국가 사이버전 대비방안 연구

김 귀 남*

요 약

지난 2003년 1월 25일 인터넷 마비사고와 2004년 주요 국가기관 해킹사건을 겪으면서 사이버 위협의 파괴력이 국가안보에 직접적이고 심각하게 위협하는 단계에까지 도달하였다. 그래서 사이버테러나 사이버전(cyber warfare)은 더 이상 가상적 상황이 아닌 현실적이며, 실체적인 안보상황으로 상대국의 군사지휘체계는 물론 통신, 에너지, 금융, 수송체계 등 국가 주요기능 무력화의 전쟁 개념의 확대로 재인식되고 있다. 이러한 시점에서 정보전, 정보작전, 네트워크 중심전 등 혼재된 유사 용어들 속에서 사이버전에 대한 명확한 개념 정립 필요하고 각 국의 사이버전 동향 분석 및 국내 사이버전 현황 분석을 통해 문제점을 식별, 보완책 마련이 필요하다. 그래서 본 논문에서는 국가적 위기를 효율적으로 관리하고, 효과적이며 능동적으로 사이버전을 수행할 수 있는 발전방향과 상대적으로 사이버전 관련 기술 및 전문 인력 운영적측면에서 열세에 놓여 있는 군의 사이버전 수행체계에 대한 혁신방향을 연구를 하였다.

A Study on the Preparation of National Cyber Warfare

Kuinam J. Kim*

ABSTRACT

The destructive power of cyber threat arrived to until the phase which it threatens to direct and seriously in national security undergoes an important national institutuin hacking event of 2004 and Internet paralysis accidents of 2003. 1. 25. So Cyber terror and Cyber warfare is not the hypothetical enemy situation. It is more actual security situation and identify as magnification of warfare concept of incapacitation national important ability include military command system of the adversary, communication, energy, finance and transportation system. consequently, with the progress of cyber threat, it is necessary that looking at a number of general plan to make up for the weak points in cyber warfare operation system. Thus, the focus of this study is to examine new ways of developing a comprehensive cyber security management system.

Key word : Information Warfare, Cyber Warfare

* 경기대학교 정보보호학과

1. 서 론

오늘날 초고속 인터넷가입율 세계 1위, 인터넷 사용자 수 세계 3위 등 세계적 수준의 IT 강국으로서 면모를 갖추고 있고, 또한 정보화 사회의 성숙기인 유비쿼터스 사회로의 진입을 눈앞에 두고 있다. 반면, IT 기술의 비약적 발전과 함께 이를 악용한 해킹, 웜 · 바이러스 등 사이버 위협 또한 첨단화 · 다양화 · 지능화되고 있는 실정이다. 지난 2003년 1월 25일 인터넷 마비사고와 2004년 주요 국가기관 해킹사건을 겪으면서 사이버위협의 파괴력이 국가안보에 직접적이고 심각하게 위협하는 단계에까지 도달하였다. 그래서 사이버테러나 사이버전(cyber warfare)은 더 이상 가상적 상황이 아닌 현실적이며, 실체적인 안보상황으로 상대국의 군사지휘체계는 물론 통신, 에너지, 금융, 수송체계 등 국가 주요기능 무력화의 전쟁 개념의 확대로 재인식되고 있다.

이러한 시점에서 정보전, 정보작전, 네트워크 중심전 등 혼재된 유사 용어들 속에서 사이버전에 대한 명확한 개념 정립 필요하고 각국의 사이버전 동향 분석 및 국내 사이버전 현황 분석을 통해 문제점을 식별, 보완책 마련이 필요하다. 그래서 본 논문에서는 국가적 위기를 효율적으로 관리하고, 효과적이며 능동적으로 사이버전을 수행할 수 있는 발전방향과 상대적으로 사이버전 관련 기술 및 전문 인력 운영적 측면에서 열세에 놓여있는 군의 사이버전 수행체계 혁신방향에 대한 연구를 하였다.

2. 사이버전 개념

2.1 일반적인 정의

정보테러리즘은 개인의 정보를 불법적으로 획득 및 이용하여 피해를 주는 것을 말하며 이는 정보화 역기능의 다양한 형태 중의 하나인 개인에 대한 사이버테러를 의미 시뮬라 전은 전쟁의 승패를 시뮬레이션 결과로 대신한다[1].

깁슨 전은 인간이 아닌 대리인(에이전트)끼리의 전쟁이라고 표현하였고, 시멘틱 공격은 표적 시스템의 물리적 또는 가시적인 변화 또는 손상 없이 정보시스템 또는 그 내부의 정보를 공격하는 형태이다. 또한 시스템을 정지시키거나 외적인 손상을 일으키는 해커전과 구별.

상기 4가지 형태의 사이버전을 통해서 볼 때 Libiki의 사이버전은 정보전의 한 분야로서 사이버 공간에서 이루어지는 공격 형태이나 정보시스템 또는 그 속에 내재된 정보의 내적인 공격(공격 여부를 외적으로 인지할 수 없는 형태의 공격)에 중점을 두었으며 방어적 개념은 제외 하였다[2].

Aquilla와 Ronfeldt는 20세기가 전격적 시대였다면 21세기는 사이버전 시대가 될 것이라고 강조하면서 "사이버전은 정보원칙에 따라 군사작전을 수행하는 것과 수행을 준비하는 것을 의미하고 적을 알기 위해서 의존하는 정보와 정보체계를 와해시키는 것을 말한다."라고 기술함으로써 지금의 정보작전 또는 지휘통제전과 유사한 개념으로 정의 한다[6].

2.2 한국군의 정의

합참은 사이버전을 "컴퓨터가 합성한 가상현실의 세계(Cyber Space)와 가상인간의 영역과 같이 인공지능체계가 운용되는 공간에서의 전쟁으로서 이는 정보화 사회의 과학기술 발전을 역이용하여 취약점을 공격함으로써 물리적인 군사시스템 파괴보다 훨씬 결정적인 손실을 강요할 수 있는 총체적인 가상공간에서의 정보 마비전을 추구하는 전쟁수행방식을 의미한다(합참, 1999)"라고 정의한다[3].

- 사이버전에서 정보 마비전을 추구하는 공격 개념만을 포함한 정의
- 지상전 또는 공중전과 같은 형식의 새로운 전쟁수행방식으로 보는 관점임

국방부는 사이버전을 "사이버 공간에서 일어나는 새로운 형태의 전쟁수단으로서, 컴퓨터시스템 및 데이터 통신망 등을 교란, 마비 및 무력화함으로써 적의 사이버체계를 파괴하고 아군의 사이버체계를 보호하는 것(국방부, 2002)"으로 정의[4].

- 정보 마비전을 추구하는 공격 개념 및 아군 사이버체계 보호를 동시에 강조함으로서 방어적 개념도 포함됨
- 사이버전을 국가 전 분야를 대상으로 하는 새로운 전쟁수단으로 개념을 정립하는 것이 타당할 것임

2.3 미군의 정의

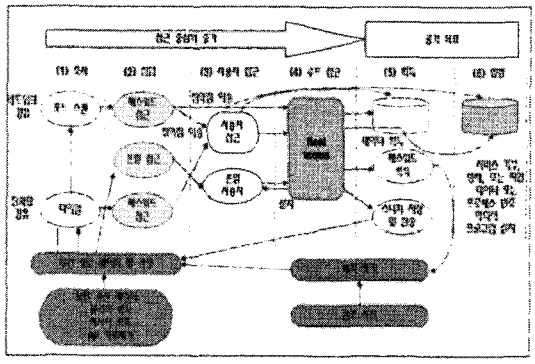
미군의 공식 문서상에 등장한 사이버전의 개념은 다양한 사이버전 유사 용어로 복잡하게 표현되는 듯 하나 정보작전 범주 내의 컴퓨터 네트워크 공격(CNA) 및 방어(CND) 그리고 정보보증(IA)으로 정리될 수 있다[6].

- 작전의 대상이 컴퓨터와 컴퓨터 네트워크 그리고 그 내부에 존재하는 정보임을 명시
- 작전의 목적을 단계적으로 방해, 거부, 감퇴, 파괴로 분류로 분류
- 작전 수행영역(공간)은 데이터 스트림에 의존한 컴퓨터 네트워크 공격
- 결론적으로, 미군의 사이버전은 정보작전의 일부로서 공격은 컴퓨터 네트워크 공격 형태로, 방어는 컴퓨터 네트워크 방어와 정보보증 형태로 수행됨

3. 사이버전 위협 및 분석

3.1 사이버전 위협 패턴

전형적인 사이버 위협 패턴은 (그림 1)과 같이 나타낼 수 있다.



(그림 1) 전형적인 사이버 위협 패턴

1단계 : 조사 단계
- 인터넷이나 기타 통신을 통해 접근 가능한 취약한 지점 조사

2단계 : 침입 단계
- 가용한 네트워크 접속점을 찾아 접속 시도 단계로 이미 알려진 취약점을 이용하거나 기획득한 정보를 이용하여 정상적 접속을 통한 침입

3단계 : 사용자 접근 단계
- 사용자 접근에 성공하는 단계로서 상당한 수준의 시스템 자원의 조사와 이용이 가능한 상태

4단계 : 루트 단계
- 시스템의 루트 권한을 획득하는 것으로 악의적인 행동을 즉각적으로 수행할 수 있는 모든 통제권을 가짐

5단계 : 획득 단계
- 스니퍼(sniffer) 프로그램을 설치하거나 관리자용 파일 또는 암호화된 패스워드 파일을 탈취하고 나아가 새로운 사용자 계정을 만들어 둠

6단계 : 영향 단계
- 마지막 단계로 표적시스템 내의 정보와 프로세스를 거부, 파괴, 방해하는 공격자의 의도하였던 목표를 달성하고 나아가 차후 작전을 위해 악의적인 프로그램을 설치

- 이러한 사이버전 위협 절차는 해커들의 시스템 침입행위와 매우 유사
- 사이버 위협 유형들은 웜·바이러스, 위·변조, 서비스거부 공격, 해킹 등이며, 이밖에도 군사적 부문에서 물리적 파괴 수단을 통한 사이버전을 수행
- 군사적 물리 수단 예시
  - 전자기펄스탄(EMP-Bomb) : 20억W 전력을 순간적으로 방출하여 반경 330m 이내 모든 전자장비 파괴
  - 정전폭탄(BlackOut Bomb) : 탄소섬유가 채워진 캔 형태의 자탄 200여개를 퍼뜨려 전력망 무력화

3.2 사이버 공격 원인 분석

전방위 사이버 공격에 대한 국가적 대응노력을 조정하는 凡국가적 차원의 컨트롤 타워가 부재하여, 조기 대응 미흡 및 피해확산 방지 미흡
- 중국발 해킹사고, 민간과 공공영역을 망라한 경유지 해킹, 1·25 인터넷 대란 등의 사태는 정부 부처간 대응 노력을 최상위에서 조정하는 컨트롤 타워 역할이 필요함을 시사하고 있음
- 이를 위하여 현재 부처별로 산재되어 있는 사이버 공격에 대한 대응업무의 책임과 권한을 한 부처에서 총괄할 수 있도록 부처 이기주의를 떠난 법적 지위 부여 필요

신종 웜, 봇넷, 방화벽 우회, 백도어(트로이 목마), 액티브 엑스 컨트롤을 이용한 해킹 등 대부분의 사이버 공격을 방지할 수 있는 사이버 공격 대응 기술 부재
- 체계적이고 일관적인 계획성 있는 사이버전 관련 기술 개발이 아닌 일회성 혹은 특정 사고 대응을 위한 임시방편적 기술 개발이 이루어지므로 원천기술 및 핵심기술 축적 기회를 상실
- 이메일 통한 사이버 공격, 사회공학적 해킹, P2P를 이용한 개인정보 및 중요정보 유출의 근본 원인은 사용자 보안 의식 결여
- 보안 패치 정기적 수행, 개인 PC 정보보호 수칙 준수 등 기본적인 보안 대책의 미준수로 인한 피해가 사이버 공격 원인의 상당수를 차지
- 온라인 게임 아이템 매매를 위한 해킹, 인터넷 뱅킹에 대한 사이버 공격, 피싱 및 파밍 등 금전적 취득을 목적으로 한 사이버공격은 정보통신 윤리의식 결여가 가장 큰 원인
- 우리나라 정보화 수준에 따라가지 못하는 정보통신 윤리의식 결여가 큰 원인이라고 판단됨
- 중국발 해킹, 중국·브라질 등 제 3국으로부터 우회공격 등에 대한 사이버 공격이 날로 증가하는 원인은 국제적인 사이버 공격 대응 공조체계 구축이 미흡하기 때문임
- 현재 NCSC, 법무부, 경찰청, KISA 등이 제각기 국제공조체계를 갖추고 있어, 업무공조의 혼선을 불러일으킬 가능성이 존재함
- 사이버전을 대비한 각 분야에서 단일화 된 국제공조체계 구축이 필요함

3.3 사이버전 현황 및 문제점

과거 이미 예견된 바와 같이 국가 간 전쟁은 재래식전에서 정보전으로 그 양상이 변화하고 있다. 전투기나 미사일 등을 동원하지 않고도 효율적으로 상대방을 제압할 수 있는 시대가 도래하였고 미국을 비롯한 선진국들은 정보전기술을 바탕으로 고도의 첨보전과 사이버전을 전개함으로써 정보전에서 우위를 차지하려고 치열한 경쟁을 벌이고 있다.

세계 각국은 사이버전을 수행하는 사이버전부대나 해커부대를 공식화하기에 이르렀고, 유력한 사이버무기들도 속속 개발되고 있다.

미국을 비롯한 영국, 중국, 프랑스, 러시아, 이스

라엘, 북한, 일본 등에서는 이미 1990년대 중반부터 준비 해왔다.

정보통신 인프라가 이루는 수천, 수만 개 노드의 사이버공간에서 국가 사이버위기관리체계는 정보 획득, 악의적 공격 행위의 감시 및 탐지, 위기대응 기술 개발, 사이버 범죄 수사 및 처벌 등 모든 예측 가능한 위협에 대하여 모든 역할을 수행하기 어렵기 때문에 명확한 역할 분장하의 체계적이고 조직적인 중앙집중식 관리체계가 요구된다.

그럼에도 불구하고, 국가 사이버전 관련 다양한 조직들은 정책·교육·기술적 측면에서 집중해야 할 역량들이 중복되어 효율성이 저하되고 있으며, 정보협력 및 교류프로그램 등을 통한 각 기관간의 연계 시도는 긍정적이나 이러한 조직간의 유기적인 공동체 구성이 이루어지지 않아 사이버공간에서 대비해야 할 위협들과 사이버범죄 및 사이버테러 행위에 대한 공동대응체계 구축이 미흡한 실정이다.

더욱 중요한 사실은 사이버 위협이 공공부문에서도 발생하지만, 민간부문에서는 아예 드러나지 않는 경우가 상당하다는 것이며, 이는 사이버공격에 대한 대비책 마련에 상당한 걸림돌로 작용하고 있다.

따라서 공공·민간부문에서의 각 조직간의 책임과 역할을 분명하게 정립하고 중복적인 요소를 제거하여, 정보통신 인프라의 체계적인 관리·운용이 이루어질 수 있도록 해야 하며, 중앙 집중식 관리체계 도입으로 사이버위협에 대해 보다 능동적 대응태세를 갖춰야 할 것이다.

한편, 군 관련 사이버전 대비 태세에서의 문제점은 국방 정보보호정책 수립·집행의 일관성 부족 및 중요성 인식의 부족에서 초래되는 것이라 판단되며, 최신 정보보호 기술 및 해킹, 바이러스 등 사이버전 위협에 대응하기 위한 실무적인 내용은 극히 미흡한 상황이다.

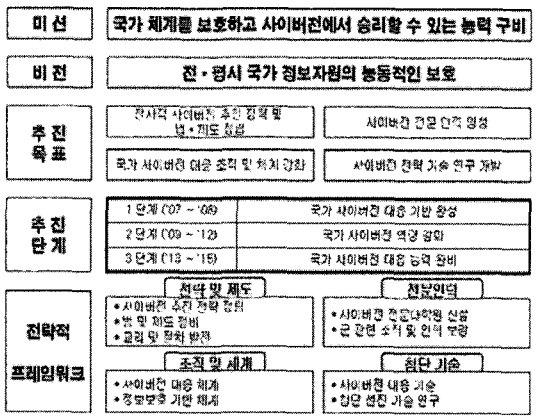
- 「군사보안업무 시행규칙」에서는 군사보안업무와 관련한 물리적/관리적 보안, 정보통신보안, 암호자재 운용관리 등의 내용만을 포함

또한 사이버전 관련 조직이 분산되어 있으며, 구성원의 정보보호 역량 부족으로 인해 최신 정보보호 기술 및 해킹, 바이러스 등 사이버전 위협에 대응하기 위한 기술 및 능력이 미흡한 상태이다.

4. 국가 사이버전 로드맵 설계

4.1 로드맵 설계

국내외의 사이버공격으로부터 국내의 국방, 정부, 민간부문의 정보체계와 중요 정보를 보호하고, 국가 사이버전 발전방향 제시를 위한 로드맵 설계하였다.



(그림 2) 국가 사이버전 로드맵

4.2 전사적 사이버전 추진 전략 및 법·제도 정립

10년 이내에 적의 사이버 공격으로부터 국가 핵심체계를 보호하고 사이버전에서 승리할 수 있는 국가 사이버전 체계를 구축·운영 하고, 국내·외 환경 변화에 효과적으로 대응할 수 있는 사이버전 관련 추진 전략, 법/제도 정비 및 교리 재정이 필요하다.

① 추진전략 정립

고유의 기능을 수행하는 다양한 정보보호 수단들을 적절히 배치, 활용하여 상호 취약점을 보완함으로써 궁극적 수준 목표 달성이 현실적이고 효율적인 접근방법으로 인식.

이와 같은 다수준·다계층 정보보호를 추진 전략으로 정립하고, 이를 구현하기 위한 구체적인 지침과 가이드라인의 개발과 보급이 필요.

사이버전 환경은 단위 시스템, 데이터 수준에서의 정교한 통제를 필요로 하기 때문에 전략 구현을 위한 지침과 가이드라인은 상위적 수준부터 하위적 수준까지, 각 수준별 세부통제 기준을 포함.

전사적 차원에서 상호 유기적으로 연계되기 위해 공통 네트워크, 시스템 방어 아키텍처 정립이 필요하며, 제반 정보보호 역량, 기능들의 중앙 집중적인 관리와 지속적인 기술 연구 개발이 요구됨.

② 법·제도 정비

현행 사이버 안전 관련 법령의 중복적용으로 관련 기관 업무의 혼란이 가중되고 있다는 비판이 제기.

기본법 제정 및 개별법 정비 등 다양한 의견이 제시되었으나, 현재는 개별법 정비와 새로운 규정(국가사이버안전관리규정)을 제정하여 시행하고 있음.

그러나, 사이버 안전 관련 법령의 개별법 정비로 접근할 경우, 법령 중복적용에 따른 관련기관의 업무혼란을 해소하기에 무리가 따를 것으로 예상

- 현 사이버 안전관련 업무 수행체계로는 국정원, 정통부 등 부처 간 업무 혼선 및 부처 간 협력관계 유지가 원활하지 못한 실정임

현행 개별법을 통합하여 단일법인 가칭 "사이버 안전기본법"을 제정하는 방향으로 추진하는 것이 바람직

- 정보통신기반보호법, 정보통신망이용촉진 및 정보보호에관한법률, 정보화촉진기본법, 전자정부법, 전자거래기본법, 국가안전보장회의운영 등에 관한 규정 및 국가사이버안전관리규정 등 현존 정보보호 관련 법률 등의 통합·단일화 추진.

③ 사이버 안전 관련 평가제도 강화

CCRA로 인한 민간/국외 정보보호제품의 국가기관 도입을 위한 보안적합성 시험 강화.

현행 정보보안 수준평가의 法的 시행근거 마련.

④ ISAC간 정보공유를 위한 강력한 法的 根據 마련

국가 사이버 안전 확보측면에서 부문 ISAC간 정보교류가 필수적이나, 현재 ISAC간 정보교류는 전무한 상태임.

현재와 같은 중대한 사고에 대해서만 관할 부처로 사고정보를 제공하는 비정기적 정보제공으로는 국가차원의 사이버 안보 위험수위를 판단하기에는 어려움이 있음.

- 정보통신기반보호법 및 정보통신망이용촉진 및정보보호에관한법률에 사고시 신고조항 규정

따라서, ISAC 간, 각 부문 책임 중앙행정기관, 국정원 등에 정기적 사이버 위협 정보 및 비정기적 사고정보 제공을 의무화하는 법적 근거 마련.

- ISAC간 원활한 정보공유를 위하여 Secure Clearing House 구축·운영에 관한 조항 명시
- 국가사이버안보청(과학기술보좌관) : 국가 사이버전 조정자 역할 수행할 중앙 조직 신설(가칭)

Clearing House를 통한 각 ISAC의 정보분석결과 결집 및 각 ISAC간 정보 분배 의무화.

⑤ 악의적 목적의 사이버 범죄행위에 대해 효율적 수사를 지원할 수 있는 수사체계 정비

사이버 범죄 증거 수집 및 활용절차, 가중처벌 조항 신설, 실질적 영향력 있는 재판관할권 적용방안 등 마련.

사이버 범죄자 이력 관리를 통한 억지력(deterrence) 확보 및 새로운 IT 기술을 활용한 위법행위 발생 시 이를 탄력적으로 수용할 수 있는 근원적 법제도 정비.

⑥ 국가 정보유출 및 이미지 손상에 대비한 실질적 영향력 있는 처벌조항 및 법적 제제근거 확보

국가의 주요정보 유출에 대해 『국가보안법』 등 관련법과 기본법에 처벌 근거 강화.

- 악의적 활동의 경유지 등으로 사용되는 경우 실질적 영향력을 가진 외국인 및 외국에 소재한 범죄수단에 대한 재판관할권 보장

⑦ 공공 및 민간영역이 보유한 개인정보의 안전한 유통 등 개인정보보호 강화를 위한 法的 根據 마련

- 각 기관의 개인정보보호 수준 평가를 위한 방법론 개발 및 결과 이행여부 점검을 위한 평가시스템 구축

국가·공공 및 민간영역의 보유 개인정보를 안전하게 하기 위한 기술 지원 및 가이드라인 제시.

⑧ 사이버전 교리 제정

- 군의 사이버전 효율적 수행을 위한 "사이버전 기본교리" 제정

- 사이버전 수행의 중심 요체인 합참 주관 기본교리 제정
- 합참교리를 근거로 하여 각 군은 사이버전 전략 및 전술 개발을 통한 각 군의 실정에 맞는 교리 발간 추진

4.3 국가 사이버전 대응 시스템 구축

① 적의 공격으로부터 국가 핵심체계를 보호할 수 있는 대응 시스템 구축

- 전사적 센서 그리드(ESG : Enterprise Sensor Grid)개발 배치

② 국가 핵심 시스템과 네트워크가 자기방어 능력을 갖출 수 있도록 위협요소, 취약점 및 결함에 대해 즉시 인지, 반응 및 대응할 수 있는 센서 그리드 개발 배치

- 국가 네트워크 방어 구조와 기준에 따라 센서 그리드 배치
- 센서 그리드를 기반으로 실시간 위협분석 실시
- 센서 그리드 운용에 대한 매뉴얼 개발 및 배포

③ 효과적 예·경보 및 대응 체계 확립

- 사이버 위협 조기 예·경보 기능 강화
- 현재 운영되는 NCSC 상황실 기능의 고도화를 통하여 사이버 위기 사전파악

- 트래픽 수집 및 분석을 통한 침입사전 분석

- 예보 및 경보 상황에 따른 조치 전파
- 민·관·군 합동으로 취약요소를 발굴하고 개선사항 권고
- 민·관·군 합동 Red team을 구성하고, Internet Security Test를 수행하는 등 주기적인 사이버 안전 준비태세 평가

⑤ 청와대(사이버안보보좌관) 또는 국가정보원 주관의 사이버 위기 대응 모의 훈련 실시

- 청와대 내 사이버안보보좌관제 신설을 통한 체계적 훈련 주관, 신설 전까지 과학기술보좌관 역할 수행 필요
- 반기별 1회 불시 위기경보 발령 후 각급기관의 대응태세 점검

- 표준매뉴얼에 근거한 대응태세 점검

⑥ 사이버 안전을 위협하는 대규모 피해 발생을 대비한 각 기관별 사이버 보안 비상계획 수립 의무화

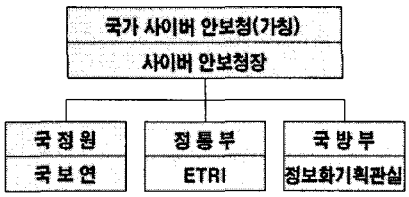
⑦ 사이버 안전 비상계획에 피해 최소화 및 복구 대책 포함
- 국가 주요정보자산 전자지도(Digital Map) 작성
  - 자산의 중요도 및 연계관계를 표현
- 주요 정보시스템의 생존성 확보 방안 마련
  - 주요 정보시스템의 다중화 구성
  - 주요 정보 데이터베이스의 미러링 및 백업
  - 주요 정보통신기반의 복구 및 재구성을 위한 별도의 비상망 운용

⑧ 공통상황도 프로그램 개발
- 통합 상황 인식과 중앙 지휘 통제 : 사이버전 지휘관(가칭 국가사이버안보청장)이 다양한 환경에서 사이버전을 수행할 수 있도록 공통상황도(CSP : Common Situation Picture) 프로그램과 사이버전 수행 프로그램의 통합으로 중앙 집권적 지휘 통제 보장

⑨ 실시간 의사결정 프로그램 개발
- 사이버전 관련 실시간 의사결정 수립 프로그램 개발을 통한 신속 대응 보장

〈표 1〉 영역별 피해복구 운영절차

피해복구단계	주요내용
1단계 : 사고성격 규정 및 피해규모 산정	- 피해 대상 범위, 피해규모 산정 - 공격 진원지 및 공격자 식별 - 공격 의도 추정
2단계 : 사고성격 및 피해규모에 따른 대응 및 복구방법 선택	- 전자지도를 활용하여 중요도, 시의성, 시급성 등을 고려한 조치 우선순위 결정 - 피해규모를 최소화 할 수 있는 대응 방법 선택 및 조치 시행
3단계 : 대응 및 복구조치 시행	- 업무 연속성 보장을 위한 신속한 복구 방법 선택 및 조치 시행



(그림 3) 국가사이버전 대응 체계

⑩ 중앙 집중형 조직 강화
- 국가사이버안보청장을 「국가 사이버전 조정자」로 임명하여 同 조정자를 중심으로 한 대응 체계 정립
  - 현재 국가·공공분야, 국방 분야 및 민간분야로 나누어져 있는 사이버 안전 관련 의사결정체계를 사이버안보청 중심으로 일원화
- 국가사이버안보청 발족 이전에는 동일 역할을 청와대 "과학기술보좌관 또는 안보실장"이 담당
  - 국정원(또는 청와대) 내 사이버위기 시뮬레이션 센터 설립
  - 새로운 사이버 위협에 대해 정보통신 자산에 대한 모델링을 통해 사전에 피해 가능성을 평가하고, 피해규모를 예측할 수 있는 사이버위기 시뮬레이션 센터를 설립 추진
  - 사이버위기 시뮬레이션 센터 내에 사이버워 게임 모의훈련 연습장을 구축·운영하여 평시 사이버 위기 대응훈련 실시
- 민간 영역을 포함한 국가사회 전 영역에 대한 사이버 위기 대응 업무 총괄 수행
  - 사이버 위기 대응정책 수립·조정 및 시행
  - 국가·공공분야, 국방 분야 및 민간분야 사이버 위기관련 정보 수집·종합 판단 및 경보 발령
  - 범국가적 차원의 사이버 위기관련 상황 모니터링
  - 사이버 위기 대응기술개발 계획 수립·조정 및 시행

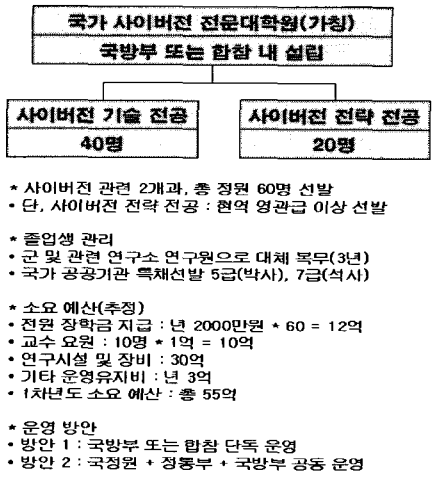
- 사이버 위기 발생 시 종합대책본부 구성 및 운영 등

⑪ 국방부 조직 및 역할 강화
- 합참에 사이버 위기에 대한 전·평시 사이버전을 지휘, 통제할 수 있는 사이버전 지휘통제소 구축
  - 현 국군기무사령부의 국방정보전대응센터는 취약점 분석, 국방 사이버 침해행위에 평시 대응 업무에 주력
- 사이버전 지휘통제소 주요 임무
  - 평시, 국방 CERT를 지휘 통제하여, 군내 사이버테러 대응 업무 총괄 수행
  - 전시, 정보작전 상황 하에서 공세적·수세적 사이버전 지휘, 통제 업무 수행
  - 사이버전 종합상황실 운영
- 사이버전을 전담 대응하는 사이버군 창설
  - 공세적 사이버전 업무를 담당하는 컴퓨터·네트워크 공격 부대와 수세적 사이버전 업무를 담당하는 컴퓨터·네트워크 방어 부대 신설

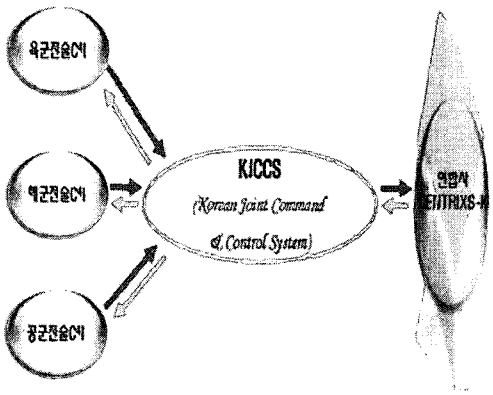
4.4 사이버전 전문 인력 양성

① 민·관·군 소요 인력 충원 방안 : 가칭 "사이버전 전문대학원" 개설

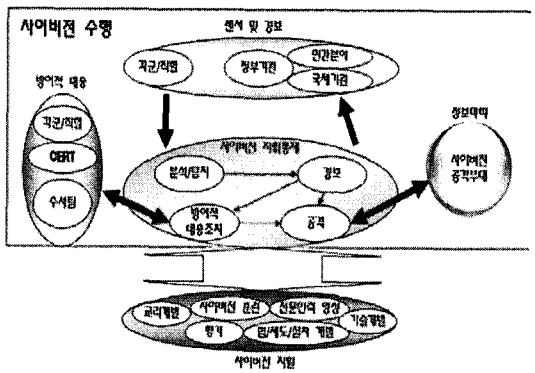
② 군 인력 충원 방안
- 정보보호분야 전공자 특채를 통한 국방부/각 군 CERT팀 조직 강화
- 각 군 대학 및 국방대 내 사이버전 전문 인력 양성 과정 개설
- 합참 내 사이버전 공격 부대 창설
  - 합참의 합동지휘통제시스템을 중심으로 각 군의 C4I체계 및 연합사 C4I체계가 연동되므로 사이버전의 중심은 합참임
- Korean Joint Command & Control System (합동지휘통제시스템)



(그림 4) 국가 사이버전 전문대학원



(그림 5) 합참의 합동지휘통제시스템



(그림 6) 전시 합참 중심의 사이버전 수행 체계도

4.5 사이버전 전략 기술 연구 개발

① 혁신을 통한 첨단 기술 개발
- 이종 데이터 융합(Heterogeneous Data Fusion) 기술 개발
  - 임의의 목적에 부합되도록 입력데이터를 분석하여 메타데이터를 생성하는 데이터 융합기술을 이용하여 사이버공격 위협 예측에 활용

② 안전한 자동제어(SCADA) 시스템기술개발
- 전력, 가스, 급수, 댐 및 대규모 플랜트의 자동제어를 위한 SCADA 시스템의 보안기술 개발

③ 트래픽 수집, 분류 및 분석을 통한 침입탐지 기술 개발

④ 공격자 역추적 기술 개발

⑤ 사이버전 관련 기술을 선도할 수 있는 전략기술 개발
- Lightweight 침입탐지 센서 개발
- secure 클러스터 기술 개발
- 침입감내(Intrusion Tolerant) 네트워크 기술 개발

⑥ 사이버전 모의 훈련 프로그램 개발

4.6 연구개발 절차(案)

① 중장기 계획 수립은 청와대 과학기술보좌관주관 하에 국책연구기관이 작성

② 각 부처는 기술조사서를 바탕으로 필요 기술에 대한 소요제기

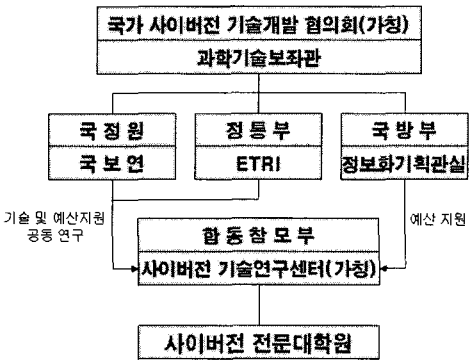
③ 대통령 직속 "국가 사이버전 기술개발 협의회(가칭)"를 신설하여 중장기 계획 확정

④ 국책연구기관은 통합 중장기계획을 바탕으로 「연구개발과제 심의 · 조정기구」에 과제 신청

⑤ 「연구개발과제 심의 · 조정기구」는 신청된 과제의 중복성, 효율성, 필요성, 경제성 등을 고려하여 과제부여

⑥ 연구기관은 과제 부여된 기술에 대한 연구개발을 수행하고 수행결과를 「연구개발 평가기구」에 제출

⑦ 「연구개발 평가기구」는 개발 결과물에 대한 평가를 수행하고, 과제 지속 여부
- 활용방안에 대한 건의를 포함한 평가보고서를 「연구개발과제 심의 · 조정기구」에 제출
- 「연구개발과제 심의 · 조정기구」에서 연구개발 결과에 대한 최종 심의가 완료하여 기술개발 성격에 따른 조치 수행
- 국가기관 소요제기 기술 : 제작업체 지정을 통한 기술전수
- 첨단 · 공통 응용기술 : 업체 기술이전



* 사이버전 기술연구센터 운영방안
• 추진 1단계('07~'08) : 국보연 및 ETRI 전문연구요원 파견
이후, 합참 요원으로 자체 운영

(그림 7) 연구개발 체계도

4.8 가칭 「사이버전 기술개발 기금」 조성 검토

① 사이버전 기술개발을 위한 안정적 예산 확보 및 지원 필요
- 사이버 안전을 위협하는 요소가 날로 증가함에 따라, 대응기술 또한 신속하게 개발되어야 하며, 첨단기술이 요구되므로 안정적 연

구재원 마련이 필요한 실정임

- 사이버전 관련 기술은 국방, 행정, 금융, 민간 통신사업 등 정보통신시설을 기반으로 하는 모든 기관에 공통적으로 적용 가능하므로, 정보통신기반시설을 관장하는 기관을 중심으로 가칭 「사이버안전 기술개발 기금」을 조성
- 국방부의 경우, 사이버전 기술 연구개발과 관련하여, 국방 투자비의 일부를 활용하기 위한 제도 정립
  - 국가 사이버전 관련 연구는 대외적으로 보안성이 요구되는 분야이므로, 국가주도의 안정적 예산지원이 필요

5. 결 론

첨단 사이버전 위협 분석 및 국가안보에 미치는 영향을 분석 조사 하였고, 유관 기술과 전략개념의 국내 적용 가능성을 첨단 정보전에 대비한 국내 사이버안보 기반 강화 방안으로 연구하였다. 국내외 사이버전쟁 역량 및 안보전략을 분석하여 정보 인프라 및 국내 기구·조직의 설치·개선방안 등을 제시하였고, 또 연구자들이 공동으로 연구방향을 확립할 수 있도록 관련 개념 및 분석틀에 대한 이론적 기반을 구축 하였다. 앞의 분석결과와 평가를 토대로 향후 국가의 미래 사이버전에 대비한 사이버안보 개선 정책 및 강화전략에 대한 대안들을 제시하였다.

끝으로 위 전략을 위해서 사이버전 기술 개발 기금 조성으로 총체적인 지원을 요구하였다. 본 논문의 로드맵이 국가 사이버전에서 안전하게 수행되길 고대한다.

참 고 문 헌

[1] 노훈, 이재욱, "사이버전의 출현과 영향, 그리고 대응방향", 국방정책연구, p. 188, 2001.

[2] Martin C. Libichi, "What Is Information Warfare?", Strategic Forum, No. 28.

[3] 황호상, "이라크전에서의 정보전분석", 국가사이버 안보정책과 전략, 제3회 사이버테러정보전 컨퍼런스, pp. 6-18, 2003.

[4] 합참, 합참 비젼 2015 합동전장 운용개념서, 1999.

[5] 남길현, "사이버테러와 국가안보", 국방연구, 제45권, 제1호, 국방대학교, 2002.

[6] Edward Waltz, Information Warfare Principles and Operations, 1998.

김 귀 남

미국 캔자스대학 수학과 (응용수학사)

미국 콜로라도주립대학 통계학과 (통계학석사)

미국 콜로라도주립대학 기계산업공학과(기계·산업공학 박사)

현재 경기대학교 정보보호학과 교수