외국의 사이버 공격전 대비 현황

세계 주요국들 사이버전쟁 공격적으로 준비해

글_임종인

고려대학교
정보보호대학원 원장
jilim@korea.ac.kr

글쓴이는 고려대학교에서 수학과 박사학위를 받았다. 1986년부터 고려대학교 교수로 재직하고 있다. 현재는 고려대학교 정보보호대학원 대학원장과 정보보호기술연구원 원장, 사이버국방학과 교수직을 맡고 있으며 사이버국방연구센터 센터장을 겸임하고 있다. 안전행정부 정책자문위원회 위원, 경찰청 정보통신위원회 자문위원, 국가정보원/국가보안기술연구소 정보보안/암호정책 자문위원 등으로 활동하고 있다.

인류의 역사를 돌이켜 볼 때 과학기술의 발달은 전쟁수단에 곧바로 접목되곤 하였으며 우리 사회의 많은 부분에 큰 파급효과를 가져왔다. 획기적으로 발전하고 있는 과학기술의 진전은 전쟁의 공간마저 바꾸고 있다. 이제 인간의 전쟁터가 육지 · 바다 · 하늘 그리고 우주에 이어 사이버공간이 제5의 전쟁터가 되었다.

첨단 군사시설뿐만 아니라 정부 활동, 국가기간산업, 민간의 기본적 경제활동 역시 컴퓨터 의존도가 높아지는 추세에서, 컴퓨터 및 네트워크 시스템에 대한 방어와 공격능력 개발은 이제 국가안보의 핵심과제로 떠오르고 있다.

본고는 사이버전쟁의 정의와 특징을 정리하고 사이버 전쟁에 대비한 세계 각국의 대응태세 현황과 이들 국가들의 정책이 우리나라의 사이버안보 정책에 주는 시사점에 대해 간략히 기술하기로 한다.

국가기반시설 포함한 민간분야 공격 목표

사이버전쟁이란 인터넷을 비롯한 사이버공간에서 일어나는 전쟁을 의미한다. 비물질적 공간인 사이버공간에서 총성 없이 수행되는 전쟁으로 적군의 정보통신 체계 및 국가기간 전산시스템을 공격해 기능을 발휘하지 못하게 하거나 그 가치를 떨어뜨림으로써 정보 우위와 특정 목적을 달성하는 동시에 아군의 정보통신체계를 보존하기 위해 수행하는 사이버 상의 전쟁을 의미한다. 주로 고도로 네트워크화된 정보사회의 취약점을 공격함으로써 물리적 군사시스템의 파괴에 버금가는 손실을 초래하는 전쟁이라 할 수 있다.

과거의 사이버공격이 전문가에 의한 수동적인 공격이었다면, 최근의 사이버공격은 자동화 · 대규모화되고 있다. 즉, 단순 사이버공격이 아닌 사이버범죄 및 사이버전의 형태로 발전하고 있다. 이러한 변화는 사이버공격이 정치적, 군사적 목적을 가지면서 더욱 위험해지고 있다. 일단 갖춰진 사이버전체계는 반드시 전시상황에서만 사용될 수 있는 것은 아니다. 평상시에도 주요 국가 기반시설에 타격을 줄 수 있고 산업 기밀을 유출하는 등의 용도로 활용될 수 있다.

사이버전의 특징은 소수인원과 적은 비용으로 지구촌 어디서든 공격할 수 있으며, 초보적인 공격기술로도 핵무기 못지않은 치명적 손상을 줄 수 있고 상대국가의 조직, 군대 기능을 무력화할 수 있다는 점이다. 이러한 사이버전의 위협은 기술의 발달과 컴퓨터 네트워크에 대한 인류의 의존도가 더 커질수록 증대된다. 그러므로 현대사회에서 사이버전에 의한 물리적 · 경제적 피해는 상상을 초월한다.

또한 사이버전에 의한 정치적 · 사회적 피해 역시 만만치 않을 것으로 예상하는데, 이는 사이버전의 여파가 정부 기능 마비, 사회적 혼란, 다른 국가로의 위험 전파, 핵심 기술 및 비밀정보의 유출 등으로 나타나기 때문이다. 여기서 주목해야 할 사항은 사이버전의 범위가 점점 넓어지고 있다는 점이다. 과거에는 정보통신 기술을 사용하는 무기 시스템이나 군사시설 등이 공격 목표였다면 최근에는 금융, 전력, 수도, 항만 등 국가 기반시설을 포함한 민간 분야도 사이버전의 공격 목표가 되고 있다.

결과적으로 사이버전은 군 관련자나 일부 전문가들의 문제가 아닌 현대를 살아가는 모든 일반인이 직면한 문제이며 이에 따라 평상시 대비가 매우 중요해지고 있다. 사이버전쟁이 국가방위 및 안보에 지대한 영향을 미침에 따라 세계 주요국들은 자국의 군사비밀보호 및 미래형 첨단 사이버전쟁에 대비하여 전문 인력의 양성, 사이버 특수부대의 창설, 예산증액 등 다양한 노력을 통해 사이버전력 역량 강화에 주력하고 있다.

사이버 전에 대비한 세계 각국의 대응태세

사이버전쟁 대비를 위한 전 세계 각국의 현황은 어떠한가. 우선 미국을 살펴보자. 미국은 정보전 또는 사이버전쟁이라는 용어를 처음 사용한 나라이고, 국가 전면전에 이용한 나라이다. 또한, 전 세계컴퓨터 용량의 46퍼센트를 사용할 정도로 세계에서 컴퓨터 및 네트워크 의존도가 가장 높은 나라로 사이버 전쟁을 우려하고 있다. 최근 미국 정보기관의 연간 전 세계 위협 평가보고서에 처음으로 사이버공격이 미국이 직면한 보안위협 중 가장 높은 것으로 발

표한 것은 이러한 우려를 명백하게 보여준다고 할 수 있다.

미국은 세계 어느 나라보다도 사이버전에 대한 다양한 대비책 강구에 국가적인 노력을 기울이고 있는데, 2009년 5월에 발표된 '사이버정책 검토 보고서'를 기점으로 지금까지 미국 정부에서 발표한 수많은 보고서를 통해 미국이 사이버 안보 및 전력에 대한 논의를 발전시키고 체계화하는 것은 물론 적극적으로 사이버전에 대응하고 있다는 것을 알 수 있다.

미국의 사이버 정책관련 보고서들을 통해 공개된 사이버안보 관련 전략적 기조는 다음과 같이 정리할 수 있는데 우선 사이버공간을 새로운 작전영역으로 보고 있다. 또한, 국방부가 운영하는 모든 네트워크 및 시스템에 대한 보안조치를 강화하고 통제 및 관리능력을 체계화하려 하고 있으며 범정부 차원의 유기적 협력을 통한 총체적 대응 필요성을 제시하고 있다.

동맹국 및 협력국과의 국제협력을 증진하고 민간영역과의 협력 필요성 역시 강조하고 있으며 집단적 자위권과 집단적 억지력 발휘를 위해서는 국제협력 및 연합 훈련을 통한 능력의 배양을 절실히 요구하고 있다. 마지막으로 사이버 분야에 대한 우수 인력을 육성 · 확보하고 각종 장비를 지속적으로 업그레이드할 필요성을 제시하고 있다. 이와 더불어 사이버전 억지력을 보유하기 위해 공격과 방어 기술이 적절한 균형을 이루어야 할 필요성을 인식하고 기술개발 및 인력양성을 강화하고 있다.

미 국토안보부는 작년 말에 고도의 기술력을 갖춘 사이버보안 전문 인력을 정부가 상시로 운용하기 위한 방안으로 사이버예비군 창설을 발표하였다. 사이버예비군은 사이버 보안인력채용, 교육 등 다양한 방법을 통해 단기간 내에 약 600여 명 규모로 구성될 예정이며 점차 인력을 확대해 나갈 것이라고 미 국토안보부는 밝히고 있다.

미 국방부 산하 사이버 사령부 키스 알렉산더 사령관은 올해 초 국가 핵심 시설 붕괴를 초래하는 사이버 공격에 대응하기 위해 국방부에 새로운 전담 부대 창설을 언급하였다. 신설되는 사이버 공격부대는 미국 국방부와 민간 IT 전문가들로 구성되며 2015년까지 총 40개 팀으로 구성될 예정이라고 밝혔다. 이 팀은 미국 핵심 인프라 시스템 대상 공격을 예방하는 임무를 맡게 될 예정이다.

이러한 사이버 전담부대는 방어적으로 운영될 뿐만 아니라 사이버 공격이 있을 경우 국가방위를 목적으로 공격적 행동에 나설 수 있다고 밝힌 바 있는데 이는 최근 미국의 주요 금융, 언론 기관의 해킹사고가 빈번하게 발생함에 따라 사이버 전담 부대 확충의 필요성에 크게 공감하여 이루어진 것으로 보고 있다. 한편, 미 국방부는 2013년부터 2017년까지 사이버무기 개발 프로젝트인 플랜X를 통해 사이버작전에 사용되는 무기들의 자동화된 능력을 개발할 것을 밝히는 등 기술적인 부분에서도 미래의 위협에 가장 발 빠르게 준비하고 있다.

중국은 1997년 4월 인민해방군 내에 사이버 해커 부대를 창설한 이후 현재 베이징과 광저우, 지난, 난징 등 4개 군구에 사이버 특수부대를 운영하고 있다. 특히, 인민해방군 총참모부 직속 사이버 사령부 산하에 창설된 61398부대는 사이버 공격 및 방어체제 구축을 전담하고 있다. 중국은 사이버전에 매우 적극적인 모습을 보이는데 미 국방부의 '중국 군사력 보고서'에 따르면 중국은 2007년부터 인민군의 컴퓨터 네트워크 공격 및 방어대책에 투자를 아끼지 않는 것으로 보고하고 있다. 이러한 중국의 적극적인 노력은 미국에 비해 육 · 해 · 공 전력이

각 국가별 주요 사이버전 관련 주요 정책

국가	주요 정책
미국	• 국방부 산하 사이버사령부 인원을 약 1만 명으로 확대할 예정 • 국방부 산하 사이버보호부대, 국가임무부대, 전투임무부대 창설 • 국토안보부 산하 사이버예비군 창설 • 내년 국방예산 중 사이버보안예산 올해보다 약 6배 인상 • 사이버보안 기술연구에 투자 및 민간 보안업체와 공동 프로젝트 수행하여 지자체 보안 시스템 마련
중국	• 인터넷 기초총부를 조직 • 인민해방군 총참모부 산하에 61398 부대를 포함하여 군 소속 정예 해커부대원 약 1만3천여 명으로 추정
이스라엘	• 국방부 산하에 8200부대 창설
영국	• 2010년 국가 사이버보안 프로그램 발표 • 국방부 산하에 사이버예비군 창설 예정
북한	• 1990년대 초반부터 해커 등 사이버전 인력 양성 • 2009년 정찰총국 산하에 사이버전 지도국(121국)창설 (약 3천 명) • 김일 자동화대학, 김책공대, 평양컴퓨터기술대학, 김일성군사종합대학 등에서 우수 인력 양성
한국	• 2009년 사이버사령부 창설하여 약 500명의 인력 보유 • 올해 안으로 사이버사령부 인력 1천명 이상으로 확대 계획 • 국방부 내에 사이버정책총괄과 개설 예정

상대적으로 약한 전통적인 전력에서의 약세를 보완하기 위해 사이버전력 증강에 전력을 기울이고 있는 것이라고 전문가들은 보고 있다.

이스라엘은 국방부 직속 정보부대인 8200부대를 운영하고 있다. 8200부대는 1952년 창설된 정보부대로, 준장급 장교가 이끄는 이스라엘 군대 내에 최대 규모로 꼽히며, 미국 사이버부대와 견줄 만한 수준인 것으로 알려져 있다. 인터넷이 일반화된 이후에 사이버 공격 훈련에 주력하는 등 사이버전 부대로 전환했으며 이란의 원자력 기간망 시설을 공격한 '스턱스넷(stuxnet)' 등의 변종 바이러스를 개발한바 있다.

유럽국가 중에서는 영국이 가장 선도적이라고 할 수 있다. 영국은 2010년 '국가 사이버 보안프로그램'을 발표하면서 사이버전 역량을 강화하고 있다. 또한, 국방부 산하에 있는 사이버보안 관련 국가 위기 상황 발생 시 영국군을 지원하기 위한 '사이버 예비군' 창설을 미국에 이어 두 번째로 발표하였다. 앞으로 4년간 6억5천만 파운드(약 1조 1천만 원)의 예산을 투입해 사이버보안 정책을 진행할 것이라고 영국 정부는 밝히고 있다.

북한은 1990년대 초반부터 정책적으로 사이버전 인력을 양성한 것으로 알려져 있으며 현재 러시아와 미국에 이은 세계 3위권의 사이버전 강국으로 평가받고 있다. 2009년에는 대남 · 해외 공작업무를 총괄하기 위해 인민무력부 산하에 정찰총국을 만들면서 사이버전 능력을 대폭 강화했다. 당시 정찰총국 산하에 전자정찰국 사이버전지도국(121국)이 생겼으며 약 3천 명의 규모로 파악되고 있다. 전문가들은 이들이 북한 사이버 부대의 중심이라고 보고 있다.

북한은 뛰어난 해커양성을 위해 10대 컴퓨터 영재들을 전국적으로 광범위하게 선발, 모집하고 있으며 일찌감치 외국의 정보 관련 대학에 조기 유학을 보내는 등 사이버전 인력 양성

에 심혈을 기울이고 있다. 북한의 경우 재래식 전력 상 한국과의 큰 격차를 만회하기 위해 사이버전에 관심을 보이고 있다. 리처드 클라크 전 백악관 대테러담당관이 언급한 바와 같이 북한은 산업시설 중 극히 일부만이 디지털 네트워크를 기반으로 하고 있으며, 사이버 공격의 영향을 거의 받지 않기 때문에 오히려 사이버전에 강한 측면이 있고 더욱 사이버전력 증강에 집중하고 있다.

우리나라 사이버안보 정책 미흡해

위에서 살펴본 바와 같이 세계 각국은 사이버안보와 사이버전에 대한 관심이 높아짐에 따라 기술적 · 제도적 준비는 물론 사이버부대 병력을 확대하고 적극적인 공격전력을 진행하고 있다. 사이버공격에 대한 물리적 대응을 포함한 능동적 방어 전략의 확대는 수동적 방어 대책을 답습하고 있는 우리나라에 시사점을 주고 있다.

한국은 7.7 DDoS 사건을 계기로 군 차원의 사이버 안전의 중요성을 감안하여 '사이버 사령부'를 창설하였다. 사이버 사령부 인력은 500여 명 수준이며, 향후 1천명 이상으로 확대할 계획이나 아직까지 사이버 사령부의 역할이 명확하지 않으며, 역량이 부족하다는 평가를 받고 있다. 최근에는 군의 사이버 업무가 기능별로 분산되어 있는 것을 고려하여 분산된 기능을 국방부로 통합해 올 상반기 내에 사이버정책총괄과 신설을 발표했다. 그러나 아직까지 한국의 사이버위협 대응인력 및 기술력은 취약한 수준이며 사이버 전쟁에 대한 대비나 인식도 낮은 상황이다.

사이버 공격이 국가 기간망까지 위협하는 상황에서 미국을 비롯한 여러 국가들은 사이버부대를 창설해 인력양성에 힘쓰고 있는 반면, 한국은 아직까지 인력양성에 소극적인 모습이다. 올해에는 주요 금융권과 방송사가 마비되는 3.20 대란을 또 겪었지만, 한국 정부의 태도는 사이버위기 상황이 있을 때마다 사후처리에만 급급하고, 관련 예산을 증액하는 데에도 미온적인 태도로 일관하고 있다. 국가차원에서 사이버위기상황에 대비하고 컨트롤할 수 있는 조직의 부재도 문제점으로 지적되고 있다.

다각적인 대응체계 수립 필요

사이버 공간은 이제 새로운 전쟁터로 떠오르고 있으며, 바야흐로 세계 각국은 이제 사이버전의 시대에 접어들고 있다. 과거에 일부 국가의 압도적인 군사력 증가 대결이 세계 평화를 위협했다면, 사이버전시대에는 모든 국가가 언제든지 공격에 나설 수 있어 그 위험은 더욱 커졌다고 할 수 있다. 세계 각국의 사이버전 능력 향상 경쟁이 치열한 가운데 사이버공간에 대해 국가안보적 차원에서 다각적인 대응체계를 수립해 나가고 있다.

이미 미국을 필두로 많은 국가가 사이버전쟁의 중요성에 대해 인식하고 있으며, 단순히 방어적인 차원이 아닌 공격적인 차원의 대응까지도 적극적으로 준비 중이다. 한국 역시 국외 사이버전의 효과적인 방어를 수행하기 위한 사이버 방어기술과 적의 사이버 도발행위에 능동적으로 대응하기 위한 사이버 공격 식별, 반격 기술, 전략적 작전 수행 등 사이버공격 기술에 관한 체계적인 연구가 필요하다. ST