9

NCW 환경에서의 국방정보보호 발전방향

한국국방연구원 ▌최 인 수

1. 서 론

네트워크중심전(NCW: Network Centric Warfare)은 전장에 참여하는 제 전력 요소에 관해 정보기술의 발전을 이용한 네트워크를 구축하면 전장상황인식의 공유와 전력의 통합화가 가능해지고 이에 따라 작전의 수행 효과를 획기적으로 높일 수 있다는 이론이다. 현재 이 이론은 미 국방부 전력변환(force transformation)에 있어 중요한 주제가 되어 있으며, 유럽의 여러 국가는 물론 호주나 싱가폴에서도 확산되어 군사발전의 중심 지향점이 되고 있다. 우리 군의 경우에도 네트워크중심전 이론은 급변하는 현대전 양상 및 미래전 환경에 대비한 군사력 발전 방향으로 인식되고 있다[1].

네트워크중심전은 기본적으로 작전 이론으로 이를 구현하는 것은 단순히 기술의 문제만은 아니다. 네트워크중심전 이론의 고안 및 발전을 주도하고 있는 미 국방부에서 '05년에 발간한 '네트워크중심전의 구현(The implementation of Network-Centric Warfare)'에서는 네트워크중심전 이론의 성공적인 구현 및 전력변환 추진을 위해서 교리(doctrine), 조직(organization), 훈련(training), 자원(기술)(material(technology)), 리더쉽 및 교육(leadership and education), 인력(personnel), 시설(facilities)의 7대 기능 영역들이 상호 병행적으로 발전하여야 함을 강조하고 있다. 하지만, 네트워크중심전 이론이 다양한 전력 요소들의 상호 유기적인 네트워킹을 전제로 하며 이를 가능하게 하는 것이 첨단 정보기술의 활용이라는 측면에서, 기술적 환경의 구축은 네트워크중심전 이론의 구현에 핵심적인 요소라고 할 수 있다.

그러면, 이와 같은 네트워크중심전 구현을 위한 기술적 환경은 어떻게 변화, 발전할 것인가?. 이는 상호 유기적인 네트워킹이라는 다분히 추상적인 개념을 각 나라가 직면한 현재 및 미래의 군사작전 환경에 어떻게 구현할 것인가에 따라 구체적인 모습은 달라질 것이다. 하지만, 네트워크중심전 이론의 기본적인 추구 방향만으로도 미래 국방정보통신 환경의 변화와 발전 방향은 어느 정도 예상 가능하다. 제 전력 요소들간의 네트워킹 보장을 위해서는 언제 어디서나 정보를 유통할 수 있는 통로가 마련되어야 하는데, 이는 열악한 전장 환경에서도 정보를 유통시킬 수 있는 새로운 네트워크가 구축되거나, 기존에 물리적·논리적으로 분리되어 운영 중인 다양한 네트워크 및 시스템들의 연동이나 통합이 확대될 필요가 있다. 또한, 유기적인 네트워킹을 통한 전장상황인식의 공유 확대와 전력의 통합화는 정보를 생성, 저장, 유통, 활용, 관리하는 방식이 현재와는 다르거나 더욱 진보한 방식으로 변화할 필요가 있다.

그런데, 이와 같은 미래 국방정보통신 환경의 변화와 발전은 정보보호 측면에서 많은 문제점을 내포하고 있다. 네트워크중심전 구현을 위한 기술적 환경은 새로운 첨단 정보기술들이 보다 적극적으로 활용되고 정보기술의 적용 범위 및 수준이 비약적으로 확대되는 등 군 임무 수행에 있어 정보기술에 대한 의존도가 더욱 심화되는 반면에, 정보보호 대상이 급격히 증가하고 정보기술을 적용, 활용하는 방식의 변화로 보안 위협의 변화와 새로운 취약점의 발생이 예상된다.

이에 본고에서는 네트워크중심전 환경에서 예상되는 정보보호 위협 및 취약점의 변화를 살펴보고, 이에 대비하여 우리 국방 환경에서 추진하여야 할 정보보호 발전 방안을 모색하고자 한다.

2. NCW 환경과 정보보호 위협/요구사항

여기서는 네트워크중심전 이론의 기본개념을 기반으로 네트워크중심전 환경의 변화 요소를 네트워크 와 시스템 측면에서 살펴보고 이에 따른 정보보호 위협을 기술한다.

2.1 NCW 네트워크 환경 변화와 정보보호 위협

네트워크중심전 추진에 따라 예상되는 네트워크 환경의 변화는 다음과 같은 것들이 있다.

첫째, 물리적·논리적으로 분리된 기반 네트워크들의 연동 또는 통합이 확대될 것이다. 제 전력 요소들 간의 상호 유기적인 네트워킹을 보장하기 위해서는 기본적으로 서로 정보를 주고받을 수 있는 통로가 열려있어야 한다. 따라서 현재와 같이 비밀 등급별 또는 체계 용도별로 분리되어 운용하고 있는 다양한 국방 네트워크들은 공통의 통합 네트워크로 통합되거나, 유기적인 정보 유통을 위해 각 네트워크들 간의 연결이나 연동 수준이 혁신적으로 확대될 것이다.

둘째, 무선/이동 네트워크 기술의 활용이 급격히 증가할 것이다. 급변하는 전장 환경에서 제 전력요소들을 네트워크로 연결하는 것은 유선 네트워킹 기술로는 많은 한계가 있다. 현재도 전술이나 전투 환경에서는 무선 통신을 주요한 네트워킹 수단으로 활용하고 있지만, 이는 대부분 음성 통신을 위주로 하고 있으며 다양한 정보를 유통하기 위한 데이터 통신 능력은 미흡한 실정이다. 또한, 네트워크중심전은 작전 환경 변화나 부대 이동에 따라 신속한 해체 및 재구성이 가능한 탄력적인 네트워크를 필요로 하는데, 이러한 요구는 무선 LAN, ad-hoc 네트워크 같은 무선/이동 네트워킹 기술들이 적극적으로 도입, 활용됨으로서 만족될 수 있다.

셋째, 네트워크를 통해 유통되는 정보의 양이 급격히 증가할 것이다. 네트워크중심전 환경에서는 정보유통의 대상 및 범위가 비약적으로 확대될 것이다. 예를 들어 현재 작전 수행을 위한 정보의 유통 수준 및 범위가 부대 지휘관까지라면, 네트워크중심전 환경에서는 개별 전투원 수준까지 확대되며, 전장 상황인식 정보의 정확한 공유를 위해 영상이나 사진과 같이 대용량 정보에 대한 요구가 더욱 증가할 것이다.

이와 같은 네트워크중심전 네트워크 환경의 변화는 정보보호 측면에서도 많은 영향을 미칠 것으로 예상된다. 다음은 이와 같은 환경 변화에 따라 발생할 수 있는 정보보호 위협 및 취약성들이다.

첫째, 네트워크 일부분에 대한 공격 및 침해가 전체 네트워크로 쉽게 확산될 수 있다. 현재와 같이 물리적·논리적으로 분리된 네트워크들을 운용하는 것은 정보의 유통 및 공유의 측면에서 많은 제한을 주지만, 정보보호 측면에서는 좋은 대책일 수 있다. 네트워크 통합 및 연동 확대는 어떠한 방식으로든 사이버 공격 및 침해가 가능한 경로가 증가하며 피해가 확산되는 원인이 될 수 있다.

둘째, 네트워크 보안성 상황에 대한 정보 분석과 공유가 제한될 수 있다. 사이버 공격 발생 시, 정보의 공유 및 체계적인 대응은 중요한 정보보호 업무 요소 중의 하나인데, 통상 이와 같은 업무는 네트워크의 규모가 커질수록 더욱 어려워진다. 따라서, 네트워킹 범위의 확대 및 연동/통합 확대에 대비한 네트워크 보안성 상황 정보의 수집, 분석, 배포/공유 및 대응 역량이 적절히 구비되지 못한다면, 제반 작전 수행에 기반이 되는 정보통신 기반의 안전성은 적절히 보호되기 어려울 것이다.

셋째, 유통되는 정보에 대한 보안 통제 및 관리가 적절히 수행되지 않을 수 있다. 네트워크들의 통합 및 연동 확대는 서로 다른 비밀등급의 정보가 다양한 네트워크 기반구조를 통해 유통될 수 있는 환경을 만들 수 있다. 이러한 환경에서도 비밀등급이 다른 정보들에 대한 보호 대책과 통제 수단은 서로 차별적으로 적용되어야 하지만, 정보의 유통 범위와 정보량이 증가할수록 이러한 통제 수단들을 정교하고 적시에 적용하는 것은 매우 어려운 일이다.

넷째, 동적으로 변화하는 네트워크 환경에서의 보안성 유지와 관리가 어려워진다. 네트워크중심전 환경은 다양한 무선/이동 네트워킹 기술들의 적극적인 활용이 예상되는데, 일반적으로 무선 환경은 기반 플랫폼의 한계로 유선 환경에 비해 정보보호 기술의 적용이 제한되며, ad-hoc 네트워크와 같은 환경에서의 정보보호를 위한 기반 및 관련 기술들은 이직 충분히 성숙되지 못한 실정이다.

2.2 NCW 시스템 환경 변화와 정보보호 위협

네트워크중심전 이론이 전제하는 유기적인 네트워킹 보장은 기술적 측면에서의 변화뿐만 아니라 임무수행 방식의 전반의 변화를 내포한다고 할 수 있다. 따라서 네트워크중심전 환경에서의 정보시스템 운영 또한 임무 수행 방식의 변화를 지원할 수 있도록 변화, 발전할 것이다. 이러한 측면에서 네트워크중심전 추진에 따라 예상되는 시스템 환경의 변화는 다음과 같은 것들이 있다.

첫째, 시스템 및 정보에 대한 접근 및 활용 범위가 확대될 것이다. 체계 간 연동이나 상호운용성 보장 등을 통해 필요한 정보들을 적시에 공유하고 유통시키기 위한 노력은 현재도 이루어지고 있지만, 네트워크중심전이 추구하는 전장상황인식의 공유와 전력의 통합화를 위해서는, 현재보다 비약적으로 많은 정보들의 공유 및 유통을 필요로 하며 이를 위해서는 시스템이나 정보에의 접근 및 활용 범위가 비약적으로 확대될 것이다.

둘째, 휴대용, 초소형 컴퓨팅 장치의 활용이 증가할 것이다. 최종 전투원 수준까지 정보의 유통 범위가 확

장되는 네트워크중심전 환경에서는 작전 본연의 임무 수행에 영향을 최소화하며 컴퓨팅 및 네트워킹 능력을 확대할 수 컴퓨팅 장치를 필요로 한다. 하지만, 이러한 환경에서 PC, 노트북 등과 같이 현재 일반적인 업무 환경에서 활용하는 컴퓨팅 장치들의 효용성, 활용성은 매우 제한될 것이다. 따라서 네트워크중심전 환경에서 사용자들이 활용 가능한 컴퓨팅 장치들은 휴대하기 편리하도록 소형화가 필요할 것이다. 또한, USN 등과 같은 첨단 감시정찰 기술의 적용과 제반 무기체계의 정보통신 능력 강화에 따라 초소형 컴퓨팅 기술의 활용은 더욱 증가할 것이다.

셋째, 정보 유통에 대한 통제 요구 수준이 높아질 것이다. 현재와 같이 정보체계와 네트워크의 연관성이 매우 높은 환경에서 정보 유통에 대한 통제는 대부분 기반 통신망이나 전체 시스템 차원에서 이루어지고 있다. 하지만, 정보의 생산자와 소비자가 확대되고 상호 유기적으로 연계되는 네트워크중심전 환경에서는 보다 정교한 정보 유통 통제가 필요하며, 따라서 단위 시스템 또는 데이터 수준까지 정보 유통에 대한 통제가 요구될 것이다.

이와 같은 네트워크중심전 시스템 환경의 변화는 정보보호 측면에서도 많은 영향을 미칠 것으로 예상된다. 다음은 이와 같은 환경 변화에 따라 발생할 수 있는 정보보호 위협 및 취약성들이다.

첫째, 지역/개별 시스템에의 공격 및 침해가 전체 시스템으로 쉽게 확산될 수 있다. 네트워크 환경 변화에 따른 정보보호 위협과 마찬가지로, 유기적인 네트워킹 보장을 위한 체계 간 연동 및 연결의 확대는 정보보호 측면에서는 공격이나 침입을 할 수 있는 경로의 증가를 의미한다.

둘째, 인가되지 않은 사용자에 의한 불법적인 시스템 접근 및 활용 위협이 증가한다. 현재 대부분의 국방정보체계들은 시스템에 저장된 인가 사용자 정보를 기반으로 시스템에 대한 접근 및 활용을 통제한다. 그런데, 네트워크중심전 환경은 언제 어디서든 시스템이나 정보에 대한 접근이 가능한 유비쿼터스 환경으로, 기존의 방식을 확대 적용하는 것이 제한된다. 즉, 보다 포괄적이고 정교한 사용자 식별 및 인증 기술이 마련되지 않는다면, 정보의 공유 및 유통이 제한되거나 부적합한 보호 대책으로 비인가 사용자에 의한 불법적인 시스템 침해 위협 및 취약성은 더욱 증가할 것이다.

셋째, 공유, 유통되는 정보의 기밀성 훼손 가능성이 증가한다. 네트워크를 통해 전송되는 정보의 기밀성 보호를 위해서는 적절한 암호기술의 활용이 필요한데, 암호기술이 안전하게 동작하려면 통신 당사자들 간에 적절한 동기화가 필요하다. 그런데, 이러한 동기화 작업을 위한 노력은 네트워킹하는 당사자들이 증가할수록 매우 어려워진다. 따라서 네트워크중심전 환경에 적합한 암호기술이 지원되지 않으면, 해당 정보들은 적절히 보호되기 어려울 것이다.

넷째, 정보의 정확성, 신뢰성에 대한 검증이 더욱 어려워질 것이다. 네트워크중심전 환경에서는 정보의 생산자와 소비자를 사전에 명확히 예측하기 어려우며, 단일 시스템 환경에서 모든 정보에 대한 획일적인 통제도 어려울 것이다. 따라서 급증하는 정보의 양에 비례하여 각 정보들이 정확하고 신뢰할 수 있는가를 판단하는 것은 더욱 어려워질 것이다.

2.3 NCW 환경에서의 정보보호 요구사항

네트워크중심전 추진에 따라 예상되는 네트워크, 시스템 환경 변화와 이에 따른 정보보호 위협의 변화를 바탕으로 볼 때, 네트워크중심전 환경에서는 다음과 같은 정보보호 역량들은 요구된다.

첫째, 사용자 및 개체에 대한 식별/인증과 권한관리(privilege management) 기반이 강화되어야 한다. 식별/인증과 권한관리는 정보자산에 대한 접근통제 기능을 구현하는데 있어 기본적으로 요구되는 요소들이다. 유기적인 네트워킹이 강조되는 네트워크중심전 환경에서는 현재와 달리 사전에 명확히 정의하기 어려운 다양한 사용자 및 개체들이 다양한 방식으로 네트워크, 시스템 및 정보에 접근하고 상호작용한다. 이러한 환경에서 사용자나 개체의 정당성, 확실성 등을 적절히 식별/인증하고 해당 정보자산에 대한 접근권한을 통제하는 것은 안전하게 정보를 공유, 유통하기 위한 전제 요건이다. 그러나, ID/Password와 같은 기존의 접근 방법은 이러한 문제점을 해결하기에는 매우 제한적이다. 개별 네트워크나 시스템 별로 모든 사용자나 개체들에 대한 식별/인증 및 권한 정보들을 저장, 관리하는 것은 현실적으로 불가능하며, 다양한 네트워크과 시스템에 산재된 정보들의 일관성있게 유지, 관리하는 것도 매우 어렵기 때문이다. 따라서, 네트워크중심전 환경에서 네트워크, 시스템 및 정보에 대한 적절한 보안 관리를 위해서는 동적으로 변화하는 전장 환경에서 다양한 사용자와 개체들을 적절히 식별/인증하고 이들의 권한을 전사적·통합적으로 관리할 수 있는 새로운 기반 역량의 구축과 강화가 요구된다.

둘째, end-to-end 네트워킹 환경에서, 다양한 수준의 정보들이 요구되는 보안성 수준에 적합하도록 통합적으로 보호, 관리, 유통되어야 한다. 현재 우리 군

은 물리적·논리적으로 분리된 다양한 사용자 통신망과 정보체계들을 이용하고 있으며, 이를 기반으로 정보의 유통이 통제되는 상황이다. 하지만, 네트워크중심전 환경에서는 폐쇄적인 네트워크, 시스템들의 연동이나 연결이 비약적으로 확대되거나 통합되는 방식으로 발전할 것이다. 또한, 정보의 생산, 처리, 저장, 관리, 유통되는 범위는 최종 사용자나 단말에 이르기까지 확대될 것이다. 이러한 환경에서 다양한 비밀 수준의 정보들을 현재와 같이 개별 시스템이나 네트워크 수준에서 보호, 관리하는 것은 매우 어려운 일이다. 따라서 네트워크중심전 환경에서는 다양한 비밀 수준의 정보들이 동일한 네트워크를 통해 공유, 유통될 수 있어야 하며, 하나의 시스템이 다양한 비밀 수준의 정보들을 처리, 저장, 관리할 수 있어야 한다.

셋째, 네트워크와 시스템에 대한 정보보호 상황정보가 실시간으로 공유되어야 한다. 네트워크중심전 환경에서는 자신의 작전 영역 내의 네트워크와 시스템이 안전하다고 하더라도 이와 연결된 다른 네트워크 및 시스템의 안전성이 지휘관의 의사결정 및 작전 수행에 직·간접적으로 영향을 미칠 수 있다. 따라서, 단위 네트워크나 시스템 별로 탐지, 분석되는 개별적인 정보보호 상황 정보들은 영향을 미칠 수 있는 제대와 체계들과 상호 유기적으로 공유될 수 있어야 한다.

넷째, 기밀성 보호를 위한 암호기술/장비는 대용량 및 다양한 유형의 데이터 처리와 동적으로 변화하는 네트워크 환경에 적용 가능하여야 한다. 암호기술/장비는 비밀 정보의 보호를 위해 사용되는 주요한 수단으로, 네트워크중심전 환경에서도 필수적인 정보보호 수단일 것이지만 기능과 성능의 비약적인 발전을 필요로 한다. 우선 암호기술/장비는 정보의 공유, 유통이 증가함에 따라 필연적으로 예상되는 통신망 대역폭 확장을 충분히 지원할 수 있도록 고속화되어야 한다. 또한, 정보통신 기술 발전으로 데이터, 음성, 영상 등 다양한 유형의 정보들이 동일한 네트워킹 환경으로 통합됨에 따라, 이들 정보들을 통합적으로 처리, 보호할 수 있어야 한다. 마지막으로, ad-hoc 네트워크와 같이 동적으로 구성, 해체되는 미래 전장 네트워킹 환경에서 비밀 정보의 공유, 유통을 적절히 보호할 수 있어야 한다.

다섯째, 암호키 자원들은 유기적인 네트워킹을 지원할 수 있도록 체계적이고 통합적으로 관리되어야 한다. 안전한 암호기술의 활용은 우선 충분한 보안성을 제공하는 알고리즘/메커니즘의 설계 및 구현이 전제되어야 하지만, 실제 운영 환경에서 더욱 중요하게 강조되는 것은 암호기술에 적용되는 암호키 자원의 안전한 관리이다. 이러한 중요성 때문에 중요 정보의 보호를 위한 암호기술의 암호키는 엄격한 통제 하에 분배, 공유, 관리되어 왔으며, 우리군 또한 오프라인 중심의 암호키 관리 체계를 운영하여 왔다. 그러나 네트워크중심전 환경에서는 암호기술의 적용 범위 및 수준 또한 비약적으로 확대되고, 암호기술이 적용되는 환경 또한 매우 동적으로 변화할 것으로 예상되는데, 이러한 환경에서 전통적인 암호키 관리 방식은 적절히 동작하기 어려울 것이다. 따라서 제반 네트워크 및 시스템의 구축, 운영 개념이 변화하는 네트워크중심전 환경에서는 이에 부합하는 새로운 암호키 관리 방식이 재정립되어야 하며, 이를 기반으로 한 정보보호체계의 구축 및 운영이 수반되어야 한다.

3. NCW 정보보호 발전 방향

네트워크중심전이 새로운 미래전 개념으로 주목을 끌고 있지만, 이는 기존에는 존재하지 않던 완전히 새로운 이론이나 개념은 아니다. 첨단 무기체계의 도입이나 C4I체계 구축과 같이 군 현대화나 국방정보화를 위해 기존에 추진하여 왔던 다양한 노력들은 네트워크중심전이 추구하는 기본 개념을 반영하고 있거나, 적어도 향후 한국적 네트워크중심전 구축 추진의 기반이 될 수 있다. 이러한 측면에서, 국방정보보호 또한 국방정보통신 환경 변화에 따라 지속적으로 변화, 발전하여 왔으며, 향후 네트워크중심전 구축 노력을 뒷받침 할 수 있는 기본적인 역량은 확보하고 있다고 할 수 있다. 하지만, 네트워크중심전 추진은 국방정보통신 환경의 많은 변화를 수반하며, 이를 정상적으로 추진하기 위해서는 기존 국방정보보호 추진 방식에도 많은 변화와 발전이 필요하다. 여기서는 이를 위한 발전 방향을 제시한다.

3.1 전사적 정보보호 추진 전략, 기준 및 아키텍처 정립

오늘날과 같은 정보통신 환경에서 모든 정보보호 위협, 위험에 대처할 수 있는 단일 솔루션을 개발하는 것은 현실적으로 불가능하다. 따라서, 고유의 기능을 수행하는 다양한 정보보호 수단들을 적절히 배치, 활용하여, 상호 취약점을 보완함으로서 궁극적으로 체계 전체의 보호 능력을 극대화하는 것이 현실적이고 효율적인 정보보호 접근방법으로 인식되고 있다. 하지만, 이러한 접근방법을 실질적으로 구현하는 것은 네트워크중심전 환경과 같이 대상 환경이 커지고 복잡해질수록 어려워진다. 독립적인 네트워크, 시스템 환경 차원에서는 고려할 필요가 없던 위협, 위험이 상호 네트워크로 연결됨에 따라 새롭게 도출될 수 있

으며, 개별적인 환경에서는 비용 대 효과적인 정보보호 대책이 전사적 차원에서는 중복 투자되거나 작전 수행을 위한 체계 성능에 부정적인 영향을 끼칠 수도 있기 때문이다. 따라서 네트워크중심전 환경에서 효율적이고 체계적인 정보보호 추진을 위해서는 우선 전사적인 정보보호 정책과 추진 전략을 명확히 수립할 필요성이 있다.

현재 우리 군은 앞서 기술한 정보보호 접근방법을 다수준·다계층 보호라는 용어로 사용하고 있다. 하지만, 우리 군의 다수준·다계층 보호는 아직 개념적 수준에서만 통용될 뿐, 보호 대책 수립이나 정보보호 체계 구축 등과 같은 실질적인 정보보호 업무 추진 시 실행 가능한 추진 전략의 수준으로 정립되어 있지 못한 실정이다. 미 국방부의 경우, 정보화 시대의 국방 환경 변화에 따라 이미 '90년대 중반 이후 종심방어(defense-in-depth) 전략이라는 공통의 정보보호 추진 전략을 정립, 발전시키고 있고, 관련 제도/규정과 업무 추진에 종심방어 전략을 기반으로 한 정보보호 추진을 명확히 요구하고 있는데, 이는 미군의 네트워크중심전 역량 구축 추진에 있어서도 일관성있게 적용되고 있다.

우리 군도 다수준·다계층 보호 전략이 실행 가능한 추진 전략으로 동작하려면 전략의 구현을 위한 구체적인 지침과 가이드라인의 개발과 보급이 필요하다. 네트워크중심전 환경은 단위 시스템이나 데이터 수준까지 정교한 보안 통제를 필요로 하기 때문에, 전략 구현을 위한 지침과 가이드라인은 상위적으로 전군 차원에서 추진할 정보보호 요소와 개별 네트워크, 시스템 구축 차원에서 추진하여야 할 정보보호 요소들을 명확히 구분하여야 하며, 하위적으로 다양한 수준을 고려한 정보, 시스템, 네트워크의 보호 및 통제 기준들을 포함하여야 한다.

네트워크중심전 환경은 언제, 어디서든 사이버 공격이 발생할 수 있으며, 공격으로 인한 피해가 쉽게 확산될 수 있는 환경이다. 이러한 환경에서 네트워크, 시스템의 성공적인 방어를 위해서는 제반 정보보호 역량, 기능들의 중앙 집중적인 관리와 지속적인 성능 개량을 필요로 한다. 실질적으로 대부분의 정보보호 기능들은 개별 네트워크, 시스템에서 구현되지만 이러한 기능들은 전사적 차원에서 상호 유기적으로 연계되어야 한다. 이를 위해서는 네트워크중심전 환경에서 공통적으로 적용될 네트워크, 시스템 방어 아키텍처 정립이 필요하며, 이를 기반으로 일관성 있는 체계 구축이 필요하다.

3.2 체계 구축과 정보보호의 유기적인 병행 및 관리 추진

과거 주요한 국방정보보호 요구사항은 통신망 상으로 유통되는 정보의 기밀성 보호였고, 이를 위해 대상 체계의 구축, 운영과는 직접적으로 연관되지 않는 통신용 암호장비를 주요한 보호 대책으로 적용하였다. 그러나 현재의 국방정보통신 환경이나 네트워크중심전 환경에서는 사이버 공격 등과 같은 새로운 위협에 대처하기 위해 기밀성뿐만 아니라 다양한 정보보호 서비스들을 필요로 하고 있다. 그런데, 이러한 정보보호 서비스들은 대부분 과거와 같이 대상 체계와 독립적인 방식으로 구축, 운영하는 것이 매우 제한된다. 예를 들어, 정보의 end-to-end 보호를 위해서는 정보의 수명주기 전반에 걸친 통제가 필요한데, 이를 위해서는 정보의 생성, 처리, 저장, 관리 등에 관여되는 시스템 기능 구현 시, 관련 정보보호 기능들이 유기적으로 고려되어 통합적으로 개발되어야 한다. 즉, 정보, 시스템에 대한 정밀한 통제가 요구되는 네트워크중심전 환경에서 안전한 체계를 구축하기 위해서는 체계 구축 및 운영을 위한 공학적 활동의 일환으로 정보보호를 위한 활동이 체계적으로 수행되어야 한다. 이를 위해서는 체계의 수명주기 업무, 활동들과 유기적으로 연계되는 보안성관리 프로세스의 정립과 시행이 우선적으로 요구된다. 보안성관리 프로세스란 대상 체계의 보호를 위해 수행되어야 하는 제반 업무, 활동, 절차들을 포괄하는 용어이다. 미 국방부의 경우, 이미 '90년대 중반부터 미국방정보체계보안성인증인가프로세스(DITSCAP: DoD Information Technology Security Certification and Accreditation Process)[1]라는 전사적인 정보체계 보안성관리 프로세스를 정립하고, 모든 국방정보체계들은 이 프로세스에 따라 획득, 운영, 폐기 등 수명주기 전반에 걸쳐 보안성관리 활동을 수행토록 요구하고 있다.

개념적으로 볼 때, 보안성관리 프로세스는 과거에는 없던 새로운 요구사항은 아니다. 현재도 우리 군은 획득 초기 시점의 보안대책 수립/검토, 체계 개발 후 시험평가 시점의 보안성 평가, 체계 운영 전의 보안측정 등과 같은 정보체계의 보안성 유지, 관리를 위한 나름대로의 활동들을 수행 중에 있다. 그러나 현재 정보체계 개발 과정 중의 보안성 관리 업무 및 활동은 명확히 정립되지 못한 실정이며, 제반 보안성관리 업무 및 활동들과 정보체계의 구축, 운영을 위한 업무 및 활동

1) '06년 7월, 미국방부는 관련법과의 일관성 유지 및 기존 프로세스의 발전을 위하여 DITSCAP을 수정, 보완한 DIACAP(DoD Information Assurance Certification and Accreditation Process)을 공표하였다.

들도 상호 유기적으로 연계되어 있지 못한 실정이다.

국방 전사적인 보안성관리 프로세스의 정립을 위해서는 우선 단기적으로 전군적인 공통, 표준 프로세스의 개발과 병행하여 현재 수행 중인 제반 보안성관리 활동들의 내실화를 위한 노력이 병행적으로 수행되어야 한다. 여기에는 체계적인 보안대책 수립 지원을 위한 기준을 재정립하고 체계 개발 과정 중의 보호 기능 구현과 검증 활동을 강화하는 것이 포함되어야 한다. 또한, 중·장기적으로 표준 프로세스를 국방정보체계의 보안성관리를 위한 기본적인 업무 활동 요구사항으로 시행하고, 체계 보안성의 지속적 유지, 관리를 위해 인증/인가와 같은 프로세스로 발전되어야 한다.

3.3 사이버 공격의 탐지, 차단 및 대응 역량 강화

정보보호의 궁극적인 목적은 모든 위협, 위험으로부터 대상 환경을 완벽히 보호, 방어하는 것일 것이다. 그러나 모든 위협, 위험을 사전에 파악하는 것은 현실적으로 불가능하다. 따라서 오늘날 정보보호는 수동적 차원에서 정보보호 기술, 체계들을 구축하는 노력과 함께, 사이버 공격과 침해 행위를 적시에 탐지, 차단하고 적절히 대응하는 능동적인 역량이 중요하게 강조되고 있는데, 이는 네트워크중심전 환경에도 특별히 중요하다고 할 수 있다.

이러한 역량 강화를 위한 요소는 크게 기술적 측면과 조직·절차적 측면으로 구분할 수 있다. 우선 기술적 측면에서는 현재 탐지, 차단, 대응을 위한 보호, 방어 체계들을 단계적으로 확장, 발전시켜야 한다. 현재 우리 군은 사이버 공격과 침해사고 대응을 위해 국방통합보안관제체계를 구축, 운영 중에 있다. 그러나 관제체계의 대응 범위는 국방전산망 환경으로만 국한되는 실정으로, 전략·전술망 환경과 인터넷망 환경까지의 확장되어야 하며, 현재 네트워크 중심의 관제 범위 또한 주요 시스템, 단말을 포함할 수 있도록 발전하여야 한다. 통합보안관제체계의 탐지, 대응 기능 또한 혁신적인 질적 발전이 필요하다. 미래 사이버전 환경을 가정할 경우, 우리 군이 대비하여야 할 잠재적인 적은 고도의 전문성과 조직력을 갖춘 적의 사이버 전사들일 것이다. 이러한 측면에서 현재 통합보안관제체계의 탐지, 분석 기능은 매우 초보적인 수준으로, 다양한 위협 정보의 상관분석과 같이 실질적인 대응 활동에 지원할 수 있는 기능적 개선이 절실히 요구된다.

조직·절차적 측면에서는 제반 탐지, 대응 활동을 군사작전 지원을 중심으로 한 통합적인 프로세스로 발전시켜야 한다. 현재 우리 군의 사이버 공격 탐지 대응 활동은 침해사고긴급대응반(CERT)을 중심으로 하여 일반·평시 업무의 지원을 중심으로 수행되고 있는데, 전쟁을 대비하는 군의 고유한 존재 목적과 정보통신 기술, 정보체계에 대한 의존도가 더욱 심화되는 네트워크중심전 환경을 가정할 경우, 이러한 역량들은 전시, 작전 지원을 중심으로 발전하여야 한다. 이를 위해서는 우선 정보작전(IO: Information Operation), 사이버전 대응, 컴퓨터네트워크방어(CND: Computer Network Defense) 등과 같은 사이버 공격 탐지/대응과 관련된 개념들을 우리 국방 차원에서 명확히 정립하여야 하며, 유관 업무 프로세스와 활동들을 합참, 작전사 중심으로 재정립하여야 한다. 또한, 작전 지휘관의 적절한 의사결정을 지원하기 위해 정보보호 상황정보의 적시 유통, 보급을 위한 사이버지휘통제체계를 개발하고, 이를 수준별 지휘통제체계와 통합하기 위한 노력을 단계적으로 추진하여야 한다.

3.4 탄력적인(flexible) 암호기술·장비 연구개발 추진

암호기술/장비는 중요 비밀 정보의 기밀성 보호를 위해 적용되는 핵심적인 정보보호 수단이다. 따라서 암호기술/장비는 엄격한 통제 하에 개발, 활용되며, 보안성이나 안전성을 이유로 하드웨어(H/W) 방식의 장비나 시스템을 활용하고 있다. 그러나 네트워크중심전 환경은 네트워킹의 범위 또한 최종 사용자 수준까지 확대되며, 전술·작전 환경에 따라 유기적으로 변화하는 매우 동적인 환경으로, 이러한 환경에서 현재와 같은 하드웨어 위주의 암호기술/장비로는 적절한 지원이 제한될 것으로 예상된다. 우선 네트워크중심전 환경에서 암호기술/장비의 적용 확대는 비용적 측면에서 막대한 부담으로 작용할 것이며, 유기적인 네트워킹을 필요로 하는 다양한 환경에서 물리적인 방식으로 암호기술/장비들을 관리하는 것이 매우 어려운 일이기 때문이다.

이러한 문제를 해결하기 위해서는 하드웨어 암호기술/장비와 병행하여 소프트웨어(S/W) 암호기술의 적극적인 활용이 요구된다. 기술적 측면에서 소프트웨어 암호기술은 하드웨어 암호기술/장비에 비해 보안성, 안전성이 낮다고 평가되고 있으나, 관련 기술의 발전에 따라 소프트웨어 암호기술 또한 지속적으로 발전하여 이미 많은 영역에서 활용되고 있으며, 대상 환경 변화에 따라 탄력적으로 적용할 수 있다는 장점이 있다. 미 국방부의 경우도 네트워크중심전 환경에서 요구하는 암호기술/장비의 요구사항을 만족시키기 위해 기존 하드웨어 기술 중심에서 소프트웨어 기술 또한 적극적으로 활용하는 방식으로 변화하여 프로그램밍이 가능하고(programmable), 내장 가능한(embed-

dable)한 암호기술/장비의 개발을 추진 중에 있는데, 향후 전술 환경의 주요한 통신 장비로 활용될 JTRS (Joint Tactical Radio System)의 경우도 이러한 기술이 적용되어 개발 중에 있다.

따라서 네트워크중심전 환경이 요구하는 암호기술/장비의 혁신을 위해서는 다음과 같은 활동들이 추진되어야 한다. 먼저, 현재 하드웨어 암호기술/장비 위주의 국방정책은 소프트웨어 기술이 병행적으로 활용 가능하도록 정비되어야 한다. 그리고 현재 개발 중이거나 계획된 국방용 암호장비의 연구개발 계획을 네트워크중심전 추진 개념에 맞추어 정비하여야 한다. 마지막으로, 하드웨어 방식의 암호기술/장비와 달리 직접적인 관리와 지속적인 지원이 요구되는 소프트웨어 암호기술의 특성상, 소프트웨어 암호기술·장비를 중심으로 한 국방 자체적인 연구개발 역량 강화도 병행적으로 추진되어야 한다.

3.5 전사적 신원 및 권한 관리기반체계 구축

사전 예측이 어려운 전장 환경에서 아군과 적군을 정확하게 구분하는 것은 중요한 작전 요소 중의 하나이다. 이것은 네트워크를 통해 수많은 개체들이 시스템, 정보에 접근하는 정보통신 환경에서도 마찬가지라고 할 수 있다. 식별/인증은 시스템이나 네트워크에 접근하는 다양한 개체들이 정당한가를 확인하고 검증하는 정보보호 서비스로 접근통제 기능을 구현하기 위한 핵심 기반이며, 다른 정보보호 통제수단을 적용하는데 있어 기준을 제공한다.

현재 대부분 국방정보체계에서 적용 중인 식별/인증 및 접근통제 기능은, ID/Password 방식과 같이, 시스템이나 정보에 접근하는 개체가 제공하는 신원 또는 권한정보를 사전에 정의되어 시스템에 저장된 신뢰 정보와 비교하는 방식으로 구현하고 있다. 그리고 사전에 정의하는 신뢰 정보의 범위 또한 단위 체계나 조직의 범위로 제한되어 있다. 그런데 이러한 접근방식은 네트워크중심전 환경에서 효율적으로 동작하는데 어려움이 예상된다. 네트워크중심전 환경에서는 모든 네트워킹 요소들을 사전에 정의하기 어려우며, 따라서 시스템이나 네트워크 별로 사전에 신뢰정보들을 명확히 정의하기 어렵다. 또한, 어떤 수준과 범위에서 이러한 신뢰정보의 정의가 가능할지라도 각 시스템이나 네트워크 별로 저장, 관리하여야 하는 신뢰정보의 양은 급증할 것이며, 이를 일관성있게 유지, 관리하는 것은 막대한 노력을 필요로 할 것이다. 따라서, 네트워크중심전 환경에서 다양한 개체들을 식별/인증하기 위해서는 기존 단위 시스템이나 네트워크 수준을 넘어서 전사적 차원에서 신원 및 권한 정보들을 신뢰성 있게 관리, 제공할 수 있는 통합적인 기반체계의 구축이 필요하다.

이러한 통합적인 기반체계 구축을 위한 추진 방향은 크게 2가지로 구분할 수 있다. 첫째는, 현재 국방부, 각군, 기관별로 관리되는 인사관리정보를 통합적으로 관리할 수 있는 체계를 구축하는 것이다. 이를 위해서는 현재 국방부, 각군, 기관별로 사용 중인 인사관리정보체계들의 물리적인 통합을 우선적으로 고려할 수 있겠지만, 네트워크중심전 작전 환경에서 요구되는 사용자 신원 및 권한 정보의 통합적인 관리 및 지원에 초점을 두어야 할 것이다. 둘째는, 사용자의 신원 및 권한 정보들을 안전하게 배포, 유통할 수 있는 정보보호 기반체계를 구축하는 것이다. 네트워크를 통해 유통되는 신원 및 권한 정보들은 불법적인 변조, 위조로부터 보호되어야 한다. 오늘날 이를 위한 기술적 대안들로는 공개키기반구조(PKI: Public Key Infrastructure)를 활용하는 방법과 독립적인 신원/권한관리기반구조를 구축하는 것이 있다. 그런데, 현재 우리 군은 국방차원의 공개키기반구조인 국방인증체계를 구축, 운영하고 있으며 향후 이를 전사적인 정보보호기반체계로 확대, 발전시킬 계획을 가지고 있다. 따라서, 중복투자의 방지와 사용자 편리성을 위해, 우리 군은 현 국방인증체계를 국방 공통의 신원관리 기반체계로 확대, 발전시키는 것이 적절할 것이다. 이를 위해서는 우선 단기적으로 현재 운영 초기 단계에 있는 국방인증체계의 활용 활성화를 위한 노력을 기울여야 할 것이다. 그리고 중장기적으로는 네트워크중심전 환경에서 요구되는 보호 수준을 만족하기 위해 국방인증체계의 보증 등급을 높이고, 무선·이동 환경의 지원 역량을 강화하며, 앞서 기술한 통합적인 인사관리정보체계와의 유기적인 연계를 강화하여 전사적인 신원 및 권한관리 역량을 구축하여야 할 것이다.

3.6 통합 암호키관리 체계 구축

현재 우리 군은 통신용암호장비 위주로 암호기술/장비를 활용하고 있으며, 암호키 배포와 관리를 대부분 오프라인, 수동 방식으로 수행하고 있다. 이러한 방식은 현 시점에서도 많은 문제점을 내포하고 있지만, 종단간 수준까지 정보 공유와 유통을 지원하기 위해 암호기술/장비의 활용이 비약적으로 확대될 네트워크중심전 환경에서는 정상적인 동작이 어려울 것이다. 따라서, 암호키 배포, 관리 방식은 기존 방식과 병행하여 온라인 환경에서 자동적인 암호키 분배, 관리를

지원할 수 있는 통합적인 기반체계로의 발전이 필요하다.

암호기술은 크게 대칭키 암호와 공개키 암호로 구분된다. 따라서, 암호키 관리의 대상은 크게 대칭키 암호키와 공개키 암호키가 포함된다. 현재 우리 군은 공개키 암호기술을 효율적으로 활용하기 위한 기반으로 국방전산망 환경과 전략/전술망 환경에서 각각 국방인증체계와 국방키관리기반체계를 구축, 운영 중에 있어, 공개키 암호키를 체계적으로 관리할 수 있는 기반은 구축하였다고 볼 수 있다. 그러나, 현 체계는 현 국방정보통신 환경에서의 임무 수행을 지원할 수 있는 수준으로, 네트워크중심전 환경이 요구하는 보안성 수준을 만족하기 위해서는 보다 높은 보증등급으로의 성능 개선이 필요하며 무선이나 이동 환경의 지원 기능도 강화되어야 한다.

공개키 암호키와 달리 대칭키 암호키에 대한 체계적인 관리 기반은 현재 매우 미비한 실정이다. 일반적으로 공개키 암호는 온라인 환경에서 대칭키 암호키를 공유하고 분배하는데 효율적으로 활용된다. 이러한 측면에서 현재의 국방인증체계나 국방키관리기반체계는 단계적인 보증등급 강화와 기능 개선을 통해 중요 정보의 보호를 위한 대칭키 암호키를 분배, 관리하는데 활용될 수 있을 것이다. 하지만 현 체계들은 공개키 암호키의 분배, 관리에 초점을 맞춘 기반체계로 대칭키 암호키의 관리를 위한 요구사항을 모두 포괄하지는 않는다고 할 수 있다. 따라서, 현 체계들과 유기적으로 연계되어 효율적이고 체계적인 대칭키 암호키를 관리할 수 있는 공통 기반체계의 구축이 요구된다.

이를 위해서는 단기적으로는 한국군의 작전과 전술환경에 적합한 통합적인 암호키 관리 방안/모델이 정립되어야 하며 이의 일환으로 대칭키 암호키의 관리 방안도 정립되어야 한다. 민간 분야에서도 널리 활용되는 공개키 암호기술과 달리 대칭키 암호기술은 국가나 국방 차원에서 주로 사용하고 있으며, 보안 특성상 이에 대한 실질적인 참고자료나 벤치마킹 대상이 거의 전무하기 때문이다. 중·장기적으로는 대칭키 암호키 관리체계의 구축 추진과 함께, 국방인증체계 및 국방키관리기반체계와의 유기적인 연계 체제를 구축하여, 제반 암호키의 생성·분배·관리를 통합적으로 지원하는 전사적 공통 기반체계로서 통합암호키관리체계를 구축하여야 한다.

4. 결 론

오늘날과 같은 정보통신 환경에서 상위적 수준의 정보보호 요구사항은 기밀성, 무결성, 가용성, 인증, 부인봉쇄 등과 같은 개념들로 정의된다. 이러한 개념들은 예상되는 네트워크중심전 환경에서도 동일하게 요구될 것으로 판단된다. 그러나 네트워크중심전 환경에서 이러한 요구사항들을 만족시키기 위해서는 현재와는 다른 방식으로의 접근이 요구된다. 네트워크중심전 목표 달성에 기반이 되는 유기적인 네트워킹 환경 구축은 기존 네트워크·시스템 구축 및 운영 방식의 확장이나 부분적인 변경이 아니라, 근본적인 변화와 혁신을 요구한다. 따라서 네트워크중심전 환경에서의 정보보호 추진 또한 새로운 방향의 모색이 필요하다.

본 고에서는 네트워크중심전 환경 변화에 따른 정보보호 위협과 요구사항 분석을 기반으로 국방정보보호 발전 방향을 제안하였다. 아직 우리 군의 네트워크중심전 추진 방향은 구체화되지 못한 상황으로, 분석된 내용은 네트워크중심전의 기본 개념을 기반으로 하였다. 따라서 향후 우리 군의 네트워크중심전 추진 방향이 정립됨에 따라, 실질적인 정보보호 위협을 도출하고 이를 사전에 대비하기 위한 노력이 추진되어야 한다.

참고문헌

[1] 한국국방연구원, 네트워크중심전(NCW) 연구, 2005.

[2] 국방부, "국방정보화정책서", 2006.3

[3] 국방부, "차세대국방정보통신망 최적화 설계 연구", 2004.12

[4] 한국국방연구원, "국방정보체계 획득의 안전성검증절차 연구", 2005

[5] D.S. Alberts, J.J Garstka, K.P. Stein, Network Centric Warfare: Developing and Leveraging Information Superiority, CCRP 1999

[6] DoD, "DoD Information Assurance Strategic Plan", Jan., 2004

[7] DoD Directive 8500.1, "Information Assurance", 2003

최 인 수

1989~1993 고려대학교 수학과(학사)
1993~1995 고려대학교 수학과(석사)
2001~2005 고려대학교 정보보호대학원(박사수료)
1995~1998 국방정보체계연구소 연구원
1999~2000 국방과학연구소 연구원
2000~2001 국가보안기술연구소 연구원
2001~현재 한국국방연구원 선임연구원
관심분야 : 정보보호, 정보전, C4I체계
E-mail : ischoi@kida.re.kr