ISSN 2233-6583

22-12

KISDI

Premium Report

중국의 정보공간 거버넌스와 사회통제

최 계 영

정보통신정책연구원 선임연구위원

KISDI 정보통신정책연구원
KOREA INFORMATION SOCIETY DEVELOPMENT INSTITUTE

KISDI
22-12
2022. 12. 30
Premium Report

중국의 정보공간 거버넌스와 사회통제

최 계 영
정보통신정책연구원 선임연구위원

요약문

중국의 정보공간 거버넌스와 사회통제

최 계 영
정보통신정책연구원 선임연구위원
*choigi@kisdi.re.kr, 043-531-4321
*현 정보통신정책연구원
디지털경제사회연구본부 플랫폼정책연구센터

요 약 문

본 리포트는 미·중 기술패권 경쟁의 한 양상인 기술 권위주의에 대한 논란에 주목하고, 기술 권위주의의 근간이 되는 중국의 총체적 국가안보 개념 및 이를 지원하는 법제도 체제를 분석함. 총체적 국가안보관에 따르면 국가안보는 당이 영도하는 정치안보를 최상위에 두고 하위 범주로 국토, 군사, 경제, 문화, 사회, 기술, 사이버. 환경, 자원, 핵, 바이오, 우주, 극지, 심해, 해외 국가이익 등 총 16개 영역을 망라함. 사실상 거버넌스의 모든 영역이 안보에 종속되는 이유는 시진핑 시대가 인식하는 새로운 위협, 즉 중국을 봉쇄하려는 서구 연합, 글로벌 평판의 훼손, 분리주의(신장, 홍콩, 타이완), 당 이외의 대안적 권력 등에서 찾을 수 있음.

이에 따라, 중국의 국가안보·정보공간 거버넌스는 공산당 최상위 조직에서부터 사회 풀뿌리(grassroot) 조직까지 망라하는 위계질서下에서 사회통제·관리가 이루어짐. 그리고 중국의 정보공간 거버넌스에 관련된 모든 법·제도는 총체적 국가안보에 복무함. 국가안보법을 필두로 反테러법, 反스파이법, 사이버보안법, 외국NGO관리법, 국가정보법, 데이터안전법, 개인정보보호법, 反외국제재법 및 홍콩안보법이 모두 이에 해당됨. 이러한 법·제도 체제는 감시·통제 기능으로 남용될 가능성이 높은데, 이는 다음과 같은 이유 때문임.

첫째, 국가안보의 개념이 공산당의 이데올로기, 영도력과 통합되어

국가보다는 당의 보호에 초점을 두고 있음.

둘째, 국가안보의 개념이 상대적으로 너무 포괄적이고 국가기관의 권한, 소관, 자원이 막강함.

셋째, 법·제도적으로 안보 관련 기관의 행위에 대한 감시가 없고 협조를 거부할 유의미한 법적 수단이나 절차도 없음.

이러한 중국의 정보 공간의 기술규범의 특성은 기술패권 경쟁에 보편적 가치를 둘러싼 경쟁이라는 성격을 부여함. 이에, 기술패권 경쟁 시대 주요국 간 기술협력체 추진과정에서 글로벌 기술규범에 대한 우리의 입장을 명확히 할 필요가 있음.

China's information domain governance & social control

Summary

This report investigates the Chinese 'comprehensive national security' concept and related legal and social systems, regarding the controversy over 'techno-authoritarianism' between U.S. and China. Comprehensive national security encompass 16 types of security : political, territorial, military, economic, cultural, societal, technological, information, ecological, resources, nuclear, cyber, overseas, bio, space, polar and deep-sea security. This securitization of everything comes from the CCP's perceived threat of Western value and geopolitical competition. The legal system on security and information domain serves as a pivotal tool of CCP's power, including National Security Law, the Counter-Terrorism Law, the Counter-Espionage Law, the Cyber Security Law, the Foreign NGO Management Law, the National Intelligence Law, the Data Security Law, Hong Kong National Security Law and the Anti-Foreign Sanctions Law.

China's norm on information and security is characterized by too broad definition of national security, integration of national security and party ideology, CCP's wide remit and resources, and no public oversights. Such differences demand our clear position on global technology usage value and norm.

1. 개요

◆ 기술 권위주의와 중국

● 미·중 기술패권 경쟁이 경제, 안보 뿐만 아니라 기술의 이용에 관한 규범·가치를 둘러싼 대립으로 심화되고 있음

● 특히 미국은 중국을 '기술 권위주의'(Techno-Authoritarianism)로 비판하고 중국식 인터넷 거버넌스의 국제적 확산 저지를 서방국간 기술 블록 형성의 주요 요인으로 제시

- 기술 권위주의 또는 디지털 권위주위는 언론이나 인권 관련 특정 대상에 대한 억압, 검열, 인터넷 셧다운 및 체제 선전에 디지털 기술을 이용함을 의미

- 바이든 행정부는 통제 및 감시를 통한 정보공간의 장악을 민주주의에 대한 위협으로 간주하고, 서구 기술불록에 기술 민주주의(Techno-democracy)의 방어·확산이라는 목표를 부여[1)]

- 바이든 행정부 국가안보전략의 평가 : 중국이 디지털 기술 역량이나 국제기구 영향력을 증진시킴으로써 권위주의 모델의 수용에 유리한 환경을 조성하고 글로벌 차원의 기술 이용 및 규범을 자신의 이익 및 가치에 유리하게 이끈다고 비판[2)]

1) 미 국무장관 블링켄(A. Blinken)의 'The Administration's Approach to the People's Republic of China' (2022. 5. 26) 참조할 것

2) 백악관, National Security Strategy (2022. 10)

● 반면 중국식 기술규범, 모델의 강화확산은 중국의 사이버공간 장기전략 목표 가운데 하나

- 중국 사이버 공간 전략은 '시진핑 총서기의 사이버 강국 전략사상을 심도 있게 이행하고 사이버보안 및 정보화 업무를 확고히 추진한다' (사이버공간 관리총국)에서 명확히 제시됨[3)]

- 이에 따르면, i) 인터넷 콘텐츠 관리 및 온라인상의 긍정적 에너지 창출[4)], ii) 사이버안보 강화, iii) 독자적인 하드웨어 및 소프트웨어 인터넷 관련 기술 기반 구축, iv) 글로벌 인터넷의 구축, 거버넌스, 운용에서 중국의 역할 증대 등을 추구

  • 특히 중국의 글로벌 역할 증대의 지침으로 제시된 네 가지 원칙(四项原则)과 다섯 가지 주장(五点主张, proposition)은 사이버 주권의 강조로 글로벌 규범이라 할 수 있는 개방적 인터넷을 거부하고 대안적 인터넷 거버넌스를 추구하며, 글로벌 네트워크 인프라를 구축해 해외 영향력을 강화하는 내용을 담고 있음[5)]

---

3) 중국 사이버공간 관리총국(CAC: Cyberspace Administration of China) 이론연구 소조, '시진핑 총서기의 사이버 강국 전략사상을 심도 있게 이행하고 사이버보안 및 정보화 업무를 확고히 추진한다' (2017. 9. 15) http://www.qstheory.cn/dukan/qs/2017-09/15/c_1121647633.htm

4) 즉 콘텐츠 통제와 선전을 강조. 동 문건에 따르면, "온라인 공공 의견 작업은 선전 및 이데올로기 작업에서 가장 중요한 과업이 되었다. 온라인 및 오프라인 세계는 동심원을 형성하고, 당의 지도하에 모든 인민을 동원하고, 모든 면에서 열정을 동원하며, 중화민족의 위대한 부흥이라는 중국의 꿈을 실현하기 위해 함께 노력해야 한다"고 천명.

5) 4대 원칙은 사이버 주권 존중, 평화 및 안보 보장, 개방적 협력, 올바른(good) 질서 확립이며, 5대 주장은 글로벌 네트워크 인프라 건설의 촉진, 온라인 문화교류를 위한 플랫폼 구축, 온라인 경제 혁신, 사이버 보안 및 질서 있는(orderly) 발전 촉진, 공평하고 정의로운 인터넷 거버넌스 건설임. 사이버 주권의 강조는 감사통제에 대한 외부간섭 거부, 공평하고 정의로운 인터넷 거버넌스 건설은 기존의 이해당사자(stakeholder) 인터넷 거버넌스의 정부주도(multilateral) 거버넌스로의 전환을 정당화하는 논리가 될 수 있음.

● 디지털 정보공간에 대한 통제 및 감시체제가 기술 권위주의의 핵심

- 통제는 단순히 외부 정보의 차단뿐만 아니라 정보공간을 프로파간다에 활용함으로써 적극적 지지그룹, 체제의 버팀목을 형성하는 것까지 포괄

- 인공지능 등 다양한 감시 기술을 활용한 사회 장악이 기술 권위주의의 또 다른 핵심

2. 중국의 정보공간 거버넌스 체제

◆ 국가안보와 정보공간 거버넌스의 연계

● 당이 주도하는 통제 및 선전, 인민의 동원, 중화민족의 부흥과 같이 글로벌 인터넷 규범과 상이한 '중국적 특성(Chinese Characteristic)'을 가진 정보공간 거버넌스는 '총체적 국가안보관(總體國家安全觀, comprehensive national security)'[6]으로 정당화됨

● 총체적 국가안보관

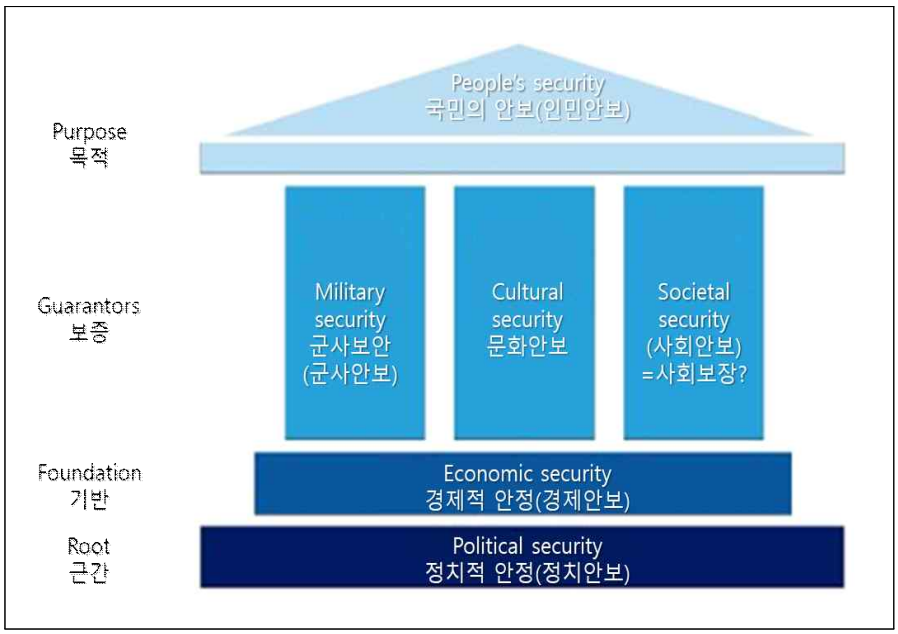
- 중국에서 국가 안보는 정치 체제 시스템의 일부를 구성함. 총체적 국가안보관 개념의 근간에는 '정치적 안보'가 자리 잡고 있기 때문

  • 총체적 국가안보관은 중국 공산당의 영도권을 보장하고 당 안팎과 중화인민공화국의 지리적 경계 안팎에서 발생할 수 있는 정치적 위협으로부터 당-국가를 보호하기 위한 요구사항을 가리킴

  • 계층적 위계질서를 갖는 국가 안보 개념의 상층부에는 문화, 안보 및 사회 안보도 포함되며, 군사 안보와 같은 국가 안보의 전통적인 구성 요소도 포함되지만 인민 해방군은 중국 공산당의 군대이기 때문에 정치적 의미도 수반됨

6) Xinhua (2014. 4). "中央国家安全委员会第一次会议召开 习近平发表重要讲话. 중앙국가안보위원회 첫 회의가 중요한 시진핑 연설을 제시하였다".
http://www. gov.cn/xinwen/2014-04/15/content_2659641.htm.

〈도표 1〉 중국의 국가 안보 개념



출처 : ASIP, Mapping China's Tech Giants: Supply chains & the global data collection

● 정보공간의 거버넌스를 규제하는 각종 법안은 정치적 안보를 근저로 하는 총체적 국가안보관에 사실상 복무

- 국가보안법, 개인정보보호법, 데이터 안전법, 사이버 보안법 등은 일차적으로 정치·사회적 안정을 위한 수단으로 기능

- 국가 안보 개념下에서 정부-당의 정책을 계획, 추진, 조율하는 거버넌스는 중앙정치국-정치국 상무위원회-중앙 국가안보위원회 CSSC: Central State Security Committee)가 담당

● 시진핑 시대의 국가 안보 개념 확장

- 총체적국가안보관은 2014년 도입 이래 그 영역을 지속적으로 확장

- 시진핑 시대가 새로이 직면한 위협으로는 중국을 봉쇄하려는 서구 연합, 글로벌 평판의 훼손, 분리주의(신장, 홍콩, 타이완), 당 이외의 대안적 권력 등이 지적되고[7], 이는 정보공간의 통제를 더욱 강화하고 사실상 거버넌스의 모든 영역이 안보에 종속되는(securitization of everything) 근거로 작용

- 체제 안정과 당의 우위를 위해 정치안보를 최상위에 두고 하위 범주로 국토, 군사, 경제, 문화, 사회, 기술, 사이버. 환경, 자원, 핵, 바이오, 우주, 극지(polar), 심해, 해외 국가이익 등 총 16개 영역을 망라

● 중국식 특색의 총체적 국가안보 개념은 이를 뒷받침하는 법제도, 기술적 인프라의 확충으로 이어지고, 장기적으로 당-국가와 사회 간의 관계도 보다 위계적 질서로 이어질 가능성

- 또한 정보흐름의 통제나 네트워크 기반의 조직적 저항 사전 방지에서 더 나아가, 중국의 경제, 기술, 지정학적 리더쉽 강화의 이념적 기반이기도 함

- 사회통제 기능을 담당하는 社会网格化管理(grid management system)[8]는 당-국가의 사회에 대한 우위를 상징

● 모든 것을 포괄하는 안보개념에 부응하여, 중국의 국가안보·정보공간 거버넌스는 공산당 최상위 조직에서부터 사회 풀뿌리(grassroot)

7) MERICS(2022. 9. 15), 'Comprehensive National Security" unleashed: How Xi's approach shapes China's policies at home and abroad' 참조할 것. 특히 중국 공산당 내부 문건 "Document No. 9,"(2013)에 따르면 중국을 불안정하게 만들 인권과 같은 보편적 가치, 서구 스타일의 시민사회, 언론 자유, 권력의 분산을 타겟으로 이데올로기 및 문화 안보를 강조. Johnson, Matthew D. (2020. 6) 'Safeguarding socialism: The origins, evolution and expansion of China's total security paradigm' 참조. https://sinopsis.cz/en/johnson-safeguarding-socialism/

8) 당 조직원이 소지역별로 사전에 지정된(designated) 개인을 담당해 감시, 보고 업무를 수행

조직까지 망라하는 위계질서下에서 사회통제·관리가 이루어짐

- 국가안보위원회(최상위) → 당 기관(서기국, 선전국, 정치·군위원회 등) 및 정부부처·기관 → 대도시, 지역 차원의 광역 안보위원회 → 소규모 커뮤니티, 마을 단위 당위원회 및 기업·사회단체·교육기관 당세포, 소지역 단위로 감시·보고 업무를 수행하는 社会网格化管理 조직원으로 이어지는 체제로 정부의 안보 관련 방침, 정책이 수행됨

◆ 중국의 정보공간 거버넌스를 규정하는 주요 법·제도

● 중국의 정보공간 거버넌스에 관련된 모든 법·제도는 총체적 국가안보에 복무

- 국가안보법은 모든 개인 및 사회조직에 적극적 모니터링과 안보위협을 알리는 책임을 부여하는 대중 동원 체제의 근간

  • 국가안보법(2015년) 제3조는 '모든 국가안보사업은 총체적인 국가안보관을 견지하고, 인민의 안전을 취지로 삼고, 정치안보를 근본으로 삼으며, 경제안보를 기초로 하고, 군사·문화·사회안보를 보장하며, 국제안보의 촉진에 의거해 중국 특색의 국가안전의 길을 걸어 나가야 한다'고 규정

  • 국가안보법을 필두로, 反테러법, 反스파이법, 사이버보안법, 외국NGO관리법, 국가정보법, 데이터안전법, 개인정보보호법 등이 모두 총체적 국가안보 의 프레임워크에 따르며, 이는 특히 최근의 反외국제재법(2020)[9] 및 홍콩안보법(2021)[10]에도 적용됨

9) 미국의 대(對)중국견제에 동참하는 국가에 대해서 상응한 제재를 취할 수 있는 근거를 제시

● 특히 디지털 공간의 거버넌스인 중국의 개인정보보호법이나 데이터 안전법은 서구와는 달리, 중국 정부가 규정한 국가 안보 개념과 연계되어 정치적 성격을 강하게 띰

- 국가안보법 및 사이버 보안법과 분리되어 생각할 수 없음

  • 개인정보보호법 : 중국內外의 모든 중국인의 개인 정보에 접근·규제할 수 있는 권한을 정부에 부여함으로써 해외의 개인, 기관에 의한 반체제 활동 제약이 가능

  • 데이터 안전법[11] : 공안기관, 국가안전기관이 국가안전을 보호하거나 범죄수사의 필요에 따라 데이터를 수집할 경우 관련 조직, 개인의 협조 의무를 부여

  • 정보기관들의 권한 및 정보수집권을 규정하는 국가정보법 : 개인정보보호를 국가가 자의적으로 우회할 수 있는 근거를 제공[12]

● 미국이 국가안보를 이유로 수출 통제, 투자 제한 등 對中 제재 조치를 취하듯이 모든 국가가 안보의 개념, 적용 범위를 확장하고 있지만, 중국은 다음과 같은 측면에서 서구와 상이

- 국가안보의 개념이 공산당의 이데올로기, 영도력과 통합되어

10) 원래 홍콩 기본법 제23조에 의해 홍콩 입법회에서 제정했어야 하는 법이지만 중국이 홍콩 기본법 부속서에 임의로 삽입해 2020년 7월 1일자로 시행. 국가 분열, 국가 정권 전복, 테러 활동, 외국 세력과의 결탁 등 4가지 범죄에 최고 무기징역형으로 처벌할 수 있음.

11) 중국 경내에서 데이터를 처리할 때와, 해외에서 데이터를 처리할 때 중국의 국가안전·공공이익 또는 공민의 권익을 침해하는 경우 동 법을 적용하도록 함

12) 동 법안의 제7조는 "모든 조직과 공민은 모두 법에 따라 국가정보업무를 지지·협조·호응하여야 하고, 국가정보업무를 통하여 알게 된 비밀을 지켜야 한다. 국가는 국가정보업무에 지지·협조·호응하는 개인과 조직을 보호해주어야 한다"고 규정하여 외국인, 반체제 인사들에 대한 인권침해 가능성도 있음

국가보다는 당의 보호에 초점을 두고 있음

- 국가안보의 개념이 상대적으로 너무 포괄적이고 국가기관의 권한, 소관, 자원이 막강

- 법·제도적으로 안보 관련 기관의 행위에 대한 감시(oversight)가 없고 협조를 거부할 유의미한 법적 수단이나 절차도 없음

※ 어느 나라나 안보를 이유로 정부의 데이터 접근 등 권리의 침해를 명확한 법·제도적 조건 하에서 일정 수준 허용하지만 투명성이 부족하고 정치적 자의성도 크고 知治를 통한 스마트 감시 시스템을 갖춘 중국에서는 특히 법안의 남용 가능성이 높다는 평가를 받고 있음[13]

● 무엇보다도 상기 법안들에 규정된 사항들은 중국의 모든 개인 및 조직에 의무로 부여되는 것으로, 특히 중국의 민간 기업들도 서구와는 달리 정부-당 주도의 정보공간 거버넌스에 따라야 한다는 점에 주목할 필요

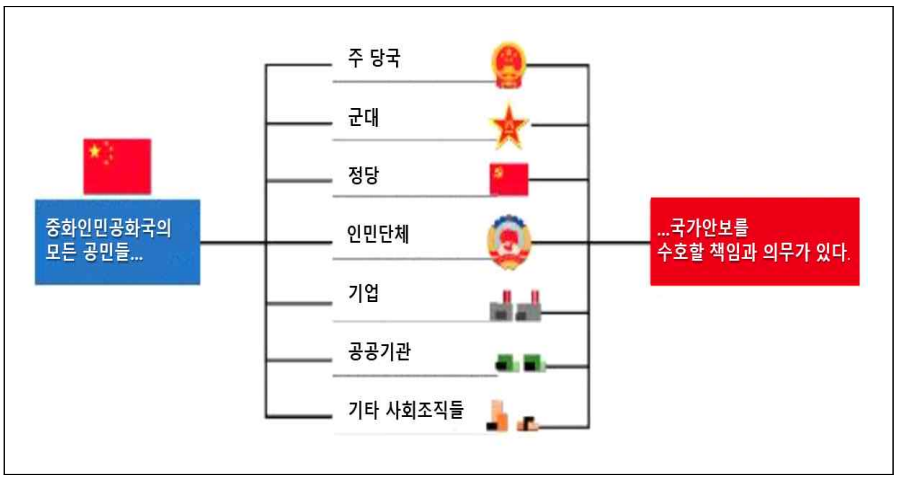
- 국가보안법(2015) 제 11조는 '중국인민공화국의 모든 공민, 주 당국, 군대, 정당, 인민단체, 기업, 공공기관 및 기타 사회조직들은 국가안보를 수호할 책임과 의무가 있다'고 규정하고 있음

⇒ 글로벌 차원에서 활동하는 중국 민간 기업에 대한 중국 정부의 통제와 글로벌 데이터 공유는 다른 나라에 대한 잠재적 안보 위협[14]

13) ASIP(2022. 6. 8), Mapping China's Tech Giants: Supply chains & the global data collection ecosystem
https://www.aspi.org.au/report/mapping-chinas-tech-giants-supply-chains-and-global-data-collection-ecosystem

14) 예를 들어, 중국 공산당 중앙선전부가 관리하는 국영기업의 자회사인 Global Tone Communication Technology(GTCOM)는 화웨이, 알리바바 클라우드 등 기술기업들과의 파트너쉽을 통하여 방대한 양의 글로벌 데이터 수집, 당의 선전활동 지원 등 국가안보 목적을 지원하는 것으로 알려짐. Hoffman, S(2019), 'Engineering global consent: The Chinese Communist Party's data-driven power expansion', ASPI Policy BriefNo. 21 참조.

〈도표 2〉 중국의 국가 안보 의무 대상



출처 : ASIP, Mapping China's Tech Giants: Supply chains & the global data collection ecosystem (2021. 6. 8)

3. 시사점

● 기술 권위주의는 우리와 무관할 수 없는 글로벌 이슈

- 인터넷이라는 정보공간은 글로벌한 성격을 가지고 있기 때문에 기술 권위주의는 우리에게도 영향을 미칠 수 있음

  • 틱톡과 같은 중국의 인터넷 서비스는 국내에서도 이용되고 있으며, 중국 시장에 진출하는 국내 기업은 중국의 인터넷 거버넌스에 따라야 함

  ※ 틱톡이 젊은 세대가 뉴스를 접하는 주요 통로로 이용되는 등, 미디어에의 영향력이 증대

  • 우리 기업을 포함한 외국 기업들은 '중국 인터넷 산업 자율통제 공동서약'[15]에 따라 기본적으로 중국의 인터넷 규범에 따라야 함

- 기술 권위주의에 복종하고 통제기관에 데이터 수집·제공·분석 수단을 제공하는 글로벌 기업(중국의 빅테크가 될 수 있음)은 안보 문제도 야기

● 이에, 중국의 디지털 정보공간 거버넌스를 이해하는 것이 기술패권 시대 우리의 국가전략 정립에 중요

- 우리 기업 및 이용자에 대한 영향뿐만 아니라, 미·중 기술패권 경쟁 과정에서 유사입장국(like-minded countries) 간의 기술 협력체 형성의 목적 또는 비전에 디지털 정보공간의 거버넌스, 가치 공유가 중요한 요소로 대두

15) China Daily, 'Public Pledge of Self-Regulation and Professional Ethics for China Internet Industry' (2002. 3. 26)

● 중국의 정보공간 거버넌스, 기술 권위주의는 단순히 경제·안보차원의 분리뿐만 아니라 가치, 정보공간의 분리, 정보경쟁 심화, 상호적대감 증대 등 우리의 대외정책 환경에 큰 영향을 미칠 것임

- 중국의 정보통제는 중국 공산당의 주요 지지계층인 20~30대 젊은 층을 중심으로 하는 폐쇄적이고 국수주의적인 세대의 등장을 촉진해, 특정 해외기업 제품 보이콧과 같은 경제적 압력(economic coercion) 등 전랑외교 수단도 강화됨

- 중국에서 사회신용 시스템에 대한 여론이 우호적으로 나타나는 등[16], 기술의 올바른 이용에 대한 인식도 큰 차이를 보여 줌

● 기술 권위주의의 중국內外 확산은 중국, 제3국 및 국내 기업에 경제적, 도덕적 문제를 야기

- 우리 기업이 중국의 규범에 따라야 한다면 (인권탄압에 남용될 수 있는 정보 제공 등) 도덕적인 문제를 야기할 수 있으며 이미 미국-유럽간 교역 및 기술 협의체(Trade & Technology Council: TTC), 미국-일본 Core Partnership 등의 기술협의체는 기술 권위주의에의 대응을 주요 아젠다로 채택하고 있음[17]

- 더구나 디지털 분야 경제개발 협력이 정치, 경제적 레버리지로 악용될 위험성도 다분

16) 베를린 자유대학의 2018년 사회신용시스템 찬성여부 조사에 따르면 어느 정도 찬성이 31.1%, 매우 찬성이 48.9%로 나타났다고 함. 즉 안전·신뢰의 편익이 감시에 따르는 불편보다 크다는 인식이 나타남. 차두원(2019. 11), '범죄 예방 vs. 사생활 침해, 하늘그물〈Skynet〉은 정말 악인만 잡아낼까?. 동아비즈니스리뷰

17) TTC는 인공지능과 같은 이중용도 기술에 대한 수출투자 통제의 이유로 사이버 감시기술에의 악용을 들고 있음

• 중국의 개도국 정보 및 디지털 인프라 장악, 감시 및 통제에 치중하는 중국 디지털 기술규범의 확산은 개방적·민주적 규범에 기반하는 국내 기업의 입지에도 부정적인 영향

- 이러한 가능성이 중국의 개발협력사업에 대한 논란으로 이어지고, 특히 첨단기술에서의 리더쉽을 둘러싼, 기술패권 경쟁의 전선을 형성

※ 개도국 디지털 인프라를 他기술권역이 장악하게 되면 데이터의 안전성, 신뢰성 측면에서 바람직하지 않음. 동일한 기술 규범을 가진 국가들과 네트워크, 클라우드, 그 위에서 작동하는 서비스에 이르기까지 공동 진출하는 것이 우리 국익에 부합

- 기술협력·동맹에 '가치'동맹의 성격이 점차 분명해질 것이기 때문에, 글로벌 기술규범에 대한 우리의 입장을 명확히 할 필요가 있음.

참 고 문 헌

중국 사이버공간 관리총국(CAC: Cyberspace Administration of China) 이론연구 소조(2017. 9. 15), “시진핑 총서기의 사이버 강국 전략사상을 심도 있게 이행하고 사이버 보안 및 정보화 업무를 확고히 추진한다”, http://www.qstheory.cn/dukan/qs/2017-09/15/c_1121647633.htm.

차두원(2019. 11), “범죄 예방 vs. 사생활 침해, 하늘그물〈Skynet〉은 정말 악인만 잡아낼까?”, 동아비즈니스리뷰.

최계영(2022. 7),『차가운 평화의 시대 : 우크라이나 전쟁 이후 미중 기술패권』, 인문공간.

A. Blinken(2022. 5. 26), “The Administration's Approach to the People's Republic of China”.

ASPI(2019. 11. 28), “Mapping China's Tech Giants : AI and surveillance”.

ASPI(2021. 6. 8), “Mapping China's Tech Giants: Supply chains & the global data collection ecosystem”.

China Daily(2002. 3. 26), “Public Pledge of Self-Regulation and Professional Ethics for China Internet Industry”.

EC(2021. 9. 29), “EU-US Trade & Technology Council Joint Statement”.

Hoffman, S(2019), “Engineering global consent: The Chinese Communist Party’s data-driven power expansion”, ASPI Policy Brief No. 21.

Johnson, Matthew D.(2020. 6), “Safeguarding socialism: The origins, evolution and expansion of China’s total security paradigm”, https://sinopsis.cz/en/johnson-safeguarding-socialism/.

MERICS(2022. 9. 15), “Comprehensive National Security" unleashed: How Xi's approach shapes China's policies at home and abroad”.

Xinhua(2014. 4). “中央国家安全委员会第一次会议召开 习近平发表重要讲话. 중앙국가안보위원회 첫 회의가 중요한 시진핑 연설을 제시하였다”. http://www. gov.cn/xinwen/2014-04/15/content_2659641.htm.