특집

정보전 개념과 주요 동향

박 상 서[1] 박 춘 식[2]

목 차

1. 서 론

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.

미군은 걸프전에서의 전쟁 양상을 연구한 결과, 정보기술과 정보화 사회의 특성상 미래의 전쟁은 국가 주요 인프라가 공격과 방어의 대상이 됨을 인식하게 되었다. 그리고, 미국방 정보 기반구조를 보호하기 위하여 DARPA(Defense Advanced Research Project Agency)를 통해 정보 보증 및 생존(Information Assurance & Survivability: IA&S) 프로젝트[1-13]를 진행하면서 정보전을 담당하는 부서를 설립하여 운영하고 있다.

특히, 9.11테러 이후 미국은 자국의 사이버보안을 강화하기 위하여 정부 부처의 기능을 조정하였으며, 법제의 신설 및 강화, 과감한 예산 투자, 우수한 전문 인력의 확보, 기술적 대응 능력 확보를 위한 연구개발 강화 등 다각적인 노력을 기울이고 있다. 일본과 유럽 등 기술 선진국에서도 미국의 9.11테러를 타산지석으로 삼아 정부차원의 사이버보안 강화 대책 마련에 부심해 왔다.

하지만 보안에 대한 관심과 투자가 부족하였던 우리는 얼마전 1.25 인터넷 대란을 겪으며 그나마 보안의 중요성과 필요성에 대한 인식과 의식을 돌아보는 계기가 되었다. 향후에는 1.25 인터넷 대란이 정부와 국가 운영의 중심이 되는 주요 정보통신 기반시설들을 대상으로 발생하게 될 것이다. 이는 곧 국가 안보 차원에서의 대책 마련이 필요하다는 의미다. 이에, 본 논문에서는 정보전의 개념과 위협을 살펴보고, 주요국의 동향을 소개함으로써 미래 정보전에 대비한 우리의 대응 방향을 논의하는 기회를 마련하고자 한다.

1) 국가보안기술연구소 선임연구원
2) 국가보안기술연구소 책임연구원

본 논문의 구성은 다음과 같다. 먼저, 2장에서는 정보전의 개념을 정의 및 특징의 측면에서 알아보고, 3장에서는 정보전의 위협 양상과 주요 사례를 소개한다. 4장에서는 정보전에 대비한 동향을 미국과 일본을 중심으로 알아본 뒤, 5장에서 결론을 맺도록 한다.

2. 정보전 개념

2.1 정보전 정의

Campen[14]은 정보전은 전장정보(information-in-warfare)에서 지휘통제전(C2 warfare)으로, 다시 지휘통제전에서 정보전(information warfare)으로 진화하고 있다고 설명한다.

미합참은 1996년 발간한 합동비전 2010에서 작전영역을 지상, 해상, 공중, 우주, 정보의 5가지 영역(domain)으로 구분하고 '전 영역에서의 우세확보(full spectrum dominance)'를 위한 전제조건으로 정보우세의 중요성을 강조하였다. 이 정보영역(information domain)에서의 우세확보를 위한 전투를 정보전이라고 볼 수 있다[15]. 그리고, 정보전이란 "정보 우위[3]를 확보하기 위하여 적의 정보, 정보에 기반을 둔 처리, 정보체계 그리고 컴퓨터에 기반을 둔 망에 영향을 미치고, 아 측의 정보, 정보에 기반을 둔 처리, 정보 시스템[4] 그리고 컴퓨터에 기반을 둔 망들을 보호하는 행위"라고 정의하였다[16].

1998년 발간된 합동교범 3-13 합동정보작전에서는 "정보작전은 적의 정보 및 정보체계를 공격하는 한편 아군의 정보 및 정보체계를 방어하기 위하여 취하는 활동이며, 정보전은 위기나 분쟁시에 특정 적을 상대로 하는 정보작전"이라고 정의하였다.

2.2 정보전 특징

그 파급효과가 핵전쟁에 버금가는 것으로 믿어지고 있는 정보전에서는 눈에 보이지 않는 정보가 공격과 방어의 대상이 되기 때문에 다음과 같은 여러 새로운 특징들이 나타난다[15, 17, 18]. 첫째, 핵무기나 화학 무기 등의 개발에 비해 정보전 기술과 무기의 연구 개발이 상대적으로 용이하고, 비용도 저렴하다. 또한, 공격 대상이 되는 정보 시스템에 연결되어 있는 네트워크에 접근할 수만 있으면 어렵지 않게 공격할 수 있다. 따라서 적국이나 반정부 단체 심지어 사회에 적의를 품는 개인도 정보전 공격을 감행할 수 있고 네트워크와 시스템을 마비시킬 수 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. 따라서 전통적인 경계에 따라서 역할이 정해져 있는 국내의 법 집행기관과 국가 안보기관 및 첩보기관 사이의 역할 구분이 모호해지며, 정보 시스템이 공격당하고 있을 때 그것이 범죄 행위에 의한 것인지 전쟁행위에 의한 것인지 구분할 수 없게 된다.

셋째, 사이버 공간에서는 사실을 인지하는 지각 능력을 쉽게 조작할 수 있다. 정보기술을 이용하

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

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

면 영상조작 능력을 크게 증가시킬 수 있으므로 기만이 용이하게 된다. 예를 들어, 정치 · 테러 단체나 반정부 기구는 인터넷과 정보기술을 이용하여 심리전을 수행함으로써 정치적인 지지를 손쉽게 획득할 수 있고, 거짓 정보를 생성하거나 특정 정보만 공개하여 여론을 조작할 수 있다.

넷째, 기존 전쟁에서 사용되던 전통적인 첩보 수집 및 분석 방법은 사이버 공간에서는 효과가 없기 때문에 새로운 전략 첩보의 수집 및 분석 방법이 요구된다. 아직까지 정보전에 대해서는 공격대상과 취약성이 명확히 정립되어 있지 않기 때문에 첩보 수집 대상을 식별하기 어렵고, 위협이 계속하여 빠르게 변화하기 때문에 이들에 대한 첩보를 수집하기가 어려운 것이 현실이다. 미국이 국토안보부를 설립하면서 사이버공간에 대한 정보활동을 강화하려는 움직임을 보이고 있는 것이 바로 이 같은 이유 때문이다.

다섯째, 사이버 공간에서는 스파이 활동이나 사고 등을 정보전 공격과 구분할 수 있는 적절한 전술 경고 시스템 및 공격 평가 방법이 명확하지 않다. 즉, 정보전 공격을 사고, 실수, 고장, 범죄 등 다른 사건과 구별하는 것이 매우 어렵다. 따라서, 현재 정보전 공격이 잘 진행되고 있는지, 누가 공격을 하고 있는지, 공격이 어떻게 수행되고 있는지 등을 파악하기가 매우 어렵다.

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. 특히, 통신, 전력, 에너지, 금융, 운송, 급수, 응급 서비스 등 국가의 모든 기반 시설이 컴퓨터화 되어 상호 연결되어 있어 정보전 무기로 무장한 적에게 쉽게 노출된다. 따라서 전방과 후방의 구분이 무의미해지고 네트워크를 통해 접근할 수 있는 곳은 어디든지 잠재적인 전장이 될 수 있다.

3. 정보전 위협과 사례

3.1 정보전 위협 양상

3.1.1 최근의 정보전 위협 양상

가장 큰 정보전 위협 양상은 익명성을 이용한 위협이다[19, 20]. 사이버공격자는 자신을 속이는 기술(예: IP spoofing)이나 여러 대의 중간 경유지 컴퓨터를 이용한다. 따라서, 마음만 먹으면 전 세계 네트워크에 자신을 은닉할 수 있다. 그리고, 위협자들은 정보전위협이 가져올 피해로 인한 비난과 자신에 대한 추적 · 검거를 피하기 위해 이러한 익명성을 이용하여 자신을 숨긴 채 사이버공격을 감행하고 있다.

두 번째 양상은 정예화, 집단화, 조직화, 소규모화 및 비대칭화다. 사이버공간에서는 개인 또는 작은 집단만으로도 네트워크에 연결되어 있는 컴퓨터를 이용하여 막대한 피해를 일으킬 수 있다[19, 20]. 즉, 사이버시위와 같이 대규모 인력의 참여가 필요한 경우를 제외하고는, 굳이 대규모 인력과 장비를 투입하지 않아도 소기의 목적을 충분히 달성할 수 있다는 의미다. 한편, 정예 공격자들이 그룹을 형성하는 집단화 양상과 함께 조직화 양상도 함께 보이고 있다. 즉, 소규모화, 조직화, 집단화, 정예화 양상을 동시에 보이고 있는 것이다.

세 번째는 대량 피해다. 하나의 컴퓨터만 점령할 수 있다면 네트워크에 연결되어 있는 이웃 컴퓨터를 공격하는 것이 상대적으로 어렵지 않은 실정이다. 이는 곧 대량 피해로 이어질 수 있다는 의미다. 클린턴 대통령의 국가 안보 보좌관이었던 앤소니 레이크(Anthony Lake)는 정보 폭발의 시대에서 세계는 점차 통신망으로 연결되고 있기 때문에 사이버위협은 여러 목표를 동시에 겨냥할 수 있다고 설명하고 있다[21].

3.1.2 미래의 정보전 위협 양상

미래의 정보전 위협은 심리적 불안감을 조성하

거나, 정보를 이용하여 사람의 의지와 행동을 공격자에게 유리하게 변화시키기 위한 심리전의 양상을 띨 것으로 예측된다. 우선, 앤소니 레이크[21]는 사이버위협이 발생할 경우 데이터 훼손의 심각성보다 목표 집단에 대한 장기적인 심리적 효과가 크다고 주장하고 있다. 이러한 사실은 미국이 1994년 뉴욕에 위치한 미공군 로마 연구실에 대한 공격[22], 솔라 선라이즈(Solar Sunrise) 사건[22], 미-중간의 사이버분쟁[23] 등으로 인한 피해를 아직까지 심리적 부담으로 생각하고 있다는 것에서도 미루어 짐작할 수 있다.

두 번째로, 주요 기반시설에 대한 위협은 연쇄적인 대량 피해로 이어질 가능성이 높아 향후의 정보전 위협은 분명히 이들을 대상으로 행해질 것이다. 국가 주요 기반을 구성하는 금융, 통신, 운송, 전력 등에 대한 공격이 성공하면 이들 컴퓨터와 네트워크에 의존하고 있는 여러 시스템들의 오작동이나 제어를 유도할 수 있다. 이는 곧 해당 시스템에 대한 신뢰성의 훼손뿐 아니라, 인명과 재산상의 손해로까지 이어질 수 있다는 의미다. 2001년도 미국 기업에 대한 사이버공격을 조사한 결과 전력과 에너지에 대한 공격은 725건, 금융 분야에 대한 공격은 895건, 하이테크 분야에 대한 공격은 961건 등으로 전반적으로 주요 기반시설 분야가 정보전 위협의 대상이 되고 있다[25].

세 번째로, 국가 주요 기반시설에 대한 사이버공격은 물리적 공격과 함께 이루어질 가능성이 높다. 9.11테러 이후 전세계적으로 물리적 공격에 대비하기 위한 물리적 보안 조치가 강화되었고, 사이버공격은 네트워크의 단절만으로도 어느 정도 피해를 사전에 축소시킬 수 있는 측면이 있기 때문에, 앞으로는 하나의 방법만을 적용하기보다는 이들 두 수단을 함께 활용하는 양상이 나타날 것이다.

네 번째로, 정략적 선전의 수단이 될 것이다. 과거에는 정치적, 종교적, 이념적 선전을 위한 수단으로 활용되던 주요 매체가 구두와 지면이었으나, 이제는 전세계적으로 방송망을 갖춘 TV(특히, 위성을 이용한)와 인터넷이 주요 수단이 되었다. 특히, 영국의 보안 회사 mi2g에서 펴낸 보고서에 따르면[26], 서방에 대한 컴퓨터 공격이 증가하는 원인이 이라크에 대한 전쟁, 테러와의 전쟁, 러시아와 체첸 분쟁, 이스라엘과 팔레스타인 분쟁, 그리고 인도와 파키스탄의 분쟁 등 정치적 이슈때문인 것으로 분석하고 있다. 즉, 미래의 정보전 위협은 핵티비스트(hactivist)에 의한 선전 및 핵티비즘 전파 · 유포를 위한 정략적 수단으로 보다 적극적으로 사용될 것이라는 예측을 가능하게 한다.

다섯 번째로, 국제화 양상도 심화될 것으로 예측된다. 미-중 공군기 충돌에 이은 사이버 분쟁을 볼 때, 분쟁의 당사자인 미국과 중국뿐 아니라 각 국가에 우호적인 국가들의 단체들도 분쟁에 참여하여 국제적 사이버분쟁 양상을 보였다는 것이다[23]. 이는 미래의 사이버위협이 국제화 및 국제연대 양상을 갖게 될 것이라는 관측을 하게 해준다. 또한, 1998년 조지 테넷 CIA 국장은 의회에서 미국을 대상으로 하는 정보전 프로그램을 준비하고 있는 나라로 중국, 러시아, 쿠바, 이라크, 이란 등 미국에 적대적인 국가 이외에도 프랑스, 이스라엘 등을 꼽은 것에서, 적성국과 우방국의 구분이 없어지는 양상을 갖게 될것이라는 예측도 가능하다[27].

마지막으로, 전쟁수단화를 들 수 있다. 현재 미국의 JTF-CNO(Joint Task Force Computer Network Operation)는 공식적으로 사이버방어의 임무와 함께 유사시 공격 임무를 가지고 있다[24]. 또한, 중국에서는 중국중앙군사위원회에서 컴퓨터를 사용하는 것이 원자탄을 사용하는 것보다 효율적이라는 결론을 내린 이후, 컴퓨터 바이러스 부대를 창설하였으며 NET FORCE를 운영하고 있는 것으로 알려져 있다. 또한, 인민해방군의 도상전쟁 및 훈련 시나리오에는 오판을 유도하

는 정보를 입력하거나, 데이터를 변경하거나, 컴퓨터의 작동을 중지시키는 내용이 포함되어 있는 것으로도 알려져 있다. 이와 같이 정보전 위협은 물리적 전력과 연계되어 강력한 마비력을 행사할 수 있는 제 4의 전력으로 인식되고 있으며, 군사 강대국은 실전에 활용할 수 있는 수준의 무기 개발을 이미 완료한 것으로 알려져 있다. 그리고, 이러한 인식은 신흥 IT 강국, 제3세계, 그리고 개발도상국을 중심으로 급속히 확산되고 있는 추세다.

3.2 정보전 사례

3.2.1 미공군 로마 연구실(Air Force Rome Lab) 공격[22]

1994년, 뉴욕에 위치한 미공군 로마 연구실에 대한 공격이 탐지되었다. 이를 추적한 결과, 당시 16세의 영국 소년이 공중전화를 통하여 인터넷에 연결한 뒤 워싱턴, 시애틀, 뉴욕을 거쳐 로마 연구실에 공격을 시도한 것으로 밝혀졌다. 이 소년은 나토사령부, 가다드 우주비행센터(Goddard Space Flight Center), 라이트-패터슨 공군기지(Wright-Patterson Air Force Base) 등도 목표로 하고 있었던 것으로 알려졌다.

3.2.2 솔라 선라이즈(Solar Sunrise)[22]

1998년 2월, 미 국방부는 솔라리스 운영체제의 취약성을 이용한 공격을 받았다. 이 공격은 하버드대학교와 아랍에리레이트연합(United Arab Emirates: UAE)에서 시작되었다. 그 후 UAE와 유타주립대학교에서 공격이 시도되었으며, 나중에는 독일, 프랑스, 이스라엘, UAE, 그리고 대만에서도 시도되었다.

3.2.3 인도 원자력 연구소 침투[28]

1998년 6월, 핵실험에 반대하는 해커 그룹 "miwOrm"이 인도의 바바원자력연구소(BARC)의 컴퓨터 네트워크에 침입, 홈페이지의 일부를 변조하고, 5MB분의 전자메일 파일을 다운로드하였다. 이들은 NASA, 미 해군, 미 공군의 서버를 경유하여 BARC에 침입한 것으로 알려져 있다.

3.2.4 루즈벨트 댐 침투[29]

1998년, 당시 12세 해커가 아리조나의 루즈벨트 댐의 컴퓨터 시스템에 침입하였다. 이 댐은 489조 갤런의 물을 담고 있었는데, 이 정도의 양은 피닉스시 일대를 약 5피트 정도의 높이로 덮으면서 흐를 수 있는 양이다. 조사결과 이 해커는 댐의 수문을 조종하는 SCADA 시스템에 대한 완전한 제어 명령을 알고 있었던 것으로 밝혀졌다.

3.2.5 호주 SCADA 시스템 제어권 상실[29]

2000년 4월, 호주의 퀸즈랜드에서 SCADA (Supervisory Control And Data Acquisition) 시스템에 침투하여 실제로 제어권을 상실했던 사건이 발생하였다. 혐의자는 훔친 컴퓨터를 이용하여 폐기물 처리 회사의 SCADA 시스템에 침투하여 제어권을 확보한 뒤, 약 40여회 이상 폐기물 운반 차량을 제어하여 호수, 공원, 상업지역 등 여러 곳에 폐기물을 쏟도록 하였다. 이 사건은 SCADA 시스템 제어에 성공한 첫 번째 공격 사례로 기록되고 있다.

3.2.6 유고전시 백악관 웹 페이지 공격[30]

1999년 나토의 유고슬라비아 폭격에 흥분한 전자적 침입자들이 백악관 웹페이지를 24시간 동안 정지시켰다. 실제적으로 물리적 피해는 별로 없었지만 수천 명의 미국인들에게 비록 전자적이기는 하지만 백악관의 보안이 다소 미약하다는 인식을 갖게 하는 큰 효과가 있었다.

3.2.7 유고전시 중국 대사관 오폭에 따른 미국에 대한 공격[23, 31]

1999년 5월 7일, 벨그라드에 있는 중국 대사관

에 대한 오폭 사건이 발발하자 즉각적으로 사이버 시위가 시작되었다. 중국 해커들은 미국 에너지부, 내무부, 그리고 백악관 웹사이트 등을 공격하였다. 이 때, 인터넷에 몇 개의 특수 목적용 사이트가 개설되어 시위에 대한 기사를 전문적으로 다루었으며, 어떤 사이트에서는 사이버 시위대를 모집하였다. 몇 개의 사이트에서는 미국 사이트에 대한 대량 컴퓨터 공격을 시도하도록 권유하였고, 미국 금융 사이트를 대상으로 한 컴퓨터 바이러스를 배포하기도 하였다.

3.2.8 미-중 공군기 충돌 사건에 이은 사이버 전쟁[23, 31]

2001년 4월 1일부터 5월 8일 사이에 발생하였다. 중국 해커들은 워싱턴 해군통신기지국(Washington Navy Communications Station)과 해군광역수송국(Navy Service Wide Transportation) 사이트를 시작으로 백악관 웹사이트까지 마비시켰다. 이 분쟁으로 미국은 1,038개의 웹사이트가 변조되었고, 중국은 1,600개의 웹사이트가 침입을 당하였다.

4. 주요국 정보전 대응 동향

4.1 미국의 정보전 대응 동향

미국은 과거 물리적 테러 대비에서 급선회하여 화학, 생물학, 핵, 방사능 등 최첨단 기술을 이용한 테러 대비에 역점을 두고 있다. 특히, 9.11테러 직후부터 사이버테러 발생 가능성에 대한 우려의 목소리가 높아지면서 미국 수뇌부는 이에 대한 대비를 계속 강조하게 되었다.

그 결과, 부시 대통령은 2001년 10월 8일 대통령 명령(Executive Order) 13228[32]을 발표하여 국토안보국(Office of Homeland Security)을 설립하여 물리적 테러뿐 아니라 사이버테러 대응 및 복구에 관한 활동을 조정하는 임무를 부여하였으며, 대통령 사이버보안특별보좌관을 임명하여 정보시스템 보안을 위한 각 부처, 연방·지방 정부의 활동을 총괄 조정하고, 침해사고 복구를 총괄하며 주요정보통신시설을 운용하고 있는 민간 분야와의 업무를 조정하고 협의하는 역할을 부여하였다. 또한, 대통령 명령 13231[33]을 발표하여 대통령주요기반보호협의회(President's Critical Infrastructure Protection Board)를 설립하고, 미국의 국가 주요 기반시설 보호를 위한 최고 정책기관의 임무를 부여하였다. 그리고 2002년 6월 6일 테러 대책을 총괄하는 새로운 부서로서 국토안보부(Department of Homeland Security)를 창설 계획을 발표하였고, 이 계획은 국토안보법(Homeland Security Act of 2002)의 형태를 갖추어 상하원의 표결을 거쳐 11월 25일 대통령이 최종 서명함으로써 국토안보부가 설립되었다[34]. 이 부서는 국토안보를 총괄하는 임무뿐 아니라 정부의 정보보안을 강화하고, 정보기술을 이용하여 사이버공격으로부터 미국을 보호하는 임무를 부여받게 되었다. 국토안보부의 설립은 1947년 CIA 창설 이후 가장 큰 규모의 정부 개편으로, 사이버보안에 관련된 정부부처 중에 FBI의 NIPC(National Infrastructure Protection Center), 상무부의 주요 기반 보증국(Critical Infrastructure Assurance Office), 에너지부의 국가 기반 시뮬레이션 및 분석 센터(National Infrastructure Simulation and Analysis Center), 총무청의 연방 컴퓨터 사고 대응 센터(Federal Computer Incident Response Center) 등 22개 기관이 올해 9월말까지 이관될 예정이다.

법제 정비와 관련하여서는 애국법(USA Patriot Act of 2001)[35], 사이버보안연구개발법(Cyber Security Research and Development Act)[36], 전자정부법(E-Government Act of 2002)[37], 국토안보법 등을 신설하였다.

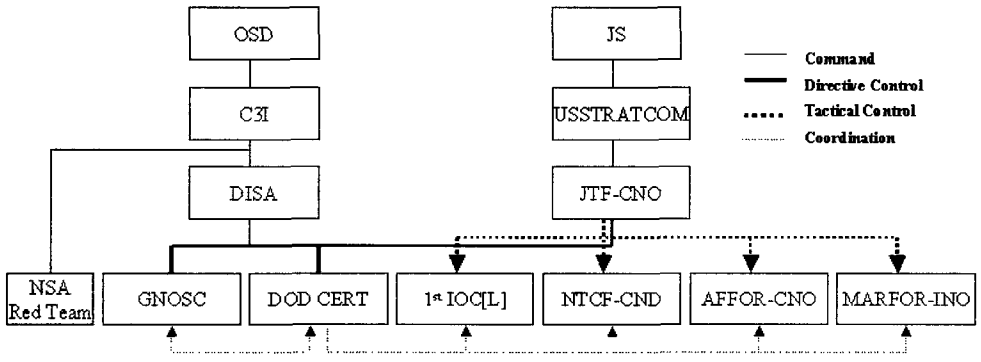
그리고 사이버보안을 강화하기 위한 국가 차원의 기획서인 사이버보안국가전략(National Strategy to Secure Cyberspace)[38]과 주요 기반물리적보호국가전략(National Strategy for the Physical Protection of Critical Infrastructures and Key Assets)[39]을 발표하는 등 다각적인 노력을 기울이고 있다.

한편 1999년 10월 1일부로 단일 지휘 계획(Unified Command Plan 1999: UCP-99)에 따라 미국 우주사령부(U.S. Space Command) 산하에 설치된 군 사이버방어 조직인 JTF-CND(Joint Task Force Computer Network Defense)를 2001년 4월 2일부로 JTF-CNO로 재편하여 사이버공격 및 방어 임무를 부여하고, 2002년 10월 1일 전략사령부 예하로 배치하였다. JTF-CNO는 (그림 1)과 같이 육군 제1 정보작전사령부(US Army's 1st Information Operations Command: 1ST IOC[L])[5], 해병대 컴퓨터 네트워크 방어팀(Marine Forces-Integrated Network Operations: MARFOR-INO), 해군 컴퓨터 네트워크 방어 작업반(Navy Component Task Force-Computer Network Defense: NCTF-CND), 공군 컴퓨터 네트워크 작전팀(Air Force Forces-Computer Network Operations: AFFOR-CNO), 그리고 국방정보체계국(Defense Information Systems Agency)의 국방 긴급대응팀(DOD Computer Emergency Response Team: DOD CERT)으로 구성되어 있다.

JTF-CNO는 UCP-2003에 의해 사이버공격팀과 사이버방어팀으로 분리될 예정인 것으로 알려지고 있다[40].

4.2 일본의 정보전 대응 동향

9.11테러 이후, 총리가 주재하는 긴급 관계성청 회의를 거쳐 생화학·핵에 대한 대응책 마련과 함께 사이버테러 대책 강화 등을 중점 추진 사항으로 의결하였다. 즉, 사이버테러를 대테러 대책의 하나로 분류함으로써 기존의 대테러 대책에서 진일보한 자세를 보여주고 있다. 현재, 일본 정부가 추진하고 있는 구체적 조치로서, 2001년 10월 2일 사이버테러 특별행동계획에 대한 후속조치[41]를 통하여 행정부 및 전력·교통 등 중요 인프라의 사이버테러 대응 연락·협력체계를 구축



(그림) JTF-CNO

5) 舊 Land Information Warfare Activity(LIWA)

하였으며, 보호 대상이 되는 정보 시스템을 지정한 바 있다. 특히, 이 후속조치에서는 내각관방을 중심으로 긴급상황 발생시 정보연락이 필요한 경우로서 다음과 같은 상황을 설정하고 각 사안별 연락체계를 정하였다[42].

- ○ 예고, 조직적인 예비행위 등의 예후
- ○ 중요시스템의 경미한 장애
- ○ 중요시스템의 중대한 장애
- ○ 사이버공격의 확인

또한, 다음과 같은 사안이 탐지된 경우에는 중요인프라 사업자가 반드시 관계중앙행정기관에 연락을 취하도록 하고 있다.

- ○ 중요시스템에의 영향이 상당정도 예상되는 공격을 탐지한 경우로서, 외부로부터 침입할 수 없는 내부네트워크의 중요시스템에 부정액세스 시도가 있었을 경우, 중요시스템에 장애를 일으킬 우려가 있는 컴퓨터 바이러스가 발견된 경우, 또는 공격 패턴이나 과거의 사례로 비추어보아, 중요시스템에 중대한 영향을 미칠 우려가 있을 것으로 예상되는 공격이 있었을 경우
- ○ 중요시스템에 대하여 특정 그룹 등이 명백한 의도와 목적을 가지고 공격한 것을 탐지한 경우

그리고, 전자정부 및 민간 중요인프라에 대한 사이버테러 대책을 원활히 수행하기 위하여 2002년 4월 1일 내각관방 정보보안대책추진실에 국가긴급대응팀(National Incident Response Team)[43]을 설치하고, 정부부처 정보보안 상담대응, 사이버테러 관련정보의 수집 · 분석, 사이버테러 피해확산 방지 및 복구에 대한 기술적 지원 등의 임무를 부여하였다.

한편, 방위청은 Info-RMA 추진에 있어서 "다양한 센서 등을 이용한 다중화 · 감내화 된 정보네트워크를 기반으로(방호화, 정보화), 육해공 자위대 각 부대가 정보를 실시간으로 공유(정보화)하고, 미군과의 상호운용성을 확보(상호운용성)하고, 사태의 변화에 유연하게 대응(유연화)하며, 최단시간(신속화)에 가장 효율적으로 전력을 발휘(통합화, 효율화)할 수 있는 태세를 구축"하기 위한 노력을 기울이고 있다. 이와 함께, 2000년 12월에 발표한 IT혁명에 대응한 종합시책 추진요강[6]을 발표하였는데, 그 중 정보 보안 확보를 위한 시책은 다음과 같은 것이 있다.

- ○ 정보보안정책 재정: 2000년 7월 내각 정보보안대책추진회의에서 제정한 정보보안정책에 관한 가이드라인을 참고로, 방위청의 기존의 업무체계 등을 고려하여 종합적 · 체계적인 보안대책을 제정한다.
- ○ 정보보안기반 정비: 실전환경하에서의 보안시스템을 평가하여 각 컴퓨터 및 네트워크에 소요되는 자원을 보완한다. 또한 방위청과 자위대의 컴퓨터 · 네트워크가 안전한 형태로 운용될 수 있도록 운용 노하우 DB를 정비하며 보안 담당 인재육성을 위하여 미국의 관계기관에 요원을 파견한다.
- ○ 사이버공격 대응부대 구축: 사이버 공격 등의 새로운 위협에 대처하기 위하여 방위청 및 각 부대의 네트워크에 대한 상시감시, 시스템 감사, 긴급사태 대처 등 정보보안 확보에 필요한 각종 기능 · 권한을 가지는 조직(부대)을 구축한다. 이 때, 통합네트워크관리운영기반 구축과 일원화시켜 추진한다.
- ○ 전자정부의 보안확보: 인적 · 기술적 기반정비와 더불어 실장환경하에서의 정보보안 운용평

6) 2003년까지 추진해야할 3대 중점시책으로 고도네트워크 환경정비, 정보 · 지휘통신기능 강화, 정보보안의 확보를 들고 있다.

가를 실시한다. 타 부처와 민간분야의 보안수준향상을 위하여 국가안보상 지장이 없는 범위에서 2003년도까지 관련 정보 및 know-how를 공개한다.

5. 결 론

지금까지의 전쟁은 주로 군사 분야에 한정되어 논의되었으나, 정보 시대에 접어든 지금은 기업은 물론 일반 개인까지 직접 관련이 되고 있다. 또한, 군은 물론이고 국가 주요 기반으로 전장이 확대되고 있다. 이에 대응하기 위해서는 기존의 사이버 보안의 개념을 한 단계 뛰어 넘어 국가 안보 차원에서 접근하여야 할 때다. 그러나 안타깝게도 우리는 아직까지 정보전의 개념과 범위 그리고 대상을 논의하고 있는 실정이다. 특히, 1.25 인터넷 대란을 겪으면서 우리의 사이버공간, 나아가 국가 기반이 되는 정보 공간을 지키는 것이 우리의 정보화를 완성시키는 지름길이라는 인식을 폭넓게 갖게 되었다.

데이터 위주의 정보보안은 데이터를 포함하여 컴퓨터와 네트워크를 보호하는 사이버보안의 개념으로 확장되었고, 이제는 국가 주요 정보 인프라를 지키고 미래 전쟁에서 승리하기 위한 정보전 개념으로 변화되었다. 이런 측면에서 정보전에 대한 인식을 확산시키고자 본 논문에서는 정보전의 개념, 위협 양상과 사례, 그리고 미국과 일본의 대응 동향을 살펴보았다.미래 정보전에 대비하기 위해서는 국가안전보장에 대한 위협요소로서의 정보전 개념을 명확하게 정의하고, 국가적 차원의 대응 방향과 대응 태세를 정립해야 할 것이며, 이를 지원하기 위한 기술개발과 함께 인적 능력 양성에 매진해야 할 것이다.

참고문헌

[1] O. Sami Saydjari, Strategic Cyber Defense, DAPRATech '99, Jun. 1999.

[2] W. M. Mularie, Information Systems Office Overview, DAPRATech '99, Jun. 1999.

[3] Gary M. Koob, Inherent Information Survivability, DAPRATech '99, Jun. 1999.

[4] -, Current ATIA Focused Research Topics, DARPA, 1999.

[5] -, Information Assurance and Survivability: Program Suite Description, DARPA, 1999.

[6] Sami Saydjari, Defense Advanced Research Project Agency(DARPA) Information Assurance Project, DARPA, 1999.

[7] Brian Witten, Automatic Information Assurance, DARPA, 1999.

[8] Sami Saydjari, Information Assurance, DARPA, 1999.

[9] Michael Skroch, Development of a Science-Based Approach for Information Assur-ance, DARPA, May 1999.

[10] Cathy McCollum, Cyber Command and Control (CC2), DARPA. 1999.

[11] 박상서, "사이버테러 대응 기술," 정보보호 심포지움 2000 논문집, pp. 259-294, 2000. 7.

[12] 박상서, "정보전 대응체계 구축 현황," WISC 2000 튜토리얼 자료집, pp. 73-177, 2000. 9.

[13] 박상서, DARPA의 정보전 대응 프로젝트, Cryptopia 제 4권 3호, 2000. 9.

[14] Alan D. Campen 외, Coming to terms with IW 사이버전 1, AFCEA국제부, 1996, p. 289.
[15] 권태환, 황호상, 정보전 개념, 정보보호학회지 제12권 6호, 2002. 12, pp. 1-11.
[16] 박상서 외, 정보전 대응체계 건설을 위한 종합 발전계획 연구, 국방정보체계연구소, 1998.
[17] 박상서, 이진석, 박춘식, "정보전 개념과 기술," 정보과학회지 제18권 12호, 2000. 12, pp. 8-19.
[18] 박상서, "정보전: 새로운 전쟁 패러다임," 공군 창군 50주년 기념 국제 학술 세미나 논문집, 교리 발전 분야, pp. 25-86, 1999.
[19] 박상서, 박춘식, "정보전 위협과 사례," 한국정보보호학회지 제 12권 6호, 2002. 12.
[20] Ed Sbrocco, Tom Ward and Chris Baden, CyberTerror: Potential for Mass Effect, IA Newsletter, Vol. 4 No. 4, Information Assurance and Technology Analysis Center, 2001.
[21] Anthony Lake, 6 Nightmares: Real Threats in a Dangerous World and How America Can Meet Them, Little, Brown and Company, Boston, 2000.
[22] Steven A. Hildreth, Cyberwarfare, CRS Report for Congress, Library of Congress, 2001. June.
[23] 박상서, 중국 네트워크 보안 위협, 국가보안기술연구소 TM, 2002.
[24] 박상서, 미군 정보전 조직 JTF-CNO, http://www.stratcom.mil, 2002.
[25] Bob Fish, Securing the U.S. Cyber-Environment, InfowarCon 2002.
[26] http://www.electricnews.net/news.html?code=9134519, 2003.
[27] 최명렬, 최근 사이버 공격 사례 및 정보전, Cryptopia 제 4권 2호, 2000.
[28] 정보처리진흥사업협회 시큐리티센터, 정보시큐리티의 현상: 2001년판, 2002. 5.
[29] 전상훈, Critical Alert for Cyber Terror: Security for Nation's Infrastructure, 2002. 10.
[30] http://abcnews.go.com/sections/tech/DailyNews/whhack990511.html
[31] Vigilinx, The People's Republic of China Network Security Threat Assessment, 2001.
[32] Establishing the Office of Homeland Security and the Homeland Security Council, Executive Order 13228 of October 8, http://www.fas.org/irp/offdocs/eo/eo-13228.htm, 2001.
[33] Critical Infrastructure Protection in the Information Age, Executive Order 13231 of October 16, http://www.fas.org/irp/offdocs/eo/eo-13231.htm, 2001.
[34] Homaland Security Act of 2002, http://www.whitehouse.gov/deptofhomeland/bill/hsl-bill.pdf, 2002.
[35] USA Patriot Act of 2001, http://www.ala.org/alaorg/oif/usapatriotact.html, 2001.
[36] Cyber Security Research and Development Act, http://www.theorator.com/bills107/s2182.html, 2002.
[37] E-Government Act of 2002, http://www.ala.org/washoff/egovact.html, 2002

[38] National Strategy to Secure Cyberspace, http://www.ala.org/washoff/egovact.html, 2002.
[39] National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, 2002,
[40] http://www.fcw.com/fcw/articles/2003/0203/web-net-02-07-03.asp
[41] http://www.kantei.go.jp/jp/it/security/tyousakai/dai1/susumekata.html.
[42] 김현수 외, 9.11테러이후 미국·일본의 대응동향, 국가보안기술연구소 TM, 2002. 6.
[43] Homeland Security Presidential Directive-1, http://www.whitehouse.gov/news/releases/2001/10/20011029-16.html, October 29, 2001

저자약력

박 상 서

1991년 중앙대학교 전자계산학과 공학사
1993년 중앙대학교대학원 전자계산학과 공학석사
1996년 중앙대학교대학원 컴퓨터공학과 공학박사
1996년~1998년 국방정보체계연구소 선임연구원
1999년~1998년 국방과학연구소 선임연구원
2000년~ 현재 국가보안기술연구소 선임연구원

박 춘 식

1981년 광운대학교 전자통신공학과 공학사
1983년 한양대학교 전자통신공학과 공학석사
1995년 일본동경공업대학교 전기전자공학과 공학박사
1989 ~ 1990 일본 동경공업대학 객원연구원
1982 ~ 1999 한국전자통신연구원 책임연구원
2000 - 현재 국가보안기술연구소 책임연구원