유비쿼터스 환경에서의 NCW 정보보호 대책

권 문 택*

요 약

본 연구는 유비쿼터스 환경에서 네트워크 중심전(NCW)을 원활하게 실시하기 위해 필요한 정보보호 대책을 제시하기 위한 것이다. 대책을 도출하기 위해 우선 유비쿼터스 환경에서 NCW가 구현 되었을 때 예상되는 전투양상을 전장기능별로 조명해보고, 유비쿼터스 환경에서 일어날 수 있는 정보보호 위협의 특징을 도출하였다. 이러한 특징을 바탕으로 위협을 해결하기 위한 국방정보보호 대응 방안을 제시하였다. 본 연구에서 제시한 대응방안을 바탕으로 추후 세부 실행과제를 도출한다면 보다 완벽한 NCW 개념 실현을 위한 국방정보보호 대책이 마련될 수 있을 것이다.

A Study on the Network Centric Warfare Information Security for Ubiquitous Network Computing Environment

Moon Taek Kwon*

ABSTRACT

Information security is a critical issue for network centric warfare(NCW). This paper provides defense information security guidelines for NCW, especially for ubiquitous network computing environment. For this purpose, this paper identified changes of battle aspect of tactical level and characteristics of information threats, and finally, the research suggested several information security guidelines for NCW. This paper is to intended to help military organization's planners determine practical and implemental plans in the near future.

Key words : Network Centric Warfare, Ubiquitous, Information Security

접수일 : 2010년 7월 5일; 채택일 : 2010년 9월 13일

* 경희대학교 테크노경영대학원

1. 서 론

NCW(NCW : Network Centric Warfare, 네트워크중심전)는 “네트워크 시스템을 통해 전투공간 내의 모든 전투원에게 정보공유 능력을 제공하고, 전투공간에 대한 공통상황인식과 동시 의사결정력을 제고함으로서 정보우위를 달성하고 전투력의 상승효과를 유발하도록 하는 정보기술 기반의 전쟁”이라고 그 개념을 정리할 수 있다. 따라서 유비쿼터스 네트워킹은 NCW 전략 개념을 수행하기 위해서 의심할 나위가 없는 정보통신 인프라이다. 즉, 이제 단순 인터넷 시대에서 센서 네트워크 및 Add-hoc 네트워크로 대표되는 유비쿼터스 인프라 시대가 국방전보통신망으로 대체되어야 할 것이다. 이렇게 되면 이제 머지않아 유비쿼터스 네트워킹을 통해 음성과 데이터, 그리고 멀티미디어 서비스 등을 시간과 장소에 구애 받지 않고 제공 받을 수 있는 환경이 구축될 것이며, 이를 통해 이른바 NCW 전략 개념이 수행 될 것으로 기대되고 있다.

NCW 전략 개념의 핵심은 정확한 표적정보 획득 및 정보의 공유를 통해 다양한 전투 기능을 연결 및 통합하여 지리적으로 분산된 전력을 효율적으로 운용하는 것이다. 그러나 이러한 요구사항이 원활하게 지원되기 위해서는 무엇보다도 전술제대의 제 기능과 연계된 네트워크 시스템을 구성하고 있는 컴퓨터와 통신망에 대한 정보보호체계의 구축이 시급이 요구되고 있다.

더욱이 최근의 추세는 기존의 네트워크 개념이 유비쿼터스 네트워킹 시대로 진화하면서 고정/이동, 유선/무선이 결합환 모바일 특성이 가미되어 대형 범용 컴퓨터나 PC, 휴대폰, 스마트폰, 스마트패드, 네비케이션, 카메라, 물체에 부착한 전자태그 등 각종 정보기기나 센서가 연결된 상태로 운영되는 모바일 컴퓨팅 상황에 이르고 있어 정보보호의 필요성이 더욱 증대되고 있다.

본 연구는 이러한 상황 인식하에 유비쿼터스 환경에서의 NCW 전략 개념이 육군 전술제대급 전장기능 활동에 어떤 변화를 일으키는가를 분석하고 이에 대한 정보보호 취약점을 도출한 후에 이를 극복하기 위한 대책을 제언하고자 한다.

2. 육군 전술제대 전장기능과 전투 양상의 변화

2.1 육군 전술제대와 전장기능

육군의 전술제대는 적과 직접적인 지상 전투를 수행하여 승리를 획득하기 위한 전투행위를 수행하는 군단급 이하의 부대를 말한다. 육군에서 사용하는 야전교범에서는 전술제대는 주 임무가 전투와 교전이며, 이를 수행하는 제대는 군단 및 사단급 이하 제대로 규정하고 있다. 또한 전술제대의 주요 전장기능은 정보, 기동, 화력, 방호, 전투근무지원, 지휘통제 6개 분야를 지정하고 있다.

정보기능은 제반 첩보 및 정보를 적시에 제공함으로서 적에 대해 정보 우위를 달성함으로서 효율적인 전투력을 보장하는 기능을 수행한다. 이를 위해 정보기능을 수행하는 부대 또는 부서는 다양한 감시 및 정찰 수단을 통합 운용하여 적보다 먼저 보고, 적의 오판을 유도하기 위한 정보작전을 수행한다.

기동기능은 부대이동 및 배치를 통해 아군에게 유리한 지형 여건을 조성하고 적의 활동을 방해하는 기능을 수행한다. 이를 통하여 적에게 불리한 지형이나 배치를 강요하고 작전의 속도와 템포를 적절히 배합하여 결정적 시간과 장소에서 상대적 전투력의 우위를 달성한다.

화력기능은 적의 심장부를 파괴하기 위해 화력을 집중할 수 있도록 화력 우세를 달성하고 기동부대의 기동이 원활하도록 여건을 조성하는 역할을 수행한다.

방호기능은 생존성을 증대시키고 기습을 방지하며 행동의 자유를 보장하여 전투원의 심리적인 안

정을 증대시키는 기능이며, 작전 보안 활동, 국지 경계 등을 통하여 생존성을 증대시키고 전투역량을 보존하게 한다.

전투근무지원 기능은 제반자원 및 근무를 제공하여 작전 지속능력을 유지하고 무형전력 발휘에 기여하는 기능으로서 작전에 필요한 제반자원을 제공하여 요구되는 적정 전투력을 유지시키고 작전 수행 간 지속적인 전투력의 복원을 지원하여 작전 지속능력을 보장하게 한다.

지휘통제기능은 지휘관이 작전을 지휘하고 제 전장기능과 작전요소를 통합하여 의사소통을 가능하게 하는 기능으로서 전장기능의 제요소들과 작전기능을 유기적으로 협조, 조정, 통합함으로서 전투력 발휘를 극대화 한다.

2.2 NCW 환경에서의 전투양상 변화

2.2.1 정보기능에서의 변화

전술제대에서의 정보기능 주 역할은 정보의 수집과 전파이다. 유비쿼터스 시대의 전장 정보기능 수단으로 활용되는 UAV, 적외선카메라 등에는 스마트먼지 등 다양한 형태의 센서가 장착될 것이며, 이러한 센서들은 현재 가시영역내의 전장정보를 위성 또는 고지 중계소를 통해 전달하고, 수작업을 통해 정보화 되는 과정을 사전 내장된 통신기능을 이용해 Ad-hoc 네트워크로 연결됨으로써 센서가 원거리에 위치하더라도 쉽게 정보를 지휘소까지 전달하고, 또 탐지와 동시에 내장된 애플리케이션을 통해 의미 있는 정보로 가공한 뒤 별도의 처리과정이나 중간 제대를 경유하지 않고도 직접 전송함으로써, 정보를 필요로 하는 요구자에게 신속히 제공되므로 적시성을 보장할 것이다[7].

특히, 위험도가 높은 적지종심작전 투입병력의 소요를 센서형의 전자매개물이 대신함으로써 아군의 위험노출 수준을 대폭 낮추게 될 것이다. 또한 적 접근로에 살포해 놓은 접착식 스마트 먼지를 이용한다면 적의 접근상황을 실시간으로 파악할 수 있고, 유비쿼터스 센서가 내장된 트로이 목마형 디코이를 적에게 고의로 제공하다면 적이 정보 분석을 위해 사용하는 위치가 식별되므로 적 접결지 또는 지휘소 위치를 파악해 낼 수도 있을 것이다.

이러한 체계는 연속적으로 자동화된 적 접근징후 분석과 조기 경보를 통해 아군의 화력 및 기동자산이 효과적으로 운용 될 수 있도록 할 수 있을 것이다.

2.2.2 화력기능에서의 변화

화력분야에 있어서 지상화력 운용의 경우 타격을 위한 표적정보의 획득은 정보에서 제시되고, 타격수행간 타격제원 산출은 텔레매틱스를 기반으로 한 표적정보와 자신의 공간정보 및 기상제원, 장비에 내장된 누적 장비 마모 특성, 공산 오차율 등이 결합되어 사격제원 산출이 자동으로 이루어지므로 최상의 수준을 유지한 상태에서 오로지 타격 결심만이 필요한 자동 사격체계를 함정이나 항공기 등에 비해 상대적으로 불안정한 환경인 지상부대 전장기반에서도 적용 가능토록 할 것이다[7].

또한 각 화기별 RFID가 부착된 단위 포탄을 사용하게 됨에 따라 일정수준 이하의 포탄을 보유하게 되면 전투 간에도 자동 경보를 제공하고 센서네트워크를 통해서 탄약보급소에 전달됨으로써 위치 정보와 탄약보유 수준의 원격파악에 의한 최적의 재보급 시기와 방법 및 소요량을 자동 결정하는 탄약 자동 보급체계를 구성하게 될 것인바 별도의 검토 및 분석과정 없이도 자동 출력된 지시서에 의해 연속적인 탄약 재보급에 의한 지속타격능력들 제공할 것이다.

타격 후 피해결과 판단(BDA : Battle Damage Assessment)은 현재까지 위성영상이나 공중정찰 자산이 제한되어 주로 육안식별을 통해 이루어져 왔으나, 유비쿼터스 전장체계에서는 개별포탄 또는 독립적으로 투발되는 센서에 의해 결과가 수집되어 네트워크를 통해 사격부대 및 지휘소에 동시전달 됨으로써 재 사격 또는 추가사격 여부를 신속히 결정토록 할 수 있을 것이다.

2.2.3 기동기능에서의 변화

기동분야에 있어서는 보다 다양한 적용이 예상된다. 현재 근거리에서 구두문답 수준에 머물고 있는 피아 식별은 함정이나 항공기에 적용된 IFF(피아 식별장치)와 유사한 개념의 자동식별로 대체되고, 유비쿼터스 네트워크를 통하여 연결된 후 디지털 전사의 고글형 디스플레이를 통해 자동식별을 제공할 것이다[7].

전술 C4I의 일환으로 적용이 진행 중인 전장 위치보고체계는 현재 일부부대의 위치 확인 수준으로 이루어지나 디지털 병사가 착용한 장비에 의해 자동적으로 네트워크 구성 및 전송이 이루어짐에 따라 모든 병사의 위치, 기동방향을 제공하고 디지털 지도에 표시하여 개인 차원으로까지 확대될 것이고, 신속한 전투 진행 및 기동속도의 가속화에도 불구하고 낙오자 발생을 최소화 할 것이며, 개별 병사의 낙오여부를 식별 할 수 있을 것이다.

지뢰는 오타와 협약에 따라 사용이 감소되는 추세이기는 하나, 지속 사용된다는 전제 하에서 개별 지뢰에는 스마트 먼지와 유사한 형태의 네트워크 트리거가 내장되어 원격조정 지뢰지대를 구성하고, 교전이 종료된 후에는 우군 및 민간인의 피해를 줄이기 위해 자폭 처리토록 하거나 후속부대에 위치 정보를 제공함으로써 차후 제거가 용이하도록 할 것이다. 이러한 원격 장애물 체계는 지뢰뿐만 아니라 교량 터널의 거부에도 효과적으로 설치 될 수 있을 것이다.

2.2.4 방호기능에서의 변화

방호분야에서는 전장 주요지점, 기동장비, 지휘소 주변에 설치된 다수의 화학 탐지수단은 자동으로 위험 여부 및 반경을 아군요소에 경보하여 피해를 예방하고, 신속한 제독조 투입을 지시하게 할 것이다.

적 항공기에 대한 대공경보 또한 신속히 개인에게 까지 전파되어 피해를 최소화하고, 개별 대공무기체계에 정착된 소형 디스플레이어를 통하여 사격제원 및 시기를 제공하여 국지방공의 효과적인 운용을 가능토록 할 것이다[7].

지휘소에는 Ad-hoc 방식의 센서들이 외곽을 연하여 설치되고, 주요 핵심 시설에는 휴대용 피아식별장치가 매치되어 형상 또는 열감지 등을 통해 1차적인 인원의 접근을 식별하고, 우군 고육의 RFID 신호를 제공하지 못할 경우에는 위치 및 경보를 제공하여 적 특수 작전부대의 침투 시 조기포착 및 타격토록 하여 안정된 지휘소 운용이 가능토록 할 것이다.

2.2.5 전투근무지원기능에서의 변화

전투근무지원은 분야에서는 이라크 전쟁 사례에서 이미 보여 주듯이 모든 기동장비, 파렛트, 컨테이너 등에는 RFID가 부착되어 보급품의 현황과 이동 상황을 실시간 식별 가능토록하고, 디지털 병사의 옷에 부착된 센서는 각각의 병사의 체온, 맥박, 혈압 등 신체상황 감지하여 부상여부 및 부상정도를 지휘소로 전달함으로써 종합된 부대 전투력 수준 및 작전 한계점 달성여부를 판단하는 자료로서 뿐만 아니라, 피해 정도에 따라 구호반 및 대량 사상자 처리반의 투입 여부에 대한 지침을 자동으로 제공할 것이다[7].

특히, 전투근무지원 분야는 RFID의 국방 분야 시범적용이 탄약관리분야인 점에서 증명하듯이 국방분야 중 유비쿼터스화가 우선적으로 적용되어 전장 환경에서도 조기에 효과를 발휘하게 될 것이다.

2.2.6 지휘통제 기능에서의 변화

육군은 전술제대에서 지휘소를 중심으로 제반 전장기능을 통합하여 상황판단과 지휘결심을 하고 화력 통제를 한다. 이를 위해서는 제 전장기능에 연결된 다양한 통신망을 유지하게 되는데 이것이 향후에는 유비쿼터스화를 통해 여러 네트워크가 통합되고 BcN으로 전환될 것이다.

본래 전술제대에서 기동을 하면서 지휘소를 이동하게 되는데 이 때 지휘소 이동 간 지휘통제의 지속적인 유지가 대단히 어려운 과업이고 또한 이것이 잘 못 수행되었을 경우에는 작전수행중에 상황에 따라 신속한 부대의 재 배치 등의 전술적 변화에 치명적인 악 영향을 미치게 된다. 그러나 NCW 상황에서는 격자형 네트워크가 확보되어 시간과 장소의 제한없이 통신이 이루어져서 지휘소 이동은 더 이상 필요하지 않거나 매우 줄어들게 될 것이다. 왜냐하면 유비쿼터스 컴퓨팅 환경에서는 IPv6 구조하의 Ad-hoc 네트워크가 구축 될 것이고, 이는 기본적으로 이동성을 보장하는 시스템으로서 상·하급 부대 뿐만 아니라 지휘관과 참모가 공간적으로 분리되어 있거나, 심지어는 이동 상황 속에서도 전체적인 지취통제 기능은 중단 없이 운용될 수 있기 때문이다[7].

또한 유비쿼터스 NCW 시스템이 구축되면 개별장비와 주요 공간에 설치된 무인 센서에 의해 수집된 정보가 즉각적으로 지휘통제센터에 제공되어 전투수행시 의사결정이 신속히 이루어 질 것이며, 이러한 지속적인 전투수행 과정에서 먼저보고, 먼저결심하고, 먼저 타격하는 형태의 작전템포가 축소되어 전승의 기반을 제공 할 수 있을 것이다. 아울러 유비쿼터스 환경에서는 진행 중인 상·하·인접부대의 모든 상황을 실시간으로 파악하여 상급 지휘관과 동일한 수준의 정보를 제공 받을 수 있으므로, 예하부대 지휘관들에 대한 권한 위임 및 분권화 작전은 더욱 그 효력을 발휘 할 수 있을 것이다.

3. 유비쿼터스 환경에서의 NCW 정보보호 위협의 특징과 대책

3.1 정보보호 위협의 특징

정보화의 진전, IT와 타 산업의 융합 등에 의한 유비쿼터스 사회로 발전하면서 네트워크 패러다임도 BcN, USN 등 인프라가 고도화 되고, RFID, LBS, 스마트카드 등 새로운 u-IT 기술로 인해 과거보다 정보의 수집, 전송, 통합이 한층 용이해 질 것이다.

특히 국방 전투장비들에 이질적 장비들이 컴퓨터 기능을 내장하고 상호 네트워크로 연결되면서 정보보호의 주 대상이 과거에는 시스템과 네트워크 중심이었으나 유비쿼터스 헌경에서의 NCW에서는 정보보호 대상이 개별 장비들로 확대 될 것이다. 예를 들면 지능형 로봇, 무인 정찰기 등 각종 지능형 장비들은 자체 운영체제 및 네트워킹 기능을 소유하고 상황인식, 위치기반 정보제공, 자기고장치료 등 지능기반 기능을 확보하고 있을 것이며 이에 대한 적절한 정보보호 대책이 요구된다. 이러한 사실을 바탕으로 유비쿼터스 환경에서의 NCW 정보보호 특징을 요약한다면 다음과 같다.

첫째, 전술제대에서의 전투 기능 수행에 있어서 군 전투원들이 다양한 신규 u-IT 서비스를 연속적으로 불편없이 사용하기 위해서는 정보보호 속성이 기존 정보보호의 핵심인 기밀성, 무결성, 가용성 보장에서 신뢰성과 개별 장비의 위치보호 등으로 확대되어야 할 것이다.

둘째, 유비쿼터스 환경에서는 네트워크의 규모 및 복잡도가 전투상황에 따라 변화하고 이동성이 증가하면서 과거 'Static' 정보보호에서 주변상황을 인지하여 그에 적합한 서비스를 제공하는 'Conformable' 정보보호가 필요한 상황이 전개 될 것이다.

셋째, 유비쿼터스 환경에서는 정보보호 위협으로 인한 피해 및 손실이 기존의 정보화 환경에서보다 한층 심화되고, 피해 복구도 이전보다 훨씬 어려울 것이 예상된다. 특히 유비쿼터스 인프라는 항만, 전력, 교통망 등 사회의 인프라와 밀접히 연계되어 있어 정보보호의 불비로 인한 피해가 한층 복잡하게 얽혀있고 규모도 클 것이다. 이러한 몇 개의 특징을 살펴 볼 때 이에 대한 포괄적 대책은 다음과 같이 도출 해 볼 수 있다.

3.2 유비쿼터스 환경에서의 NCW 정보보호 대책

지금까지의 국방정보보호 기술은 인터넷 망에 대한 유선 네트워크 보안 기술이 중요하게 고려되었다. 그러나 향후에는 무선 액세스를 기반으로 하는 센서 네트워크에 대한 요구가 늘어나게 될 것이며, 무선 통신 단말과 사용자에 대한 확인 절차와 보호가 필요하게 되고, 기존의 인터넷 인프라 보호에 더하여 네트워크의 운영성과 안정성, 그리고 신뢰성까지 정보보호의 영역이 확대됨으로서 네트워크 보호 대상과 기술의 수준도 한층 복잡하게 되었다. 따라서 이에 대한 대응방향을 요약한다면 다음과 같이 정리 할 수 있다.

첫째, 유비쿼터스 환경에서 요구되는 국방정보시스템에 대한 보안 서비스를 만족하기 위해서는 네트워크 보안 개념에 대한 확장과 명확한 정의가 필요하다. 이를 실현하기 위한 네트워크 보안 기능도 시스템 레벨, 네트워크 레벨, 제어 레벨 등으로 역할을 할당하고 이들이 유기적으로 엮어진 개념으로 네트워크 보안을 정의하는 것이 필요하다.

유비쿼터스 환경에서의 네트워크의 개념은 단순히 라우터와 스위치 등의 통신 시스템의 집합만으로 정의하여 네트워크 보안장비, 트래픽 조절 장비 등에 비중을 두던 것에서 더 나아가 유비쿼터스 네트워크 장비들로 확대하고 이들을 제어하고, 관리하는 기능 등을 포함하는 전체적인 수준으로 확대되어야 할 것이다. 따라서 데이터 보호, 장비 보호 등을 담당하는 시스템 레벨 뿐만 아니라, 트래픽 조절, 경로 보호, 네트워크 신뢰성 보장 기술, 통합보안관리 기술 등이 포함된 종합적인 기능으로서, 이들 시스템 들이 유기적으로 엮어지는 개념으로 정의 할 필요가 있다.

둘째, 유비쿼터스 환경에서는 네트워크가 진화 및 발전함에 따른 취약점이 점차 확대되고 이들 취약점간의 연관성과 연계성이 높아지고 있으므로 네트워크를 보호하기 위한 융합 보안 기술의 개발과 네트워크 보안 프레임워크 정립이 필요하다. 보안 프레임워크에는 네트워크 장비에 대한 보호, 통신 경로에 대한 보호, 관리 기능에 대한 보호, 나아가 네트워크 제어 절차에 대한 검증까지 포함된다.

셋째, BcN 통합안전관리 대책을 수립하고 시행해야 한다. 이를 위해서는 1) 소부대에까지 보급될 지능형 휴대 단말기기의 보급증가에 따라 증가할 신종 웜 및 바이러스 출현에 따른 피해 방지를 위해서 차세대 웜 및 바이러스 예방대책이 필요하고, 2) 소부대 단말기기에 대한 바이러스 확산 방지를 위한 보안 API가 마련되어야하며, 정보유출 등 바이러스로 인한 피해 방지를 위한 기능 검토가 요망되며, 3) BcN 환경의 이상 징후 수집 및 분석, 침해사고 진단 및 예측, 실시간 침해사고 대응을 위한 조기 예/경보 시스템을 개발 할 필요가 있고, 4) BcN 일부 서비스의 장애나 침해사고가 발생 할 경우에 이것이 전체망으로 확산되는 것을 방지하기 위해서 침해사고 격리 메카니즘을 개발하되, 장애발생시 분리가 용이하도록 네트워크별, 제대별 등 그룹별 IPv6 주소 할당체계를 수립해야 할 것이다.

넷째, 무인 지능형 장비(UAV, 지능형 로봇 등)에 대한 정보보호체계를 구축해야한다. 국방부는 향후 10년 이내에 UAV나 지능형 로봇 도우미를 활용하여 전선에서 정보를 수집하고 신속히 전파하여 먼저보고, 먼저 결심하는 체계를 확립하고자 계획을 수립 추진하고 있다. 이러한 계획을 원활하게 추진하고 실제 효과를 발휘하기 위해서는 이 장비들에 대한 정보보호 시스템을 개발하여 장착해야 한다. 이를 위해서는 이들 장비들과 광대혁 네트워크, 지능형 정보관리 서버, 컨텐츠 서버 등 전체 구성요소 및 데이터 경로에 대한 취약점, 위협 분석을 통한 정보보호 프레임워크가 개발 되어야 한다. 여기에 더하여 이들 단말기들의 오작동 및 전자적 침해 사고 피해 최소화를 위한 안전성 평가 방안도 마련해야 할 것이다.

다섯째, 유비쿼터스 환경에 적합한 인증체계를 정립 하여야 한다. 유비쿼터스 환경에서는 다양한 기기와 사물이 국방네트워크에 연결되어 통신주체

로 등장하고 전술상황에 따라 운용되게 된다. 따라서 인증체계의 정립이 매우 중요하다. 지금까지의 인터넷 환경에서는 신원 확인 정도의 인증에 중점을 두었으나 센서, 정보장치, RFID 태그 등 신종 유비쿼터스 장비들에 대한 신뢰성 있는 식별 방법이 부재한 상태이다. 적절한 인증 기능을 갖추지 못한 RFID 등 단말장치들은 주변에 산재한 태그를 통해 전투원이 인식하지 못하는 사이 위치정보, 이동상황 정보 등 민감한 정보의 유출 위협이 증가할 것이다. 여기에서 유념할 것은 ID 도용을 통해 접근 권한을 획득한 적은 이 권한을 이용하여 유비쿼터스 환경이 제공하는 국방 NCW 지휘통제 중심부에 접근이 가능하다는 것이다.

4. 결론 및 제언

네트워크 중심전(NCW)은 전투공간내의 모든 전투원에게 정보공유 능력을 제공하고, 전투공간에 대한 공통상황인식과 동시의사결정력을 제고함으로서 정보우위를 달성하고 전투력의 상승효과를 유발하도록 하는 정보기술 기반의 전쟁개념이다.

이러한 개념은 원활하게 구현하기 위해서는 무엇보다 네트워크 시스템을 구성하고 있는 컴퓨터와 통신망에 대한 정보보호체계의 구축이 시급이 요구되고 있다. 국방부는 이러한 상황 인식하에 최근 수년간 네트워크 공간에서의 정보보호를 위하여 관련 기술 및 정책에 대해 많은 연구와 노력을 기울여 왔다. 그러나 최근에 이슈가 되고 있는 것은 NCW 환경이 점차 유비쿼터스화 되어가고 있다는 것이다. 무인 센서, UAV 증 다양한 지능형 장비들이 네트워크와 연결되고, 최 말단 부대 전투원까지 보급되는 정보 단말기는 모바일로 운용되면서 작전 상황에 따라 수시 이동을 하면서 즉시적인 상호 운영성을 보장해야 되는 환경으로 바뀌고 있다. 따라서 여기에서 가장 큰 문제점으로 대두되는 것은 이러한 모바일 유비쿼터스 환경에서의 NCW 개념을 원활하게 구현할 수 있는 국방정보보호체계 구축이라고 할 수 있다.

본 연구는 이러한 문제점을 해결하기 위하여 국방 정보체계 분야에 다년 간 근무했던 경험을 바탕으로 유비쿼터스 환경에서의 NCW 정보보호 대책을 마련하기 위한 방안을 제시였다. 본 연구는 이러한 대책을 제시하기 위하여 우선 유비쿼터스 환경에서의 전투양상 변화와 정보위협의 특징을 살펴보았고, 이러한 변화에 부응하는 대응 방향을 제시하였다.

본 연구에서의 미진한 부분은 상기 대응방향에 대한 세부적인 추진 과제를 추가적으로 발굴하여 국방실무자들에게 실질적인 참조사항을 제시하지 못한 것인바 이에 대한 관심 있는 연구자들은 향후 연구 과제로 계속적인 연구를 진행하여 주기를 바란다.

참 고 문 헌

[1] Cebrowski, Arthur K. and Garst Ka, John J., “Network Centic Warfare : Its Origin and Future”, U.S Naval Institute Proceedings, 1998.
[2] Department of Defense, 『Network Centric Wrafare』, DOD report to Congress, 2001.
[3] 박창권, “네트워크 중심의 미래전 양상과 군사혁신”, 『합참』, 제15권, 2000.
[4] 손태종, “유비쿼터스 국방추진 방안”, 국방연구원, 2005.
[5] 육군본부, 「육군비전 2025」, 대전, 2004.
[6] 육군본부, 「지상작전」, 대전, 2003.
[7] 정현식, “유비쿼터스 기술이 전장지휘통제에 미치는 영향에 관한 연구”, 동국대학교 석사논문, 2006.
[8] 최종연구보고서, “유비쿼터스 정보보호 기본전략 연구”, 한국인터넷진흥원, 2006.
[9] 한국전자통신연구원, “무선, 이동통신망 보안대책(안)”, 한국전자통신연구원, 2002.
[10] 연구보고서, “무선, 이동통신망 보안대책”, 한국

인터넷진흥원, 2002.
[11] 합동참모본부, 「합동전장운영개념서」, 서울, 2004.
[12] 홍진기, “미래 전장정보체계 구축방안”, 한국국방연구원, 2005.
[13] www.etnews.co.kr, 전자신문.
[14] www.etri.re.kr, 한국전자통신연구원.
[15] www.krcert.or.kr, 인터넷침해대응센터.
[16] www.kisdi.re.kr, 정보통신정책연구원.
[17] www.mke.go.kr, 지식경제부.

권 문 택

1970년 육군사관학교(이학사)
1981년 미국 University of Iowa(공학석사)
1987년 University of Wisconsin(경영정보학 박사)

경희대학교 테크노경영대학원 정교수
경희대학교 정보지원처장
경희사이버대학교 초대 학장