네트워크에 연결되어 있는 시스템을 식별하여 그 시스템이 어떠한 일을 하고 있는지 판단할 수 있으며, 접근 및 행동 규칙을 파악할 수 있고, 보안 등급을 조절할 수 있는 능력을 갖춘 관리 프로그램을 보유하며, ③ 운영체제 코드와 여러 소프트웨어에 악성 코드(예: 논리 폭탄, 크랩 도어 등)가 삽입되어 있는지 분석할 수 있는 능력을 보유하고 있는 침입탐지 모니터를 설치한다. 그 다음, 기관 차원의 침입탐지 모니터들을 GSA의 연방 컴퓨터사고 대응부서(Federal Computer Incident Response Capability: FedCIRC)에 연결하여 여러 기관으로부터 전달되는 비정상적 행위를 실시간으로 분석한다. 단, 각 기관 또는 FedCIRC에서 판단하기에 범죄에 해당하는 침입 또는 국가 안보에 직결되는 위협은 NIPC를 포함한 해당 사법기관에 통보된다.

3.4 프로그램 3: 첩보/법적 대응 능력 확보

세번째 프로그램은 컴퓨터 네트워크를 기반으로 하는 새로운 종류의 위협과 범죄에 대응하기 위한 법 집행과 첩보 조직을 지원 및 강화하기

위한 것이다. FBI에서 주관하는 NIPC는 국방, 첩보, NSA 및 기타 연방 기관의 대표로 구성되며, 법 집행과, 외국에 대한 대첩보(counter-intelligence) 임무, 그리고 이들 두 영역에 해당하는 활동을 수행하는데 필요한 권한을 부여받는다. NIPC는 공개된 자료, 민간 기관, 법 집행 기관, 미국의 첩보 기관 등의 모든 정보를 이용하여 사이버 공격에 대한 조기 경보를 발령하며, 공격자를 찾아내는데 필요한 정보를 수집한다. 또한, 공격의 발발 시점을 판단하고, 공격의 범위와 근원지를 분석하며, 가해자를 파악하는데 소요되는 능력을 개발 및 향상시킨다.

3.5 프로그램 4: 경보 및 정보 공유

네번째 프로그램은 공격 경보와 정보를 실시간으로 공유할 수 있는 효율적인 국가 차원의 시스템을 구축하는 것이다. 이를 위하여 먼저, 연방 차원의 정보 공유를 개선시킨다. 연방의 각 기관에 설치되어 있는 시스템에서 발견한 비정상적 행위와 침입에 대한 데이타는 FedCIRC에 보내도록 한다. 그리고 불법적 행위와 침입의 징후는 곧바로 NIPC에 보내져 분석되도록 한다. NIPC와 FedCIRC는 모든 정보에 접근할 수 있기 때문에 이러한 보고와 다른 정보 근원으로부터 수집되는 정보를 결합하여 침입 패턴을 알아낼 수 있다. 국방성에서는 NMCC(National Military Command Center)와 JTF-CND가 국방 분야의 침입 관련 징후를 취합·정리하여 NIPC에 전달하고, 국방 경보를 발령한다. 그리고, NIPC의 국가 경보를 전달받아 예하 부대에 발령한다.

두번째로, 민간 영역과 주/지방 정부를 위하여 ISAC(Information Sharing and Analysis Center)을 설립하여 민간 기업, 주/지방 정부가 정보를 공유하고 국가로부터 경보와 정보를 전달받을 수 있도록 한다. '99년 10월 1일 미 재무성 장관은 은행 및 금융 서비스 정보 보안 기관인 FS/ISAC(Financial Services Information Sharing and Analysis Center)의 설립을 발표하였고, 전력, 급수, 운송, 의료 등의 분야에서도 동일 역할을 수행하는 센터를 올해 안에 설립할 예정이다.

세번째로 FIDNet과 JTF-CND의 사고 탐지 시스템들간에 서로 사고 데이타를 주고받을 수 있도록 하며, 사고를 보다 자세히 분석하고 취약성을 평가하기 위해 FedCIRC와 JTF-CND는 NSIRC에 사고 관련 자료를 전달하도록 한다.

3.6 프로그램 5: 대응, 재구성 및 복구 능력 확보

다섯번째 프로그램은 주요 기반구조가 공격을 당하는 동안 그 공격을 제한하고 공격에 대항할 수 있는 지속 및 복구 계획(continuity and recovery plan)을 작성하는 것이다. 공격이 발발하면, JTF-CND, FIDNet, ISAC, NIPC는 연방 기관 및 민간 기관과 함께 진행되고 있는 공격 범위를 파악한다. 만약, 공격이 광범위하게 진행된 것으로 파악되면 NIPC는 법 집행 기관 및 여타 기관과 함께 다음과 같은 절차에 따라 대응을 시작한다. ① 의심스러운 사용자가 네트워크에 접근하는 것을 방지하고, ② "방어 상태"에 돌입하여 예방 조치를 취하고, ③ 공격 기술을 제압할 수 있는 보안 소프트웨어 패치를 적용하고, ④ 네트워크 구성 요소를 격리시키며, ⑤ 네트워크의 운영을 일시적으로 중지시키고, ⑥ 비상 지속 시스템을 가동시킨다.

3.7 프로그램 6: 연구개발

여섯번째 프로그램은 국가 계획을 구현하는데 필요한 연구 요구사항을 추출하고, 이들간의 우선순위를 설정하고, 연구비를 지원하기 위한 것이다. OSTP(Office of Science and Technology Policy)에서는 '98년도에는 이 프로세스에 따라 CIP에 관련된 연구개발 예산으로 2000년도에 5억 달러, 2001년도 6억6백만 달러를 집행하도록 확정하였고, 연구개발 주제를 식별하였으며, 연도별 연구비 지원 전략을 수립하였다. CICG(Critical Infrastructure Coordination Group)에서 식별한 주요 연구개발 주제는 다음과 같다.

○ 대규모 네트워크에 대한 침입 탐지 모니터 기술

○ 운영체제 코드에 설치되어 있는 악성 코드(트랩도어)를 식별하기 위한 인공지능 기법 및 기타 기법

○ 공격이나 재난 발생시 침입자를 발견, 정지 및 제거하며, 피해를 약화시키고 정보 처리 서비

스를 복구하기 위한 방법론

○ 네트워크의 신뢰성, 시스템의 생존성, 그리고 주요 기반구조 구성요소와 시스템의 견고성(robustness), 주요 기반구조 자체의 견고성을 향상시키기 위한 기술

○ 공격에 대한 기반구조 대응을 모델화하기 위한 기술, 기반구조간의 상호 의존성을 식별하기 위한 기술, 취약한 핵심 노드, 구성요소 또는 시스템을 발견하기 위한 기술

이 프로그램에 의거하여, 2001년에는 NII(National Information Infrastructure)를 견고히 하고, 신뢰성 있게 동작하기 위해서는 필요하지만, 민간과 정부 누구의 영역도 아닌 분야를 찾아 연구개발하는 기관인 정보 기반구조 보호 연구소(Institute for Information Infrastructure Protection: I3P)를 설립할 예정이다.

3.8 프로그램 7: 전문가 확보

일곱번째 프로그램은 연방 정부와 국가적 차원에서 필요로 하는 정보 보안 전문가들의 수와 이들이 갖추어야 할 기술들을 파악하고, 현재의 연방 정보 기술자들을 훈련시키고, 부족 인력에 대해서는 초빙하거나 교육을 통해 충원하여 CIP 전문가를 확보하는 것이다. 이를 위하여, 2001년까지 2,500만 달러를 배정하며, FCS(Federal Cyber Services)에서는 다음과 같은 다섯 가지 교육훈련 프로그램을 통하여 연방 정보기술 보안 전문가 부족 문제를 해결한다.

○ OPM(Office of Personnel Management)에서는 연방 정보 기술 보안 보직자가 갖추어야 할 핵심 능력을 식별 및 개발하고, 이들이 받아야 할 훈련 및 인증(certification) 요건을 식별한다.

○ 정보기술 훈련 지원 센터로 CITE(Center for Information Technology Excellence)를 설립하여, 현존하는 연방 정보 기술자들을 교육함으로써 기술자들이 그 기술을 지속적으로 보유할 수 있도록 한다.

○ 차세대 연방 정보 기술자들과 보안 관리자들을 모집하고 교육하기 위한 장학금제도(Scholarship for Services: SFS)를 개설한다. 이 프로그램에 의해 연간 300명이 학부 또는 대학원에 등록할 수 있도록 하고, 학생들은 졸업후 일정기간 연방 정보기술 분야에 종사하도록 한다. 이를 위하여 대학이 이 프로그램에 참여하도록 유도하며, 정보 보안 과목과 연구실을 운영하도록 지원한다.

○ 고등학교를 대상으로 하는 인력 보충 및 훈련 과정을 개설한다. 이 프로그램에 의하여 고등학생들은 여름 과정이나 인턴 프로그램에 참여할 수 있도록 하여 이들이 연방 정보 기술 분야에서 추후 종사할 수 있는 기회를 부여한다.

○ 연방 정보보안(INFOSEC) 교육과정을 개발하여 운영함으로써 연방 전체가 컴퓨터 보안 인식을 가질 수 있도록 한다.

3.9 프로그램 8: 홍보

여덟번째 프로그램은 재난이 발생하기 전에 고의적인 사이버 공격에 대한 방어 능력을 향상시키기 위해서는 현재부터 준비하고 활동하여야 한다는 점을 홍보하기 위한 것이다. 이를 위하여, 다음과 같은 사항을 추진한다.

○ 미국의 어린이들에게 사이버 윤리와 사이버 공간에서의 적절한 행동을 교육하고, 인터넷과 다른 통신 도구를 사용하는 방법을 가르치기 위한 사이버 시민(CyberCitizen) 프로그램을 운영한다.

○ 미국 기업과 정보 기술자들간의 연계를 강화하기 위한 주요 기반구조 보호 연계(Partnership for Critical Infrastructure Security)을 운영하여, 민간과 정부가 함께 국가의 사이버 보안을 향상시키기 위한 행동을 취할 수 있도록 한다.

○ 연방 정부의 고용자들 자신이 정보 시스템 보안의 필요성을 인식할 수 있게 한다.

○ CIP에 대한 사항을 다른 민간 조직과 공공기관에도 알리기 위한 노력을 기울인다.

3.10 프로그램 9: 프로그램 1-8을 수행하기 위한 법률적 지원

아홉번째 프로그램은 앞에서 제시된 프로그램에서 제시된 사항들을 지원하기 위한 법률적 기반을 구축하는 것으로서 의회를 포함한 연방 정부와 민간 업계가 긴밀히 협력하도록 한다.

3.11 프로그램 10: 개인의 권리와 사생활 보호

CIP의 목적은 미국의 이익과 민간의 자유를

유지하고 강화시키는 것이므로, 마지막 열 번째 프로그램은 앞에서 제시된 프로그램을 수행함에 있어서 사생활 보호를 위한 메카니즘을 구축한다. 이를 위하여, 2000년부터 매년 사이버 보안, 민간의 자유 그리고 시민의 권리에 대한 세미나(colloquium)를 개최한다. 또한, 클린턴 대통령의 '99년 7월 14일 행정 명령(Executive Order) 13130에 의하여 설립된 국가 기반구조 보장회의(National Infrastructure Assurance Council: NIAC)가 공공-민간간의 동반관계를 포함하여 주요 기반구조 보장이 민간의 자유, 사생활 권리, 그리고 개인적 자료 등에 어떠한 영향을 미치는지 조사하여 대통령에게 자문과 조언을 제시하도록 한다.

4. 미국방성의 정보전 대응 기술 개발 프로젝트

IA&S는 정보전에 대한 미국방성의 기존 인식이 변화하면서 대두된 개념으로[20], 정보전 개념은 정보보안(INFOSEC)에서 CIP로, 그리고 CIP에서 IA&S로 변화하고 있음을 의미한다[21]. DARPA를 중심으로 전략적 사이버 방어(Strategic Cyber Defense)를 위해 개발되고 있는 IA&S 기술은 그림 2와 같이 여섯 가지 영역에 걸쳐, 여덟 가지 연구개발 프로그램으로 구성된다[10,12].

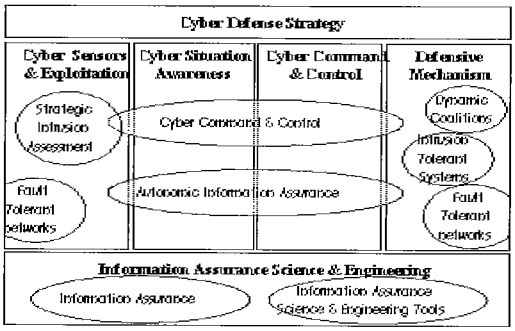


그림 2 Strategic Cyber Defense Map

4.1 전략적 침입 평가(Strategic Intrusion Assessment) 기술

최근의 사이버 공격은 오랜 시간동안 대규모로 시도될 뿐 아니라 LAN과 WAN을 넘나들며 발생하고 있어서 하나의 침입탐지 시스템만으로는 사이버 공격을 탐지하기가 어렵다. 이러한 환경에서 침입을 탐지하고 평가하기 위해서는 침입탐지 시스템이 서로 침입에 대한 정보를 교환할 수 있어야 한다. 또한, 대응 시스템과 네트워크 관리 시스템과도 통합되어서 시스템 운영자와 의사결정자들이 대응과 복구 방법을 찾을 수 있도록 해야 한다.

이와 같이 다양한 침입탐지 시스템들과 대응 시스템들을 함께 동작시키고 서로 정보를 공유할 수 있게 하기 위해서 공통 침입 탐지 프레임워크(Common Intrusion Detection Framework)를 개발한다. 이 프레임워크는 침입 및 피해에 관련된 정보를 수집하기 위한 센서, 보고된 침입 정보의 타당성(validity)과 대응의 필요성을 판단하기 위한 분석 엔진, 그리고 침입에 대응하기 위한 대응 엔진으로 구성된다.

현재, 센서 개발에는 에이전트 기술을 적용하고 있고[22], 알고리즘 측면에서는 통계적 상관관계 및 정성적 추론 기법을 사용하여, 수집된 정보를 여과하여 상위 계층에 보고하도록 개발하고 있다. 또한, 분석을 위해 자동 패턴 감지, 이벤트 분류, 모델기반 추론 등의 기법을 사용하여 공격자의 의도를 추측하고 미래의 행동을 예측하고 있으며, 피해 평가를 위해 이벤트의 상관관계를 피해 평가에 적용하고 그 확실성을 판단하기 위해 증거에 의한(evidential) 추론도 수행한다.

4.2 침입 감내 시스템(Intrusion Tolerant Systems)

침입 감내 시스템은 mission-critical한 시스템들로서 사이버 공격에 직면하여도 자신의 기능을 정확하게 지속적으로 수행하고 시기적절하게 사용자에게 서비스를 제공하는 정보 시스템이다. 이 프로그램은 침입에 탄력적이고 내성이 있는 시스템을 구축하기 위한 구조, 방법론, 그리고 기술을 구상, 설계, 개발, 시연 및 확인하는 것이 목적이다. ITS 개발 프로그램은 침입과 결함이 발생한 상황에서도 데이타와 프로그램의 일관성을 유지하기 위한 기술과 서비스 거부 공격에 대응하는 기술과 높은 시스템 가용성을 유지하는 기술을 위주로 개발한다.

일관성 유지를 위하여 의심스러운 코드와 데이

타에 대해서는 손상되지 않은 코드 및 데이타와, 변조된 코드 및 데이타를 실행 또는 사용하기 이전에 재빨리 구분하기 위한 메카니즘을 개발한다. 이 메카니즘은 확장 가능하고, 효과적이며, 개발 언어와 대상 시스템에 의존적이지 않다. 또한, 악성 코드가 피해를 입히기 전에 이를 제지하기 위한 모니터도 개발한다. 이 모니터는 최소한의 변경 또는 전혀 변경이 없이도 COTS 소프트웨어와 함께 동작할 수 있고, 성능 저하가 최소화되며, 다양한 보안 정책을 수용한다.

시스템 가용성을 유지하기 위해서는 피해가 확산되지 않도록 하는 기술, 하드웨어와 소프트웨어 자원을 재구성(reconfiguration)하는 기술을 개발하며, 시스템 기능의 선별과 자원 재할당(reallocation) 기술도 개발한다.

4.3 고장 감내 네트워크(Fault Tolerant Networks) 기술 개발

이 프로그램은 사이버 테러를 당하고 있는 중에도 네트워크가 계속 정상적으로 동작하도록 하는 기술을 개발하는 프로그램이다. 이 프로그램에서 개발되는 기술은 공격이 지속되는 동안 네트워크에 대한 피해를 감소시키고, 네트워크가 용인할 수 있는 최소 수준의 기능을 유지하도록 하는 것이다. 즉, 사이버 공격에 대한 고장 감내 능력을 네트워크 수준에서 가지도록 네트워크를 강화하기 위한 기술, 일관성과 가용성을 보장하도록 하는 기술, 서비스 거부 공격에 대한 잠재적 취약성을 감소시키는 기술, 그리고 액티브 네트워크 기술을 이용한 공격 대응 메카니즘을 개발한다.

이 프로그램에서는 고장 감내 생존성(Fault Tolerant Survivability), 서비스 거부 방지(Denying Denial-of-Service), 그리고 액티브 네트워크 대응(Active Network Response) 기술을 개발한다. 먼저, 고장 감내 생존성 기술 개발에서는 고장 감내 시스템의 메카니즘을 이용하여 네트워크가 결함을 견디도록 하는 기술을 개발하는 것으로서 가상 자원의 중복 및 복제를 위하여 네트워크를 중첩시키고 관리하는 기술, 생존성있는 서비스를 제공하기 위한 네트워크 분할 기술, 네트워크가 공격에 보다 잘 견디도록 네트워크 구조를 강화하는 기술, 네트워크 성능 저하를 감소시키는 기술, 분산 네트워크의 자가 안정화(self-stabilization) 알고리즘, 고장 감내 네트워크의 확장성 이슈, 그리고 네트워크의 파괴 모델 등을 개발한다.

서비스 거부 방지 기술 개발에서는 공격자의 자원 소비를 제한함으로써 서비스 거부 공격을 방지하는 기술을 개발하는 것으로서 시장기반(market-based) 네트워크 할당 전략과 경과기반(progress-based) 프로토콜 기술로 구성된다. 전자는 중요하지 않은(non-critical) 작업 처리에 의한 자원 소모를 제한하는 기술을 개발하는 것이고, 후자는 서비스 거부 공격의 가능성을 최소화하는 통신 프로토콜을 개발하는 것이다. 이 프로토콜은 강력한 인증 기능을 가지고 있으며, 신뢰 정도에 따라 소모할 수 있는 자원을 할당하는 기능도 가지고 있다.

마지막으로, 액티브 네트워크 대응 기술 개발에서는 이전에 개발되었던 액티브 네트워크와 침입탐지 메카니즘을 개선하여 공격 또는 고장의 경우에도 네트워크의 생존성을 보장하는 기술을 개발한다. 이 기술에는 네트워크에 자료가 범람하더라도 네트워크 구성요소를 "push back"할 수 있는 기능을 반드시 포함시킨다. 또한, 공격의 추적, 근원지 발견 및 차단 기술을 개발하여 네트워크 울타리를 제공하며, 자가배치(self-deploying) 침입탐지 및 대응 응용 프로그램을 설계·개발한다.

4.4 동적 연립(Dynamic Coalitions) 기술 개발

동적 연립 기술 개발 프로그램의 목적은 최소한의 운영을 위한 분산된 제휴 보안 정책을 수립하기 위한 기술을 개발하는 것이다. 이를 위해, 다차원 보안 정책 관리, 안전한 그룹 관리, 그리고 연립 기반구조 서비스에 대하여 기술을 개발한다.

먼저, 다차원 보안 정책 관리 기술 개발은 정책 표현 및 번역 기술, 정책 협상 및 합의 기술, 정책 분배 및 집행 기술, 그리고 정책 발견 기술 등을 개발하는 것이다. 특히, 정책 표현 및 번역에 관련된 세부 기술로는 사람이 읽기 쉬운 형태로 표현된 정책을 컴퓨터가 해독할 수 있는 형태로 변경하는 기술, 보안 정책을 광범위하게 표현할 수 있는 표현 언어 기술, 호스트와 네트워크

보안 정책을 정의하는데 있어서 사용자를 도와줄 수 있는 도구모음 등을 개발한다.

안전한 그룹 관리 기술 개발을 위해, 멤버가 그룹에 합류 또는 탈퇴할 때에도 관리 행위가 수행될 수 있게 하는 기술, 새로 합류한 멤버는 대화 이력에 접근하지 못하게 하는 기술, 재합류하는 멤버에게는 탈퇴 이전의 키를 부여하기 위한 기술, 다른 기관의 사용자들이 동적으로 그룹을 구성하는 경우 사용자와 조직의 보안 정책에 적합한 보안 제어를 수행하는 기술, 연립 환경에서의 익명성 보장 기술, 연립 내에서의 부인 방지 기술, 그리고 연립 내에서의 감사(auditing) 기술 등을 개발한다.

연립 기반구조 서비스 기술은 인증서와 인증기관에 관한 것으로서, 인증서의 온라인 확인, CRL의 "push", 그리고 장기적으로는 오프라인 기술 등을 개발하고, 미래의 다중 인증서 기반구조(예: X.509, DNSSEC, PGP, SPKI 등)에 대비한 다른 인증서 관리 기반구조간의 상호 인증, 도메인 보안 정책, 주소 매핑 정책, 그리고 인증서 포맷 등에 관하여 연구한다.

4.5 정보 보증(Information Assurance) 기술 개발

DARPA의 기본적인 정보 보증 전략은 위험균형 최적화(Risk-Balanced Optimizing)와 계층적 방어(Layered Defense)이다. 전자는 위험 요소 중 취약성이 심각한 부분부터 점차적으로 보완하여 일정 시간이 경과되면 보호되어야 할 주요 정보에 대하여 전체적으로 향상된 보안성을 갖게 하는 것으로서 DARPA/ISO(Information Systems Office)에서 추진되고, 후자는 침입을 단계적 즉, 예방(prevention), 탐지(detection), 그리고 감내(tolerance)의 단계로 구분하여 방어하는 것으로서 DARPA/ITO(Information Technology Office)에 의하여 추진된다.

DARPA에서 정보 보증을 추진하는 접근 방법은, 우선 표준 API를 이용하여 반투명한(semi-transparent) 보안 서비스를 제공함으로써 공통적인 보안 프레임워크와 서비스를 구축하고, 그 다음으로 기존의 프로그램의 보안 기능을 통합하고 COTS에 제한된 기능을 추가함으로써 통합된 솔루션을 제공하는 것이다.

이 프로그램에서는 시스템 보안 관리(Management System Security), 공격 예방(Prevent Attack), 탐지 및 대응(Detect and Respond), 그리고 IA를 위한 구조와 통합(Architecture and Integration)을 네 분야의 기술을 개발한다. 먼저, 시스템 보안 관리 기술을 개발하기 위해서, 기존의 다양한 보안 관리를 통합된 환경에서 제공하기 위한 SSD(Security Service Desk)를 개발하고, 다양한 보안 요소(예: 방화벽, 감사 기록, CORBASEC 등)들을 이용하는 보안 관리를 추상화시키고, 이들을 정책 시스템과 연계시킬 수 있는 미들웨어 서비스인 SMART(Security Management and Administration of Remote Trusted Systems)를 개발한다.

예방 기술 개발을 위해서, 네트워크 측면에서는 DNS(Domain Name Server)의 보안을 강화하여 이름과 주소 매핑을 인증하게 하고, DVPN(Dynamic Virtual Private Network)을 구축한다. 미들웨어 측면에서는 CORBA(Common Object Request Broker Architecture) 보안을 강화하여 CORBA 보안 서버를 구축하고, 역할 기반의 접근 통제 도구를 개발한다. 운영체제 측면에서는 내장 프로세스 개념을 도입하여 신뢰할 수 없는 응용 프로그램은 보안 매니저 프로세스가 실행시키도록 한다. 응용 프로그램 측면에서는 필터링, 모니터링, 암호화 기능을 갖는 wrapper를 사용하여 악성 코드에 대비한다. 또한, 바운더리 관리를 위하여 Pump, Starlight, ORB 게이트웨이를 적용한다.

탐지 기술 개발을 위해서는, 침입 탐지 및 격리 프로토콜(Intrusion Detection and Isolation Protocol)과 공통 침입 탐지 프레임워크를 개발하며, 공격 신호 감지를 위하여 Net Radar를 이용한다.

4.6 정보 보증 과학 및 공학(Information Assurance Science and Engineering Tools) 개발

다른 프로그램들이 정보 보증 위협에 대응하는 활동에 관련된 것인 반면, 정보 보증 과학 및 공학은 정보 보증 기술 및 체계의 설계와 평가 활

동에 관련된 것으로서, 설계 및 평가를 위한 통합된 환경과 도구를 개발하는 것이 목적이다.

정보 보증 과학 측면에서는 사이버 과학, 정보 보증 메트릭, 그리고 수학과 모델을 개발한다. 먼저, 사이버 과학(syberscience)은 현존하는 정보 보증 연구를 조사분석하여, 누락된 영역을 찾아내고, 이 영역에 현존하는 과학적 기법(예: 위험 분석, 공격 그래프 작성 등)을 적용하여 정보 보증 연구를 보완하기 위한 사항을 연구한다. 정보 보증 메트릭 개발은 정보 보증 설계, 평가, 운영 및 시험에 활용할 메트릭들을 찾고, 이 메트릭들을 적용하기 위한 방법론을 개발한다. 수학 및 모델 개발에서는 정보 보증에서 논리, 추론, 의사결정 등에 사용하는 수학과 모델을 개발한다.

정보 보증 공학에 관련되어서는 정보 보증 설계, 정보 보증 평가, 벤치마크에 사용할 정보 보증 메트릭, 정보 보증 모델, 정보 보증 수학, 사이버 과학 등을 적절히 적용하기 위한 과학적이고 신뢰성있는 방법론을 개발하고, 정보 보증을 설계 및 평가하기 위한 도구를 개발하며(예: 의사결정을 지원하기 위한 위험 평가 결과 비교판단 도구), 정보 보증 설계 및 평가를 위한 통합 환경을 구축하기 위한 기술을 개발한다.

4.7 자율적 정보 보증(Autonomic Information Assurance) 기술 개발

자동화된 사이버 공격은 광범위하게 분산된 환경에서 발생하기 때문에 수동으로는 시기적절하게 대응하기 어렵다. 이러한 공격에 대응하기 위해서는 공격을 중단시키거나 그 피해를 최소화시키기 위한 자동화된 방어가 필요하다. 이 프로그램은 자동화된 공격에 빠르게 그리고 적절하게 대응하기 위한 자동화된 방법을 개발하는 프로그램이다.

이 프로그램에서 개발할 기술은 공격에 대하여 효과적으로 대응하기 위한 방법을 빠른 시간내에 선택하기 위한 기술, 지역 및 분산된 자원과 밀접하게 연계되어 있는 경량의 자동화된 방어 기술, 분산되어 있는 재귀적 방어 능력을 결집시킬 수 있는 통제 및 정합 전략, 그리고 다양한 형태의 통제 이론 및 게임 이론에 대한 연구 등이 있다. 또한, 방어 통제 시스템의 프로토타입을 개발하고, 모델링된 시스템, 위협 등에 시나리오를 적용할 수 있도록 확장된 모델을 제안한다. 또한, 각 시스템 요소(운영체제, 방화벽, 응용, 데이타베이스 등)별로 적용할 수 있는 대응 방법과 기능을 정립하기 위한 연구도 수행한다.

4.8 사이버 지휘 통제(Cyber Command and Control) 기술 개발

현존하는 기술로는 전략적 및 분산된 사이버 공격의 전체 범위를 식별하고 이해하여, 그 상황에 효과적으로 대응할 수 있는 의사결정을 돕지 못한다. 또한 임무에 의한 의도적 공격을 평가하고 대응 방법을 제시할 수도 없다. 현재의 공격 탐지 및 보고 기술은 컴퓨터 네트워크 상태 정보와 자세한 공격 발생 이벤트와 같은 사항을 보고하는 저수준의 능력을 보유하고 있을 뿐, 의사결정자가 필요로 하는 상위 수준의 정보를 제공하지 못하고 있다.

이 프로그램은 상위 수준의 의사결정을 지원하기 위한 기술 개발 프로그램으로서 자동화된 공격에 대응하기 위한 Cyber OODA(Observe, Orient, Decide, Act) 기술을 개발하는 것이다. 즉, 이 프로그램에서는 사람이 공격자의 행동과 목표를 조사하고, 공격자에게 대항하기 위한 가장 효과적인 행동(course of action: COA)을 결정 및 수행하게 도와주는 기술을 개발한다.

이 프로그램에서 개발하는 기술은 상황 인식(situation awareness), 행동 양식 개발 및 수행(COA development and execution), 그리고 의사소통 및 피해 평가(forensics and damage assessment)이다. 먼저, 상황 인식은 모니터 시스템이 붕괴되었는지, 공격 행동이 탐지되고 있는지, 또는 전략적 공격이 발생하고 있는지 등을 평가하기 위한 평가 기능의 상태와 평가 진도 등의 정보를 취합하는 기술을 개발하는 것이다. 또한, 전략적 공격에 대비해서 공격의 목표와 의도가 무엇이고, 공격자가 앞으로 어떠한 행동을 취할 것인지도 결정하기 위한 기술도 개발한다. 뿐만 아니라, 공격이 발생되고 있는 상황을 지휘관이 잘 이해하도록 도와주기 위한 시각화 기술도 함께 개발한다.

행동 양식 개발 및 수행에서는 현재 어떠한 방어 대책이 있고, 그 대책을 적용할 경우 공격을 얼마나 효과적으로 방어할 수 있으며, 대책

적용이 시스템에 어떠한 영향을 미칠 수 있는지 비교판단(trade-off)하는 기술을 개발한다.

의사소통 및 피해 평가 기술은 사이버 공격으로 인하여 시스템의 어떠한 기능과 자료가 파손, 변조 또는 훼손당했는지 분석하고, 시스템의 성능과 임무 수행에 전반적으로 어떠한 영향을 미쳤는지 분석하는 기술을 개발한다. 또한, 전략적 사이버 공격에는 지금까지 알려지지 않은 방법이 사용될 것이기 때문에, 사람이 어떠한 문제가 어느 지역에서 발생하였는지 판단하고, 공격을 중지시키거나 피해 확산을 방지하기 위하여 어떠한 행동을 취하여야 하는지 결정할 수 있도록 사이버 지휘 통제에 의사소통 능력, 조사 도구 그리고 경험적 방법을 제공하기 위한 기술도 개발한다.

5. 결 론

본 고에서는 정보전 대응을 위한 체계 구축과 기술개발에 대한 공감대를 형성하고자 정보전의 개념과 미국의 CIP 국가 계획, 그리고 DARPA의 IA&S 프로젝트에 대하여 간략히 소개하였다. 미국에서는 정보전에 대비하기 위하여 '98년도에는 11억4천4백만 달러, '99년도에는 14억2천9백만 달러를 집행하였고, 2000년도에는 17억3천7백만 달러를, 20001년에는 예산을 15% 증가시켜 20억 달러를 집행할 예정이며, 그 예산의 80% 이상이 국가 안보에 관련된 기관에 지출되고 있다. 또한, 관련된 기능 배분중 26%가 연구개발에, 57%가 국가 안보 프로그램의 운영에, 그리고 17%가 국가 안보에 관련되지 않은 연방 프로그램 운영에 사용되고 있다[4].

현재, 우리나라에서도 정보전에 대응하기 위하여 다양한 노력이 시도되고 있다. 먼저, 정부에서는 금년 3월 총리를 위원장으로 하는 사이버테러 방지 대책 장관회의를 구성하였고, 사이버범죄 방지를 위하여 250억원의 예비비 배정과 사이버테러 방지를 위한 기본법 제정을 지시한 바 있다. 또한, 정보통신부에서는 주요 정보 기반구조 보호를 위하여 가칭 정보통신기반보호법의 연내 제정을 추진하고 있으며, 국가정보원에서도 범정부 차원의 사이버테러 대응 협의체의 구성과 국가정보기반보호규정을 대통령 훈령으로 제정하기 위해 노력하고 있다. 이와 같은 법제도적 측면이외에도 국방부에서도 군 사이버테러 방지를 위한 CERT를 가동하고 있고, 국군기무사는 해킹 등 사이버 테러에 대비할 정예 요원을 양성하기 위해 사이버 학교를 설립할 계획인 것으로 보도되었다. 경찰에서는 사이버범죄수사대를 사이버테러 대응 센터로 확대 개편하였으며, 경찰청 소속의 연구기관을 설립하여 사이버 테러 대응책에 대한 연구를 추진할 계획이다. 검찰에서는 사이버 범죄에 적극 대처하기 위해 컴퓨터수사부를 발족하였고, 컴퓨터 범죄에 효율적으로 대처하기 위하여 컴퓨터 수사 자문위원회를 발족하였다. 연구개발 측면에서는 (구)국방정보체계연구소, 국방과학연구소, 한국전자통신연구원, 한국정보보호센터, 국가보안기술연구소 등에서 사이버테러와 정보전에 대응하기 위한 기술을 연구하고 있다. 학계에서는 해킹방지 인력 양성을 위하여 정보보호 교육연구센터를 설치하고 있고, 동아리 활동을 통해 해킹·해킹대응 및 정보보호 기술을 연구 중에 있다. 업체에서는 침입경로를 추적하는 프로그램, VPN 제품, 침입차단, 침입탐지, 바이러스 백신 등 사이버테러와 정보전 대응에 필요한 제품들을 개발하고 있다.

현재 우리는 선진국 수준의 정보 기반구조도 갖추었고, 그에 걸맞는 콘텐츠도 어느 정도 확보하고 있다. 이제 앞으로 우리에게 남은 과제는 우리가 보유하고 있는 정보 기반구조와 콘텐츠를 어떻게, 그리고 얼마나 잘 보호하느냐 하는 것만 남아 있다. 이제는 미래를 여는 자세로 정보전 대응에 관련된 기술 개발에 박차를 가할 때이며, 지금까지 정보전 대응을 위하여 각계에서 추진되어 온 다양한 노력들을 결집시킬 때이다.

참고문헌

[1] R. E. Haeni, "Information Warfare: An Introduction," The George Washington University, 1997.

[2] 박상서 외, 정보전 대응체계 건설을 위한 종합 발전계획 연구, 국방정보체계연구소, 1998.

[3] CIAO, National Plan for Information Systems Protection, Version 1.0: An Invitation to a Dialogue, 2000. 1.

[4] 박상서, 정보전 대응 관련 미국의 동향, Cryptopia 제 4권 1호, 2000. 3.

[5] 박상서, "사이버테러 대응 기술," 정보보호

심포지움 2000 논문집, pp. 259-294, 2000. 7.
[6] 박상서, 정보전 대응체계 구축 현황, WISC 2000 튜토리얼 자료집, pp. 73-177, 2000. 9.
[7] O. Sami Saydjari, Strategic Cyber Defense, DAPRATech '99, Jun. 1999.
[8] W. M. Mularie, Information Systems Office Overview, DAPRATech '99, Jun. 1999.
[9] Gary M. Koob, Inherent Information Survivability, DAPRATech '99, Jun. 1999.
[10] -, Current ATIA Focused Research Topics, DARPA, 1999.
[11] -, Information Assurance and Survivability: Program Suite Description, DARPA, 1999.
[12] Sami Saydjari, Defense Advanced Research Project Agency(DARPA) Information Assurance Project, DARPA, 1999.
[13] Brian Witten, Automatic Information Assurance, DARPA, 1999.
[14] Sami Saydjari, Information Assurance, DARPA, 1999.
[15] Michael Skroch, Development of a Science-Based Approach for Information Assurance, DARPA, May 1999.
[16] Cathy McCollum, Cyber Command and Control (CC2), DARPA. 1999.
[17] M. Libicki, "What is Information Warfare?", Aug. 1995.
[18] 박상서, "정보전: 새로운 전쟁 패러다임," 공군 창군 50주년 기념 국제 학술 세미나 논문집, 교리 발전 분야, pp. 25-86, 1999.
[19] 박상서, 정보전 개념 및 무기체계, 합동참모본부 지휘통제 심사분석 회의 발표자료, 1999. 9.
[20] -, Department of Defense Directive (DoDD) S-3600.1 Information Operations (IO), Dec. 9, 1996.
[21] 이철원 외, "정보 보증: 컴퓨터 보안 개념의 변화," WISC '99, pp. 141-156, 1999.
[22] J. Brian Sharkey, Total Information Awareness, DAPRATech '99, Jun. 1999.
[23] 박상서 외, "해외 정보전 동향," WISC '99 Proceeding, pp. 319-329, 1999. 9.
[24] 박상서, DARPA의 정보전 대응 프로젝트, Cryptopia 제 4권 3호, 2000. 9.

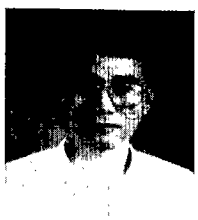
박 상 서

1996 중앙대학교 컴퓨터공학과 공학박사
1996~1998 국방정보체계연구소 선임연구원
1999~2000 국방과학연구소 선임연구원
2000~현재 국가보안기술연구소 선임연구원
관심분야: 병렬 및 다중처리, 운영체제, 디버깅, 성능 평가, 정보보증, 정보전
E-mail:sangseo@dingo.etri.re.kr

이 진 석

2000 한남대학교 컴퓨터공학과 공학박사
1986~1999 한국전자통신연구원 선임연구원
2000~현재 국가보안기술연구소 책임연구원
E-mail:jinslee@etri.re.kr

박 춘 식



1981 광운대학교 전자통신공학과 공학사
1983 한양대학교 전자통신공학과 공학석사
1995 일본동경공업대학교 전기전자공학과 공학박사
1989~1990 일본 동경공업대학 객원연구원
1982~1999 한국전자통신연구원 책임연구원
2000~현재 국가보안기술연구소 책임연구원
E-mail:csp@etri.re.kr