북한의 비대칭 전략-'사이버 기습공격'에 대한 대책 연구

권 문 택*

요 약

본 연구는 한반도내에서 발생 가능한 비대칭 전략으로서의 '사이버 기습공격'의 발생 가능성에 대해 분석하고 이에 대한 정책적 대책을 제시하기 위해 작성한 것이다. 최근 발생하고 있는 이란, 중국 등에서 발생한 'Stuxnet' 사이버 기습공격 피해 사례로 볼 때 만일 북한이 남한의 인프라 시설을 공격한다면 남한 사회에 큰 혼란과 피해를 줄 수 있을 것이다. 최근 발생한 연평도 기습도발 사건 이후 계속적인 도발 위협을 하고 있는 북한의 태도로 볼 때 'Stuxnet'과 같은 사이버공격을 감행할 개연성이 높기 때문에 이에 대한 정책적 대책을 제시하였다. 주요 대책은 1) 독립된 중앙집권적 정부통합조직 신설, 2) 특수대학 설립으로 사이버전 전문인력 양성, 3) 예산 증액 및 전문인력 관리체계 개선이다.

A Study on Countermeasures to the North Korean Asymmetric Strategy-'Cyber Surprise Attack'

Moon Taek Kwon*

ABSTRACT

Information security is a critical issue for national defense. This paper provides a result of a study on the countermeasures to the North Korean Asymmetric Strategy-'Cyber Surprise Attack'. After the attack on Yeonpyeong island, the North Korea threatened there will be more surprise attack to the South Korea. Based on the analysis of 'Stuxnet' cyber attack to Iran and China, the North Korean surprise attack may be 'Stuxnet' class cyber attack. This paper several strategic countermeasures in order to overcome the anticipated the North Korean cyber surprise attack.

Key words : Information Security, National Defense, Cyber Attack

접수일 : 2010년 11월 20일; 채택일 : 2010년 12월 19일

* 경희대학교 테크노경영대학원

1. 서 론

북한의 2010년 11월 23일 연평도 도발은 우리정부의 대북정책과 안보의식 등 한국 사회 전반을 급격히 변화시키고 있다. 북한의 불장난에 주요 20개국(G20) 서울 정상회의의 성공적 개최를 어렵게 일구어 낸 남한의 국제적 위상은 큰 타격을 받게 되었고, 전 세계가 한국을 전쟁 위험 국가로 인식하는 '코리아 리스크'가 남한 경제의 발목을 잡을 가능성이 높아지고 있다. 북한의 목적은 핵 폭탄 개발과 무력도발을 통해 동족을 대상으로 인질극을 벌이면서 북한 정권의 세습을 보장 받는 동시에 체제를 공고히 하고자 하는 것이다.

북한은 연평도를 기습공격 한 이후에도 남한에 대해 추가 공격 가능성은 계속 제기되고 있다. 서해상에서의 한·미 합동군사훈련이 끝나면서 미국 항공모함 조지워싱턴함도 떠났다. 군은 연평도가 공격당한 뒤 연평도에 K-9 자주포와 대 포병 레이더를 보강하는 등 각종 무기를 추가로 배치하고 있다. 국회 국방위원회도 신속히 연평도·백령도를 비롯한 서해 5도의 전력보강을 위한 새해 예산 3100억 원을 승인했다. 군은 이 예산으로 진지 파괴용 벙커버스터, 지상표적 정밀타격 유도무기 등을 배치할 계획이다.

이와 같이 연평도가 공격 받은 탓에 연평도에 각종 무기를 집중 배치하는 것은 이해는 가지만 군은 서해 5도만이 아닌 전 국토에 대한 대비 뿐 아니라 각종 비대칭 기습공격에도 철저히 대비해야 한다. 북한이 다시 불장난을 한다면 기존과는 도발 방식이 다를 것이다. 일본 도쿄 신문은 2010년 12월 3일 북한 정보소식통을 인용, "북한이 경기도를 포격할 수 있다."고 보도했다. 북한 리영호 인민군 총참모장이 연평도 공격 직후 "불벼락이 계속될 것"이라고 말한 데다, 북한은 무지막지한 집단이라는 점에서 흘려버릴 수만은 없다. 북한이 서해 5도나 포항과 울산을 동시 타격할 계획을 세웠다는 설도 있다. 18만 명이나 되는 북한의 특수전 부대 능력으로 볼 때 충분히 가능한 일이다. 따라서 전·후방이 따로 없다는 개념으로 군과 정부, 국민 모두 정신을 바짝 차려야 한다.

그러나 여기서 간과해선 아닐 될 중요한 사항은 남한의 전력, 금융, 공항 및 항만 등 주요 인프라 시설에 대한 북한의 '사이버 기습공격'의 가능성이다. 어쩌면 과거 북한의 기만전략 및 전술 행태로 볼 때 서해 5도, 경기도 지역 등에 대한 추가 공격을 하겠다는 등의 공갈 협박은 일종의 위장 전술에 불과하고 사실은 치밀하게 남한의 주요 인프라 시설과 정보통신망에 대한 '사이버 기습공격'을 준비하고 있다가 적절한 시기에 공격을 감행하여 사회 혼란을 야기 시키고 '코리아 리스크'를 부각 시키려고 할 가능성이 충분히 예측되는 상황이다.

과거의 사례를 보자. 2009년 7월 7일, 8일, 9일 연속적으로 청와대 등 국가 주요 핵심기관에 대한 동시다발적 사이버공격은 남한 국가 안보에 큰 충격을 준 사건으로서 공격이 사전 계획에 따라 매우 조직적으로 진행된 것으로 판명되었다. 이 사건은 사이버 라이프(cyber life)가 일상생활의 큰 부분을 차지하고 있는 남한 사회 전체를 마비시키려는 의도가 읽히고 있으며, 국가정보원은 이 공격이 북한에 의한 사이버테러로 잠정 결론을 낸 바 있다.

이 사태는 세계 최고 수준의 IT 인프라를 자랑하는 한국이 사이버 전쟁에 얼마나 취약한지 여실히 드러냈다. 즉, 대한민국을 적대시하는 세력들이 마음만 먹으면 얼마든지 우리 안보와 경제·사회 시스템을 마비시킬 수 있다는 사실을 보여줬다. 민간부문의 정보보안 주무기관인 방송통신위원회는 사건 발생 6시간 뒤에야 겨우 대국민 경보를 발령했고 뚜렷한 대응책도 내놓지 못했다. 사흘째인 9일에야 바이러스에 감염된 PC의 인터넷 접속을 차단하는 방안을 논의할 정도로 거북이 걸음이었다.

이런 점에서 볼 때 북한이 남한 사회를 혼란에

빠뜨리기 위해 서해5도든 경기도든 추가적인 공격을 하겠다고 공공연히 위협하는 현 상황에서 '사이버 기습공격'도 그 가능성을 열어두고 민/관/군이 합심하여 국가적 총력 대응체제를 갖춰야 한다. 따라서 본 논문에서 연구자는 북한이 '사이버 기습공격'을 감행할 것을 가정하고 이에 대한 국가적 대책을 제안하고자 한다.

2. 비대칭 전력으로서의 사이버전력

2.1 비대칭 전력의 개념

전항에서 언급한 북한의 도발 사건들은 남한 안보에 있어서 북한의 비대칭 전력이 매우 큰 위협요소라는 것을 인지하는 계기가 되었다. 비대칭 전력이란 상대의 비교 우위 전력을 피하고 상대의 상대적 취약점을 공격해 타격을 입힐 수 있는 전력 체계를 말한다. 재래식 무기에서 열세인 나라가 이를 만회하기 위해 핵무기를 갖게 되면 그것이 바로 비대칭 전력이라고 할 수 있다. 이런 관점에서 본다면 북한은 남한과 재래식 무기에서의 상대적 열세를 핵 무장, 대규모 특수부대 보유 및 화생방 무기 등 비대칭 무기체계를 보유함으로서 만회를 하고자 하고 있다. 여기에 더하여 최근에는 사이버전 전력도 비대칭 전력의 범주에 포함된다.

야포, 군함, 전투기 등 재래식 무기체계에 대한 전력 증강은 비용이 많이 드는 사업이다 또한 핵・미사일・잠수함 등의 비대칭 전력도 개발에 상당한 비용이 든다. 그러나 사이버전 수행 능력의 향상은 상대적으로 싸게 이룰 수 있다. 북한의 입장에서 매우 매력적이라 할 수 있다. 북한은 이미 1989년 조선컴퓨터센터(KCC)를 시작으로 현재 미림자동화대학 등을 통해 사이버전 엘리트들을 양성하고 있다. 2009년 7월 7일 DDoS 대란을 일으킨 주체가 북한일 것이라는 징후가 다수 발견된 바 있고, 미국 CIA도 그렇게 추정하고 있다.

2.2 비대칭 전력으로서의 사이버전 전력 가치

북한의 남한에 대한 비대칭 전력은 전항에서 언급한 바대로 핵무장, 특수전 부대, 생/화학 무기를 들 수 있다. 그러나 최근 급부상하고 있는 또 하나의 옵션은 바로 사이버전 전력이다. 북한이 사이버전 전력을 비대칭 전략으로 활용할 것이라는 추정이 가능한 이유는 다음과 같다.

첫째, 남한사회는 북한사회와 비교가 되지 않을 정도로 세계 최고 수준으로 정보기술이 발달되어 사회 모든 분야의 업무가 정보화에 의한 시스템으로 움직이고 있다는 것이다. 상대적으로 북한사회는 이제 막 인터넷이 공공기관을 중심으로 구축되는 단계이고, 일반 대중의 정보기기 활용은 극히 일부 특권층에 한정되어 있기 때문에 쌍방 간에 사이버전이 발생 할 경우에 사회 근간을 움직이는 정보기기 시스템에 대한 피해 범위와 규모는 상상을 초월 할 정도로 남한에 불리하다는 것이다.

둘째, 한국군은 10여전부터 국방정보화 계획을 추진하여 많은 무기체계 및 지휘통제시스템이 자동화되어 있다. 아직 완성단계는 아니지만 일부 무기체계는 C4I시스템으로 통합되어 구축되어 있으며 점차 이를 확대 발전시켜 나아가고 있다. 따라서 무기체계는 전자화되고 전장관리와 의사결정 지휘체계는 인터넷 기술을 활용하여 시스템화 되어가고 있다. 이와 같이 국방정보화가 진전 될수록 점점 더 사이버 공격으로부터 취약하게 될 것은 당연한 결과이다.

셋째, 사이버 기습 공격은 전통적이고 물리적인 공격과는 달리 인명 살상, 건물 파괴 등 직접적이고 물리적인 피해와는 거리가 있어 국제적 비난의 화살을 어느 정도 피해 나갈 수 있다는 것이다. 북한의 연평도 포격도발은 2명의 해병대 용사와 2명의 무고한 민간인을 살해하고 많은 민간 주택을 파괴하였다. 따라서 남한 영토에 대한 도발 행위에 더하여 인명 및 주택 파괴로 인해 국제적 비난과 함께 북한 정권의 야만적인 실체를 만천하에

알리는 계기가 되기도 한 사건이다. 그러나 사이버 공격은 이러한 문제에서 비교적 자유로운 옵션이 될 수 있다는 것이다.

넷째, 비록 북한이 남한의 군사 및 민간 시스템에 대하여 사이버 공격을 감행하였다 하더라도 남한 당국에서 북한이 공격했다라고 주장 할 수 있는 사실 관계 입증이 어렵다는 것이다. 주로 인터넷을 통한 공격이기 때문에 다른 나라에 있는 서버를 이용할 수 있어 공격자의 신원을 확인하기가 쉽지 않고, 또한 공격행위와 결과 사이에 시간적인 간격이 있을 수 있어 자위권 등의 대응 수단을 선택하기가 쉽지 않다는 것이다. 사이버 정보전은 즉시 효과가 나타날 수도 있지만 공격 유형에 따라서는 공격행위와 실제 결과가 발생하는 시간 간격이 장시간에 걸쳐 일어 날 수 있기 때문이다.

다섯째, 비록 사이버 공격의 진원지가 북한이라는 물증을 확보한다 하드라도 그 행위 주체가 북한군이라는 증거를 입증하기가 쉽지 않다는 것이다. 사이버테러 행위는 얼마든지 개인이 할 수 있기 때문이다. 사회에 불만을 품은 해커일 수도 있고, 호기심에 의한 충동행위일 수도 있기 때문이다. 과거 사이버 피해 사례에 보면 이러한 사례를 다수 발견할 수 있기 때문에 호전적인 북한군의 전문 사이버전 공격팀에 의해 감행된 행위라 하더라도 사전 치밀한 계획하에 위장을 할 수 있기 때문에 충분히 공격 주체를 숨길 수 있기 때문이다.

3. 비대칭 사이버공격 사례/공격대상

3.1 최근의 비대칭 사이버공격 사례

미국 보스턴대학교의 정치학 교수 이반 아레긴-토프트는 1800년 이후 무력에서 상대적으로 열세이면서도 비대칭전략을 사용하여 전쟁에서 승리한 경우가 전체 분쟁에서 28%를 차지한다고 하면서 이러한 승률은 최근 들어 점차 증가한고 있다고 주장한 바 있다. 이러한 '약자'를 위한 신종 무기 중 최근 가장 유망하게 떠 오른 사이버전 사례는 'Stuxnet'와 같은 신종 바이러스일 것이다.

'Stuxnet' 바이러스는 핵 시설 같은 산업시설의 통제 시스템 프로그램을 조작해 물리적 손상을 일으키는데, 발전소, 정유소, 화학공장, 파이프라인, 교통 시스템 등 자동화시스템을 갖춘 다양한 기간 인프라가 표적이 될 수 있다. 따라서 앞으로 불과 몇 개월 안에 해커들이 이미 공개된 'Stuxnet' 코드를 이용, 다양한 변종 바이러스를 만들어 각국 정부와 테러집단, 범죄조직 등에 팔아넘길 수 있다고 일부 보안전문가들은 지적하고 있다.

최근 마무드 아마디네자드 이란 대통령은 'Stuxnet'이 이란 우라늄 핵 농축 프로그램의 원심분리기의 일부를 감염시켰다고 공식 발표한 바 있다. 이는 'Stuxnet'이 사이버공격 무기임이 입증됐다는 증거로 볼 수 있다. 또한 홍콩 사우스차이나모닝포스트(SCMP)는 2010년 10월 1일 "지난 며칠 새 중국 전역의 600만대 컴퓨터와 거의 1000곳의 산업 시설이 감염됐다"고 보도한 바 있으며, 중국 신화통신은 자국 컴퓨터 전문가의 말을 인용해 "Stuxnet에 명령을 내리는 서버가 미국에 있다"고 주장한 바 있다. 아직까지 중국 정부가 중국의 기간 시설이 'Stuxnet'에 감염됐다고 공식 공표하지는 않았으나 중국 최대의 수력발전소인 싼샤댐, 베이징의 서우두 국제공항과 시내 교통 통제 시스템, 베이징~톈진 간 고속철도, 상하이의 자기부상열차 등이 감염됐을 가능성이 있는 것으로 알려지고 있으며, 이들을 포함한 상당수 중국 기간 시설은 'Stuxnet'이 공격 목표로 삼는 독일 지멘스사의 통제 소프트웨어(SCADA)를 사용하고 있음도 확인된 바 있다.

3.2 예상되는 남한의 사이버공격 대상

전항에서 살펴 본 사례를 종합해 볼 때 만약 어느 나라든 국가급 전문 기관이 'Stuxnet'과 같은 사이버공격 무기를 정교하게 개발하여 '크루즈 미사일'과 같이 특정 목표에 대하여 공격한다면 마치 '사이버 크루즈 미사일'과 같은 효과를 볼 수 있기 때문에 향후 비대칭 무기로 충분히 고려 할 수 있는 가능성이 매우 높다고 볼 수 있고, 북한이 이러한 사실을 예의 주시하고 있을 것이라 판단된다.

따라서 향후 북한이 남한에 대해서 도발을 한다고 하면 인명살상과 가옥 파괴 등 전 세계가 공분할 소지가 있는 재래식 무기를 사용하기보다는 우선 'Stuxnet'과 같은 사이버전 무기를 사용하여 '사이버 기습공격'일 가능성이 매우 높다. 'Stuxnet'는 발전소, 공항, 철도 등 기간 시설을 파괴할 목적으로 제작된 컴퓨터 악성코드로서 일반대중이 흔히 사용하는 USB와 네트워크 공유 취약점 등을 이용해서 전파된다. 최근에 유포된 전체 'Stuxnet'형 바이러스 감염 사례의 60%가 이란에 집중돼 있는 통계를 볼 때 아마도 미국이나 이스라엘이 이란 핵시설을 마비시키기 위해 퍼뜨린 사이버 무기일 가능성도 매우 높다고 볼 수 있다.

따라서 이 악성코드를 이용하여 북한이 은밀하게 남한의 주요 기간 시설, 즉 원자력 발전시설, 첨단 자동화 산업 생산시설, 은행을 비롯한 금융기관, 댐 수위조절 시설, 공항 관제시스템 등을 공격한다면 연평도 도발과 같은 인명 살상과 파괴로 인한 도발자라는 증거를 남기지 않고 더 큰 사회적 혼란과 피해를 줄 수 있고, 또한 공격주체자의 모호성으로 인해 어느 정도 국제적 비난도 피해갈수 있기 때문에 북한으로서는 충분히 고려해 볼 만한 카드로 생각 할 수 있을 것이다. 이런 점에서 볼 때 영화 '다이하드 4.0'에서와 같이 국가 기간망을 공격한 사이버 전쟁으로 인한 혼란상을 볼 때 국가 주요 기간 시설 및 산업 자동화 시설에 대한 안전 대책이 시급히 필요하다.

4. '사이버 기습공격'에 대비한 정책적 대책

4.1 독립된 중앙집권적 정부통합조직 신설

현재 남한의 사이버안전을 위한 국가급 대비 체계는 『국가정보원법』 및 동법에 근거한 『정보 및 보안업무기획/조정규정』(대통령령 제16211호)에 정보보안 업무에 관한 기획/조정 업무를 국가정보원의 임무로 규정함에 따라 국가정보원이 국가 정보보안 업무 총괄기관으로서의 역할을 수행하고 있다. 또한 정부는 『국가 사이버안전관리규정』(대통령훈령 제141호)에 근거하여 '국가 사이버안전 전략회의' 및 '국가 사이버안전 대책회의'를 설치하고 민/관/군 대응체계를 구축하는 등 국가 사이버안전 관리체계를 설치 운영하고 있다.

그러나 2008년 2월 출범한 현 정부는 정보보안 관련 조직을 전면 개편하여 국방부 산하에는 최근 사이버사령부를 신설하고 민간분야 정보보호는 방송통신위원회, 행정안전부, 지식경제부 등으로 분산하여 관리하도록 개편한 바 있다. 방송통신위원회는 방송통신망 보호대책 수립, 침해사고 대응 등 방송통신 분야 정보 보호를 담당하고, 행정안전부는 개인정보보호, 전자서명 인증, 정보통신기반 보호 등의 업무를 담당하며, 지식경제부는 정보보호 관련 기술개발 등 산업 육성을 담당하게 되었다. 이에 따라 각 부처는 민간분야 정보보호에 대한 계획을 각각 수립하여 개별적으로 추진 중이며, 집행기구로서 국가정보원은 "국가사이버안전센터", 국방부는 산하에 "사이버사령부", 방송통신위원회는 산하 한국인터넷진흥원(KISA)에 설치된 "인터넷침해사고대응지원센터"를 설립하여 해당 분야 사이버안전 업무를 수행하고 있다. 이 외에 전문기관으로서는 국가보안기술연구소(NSRI), 한국인터넷진흥원, 한국전자통신연구원, 금융보안연구원 등이 설치 운영되고 있다.

이러한 남한의 사이버안전 관리체계는 구조적

으로 볼 때 분권형 관리체계로 운영되고 있다. 비록 국정원을 주무부처로 규정하고, 그 상위 개념으로 위원회 성격의 '국가사이버안전 전략회의' 및 '국가사이버안전 대책회의' 기구를 설치하고 있으나 각 부처 및 민간 섹터별로 거의 독자적인 권한과 운영을 하고 있는 실정인 바 국정원, 국방부, 방송통신위원회 등 분산된 분권형 구조를 가지고 있다. 이러한 분권형 사이버안전 관리체계는 다음과 같은 문제점으로 인해 유사시 치명적인 위기를 맞을 우려가 있다.

첫째로는 업무한계가 모호하여 적시의 위기관리가 어렵고, 서로 통제가 어려운 여러 기관들이 위기관리에 참여하다 보니 권한과 책임이 분산되는 동시에 중첩되고 있는 실정이다.

둘째로는 사이버안전 관리 주기(정책수립-준비-예방-대응-복구)를 통합적으로 관리할 수가 없어 공격의 사전예방보다는 언제나 공격당한 후 사후복구에 임할 수밖에 없는 한계점을 지니고 있다. 사이버 공격은 그 특성상 공공업무, 국방업무, 민간업무별로 나누어 발생하는 것이 아니라 경계가 없이 동시 다발성을 띄기 때문에 위기에 대한 통합적 대응기구가 필요하다.

셋째로는 자원의 중복 투자로 인한 비효율성이 대두되고 있다. 사이버공격 무기는 업무의 특성에 따라 달리 운용되는 기술이 아님에도 불구하고 각 부서별로 독립된 연구지원 조직이 구축되어 있어 유사한 업무에 중복 투자가 이루어짐으로서 예산의 낭비를 초래하고 있다.

따라서 전항에 분석한 여러 가지 문제점을 해소하기 위해서는 사이버 안전에 대하여 총괄적인 권한과 책임을 가진 독립된 중앙집권적 정부통합조직이 설치되어야 한다. 이 조직을 통해 정책수립-준비-예방-대응-복구를 통합적으로 관리하고 개별적인 관리주체와는 상시적으로 협조하고 모니터링하면서 대응할 필요가 있다.

4.2 전문인력 양성을 위한 특수대학 설립

사이버전을 대비한 특수대학이란 사이버전 전문인력을 국가에서 양성하여 사이버전에 대비하기 위한 인력양성 기관으로서 국가 인프라 및 정보체계를 보호하고 나아가 필요시 상대국의 국가 인프라 및 정보기반체계를 파괴 또는 마비시킬 수 있는 수준의 강력한 역량을 갖춘 전문 인력을 양성하기 위한 대학 수준의 교육기관을 말한다.

2010년 KISA가 발간한 '2010년도 국가정보보호백서'에 의하면 남한의 정보보호 산업에 종사하는 정보보호 인력을 전공별로 보면 정보보호학을 전공한 인력은 400명으로 집계되었고, 정보보호 관련학을 전공한 인력은 3,396명으로 조사되었다. 이 중에서 사이버전을 수행할 만한 수준의 특급 연구개발 인력은 불과 213명 수준으로 파악되고 있고, 나머지 인력은 관리직, 영업직 및 수준이 비교적 낮은 인원으로 파악되고 있다. 이러한 현황을 살펴 볼 때 현재의 남한의 정보보호 대응력은 매우 낮은 수준으로 평가되고 있다.

반면 북한의 사이버전 전문 인력 양상은 매우 체계적으로 수행되고 있는 바 소학교 졸업생 들 가운데에서 지능이 높은 학생들을 뽑아 중학교 컴퓨터 영재반에서 집중적으로 교육을 시키고 대학에 진학 후에는 저 수준의 어셈블리어, C언어에 의한 프로그램 작성을 최고의 수준에 도달 할 때까지 체계적으로 교육시키고 중국 유학 등 해외연수를 거쳐서 사이버전 전문 부대 또는 기관에 배치하고 있는 바, 엄격한 통제하에 최고수준의 목표에 도달할 때까지 이론과 실습을 반복하여 교육하는 것이 마치 사관학교와 같이 한다는 취지로 보면 될 것이다. 특히 북한의 전문 요원들은 순수한 프로그래밍적인 기법만을 배우는 것이 아니고 사회공학적 방법들에 대한 연구도 적극적으로 진행하고 있어 그 수준이 미국 CIA 수준을 능가할 것이라는 평가를 받고 있다. 또한 교육하여 인재를 양성하는데 그치지 않고 직장과 보직도 보장함

으로서 북한 정권에 충성심을 갖도록 하고 있다는 사실도 유념해야 할 것이다.

이러한 맥락에서 볼 때 남한도 이에 상응하는 조치로서 사이버전 사관학교를 설립하여 처음부터 공무원과 같은 신분으로 전문 교육을 체계적으로 실시하여 군장교 임관 및 정부주요 사이버전 담당요원이나 국가 인프라 시설에 배치하여야 할 것이다.

4.3 예산 증액 및 전문 인력관리 개선

2010년 KISA가 발간한 '국가정보보호백서'에 자료에 의하면 남한의 주요기관의 정보보호 예산이 2% 이하인 기관이 35.9%로 가장 많은 것으로 나타나고 있다. 또한 주요기관의 관계자들에 대한 설문조사에서 정보보호 업무수행의 애로사항으로는 기술인력 부족과 함께 예산부족 및 기관장의 인식부족으로 인한 소외감이 상위 그룹을 차지하고 있음이 파악되었다.

이러한 통계는 정부기관이나 주요 인프라 담당 기관장들이 정보보호에 대한 관심 부족으로 인해 예산 편성에서 소극적이거나 전문 인력에 대한 관심 부족으로 인해 조직편제상의 직위, 보직, 승진 등에서 전문 인력이 소외감을 받거나 불이익을 받아 업무에 매진하고 기술 개발에 노력을 쏟을 동기부여가 이루어지지 않을 개연성이 높다는 것을 의미한다.

또한 정보보호 전문 인력은 양성 못지않게 유사분야에서 장기 보직하여 관리를 하여야 할 것이다. 이를 위해서는 정부 각 부처 및 공공기관은 사이버전 전문 인력을 정보보호 전문분야에 장기 활용하도록 하기 위하여 해당 특기 실무부서 직위를 편제화하고, 주기적으로 전문성 계발 및 학문적 성과 접목 등을 위해서 각종 교육기관에서 보수교육을 받을 수 있도록 배려를 하여야한다. 이렇게 함으로써 전문교육과정에서 습득한 지식을 자신의 것으로 소화할 수 있는 기회를 갖게 됨은 물론 전문성 계발을 촉진하고 실무 보직 경험을 통하여 정보보호 전문 인력이 되었을 때 사이버테러 정보전에 대응할 수 있는 능력이 체득화 될 수 있을 것이다

또한 정보보호 전문 인력직위에 대하여 직무분석을 실시하여 적재적소의 배치가 이루어지도록 하여야 할 것이다. 예컨대 과거에 인력수급계획의 잘못으로 고급 정보보호 기술 교육을 이수하고도 적절한 직위소요가 없어 일반화 직위 또는 교육과 일치되지 않는 직위에 보임된 사례가 자주 발생한 사례가 있는데 이는 잠재역량을 최대로 발휘할 수 있는 보직 체계가 제대로 정립되어 있지 않았기 때문이다

그리고 정보보호 전문인력에 대한 적절한 승진과 금전적 보상이 보장되어야 한다. 자본주의 사회에서는 인간을 움직이는 힘의 원천 중에 하나가 승진과 금전적 보상이다. 따라서 아무리 정보보호 전문 인력의 활용을 위해서 제도적 장치가 잘 마련되어 있다 하더라도 적절한 보상이 주어지지 않는다면 자신의 잠재능력을 최대로 발휘하지 않음으로써 높은 성과를 기대할 수 없게 된다.

5. 결 론

남한에서 발생한 최초의 '전략적 사이버 기습공격 사건'은 2009년 7월 7일 발생한 청와대 등 국가 주요 핵심기관에 대한 동시다발적 DDoS 사이버공격이다. 이 공격으로 인해 잠시나마 청와대와 국가 주요 기관이 혼란에 빠진 일이 있었다. 이와 같은 사건은 앞으로 언제든지 반복 발생할 수 있으며, 우리는 이 사건으로 인해 만일 공격자가 국가 전복의 악의적인 의도를 가지고 본격적인 공격을 한다면 중대한 국가안보 위협이 초래 될 수 있다는 교훈을 얻은 바 있다.

그러나 'Stuxnet'급 '사이버 기습공격'이 발생한 현 시점에서 볼 때 과거 발생했던 DDoS 수준의 '사이버 기습공격'은 'Stuxnet'급에 비교해 볼 때

그 위협의 수준이 대포와 소총의 차이만 큼이나 크다는 것을 실감하게 되었다. 이제 어느 나라든 국가급 전문 기관이 'Stuxnet'과 같은 사이버공격 무기를 정교하게 개발하여 상대방의 주요 국가 인프라 시설에 공격한다면 마치 '크루즈 미사일'을 발사하는 것과 같은 효과를 볼 수 있기 때문에 향후 비대칭 무기로 충분히 고려 할 수 있는 가능성이 매우 높다고 볼 수 있다.

이런 관점에서 볼 때 향후 북한이 남한에 대해서 도발을 한다고 하면 인명살상과 가옥 파괴가 따르는 물리적 무기체계 수단 보다는 'Stuxnet'과 같은 사이버전 무기를 사용하여 남한의 발전소, 공항, 철도 등 기간 시설을 파괴하려 할 개연성이 매우 높다

따라서 이제는 사이버안전 위기관리 체계가 국가기관 조직의 일부 부서가 담당해야 할 업무가 아니라 국가안보의 차원에서 범국가적 차원에서 관심과 지원이 이루어져야 할 때가 되었다고 판단된다. 이러한 취지에서 본 논문에서는 1) 독립된 중앙집권적 정부통합조직 신설로 권한과 책임을 가지고 일체된 대응책을 수행하고, 2) 특수대학 설립으로 사이버전 전문인력 양성을 체계적으로 실시하여 최고의 인재를 확보하고, 3) 예산 증액 및 전문인력 관리체계를 개선하여 보직, 승진, 보상 등이 원활하게 이루어져서 애써 양성한 전문 인력이 사장되지 않는 체계를 확립할 것을 제안한다.

참 고 문 헌

[1] Davies, P. H. J, "Intelligence, Information Technology, and Information Warfare", Annual review of information science and technology, Vol. 36, 2002.

[2] FEMA, A Nation prepared Federal Emergency Management Agency Strategic Plan, 2001.

[3] George J. Stein, "Information Warfare", Airpower Journal(Spring), 1995.

[4] Libicki, Martin C., "Information Warfare : A Brief Guide to Defense Preparedness", Physics Today, Vol. 50, No. 9, 1997.

[5] KISA, 2010 국가정보보호 백서, 2010.

[6] 김종훈 외, "국가 주요기반 구조 보호를 위한 정보전 대응체계 연구", WISE 제99호, 1999.

[7] 이재은, "통합위기시스템의 통합방안", 한국위기관리논집, 제1권, 제2호, pp. 25-43, 2005.

[8] 한국정보보호센터, "정보전 대응체계 구축방안", 1999.

[9] 행정자치부, 국가위기관리시스템 구축방안, 2003.

[10] http://www.readwriteweb.com/archives/new_research_stuxnet_deigned_to_sabotage_irans_nu.php.

[11] http://citrain64.blog.me/100113833905.

[12] http://boanin.tistory.com/198.

[13] http://news.chosun.com/site/data/html_dir/2010/10/01/2010100100095.html.

[14] http://www.newshankuk.com/news/news.asp?articleno = t2010121712512619104.

[15] http://www.idg.co.kr/newscenter/common/newCommonView.do?newsId = 63319.

[16] http://www.naeil.com/News/economy/ViewNews.asp?nnum=586721&sid = E&tid = 6, http://www.ytn.co.kr/_ln/0101_201012031626264781.

권 문 택

육군사관학교 졸업(이학사)
경희대학교 경영대학원 졸업
(경영학 석사)
경희대학교 행정대학원 졸업
(행정학 석사)
미국 University of Iowa/Iowa city 대학원 졸업(공학석사)
미국 University of Wisconsin/Madison 박사과정 졸업(경영학 박사)
한국정보기술응용 학회 회장
한국지능정보시스템 학회 회장
한국사이버테러정보전 학회 부회장
경희대학교 정보지원처장
경희사이버대학교 초대 학장
현 경희대 테크노경영대학원 정교수