情 報 保 護 學 會 誌
第22卷 第8號, 2012. 12

국가사이버위협에 따른 국방사이버대응 실태

최 광 복*

요 약

북한은 사이버공간을 해방구로 보고 지난 2003년도에 인터넷 대란 공격을 실시한 이래 사이버 공격을 지속적이고 강력하게 감행하고 있다.[1] 지난해에는 농협전산망을 공격하였으며 최근에는 서해상에서 GPS교란 공격을 실시하여 인천 국제공항에 이착륙하는 항공기에 심각한 위협을 초래하기도 하였다. 이처럼 북한을 포함한 전 세계적인 사이버 공격이 이제는 국가안보상의 심대한 위협이 되고 있어 각국은 사이버전 대비에 심혈을 기울이고 있다.

이제 우리나라는 사이버공격을 가장 많이 받는 국가 중의 하나가 되고 있다. 국가적인 사이버위협이 지속되는 상황하에서 국방차원에서의 사이버대응 실태를 살펴보고 발전책을 제시하고자 한다.

Ⅰ. 서 론

최근 미국을 비롯한 세계 주요국들은 사이버전을 제5의 전장으로 규명하고 사이버전에 발 빠르게 대비하고 있다. 조직과 인력 그리고 기술개발은 물론이고 상대국에 대한 관련 정보 입수 및 보이지 않는 사이버전을 전개하고 있다.

사이버공격은 다른 공격행위와 비교해 볼 때 대단히 독특한 특징을 보이고 있다. 우선 공격을 위한 전력구축과 유지비용이 아주 저렴할 뿐 아니라 사이버공간의 특성으로 전투영역의 경계가 불분명하여 군사영역과 민간영역, 적군과 아군, 공격지점의 확인 등이 어려운 관계로 지금까지와는 완전히 다른 개념의 대비가 필요하다. 또한 전술적 경고나 평가가 어려워 사전 예방차원의 대응이 무엇보다 중요하다.[2]

과학기술이 발전하고 정보기술이 급속도로 발전하여 국방 분야의 많은 시스템들이 정보기술에 크게 의존하는 상황에서 사이버전의 피해는 예상보다 점차 커질 것으로 확실시 된다.이러한 특징들로 인해 사이버전을 핵무기처럼 비대칭 또는 전략적 군사력으로 운용하는 경향이 높아지고 있다.[3]

인터넷과 스마트폰이 우리의 생활 속에 깊이 자리잡고 있는 상황에서 우리와 대적하고 있는 북한은 이러한 사이버전의 이점을 십분 활용하여 집요한 사이버 공격을 지속하고 있고 그기술 또한 나날이 교묘해지고 있다. 국가차원에서 사이버공격에 대응하기 위한 다각적인 노력을 계속하고 있는 가운데 국가 안보를 책임지고 있는 국방부에서도 지난 2010년에 사이버사령부를 창설하여 운용하고 있는 등 다양한 대응책을 강구하고 있다.

Ⅱ. 국방 정보화 발전 개념

국방 사이버전 대응 실태를 알아보기에 앞서 우선적으로 국방부의 정보화 정책을 살펴보는 것이 사이버전 대응 실태를 이해하는 데 도움이 될 것으로 보여 국방정보화의 비전과 추진전략등을 확인하였다.

국방정보화의 비전은 `네트워크 중심으로 미래 전장 운영 개념 및 국방경영 효율화`에 두고 있으며 추진방향으로서 통합, 목표지향적인 정보화 추진,상호운용성 중심의 정보공유, 정보체계 활용성 향상,민관군 협력 발전을 설정하여 정보화를 추진해 나가고 있다.[4]

국방 정보화의 추진 전략은 정보우위의 네트워크 중심 작전환경을 구현하기위해 전장관리 정보체계를 구축하고 있는데 감시체계 및 타격 체계를 통합한 C4I중심의 복합체계를 발전시키고 있다. 또한 전투원, 무기체계. 감시정찰 체계 등의 전력요소를 통합 운용하고 있으며 정부 광대역 통신망(BCN)과 연계하여 차세대 정보통신망(NGN)을 구축해 나가고 있고 각급 부대별로 분

*세종대학교 컴퓨터공학과 교수 (choik125@naver.com)

산되어 있던 전산소를 2개의 국방 통합 정보관리소로 통합하여 운용하고 있다. 국방 정보화를 촉진하기위해 거버넌스 체계를 도입하여 체계적이고 전사적 차원의 국방 정보화를 추진해나가고 있다.

그동안 국방 정보화가 국방부만의 독자적 시스템으로서 외부에 철저히 폐쇄된 시스템으로 분산, 다원화 개념이었다면 앞으로는 통합, 목표지향적인 정보화로 발전을 추진해나갈 예정이며 또한 기능 체계단위의 정보처리에서 상호운용성 중심의 정보공유를 추구해나면서 민관군 협력개념으로 발전시켜나갈 예정이다. 추진전략으로는 5대 정보시스템인 전장관리 정보시스템, 자원관리 정보시스템,모델링 및 시뮬레이션,정보통신 네트워크,정보보안시스템을 발전시켜나가면서 4대 전략과제인 국방정보기술 아키텍처,국방클라우드 서비스, 상호운용성 및 표준화,소프트 인프라 웨어를 발전시켜나갈 방침이다.

국방 정보기반 시스템을 살펴보면 국가 정보시스템과 연동되어 운영하는 자원관리 정보시스템이 있으며 연합정보시스템과 연계하여 운용하고 있는 전장관리 정보시스템, 그리고 국방정보통신망등이 운용되고 있다.

이러한 국방정보시스템은 그 구성과 성격 면에서 대단히 특징적인 양상을 보이고 있다. 평시 국방관리 업무 시스템과 전장관리 영역 시스템이 동시에 운영되고 있으며 유, 무선 인프라와 2000여개의 복잡다양한 응용체계로 구성되어 있다. 또한 상용체계와 군용체계가 복합적으로 운영되고 있어 다양한 하드웨어와 소프트웨어 등으로 구성되어 있다. 전쟁이라는 특수한 임무를 수행하는 국방정보시스템의 특성상 전장지역에 대한 신속한 이동과 즉각적인 가용성, 확장성이 요구되고 있으며 견고성,생존성,이중화 요구등 전, 평시 정보체계의 중단없는 지원이 필요하다. 또한 정보의 정확성과 기밀성등이 필요한바 운용되는 정보에 대한 정보보증이 다른 분야보다 절대적으로 필요하다. 이러한 국방 정보화 기반 시스템의 특성을 감안시 고도의 정보보호태세 구축이 긴요하다.

그러나 이러한 국방 정보화가 발전하면 발전할수록 사이버 위협은 상대적으로 더 커질 가능성이 높아짐에 따라 국방 사이버 보안대책의 발전도 함께 이루어져야 할 것으로 보인다. 지금까지는 최우선적으로 국방 정보화가 이루어진 다음에 이어서 보안대책을 강구하는 수순으로 국방 정보화가 이루어져 왔으나 앞서서 언급하였듯이 북한을 포함한 주변국들의 사이버 위협이 24시간 가열차게 진행되는 현 상황을 직시하여 볼 때 국방 정보화를 계획하는 단계에서부터 사이버 보안대책을 함께 수립하고 시스템을 구축해나가는 노력이 절실하다고 본다.

Ⅲ. 국방 사이버 위협 대응실태

3.1. 국방사이버 위협 대응 체계 및 관제 시스템

사이버사령부에 위치한 국방 사이버 지휘통제센터에서는 국가 위기관리센터와 위기상황에 대한 정보를 실시간대로 상황을 공유하고 각군본부 및 작전사급 CERT, 국직부대 CERT와 각종 사이버 상황을 보고받고 있으며 필요시 경보를 전파하는 등 국방 사이버위협의 두뇌역할을 수행하고 있다.

관제는 자원관리체계와 전장관리체계로 이원화하여 관제하고 있는데 자원관리체계는 각급부대CERT에서 해당 시스템에 대한 관제를 하고 이러한 정보를 각군본부에서 통합관제하며 이를 다시 국방사이버 지휘통제센터에서 통합하여 관제를 하는 방식으로 이루어지고 있다.

전장관리체계는 자원관리체계에 비해 상대적으로 더 중요한 시스템이나 관제는 다소 미흡한 면이 있다. 우선 합참의 전장관리체계인 KJCCS와 해군의 전장관리체계인 KNCCS,공군의 전장관리체계인 AFCCS는 합참 및 해, 공군이 각각 관제체계를 구축하여 운영하고 있다. 육군의 전장관리체계인 ATCIS는 각급부대에서 관제를 실시하나 육군차원의 통합관제는 이루어지지 않고 있는 것으로 확인되었다. 각군의 전장관리 체계는 작전의 성격상 상호 연동되지 않고 각 군별로 운영되고 있으며 따라서 국방부 차원에서의 통합관제는 이루어지지 않고 있는데 이는 각관리체계가 독자적으로 구축되다보니 상호연결이 미흡하여 통합보안관리체계가 이루어지지 않은 것으로 보인다. 전장관리체계는 매우 중요한 시스템이기 때문에 통합적인 관제가 구축되어야 할 것으로 본다.

3.2. 국방 사이버 보안 인력 선발 및 교육실태

군내에 정보통신분야에서 근무하는 장병은 수만 명

에 이르고 있다. 대부분이 통신 병과이거나 전산 주특기 자로서 통신 분야와 컴퓨터 분야에서 근무하며 전투지원임무를 수행하고 있다. 그중에서 사이버보안을 전문으로 하는 장병 수는 소수에 불과하다. 이들은 대부분 사이버사령부나 기무사령부 및 군단급이상 부대의 CERT팀에서 근무하는 인원들이다. 과거 사이버 공격이나 사이버보안이 크게 중요시 되지 않았던 시절에 구성되었던 군 구조에 따른 인력 배정의 결과가 지금까지도 지속되고 있는 것이다.

국방사이버 보안 인력의 선발 및 교육실태를 확인해 보면, 장교의 경우 사이버전을 전담하는 병과나 주특기가 없고 전산 및 자격증 보유자중 자원에 의해 선발된 인원으로 사이버 보안을 담당하고 있다. 간부의 경우 고졸 또는 전문대 이상 자중에서 전산/통신/정보보호전공자를 선발하고 있으며 병사의 경우 육군과 공군은 정보보호병을 병무청에서 모집하고 있으나 해군의 경우 정보보호특기병이 없으며 전산 직렬로 모집 관리하고 있다.

교육은 각 군 정보통신학교의 교육과정에 포함하여 일부 실시하고 있으며 각 군별로 정보보호실무자반을 운영하고 있으며 기무사에는 초급, 중급, 고급반과정을 운영하고 있다.

그러나 정보보호가 고도의 기술을 바탕으로한 전문가를 필요로 하는 업무이고 군 전체의 전투력에 미치는 영향이 점차 높아지는 상황에서 지금보다 좀 더 체계적이고 조직적인 인원선발과 보직관리는 물론이고 필요시 정보보호병과 및 주특기를 신설하여 운용하고 고강도의 집중 교육이 필요할 것으로 예상된다.

3.3. 국방 사이버 방호 체계

국방 사이버 방호체계 구축개념은 우선 국방망과 전장망을 인터넷망과 물리적으로 완전히 분리하여 외부의 침입을 원천 차단하는 개념이다. 또한 네트워크의 기밀성, 체계 중요도를 고려하여 수준별 보호체계를 구축하는 개념으로 1차 방호로 네트워크보호,2차방호인 시스템 보호,3차 방호로 장병개인이 사용하고 있는 PC를 보호하는 개념으로 사이버 방호를 하고 있다.

그러나 지난해 4월에 발생하였던 농협 전산망 피해 사건에서 보았듯이 외부망과 물리적으로 완전 분리된 농협 전산망이 직원의 노트북 반출로 악성 코드가 메인 서버에 오염되어 금융 데이터가 사용불가능하게 된 것은 시사 하는 바가 크다.[5] 장병들의 USB사용 및 스마트폰 사용이 자연스런 일상사가 된 현시점에서 물리적으로 독립되었다고 하더라도 언제든지 내부망에 악성코드가 오렴될 가능성은 항시 열려있다고 보아야 할 것이다. 노트북과 이동저장매체에 대한 철저한 통제와 교육 및 내부 폐쇄망의 지속적인 관제가 필수적인 이유이다.

3.4. 관련 법규 및 훈령

국방사이버보안과 관련된 규정에는 군사보안업무훈령, 국방정보화 업무훈령, 정보작전 방호태세규정, 사이버 안전 국방분야 위기대응 실무 매뉴얼 등이 있다.

군은 이러한 훈령, 규정을 근간으로 국방 정보보호 조직과 임무, 정보체계 및 조직, 인력에 대한 보안 수준관리,사이버 위협에 대한 대응태세유지등 국방분야 정보보호 업무를 수행하고 있다.

우선 군사보안 업무 훈령은 군사시설보호법 제 10조 및 보안업무 규정시행규칙 제 69조에 의하여 군사보안업무의 시행에 대한 필요사항을 규정하고 있다.[6] 군사보안업무훈령은 1965년에 처음 제정되어 그동안 수차례의 전면 또는 부분 개정을 통하여 현재의 규정에 이르고 있다. 군사보안환경의 변화에 따른 내용 수정 및 보완사항이 대부분의 이유이었다.

그 구성은 총칙, 정신보안,문서보안,인원보안,시설보안,정보통신보안,보안측정,보안감사,사고조사,기타보안의 8개장과 48개절,216개조항으로 구성되어 있다. 이처럼 군사보안 업무 훈령은 각 보안 분야별로 상세하고 기술적인 사항까지 제시하고 있어 가히 군사보안의 총론이라고 말할 수 있으나 정보시스템에 대한 보안을 수시 진단하고 처리하기에는 다소 적용하기 어려운 점들이 많이 있다. 보안 진단목적보다 각 조직원들이 준수해야할 보안의무사항들을 규정하고 위반자에 대한 처벌을 목적으로한 규정으로 각급부대의 보안이 누설되지 않도록 하는 군사보안 지침서라고 볼 수 있겠다.

국방정보화 업무훈령은 2011년에 국방정보화 기반조성 및 국방정보자원관리에 관한 법률에 의해 정한 사항을 시행하기위한 업무 절차 및 기준을 마련하고 국방부 내에 산재된 기존의 정보화 관련 15개의 훈령, 지침, 지시를 통합하기 위하여 제정하였다.[7]

총 9장 42절 360조로 구성되어 있다. 그러나 국방정

보화 업무훈령이 15개나되는 각종 훈령 지침 등을 통합하여 제정되다보니 내용이 방대하고 정작 보안에 관한 부분은 6장으로 국한되어 있어 보안 실무자나 관련자가 보안진단 자료로 활용하기에는 미흡한 점이 다수 있는 것으로 확인되었다.

정보작전 방호태세 규정은 사이버 위협에 효과적으로 대비하기 위하여 2001년에 합참에서 제정되었다.[8)]

정보작전 방호태세 규정은 아군의 정보 및 정보체계에 대한 공격징후 또는 침해사고 발생 시 신속한 대응으로 피해를 최소화하기 위한 정보작전방호태세에 관한 사항을 명시하고 있다.

방호태세는 5단계로 구분되어 있는데 이는 국가 사이버 안전센터 및 인터넷 침해 대응센터에서 사이버 위협 대응 단계에 적용되는 정상, 관심, 주의, 경계, 심각 단계와 동일하다.

사이버안전 국방분야 위기대응 실무 매뉴얼은 국가위기관리기본 지침 및 사이버 안전 분야 위기관리 표준매뉴얼에 근거하여 국방부에서 제정하였다. 사이버 위기 경보에 대한 판단기준과 피해 상황,조치사항등을 상세하게 설명하고 있다.[9)]

정보작전방호태세 규정이 제반 사이버 위협 대응 단계를 규정하고 있다면 사이버안전 국방분야 위기대응 실무 매뉴얼은 제반 위협 단계를 판단하기위한 징후와 상세 대응 지침을 기술하고 있다고 할 수 있다.

3.5. 국방사이버보안정책의 미래 발전 계획

국방부에서는 2012년을 정보보호 기반이 조성되는 해로 정하여 국방부 및 예하부대의 정보보호 수행 조직을 보강하고 사이버전을 수행하기위한 기본정책을 수립하고 민관군 대응체계를 구축하는 등 다중 방호체계를 마련하는 것으로 다양한 사업을 추진하고 있다.

2015년에는 정보보호기반 확충을 목표로, 2020에는 정보보호 대응 능력을 확보하는 것을 목표로 계획을 발전시켜 나가고 있다. 물론 예상되는 목표이기는 하나 작금의 사이버 공격의 횟수나 강도,IT발전 속도 등을 고려하여 보았을 때 국방 사이버전 대응 속도를 보다 빠르게 그리고 적극적으로 수행해나가야 할 것으로 본다.[10)]

Ⅳ. 발전방향

사이버사령부가 창설되었고 계속적으로 인원을 증원하고 기술력을 보강하는 등 사이버전 대응능력을 확충해나가고 있는 것으로 알고 있다. 몇 년 전에 비해 사이버테러 및 사이버 공격 횟수가 기하급수적으로 증가하고 있으며 온 국민이 인터넷과 스마트폰을 생필품으로 사용하고 있는 시대가 되었다.

또한 사이버 공격의 위협과 피해가 확대되고 있고 앞으로 더욱 그 정도는 커질 것이다.

따라서 이러한 위협을 적극적으로 차단하고 대응체계를 완비하기위해서는 전문 인력을 확보하고 관련 교육을 강화하는 것이 가장 중요하다고 본다.

대학교에서 정보보호를 전문으로한 유능한 인재가 군 입대 시 사이버전사로 복무할 수 있도록하는 정책을 마련해주어야 할 것으로 본다.

또한 군에 사이버 병과를 창설하여 능력 있는 사이버 인재를 선발, 교육, 관리하는 체계를 구축하여야 한다. 육군, 해군, 공군, 해병대에 이어 제 5군으로 사이버군을 창설하여 전문화 관리하는 것이 사이버위협에 대응하는 지름길이라고 본다. 현재 통신 및 전산분야에 근무하는 인력을 사이버전 전문인력으로 전환하여 활용하는 방안도 고려해 볼 가치가 있다.

관련 규정과 방침에 대한 심도 깊은 검토도 필요하다. 복잡다양하고 유사한 관련 규정을 신속한 사이버 대응이 가능한 규정으로 정리하고 통합할 필요가 있다. 현재의 규정들이 부대의 기밀을 지키기 위한 지키는 보안에 중점을 둔 규정들인데 여기에 사이버전에 대비한 규정이나 현재의 시스템을 24시간 감시하고 사이버공격징후에 대한 적극적인 대응이 가능한 진단 체계로 보완시켜 나가야 하겠다. 다른 분야와 확연히 구분되는 국방시스템의 특성을 고려하여 국방사이버시스템을 진단하고 취약점을 쉽게 도출 해낼 수 있는 특화된 국방정보보호관리 시스템(Defence-ISMS,D-ISMS)[11)]을 도입해야 할 시점이라고 본다.

Ⅵ. 결 론

사이버전에 대응하는 시스템들은 대부분이 고도의 IT기술이 접목되거나 최신의 기술이 접목된 가장 현대화된 장비들이다. 그리고 이러한 장비나 프로그램들은

계속적으로 진화하여 발전을 거듭하기 때문에 사용기간이 짧은 관계로 많은 예산과 관심이 필요하다. 불확실한 먼 미래에 대해 정밀한 계획을 수립하기보다 현재의 사이버 위협을 적극적으로 대응할 수 있는 발빠른 계획과 그 계획을 실행할수 있는 적극적인 관심과 예산 지원이 중요하다.

참고문헌

[1] 국민일보, 「총 대신 마우스... 中 '사이버 사령부' 창설」 2010년 7월 22일.

[2] 엄정호, 최성수와 정태명, 「*사이버전 개론*」 ,홍릉과학출판사, 서울, pp.25-27, 2012.

[3] 중앙일보, 「"사이버 공격이 핵보다 효율적", 중국 '100만 홍커' 출격 대기」 2009년 7월 11일.

[4] 국방부, 「*국방 사이버위협 대응정책*」 2012년 9월 13일.

[5] 서울중앙지방검찰청, 「농협 전산망 장애사건 수사결과」 ,2011년.

[6] 국방부, 「*군사보안업무훈령*」 2010년 9월.

[7] 국방부, 「*국방정보화업무훈령*」 2011년 2월.

[8] 합동참모본부, 「정보작전방호태세 규정」 2010년 7월.

[9] 국방부 , 「*사이버안전 국방분야 위기대응 실무매뉴얼*」 2006년 12월.

[10] 국방부, 「*국방 사이버위협 대응정책*」 2012년 9월 13일.

[11] 디지털데일리, 「"사이버전 대응, 국방 보안관리모델(D-ISMS) 개발 필요"」 2011년 11월 17일.

〈著者紹介〉

최 광 복 (Kwangbok Choi)
정회원

1980년 2월 : 육군사관학교 졸업
2005년 8월 : 경남대학교 정치학 박사
2012년 8월 : 수원대학교 컴퓨터학 박사
자격증 : CISA, CISSP
<관심분야> 네트워크 보안, ISMS, IT 거버넌스, IT 감사, 위험관리