# 미·중 사이버안보와 프레임워크 형성의 역사적 다이내믹스

[1] 고경민, [*2] 정영애
[1] 제주연구원, kmkolej@naver.com
[*2] 선문대학교 IT 교육학부, [*2] dr.youngae.jung@gmail.com

# Historical Dynamics of Cyber Security and Framework Formation between the U.S. and China

[1] Kyungmin Ko, [*2]Young-Ae Jung
[1]Jeju Research Institute, kmkolej@naver.com
[*2,] Division of Information Technology Education, Sun Moon University,
dr.youngae.jung@gmail.com

## 요 약

사이버 안보 영역에서의 미·중간 경쟁은 갈수록 치열해지고 있다. 이글은 미·중간 사이버 관계가 형성된 역사적 맥락에 대한 이해를 통해 향후 미·중간 사이버 안보 영역에서의 경쟁과 협력의 함의를 도출하는 데 목적을 두고 있다. 이 글은 미국의 클린턴 행정부가 중국을 세계경제체제로 편입시키면서 인터넷을 통해 중국의 변화를 추동하고자 했던 정보기술 수출통제 자유화 정책 사례에 주목한다. 이 사례에 대한 분석을 통해 미·중간 사이버 안보 관계가 형성된 역사적 맥락을 파악하고, 향후 G2 국가로서 사이버 안보 영역에서 치열하게 전개될 것으로 예상되는 사이버 안보 경쟁과 협력을 전망한다.

## *Abstract*

*In the cyber security area, competition between the US and China are becoming more and more intense. The purpose of this paper is to derive the implications of competition and cooperation between the US and China in the cyber security area, through the understanding of the historical context of the cyber relationship which has been formed between the US and China. This paper focuses on the case of the liberalization policy of information technology export controls that the US Clinton Administration has tried to push China's change through the Internet by incorporating China into the global economic system. We grasp the historical context of the US-China cyber security relationship formation through the analysis of this case and we anticipate the cyber security competition and cooperation between the US and China as a G2 nation expected to be fierce in the cyber security area in the future.*

***Keywords:*** *Cyber security, Framework, US, China, Policy of export controls*

* Corresponding Author
Received: Dec. 7, 2017, Revised: Dec. 19, 2017, Accepted: Dec. 21, 2017

# 1. 서론

사이버 공간에 대한 의존성이 커질수록 개인과 사회뿐만 아니라 국가도 사이버 위협에 대한 취약성이 커질 수밖에 없을 것이다. 국가 차원에서 직면하게 되는 사이버 위협은 국가의 사이버 안보 문제로 간주될 수 있다. 2007 년 에스토니아 사태, 2010 년 미국과 이란의 공방과 같이 명시적으로 드러난 국가간 경쟁과 갈등 이외에도, 그동안 지속되어 오고 있는 북한의 대남 사이버 공격과 최근의 미·중 사이버 갈등이 주요한 관심사로 부상하면서 사이버 안보가 국가안보의 핵심 사안이 되고 있다[1].

사이버 안보 영역에서 글로벌 경쟁이 치열하다. 미국과 중국의 패권 경쟁이 오늘날 세계정치의 가장 중요한 화두의 하나인 것처럼 미·중간 안보 차원의 힘겨루기는 사이버 영역으로까지 확대되고 있다. 미국과 중국은 사이버 공간에서도 G2 국가로서의 위상만큼 중요한 관계를 형성하고 있으며, 상호 대립적인 구도를 형성하면서 사이버 안보 담론과 정책 및 제도를 구축해 나가고 있다.

사이버 안보 영역에서의 미·중간 경쟁은 갈수록 치열해지고 있다. 그러나 아직까지 사이버 충돌을 유발한 구체적인 사례는 찾기 쉽지 않다. 아직까지는 잠재적인 갈등이면서 물밑 경쟁 상태에 있는 것으로 보인다. 그런데 의문은 어떻게 중국이 사이버 최강국인 미국에 필적할 만한 수준으로 사이버 역량을 강화할 수 있었는가 하는 문제이다. 중국 정부가 각종 국가 프로젝트를 통해 사이버 역량 강화를 위해 노력해 왔다는 것은 이미 잘 알려진 사실이다. 그러나 중국의 사이버 역량 구축에는 미국의 영향도 적지 않았다는 것이 이 글의 기본적인 문제의식이다. 중국이 인터넷을 처음으로 공식 연결한 것이 1994 년 4 월이지만[2], 중국이 명실상부한 국가 행위자로서 사이버 공간에 진입한 것은 그보다 훨씬 뒤 늦은 2000 년대 중반 정도로 볼 수 있을 것이다. 짧은 역사적 속에서 중국이 사이버 역량을 축적해 올 수 있었던 과정을 이해할 필요가 있다. 왜냐하면, 그 발전 과정이 역사적으로 형성되어 온 미·중 사이버 관계라고 볼 수 있기 때문이다.

이글의 목적은 미·중 간 사이버 관계가 형성된 역사적 맥락에 대한 이해를 통해 향후 미·중 간 사이버 안보 영역에서의 경쟁과 협력의 함의를 도출할 것이다. 특히 미국의 클린턴 행정부가 중국을 세계경제체제로 편입시키면서 인터넷을 통해 중국의 변화를 추동하고자 했던 정보기술 수출통제 자유화 정책 사례에 주목한다. 이 사례에 대한 분석을 통해 미·중 간 사이버 안보 관계가 형성된 역사적 맥락을 파악하고, 향후 G2 국가로서 사이버 안보 영역에서 치열하게 전개될 것으로 예상되는 사이버 안보 경쟁과 협력을 전망할 것이다.

# 2. 기존 연구와 이론적 검토

## 2.1. 기존 연구의 검토

사이버 안보가 국내에서 학문적 관심의 대상이 된 것은 비교적 최근이다. 초기에는 주로 공학적 관점에서 연구가 진행되었다. 사이버 안보가 사회과학자들의 본격적인 관심은 북한의 사이버테러 위협 가능성이 제기되면서 시작되었다고 할 수 있다. 그러나 그에 관한 선행연구들의 거의 없는 상태였기 때문에 주로 선진국들의 사이버 보안 기술 동향이나 정책에 대한 관심이 주류를 이루었던 것으로 보인다. 이 중에서도 주목할 만한 연구로는 사이버 안보 이슈를 둘러싸고 나타나기 시작한 사이버 안보 담론의 경쟁에 관한 연구이다.

우선 김상배의 연구에 따르면, 사이버 안보 이슈를 보는 미국과 중국의 시각차가 두드러진다. 표 1 과 같이, 사이버 안보 담론에 내재해 있는 사이버 위협의 성격, 대상과 주체 뿐만 아니라 사이버 세계질서가 구성되는 원리 및 방식 등에서 양국의 인식은 큰 차이를 보이고 있다[3].

또 따른 연구로 조화순·김민제는 표 2 와 같이 사이버 공간에 대한 위협, 사이버 위협으로부터 보호되어야 할 가치와 사이버 공간의 질서 유지 및 수행 주체 등 안보화 경쟁의 양상을 세 가지로 구분하여 양국의 확연한 입장 차이를 보여준다[4].

**Table 1.** Comparison of the US and Chinese perspectives on cyber security [3]

| *Categorization* | *The US perspectives* | *Chinese perspectives* |
|---|---|---|
| Feature of the cyber threat | · Blames for attacks on US knowledge information resources by Chinese hackers. | · Considers the technology hegemony of US IT companies as the biggest threat to Chinese cyber security. |
| Target and subject of cyber security | · Is concerned with maintaining physical infrastructure stability and protecting the individual internet liberty. | · Focuses on the safety of information content distributed over the Internet and the national policy rights to conduct Internet censorship and regulation. |
| Formation of cyber world order | · Emphasizes a global governance model involving various stakeholders. | · Insists on utilizing the framework of traditional international organizations led by national actors. |

**Table 2.** Comparison of the US-China stance on cyber security [4]

| *Categorization* | *The US perspectives* | *Chinese perspectives* |
|---|---|---|
| Threats to cyberspace | · Invasion and destruction of computer systems and network infrastructures | · Internet safety |
| Value to be protected from cyber threats | · Protection of civilians' privacy<br>· Freedom of expression and human rights<br>· Circulation of intellectual information and rights of intellectual property | · State sovereignty (Internet sovereignty) |
| Executing subjects for maintaining the order of the cyberspace | · A community composed experts from government, business, civilian, technician and academics | · National and governmental organizations |

이들 두 연구들에서 나타나는 비교적 분명한 문제는 미국과 중국이 사이버 안보를 보는 인식이나 시각의 차이가 뚜렷하다는 점이다. 즉 미국이 사이버 안보를 개인적 자유와 기본권에 초점을 맞추는 데 반해, 중국은 사이버 안보를 국가 주권과 정책에 초점을 맞추는 경향을 보인다. 이러한 차이는 사이버 안보 영역에서 나타나는 미국과 중국의 경쟁과 갈등의 특징적 양상을 보여주고 있다. 양국 간에 나타나는 사이버 안보에서의 경쟁과 갈등은 표면적으로는 컴퓨터 해킹의 문제로 보이지만 실상은 미·중 간 벌어지고 있는 21 세기 패권 경쟁의 '사이버 버전'으로 볼 수 있다.

그런데 이러한 미·중 간 사이버 안보 분야에서의 경쟁과 갈등은 비교적 최근에 나타나고 있는 현상이다. 사실, 중국이 경제적 부상으로 미국 패권에 도전하는 이른바 G2 국가로 인식되기 시작한 것이 불과 2000 년대 초부터 였지만 사이버 안보에 대해 중국이 주도적인 목소리를 내지는 않았다. 중국은 미국 등 서구 국가들에 비해 뒤늦게 사이버공간에 진입한 후발국가라고 할 수 있다. 그럼에도 중국은 미국 등 서구 선진국들이 중심이 되어 추진하는 세계적인 정보 자유화의 압력을 수용하지 않았다[5].

중국이 사이버 안보와 관련하여 자기 목소리를 비교적 분명하게 내기 시작하게 된 계기는 세계 최고의 인터넷 인구와 세계 최대의 온라인 시장을 가진 국가가 되면서 인터넷이 경제발전을 위해서뿐만 아니라 안보적으로도 중요한 영역이기 때문에 사이버공간의 질서 형성은 중국의 미래 전략 차원에서 중요한 문제라고 인식하기 시작했기 때문인 것으로 보인다. 2015 년 3 월에 개최된 중국 양회(兩會)에서 리커창(李克强) 총리가 발표한 '인터넷 플러스(Internet plus)' 행동계획은 이러한 중요성을 상징적으로 보여주는 최근 중국 정부의 입장이라고 볼 수 있다[6]. 같은 맥락에서 시진핑(習近平) 주석도 2015 년

세계인터넷대회(World Internet Conference) 개막 연설에서 기존에 미국이 주도하던 사이버 공간의 질서와는 다른 중국식 사이버 질서와 안보에 관한 구상을 주창했다[4].

미국에 비해 뒤늦게 사이버공간에 진입한 후발주자인 중국이 사이버 공간의 질서와 사이버 안보에 대해 미국과 차별화된 입장을 표명하는 것은 주목할 문제이다. 사이버공간으로 미·중 간 패권 경쟁이 확장되고 있음을 뜻하는 것이기 때문이다. 따라서 앞으로 미·중 간 사이버 안보 이슈를 둘러싼 경쟁과 갈등은 갈수록 치열해 질 것으로 예상된다.

그렇지만 미국과 중국이 이러한 사이버 관계를 형성하게 된 역사적 맥락에 대한 연구나 이해는 부족한 것으로 보인다. 국내뿐만 아니라 외국에서도 현상적 측면에서 미·중 사이버 안보 이슈를 다룰 뿐, 역사적으로 중국의 인터넷 발전과 사이버 전략 형성 등에 관한 연구들은 찾기 쉽지 않다. 이 글은 이러 맥락에서 미·중 간 사이버 관계가 형성된 역사적 맥락을 파악하는 데 초점을 맞춰 미·중 사이버 안보 문제에 접근할 것이다.

## 2.2. 소프트웨어 문서 산출물

미·중 간의 사이버관계의 역사적 맥락에 대한 이해를 위해서는 미국이 중국을 세계경제체제에 편입시키는 과정에서 인터넷을 통해 중국을 변화시키고자 했던 클린턴 행정부의 대외 전략과 그러한 정책 담론의 기반에 대한 이해가 필요하다.

탈냉전에 따른 새로운 안보환경에 직면하여 미국은 그에 부응한 새로운 세계 전략이 필요했다. 클린턴 행정부는 전임 부시 행정부의 봉쇄 전략에서 개입과 확장(engagement and enlargement) 전략으로 전환했다. 미국의 개입과 확장 전략의 핵심은 두 가지이다. 하나는 강력한 군사력을 통해 미국의 안보를 확보하는 것이고, 다른 하나는 외국의 시장을 개방하고 아울러 민주주의를 세계적으로 확산시켜 나가는 것이다. 특히 민주주의 세계적 확산이라는 전략은 미국의 국익을 구성하는 핵심 요소의 하나였다.

클린턴 행정부의 개입과 확장 전략에 기반한 민주주의의 세계적 확산을 위해 정보 분야는 중요한 전략적 영역으로 강조되기 시작했다[7]. 클린턴 행정부는 이러한 전략 환경의 조성은 정보기술과 정치적 변화, 특히 민주화의 관계에 대한 이론적 논쟁과 무관하지 않았다. 클린턴 행정부가 인터넷을 중국에 확산시키고자 했던 분명한 이유는 인터넷의 정치적 영향, 특히 중국 사회를 정치적으로 변화시킬 수 있는 가능성, 즉 정보기술과 민주화의 관계에 대한 인식이라고 할 수 있다.

인터넷과 같은 정보기술과 민주화의 관계에 관해서는 다양한 시각들이 경쟁해 왔으며, 주로 정보기술이 국가에 미치는 정치적 영향에 관심을 가져왔다. 특히 권위주의 국가들의 경우 인터넷이 체제에 미치는 정치적 파급효과에 따른 민주화의 가능성 여부가 중요한 관심사였다. 역사적 측면에서 전 세계적으로 민주주의를 보호하고 확장하는 것은 미국의 국가안보를 위한 지속적인 관심사 중의 하나였다.

민주주의를 옹호하며 민주주의·자본주의의 확산과 개입주의 및 민족자결주의 등을 제창한 윌슨주의(Wilsonianism) 등장은 바로 이러한 미국의 대외전략 목표가 형성되는 계기가 되었다. 그 이후, 루즈벨트와 트루먼 행정부를 거쳐 1981 년에 출범한 레이건 행정부 때부터 적극적으로 추진되기 시작했다. 특히 세계 각지에서 발생하는 무력 분쟁과 같은 중차대한 외교정책 이슈가 발생할 경우에 민주주의의 지원 또는 수호는 해당 분쟁에 대한 개입 또는 참전의 주요 명분으로 작용했다[8].

동구 공산체제의 붕괴와 더불어 전 세계적으로 확산된 '제 3 의 물결', 즉 민주화의 확산에 발맞춰 1990 년대 초부터 민주주의를 옹호하고 나아가 확산시켜 나가야 한다는 민주주의 담론이 부상하기 시작했다. 그리고 이는 더 나아가 미국의 국익을 도모하는 데 권위주의 체제가 적지 않은 파급효과가 작용할 수 있다는 인식이 자리잡게 되었다[9-10]. 특히 소련의 체제전환 이후 중국의 부상이 공공연하게 거론되고 새로운 강대국으로의 부상 가능성이 논의되기 시작했다. 그에 따라 미국은 중국이 미국의 새로운 경쟁자 또는 도전자로 부상할 것으로 예견하면서 중국의 민주주의 체제로의 전환 필요성이 제기되기 시작했다. 소련을

대체하는 미국의 새로운 경쟁자이자 도전자가 될 중국이 당시 미국의 단일 패권을 위협하는 새로운 대항 세력이 될 것이라고 보았기 때문에 중국을 정치적으로 변화시킬 필요성이 높아지게 된 것이다.

이러한 미국의 대중국에 대한 인식에 따라 민주주의를 전 세계적으로 확산시켜 나갈 수 있는 정책 수단으로써 1990 년대부터 산업뿐만 아니라 군사적으로도 중요한 정책 영역으로 정보기술이 부상하게 되었다. 그리고 그 새로운 기술로서 정보기술, 그리고 새로운 미디어로서 인터넷의 정치적 중요성이 전례없이 높게 평가되기 시작했다. 이러한 상황에 직면하여 미국은 대중국 정보기술 이전과 확산이 중국 정치에 영향을 미칠 것이라는 판단 아래, 미국의 첨단 정보기술이 합법적으로 중국으로 이전될 수 있도록 하는 제도를 변경했다. 즉 수출통제체제를 완화하는 조치를 취한 것이다. 이로써 정보기술 이전을 통한 민주주의의 확산이 미국 정부의 주요 외교정책 수단의 하나로 등장하게 된 것이다.

## 3. 최근 미·중 사이버 경쟁 현황

정보기술의 발전과 더불어 최근 4 차 산업혁명이 미래 발전의 화두로 등장하고 있다. 아날로그와 디지털이 합해지고 하드웨어와 소프트웨어가 결합될 뿐만 아니라 알고리즘(algorithm)과 데이터가 합해지고 피지컬(physical)과 사이버(Cyber)가 결합되는 '하이브리드 현상'이 4 차 산업혁명 시대에 일어날 것으로 예측되고 있다[11]. 이런 상황의 도래를 앞두고 국가안보 분야에서의 대응도 갈수록 중요해지고 있다. 현실공간에서의 안보 못지 않게 사이버 공간에서의 안보가 중요해지고 있는 것이다. 안보 영역도 현실과 가상의 공간이 별개의 문제가 아니라 상호 융합되어 '하이브리드 안보'의 중요성이 대두될 것으로 전망된다.

이런 미래 안보의 새로운 위상을 감안할 때 세계 각국은 사이버 전(戰) 능력을 강화할 필요성이 갈수록 커지고 있다. 사이버 위협에 대응해 세계 각국은 사이버 전력 강화를 위한 노력을 하고 있다. 사이버 안보를 둘러싼 국가 간 경쟁은 세계적 주도권을 쟁패하기 위해 벌이는 미·중 관계의 주요 현안 중의 하나로 등장했다. 현실 공간에서의 강대국이면서 사이버 공간에서도 선도적인 사이버 전력을 구축하기 위해 노력하는 미국과 중국은 국가안보를 위한 사이버 전략 수립에 지속적인 노력을 보이고 있다. 미국은 사이버 작전 수행 능력을 확보하기 위한 전력을 증강할 필요성에 따라 국방부 차원에서 국가안보를 위한 사이버 전략(DoD Cyber Strategy)을 수립했다[12]. 중국 또한 2016 년 1 월 사이버 전에 대비한 10 만 명 규모의 사이버통합부대를 창설했다[4].

일찍이 미국은 중국 해커들이 중국 정부의 지원 하에 자국 정부나 민간 부문의 정보통신망을 공격한다고 인식해 왔다. 그리고 2000 년대 후반부터는 이러한 인식을 정부 대변인이나 언론을 통해 공공연하게 공표해 왔다[13]. 중국에 의해 제기되는 해킹 등의 사이버 위협에 대한 미국의 인식은 사이버 안보 문제를 양국의 현안으로 제기하게 만들었다. 2013 년 6 월 미·중 정상간의 논의를 토대로 사이버 안보는 미국과 중국간 관계의 핵심 이슈로 부상했다. 이후 사이버 안보 이슈는 미·중 간 전략경제대화 의제의 하나로서 다루어지기 시작했고, 사이버 보안에 관한 실무적 협의가 이루어지기도 했다[14]. 이러한 양국 간 공식적인 차원의 협의와 협력 분위기가 있었지만, 양국 모두 물 밑에서는 사이버 전을 준비하고 있다.

이와 관련하여 주목할 만한 사건으로 이른바 '스노든 사건'을 들 수 있다. 스노든 사건은 2013 년 6 월 전 미국 중앙정보국(CIA) 직원이던 스노든(Edward Snowden)이 중국을 상대로 한 미국의 비밀 정보 작전을 폭로한 사건이다. 그 폭로에 따르면, 미국 정부의 국가보안 전자감시 체계인 '프리즘(PRISM)'을 통해 오랫동안 개인의 이메일 등 각종 정보들을 감청해 온 것이 폭로되었다. 이 문제는 중국 정부가 미국 정부를 공격할 수 있는 빌미가 되기도 했다.

그리고 또 다른 주목할 만한 사건으로 미국 정부가 중국 장교를 기소한 사건을 들 수 있다. 미국은 2014 년 미국의 정보통신 인프라를 해킹한 혐의로 중국 61398 부대에 소속된 장교

5 명을 산업스파이와 기업비밀 절취 혐의 등으로 기소했다. 그러나 중국도 이러한 미국의 조치에 대해 사이버 안보를 빌미로 자국 이익의 보호에 나선 것이라고 반발했다.

또 2015 년 7 월 8 일 미국의 뉴욕증권거래소, 유나이티드항공, 월 스트리트 저널의 컴퓨터 시스템에 이상으로 주식거래가 중단되고 전 세계적으로 4,900 편의 항공편 운항에 직간접적 악 영향을 미치는 사건이 발생했었다. 미국 국토안보부에서는 단순한 기술적 결함에 의한 사고라고 발표했지만, 일각에서는 이 사건이 중국의 해킹 공격에 의한 것이라는 문제가 제기된 바 있다[15].

현실 공간과 사이버 공간의 최강자인 미국과 중국은 국가 안보 차원에서 사이버 안보를 확대, 강화하기 위해 공방을 계속하고 있다. 미국의 몇몇 사이버 보안 업체들은 이러한 상황을 시각적으로 보여주는 자료를 제공한다. 먼저 사이버 보안 인텔리전스 업체인 노스 코오퍼레이션(Norse Corp.)은 마치 비디오게임과 같이, 실시간으로 사이버 공격이 감행되는 것을 관찰할 수 있는 인터렉티브 맵(interactive map)을 개발했다.

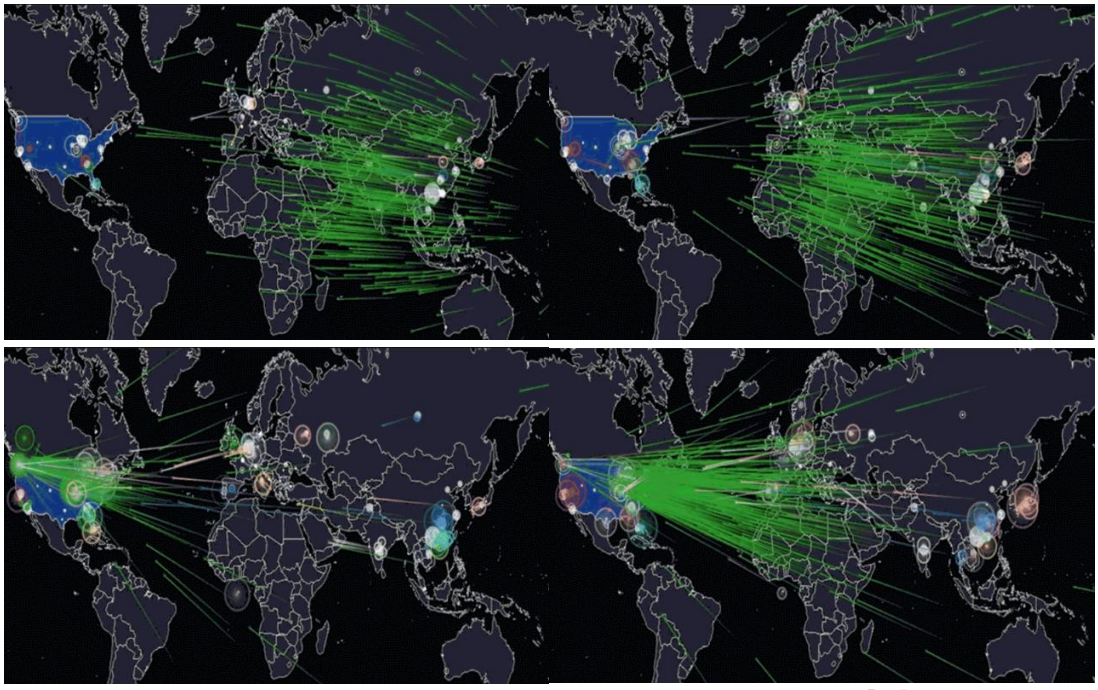

**Figure 1.** Examples of the interactive cyber maps by Norse Corp. [16]

그림 1 은 중국이 미국을 대상으로 벌였던 사이버공격 사례를 시각화한 것이다. 이 사례는 2015 년 6 월에 중국인 스파이 작전의 일환으로 미국의 인사관리처 (Office of Personnel Management)를 겨냥한 해커들이 정부 기관 종사자와 구직자 등 560 만 명의 지문이미지를 탈취한 사건이다. 이 사건은 미 정부기관을 대상으로 한 최악의 해킹 사건이었다. 노스 코오퍼레이션은 이 사건을 통해 사이버 공격의 발생 위치, 타깃 위치, 공격 유형 등을 보여주고 있다.

이러한 사례는 한 예에 불과할지 모른다. 미국과 중국 간에 벌어지는 해킹이나 사이버 공격에 대한 정보는 극히 제한적일 수밖에 없기 때문이다. 그러한 상황을 유념한다고 해도 미·중 간에는 오랫동안 보이지 않는 '사이버 전쟁'을 치열하게 벌이고 있는 것으로 추측되고 있다[3]. 세계 패권을 놓고 경쟁하는 미국과 중국에게 사이버 안보에서의 경쟁은 불가피한 상황이며, 양국의 사이버 안보 영역에서의 갈등과 경쟁은 갈수록 치열해질 것이다.

## 4. 미·중 사이버 관계 형성의 역사적 다이내믹스

국가별로 볼 때 세계에서 인터넷 인구가 가장 많은 국가는 단연 중국이다. 그리고 2017 년 3 월 말 현재 인터넷 이용자수 7 억 3,140 만 명(보급률 52.7%)이다. 중국은 1990 년대 말부터 독점적 통신사업 구조와 각종 관련 제도의 개혁에 나섰고, 법률·제도·사회규범 등의 측면에서 인터넷 통제를 위한 각종 규제 조치들을 발표했고, 기술 면에서도 확고한 인터넷 검열 체제 확립을 위한 금순공정(金盾工程)을 추진했다[17]. 그리고 2000 년대 들어 중국은 인터넷에 대한 통제 시스템을 구축하는 동시에 인터넷 보급률도 확대해 나가는 데 미국을 비롯한 서구 국가들의 통신 장비와 기술을 이용했다.

현재 미국과 경쟁을 벌이는 중국의 사이버 안보 역량은 기본적으로 미국에서 개발된 컴퓨터와 통신 장비, 암호기술 등을 기반으로 구축된 것이다. 그런데 이러한 기술과 장비들은 당초 민간에서 제조·개발되었지만 군사용으로도 사용할 수 있는 '이중용도 품목(dual use items)'으로 분류되어 있었다. 그리고 이러한 품목들은 미국 정부가 규정한 수출통제 리스트에 포함되어 왔다. 그럼에도 이러한 기술과 장비들이 어떻게 중국으로 이전될 수 있었는가?

미국 정부는 민군 겸용이 가능한 이중용도 품목이 적성국가로 유출되는 것을 막기 위해 수출통제체제를 구축하고 있다. 상무부 산하의 산업안전국(Bureau of Industry and Security)에서 담당하고 있는 수출통제 문제는 '수출관리규정(Export Administration Regulations: EAR)'에 따라 이루어지며, 경제적 차원에서뿐만 아니라 국가안보 및 외교정책의 차원에서 다루어진다. EAR 의 통제 대상 아이템 중에서도 특히 군사적으로 민감한 아이템들의 경우는 상품통제리스트(Commerce Control List: CCL)에 규정되어 있다. 정보기술 관련 아이템은 CCL 이 규정하고 있는 아이템들 중 '카테고리 4' 에 포함되어 있는 '컴퓨터' 와 '카테고리 5' 에 포함되어 있는 '통신' 과 '정보보안' 이다[18].

구소련의 붕괴 이후, 대공산권수출통제위원회(COCOM)의 해체 직전인 1994 년 4 월에 미국은 이를 대체하기 위한 새로운 수출통제제도를 도입할 필요가 있었다. 그에 따라 새롭게 도입된 제도가 '일반허가(general license) GLX' 이다[19]. 기존 수출통제 제도는 이중용도의 상품, 소프트웨어, 기술에 대해 허가예외(license exception)가 적용되지 않을 경우 수출 선적에 앞서 '유효허가' (validated license)를 얻도록 규정하고 있었다. 그러나 일반허가 GLX 는 정부로부터의 허가를 받지 않고도 민간기업의 자체 책임에 따라 수출이 가능하도록 한 제도이다[18].

이러한 새로운 제도가 도입되었을 뿐만 아니라 미 의회 차원에서도 과거 COCOM 의 규제대상 국가들이었던 구공산권 국가들로 정보기술을 이전할 수 있도록 하기 위한 입법 활동을 벌임으로써 미국이 제조·개발한 이중용도 아이템들의 수출 가능성이 크게 확대되었다.

한편, 클린턴 행정부는 암호화(encryption)와 고성능 컴퓨터(high performance computers: HPCs) 같은 영역에 대한 수출 통제도 완화하기 시작했다. 당시 미국 정부는 데이터를 복구할 수 있는 암호화 기술의 수출통제 완화 조치와 함께 EAR 에 규정되어 있는 암호 관련 통제의 내용도 완화하는 방향으로 개정했다[20]. 이 당시까지 미국 정부는 암호 기술을 군수품 리스트(Munitions List)의 영역에 포함시켜 수출을 통제해 왔지만, 이 리스트는 상무부 EAR 의 통제를 받게 되었다[20]. 그리고 56 bit 까지의 암호 제품들의 경우는 한 차례의 검토만으로도 테러국가 이외의 국가들을 대상으로 수출할 수 있도록 했다. 이러한 암호화 기술 분야에서의 수출통제 완화 조치에 따라 2001 년이 되면 정부의 관여나 허가 없이도 테러국가 이외의 모든 국가를 대상으로 수출할 수 있도록 되었다[21].

암호화 기술뿐만 아니라 HPCs 부문에서도 클린턴 행정부는 통제 수준을 대폭 완화했다. 1993 년 HPCs 의 정의는 195 MTOPS(million theoretical operations per second: 컴퓨터 수행 속도 측정 단위)에서 2,000 MTOPS 로 수정되었고, 수출을 위해 허가를 받는 데 걸리는 시간도 25% 정도 감축하였다[22]. 그리고 1995 년 이후 HPCs 의 수출허용 한계도 크게 낮아지게 되었다[23]. 클린턴 행정부는 이에 따라 1996 년에 수출을 허용 한계를 7,000

MTOPS 로 조정했다. 그리고 테러지원국에 포함된 국가를 제외한 국가이면 어떤 국가든 HPCs 를 수출할 수 있도록 하는 새로운 제도를 도입했다. 그리고 MTOPS 수준에 따른 국가 등급제도 적용했다[24]. 이외에도 '허가 예외' (License Exceptions) 규정을 담았는데, 이 제도의 도입으로 기존 일반 허가 때의 의무적인 허가 품목의 수도 대폭 줄어들었다[25].

클린턴 행정부는 이상과 같은 컴퓨터와 통신, 정보보안 등과 관련된 영역에서 수출통제를 완화하는 일련의 정책적 조치들을 통해 중국의 사회적·정치적 변화를 이끌어내고자 했다. 그러나 그러한 효과를 가시적으로 기대하기 쉽지 않았다. 미국의 수출통제 자유화에 대한 중국의 전략적 접근을 간과했던 것이다. 그 대표적인 사례가 미국의 수출통제체제의 약화를 이용하여 이중용도 품목이었던 미국의 광대역 통신 장비를 중국으로 이전했다는 의혹이 제기된 사건이다. '후아메이(Hua Mei) 스캔들'로 불리는 이 사건에는 미·중 합작기업인 '후아메이 커뮤니케이션즈'가 관련되어 있었는데, 이 기업은 중국의 군부와 연계된 갤럭시 뉴테크놀로지(Galaxy New Technology)와 미국의 기업체가 합작으로 투자하여 설립한 업체였다.

이 사건과 관련하여, 미국 하원의 국가안보위원회는 1996 년 11 월 회계감사원(General Accounting Office: GAO)에 당시 최첨단 통신기술이라고 할 수 있는 비동기 전송 모드(Asynchronous Transfer Mode: ATM)와 동기식 디지털 계층구조(Synchronous Digital Hierarchy: SDH)의 중국 판매에 관한 검토 보고서 작성을 의뢰했다[26]. 이들 장비는 텍스트는 물론 영상과 음성 데이터를 초고속으로 전송할 수 있게 해주는 이중용도 아이템이다. 이 품목은 원격 지휘 통제와 광대역 네트워크의 구축을 위해서는 없어서는 안 될 통신 장비라고 할 수 있다. GAO 의 검토 결과에 따르면, 당시 SDH 장비는 중국의 통신 네트워크를 국제 표준으로 업그레이드하는 데 필수적인 장비로 활용되고 있었다. 특히 기존의 전통적인 통신 시스템을 현대화하는 데 필요한 것은 물론, 군사적 현대화, 특히 지위 통제 네트워크의 선진화를 위해서도 이 장비들을 이용하려 했던 것으로 나타났다[26]. 뿐만 아니라 1997 년에는 공화당 소속의 헨리 하이드(Henry Hyde) 의원에 의해 미·중 합작기업인 후아메이에 최첨단 통신장비 및 암호 소프트웨어도 판매되었다는 사실을 지적하면서 법무장관에게 후아메이 스캔들을 조사할 것을 의뢰하기도 했다[27]. 이러한 심각한 상황임에도 이 스캔들은 최첨단 정보통신 기술 및 장비의 수출통제를 완화하는 새로운 제도로의 변화를 막지는 못했다.

구소련 및 동구권 붕괴에 따른 국제 환경 변화에 직면하여 중국 정부는 미국 정부의 수출통제체제의 완화를 계기로 정보통신 인프라를 선진화하고 보다 확고한 통제 시스템을 구축할 수 있었다. 특히 중국 정부는 이러한 미국의 선진 정보기술 도입을 위해 신중하게 접근했다. 즉 미국 IT 기업들에게 중국 현실에 맞도록 기존 기술의 변용을 요청했다. 그리고 미국의 여러 중국 진출 기업들은 중국 정부의 요청을 반영하여 중국식으로 최적화된 네트워크 보안 및 검열을 가능케 하는 맞춤화된 기술들을 개발하여 제공했다. 또 중국 정부는 구글이나 야후 같은 인터넷 서비스 업체들에게도 중국의 정치사회적 환경에 적합한 서비스를 하도록 압력을 가하여 자신들의 의도를 관철시킬 수 있었다. 따라서 미국이 의도했던 정보기술에 의해 중국의 사회적·정치적 변화를 촉진하려는 의도는 그다지 성공적이지 못했다.

사실, 정보기술은 사회변혁을 가능케 하는 중요한 수단이다. 그러나 문제는 그것이 절대적이라고 할 수는 없다는 점이다. 아무리 최첨단의 정보기술이 있다고 하더라도 그것이 자동적으로 민주화와 같은 정치적 변화를 추동하는 것은 아니기 때문이다. 래리 다이아몬드가 적절하게 지적한 바와 같이, 사이버 경쟁과 갈등에서 승패는 정보기술에 의해서 결정되는 것이 아니라 정부의 역할, 특히 사람과 조직의 역할이 중요하게 작용한다[28].

## 5. 결론

사이버 안보 분야에서 미·중 관계의 역사는 그리 오래되지 않았다. 중국이 인터넷을 연결한 1994 년 이래, 미국의 인터넷 인구를 추월해 세계에서 가장 많은 인터넷 이용자를 보유한 국가가 된 시점은 2008 년 2 월 말로, 이 때 2 억 2,100 만 명에 도달했다[29]. 중국이 인터넷 인프라 구축을 위한 투자를 강화하고 인터넷 인구가 증가하는 과정에서 미국 정부의 정보기술 수출통제 자유화 조치와 미국 IT 기업의 중국 진출이 이루어졌다. 결과적으로 중국의 인터넷 발전은 미국 정부와 IT 기업의 영향이 적지 않았다는 것이 이 글의 주장이다.

앞에서 검토한 바와 같은 역사적 맥락 속에서 형성된 미·중 간의 사이버 안보 관계는 갈등과 협력이 상시적으로 교차할 수밖에 없는 이중적 구조라고 할 수 있다. 미국과 중국은 거의 상시적으로 사이버 안보 담론과 정책 분야에서 경쟁을 벌이고 있지만, 다른 한편 G2 국가인 양국의 협력 또한 불가피한 상황임을 인지하고 있다.

사이버 안보 담론과 정책 분야에서 미·중 양국은 상충되는 경우가 적지 않다. 미국은 수정헌법 제 1 조에서 언급된 정보 접근의 권리에 높은 우선순위를 두는 반면, 중국은 국가안보, 정치안정, 사회질서 등에 대한 관심 때문에 정보를 제한하는 경향이 높다[30]. 중국의 인터넷 연결 초기에 미국이 적극적으로 중국의 인터넷 발전을 추동했던 가장 큰 이유 중의 하나는 인터넷과 같은 정보기술이 갖고 있는 민주적 동력 때문이었다. 그러나 중국의 인터넷 발전을 촉진하고자 했던 미국의 정책이 제한적일 수밖에 없었던 이유는 정보기술과 인터넷을 보는 중국 정부의 인식이 미국 정부와는 크게 달랐기 때문이다. 자유로운 인터넷에 대한 미국의 관념과 달리, 중국에서는 통제와 규율 속 인터넷이라는 관념이 중국 정부의 인터넷 정책 이념이었기 때문이다.

미·중 간 사이버 안보 담론에서 많은 서구 학자들은 양국 간 담론 경쟁의 원인으로 정치체제의 성격, 즉 민주주의 체제와 사회주의 체제의 차이를 강조하는 경향을 보인다. 그러나 그것이 전부라고 할 수는 없다. 종종 미국 정부가 정치적인 이유로 중국의 인터넷 통제를 공격했을 때, 중국 정부는 주로 사회적·문화적 관심을 들어 방어했다. 이런 중국의 주장처럼, 중국은 독특한 역사와 문화, 전통을 가진 국가이다. 중국이 돌연 서구적 표준에 따라 민주적인 국가가 된다고 해도, 중국은 여전히 서구 민주주의 국가들과는 다른 접근방법으로 사이버 정책을 형성할 것이다. 양국 간의 문화적 거리(차이)는 오랜 기간 동안 존속할 것으로 보이기 때문이다. 이와 같은 차이를 통해서 볼 때, 미·중 간 사이버 안보 담론과 정책은 양국의 역사와 문화와 전통의 거리만큼, 그리고 세계적 강대국으로서의 양국의 미래 전략의 차이만큼 거리를 보일 것이다.

그러나 다른 한편, 미국과 중국이 사이버 안보 분야에서 항상 대립각만을 세울 것으로 보이지는 않는다. 2015 년 9 월에 있었던 미·중 간 전략경제대화에서 미국 내에서 발생한 해킹과 개인정보 유출 사건이 중국과 관련되었을 것이라는 의혹을 미국 측에서 제기하면서 공방을 벌이기도 했다. 그런데 시진핑 주석의 언급처럼, 분명한 것은 미국이 사이버 역량(cyber strength)에서는 세계 최강국인 반면, 인터넷 이용자 수에서는 중국이 세계 최대 국가이다. 따라서 시진핑 주석에 따르면, 양국은 사이버 상에서의 대결을 회피할 필요가 있고, 또 사이버 이슈를 정치화해서는 안 될 것이라고 언급했다[31]. 또 2017 년 미·중 정상회담에서도 트럼프 대통령과 시진핑 주석은 미·중 정상이 좌장을 맡는 새로운 고위급 대화 설립에 합의했는데, 사이버 안보 분야가 안보, 외교, 경제, 통상, 법, 인문사회 교류 등과 같은 핵심 의제들과 함께 새로운 고위급 대화 의제의 하나로 포함되었다.

미국과 중국은 이처럼 전략 대화나 정상회담 등을 통해 사이버 산업스파이 지원 중단 합의나 고위급 대화 협의체 설립 등과 같은 결실을 맺었다. 그러나 사이버 공간에서 자국의 영향력 축소를 원치 않기 때문에 미·중 양국의 사이버 경쟁과 사이버 안보를 둘러싼 갈등과 충돌은 계속될 것이다.

## 6. 참고문헌


[1] S. Kim, “Four Neighbouring Network-States and South Korea in Cyber Security: Network Structure of Powers and Strategies of a Middle Power,” Korean Journal of International Relations, Vol. 57, No. 1, pp. 111-154, 2017.

[2] CNNIC(China Internet Network Information Center). 2004. “The Internet Timeline of China 1987~1996.” http://www.cnnic.cn/html/Dir/2003/12/12/2000.htm

[3] HyunYong Lee, SooJin Lee, "Enhanced EPS-AKA for adapting LTE technology in Military Tactical Communication Network", Journal of Security Engineering, Vol.12, No.5 (2015), pp.455-468, http://dx.doi.org/10.14257/jse.2015.10.07

[4] W. Jho, M. Kim, “Securitization of Cyberspace and the Limits of Cyber Security Governance,” Information Society & Media, Vol.17, No.2, pp. 77-98, 2016.

[5] T. C. Boas, “Weaving the Authoritarian Web: The Control of Internet Use in Non-Democratic Regimes,” in How Revolutionary was the Revolution? National Responses, Market Transitions, and Global Technology in the Digital Era, John Zysman & Abraham Newman eds. Stanford, CA: Stanford University Press, 2006.

[6] H. Ma et al., “Internet plus”, Seoul, Business books, 2016.

[7] J. Arquilla, D. Ronfeldt, “Information, Power, and Grand Strategy.” in Athena’s Camp: Preparing for Conflict in the Information Age, John Arquilla and David Ronfeldt eds. Santa Monica, California: RAND, 1997.

[8] Ki-Young Lee, "Activity plan of guaranteing Software Security of Weapon system for realizing Software Security Policy ", Journal of Security Engineering, Vol.12, No.2 (2015), pp.131-138, http://dx.doi.org/10.14257/jse.2015.04.03

[9] S. Ma, “American Democracy Promotion Abroad: Motives and Dilemmas,” National strategy, Vol. 11, No. 4, pp. 41-68, 2005.

[10] S. Lee, “The American Neoconservatism and Democracy: A Peculiar Case of Marriage between Realism and a Moral Philosophy,” National strategy, Vol.11, No.2, pp. 81-112, 2005.

[11] K. Wohn. (2017, Apr.). There is no 'reality' of the Fourth Industrial Revolution. Available: http://www. sciencetimes.co.kr/

[12] The Department of Defense, “The DoD Cyber Strategy,” 2015.

[13] K. Kim, “The Rise of Cyber-Attacks-Short-of-War: The Case for a New Cyber Treaty,” Asan Institute for Policy Studies, Feb. 2017.

[14] Jung-Ho Eom, "Problems and Improvement of the Curriculum for Effective Cyber Security Education and Training", Journal of Security Engineering, Vol.12, No.4 (2015), pp.337-350, http://dx.doi.org/10.14257/jse.2015.08.01

[15] A. Moore. (2015, Sept.). Cyber Experts: China Attacked U.S. Stocks, Companies. Available: http://www.wnd.com/2015/07/cyber-experts-china-attacked-u-s-stocks-companies/

[16] (2017, Sept.) Available:http://www.extremetech.com/wp-content/uploads/2014/06/norse-china-usa-hacking-smaller.gif

[17] K. Kraemer, J. Dedrick, “Creating a Computer Industry Giant: China’s Industrial Policies and Outcomes in the 1990s,” Center for Research on Information Technology and Organizations, University of California, Irvine, 2001.

[18] K. Ko, “A Paradox of Information Technology and Democratization?: Change in U.S. Export Control Policies on Information Technology and China's Internet Development,” The Journal of Peace Studies, Vol. 13, No. 3, pp.25-50, 2012.

[19] U.S. Department of Commerce, “Establishment of New General License for Shipments to Country Groups QWY and the People's Republic of China,” Federal Register, pp. 59-64, Apr. 1994.

[20] W. J. Clinton, “Executive Order 13026: Administration of Export Controls on Encryption Products,” Weekly Compilation of Presidential Documents pp. 32-46, Nov. 1996.

[21] T. Kremic, “Why the Lack of Academic Literature on Export Controls?,” NASA/TM.2001-210982, National Aeronautics and Space Administration, Glenn Research Center, Jul. 2001.

[22] R. Johnston, “U.S. Export Control Policy in the High Performance Computer Sector,” The Nonproliferation Review, Vol. 5, No. 2, pp. 44-59, 1998.

[23] S. Goodman, P. Wolcott, G. Burkhart, "Building on the Basics: An Examination of High-Performance Computing Export Control Policy in the 1990's," A Report of the Center for International Security and Arms Control, Stanford University, pp.13-21, Nov. 1995.
[24] U.S. Department of Commerce, "Revisions to the Export Administration Regulations: Reform of Computer Export Controls; Establishment of General License G-CTP," Federal Register, pp. 61-17, Jan. 1996.
[25] U.S. Department of Commerce, "Export Administration Regulation: Simplification of Export Administration Regulations," Federal Register, pp. 61-58, Mar. 1996.
[26] GAO, "Export Controls: Sale of Telecommunications Equipment to China," Report to the Chairman, Committee on National Security, House of Representatives, GAO/NSIAD-97-5, Nov. 1996.
[27] C. R. Smith. (2001, Jan.). The Chinese Army Spy and Condoleezza Rice. Available: NewsMax.com
[28] L. Diamond, "Liberation Technology," Journal of Democracy, Vol. 21, No. 3, pp. 69-83, 2010.
[29] The Economic Times.(2008, Jul.). China Surpasses US in Internet Use. Available: https://economictimes.indiatimes.com/tech/internet/china-surpasses-us-in-internet-use/articleshow/3279347.cms
[30] L. Zheng, "Cross-national Information Policy Conflict Regarding Access to Information: Building a Conceptual Framework," in Proc. of the 8th Annual International Digital Government Research Conference, Bridging Disciplines & Domains, DG.O 2007, Philadelphia, Pennsylvania, USA, May 20-23. 2007, pp. 201-211.
[31] The White House Office of the Press Secretary, "Statement by the President on the Trans-Pacific Partnership," 2015.