https://doi.org/10.33778/kcsa.2022.22.4.011

림랜드 이론으로 본 사이버공간 통제방안 (북한의 사이버전 사례연구를 중심으로)

김 동 현*, 이 수 진**, 김 완 주***, 임 재 성****

요 약

오늘날 과학기술의 발전은 사이버공간과 물리적 공간이 통합된 사이버-물리체계를 출현시켰다. 사이버공간과 물리적 공간은 별개의 공간이 아니라, 사이버-물리체계로 통합된 하나의 시스템으로 구현되고 있다. 현실은 멈춰진 것이 아니라, 끊임없이 변화하고 있고, 공간의 개념도 진화 중이다. 그러나 대부분의 연구는 아직도 사이버공간과 물리적 공간을 같은 관점으로 보지 못하고, 공간별 특성에 맞는 맞춤식 대응을 고수하고 있다. 변화된 현상을 반영하지 못하는 이론적 접근은 과거에 머물 수밖에 없으며, 진보된 현실을 반영하지 못하는 뜬구름 속 이야기로 전락할 위험이 크다. 본 연구는 물리적 공간에서 적용하는 림랜드 이론의 관점에서 사이버공간 통제방안을 제시하였다. 이러한 연구는 물리적 공간과 사이버공간으로 분리된 통제개념을 림랜드 이론의 단일한 관점에서 재해석할 수 있고, 사이버공간의 통제방안도 구체화할 수 있었다. 특히, 북한의 사이버전 공격사례를 인적요소를 포함한 림랜드 이론의 관점으로 접근하여 내·외부자 위협 공격에 대한 정책적 대안을 제시하기도 하였다. 단순함은 궁극의 정교함이다. 본 연구는 개별적으로 발전되어 온 물리적 공간과 사이버공간의 통제방안을 단일한 관점으로 통합하여 다가올 사이버-물리체계 시대에 대비하기 위한 통섭적 시각을 제시하는 등 변화된 현상을 이론적 관점에서 분석한 연구성과가 있다.

Control measures in Cyberspace in the light of Rimland theory

Dong-hyun Kim*, Soo-jin Lee**, Wan-ju Kim***, Jae Sung Lim****

ABSTRACT

Development of science technology make integrated CPS(Cyber-Physical System) appear. In CPS era, cyberspace and physical-space are hard to separate anymore, that is developing toward integrated CPS. The reality is not stopping, that is consistently changing and the concept of space is developing too. But several articles are considering for cyberspace and physical-space separately, and they are developing tailed alternative each case. The theorical approaching that is not considering reality is dwelled on past, and is dangerous from dropping down to floating cloud that is not considering progressed reality. This article is suggested to consider rimland theory to control measures in cyberspace. That is dedicated to integrated approaching from physical-space to cyberspace. And that is developing concreted controling measures in cyberspace. Especially, this article is suggested to policy alternative by analyzing north korea cyber warfare from rimland theory including human sources. Simplicity is the ultimate sophistication. This article make integrated approaching effects about cyberspace and physical-space to preparing in the CPS era.

Key words : Rimland theory, CPS(Cyber-Physical System), Cyberspace

접수일(2022년 09월 20일), 수정일(2022년 10월 14일), 게재확정일(2022년 10월 20일)

* 국방부 합동군사대학교(주저자)
** 국방대학교 국방과학학과(공동저자)
*** 아주대학교 국방디지털융합학과(공동저자)
**** 아주대학교 국방디지털융합학과(교신저자)

1. 서 론

4차 산업혁명 이후 세상은 물리적 공간과 사이버 공간이 하나로 연결되고 있다. 오늘날 정보통신기술(ICT)의 발전으로 물리적 공간과 사이버공간은 상호 연계되는 중이며, 별개의 공간이 아니라 사이버-물리체계의 단일공간으로 인식되어야 한다. 사이버-물리체계는 손에 잡히지 않는 형이상학적인 세계가 아니라, 이미 우리의 일상과 떨어질 수 없는 현실이다.

오늘날 사이버-물리체계로 진화 중인 공간 개념의 변화로 사이버공간과 물리적 공간은 상호 연결된 하나의 시스템으로 발전되고 있다. 우리는 물리적 공간과 사이버공간의 벽을 허물고, 사이버공간을 통해 물리적 공간을 통제하는 새로운 현실 속에서 삶을 살고 있다. 변화된 사회는 변화된 시각을 요구하듯이, 사이버-물리체계 시대는 새로운 패러다임을 요구한다. 그러나 사이버공간에 관한 최근 연구는 여전히 과거에 머물러 있으며, 물리적 공간과 사이버공간을 별개의 개념으로 구분한 공간별 맞춤식 대응방안에 급급하기만 하다.

본 연구는 공간 개념의 변화를 반영하고, 기존연구[1~2]에서 다루지 않은 물리적 공간의 관점에서 사이버공간 통제방안을 연구하여 2가지 연구성과를 달성하겠다. 첫째, 사이버공간을 물리적 공간의 림랜드 이론의 관점에서 분석하여 이원화된 통제개념을 단일관점으로 제시하겠다. 사이버-물리체계는 새로운 패러다임을 요구하며 통합된 개념이 필요하기 때문이다. 둘째, 사이버공간의 물리적 계층을 분석하여 구체적인 통제방안을 정립하겠다. 본 연구는 단순히 인식에 그치지 않도록 손에 잡히는 청사진을 그리는 첫걸음을 내딛겠다. 따라서 이번 연구는 림랜드 이론의 관점에서 사이버공간을 분석하고, 북한의 사이버전 사례연구를 통해 연구의 타당성을 검증하고자 한다.

2. 기존연구 검토

2.1 사이버공간 통제방안

2001년 9.11 테러 이후 미국은 어떻게 사이버공간을 정의하고 통제할 것인지에 대한 관심이 높아졌다. 일례로, 미국 국토안보부는 사이버공간을 인터넷, 텔레커뮤니케이션, 네트워크, 컴퓨터 시스템, 주요 연관 산업들에 설치된 프로세서와 통제장치 등을 포함하는 정보통신 인프라의 상호 의존적인 네트워크라고 보았다.[3] 또 미국 사이버 교범에서는 사이버공간을 인터넷, 통신 네트워크, 컴퓨터 시스템, 임베디드 프로세서 및 컨트롤러를 포함한 정보기술 인프라와 상주 데이터의 상호 의존적 네트워크로 구성된 정보환경 내의 글로벌 도메인으로 규정하였다.[4]

본 연구는 연구범위를 제한하고, 연구 방향을 집중하기 위해 사이버공간을 재정의하였다. 이번 연구는 변화하는 정보통신기술의 발전 추세를 반영하여 광의적 개념을 빌려 “사이버공간은 컴퓨터, 사물인터넷 등 광범위한 네트워크망으로 구성되고, 인간과 인공지능 등으로 운영되는 인적 영역과 물리적 영역이 상호 영향력을 미치는 가상의 공간이다.”라고 정의하겠다. 연구범위는 물리적 기반시설을 포함하되, 기존연구에서 다루지 못한 사이버공간과 물리적 공간의 통합된 통제방안을 검토하겠다.

대부분의 기존연구는 사이버공간만의 맞춤식 대응을 강조한다. 이러한 연구는 사이버공간의 특성은 구현할 수 있지만, 사이버공간과 물리적 공간이 상호 연계된 사이버-물리체계의 현주소를 반영하지는 못한 한계가 있다. 본 연구는 ‘물리적’ 관점에서 어떻게 사이버공간을 통제할 수 있는지 고민하였고, 사이버공간에 접목하는 구체적인 방안을 제시하였다. 가상의 공간이라 불리는 사이버공간도 결국 네트워크망으로 상호 연결되어 있고, 목표에 이르는 연결지점도 한정적이므로 물리적 공간의 개념과 다르지 않기 때문이다. 따라서 이번 연구는 사이버공간만의 맞춤식 대응이 아니라, 물리적 공간에서의 ‘림랜드 이론’의 관점에서 사이버공간 통제방안을 제시하고자 한다.

2.2 림랜드 이론

림랜드 이론은 스파이크만이 주장한 이론이다.[5] 그는 교통, 자원, 기후에 따라 개별 공간의 가치를 부여하였다. 그 결과, 스파이크만은 “림랜드를 정복하면 유라시아 대륙을 지배할 수 있고, 유라시아 대륙을 지배한 자는 세계를 장악할 수 있다.”고 보았다.

본 연구는 사이버공간을 지정학적 관점인 림랜드 이론으로 분석하여 사이버공간의 통제방안을 제시한다. 이를 위해 림랜드 이론에서 제시된 물리적 공간

에서의 교통, 자원, 기후의 변수를 사이버공간에 적용하여 적합한 변수를 도출하고, 물리적 공간과 사이버공간과의 유사성을 분석하였다. 첫 번째, 사이버공간에서의 교통은 데이터가 원활히 유통되기 위한 기반체계를 의미한다. 우리는 사이버공간에서 원하는 정보가 보관된 장소까지 도달하기 위해 물리적 계층에서 제공하는 라우터 등을 통과해야만 하므로 물리적 공간에서의 교통은 사이버공간의 네트워크 기반체계로 볼 수 있다.

두 번째, 물리적 공간에서의 자원은 가치를 창출하는 자산을 말한다. 사이버공간의 자원을 데이터의 유통량만 평가하기에는 어렵다. 데이터가 클라우드 공간과 같이 데이터의 보관장소를 특정할 수 없는 임의의 장소에서 유통될 수도 있기 때문이다. 또한, 데이터는 그 중요도에 따라 주관적으로 인식되는 가치의 높고 낮음에 따라 분류되기도 한다. 따라서 데이터는 절대적인 유통량뿐만 아니라, 정량·정성적인 부문이 통합적으로 평가 및 판단되어야 하므로 본 연구에서 데이터는 주요 변수에 포함하지 않겠다.

세 번째, 기후는 환경적 요소이며, 물리적 공간에서 온난한 환경은 양호한 조건이 된다. 사이버공간은 전송속도, 전송용량 등이 통신서비스 구성을 위한 필수조건이다. IT 선진국이라 불리는 한국의 통신서비스 환경은 인터넷 서비스 제공자마다 일부 차이(0.71~0.93Gbps)는 있지만, 크게 다르지 않다. 한국의 인터넷 서비스 제공자는 특정 업체로 국한되어 있고, 업체는 유사한 수준의 서비스 환경을 제공하기 때문이다. 이번 연구는 지역 및 기관별로 통신서비스 환경의 변별력이 없는 한국의 특성을 고려하여 스파이크만이 제시한 기후 변수도 연구범위에서 제외하겠다.

<표 1> 림랜드 이론으로 본 사이버공간

구분	림랜드 이론 변수		
물리적 공간	교통	자원	기후
사이버 공간	기반체계	정보	서비스 환경
	단말기, 서버, 네트워크장치	데이터센터, 클라우드 등	전송속도, 전송용량 등

본 연구는 물리적 공간 개념의 림랜드 이론을 사이버공간에 접목하여 <표 1>과 같이 변수를 도출하였다. 다만, 언급한 3가지 변수 이외에도 인적요소를 추가 변수로 포함하겠다. 사이버공간에서도 첨단 과학기술의 발전으로 인공지능 등 의사결정에 관한 인지적 차원이 획기적으로 진보되는 등 인적계층이 주목받고 있기 때문이다.[6] 따라서 본 연구는 스파이크만이 제시한 림랜드 이론의 주요 변수와 인적요소를 동시에 고려하여 북한의 사이버전 사례연구를 통한 사이버공간의 통제방안을 제시하겠다.

2.3 분석의 틀

사이버-물리체계는 수많은 컴퓨팅된 매체가 상호연결되어 사이버공간과 물리적 공간이 통합된 개념이다. 이러한 현상은 과거에는 해킹이 매체에 대한 직접 접근만을 통해 가능했다면, 사이버-물리체계는 제3의 매체를 통한 간접 접근도 가능하다. CPS로의 개념 변화는 사이버공간에서의 통제방안 변화도 요구하고 있다. 이번 연구는 물리적 공간과 사이버공간과의 연계성을 분석하여 <표 2>와 같이 물리적 계층과 인적요소에 한정하여 대응방안을 제시하고자 한다.

<표 2> 인적요소를 고려한 림랜드 이론으로 본 사이버공간

구분	림랜드 이론 변수			인적요소
물리적 공간	교통	자원	기후	
사이버 공간	네트워크장치, 단말기, 서버	-		사람, 가상인물

본 연구는 사이버-물리체계를 보호하기 위해 인적요소를 포함한 림랜드 이론의 관점으로 접근한다. 사이버-물리체계는 사이버공간의 위협이 물리적 공간으로 확장되며 역으로, 물리적 공간의 위협이 사이버공간으로 전이되는 등 공간별 맞춤식 대응만으로는 궁극적인 대안이 될 수가 없기 때문이다. 따라서 본 연구는 림랜드 이론과 인적요소의 통섭적인 관점으로 접근하여 북한의 사이버전 사례분석을 통해 네트워크의 물리적 계층과 인적 자원 관리의 취약점을 도출하고, 현실적인 통제방안을 제시하겠다.

3. 북한의 사이버전 사례분석

3.1 현역 대위 군사기밀 유출사건

2022년 4월, 특수전사령부 현역 대위가 북한 공작원으로부터 뇌물을 받고, 군사기밀을 유출한 사건이

발생하였다.[7] 현역 장교가 북한 해커에게 포섭돼 간첩 활동하다가 붙잡힌 것은 처음 발생한 일이다. 수사 당국은 현역 대위가 메신저를 통해 북한 해커의 지령을 받고, 이적행위를 자행하였다고 발표하였고, 현역 대위는 도박 빚을 갚기 위한 경제적 이득을 얻고자 북한 해커와 연락하게 되었다고 밝혀졌다.

현역 대위의 이적행위는 내부자 위협의 전형이다. 단 한 명의 내부자 위협으로 인해 보안자료, 군 지휘통제체계, 작전계획 등의 유출은 물론, 국민으로부터 대군 신뢰를 무너뜨렸으며, 안보 공백과 새로운 작전계획을 수립해야 하는 불편한 현실에 맞닥뜨렸다. 본 연구는 사이버공간에서 반드시 지켜야 하는 림랜드 지역, 즉 물리적 계층과 인적요소의 관점에서 내부자 위협을 분석하여 3가지 취약점을 도출하였다.

첫째, 군사 보호시설의 물리적 보안대책이 취약하였다.현역 대위는 전장망 해킹 시도 이전에 국방망 육군 홈페이지 화면, 육군 보안수칙, 군 시설물과 작전계획 등을 촬영하여 임의로 전송하기도 하였다. 안타깝게도 이러한 현역 대위의 이적행위를 제지하거나 통제하는 감독관은 없었다.

둘째, 보안장비에 대한 사용자 인증 및 권한 관리 체계가 부실하였다. 현역 대위는 전장망에 접근하여 로그인 화면 등을 촬영하여 북한 해커에서 전송하였다. 그는 별도 통제 없이 전장망에 접속했고, 북한 공작원의 해킹을 돕기 위해 전장망 관련 자료를 핸드폰으로 촬영하여 외부로 유출하였다.

셋째, 핵심 시스템 관리자와 사용자에 대한 신상관리가 소홀하였다. 북한 해커는 사이버 도박 빚이 있는 현역 대위에게 의도적으로 접근하였고, 금전적 이유로 현역 대위는 북한 해커에게 포섭당하였다. 금전 문제는 개인정보이기 때문에 당사자가 언급하기 전에는 알 수가 없으며, 누구도 현역 대위의 변화된 개인정보를 사전에 인지하지 못하였다.

3.2 국방통합데이터센터 해킹사고

2016년 8월부터 같은 해 9월까지, 국방통합데이터센터는 북한 소속으로 추정되는 해커로부터 해킹을 당하였다.[8] 이번 사고는 해커가 군 인터넷망 백신서버에 침투한 후 악성코드를 이용하여 내부 자료가 유출된 사건이다. 드러난 현상만을 본다면, 언론에서 보도한 '네트워크망 혼용'으로만 단정 지을 수도 있다. 그러나 본 연구는 림랜드 이론의 관점에서 이번 사건을 되짚어 본 결과, 이번 사고는 '네트워크망 혼용'뿐만 아니라, 또 다른 취약점도 식별되었다.

첫째, 라우터가 침입 행위를 탐지하지 못했다. 이번 해킹사고의 주범으로 추정되는 IP주소는 중국 내 북한 해커의 주요 근거지 중 하나인 선양으로 밝혀졌다.[9] 물론, 해커의 주요 활동지역이라고 하여 IP주소를 차단하는 것은 정보 교환 및 공유를 위해 존재하는 인터넷의 목적에 부합되지 않는다. 다만, 국방망을 포함한 국가안보에 직접적인 영향을 미치는 특정 네트워크망은 위협세력의 IP 발신지로부터 선별적으로 차단하는 방안을 고려해봐야 한다.

둘째, PC, 서버 등 단말기의 정보보안 공백이 발생하였다. 해커는 군 인터넷 PC에 침투한 후 파일공유서버를 거쳐 국방망을 공격하였다. 해커의 군 인터넷 PC에 대한 공격 방식은 공식적으로 밝혀지지는 않았다. 다만 추정컨대, 해커는 관리가 취약한 인터넷 홈페이지에 악성코드를 탑재하고, 군 인터넷 PC 사용자가 방문하여 감염되었을 수도 있다. 이번 사건은 백신 서버의 부실한 관리와 외부 공격을 탐지하기 위한 침입 탐지시스템, 방화벽 등의 정보보호체계가 정상 작동하지 못했다고 보여진다.

셋째, 군 인터넷망과 국방망이 혼용되었다. 국방망은 외부로부터 차단된 폐쇄망이다. 일반적으로 국방망은 폐쇄망이기 때문에 가장 안전한 업무 환경이라고 인식되었다. 그러나 해커는 인터넷망과 국방망을 정찰하고 취약점을 식별하였다. 그 취약점은 군 인터넷 사용자 PC와 백신서버 관리자 PC가 관리의 편의를 도모하고자 물리적 망 분리가 되어 있지 않았고, 무엇보다 파일공유서버가 망 혼용 상태로 운용되고 있었다.

4. 사이버공간 통제방안

4.1 내부자 위협 대응방안

모든 것이 연결되어 있는 사이버-물리체계 세상은 내부자가 핵심 데이터에 접근할 수 있는 지점을 획기적으로 증가시켰다. 현역 대위의 간첩행위를 되짚어 본 결과, <표 3>과 같이 사고 재발 방지를 위해 3가지 내부자 위협 대응방안을 도출할 수 있었다.

<표 3> 내부자 위협 대응방안

구분		`림랜드 이론 변수	인적요소
사이버 공간	변수	네트워크장치, 단말기, 서버	사람, 가상인물
	대응 방안	①물리적 보안대책	③신상관리방안
		②인증/권한 관리체계	

첫째, 군사 보호시설의 물리적 보안대책이다. 앞으로 유사 사고가 재발하지 않기 위해 시설의 중요도를 고려한 맞춤형 출입통제 대책을 정립해야 한다. 또한, 시설보안은 시설의 위치, 용도, 기능 등을 고려하여 보안대책을 수립되어야 하고, 지정된 통제지역은 다중의 보안장비를 추가 설치하여 엄격하게 통제되어야 한다. 그뿐만 아니라, 시설보안 책임자는 사물인터넷 기반의 초연결 지능 인프라를 활용한 위험예측 시스템을 설계하고, 드론을 활용하는 등 감시 사각지대를 최소화하는 방안도 검토할 필요도 있다.

둘째, 보안장비에 대한 사용자 인증 및 권한 관리체계이다. 인증과 권한 관리체계가 정상 작동한다면, 비인가자의 시스템 접속은 원천적으로 불가하다. 이를 구현하고자 본 연구에서는 전장망 인증과 권한 관리체계가 강화된 역할+블록체인 기반의 접근제어 모델을 제시하였다. 역할기반 접근제어는 사용자의 역할에 따라 접근 권한을 효율적이며, 체계적으로 관리할 수 있는 장점이 있다. 그러나 이 모델은 동료의 데이터를 이용하여 접근하는 내부자 위협에는 취약하므로 이에 대한 해결책을 블록체인 기술에서 찾았다. 물론, 오늘날 블록체인 기술은 확장성, 데이터 수명주기 등 연구해야 할 일부 과제가 남아 있지만, 4차 산업혁명 기술의 발전 추세를 반영하여 역할+블록체인 기반의 접근제어 모델을 도입할 것을 주장한다.

셋째, 핵심 시스템 관리자와 사용자에 대한 신상관리방안이다. 이번 연구는 비밀 취급 인가자에 대한 주기적인 신원조사 제도를 제시하였다. 비밀취급 인가 예정자는 직무를 수행하기 전에 국가 안전보장에 해를 끼칠 정보가 없음을 검증받아야 한다. 다만, 신원조사가 일회성에 그치기 때문에 신원조사 이후 대상자의 변화와 이러한 변화로 인해 대상자가 국가안보에 악영향을 미칠 수 있는지 그 여부를 확인하기가 어렵다. 본 연구는 신원조사 체계를 운전면허증 갱신 개념의 반영구적 방안을 도입할 것을 제안한다.

4.2 외부자 위협 대응방안

사이버공간의 이상적인 통제방안은 관리자가 사전 승인한 사용자가 아니면, 그 누구도 시스템에 접근할 수 없어야 한다. 본 연구는 국방통합데이터센터 해킹 사고를 분석하여 외부자 위협의 3가지 취약점을 도출하였고, <표 4>와 같이 대응방안을 제시하였다.

<표 4> 외부자 위협 대응방안

구분		림랜드 이론 변수	인적요소
사이버 공간	변수	네트워크장치, 단말기, 서버	사람, 가상인물
	대응 방안	①선별적 네트워크 접근방안	-
		②방어/탐지체계 (시스템 분야)	②방어/탐지체계 (관리 분야)
		③망혼용 통제방안	-

첫째, 의심 IP를 목록화하여 선별적 네트워크망 접근방안을 도입해야 한다. 라우터는 공항에서의 세관처럼 신고되지 않거나 위험한 물건과 사람은 없는지 자체 확인할 수 있는 검역 기능이 있어야 한다. 본 연구는 동일 사고 예방을 위해 접근제어 목록기반의 라우터, 네트워크 접근제어 시스템을 국방망에 도입하여 국방망 물리적 계층의 심층 방어전략을 주장한다. 국방부는 선별적으로 우선순위에 따라 예상되는 침투로에 대한 다중 중첩 보호체계를 갖춰야 한다.

둘째, PC·서버 등 물리적 매체의 방어 및 탐지시스템을 보완해야 한다. 변화된 사이버 환경에 적용할 수 있는 방화벽을 구축하여 내·외부망 간의 진입 장벽을 세우고, 방화벽을 보완하기 위해 다중화된 방어시스템과 관제 및 자체 취약점 개선 시스템을 도입해야 한다. 또한, 시스템 개선과 더불어 책임있는 관리자가 중앙관제하는 방법을 병행할 것을 제안한다.

셋째, 내부망은 외부망과 혼용되어서는 안된다. 망분리 정책을 시행하는 기관은 망 분리가 제대로 되고 있는지 관제할 수 있는 인원과 조직을 편성해야 하고, 변화하는 보안환경에 적응할 수 있도록 전문·보수교육도 뒷받침되어야 한다. 디지털 금융산업의 망분리 규제 완화 바람이 불고 있다. 변화하는 사이버 안보환경 속에서 보안과 효율이라는 선택지 중에 국가안보를 다루는 주요 기관에서의 망분리 정책은 어떤 방향으로 나아갈지 고민해야 한다.

5. 결론

우리는 사이버공간과 물리적 공간이 하나의 사이버-물리체계로 통합되어가는 세상에 살고 있다. 새로운 공간과 개념의 출현은 사이버공간과 물리적 공간의 구분을 어렵게 만들었고, 사이버공간은 물리적 공간에서 운용되는 기반시설의 중심체계로 자리매김하였다. 미래에는 물리적 정보 기반시설이 상호 의존적 네트워크에 더욱더 강화될 것으로 전망되기도 한다. 이러한 추세는 국방 분야에도 나타나고 있다.

단순함은 궁극의 정교함이다. 사이버-물리체계의 출현은 새로운 대안이 필요하다. 본 연구는 개별적으로 발전되어 온 물리적 공간과 사이버공간의 통제방안을 단일한 관점으로 통합하여 다가올 사이버-물리체계 시대에 대비하기 위한 통섭적 시각을 정립하였다. 또한, 내·외부자 위협 사례를 분석하여 정책 및 기술적 대안을 제시한 성과도 있다.

만약 아무도 들어가고 싶지 않은 문이 있다면, 그 문이 열려 있다고 하여도 취약한 것이 아니다. 반대로, 모두가 들어가고 싶은 문이 있다면, 그 문은 허가된 인원만 출입할 수 있도록 별도의 통제방안이 마련되어야 한다. 오늘날 사이버공간은 무한한 가치를 창출할 수 있는 모두가 가고 싶어 하는 공간이며, 앞으로 사이버-물리체계로 통합될 것으로 예측된다. 사이버-물리체계의 세상은 아직은 낯설고 어색할 수 있지만, 새로운 기회의 땅을 선점하기 위한 경주는 이미 시작되었고, 우리는 공략법과 통제방안을 동시에 고려해야 한다. 앞으로의 연구를 통해 본 연구의 한계를 극복한다면, 사이버공간의 통제방안이 구체화될 수 있을 것으로 기대된다.

참고문헌

[1] Fenghua Li, Cyberspace-Oriented Access Control, "IEEE", 2019.
[2] 김상배, 사이버안보의 복합지정학, "국제·지역연구", 24권 3호, 2015.
[3] 신성호, 미 오바마 행정부의 사이버안보 정책과 쟁점, "국제·지역연구", 25권 4호, 2016. 겨울.
[4] 국방대학교, 지상군 사이버·전자전 작전수행절차 정립방안 연구, 국방대학교, 2021.
[5] Nicholas J. Spykman, The Geography of the Peace, Harcourt, 1944.
[6] 국방대학교, 미래 한국군 사이버전 수행개념 및 역량 강화방안, 국방대학교, 2021.
[7] 김기윤, '현역 軍대위, 北해커에 포섭돼 간첩활동 벌이다 체포', 동아일보.
[8] Derek S. Reveron, Cyberspace and National Security, Georgetown, 2012.
[9] 국가정보원·과학기술정보통신부·방송통신위원회, 2018 국가정보보호백서, 한국인터넷진흥원, 2018.

〔저자소개〕

김 동 현 (Dong-hyun Kim)
2006년 3월 육군사관학교 물리학과 학사
2013년 1월 국방대학교 군사전략학과 석사
2022년 1월 합동군사대학교 학생장교
email : c14978@naver.com

이 수 진 (Soo-jin Lee)
1992년 3월 육군사관학교 전산학과 학사
1996년 2월 연세대학교 컴퓨터과학과 석사
2006년 2월 KAIST 전산학과 박사
2006년 3월~ 국방대학교 국방과학학과 교수
email : cyberkma@gmail.com

김 완 주 (Wan-ju Kim)
1998년 2월 서울과학기술대학교 전자공학 학사
2008년 1월 국방대학교 전산정보 석사
2017년 2월 아주대학교 NCW학 박사
2017년 3월~ 아주대학교 국방디지털융합학과 겸임교수
email : sizipus1@ajou.ac.kr

임 재 성 (Jae-sung Lim)
1983년 2월 아주대학교 전자공학 학사
1985년 2월 KAIST 영상통신 석사
1994년 8월 KAIST 전자공학 박사
1998년 3월~ 아주대학교 국방디지털융합학과 교수
email : jaslim@ajou.ac.kr