Crisisonomy Vol.13 No.7, 89-107
ISSN 2466-1198 (Print) ISSN 2466-1201 (Online) http://dx.doi.org/10.14251/crisisonomy.2017.13.7.89

Crisisonomy

An Integrated Approach of China's Cyber Security Strategy

Hyun Suk Cho[1#], Eun Mi Lee[2+], Dong Wook Kim[3]

[1] Department of Public Administration, Seoul National University of Science & Tech, 232 Gongneung-ro, Nowon-gu, Seoul, Korea
[2] SSK Research Center, Seoul National Univ. of Science&Tech, 232 Gongneung-ro, Nowon-gu, Seoul, Korea
[3] Graduate School of Public Administration, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, Korea

Abstract

This research argues that China's cyber security strategy needs to be analyzed from a different approach than the strategy in the United States. On the other hand, it is necessary to investigate national security and economic development in an integrated analysis framework. This study thus analyzed ideology, goals, organization, institution and cyber competence as important components of China's cyber security strategy. They are based on nationalism and socialist ideology, pointing out that it includes the power domination and legitimacy of the Chinese Communist Party, the pursuit of political and social stability, information technology innovation and economic development. In addition, China 's cyber security strategy has significantly changed since 2014, both organizationally and institutionally. It is also found that China has gradually improved its cyber competence along with technological innovation.

Key words: China's cyber security strategy, integrated approach, innovation

Ⅰ. 서 론

세계적인 정보혁명의 흐름 속에서 한국은 1990년대 초반과 중반에 걸쳐 '산업화에는 뒤졌지만 정보화에는 앞서가자'는 구호를 사용했다. 신발전주의 경제성장 전략을 추구해온 중국도 한국보다 다소 뒤늦은 시기인 2000년대에 들어 정보화를 적극적으로 추진하였다. 중국은 경제를 비롯해서 정치, 사회, 문화 전반에 걸쳐 정보기술을 받아들이고 활용하고 있고, 이에 따라 정보화를 경제성장과 국가안보의 핵심으로 간주해 왔다.

2015년 말 기준, 중국에서 약 6억 6,800만 명이 인터넷을 사용하고 있다고 집계되었다. 이는 중국인구의 48.8%에 해당하며, 전 세계 인터넷 사용자의 20%에 달하는 비율이다. 이미 중국은 전 세계 인터넷 사용자의 절대 다수를 차지하면서, 중국 내 인터넷 이용자 또한 매해 빠른 속도로 늘어나고 있다. 인터넷 사용자의 증가 속도만큼 정보기술산업이 중국의 경제 구조에서 차지하는 비중 또한 빠르게 증가하고 있는 추세이다. 중국의 정보통신 산업의 부가가치는 연평균 약 30%씩 성장했으며, 국내총생산(GDP)에서 차지하는 비중도 1%에서 15%로 높아졌다(Cho & Chung, 2016: 151-152).

중국은 정보기술 산업의 육성과 정보화를 국가발전

The 1st author: Hyun Suk Cho, Tel. +82-2-970-6286, e-mail. hyunsuk@seoultech.ac.kr
+ Corresponding author: Eun Mi Lee, Tel. +82-2-2123-8172, E-mail. foodbo@msn.com

의 핵심 동력으로 설정해 왔다. 이러한 정보화 정책은 중국이 단기간에 서방의 기술을 따라잡고 경제성장을 달성한 기반이 되었지만 또한 많은 부작용을 낳았다. 그 중에 하나가 사이버 불안과 취약성(cyber insecurities)의 만연이다. 정보 안전, 사이버 안전에 대해 적절한 관심을 주지 않고 추진된 정보기술 발전과 정보화로 인해 엄청난 규모의 사이버 지하경제가 생겨났고, 사이버 범죄와 절도가 창궐하게 되었다. 중국의 정보화 지하경제는 압축적 정보혁명의 필연적 부산물로 여겨질 수 있다. 이러한 대규모 사이버 위협의 만연은 경제적 문제에 그치지 않고 사회 안정과 체제 안정의 문제로까지 인식되기에 이르렀다.

중국사회의 사이버 불안정이 글로벌 네트워크에서 국경 내에 머물 것이라고 기대하는 것은 희망사항에 불과하다. 중국의 사이버 위협 세력들과 네트워크는 자연히 정보경제와 기술의 세계적 중심지인 미국으로 향하게 되었다. 미국의 산업계와 기업들에 대한 사이버 산업스파이가 조직적이고 대규모적인 방식으로 이루어지게 되었다. 게다가 중국의 군부는 미국과의 군사기술의 격차를 줄이기 위해 미국의 고도무기체계에 관심이 많다. 이러한 목적을 위해서, 보다 조직적인 사이버 스파이가 이루어졌고 성과도 매우 컸다고 분석되고 있다.

중국 정부와 군대가 사이버 위협의 주체로 나서기도 했지만 사이버 공간의 특성상 중국의 정부와 기업도 사이버 위협의 대상이 되었다. 중국의 사이버 안보 전략은 이러한 대내외 사이버 위협과 불안정에 대한 대응을 통해서 형성되어 왔다고 할 수 있다. 중국의 사이버 안보 전략의 기본 개념이 '적극적 방어'(active defense)로 개념화될 수 있는 것도 이러한 맥락과 관계가 깊다. 중국의 사이버 안보 전략은 외부 지향성과 함께 내부 지향성을 강하게 가지고 있다. 또한 초기부터 안보적 동기와 함께 경제적 동기를 크게 내포하고 있다. 이런 문제의식에서 중국의 사이버 안보 전략을 제대로 파악하기 위해서는 통합적 접근이 필요하다. 안보적 시각이나 외부 지향적 동기에 초점을 맞추는 분석은 중국이 추구해온 정보기술발전과 정보화의 중요성과 정보화에 바탕을 둔 중국의 사이버 역량의 구축과 사이버 안보전략을 반영하는데 어려움이 있기 때문이다.

II. 이론적 논의와 연구방법

1. 이론적 논의

1) 사이버 안보의 개념적 이해

사이버 안보는 미국, 중국, 한국에서 각기 다른 용어로 표현되어 왔다(Kim, 2015b: 75-78). 미국과 한국에서는 사이버 안보(cyber security)와 더불어 정보안전(information security), 정보보호(information protection), 컴퓨터 보안(computer security), 인터넷 보안(internet security), 네트워크 안전(network security) 등의 용어가 혼용된다(Kim, 2015b). 중국에서 인터넷은 '互聯網(互联网)'으로 쓰고 있지만, 인터넷, 네트워크, 사이버 등은 대체로 網絡(网络)이라 번역하고 'security'는 대체로 '안전(安全)'으로 사용하고 있다. 최근 중국에서 가장 많이 쓰는 용어는 '인터넷안전 혹은 네트워크안전(網絡安全)'이다(Kim, 2015).

사이버 안보 논의는 사이버, 안보, 국가라는 세 가지 범주의 상호관계에 토대를 두고 있다. '사이버(cyber)'라는 접두어는 보통 정보통신기술 관련 행위에 대하여 포괄적인 의미로 사용 하는데, 주로 네트워크 인프라의 물리적 층위, 소프트웨어나 기술표준 등의 논리적 층위, 지식, 이념, 정체성의 콘텐츠 등의 세 층위를 지칭한다(Kim, 2015b). 사이버 안보는 1990년대 초반에는 하드웨어와 소프트웨어의 오작동으로부터 기인하는 컴퓨터 시스템의 장애방지나 인터넷이라는 물리망의 보호에 중점을 둔 컴퓨터 보안, 정보보호, 네트워크 안전 등의 의미로 이해되었다. 2000년대 인터넷의 활용이 세계적으로 확산되면서, 보호라는 용어의 논리적 층위가 각국의 주권적 관할권을 넘어서는 안보문제로 인식되기 시작했다(Kim, 2015b). 2000년대 후반 이후에는 사이버 공간에서 정치, 사회, 문화적 활동이 많아지면서 사이버 공간의 안전이나 안보에 대한 논의가 활발해지기 시작하였다. 특히 9.11 테러 이후, 외부로부터 악

의적이고 의도적인 테러의 공격보다는 사이버 공간에서의 활동이나 그 기반이 되는 시스템과 지식정보를 보호하려는 정책적 목적이 강조되기 시작하였다.

영어에서 '안보'라는 용어는 주로 'security'라고 하지만, 쓰임에 따라 안전(安全, safety)이나 보호(保護, protection) 등과 같은 중립적인 뉘앙스의 용어로 번역되기도 하고, 국내정치나 치안의 뉘앙스를 갖는 보안(保安)이나 공안(公安)이라는 말로 쓰이기도 하며, 대외적인 함의를 가질 때는 주로 안보(安保)라고 한다(Kim, 2015b). 네트워크의 세 층위 중에서 물리적 층위나 논리적 층위에 해당하는 'security'를 논할 경우는 안전이나 보호, 경우에 따라서는 안보라고 번역하기도 하고, 콘텐츠 층위의 'security'를 염두에 둘 때는 정치사회적 측면에서 이해된 보안이라고 번역되는 경향이 있다(Kim, 2015b). 최근에는 사이버 안보의 문제를 단순한 시스템과 정보의 보호, 안전의 의미를 넘어서 좀 더 넓은 의미에서 이해하기 시작하면서 안보라는 용어로 더 많이 사용되고 있다.

'국가(state)'의 개념을 '사이버'와 '안보'라는 용어와 결합시키면, 사이버 안보논의를 이해하는 데 도움이 된다. 사이버 안보만을 살펴본다면, 'security'의 개념은 세 가지 차원의 국가 개념, 즉 '정부(government)', '정권(regime)', '네이션(nation)' 등과 만나서 다르게 구성될 수 있다(Kim, 2015). '정부'와 결합시키면 다소 중립적인 안전(safety)이나 보호(protection)의 의미로, 사회(society)와 대립되는 의미에서 파악된 '국가'로서의 '정권'과 만나면 보안(保安)이나 공안(公安)의 의미로, 대외적 차원의 '네이션'과 조합을 하면 안보(安保)의 의미로 구성되곤 한다.

국가안보, 정권안보, 경제안보, 사회안보, 개인안보, 네트워크 안보 중에서 무엇을 우선시하느냐에 따라서 사이버 안보의 성격이 달라진다(Deibert, 2002). 위협의 대상에 따라 물리적 인프라냐, 정보지식 자산이냐, 이념과 사상의 콘텐츠냐에 따라 사이버 안보를 보는 시각과 해법이 다양해질 수 있다. 특히 이러한 사이버 안보의 성격은 국가, 정권, 사회, 기업, 개인 등과 같은 주체와 관련해서 구체적인 정치적 함의를 가지게 된다.

2) 사이버 위협의 분류

사이버 안보는 무엇보다 다양한 형태와 성격의 사이버 위협으로부터, 국가를 비롯한 다양한 주체의 안보 혹은 안전을 지키거나 네트워크 자체를 보호하는 것을 의미한다. 사이버 위협과 공격은 매우 다양한 성격과 형태를 보인다. 그러나 모든 사이버 위협의 형태를 사이버 안보의 대상에 포함시키는 것은 적절하지 않다. 개인 사용자들이 겪는 스팸 메일, 인터넷 피싱, 개인정보 도용, 사이버 사기, 심지어 사이버 범죄 등은 사이버 안보의 대상에 포함시키지 않는 것이 간결한 논의를 위해 필요하다.

여러 분류 중에서 Bendiek(2012)는 유럽의 공식 보고서를 참조하여 사이버 안보 위험을 사이버 범죄, 사이버 스파이행위, 사이버 전쟁 등 세 가지로 분류하고 있다. 유럽집행위원회는 사이버 위협을 위협의 목적에 따라 착취(exploitation), 교란(disruption), 파괴(destruction)로 나뉜다(Bendiek, 2012: 8). Nye(2011)도 위협의 심각성, 목적, 주체 등을 기준으로 사이버위협을 네 가지－사이버전쟁, 사이버범죄, 사이버테러, 사이버스파이－로 구분하였다. 또한, 사이버 공격의 주체나－범죄조직, 해커집단 혹은 국가간 상호 연계성 유무－연구의 목적에 따라 구분을 상이하게 설정할 수 있다(Jang & Han, 2013: 599-600). 본 논문에서는 Nye(2011)의 분류를 따르고자 하며 아래에서 네 가지 사이버 위협을 간략하게 검토한다.

Table 1. Types of cyber security

	State Actor	Non-State Actor
Lower National Security Level	Cyber Spy	Cyber Crime
Higher National Security Level	Cyber War	Cyber Terror

첫째, 사이버 조직범죄(cyber crime)는 사이버 범죄집단에 의한 해킹으로 일어나는 것으로 개인이나 기업

의 지적재산권이나 금융자산을 절취하고 신용카드 번호 등 신용기록을 영리적 목적을 위해 탈취하고 거래하는 행위들을 말한다. 최근에 들어 사이버 범죄는 무엇보다 조직화되고 다양화되었으며 분야별로 특화되고 전문화된 특성을 보이며 글로벌 경제 환경에서 자연스럽게 초국가화되는 경향을 보인다(Deibert, 2012: 265-266). 사이버 범죄 집단들이 반드시 경제적 행동만을 하는 것은 아니다. 국가 기관에 협조하여 사이버 스파이 행위를 할 수 있고 사이버 전쟁에 가까운 행동에 자발적으로나 혹은 타율적으로 참여하기도 한다.

둘째, 사이버 스파이(cyber spy)는 사이버 공간에서 컴퓨터나 관련 시스템을 이용하여 정보와 첩보를 수집하고 작전을 가능하게 하는 것을 말한다. 사이버 스파이 행위는 외관상 사이버 범죄 집단이나 애국주의 해커 등 비국가 행위자에 의해 촉발될 수도 있지만, 목적이나 동기는 명백히 국가적인 성격을 가지고 있다. 실례로 정보기관이나 군사기관에 대한 침투 행위가 이러한 점을 보여준다. 경제적 동기보다는 정치적, 전략적 동기가 크게 작용한다(Information Warfare Monitor and Shadowserver Foundation, 2010: 5).

셋째, 사이버 테러(cyber terror)는 다양한 비국가 행위자들에 의해서 초래되지만 외연의 범위는 매우 넓다. 그러나 경제적 동기보다는 주로 정치적, 이념적 동기에 의해서 촉발된다는 점이 중요한 특징이다. 사이버 테러는 비국가 행위자들과 이들의 네트워크에 의해 이루어지는 사이버 공격의 한 형태로서 대상은 국가 최고지휘부, 정보기관, 군대, 중앙은행과 같은 중요한 국가기관이나 국가의 정보통신 인프라와 같은 핵심 기반 시설이다. 사이버 테러 집단은 매우 비밀리에 조직되고 활동하며 고도의 기술을 갖추기도 한다. 사이버 테러는 비국가 행위자에 의해 기도되지만 거의 대부분 정치적인 동기를 가진다는 점에서 사이버 조직범죄와는 구별된다(Deibert, 2010).

넷째, 사이버 전쟁(cyber war)은 가장 논란이 되는 유형이다. 국가 행위자에 의한 사이버 공격, 민간인에 대한 공격, 전력망과 같은 국가 핵심 인프라에 대한 대대적인 공격 등을 포함하면 실제적인 사례는 거의 없다고 볼 수 있다. 여러 논의 중에서 사이버 전쟁의 논리는 매우 과장되었다는 주장도 설득력을 가지고 있는 것은 사실이다.[1] 그러나 2010년 이란의 핵연료재처리시설에 대한 스턱스넷(stuxnet) 공격은 이러한 회의적 시각을 재검토하게 하는 계기가 되었다.[2] 이 공격은 국가 행위자들에 의해 기도되었다는 것으로 밝혀졌는데, 사이버 전쟁에 근접한 사례도 발생하고 있다.[3] 원자력 설비와 국가 핵심 인프라를 훼손하려는 시도는 사이버 테러의 범주를 벗어나는 것이라고 할 수 있다(Segal, 2016a).[4]

2. 중국의 사이버 안보 전략 분석틀: 통합적 접근

본 논문에서 중국의 사이버 안보전략에 대한 통합적 분석을 위하여 기존의 정치외교적・경제적・사회적 접근을 중심으로 비교연구를 실시한다. 대외적인 차원에서는 미국과의 갈등과 협력의 문제들을 다루고 UN GGE(국제연합 정부전문가그룹)의 논의, 중국과 러시아가 주도하고 있는 상하이조직기구(SCO), 아세안지역안보포럼 내 사이버 안보 논의를 다룬다.

중국의 사이버 안보전략을 정치경제적 측면에서 다루어 본다(Chang, 2014: 21-23). 사이버 안보 인민해

1) 사이버 전쟁 담론에 대한 비판적인 견해들에 대해서는 O'Connell(2012), Cavellty(2012), Libicki(2012), Gartzke(2013) 등 참조. 미중 사이버 갈등의 맥락에서 사이버 전쟁 담론에 대한 비판적 시각은 Lindsay(2015a) 참조.

2) 스턱스넷의 제조와 사용은 매우 다양한 전문성과 조직이 필요하다. 소규모 해커 그룹이 보유한 자원과 지식으로는 스턱스넷을 제조하고 사용하는 것은 거의 불가능하다고 한다. 사이버 전문가뿐만 아니라 정보, 감시 분야의 전문가들도 필요하고 핵물리학자들도 필요하다. 또 독일의 지멘스가 제조한 산업통제시스템을 잘 아는 엔지니어도 필요하다. 또한 제조 후에도 큰 비용이 들어가는 시험과정도 거쳐야 하는데 하드웨어뿐만 아니라 소프트웨어도 시험 대상에 포함된다. "The Meaning of Stuxnet." Economist(Sep. 30, 2010); Singer(2012) 참조.

3) 워싱턴 포스트(WP)는 2012년 6월 2일자에서 이란에 대한 스턱스넷 공격이 미국과 이스라엘의 작품이라는 기사를 게재했다. Nakashima & Warrick(2012) 참조.

4) Jang & Han(2013)도 이란 핵연료재처리시설 두 군데에 가해진 스턱스넷 공격을 사이버 전쟁의 형태로 이해한다. p.601 참조.

방군의 역할은 경제와 정치라는 두 가지 중요한 영역에 밀접하게 관련되어 있다. 인민해방군은 성격상 당군대이므로 일차적 목표는 공산당의 지배를 공고히 할 수 있도록 힘을 보장하는 것이고, 2차적 목표는 국가발전을 위한 강력한 안전 보장을 제공하고 국가이익을 수호하는 것이다. 중국의 국가이익은 국내적 차원에 의해서 동기화된 정치적, 경제적 목표와 관련된다.

다음으로, 중국의 사이버 안보전략의 개념적 논의를 정리해본다. 중국의 관점은 서방 국가 특히 미국의 사이버 안보전략과는 상당히 다르다. 중국은 사이버 안보 혹은 안전의 용어 보다는 네트워크 안전이나 정보 안전의 용어를 사용한다. 이런 점에서 보면 형태적인 측면에서 보아도 중국의 사이버 안보전략은 미국의 사이버 안보전략과 다른 것이다. 미국의 사이버 안보전략은 국가안보와 군사안보에 직접 관련되어 있다. 정보화와 정보기술의 혁신과 경제발전은 시장 영역의 문제로 인식되고 국가 안보와 구분되고 있다. 미국의 사이버 안보는 정치군사적 목적의 사이버 스파이를 다루는 NSA와 사이버 공격과 군사적 방어를 중심으로 하는 사이버사령부가 사이버컴(cybercom) 사령관의 통합적인 지휘하에서 움직인다는 점에서 이를 확인할 수 있다.

이에 사이버 안보전략을 국가안보와 경제발전의 영역과 대내대외적 차원으로 구분하는 통합적 비교분석틀을 다음과 같이 제시한다.

중국은 시장 경제를 표방하고 있고 자유무역을 지향하는 세계무역기구의 회원국이기도 하지만 실제로는 서구의 시장경제원리를 명실상부하게 제도화하고 있지 않다고 평가된다. 중국의 경우 사이버 안보 영역은 네트워크 안전과 정보화를 포함한다. 이런 점에서 중국의 사이버 안보전략에서는 정치군사적 차원의 국가안보와 정보기술의 혁신과 발전을 의미하는 경제발전이 인식에서나 제도적으로 분명하게 분화되어 있다고 보기 어렵다(Cheung, 2011). 앞에서 검토한 중국의 사이버 안보전략에 관한 국내외 선행연구에서 이러한 점을 확인할 수 있다. 중국의 사이버 안보전략을 논의할 때는 정치군사적 차원의 국가안보를 중심으로 다루는 서구의 사이버 안보전략과는 형태적으로 매우 다르다고 보아야 하는 것이다. 이런 맥락에서 본 연구에서는 중국의 사이버 안보전략을 통합적 시각에서 다루어야 한다고 주장하는 것이다.

또한 중국의 사이버 안보전략이 서구 국가와 차이를 보이는 부분 중의 하나가 국가안보 영역이나 경제발전 영역에서 공히 대외적 차원뿐만 아니라 대내적 차원을 포함한다는 것이다. 경제 발전의 영역에서 대내적 차원의 디지털 보호주의와 미국의 기술패권경계론은 사실은 동전의 양면에 해당되는 것이라고 볼 수 있다. 사이버 안보전략의 중국적인 특성은 국가 안보 영역에서 나타난다. 중국은 서구 국가와는 달리 국가 안보를 대외적 차원의 이슈로 이해하는 것이 아니라 전통적인 대외적 차원은 물론 대내적 차원을 포함하는 것으로 인식하는 것이다. 사이버 안보에 관한 한 중국은 정보관리와 통제를 통한 공산당 정권의 안정과 대내외적인 사이버 위협에 의한 정치적, 사회적 안정을 국가 안보의 영역에 포함시키고 있는 것이다. 네트워크 안전에서 인민해방군의 역할을 보면 이러한 점을 확인할 수 있다. 사이버 안보전략에서 인민해방군의 역할은 군사안보적 영역에 한정되어 있지 않고 경제와 정치라는 중국의 네트워크전략의 두 가지 중요한 영역에 밀접하게 관련되어 있다. 이것은 인민해방군은 성격상 당 군대(party army) 즉 중국공산당을 위한 군대라는 점을 반영하는 것이다. 인민해방군은 미국의 군대처럼 어느 세력이 정권을 잡고 있느냐와 상관없이 국민과 국가를 보호하는

Table 2. Framework of China's cybersecurity strategy

	National Security	Economic Development
Domestic	Communist Party Domination, and Political and Social Stability	Digital Protectionism
International	Military Network Protection and Network Attack Capability	US technology hegemony

데 봉사하는 국가 군대가 아니라는 것이다. 이러한 점은 인민해방군의 목표와 기능에 큰 함의를 가진다. 인민해방군의 일차적 목표는 당이 지배를 공고히 할 수 있도록 힘을 보장하는 것인데 군대작전이 중국 공산당의 목표와 연결되어 있는 것이다. 인민해방군의 2차적 목표는 국가발전을 위한 강력한 안전 보장을 제공하고 국가이익을 수호하는 것이다. 중국의 국가이익은 국내적 차원에 의해서 동기화된 정치적, 경제적 목표와 관련된다. 이러한 이유에서 인민해방군이 정치적 목표를 위해 네트워크 작전에 관여하고, 경제적 이득을 위해서 서구 개발 국가들에 대한 사이버산업스파이에 관여하는 것이 관찰되는 것이다. 여러 분석에서 드러나는 것처럼 2014년 홍콩의 반대세력의 모바일폰에 중국 군부대가 악성 웨어를 심은 것은 인민해방군의 활동이 공산당의 정치적, 경제적 목표와 연결되어 있다는 것을 잘 보여준다(Chang, 2014).

Ⅲ. 중국 사이버 안보전략의 성격

본 장에서는 다양한 이슈를 중심으로 중국 사이버 안보전략의 성격에 대해 논의하고자 한다. 이러한 이슈에 대한 분석은 중국 사이버 안보전략의 이념, 조직과 제도, 사이버 능력에 대한 통합적 분석에 필요한 선행적 연구다. 세 가지 이슈로 분류하여, 사이버 위협에 대한 인식을 검토하고, 중국 사이버 안보전략이 반응적이고 수동적인가 아니면 선제적이고 적극적인 성격을 보이는가 하는 점을 분석한 후, 사이버 안보 거버넌스의 제도화의 수준과 투명성 이슈를 검토하고자 한다.

첫째, 사이버 위협을 어떻게 인식하느냐 하는 점은 사이버 안보전략의 핵심적인 구성 요소를 이룬다. 이러한 인식에 따라서 사이버 안보전략의 이념적 측면, 거버넌스 구조의 측면, 사이버 역량의 측면에 영향을 미치기 때문이다. 중국에 대한 사이버 위협의 기원은 국내와 국외로 구분되는데 우선 중국 국내적으로는 사이버 위협은 사이버 조직범죄가 지배적인 사이버 위협에 해당한다. 중국 내에서 사이버 범죄는 주로 금전적인 동기에서 발생하는 것이 대부분인데 네 가지 형태가 얽혀 있다(Jianwei, *et. al.*, 2015: 90). 우선, 금전 자산의 절도인데 은행 계좌나 신용카드에서 돈을 훔치는 것을 말한다. 또, 네트워크 가상 자산의 절도가 있는데 온라인 게임 계정에서 가상화폐나 도구를 훔쳐서 현금으로 환금하는 것을 말한다. 다음, 인터넷 자원이나 서비스의 오용이 있는데 금전적 이득을 위해 해킹한 서버와 웹페이지나 감염시킨 스마트 기기들을 악용하는 것을 말한다. 마지막으로 악성 해커들이 해킹 기술, 도구나 기술 전문성을 판매하거나 교육하는 등 사이버 범죄를 지원하고 훈련하는 것을 통해 금전적 이득을 취하는 것을 말한다. 이러한 조직과 활동의 연결을 '사이버 절도 공급망'이라고 말하기도 한다. 이러한 사이버 절도 공급망은 중국 내에서 우려할만한 규모로 성장해온 온라인 지하경제의 온상이기도 하다. 중국 정부는 국내에서 일어나는 사이버 테러에 대해서도 매우 민감하게 인식하고 있는데 소수민족이나 분리주의 종교집단에 의한 사이버 테러와 정치적 목적을 가진 사회집단의 사이버 교란 행위들이 이에 해당한다고 볼 수 있다. 이러한 사이버 테러 집단들은 경제적 목적을 추구하는 사이버 조직범죄와는 달리 정치적 목적을 추구하는 점이 큰 차이점이라고 할 수 있다. 이러한 정치적 목적의 사이버 테러 위협은 중국 공산당 지배와 정권의 정치적, 이념적 정통성을 비판하고 부정한다는 점에서 사이버 조직범죄와 비교해 규모는 훨씬 작지만 중국 지도부에 의해 매우 심각하고 민감한 사이버 위협으로 다루어져 왔다.

중국 정부는 또한 사이버 위협이 국내에서 기원할 뿐만 아니라 외국에서 중국 내부로 침투한다고 인식한다. 중국은 미중 관계에서 이러한 사이버 위협을 심각하게 보고 있다. 중국 외부에 기원하는 사이버 위협의 경우 가장 지배적인 형태는 다른 국가, 특히 미국에 의한 사이버 첩보 수집과 스파이 행위라고 할 수 있다. 이러한 중국의 정부, 군대, 기업에 대한 미국 NSA의 스파이 행위는 미국 NSA의 사이버감시 프로그램의 폭로로 확인되는 결과가 생겼다(Chang, 2014: 28). 중국의 외교부 대변인은 스노든의 비밀문건 유출은 "다시 한 번 중국

이 사이버공격의 희생자라는 것을 보여준다"고 주장했다. 중국의 이러한 입장은 스노든 폭로 사건을 이용하여 중국이 사이버스파이에 대한 비난을 회피하고 비난을 미국으로 향하게 하며 큰 반향 없이 사이버 스파이 작전을 계속하려는 것으로 간주될 수 있다. 미국은 중국을 포함한 외국에 대해 사이버감시를 지속적으로 실시하고 있다. 2013년 6월 중국의 국가주석 시진핑의 미국 방문 전에도 미국 NSA는 중국 정부에 대해 사이버 첩보 수집을 했다고 한다(Aid, 2013).

중국의 경우 사이버 전쟁의 위협은 다른 국가들과 마찬가지로 현실적 사이버 위협으로 인식하지 않았다. 그러나 2010년 이란 핵물질 재처리시설에 대한 미국과 이스라엘의 사이버 공격과 교란은 이러한 인식을 바꾸는데 큰 영향을 미쳤다. 이와 함께 2009년 6월 미국이 사이버사령부를 설립한 것과 2011년 7월 미국 국방부의 사이버 안보전략 문서에서 사이버공간을 육지, 해양, 공중, 우주공간에 이은 전쟁의 또 다른 새로운 영역으로 선언한 것으로 인해 중국은 사이버 전쟁의 위협을 보다 현실적으로 인식하게 되었다. 그러나 미중관계에서 보아도 사이버 전쟁보다는 정치군사적 목적이든 상업적 목적이든 사이버 스파이가 더 현실적인 사이버 위협으로 인식되고 있다(Segal, 2016a: 5장). 2013년 이후 미중 사이버 안보 관계의 안정을 위한 두 국가의 협상 노력도 사이버 산업스파이 행위를 억제하는 데 초점을 맞추고 있다. 2015년 9월 시진핑 방미와 미·중 정상회담에서 합의된 사이버 협약은 국가에 의한 상업적 목적의 스파이 행위를 금지하는 내용을 주로 포함하고 있다(Segal, 2016b). 마지막으로 이러한 중국에 대한 국내외 사이버 위협은 또한 서로 연결되어 있다는 점이, 중국 정부의 사이버 안보전략의 큰 도전이라고 할 수 있다. 2000년대 이후 본격화된 중국의 정보화정책과 기술혁신 노력은 중국 정보기술 산업의 성장을 가져 왔지만 네트워크 안전과 정치적 목적의 정보 통제 정책으로 인해 네트워크 안전과 보호 및 개인정보보호와 사용자 보호에 대한 정책들이 소홀하게 되었다. 이로 인해 정보산업 부문에서 온라인 지하경제가 조성되고 이것을 온상 삼아 사이버 범죄가 만연하게 되는 결과가 생겼다. 이러한 정보기술환경은 의도하지 않게 외부로부터 사이버 스파이와 교란 활동이 중국 경제와 정부 부문으로 침투하게 되는 통로와 기회로 작용하게 된 것이다.

둘째, 대외적인 차원에서 중국의 사이버 안보전략이 수동적이고 반응적인가 아니면 적극적이고 선제적인 성격을 띠는가 하는 이슈가 있다. 현실주의적 시각에서는 중국의 사이버 안보전략이 선제적이고 적극적이라고 주장한다. 예를 들어, 초기에 중국의 사이버 안보전략이 수동적이었지만 점차 선제적인 성격을 강화하게 되었다고 주장한다. 미중 사이버 안보관계의 맥락에서 상호간 사이버 공격능력을 확대하게 되는 안보딜레마 현상이 형성되었다는 것이다(Kim, 2015a). 그러나 이러한 분석은 미중 관계에서 사이버 안보 위협을 지나치게 과장하는 것이고 양국간 사이버 협력을 위한 신뢰를 손상하는 것이라고 비판받고 있다(Lindsay, 2015c).

중국이 미국과 사이버 공간에서 각축과 경쟁관계에 있지만 중국이 미국을 선도하고 있다고 보기는 어렵다. 이와 관련해서는 두 가지 점을 지적하는 것이 필요하다. 우선 정보기술 혁신, 보안기술의 발전, 사이버 무기역량에서 중국은 미국을 추격하려고 노력하고 있지만 미국에 앞설 수 있는 우위를 가지고 있지 않다. 정보기술 부문에서 중국이 자주 보장과 자주 혁신을 강조하고 있지만 여전히 미국에 크게 뒤지고 있다는 것은 부인할 수 없는 현실이다. 중국은 사이버 안보 거버넌스 구축에서 미국을 앞서고 있다고 보기 어렵다. 중국이 2014년, 사이버 안보 거버넌스의 혁신을 시도한 것은 미·중 관계에서 일어난 일련의 사태와 밀접한 관계에 있다고 볼 수 있다(Sanger & Perlroth, 2014). 2009년 6월 미국이 사이버사령부를 설립하고 미국 NSA와 통합적으로 운영한 것과 2011년 7월 미국 국방부의 사이버 안보전략 문서에서 사이버공간을 육지, 해양, 공중, 우주공간에 이은 전쟁의 또 다른 새로운 영역으로 선언한 것이 중국의 사이버 전략에 큰 영향을 미쳤다고 볼 수 있다. 2013년 6월 미·중 정상회담에서 사이버 안보 이슈가 중요하게 다루어 졌고, 스노든 폭로 사건으로 미

국 정보기관의 대외적인 사이버 감시와 스파이활동이 매우 광범위하게 이루어져 왔다는 사실이 재인식되었다(Chang, 2014: 27-31). 2015년 9월 상업적 목적의 사이버 스파이를 미국이 집요하게 금지시키고자 중국을 압박한 점도 중국의 사이버 안보전략의 점진적 진화에 영향을 미친 요인으로 평가된다.

셋째, 낮은 제도화 수준과 투명성의 결여가 중국 사이버 안보전략의 중요한 특성이라고 볼 수 있다. 물론 이러한 사이버 안보와 관련된 제도와 정책의 투명성 이슈는 중국에 한정된 문제는 아니다. 정도의 차이는 있지만 어느 국가이든지 겪는 문제이다. 그러나 중국의 정치적, 제도적 환경으로 인해 사이버 안보 거버넌스의 낮은 제도화와 투명성의 결여가 중국에서 특히 문제로 지적되고 있다. 이러한 특성의 주요한 요인으로는 다양한 행위자와 조직이 사이버 안보 거버넌스에 관여하고 있다는 점을 들 수 있다. 공식적인 참여자는 중앙과 지방에 걸쳐서 다양하게 있고 국영기업, 민영기업, 대학, 연구소, 군대 등 여러 가지가 있다. 사이버 위협과 안보의 복합적인 성격에서 볼 때 이러한 공적, 사적 부문에 걸쳐 있는 다양한 행위자와 조직의 권한과 책임을 분명하게 정하는 것이 매우 지난한 과제가 될 수밖에 없다. 또한 사이버 안보와 안전의 대상과 범위가 물리적 인터넷 인프라에서 정권과 이념의 정통성, 기업의 영업 활동과 재산권, 사용자들의 개인 정보에 이르기까지 매우 다양하고 이질적이어서 행위자와 조직의 권한과 책임을 분명하게 설정하는 것이 용이하지 않다. 서구 사회와는 달리 중국에서는 정치사회적 안정을 위한 정보관리와 통제가 국가조직에 의해 광범위하게 이루어짐으로써 제도적 투명성의 문제를 더 악화시키고 있다.

이러한 제도적 투명성의 부족은 국내적으로 부정적인 외부효과를 초래할 뿐만 아니라 대외관계에서도 부정적인 영향을 미치고 있다. 국내적으로는 중국의 인터넷 환경의 고질적인 문제로서 국내 사이버 범죄 활동이 감소하지 않고 오히려 확대되고 있다는 점이 지적되고 있다. 중국의 경우 애국주의 해커들이나 사이버 민병대 조직이 대외적 논쟁에 참여하는 경우가 많은데 이러한 점으로 인해 사이버 범죄활동에 대한 느슨한 규제와 법 집행이 의도하지 않은 결과를 초래할 수도 있다.

사이버 안보에 관련된 제도적 투명성의 부족은 또한 대외관계에서도 부정적인 영향을 미친다. 특히 미중 사이버 안보 협력에서 신뢰성의 문제를 야기하는 요인으로 작용한다. 흔히 미·중간 사이버 안보경쟁을 냉전기간의 미국과 소련 간 핵무기 경쟁과 비교하는 경우가 있다. 이 두 가지 전략적 경쟁의 가장 큰 차이는 투명성의 원칙이 지켜지느냐 그렇지 않느냐 하는 점이다. 핵무기 경쟁에서 상호간 억지전략이 핵전쟁의 위험을 방지하는 요인으로 작용한 것은 제도와 능력의 측면에서 투명성의 원칙이 어느 정도 지켜졌기 때문이다. 그러나 사이버 안보 경쟁에서는 제도, 전략, 사이버 역량의 측면에서 투명성의 원칙이 지켜지기가 훨씬 더 어렵다고 할 수 있다. 예들 들어 미국과 중국은 사이버 공격의 인식에서도 큰 차이를 보인다. 미국은 사이버 공격을 보다 엄격하게 군사적인 관점에서 정의하는데 비해 중국은 이 보다 더 넓게 정치적, 이념적, 군사적인 관점에서 정의하고 있다(Segal, 2016a: 91-94). 또한 사이버 전술과 역량의 경우에도 은닉과 기만이 훨씬 더 용이하게 이용될 수 있다. 이러한 투명성의 결여는 상호간 전략적 신뢰 형성과 인식에 악영향을 미치는 것이다. 이렇듯 사이버 전략에 있어서 제도적 투명성의 결여는 대내외적으로 사이버 협력을 어렵게 하고 사이버 갈등을 심화시키는 요인으로 작용한다고 볼 수 있다.

Ⅳ. 중국 사이버 안보 전략의 분석

1. 이념과 목표

중국에서 최근에는 사이버 안보라는 용어를 사용하는 경우가 늘어나고 있다고 하지만 전통적으로 사이버 안보라는 용어대신 정보 안전 혹은 네트워크 안전의 용어를 선호해 왔다. 이 두 가지 용어 중에서 네트워크 안전이 사이버 안보 혹은 안전에 더 가까운 개념이고 정보안전은 이 두 용어보다 훨씬 더 넓은 개념이다(Chang, 2014: 24). 인터넷을 의미하는 네트워크나 사

이버는 정보기술의 발전을 배경으로 사용되는 것이지만 정보는 정보기술의 맥락과도 관련되지만 이것을 훨씬 넘어서는 개념이기 때문이다. 중국의 사이버 안보를 논의할 때는 네트워크 안전과 정보 안전을 통합적으로 고려하는 것이 필요하다. 2014년 초 중국의 사이버 안보전략의 최고 의사결정 조직이 '국가정보화영도소조'에서 '중앙네트워크안전·정보화영도소조(中央网络安全和信息化领导组)'로 재편된 데서 이러한 통합적 인식의 필요성을 확인할 수 있다(Cho & Chung, 2016: 159-160).

중국의 사이버 안보전략의 바탕에 깔려 있는 이념적 요소는 다른 국가전략과 마찬가지로 기본적으로 사회주의적 이념과 민족주의적 이념으로 구성되어 있다고 볼 수 있다. 조금 단순화하면 사회주의적 요소는 국내적으로 중국 공산당 정권의 지배를 확고히 유지하는 것이고 더 나아가 이를 통한 국내정치적, 사회적 안정을 확보하는 것을 말한다. 이러한 이념과 관련해서는 정보통제와 관리가 사이버 안보전략의 중요한 요소로 상정된다. 또한 민족주의적 요소는 대외적으로 사이버공간의 국제질서에 있어서 국가주권의 확립을 위한 것이다. 사이버 안보전략의 민족주의적 이념은 이른바 정보기술에 의해 창출된 새로운 질서 공간인 사이버 공간에서 정보주권, 네트워크 주권, 인터넷 주권, 사이버 주권 원리를 적용하고 실현하는 것을 의미한다. 중국은 정보기술을 정치경제적 발전과 사회문화적 변화의 수단으로 수용했지만 서방 국가들이 전제하고 또 주장하는 자유롭고 개방적이며 글로벌한 범위로 작동하는 인터넷의 성격을 인정하지 않았다. 정보기술과 인터넷의 자유롭고 개방적인 요소가 중국의 공산당 지배에 바탕을 둔 국내정치적 안정, 국가안보, 그리고 정보기술의 혁신 및 경제발전에 부정적인 힘으로 작용하지 않도록 하는 데 사이버 안보전략의 궁극적인 목표를 두고 있다고 할 수 있다. 이러한 중국의 사이버 안보전략의 정책목표는 보다 구체적으로 세 가지 측면으로 나누어 논의할 수 있다.

첫째, 정치적 측면에서 정책목표는 공산당 지배의 지속과 국내 정치적, 사회적 안정의 기본 목표 아래 여러 가지 세부 목표를 추구한다. 우선 정보관리와 정보 유통의 제한을 추구한다. 중국 정부는 제약 없는 인터넷 접근이나 통제되지 않은 정보의 배포는 중국 공산당 지배의 정권 안정과 권력에 심대한 위협이 된다고 우려한다. 이러한 위협에 대처하기 위해 중국은 소셜 미디어나 이동통신에 실명 등록을 의무화하는 실명제를 실시한다. 이러한 조치들은 온라인 사용자들의 이익을 보호하고 인터넷 활동의 신뢰성을 높이기 위한 것이라고 하지만 사실은 국가 기밀을 누출시키고 국가안보와 이익을 훼손하고 인종 적개심, 차별 혹은 사회질서를 교란하는 불법적 집회를 조장하는 정보의 배포를 제한하기 위한 목적이 크다. 또한, 이러한 정보 관리와 유통의 제한을 통해 소위 "분리주의, 극단주의, 분열주의자들"의 사이버 교란이나 불안을 조성하는 사이버 활동을 단속하고 통제하는 것을 중시한다. 2014년 10월 중국 관영매체의 보도에 따르면 중국 정부는 2011년부터 이루어진 온라인 단속에서 사이버범죄에 관련된 3만 명의 혐의자를 잡았다고 밝혔다. 2011년부터 3년간 북경 공안국은 1,700만개의 불법적인 온라인 메시지를 삭제했으며 테러활동에 관련된 50명의 혐의자를 억류했다고 한다(Chang, 2014: 25).

중국의 국가 행위자들은 해커들과 유사하게 악성 웨어를 사용하여 정치적으로 중요한 국내 감시 대상을 감시하거나 정보를 훔친다. 민주주의를 주창하는 비정부 집단, 중국내 정치적 반대파, 홍콩의 대학들이 이러한 대상에 포함된다. 특히 중국은 홍콩의 반대 활동가들에 대한 감시를 강화해 왔다. 이러한 정보통제 외에 중국 정부는 감시 기술(모바일 원격접근트로이목마 악성웨어, mRAT)을 이용하여 모바일 기기를 감염시켜 대량의 정보를 빼내고 있다. SMS, 이메일, 메신저의 내역, 사용자 이름, 비밀번호, 접촉 정보 등이 이러한 정보에 포함된다. 중국 정부는 이러한 정보를 분석하여 저항활동의 성격과 내용을 파악하여 저항 활동을 관리하려고 노력하는 것이다.

중국은 대외문제에서도 비정부 행위자를 고용하여

다른 국가와의 분쟁에 대해 '상당한 힘이 행사되는 위협'을 하도록 하거나 그러한 사이버 공격을 하는 것을 막지 않는다. 이러한 비정부 행위자들의 국가와의 관계는 경계를 명확하게 짓기 어렵다. 그러나 외국과의 양자 혹은 다자 분쟁의 발발과 분쟁 적대국을 향한 중국의 악성 사이버활동의 빈도의 증가 간에는 상관관계가 있는 것도 사실이다. 예를 들어 일본의 경우 중국과의 해양 영토 분쟁이 시끄러워지자 일본 정부 웹사이트와 시스템에 대한 사이버 침해활동이 크게 증가하였다. 2012년 9월 일본 정부가 일본은 분쟁 중인 센카쿠 열도에 있는 세 개의 섬을 구입한다는 것을 선언했을 때 일본 정부의 웹사이트가 공격을 받았던 것이다. 중국의 경우 정부가 비정부 행위자들에 의한 경제적, 산업적, 군사적 사이버 스파이행위와 연관이 있다는 의심은 받으나 확인되지는 않는다. 중국 정부 행위자와 국가 후원 비국가 행위자간의 모호한 경계로 인해 외부의 법집행기관, 정책결정자들과 정보기관들이 중국을 쉽게 비난하기 어렵게 되어 있다(Chang, 2014: 24).

둘째, 중국 사이버 안보전략의 경제적 동인은 두 가지 요소를 가지고 있다. 지속적인 경제성장의 보장과 국내 사이버범죄활동의 억제가 바로 이것이다. 우선, 중국은 사이버 산업스파이를 감행함으로써 특히 미국에 대항하여 국내기업의 경쟁력을 유지하기 위해 노력해 왔다. 사이버산업스파이는 국가나 비국가행위자들이 네트워크에 침투하여 많은 양의 산업정보(영업비밀, 연구개발 성과, 제품 등)를 탈취하는 것을 말하는데 중국이 주된 당사자로 지목받아 왔다. 중국의 상업적인 목적을 띤 사이버 산업스파이행위는 미·중간 사이버 갈등의 주요 요인으로 작용했다. 미국은 중국에 대해서 중국의 기업과 산업계를 위한 특히 국가 행위자들에 의하거나 국가에 의해 방조된 행위자들에 의한 상업적인 목적의 사이버 산업스파이는 국가들 간 암묵적으로 인정해온 통상적인 사이버 스파이와는 달리 금지되어야 한다고 요구했다. 2014년 5월 20일 미국 법무부는 펜실베니아주 미국 연방지방법원에 왕둥 등 중국 한 군부대 소속 장교 5명을 산업스파이와 기업비밀절취 등 6개 혐의로 기소했다. 미국 법무부에 따르면 이들 5명은 웨스팅하우스와 US스틸 등 5개 기업과 미국 철강노조의 컴퓨터를 해킹해서 피해 기업의 제품이나 재무구조에 대한 기밀 정보를 빼냈으며, 이로 인해 해당 기업과 경쟁관계에 있던 중국 기업들이 큰 이익을 보았다고 주장했다(Electronic Times Internet, 2014.6.15). 중국은 오히려 미국이 중국 정부와 기업을 해킹해왔다고 반박했다. 중국 국방부는 미국이 사이버 안보를 강화하기 위해서 이번 사건을 조작했다고 비난했다. 중국 국방부 대변인은 "미국은 사이버 안보를 강화하고 싶을 때 사이버 위협을 핑계로 댄다"며 "미국의 중국군 기소는 계획적이며 불순한 의도를 갖고 있다"고 비판했다(Electronic Times Internet, 2014.6.15).

중국 정부는 사이버 안보전략을 통해 국내적으로 중국 내에서 사이버해킹과 범죄활동이 증가하는 것에 대응하기 위해 노력하고 있다. 중국 스스로가 사이버해킹과 범죄로 중국경제가 크게 저해될 수 있다는 것을 인정하고 있는 것이다. 이러한 사이버해킹과 범죄에는 은행계좌나 신용카드 절도를 통해서 개인, 은행, 개인의 재산을 절취하는 것, 온라인 공간에서 아이디를 훔치는 것, 인터넷 서비스의 취약점을 이용하여 인터넷 자원과 서비스를 남용하는 것, 사이버범죄자들에게 바이러스, 공격 도구, 훈련을 판매하는 것들이 포함된다. 서방의 전문가들에 따르면 중국에서 해적판 기술의 이용과 배포가 광범위하게 일어남으로써 사용자들의 효과적인 보안 업데이트와 패치가 어렵게 되어 사이버범죄자들이 이러한 취약점을 악용하는 경우가 자주 많이 생긴다는 것이다. 중국의 관련 연구소에 따르면 2013년 점검받은 중국 내 컴퓨터의 54.9%가 바이러스로 감염되어 있고 2,714개 정부 포털 중에서 1,367개가 취약점을 가진 것으로 보고되었다(Chang, 2014: 23).

셋째, 중국 사이버 안보전략의 군사적 측면은 전쟁에서의 네트워크 전략과 작전과 이를 통한 국가 방위와 안보를 확보하는 것을 말한다. 군사 분야에서 네트워크와 정보기술에 관한 중국의 담론은 몇 십년동안 존재해 왔지만 정보기술과 정보전에 대한 중국의 접근방법의

큰 전환점은 1990-91년 걸프 전쟁에서 미국이 고도 군사기술을 도입한 것에서 비롯되었다(Mulvenon, 1999). 이후 중국은 미래의 전쟁에서 정보통신기술의 중요성을 강하게 강조하고 "2050년까지 정보화된 환경에서 국지전쟁"에 승리할 것이라는 목표를 내세웠다.

네트워크 작전은 대만을 포함한 다른 영토적 분쟁이나 해상 갈등 혹은 미국을 포함하는 군사 작전 시나리오에서 중요한 역할을 한다. 중국의 전략가들은 정보화로 "새로운 패턴의 사이버화 된 전쟁이 나타날 것"이라고 가상해 왔으며, 인민해방군은 정보전쟁(예: 네트워크 연결을 둘러싸고 적을 공격하는 것)과 같은 전쟁 상황의 시나리오와 지위, 통제, 통신, 컴퓨터, 첩보와 정찰(C4ISR)에서 정보기술의 잠재적 응용에 관해 잘 인식하고 있다. 군사전략학에서는 전쟁 시 고도 기술의 진화 및 전개와 국가안보와 발전 이익에 대한 정보 영역의 중요성을 논하고 있다. 최근에 업데이트한 2013년 판 '군사전략학'은 네트워크 영역의 갈등에 대해서 많은 부분을 할애하고 있으며 네트워크 영역에서의 군사갈등의 형태(네트워크 정찰, 네트워크 공격과 작전, 네트워크 억제 등)와 잠재적인 군사 갈등에 대비하는 방법을 논하고 있다(Chang, 2014: 25).

Lindsay(2014: 30-32)에 따르면 중국은 정보기술을 혁명적으로 영향을 미치는 기술로 이해한다. 공식적인 중국의 군사교본과 전문적인 군사학 문헌에서는 사이버전쟁을 군사분야의 혁명으로 인식한다. 핵전쟁이 산업시대의 전략적 전쟁이었던 것과 마찬가지로 네트워크전쟁이 정보시대의 전략적 전쟁이라고 본다. 네트워크 전쟁은 매우 높은 수준의 전쟁으로 파괴적인 결과를 낳고 국가안보와 생존과 관련되어 있다. 사이버무기는 힘의 증폭자로서 다른 국가의 경제를 마비시키고 전체 주민들에게 사회적, 심리적 영향을 미치는 것과 같은 전략적 효과를 위한 통합적 수단이다. 네트워크 전쟁이 적대 국가체제에 대해 부분적 혹은 대규모적인 마비를 시키며 악성 바이러스가 적의 지휘통제체제에 침투하면 막대한 파괴를 결과할 수 있고 네트워크 전쟁은 미래의 전쟁에서 적을 마비시키는 중요한 수단이 될 수 있다.

중국은 사이버 전쟁 혹은 네트워크 전쟁에서도 일반 전쟁에서와 마찬가지로 '적극적 방어'의 원리를 주장하는데 이는 주도권을 잡기 위한 공세를 강조하는 것이다.[5] 중국군 교범은 네트워크 전쟁의 시작이 작전의 성과를 결정한다고 주장한다. 기술적으로 앞선 적을 공격할 때 핵심적 대상은 정보시스템인데 그것을 비밀리에 선제공격함으로써 적의 조직, 전략적 결정, 국가경제의 마비를 담보할 수 있다. 상대적으로 약한 중국 군대가 초기에 마비시킬 정도의 타격을 가하며 적에 대해 정보우세를 달성할 수 있다는 것이다. 이러한 중국의 정보전쟁의 전략과 전술은 두 가지의 사태 변화와 관계가 깊다. 하나는 1990년대 미국에서 일어난 군사분야 혁명(RMA)의 움직임이며 다른 하나는 1990년대 초반 이후에 벌어진 이라크 전쟁, 발칸 반도의 전쟁이다. 중국은 이라크 전쟁에서 미국이 압도적 군사적 우세를 보인 것은 미국의 하이테크 전력뿐만 아니라 동시에 전개한 정보전 혹은 네트워크전에 힘입은 바에 크다고 분석하고 있다. 중국은 특히 2010년 이후 미중 사이버 안보 갈등이 고조되면서 정보전과 네트워크 전쟁에 대한 연구와 함께 사이버 전력을 강화하기 위한 제도적, 재정적 노력을 기울이고 있다(Lindsay, 2014).

2. 조직과 제도

중국의 사이버 안보전략의 추진을 위한 조직과 제도의 발전은 2014년 이전과 이후로 크게 구분된다. 2014년 이전에는 정책결정 조직이 체계를 이루지 못했으며 중앙적인 정책조정도 잘 이루어지 못했다. 2014년 들어 가장 두드러진 변화는 시진핑을 조장으로 하는 '중앙네트워크안전·정보화영도소조'(이하 중앙인터넷영도소

5) 중국의 네트워크 전쟁의 전략적 원칙인 '적극적 방어'를 서방 국가들이 인정하는 것은 물론 아니다. 서방 전문가들의 평가에 의하면 중국의 네트워크 전략은 네트워크 공격을 포함할 뿐만 아니라 사이버 공간에서 공격과 방어는 현실 공간보다 구분하기가 훨씬 더 어렵기 때문이다.

Table 3. Cybersecurity and informatization leading group

Leadership
Chair: Xi Jinping (Central Military Commission Chairman, CCP general secretary, PRC president)
Vice-Chair: Li Keqiang (premier)
Vice-chair: Liu Yunshan (Standing Committee, Central Party School president)
Politburo and senior leaders
Ma Kai (vice-premier)
Wang Huning (Central Policy Research Office, director)
Liu Qibao (Central Propaganda Committee, director)
Fan Changlong (Central Military Commission, vice-director)
Meng Jianzhu (Central Political-Legal Committee, secretary)
Li Zhanshu (Central Committee General Office, director)
Yang Jing (Central Secretariat, secretary)
Zhou Xiaochuan (governor of the People's Bank of China)
Ministries involved in cybersecurity policy implementation
CILG office director: Lu Wei (SCIO vice-director and SIIO/CAC director)
Guo Shengkun (minister of public security)
Fang Fenghui (chief of the PLA General Staff)
Wang Yi (minister of foreign affairs)
Xu Shaoshi (National Development and Reform Commission, director)
Yuan Guiren (minister of education)
Wang Zhigang (Ministry of Science and Technology, secretary)
Lou Jiwei (minister of finance)
Miao Wei (minister of industry and information technology)
Cai Wu (minister of culture)
Cai Fuchao (State Administration of Press, Publications, Radio, Film, and Television director)

※ Source: Lindsay(2015b: 14).

조)가 출범했다는 점이다. 2014년 2월 27일 시진핑은 '국가 안보와 국가 발전 측면에서 네트워크 안전 및 정보기술을 혁신하고 개발하는 것이 중요하다'고 말했다(Cho & Chung, 2016: 159). 사이버 안보가 없다면 중국의 국가안보도 없다는 것이다.

영도소조(領導小組)는 중국의 공식화된 통치조직은 아니지만 국가안보나 외교, 당무 등 중요한 핵심적 국가정책 영역에서 소수의 최고 정치지도자들에 의해서 구성되고 또 주도하는 정책결정단위이다. 영도소조는 정치체제 내의 최고 지도자들과 정보를 생산하고 정책을 집행하는 주요 관료기구들 사이에서 가교 역할을 한다. 각각의 주요한 영도소조는 그들과 관련된 기능적인 직무의 정점에 위치하면서 해당 당, 정부, 군대의 관료기구들을 영도한다(Lieberthal, 1995).

2014년, 새롭게 중국의 최고지도자로 등극한 시진핑 국가주석이 새롭게 출범한 '중앙인터넷영도소조'를 직접 지휘한다는 것은 중국의 사이버 안보전략이 국가정책 의제에서 높은 우선순위를 차지하게 되었다는 것을 의미한다. 이것은 당, 군대, 정부의 관료기구 내에서도 사이버 안보전략을 담당하는 조직과 제도들이 정비되고 이러한 조직과 제도들의 관계가 재설정된다는 것을 의미한다.

2014년 이후 이러한 제도적 발전은 무엇보다 사이버 안보 이슈를 둘러싼 대외적 환경의 변화를 반영하는 것이다. 우선 2012년 6월 미국 언론에서, 2008~2010년 사이 이란이 겪은 핵연료재처리시설에 대한 스턱스넷 공격이 미국과 이스라엘 정부에 의해서 시도된 것이라는 사실이 폭로되었다.[6] 또 2013년 6월 미국 정보기관 NSA의 대대적인 사이버 감시활동에 대한 스노든(Snowden) 폭로 사건으로 미국의 사이버작전과 스파

이활동의 위협을 직접적으로 경험하고 인식하게 되었다.[7] 또한 미·중 관계에서도 2013년 6월 초 미중 정상회담에서 처음으로 사이버 안보 이슈가 중요하게 다루어졌으며, 2014년 5월 미국 재무부가 중국의 인민해방군 장교 5명을 미국의 기관과 기업에 대한 사이버 산업스파이 혐의로 미국 재판정에 기소한 사건이 발생하였던 것이다.

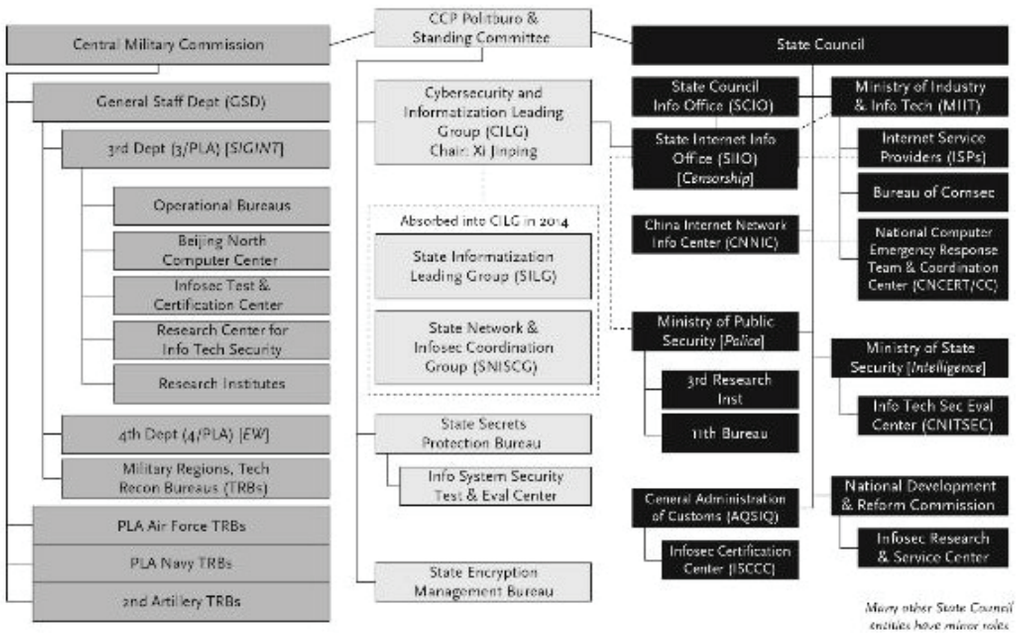
이러한 중앙인터넷영도소조의 구성과 함께 중요한 것은 사이버안보와 정보화 집행조직을 일원화하여 집행을 보다 체계화하고 효율화하는 것이다. 이러한 집행의 체계화를 위해 부조장은 중국 권력 서열 2위인 리커창 국무원 총리와 류윈산 중앙서기처 서기가 맡고 조원들도 사이버 안보 관련 부서의 책임자를 거의 포함시켰다. 정보기술산업을 담당하고 2014년부터 시작된 대규모 반도체산업 육성계획 책임자이며 국무원 부총리인 마카이(马凯), 국가신문출판광전총국 차이푸차오(蔡赴朝) 국장, 국무원 공업정보화부 미아오웨이(苗圩) 부장, 류치바오(刘奇葆) 공산당 중앙 선전부장, 리잔슈(栗战书) 공산당 중앙판공청 주임, 공산당 중앙 군사위원회 판창롱(范长龙) 부위원장, 궈셩군(郭声琨) 공안부장, 왕 이(王毅) 국무원 외교부장, 러우지웨이(楼继伟) 국무원 재정부장 등 사이버/네트워크 안전정책의 집행에 관련된 핵심 기관장들이 포함되었다.

2005~2013년 운영되었던 국가정보화영도소조는 경제구조의 현대화를 위한 정보통신산업의 발전에 중점을 두고 정책을 추진했다. 국가정보화영도소조에서 제시하는 정책에 따라 국무원 공업정보화부에서 정책을 집행하였고, 사이버 공간상의 취약성을 분석하고 평가하는 기관은 그 산하 인터넷네트워크정보센터(互联网络信息中心, CNNIC), 국가인터넷사고긴급대응팀(国家互联网应急中心, CNCERT/CC)에서 담당하여 보안 기술을 개발해 나갔다.

2014년 이후에는 시진핑이 직접 지휘하는 중앙인터넷영도소조에서 전략을 수립한 후 집행권한과 기능이 강화된 국가인터넷정보판공실(CAC, Cyber Administration of China)이 집행을 총괄한다. 판공실은 기존 공업정보화부 산하 조직인 인터넷네트워크정보센터(CNNIC), 국가인터넷사고긴급대응팀(CNCERT/CC) 등을 총괄하고 안전개혁위원회, 국가안전부, 공안부, 중국과학원 등의 사이버 안보 관련 정책 집행을 총괄하는 역할을 담당한다. 또한 중앙군사위원회 내 네트워크 안전 관련 과학기술교육을 지원하는 역할을 담당한다. 실무담당으로 루웨이(鲁炜) 당 중앙선전부 부부장이 판공실 주임을 맡음으로써, 중국 지도부가 직접 사이버 관련 기술개발과 국내 사이버 및 정보 통제를 중요하게 다루기 시작했음을 알 수 있다(Cho & Chung, 2016: 160). 이러한 중앙 정부의 조직뿐만 아니라 지방정부도 사이버 안보 부분에서 상당한 자율성을 갖고 있으며 중앙의 예산을 차지하기 위한 경쟁을 치열하게 벌이고 있다. 또 인민해방군은 국무원과 같은 국가 조직과는 독립적으로 공산당에 직속되어 있는데, 네트워크 안전과 정보안전을 위한 군사 및 정보활동을 책임지는데 그치는 것이 아니고 일부 민간 부문도 책임지고 있다. 예를 들면 수송 부문에서 사이버 안보 임무는 인민해방군의 영역에 속한다. 이렇듯 중국의 사이버 안보와 관련된 조직과 제도들은 당, 군부, 국무원의 여러 부서가 관련되어 있고 지방 정부들도 참여하고 있어서 정책조정 메커니즘의 작동이 효율적이고 효과적으로 작동하기 어렵다는 문제를 안고 있다. 2014년 시진핑이 직접 책임지는 새로운 중앙인터넷영도소조가 출범하고 집행을 총괄하는 국가인터넷정보판공실의 권한이 강화되었지만 정책집행 기능이 효과적으로 조정되고 제도적으로 공식화된 거버넌스 구조를 형성하는데 까지는 이르지 못하고 있다(Lindsay, 2014).

중국은 사이버 안보 관련 조직을 개편하고 또 사이버 안전법 제정을 통해 사이버 공간 통제의 제도적 기반을 마련했다. 2015년 사이버 안전법을 제정하고 제1장 제1조에서 '사이버 주권과 국내 네트워크 구축, 운영, 보

6) Segal(2016a: 2)는 일련의 사건이 일어난 2012-2013년을 사이버전쟁 원년이라고 주장한다.
7) 스노든 폭로에 의하면 화웨이 등 중국 통신회사에 대한 감시활동뿐만 아니라 중국 인민해방군에 대한 감시도 행해졌다고 한다.



※ Source: Lindsay (2015b: 9)

Figure 1. China's national cybersecurity system

호, 사용, 관리와 감독 등에 적용한다'고 명시하고 있다. 법적 근거를 마련함으로써, 국가가 중앙에서 국내 사회 안정과 경제적 이익을 보호하기 위해 사이버 공간을 포괄적으로 통제할 수 있게 된 것이다. 이를 바탕으로 중국은 거시적으로는 국가 안보, 미시적으로는 사회, 기업, 개인 이익에 악영향을 미치는 유해 활동에 대응하여 인터넷 공간을 보호하고자 한다. 특히, 국내의 사회적· 정치적 규율과 가치, 또는 주권에 위협을 가하는 사이버 공격에 강력한 대응 자세를 견지하고 있다(Cho & Chung, 2016: 161).

2014년 이후 중국 사이버 안보전략의 추진을 위한 조직과 제도가 상당히 발전되었지만 여전히 여러 가지 문제점을 노정하고 있다(Lindsay, 2014: 16-18). 우선 중국의 궁극적인 지배 권력인 중국 공산당이 정치적 '정보 안전'에 사로잡혀 있어서 사이버 안보전략의 목표인 효과적인 기술적, 제도적 네트워크 안전이 실현되지 못하고 있다. 〈Figure 1〉에서 보는 바와 같이 네트워크 안전과 정보 안전을 위한 중국의 조직과 제도들은 다양하고 파편화되어 있으며 특히 사이버 안보와 안전을 위한 국내적 법집행이 느슨하고 불균등하다. 이러한 환경에서 중국 국내에서는 사이버 범죄가 크게 만연되어 있고 디지털 지하경제의 규모가 다른 국가와 비교해서 매우 크다. 국내에서는 사이버 공격을 자제하는 동구유럽의 해커들과는 달리 중국의 사이버 범죄조직들은 느슨한 법집행의 틈을 타서 국내 대상을 해킹하는 데 주저하지 않는다. 해킹 도구들이 바이두와 같은 소셜 네트워크를 통해서 공공연하게 거래되며 2011년 사이버 범죄가 국내경제에 미친 피해가 8억 달러를 상회하고 사용자와 웹사이트의 20% 이상이 해킹 피해를 받았다. 이러한 국내 사이버 범죄의 만연은 국내 경제질서와 사회질서에 부정적인 요인으로 작용하는데 그치지 않고 외국 정보기관의 사이버 스파이 활동이 침투하는 네트워크 환경이 생길 수 있다는데 문제가 있다.

3. 사이버 안보 능력

중국은 공식적으로는 사이버 군사력을 보유하고 있지 않다고 주장한다. 그러나 중국 인민해방군 연구소에 의해 저술되고 권위가 인정되고 있는 '군사전략학' 최신판에서는 세 가지 형태의 사이버 전력의 존재를 인정하고 있다(Segal, 2016a: 93-94). 첫째, 인민해방군 사

이버전 전력이 존재하며 공격과 방어의 임무를 수행한다. 둘째, 국가안전부(미국 CIA에 해당)와 공안부(미국 FBI에 해당)의 특수전문인력은 공격을 수행하는 권한을 보유하고 있다. 셋째, 디지털 공격을 위해 '외부 조직체'를 운영하고 있다.

우선, 중국 인민해방군은 상당한 재정 자원, 인력 및 기술적 전문성을 보유하고 있으나 작전의 초점과 경험은 첩보 작전에 집중되어 있다. 인민해방군의 사이버 작전을 위한 인프라는 인민해방군 총참모부 3부와 4부에 귀속되어 있는데 3부는 신호 정보와 네트워크 방어를 책임지는 미국의 NSA에 비견될 수 있고 4부는 전자전을 주로 담당한다. 전문가들은 중국 사이버전 군사력의 성격을 평가하기 위해 컴퓨터 네트워크 활용(computer network exploitation)과 컴퓨터 네트워크 공격(computer network attack)을 구분한다. 컴퓨터 네트워크 활용은 첩보 활동을 주로 의미하며 컴퓨터 네트워크 공격은 사이버 교란을 위한 네트워크 작전을 의미한다. 한 연구에 의하면 중국의 네트워크 작전 능력은 공격보다는 스파이 혹은 첩보활동에 더 치중되어 있다고 분석되고 있다. 컴퓨터 네트워크 공격은 2010년 이란의 핵연료재처리시설에 가해졌던 스틱스넷 공격처럼 핵심 인프라에 대한 공격과 교란을 의미한다. 그러나 네트워크를 통해서 이루어지는 첩보 활동과 네트워크 공격이 확연히 구분되는 것은 아니다. 첩보 활동이 네트워크 공격을 시작하는 준비 활동으로 여겨질 수 있는 상황도 생길 수 있기 때문이다. 2010년 이후 중국은 네트워크 공격 능력의 향상에 더 큰 관심과 정책 노력을 기울이고 있다고 분석되고 있다(Lindsay, 2014: 33).

중국의 경우 정부 행위자나 군대 조직과 같은 사이버 행위자들 외에 제3의 세력들이 존재한다고 보는 관점도 있다. 애국주의 해커나 대학과 연계된 사이버 민병대들이 바로 이러한 세력들이다. 그러나 이러한 사이버 단위들이 중국 정부나 군대와 어떤 관계를 맺고 있는지 분명하지 않다. 서방의 전문가들은 사이버 범죄 집단과 달리 중국 정부에 의해 이들의 사이버 공격 행위나 사이버 산업스파이행위가 암묵적으로 묵인되거나 방조되고 있다고 분석하고 있다(Lindsay, 2014: 32).

또한 2000년대에 들어 중국의 사이버 안보 예산이 크게 늘어났다. 중국의 사이버 예산에 관한 자료가 거의 공개되고 있지 않지만 예산과 재정 투자의 증가를 간접적으로 확인할 수 있다. 한 분석에 의하면 중국의 정보 안전산업의 지출이 2003년 5억 달러의 규모에서 2011년 28억 달러로 크게 증가했다(Lindsay, 2014: 18).[8)]

앞에서 제시한 사이버 위협 유형론과 관련시켜 보면 중국의 경우 최근까지는 중국의 경우 최근까지는 안보와 군사적 목적의 사이버 첩보 역량의 구축에 노력을 기울여 왔고 또한 정부 행위자나 비정부행위자들에 의한 상업적 목적의 사이버 산업스파이 활동에 큰 관심을 경주해 왔다. 사이버 전쟁을 위한 사이버 역량의 구축은 최근에 와서 본격적으로 이루어지고 있다고 평가할 수 있다. 이러한 사이버 역량의 구축은 다음과 같은 측면들을 포함한다(Chang, 2014: 27-28). 첫째, 집권화된 지휘구조를 개발하여 군대, 국가, 조직들, 산업 및 개인들까지 통합시킨다. 둘째, 네트워크전쟁에 필요한 민간 및 군 인력을 양성하며 미국, 영국, 한국의 유사한 조직 모델을 참고하여 인민해방군은 네트워크전쟁 부대, 사이버군대, 사이버예비부대를 육성한다. 셋째, 더 높은 효과성을 위해 공격과 방어 양면의 모든 조치들을 충분히 활용한다. 마지막으로 우수한 토착기술과 혁신을 광범위하게 확보, 이용해야 하며 또한 연구개발을 기반으로 신 공격무기들을 개발해야 한다.

V. 결론과 함의

본 연구는 중국의 사이버 안보전략은 서구 국가 중에서 특히 미국의 사이버 안보전략과는 다른 관점에서 분석할 필요가 있다는 문제의식을 바탕으로, 국가안보와

8) 중국의 네트워크와 정보 안전은 국가의 영역이라는 점에서 이 분야 산업 지출의 규모는 정부 예산의 증가를 반영한다고 볼 수 있다.

경제발전을, 다른 한편 대내적 차원과 대외적 차원을 통합적으로 고려하는 분석틀이 필요하다고 주장한다. 이러한 통합적 시각에서 중국 사이버 안보전략의 중요한 구성요소로 이념과 목표, 조직과 제도, 사이버 역량을 각각 분석하였다.

우선 중국의 사이버 안보전략의 이념과 목표는 민족주의와 사회주의 이념의 바탕 위에 중국 공산당의 권력 지배와 정통성의 유지, 정치적, 사회적 안정의 추구, 정보기술 혁신과 발전 및 경제발전을 포함하고 있다는 점을 지적하였다. 또한 조직과 제도 부문에서 중국의 사이버 안보전략은 2014년 이후가 크게 달라졌다고 분석하였다. 시진핑 국가 주석을 조장으로 하는 중앙인터넷안전정보화영도소조가 전략적 결정단위로 출범했고 총괄 집행조직으로 국가인터넷정보판공실을 설치했다는 점을 알 수 있었다. 중국은 기술혁신과 함께 사이버 역량도 점차 향상시켜 왔음을 확인할 수 있었다.

이러한 분석을 토대로 중국 사이버 안보전략의 특성으로 세 가지를 지적하였다. 첫째, 중국은 외부적인 사이버 위협뿐만 아니라 내부적 사이버 위협도 중시하고 있음을 알 수 있다. 중국은 온라인 지하경제에 서식하고 있는 국내의 사이버 범죄의 만연을 심각한 사이버 위협으로 인식하고 있으며 소수민족과 분리주의 집단에 의한 사이버 테러도 심각한 사이버 위협으로 인식한다. 외부적으로는 특히 미국의 정치군사적 목적으로 사이버 감시와 스파이행위를 심각한 사이버 위협으로 인식한다. 그렇지만 사이버 전쟁의 위협은 최근에 들어와서 미중 관계의 맥락에서 현실적인 사이버 위협의 한 형태로 설정하고 있다. 둘째, 중국의 사이버 안보전략은 현실주의 시각에서 보는 것처럼 선제적이거나 적극적인 성격을 보인다고 보기 어렵다. 중국은 사이버 안보관계에서 미국과 경쟁하고 있지만 정보기술의 차원이나 사이버 전략의 전개에서 미국을 추격하고 있는 상황을 반영한다고 볼 수 있다. 셋째, 중국의 사이버 안보 관련 제도와 전략은 투명성이 크게 결여되어 있다는 비판을 받고 있다. 이로 인해 국내적으로 사이버 범죄의 감소를 달성하는데 어려움을 겪고 있고 대외적으로 이러한 특성이 전략적 불신과 오식(misperception)을 야기하여 미중 사이버 안보협력을 어렵게 하는 요인이 되고 있다.

감사의 글

This work was supported by the National Research Foundation of Korea Grant funded by the Korean Government(NRF-2014S1A3A2044645).

References

Aid, Matthew M. 2013. Inside the NSA's Ultra-secret China Hacking Group. *Foreign Policy* (June 10). http://www.scmp.com/news/china/article/1259175 /inside-nsas-ultra-secret-china-hacking-group (accessed 2017.2.28.).

Bendiek, Annergret. 2012. *European Cybersecurity Policy*. SWP Research Paper, German Institute for International and Security Affairs.

Cavellty, Myriam Dunn. 2012. The Militarization of Cyber Security as a Source of Global Tension. *ETN Zurich*.

Chang, Amy. 2014. Warring State: China's Cybersecurity Strategy. *Center for a New American Security*.

Cheung, Tai Ming. 2011. The Chinese Defense Economy's Long March from Imitation to Innovation. *Journal of Strategic Studies*. 34(3): 325-354.

Cho, Yoon Young and Jong Pil Chung. 2016. China and Cybersecurity: Responding to Internal and External Challenges. *21st Century Political Science Association*. 26(4): 151-178.

Clarke, Richard Alan and Robert K. Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do about It*. New York: Harper Collins.

Deibert, Roanld. 2010. Militarizing Cyberspace. *Technological Review*. MIT.

Deibert, Ronald J. 2002. Circuit of Power: Security in the Internet Environment. In James, N. Rosenau and J. P. Singh(eds.). *Information Technologies and Global Politics: The Changing Scope of Power and Governance*. Albany, NY: SUNY Press.

Deibert, Ronald. 2012. The Growing Dark Side of Cyberspace (...and What To Do About IT). *Penn State Journal & International Affairs*. 1(2): 260-274.

Electronic Times Internet. 2014.6.15. http://www.etnews.com/

Gartzke, Erik. 2013. The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *International Security*. 38(2): 41-73.

Information Warfare Monitor and Shadowserver Foundation. 2010. *Shadows in the Cloud: Investigating a Cyber Espionage 2.0*.

Jang, Noh Soon and In Taek Han. 2013. Controversial Issues and Research Trends in Cybersecurity. *The Korean Journal of International Relationship*. 53(3): 579-617.

Jianwei, Zhuge, *et. al.* 2015. *Investigating the Chinese Online Underground Economy*. In Jon, R. Lindsay, Tai Ming Cheung, and Derek Reveron(eds.).

Jin, De Jong Chen. 2014. U.S.-China Cybersecurity Relations: Understanding China's Current Environments. *Georgetown Journal of International Affairs*.

Kim, Kwan Ok. 2015a. Cybersecurity Competitions and Conflicts between the U.S. and China. *Korean Journal of Political Science*. 23(2): 231-255.

Kim, Sang Bae. 2015b. U.S.-China Relations in Cyber Security: A Perspective of Securitization Theory. *Korea Political Science Association*. 49(1): 71-97.

Li, Yuxiao and Xu Lu. 2015. *China's Cybersecurity Situation and the Potential for International Cooperation*. In Jon, R. Lindsay, Tai Ming Cheung, and Derek Reveron(eds.).

Libicki, Martin. 2012. Cyberspace Is not a Warfighting Domain. *I/S: A Journal of Law and Policy for the Information Society*. 8(2): 321-336.

Lieberthal, Kenneth. 1995. *Governing China: From Revolution through Reform*. WW Norton.

Lindsay, John R. 2015c. Inflated Cybersecurity Threat Escalates US-China Mistrust. *The Huffington Post*. May 17, 2015. http://www.huffingtonpost.com/jon-r-lindsay/cybersecurity-threat-escalates-us-china-mistrust_b_7302282.html?utm_hp_ref=world (accessed 2017.2.25.)

Lindsay, Jon R. 2014. The Impact of China on Cybersecurity: Fiction and Friction. *International Security*. 39(3): 7-47.

Lindsay, Jon R. 2015a. Exaggerating the Chinese Cyber Threat. *Policy Brief, Belfer Center for Science and International Affairs*. Harvard Kennedy School.

Lindsay, Jon R. 2015b. *Introduction - China and Cybersecurity: Controversy and Context*. In Jon, R, Lindsay, Tai Ming Cheung, and Derek Reveron(eds.).

Lindsay, Jon R. and Tai Ming Cheung. 2015. *From Exploitation to Innovation*. In Jon, R. Lindsay, Tai Ming Cheung, and Derek Reveron(eds.).

Lindsay, Jon R., Tai Ming Cheung, and Derek Reveron. 2015. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. Oxford: Oxford University Press.

Lindsay, Jon R., Tai Ming Cheung, and Derek Reveron. 2015. Will China and America Clash in Cyberspace? *The National Interest*.

Manson, George Patterson, III. 2011. Cyberwar: The United States and China Prepare for the Next Generation of Conflict. *Comparative Strategy*. 30(2): 121-133.

Mulvenon, James. 1999. The PLA and Information Warfare. In James, Mulvenon and Richard Yang(eds.). *The People's Liberation Army in the Information Age*. Washington, D.C.

Nakashima, Ellen and Joby Warrick. 2012. Stuxnet Was Work of U.S. and Israeli Experts, Official Say. *Washington Post*. https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.8186d78ba113 (accessed 2017.2.22.)

Nye, Joseph S. Jr. 2011. Power and National Security in Cyberspace. In Kristin, M. Lord and Travis Sharp(eds.). *America's Cyber Future: Security and Prosperity in the Information Age*. Vol. II. (June). Washington, D.C.: Center for a New American Security.

O'Connell, Mary Ellen. 2012. Cybersecurity without Cyber War. *Journal of Conflict & Security Law*. 17(2): 187-209.

Sanger, David E. and Nicole Perlroth. 2014. N.S.A. Breached Chinese Services Seen as Security Threat. *New York Times*. http://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-sevices-seen-as-spy-peril.html (accessed 2017.2.19.)

Segal, Adam. 2016a. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. New

York: Public Affairs.

Segal, Adam. 2016b. The U.S.-China Cyber Agreement: New Beginning or Tactical Pause?. *Cyfy Journal*. 3: 15-19.

Singer, Peter W. 2012. The Cyber Terror Bogeyman. *Armed Forces Journal*.

The Economist. 2010.09.30. The Meaning of Stuxnet.

Korean References Translated from the English

김관옥. 2015. 미중 사이버패권경쟁의 이론적 접근. 대한정치학회보. 23(2): 231-255.

김상배. 2015. 사이버 안보의 미중관계: 안보화 이론의 시각. 한국정치학회보. 49(1): 71-97.

리버살, 케네스. 2013. 거버닝 차이나: 현대중국의 이해. 서울: 심산 출판사.

장노순, 한인택. 2013. 사이버안보의 쟁점과 연구 경향. 국제정치논총. 53(3): 579-617.

전자신문. 2014년. 6월. 15일자. [이슈분석]미·중, 신사이버 냉전...태평양에 사이버 전운. http://www.etnews.com/

조윤영, 정종필. 2016. 사이버안보를 위한 중국의 전략: 국내정책 변화와 국제사회에서의 경쟁과 협력을 중심으로. 21세기정치학회보. 26(4): 151-178.

Received: Jun. 4, 2017 / Revised: Jun. 27, 2017 / Accepted: Jul. 17, 2017

중국의 사이버 안보전략 연구의 통합적 접근

국문초록 중국의 사이버 안보전략은 국가안보와 경제발전을 한 축으로 하고, 다른 한편으로는 대내적 차원과 대외적 차원을 통합적으로 고려하는 분석틀이 필요하다. 본 연구는 중국 사이버 안보전략의 중요한 구성요소로 이념과 목표, 조직과 제도, 사이버 역량을 통합적으로 분석하였다. 중국의 사이버 안보전략의 이념과 목표는 민족주의와 사회주의 이념의 바탕 위에 중국 공산당의 권력지배와 정통성의 유지, 정치적, 사회적 안정의 추구, 정보기술 혁신과 발전 및 경제발전을 포함하고 있음을 확인하였다. 조직과 제도 부문에서 중국의 사이버 안보전략은 2014년 이후가 크게 달라졌다고 분석하였다. 시진핑 국가 주석을 조장으로 하는 중앙인터넷안전정보화영도소조가 전략적 결정단위로 출범하였고, 총괄 집행조직으로 국가인터넷정보판공실을 설치했다는 점을 알 수 있었다. 중국은 기술혁신과 함께 사이버 역량도 향상시켜 왔음을 확인할 수 있었다.

주제어 : 중국의 사이버 안보전략, 기술혁신, 사이버 역량, 통합적 분석

Profiles **Hyun Suk Cho** : He received Ph.D. in Political Science from Seoul National University in 1994. He is a professor at the Department of Public Administration at Seoul National University of Science and Technology. His major fields are international political economy and IT policy. His recent papers are "A Study on the path dependence of personal information protection policy(KOREAN POLICY SCIENCES REVIEW, 2016)" and "A Dispute over Data Protection between the United States and the European Union and its implications for Information Sovereignty Discourse in the Age of Big Data (21st Century Political Science Review, 2016)"(hyunsuk@seoultech.ac.kr).

Eun Mi Lee : She is a researcher of Social Science Research Institute at Yonsei University. She received a Ph.D. in Public Administration at Yonsei University. Her research interests include urban and local administration, decision making, and ICT policy(foodbo@msn.com).

Dong Wook Kim : He is a professor in Graduate School of Public Administration, Seoul National University. He received his Ph.D. in Public Policy & Management at the Ohio State University. His research focuses on informationization policy, information&communication policy, and policy analysis & evaluation for public policy(dong@snu.ac.kr).