시스템 사고를 이용한 사이버전 보안 정책 레버리지 전략 연구

양호경* · 차현종* · 신효영** · 박호균*** · 유황빈****

요 약

정보기술의 발전에 따라 전쟁의 양상이 무기체계 위주 재래식 전쟁에서 네트워크를 기반으로 한 네트워크중심전(NCW)로 바뀌어 가고 있다. 전장의 개념 또한 물리적 공간뿐만 아니라 군사시설, 에너지시설, 교통, 통신망 등 국가 기간산업의 전산망을 비롯한 모든 영역을 포함하는 것으로 변모하고 있다. 변화하는 전쟁 수행 개념과 방식의 발전추세에 비추어 볼 때 우리 군은 사이버전 위협에 효과적으로 대응할 수 있는 방안을 모색하여야 한다. 기존에는 사이버전에 대한 부분적인 전략은 연구되었으나 시스템 전반적인 흐름을 통한 연구는 이루어지지 않았다. 본 논문에서는 사이버전 보안 관련 주요 변수들을 인력, 운영, 기술로 구분하여, 각 분야별 단순모형과 확장모형을 제시하고 제시된 확장모형 중 기술분야를 중심으로 정형기법을 사용하여 타당성을 검증하고 식별된 레버리지에 따른 구체적인 대응 전략을 제시하고자 한다.

A Leverage Strategy of the Cyber warfare Security Policy Based on systems Thinking

Ho-Kyung Yang* · Hyun-Jong Cha* · Hyo-Young Shin** · Ho-Kyun Park*** · Hwang-Bin Ryou****

ABSTRACT

As the network composed of numerous sensor nodes, sensor network conducts the function of sensing the surrounding information by sensor and of the sensed information. The concept of the battlefield is also changing to one that includes not only physical spaces but all areas including the networks of the nation's key industries and military facilities, energy facilities, transportation, and communication networks. In light of the changing warfare in terms of how it is conducted and what form it takes, the Korea military has to seek ways to effectively respond to threats of cyber warfare. In the past, although partial strategies on cyber warfare were studied, no research was done through the overall system flow. In this paper, key variables related to cyber warfare security are classified into personnel, management, and technology. A simple model and an extended model are suggested for each area, and based on the technology area of the extended model, formal methods are used to verify the validity and a detailed response strategy is suggested according to the identified leverage.

Key words : Systems Thinking, Cyber warfare

접수일(2013년 9월 2일), 수정일(1차: 2013년 9월 14일, 2차: 2013년 9월 27일), 게재확정일(2013년 9월 27일)

* 광운대학교 방위사업학과
** 경복대학교 IT보안과
*** 신흥대학교 컴퓨터정보계열
**** 광운대학교 컴퓨터 과학과

1. 서 론

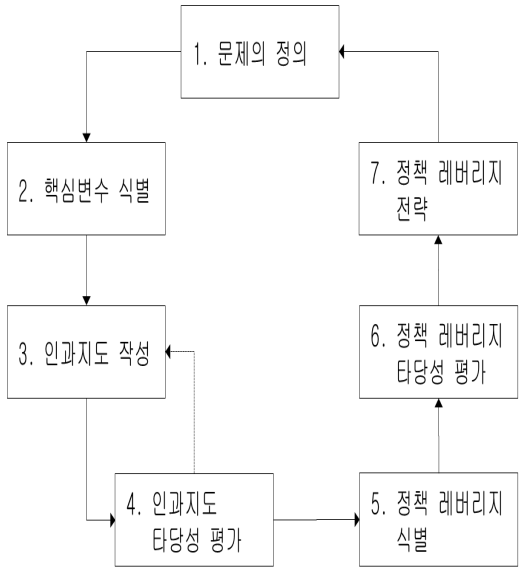
정보통신 기술의 발전에 따라 미래 전장 수행개념은 비접적, 비선형, 원거리 전투, 네트워크 중심 전쟁, 병렬, 동시· 통합작전 그리고 효과 중심의 신속 기동전 형태로 변화하고 있다. 전쟁의 양상도 무기체계 위주의 재래식 전쟁에서 각 무기체계 및 관련 시스템이 서로 연결되어 있는 네트워크 중심전(NCW : Network Centric Warfare)의 개념으로 변하고 있다. 군에서는 임무의 특수성으로 인해 독자적인 전용 지휘통신망을 발전시키고 있었다. 미래 전장 수행개념은 비접적, 비선형, 원거리 전투, 네트워크 중심 전쟁, 병렬, 동시· 통합작전 그리고 효과 중심의 신속 기동전 형태로 변화하고 있다. 이런 세계적인 발전방향에 부합하고 북한은 물론 다양한 미래의 위협에 능동적으로 대비하기 위하여 우리군도 장거리 정밀타격과 지·해·공 입체 공격능력을 향상시키고 생존성을 보장하기 위한 방향으로 전력구조를 발전시키고 있다. 이러한 혁신적인 발전과 더불어 군의 전쟁수행 환경도 빠르고 다양하게 변화하고 있다. 새로운 정보기술의 발전은 21세기 변화된 형태의 전쟁을 수행하기 위해 군 정보통신분야의 적용이 필수적이며 이를 통해 전술적인 감시나 추적 또한 전장정보의 실시간 수집 등의 효과를 공유하기 위하여 노력하고 있다. 그러나 이러한 네트워크 발전과 같이 보안적인 위협도 늘어나고 있는 실정이다. 네트워크가 확장됨에 따라 공격할 수 있는 루트도 증가하게 되고 이동하는 데이터의 양도 증가함에 따라 유출되면 위험한 데이터의 양도 증가하게 된다. 단순한 데이터 유출을 위한 침입이 아닌 사이버전 양상의 네트워크상의 전쟁이 일어날 가능성도 날로 증가하고 있는 실정이다. 특히 군과 같은 정보와 데이터가 중요한 집단에서는 사소한 정보 유출도 큰 위험으로 나타날 수 있기 때문에 다른 네트워크 환경보다 보안을 중요시해야 한다[1].

본 논문에서는 시스템 사고 방법론을 이용하여 사이버전 보안 전체 시스템을 이루는 주요 변수를 선정하여 인력, 운영, 기술로 구분하고, 각 분야별로 변수들의 인과관계를 단순모형과 확장모형을 제시하고 제시된 확장모형 중 기술 분야를 중심으로 정형기법을 사용하여 타당성을 검증하고 식별된 레버리지에 따른 구체적인 대응 전략을 제시하고자 한다.

2. 관련연구

2.1 시스템 사고

시스템 사고란 시스템의 작동 메커니즘을 직관적으로 파악하여 시스템을 효과적으로 변화시킬 수 있는 전략을 발견하기 위한 사고방식이다.



(그림 1) 시스템 사고 방법론의 연구절차

시스템 사고의 근본적인 목적은 문제의 원인에 대한 근본적 진단과 해결책을 제시하는 것이고 연결을 위한 모형을 제시하는 것이다. 시스템 사고의 연구절차는 (그림 1)과 같다. 연구 절차 중에서 문제의 정의, 인과지도 작성까지는 시스템 다이나믹스 연구절차와 동일하다. 그러나 모형의 구축 단계에서 시스템 사고 기법에서는 시뮬레이션을 위한 스톡 앤 플로우 다이어그램을 구축하지는 않는다. 다만 관심의 대상이 되는 시스템의 전체적인 구조적인 문제를 파악하고 정책 레버리지를 식별하기 위한 인과지도를 작성하며 작성된 인과지도에 대한 타당성 평가를 시행한다. 정책 레버리지를 식별한 이후에 식별된 레버리지에 대한 타당성 평가를 수행하고 전략을 구체적으로 수립한다[2][3][4][5].

2.2 사이버전

사이버전이란 단순히 컴퓨터 시스템을 파괴하는 것 뿐만 아니라 이에 의존하는 물리적 체계 및 기반시설까지 영향을 주는 것을 말한다. 사이버전의 형태는 행위의 주도권이 어느 편에 있는가에 따라 사이버 공격과 방어로 구분이 되며, 사이버 공격은 다시 해킹과 물리적 파괴로 나뉜다. 사이버 방어는 정보보호와 물리적 방호로 세분화된다. 국가의 정보 기반구조가 잘 갖추어져 있고, 정보기반 처리체계와 사회의 주요 시스템이 컴퓨터에 의존하는 정도가 높은 나라일수록 사이버공격의 가능성과 피해 정도도 높을 수밖에 없다. 과거의 전쟁형태와 비교할 때, 사이버 전쟁은 상대방의 신념과 지식 체계를 공격하기 때문에 전투의 전개 과정을 단계적으로 상상하거나 그 결과를 정확하게 예측하기가 어렵다[6][7].

2.3 정형기법

정형기법은 전산학과 소프트웨어 공학에서 사용되는 소프트웨어와 하드웨어 시스템의 명세, 개발, 검증을 위한 수학적 기반의 기법이다. 정형기법 사용을 통해서 시스템이 가질 수 있는 불일치성, 모호성, 불완결성을 찾음으로써 시스템의 이해를 증가시킬 수 있다. 정형기법은 요구사항 내에 존재하는 결함들의 잘못된 해석으로 인해 발생할 수 있는 문제점을 초기에 바로잡고 올바른 요구사항을 작성할 수 있게끔 한다.

또한 정형기법은 시스템/소프트웨어의 특정 속성(기능적, 안전성)이 만족되는지를 수학적인 방법으로 검증하며, 특히 정형 언어로 작성된 명세는 자동 검증이 가능한 이유에서 잠재적으로는 모든 공학 분야에서 적용이 가능하다. 정형기법은 크게 여러 가지로 분류가 될 수 있는데, 이것은 사용 목적이 표현적인지 또는 분석적인지에 의해서 분류할 수 있고, 정형화의 정도에 따라서 사용되는 명세언어가 대수 기반인지 모델 기반인지에 따라서 분류될 수 있다[8][9].

3. 시스템 사고에 기초한 사이버전

3.1 문제의 정의

최근 세계적인 양상을 볼 때 전쟁이 전면전보다는 테러전의 양상을 나타낸다는 것은 이미 널리 알려진 사실이다. 사이버 공간에서의 해킹 및 바이러스 역시 2000년대에 들어와 사이버 테러의 양상을 나타내고 있다. 세계는 이미 보이지 않는 사이버 안보 전쟁이 일어나고 있다. 사이버 공간에서 사이버 전쟁은 실제 일어나기 희박할지 모르지만 기존의 전쟁 무기의 일환으로 컴퓨터 바이러스 등이 사용될 가능성이 있고, 사이버 테러의 수단으로 활용될 가능성은 더욱 커지고 있다.

따라서 국내에서도 인터넷을 경유한 중요 정보 기반구조에 대한 공격 등 실제 정보전을 예측하여 대응방법을 훈련할 수 있는 도구를 개발하고 해커들의 해킹공격과 대응방법, 관련 정보보호 대상 정보 등을 데이터베이스로 관리하며 새로운 해킹공격 동향 등을 사전 예측해 경보를 발생 할 수 있는 방안이 필요하다.

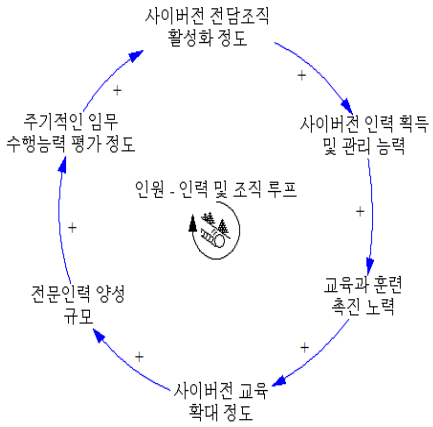
3.2 핵심 변수 선정

시스템 사고는 전체 구조를 파악하는 것을 목표로 하기 때문에 세부 형태를 알아보기 위한 구조 파악을 위하여 인과지도를 작성해야 하며, 인과지도의 작성을 위하여 시스템을 구성하는 핵심 변수를 도출해야만 한다. 핵심 변수를 도출하는 방법은 관련 논문이나 연구보고서, 관련자들과의 심층면담 또는 설문 등을 통해 이루어진다. 핵심 변수를 선정하기 위한 주요 변수를 우선 식별하고 종심방어 전략에서는 정보보증 달성을 위하여 인원, 운영, 기술 등 3대 요소로 분류한 후 주요 변수 중에서 중복되거나 덜 중요한 것을 제거한 핵심 변수를 확정하게 된다.

3.3 인과지도 작성

3.3.1 인원 분야의 단순모형

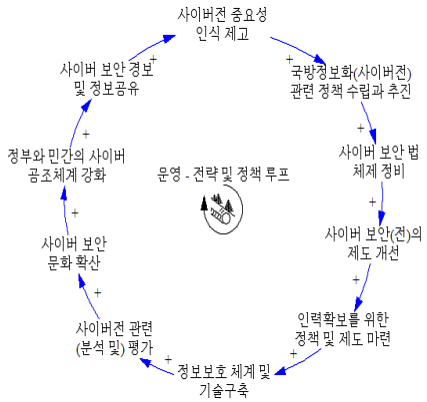
(그림 2)는 인원분야의 단순모형이다. 기존 연구에서 나타난 것과 같이 사이버전에서의 인원(인력)에 관한 내용은 많은 영향을 미친다. 사이버전은 단순히 고가 장비나 무기를 얼마나 많은 소유하고 있는지가 아닌 그것을 얼마나 효율적으로 사용하는지가 가장 중요한 문제이기 때문에 인원에 대한 분야가 중요시된다. 인원 분야에 대한 루프는 자기강화 루프로서 전체적으로 양(+)의 영향을 미친다.



(그림 2) 인원 분야의 단순모형

3.3.2 운영 분야의 단순모형

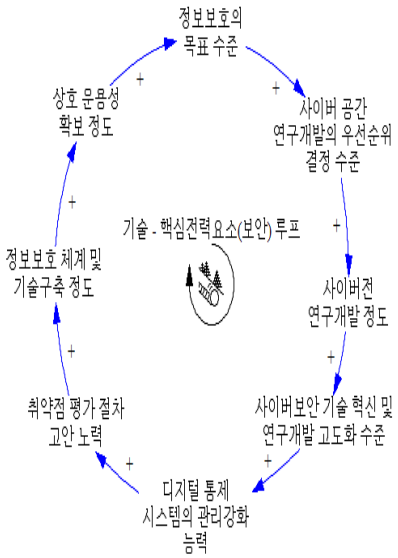
(그림 3)은 운영분야의 단순모형이다. 기존 연구에서 사이버전을 어떠한 방식으로 운영하면 좋을지 많은 의견이 나와 있다. 운영 분야에 대한 루프는 자기강화 루프로서 전체적으로 양(+)의 영향을 미친다.



(그림 3) 운영 분야의 단순모형

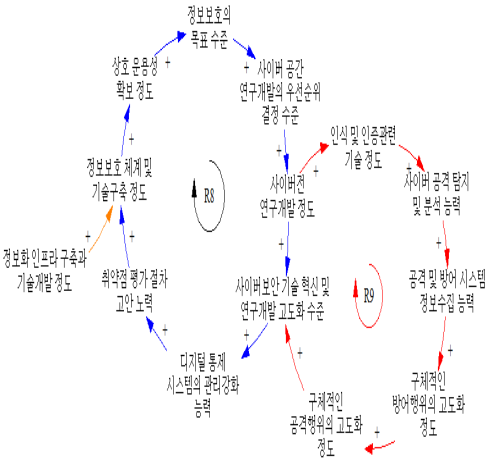
3.3.3 기술 분야의 단순모형

(그림 4)는 기술 분야의 단순모형이다. 기술 분야에 대한 루프는 자기강화 루프로서 전체적으로 양(+)의 영향을 미친다. 먼저 사이버전 보안을 이루기 위하여 기반이 되는 정보보호의 목표 수준 결정이 이루어져야 한다. 이것을 기반으로 사이버 공간 연구개발의 우선순위가 결정되고 이 순위에 맞춰 연구개발이 이루어지며 사이버 보안 기술 혁신 및 연구개발 고도화가 이루어진다. 또한 디지털 통제 시스템의 관리가 강화되고 취약점에 대한 평가가 이루어지며 정보보호 체계 및 기술이 구축된다. 이어서 상호운용성을 확보하면 전체적인 사이버전 보호가 이루어진다.



(그림 4) 기술 분야의 단순모형

3.3.4 기술 분야의 확장모형



(그림 5) 기술 분야의 확장모형

기술 분야의 확장모형은 (그림 5)와 같이 총 2개의 루프로 형성되어 있다. 각 루프를 형성하는 변수들 간의 연관성을 보면, R8 루프를 중심으로 여러 개의 루프가 형성되어 있다.

기술 분야에 대한 루프는 자기강화 루프로서 전체적으로 양(+)의 영향을 미친다.

4. 사이버전 모형 평가

4.1 확장모형의 타당성 평가

본 논문에서는 전체 모형의 타당성을 평가하지 않고 기술 분야에 대한 타당성만을 평가하려고 한다. 검증기준은 국제적으로 사용되는 정보보호시스템 공통평가기준인 CC를 기반으로 중복되는 평가 활동을 배제한다. 핵심 변수를 명확히 정의하여 오해가 발생할 소지를 줄이고, 실제 기술 측면에 대한 평가 활동을 재구성하며 필요할 경우 새로운 공통평가의 기준 요구사항을 추가한다.

평가기준은 기술명세서로 세분화한다. 우선 기술명세서는 각 변수별로 용어를 정의하고 그에 대한 기준 요소를 단계적으로 분류한다. 사이버전 기술 분야의 수준을 책정할 수 있는 과정을 위한 공식은 (식 1)과 같다[10].

$$x = \sum_{k=1}^{n} M_{k1} + M_{k2} + \cdots + M_{kn} \quad (식1)$$

* 수식의 각 기호의 설명
: 현재 기술 분야의 요소를 책정한 점수
: 요소의 수
: 번째 요소
: 각 요소에서 책정된 점수

(표 1) 전체점수 구성

요소	점수
1. 정보보호 목표 수준	15
3. 사이버전 연구개발 정도	25
3-1. 인식 및 인증관련 기술 정도	15
3-2. 사이버 공격 탐지 및 분석 능력	20
3-3. 공격 및 방어시스템 정보수집 능력	15
3-4. 구체적인 방어행위의 고도화 정도	15
3-5. 구체적인 공격행위의 고도화 정도	15
4. 사이버보안 기술 혁신 및 연구개발 고도화 수준	40
5. 디지털 통제 시스템의 관리강화 능력	10
6. 취약점 평가 절차 고안 노력	5
7. 정보보호 체계 및 기술구축 정도	5
8. 상호운용성 확보 정도	25
총 배점	205

기술 분야에 대한 변수들의 총 배점은 (표 1)과 같다. 점수는 1점부터 최대 5점으로 책정된다. 각 변수는 나뉠 수 있는 세부항목으로 나뉘어 평가된다. 변수마다 할당된 배점이 다른 것은 이러한 세부항목의 수가 다르기 때문이다. 즉, '정보보호 목표 수준'은 세 가지의 세부 평가항목으로 나뉘어 평가된다. 또한, '사이버전 연구개발 정도'는 평가항목을 다섯 가지로 나뉘어 평가되기 때문에 점수 배점이 25점이 되는 것이다.

4.2 레버리지 전략

기술 분야 루프의 변수들을 살펴본 결과 기술 분야의 적정한 첫 번째 전략 지점은 암호화 수준의 향상이라고 하겠다. 앞으로도 정보보호 목표수준은 계속적으로 향상 될 것이고 이에 따라 암호화 수준을 향상시켜 높은 목표수준을 유지할 수 있도록 할 것이다.

기술 분야의 적정한 두 번째 전략 지점은 적절한 연구인력 확보라 하겠다. 사이버전의 연구개발 정도를 향상시키기 위하여 많은 연구개발과 노력이 필요하다. 이러한 연구개발을 이루기 위하여 우선 기본적으로 적정한 연구 인력을 확보해야 한다[11].

5. 결 론

전쟁 수행 개념과 방식의 발전추세에 비추어 볼 때 우리 군은 사이버전 위협에 효과적으로 대응할 수 있는 방안을 모색하여야 한다. 기존에는 사이버전에 대한 부분적인 전략은 연구되었으나 시스템 전반적인 흐름을 통한 연구는 이루어지지 않았다. 본 논문에서는 사이버전 보안을 파악해 보기 위해서 연구방법론 중 시스템 사고 방법론을 이용하여 사이버전 보안 전체 시스템을 이루는 주요 변수들을 식별하고 핵심변수로 뽑힌 각 요소들을 인원, 운용, 기술을 중심으로 분류하였다. 분류된 핵심변수별로 변수들의 인과관계를 단순모형과 확장모형으로 작성하여, 사이버전의 전체 구성을 가시화해보았다. 기술 확장모형의 각각의 요소들을 명세화 하고 점수를 배점하여 그 합계와 전체 요소의 관계를 검증하고 식별된 정책 레버리지에 따른 구체적인 전략을 제시하려 한다.

본 논문에서 제시된 사이버전 보안의 전체적인 구조와 기술 분야에 투입할 수 있는 레버리지 전략을 이용하면 사이버전에 대비하는 법・제도뿐만 아니라 정책 수립을 할 때 기본 자료로 사용될 수 있을 것이다.

참고문헌

[1] 나재훈, 채기준, 정교일, “센서 네트워크 보안 연구 동향”, 전자통신동향분석 제20권 제1호 통권91호, pp112-122, 2005

[2] 김도훈, 문태훈, 김통환, “시스템 다이나믹스”, 대영문화사, 1999.

[3] 김동환, “시스템 사고”, 선학사, 2004.

[4] Richmond, B. “System Thinging: Critical Thinking Skills fr the 1990s and Beyond”, Systems Dynamics Review, 1993.

[5] Richardson G. P., “Feedback Thoght in Social Science and Systems Theory, Philadelphia”, The University of Pennsylvania Press, 1991.

[6] 김학권, “군 사이버전 수행을 위한 사이버 전사 양성방안”, 경희대학교 경영대학원, 2008.

[7] 정현수, 사이버 전쟁에 대한 능동적 대응방향 연구, 숭실대 정보과학대학원, 2001.

[8] 이혁, “안전 필수 시스템 개발을 위한 정형기법 기반 개발 프로세스”, 고려대학교 대학원, 2008.

[9] 정금택, “정형기법을 이용한 위기대응 매뉴얼 신뢰성 향상”, 고려대학교 대학원, 2010.

[10] CCRA 관리위원회, “CC(Common Criteria for Information Technology Security Evaluation), 정보보호시스템 공통평가기준 v3.1 개정4판”, CCRA, 2012.

[11] 양호경, "사이버전의 기술적 보안정책 레버리지 전략연구", 광운대학교 대학원, 2013.

[저 자 소 개]

양 호 경 (Ho-Kyung Yang)

2005년 광운대학교 컴퓨터 소프트웨어학과 공학사
2007년 광운대학교 컴퓨터과학과 공학석사
2010년 광운대학교 방위사업학과 공학석사
2013년 8월 광운대학교 방위사업학과 공학박사

email : porori2000@nate.com

박 호 균 (Ho-Kyun Park)

1987년 광운대학교 전자계산학과 이학사
1989년 광운대학교 전자계산학과 이학석사
1998년 광운대학교 전자계산학과 이학박사
1992년~현재 신흥대학교 컴퓨터정보계열 교수

email : hkpark@shc.ac.kr

차 현 종 (Hyun-Jong Cha)

2005년 광운대학교 컴퓨터소프트웨어학과 공학사
2008년 광운대학교 컴퓨터과학과 공학석사
2011년 광운대학교 방위사업학과 공학석사
2011년~현재 광운대학교 방위사업학과 박사과정

email : chj826@kw.ac.kr

유 황 빈 (Hwang-Bin Ryou)

1968년 인하대학교 전자공학과 학사
1975년 연세대학교 전자공학과 공학석사
1984년 경희대학교 전자공학과 공학박사
1981년~현재 광운대학교 컴퓨터소프트웨어학과 교수

email : ryou@kw.ac.kr

신 효 영 (Hyo-Young Shin)

1986년 광운대학교 전자계산학과 이학사
1988년 광운대학교 전자계산학과 이학석사
1998년 광운대학교 전자계산학과 이학박사
1988년~1993년 ㈜LG소프트 연구원
1994년~현재 경복대학교 IT보안과 부교수

email : hyshin@kyungbok.ac.kr