아시아리뷰 제10권 제1호(통권 19호), 2020: 53~79 https://doi.org/10.24987/SNUACAR.2020.08.10.1.53

중국의 사이버 안보전략과 북한에의 적용: 정체성과 인식을 중심으로*

박차오름 연세대학교 통일학협동과정 석사과정
부승찬 연세대학교 통일학협동과정 겸임교수

본 연구는 중국의 사이버 안보전략을 정체성과 인식을 바탕으로 분석하고, 이를 북한에 적용함으로써 향후 북한의 사이버 안보전략이 어떻게 구체화될 것인지를 전망하고자 한다. 구체적으로 유형 정체성과 위협인식에 따른 '체제의 위협 최소화'와 역할 정체성과 기회인식에 따른 '지위의 기회 최대화'로 세분화해 중국의 사이버 안보전략을 분석했고, 이를 토대로 북한의 사이버 안보전략의 방향성을 제시했다. 연구 결과, 중국과 북한 모두 '체제의 위협 최소화'를 추구하나, 중국은 공산당 영도의 사회주의체제라는 유형 정체성과 관련된 위협인식을 사이버 안보전략에서 구체화하고 있는 반면 북한은 최고지도자 중심의 1인 지배체제라는 유형 정체성과 관련된 위협인식을 근간으로 사이버 안보전략을 구체화할 것으로 보인다. 역할 정체성과 기회인식의 측면에서도 양자 모두 '지위의 기회 최대화'를 추구하나 중국은 경제발전의 새로운 동력으로 사이버 공간을 인식하고 '중국몽'이라는 역할 정체성을 실현하고자 한다면, 최근 '사회주의 경제건설 총력 집중 노선'으로의 전환을 선언한 북한은 중국의 정보화에 따른 경제발전을 예의주시하면서도 대북제재라는 제한적인 상황에서 지위 정상화를 위한 수단으로 사이버 활동을 강화할 것으로 보인다.

주제어 중국, 북한, 사이버 안보전략, 정체성, 인식

I. 서론

최근 북한은 사이버 공간에서의 안전보장이 전 세계적 관심사라고 언급하며(리효진, 2019), 국가 간 '새로운 전선'이 되고 있는 사이버 공간에 대한 대응으로 사이버 안보전략의 중요성과 필요성을 역설했다(김광명, 2019). 이는 열악한 대내외 환경에도 사이버 전력은 세계적 수준에 도달한 북한의 비대칭성을 지적한 것(김인수·KMARMA, 2015; 김흥광, 2011; 임종인 외, 2014; 황지환, 2017)에서 한 걸음 더 나아

* 본 논문의 발전을 위해 유익한 논평을 해 주신 두 분의 심사위원들께 감사드립니다. 더불어 논문의 수정·보완에 도움을 주신 연세대학교 정치외교학과 서정민 교수님과 정치학과, 통일학협동과정 원우들께도 감사드립니다.

간 새로운 상황인식이다. 이러한 상황인식은 결국 북한의 사이버 안보전략으로의 학술적, 정책적 접근을 요하나 관련 논의는 사실상 부재하다. 그렇다면 북한은 사이버 안보를 어떻게 인식하고 있고, 어떠한 상(像)을 그려 나가고 있는가? 본 연구는 이러한 문제의식에서 출발한다. 하지만 북한 체제의 폐쇄성에 따른 자료 접근 제한으로 북한의 사이버 안보전략에 대한 논의는 상대적으로 간접적이며 유추에 의존해야 하는 제약이 있다. 이러한 맥락에서 최근 발표된 중국의 사이버 안보전략은 북한의 사이버 능력을 분석하고, 사이버 안보전략을 전망하는 데 주요한 참고가 될 것이다. 무엇보다 복수의 연구에서 밝히듯이 사이버 영역에서의 북·중 협력과 의존관계의 중요도를 고려하면 더욱 그러하다(임종인 외, 2014: 31-34; 차정미·박차오름, 2019: 302; 황지환, 2017: 152).

특히 연구진행에서 사이버 영역에서의 '공격능력'에 집중한 권위주의 체제의 특수성에 대한 접근뿐만 아니라 '방어능력'에 초점을 두고 있는 보편성에 대한 접근이 필요하다. 물론 권위주의 체제의 정책결정이 다른 체제에 비해 비밀리에 결정돼 명확하게 의도를 파악하기 어려운 것은 사실이지만(Geddes et al., 2018) 특수성과 보편성을 함께 고려할 때, 보다 객관적인 분석이 가능해지기 때문이다.

따라서 본 연구는 중국의 사이버 안보전략에서 정체성과 인식이 어떻게 발현되는지를 살펴보고, 이를 통해 향후 북한이 수립할 혹은 이미 존재하는 사이버 안보전략에 대해 고찰할 것이다. 구체적으로 정체성에 해당하는 유형 정체성, 역할 정체성과 이에 상응하는 인식으로 위협인식과 기회인식을 통해 분석할 것이다. 이와 같은 접근은 안보학 이론의 구성주의 관점에 따른 것으로, 행위자의 정체성과 인식에 따른 행위 원인과 동기에 대한 고찰을 목적으로 함과 동시에 행위자의 본질적인 의도에 접근하기 위한 '관념변수'를 이용한 분석이라는 점에서 적합하다. 연구의 논리 전개상 우선 안보학 이론의 사이버 안보전략에 대한 시각과 특징을 알아보고 정체성과 인식의 상관관계를 유형화할 것이다. 다음으로 유형화한 결과를 토대로 중국의 사이버 안보전략을 분석한 후, 이를 북한에 적용해 북한의 사이버 능력과 사이버 안보전략에 대한 전망을 제시할 것이다. 마지막으로 분석 결과를 요약한 다음, 정체성과 인식을 통한 사이버 안보전략에 대한 연구 의의와 향후 북한의 사이버 안보전략에 대한 함의를 도출하고자 한다.

II. 안보학 이론에서의 사이버 안보전략

1. 기존 연구 검토 및 한계

사이버 안보전략(Cyber Security Strategy)은 사이버 안보(Cyber Security)[1]를 위한 하위영역으로 국가가 추진하고자 하는 전략적 차원의 구체적인 기조나 방향을 의미하는데, 국가별로 차이는 있지만 공통적으로 사이버 공간에서의 위협으로부터 국민의 이익을 보호하고 국가경쟁력 향상을 핵심 목표로 한다.[2] 이를 안보학 이론에 적용하면 사이버 안보전략에 대한 시각과 특징을 구체화할 수 있다. 우선 현실주의적 관점에서 국가는 국익을 위해 합리적으로 행동하며 권력과 안보를 핵심 가치로 전제하기 때문에(Eriksson and Giacomello, 2007: 11) 무정부 상태에서 힘의 분배(distribution of power)에 초점을 맞춰 국력 확보를 주장한다. 또한 안보는 국력으로 보장된다는 자조(self-help) 개념이 안보 딜레마를 심화시켜 국가 간의 협력을 어렵게 한다고 인식한다(이동선, 2009: 57-60). 따라서 안보 불안을 극복하고자 하는 국가 간 국력 증강이 현실주의가 주목하는 지점인데, 최근 미·중 간 사이버 패권 경쟁이 대표적인 사례다. 이에 대한 국내외 연구는 사이버 공간에서의 이른바 '위협 실재론'[3]에 대한 관심을 방증하는 대목이다(Akdag, 2019; Hjortdal, 2011; Manson, 2011; 김관옥, 2015; 차정미, 2019). 이러한 맥락에서 사이버 억지전략(cyber deterrence strategy)의 적용 가능성이 논의의 쟁점인데 전통적 억지

1 사이버 공간(Cyber Space)에서의 안전보장(Security)을 의미하는 것으로 전통적 안보와는 다른 특성과 환경(컴퓨터 시스템 기반, 공격이 방어보다 유리, 피해여부 및 피해대상 구분의 어려움 등)을 바탕으로(김상배, 2017: 71), 다양한 형태·성격의 사이버 위협(Cyber Threat)으로부터 국가뿐만 아니라 여러 주체의 안전보장 혹은 네트워크 자체에 대한 보호를 의미한다(조현석 외, 2017: 91).

2 우리나라는 "자유롭고 안전한 사이버공간을 구현하여 국가안보와 경제발전을 뒷받침하고 국제평화에 기여"함을 비전으로 목표, 기본원칙, 전략과제를 제시하며(국가안보실, 2019), 미국은 "미국인의 원칙을 반영하고, 안보를 보호하고, 번영을 촉진하는 안전한 사이버 공간의 혜택 지속"을 비전으로 4개의 핵심 근간(Pillar)을 제시하며(The White House, 2018), 중국은 "사이버 안보는 중화민족의 위대한 부흥, 즉 중국의 꿈을 실현하는데 중요"하므로 기회와 위협, 목표, 원칙, 전략적 임무를 제시한다(国家互联网信息办公室, 2016). 다른 국가들의 사이버 안보전략에 대해서는 김상배(2017: 75-101) 참고.

3 사이버 공간의 위협 실재론에 대해서는 장노순·한인택(2013: 581-585) 참고.

전략을 그대로 적용하는 한계로 인해 보완된 사이버 억지전략이 제시되고 있다.[4] 그러나 현실주의는 사이버 안보가 복합적 이슈와 여러 행위자가 결합된 초국적 신흥안보(emerging security)임에도 불구하고 안보 불안에 따른 국력 증강에 초점을 맞춰 국가 중심의 군사안보 개념으로만 접근한 한계가 있다(김상배, 2015: 26-27).

자유주의적 관점에서는 국제 행위자의 다원성, 특히 국가 행위에서 국내정치 요인의 중요성을 인정한 가운데 국가 행위를 규율하는 국제 제도의 역할에 주목한다(Eriksson and Giacomello, 2007: 13). 국제체제의 무정부성을 인정한다는 점에서 현실주의와 유사하지만, 안보위협은 행위자 간 협력이 실패할 경우에 발생하고, 제도를 통한 협력으로 극복할 수 있다고 보는 점에서 차이가 있다(이근욱, 2009: 37-45). 무엇보다 자유주의는 사이버 안보에서의 상호 협력을 통한 일종의 집단 안전보장(collective security)이 가능하다고 보는데(Austin, 2016; Burton, 2015; Carr, 2016; O'Connell, 2012), 다양한 수준의 행위자 간 국제 협력을 촉진하고 지원하기 위해 장려책으로 마련된(O'Connell, 2012: 208) 대표적 사례로 '국제안보 영역에서 정보통신분야 발전에 관한 정부전문가그룹(UN Group of Governmental Experts)'을 들 수 있다. 이 그룹은 집단적 위험을 줄이기 위한 정보통신기술의 국가 사용에 관한 규범이 필요하다고 인식했고(장노순·한인택, 2013: 608), 2013년 최종 보고서를 통해 사이버 안보 분야에서 국가 간 협력 방안을 제시해 국제 규범의 초석을 마련했으나 국가 간 입장 차이로 실제 이행에는 한계[5]를 드러냈다(조화순·김민제, 2016: 86). 이는 국제 영역에서 다양한 행위자 간 규범 마련이나 공조가 쉽지 않음을 보여 주며, 특히 국제기구와 같은 제도를 통한 협력을 강조하는 자유주의의 한계가 나타난다.

현실주의나 자유주의와는 달리 구성주의는 현실이 가변적이라는 인식하에 국가의 인식과 역할에 초점을 두고 국가 행위의 원인과 동기를 분석한다. 구성주의는 국가의 정체성으로부터 국가 행위가 발현되어 간주관성(inter-subjective understanding)에 영향을 주고, '국제정치가 사회적으로 구성'되는 동태성(動態性)

4 사이버 억지전략 관련 논의에 대해서는 장노순·한인택(2013: 591-599) 참고.

5 사이버 안보의 국제 협력 한계에 대해서는 조화순·김민제(2016: 83-88) 참고.

을 강조함으로써 안보학 이론에 새로운 인식론적 시각을 제공한다(최종건, 2009: 84-87). 사이버 안보 분야에서도 인식의 분배(distribution of idea)를 강조하는 구성주의적 접근(Wendt, 1999: 370-372)을 적용한 연구들이 등장하는데, 이들의 대체적인 시각은 정체성과 국가정책이 상호연관성을 갖기 때문에 균형이 나타난다는 것이다(Ciolan, 2014; Eriksson and Giacomello, 2014; Kiggins, 2012; Simons, 2014).

한편, 중국과 북한의 사이버 안보전략에 대한 기존 연구 중 우선 중국의 사례는 서구와는 다른 형태, 개념, 인식의 특징이 나타난다(Chang, 2014; Swaine, 2013; 조윤영·정종필, 2016; 조현석 외, 2017). 즉 대외적 차원뿐만 아니라 대내적 차원의 정치·경제적 목표에 직결된 '중국 특색'으로 사이버 안보전략은 통합적 시각에서 다뤄져야 한다는 것이다(조현석 외, 2017: 93-94). 이는 시진핑(習近平) 체제에 들어 국제적이고 공세적인 사이버 안보정책 수립으로 역량을 강화하는 한편, 여전히 내부적 차원의 통제와 발전을 병행하는 양면적 양상으로 구체화된다(김상규, 2019: 56-61; 차정미, 2018: 17-18). 북한에 대한 기존 연구는 주로 현실주의에 근거한 사이버 전력 분석에 집중되어 있는데 정보전에 대한 필요성을 바탕으로 구축 과정과 현황 분석(김흥광, 2011), 다양한 차원의 기준을 통한 사이버 전력의 종합적이면서도 다각적인 평가(임종인 외, 2014), 정치·경제·사회·군사적 조건으로 사이버전의 교리·조직 분석(김인수·KMARMA, 2015), 국제정치 관점에서 사이버전의 위협 영향 고찰(황지환, 2017) 등이 이뤄져 왔다.

종합해 보면, 현실주의는 무정부 상태에서의 상대적 힘이라는 '구조변수', 자유주의는 국내정치와 국제제도라는 '과정변수', 구성주의는 무정부 상태와 국가의 정체성 간 상호작용이라는 '관념변수'에 초점을 두고(이근욱, 2009: 35-38) 사이버 안보전략을 분석하고 있다. 하지만 중국과 북한에 대한 기존 연구는 '관념변수'가 사이버 안보전략의 핵심원리로 작용함에도 이를 간과한 한계가 있다.[6] 물론 관념변수와 사이버 안보전략 간의 인과관계가 명확히 드러나지 않기 때문에 어느 정도 유추에 의존해야 하나, 행위 원인과 동기에 대한 구체적 분석 없이 위협 혹은 협력만을 강조하는 것은 객관성 담보에 일정 부분 한계가 따른다. 이

6 국가가 추진하는 사이버 안보전략의 특성을 고려하면 행위 주체인 해당 국가의 관념을 주목해야 하기 때문이다.

러한 흐름에서 본 연구는 구성주의적 접근에 입각해 정체성과 인식을 중심으로 중국의 사이버 안보전략을 분석하고, 분석 결과를 바탕으로 북한 사이버 능력의 현황과 사이버 안보전략에 대한 전망을 고찰하고자 한다. 이는 국가 정체성 역학(national identity dynamic)이 국가 정체성에 대한 위협인식, 기회인식과 밀접한 연관을 갖고 사회-심리학적 설명을 목적으로 하는 맥락과도 일치한다(Bloom, 1993: 79). 다시 말해, 구성주의는 이론과 실증의 측면에서 현실주의, 자유주의에 비해 빈약할지 몰라도 관념적 가치(ideational value)로 국가의 행위를 설명하는 당위성 측면에서는 오히려 지나치게 사이버 위협과 협력을 강조하는 현실주의와 자유주의의 한계를 극복할 수 있는 것이다(최종건, 2009: 91). 더불어 중국의 인터넷 발전전략에 국가의 핵심 지도원리가 반영되어 있고, 북한도 이를 벤치마킹할 가능성을 시사했던 기존 연구(차정미·박차오름, 2019)의 문제의식을 '관념변수'의 측면에서 발전시키는 의미가 있을 것이다.

2. 정체성과 인식 기반의 사이버 안보전략

중국은 개혁개방 이후 현재까지 사회주의 체제에서의 경제발전을 이루겠다는 '1개 중심 2개 기본점 원칙(一个中心两个基本点)'을 고수하는데, 공산당의 사회주의 영도를 통해 경제발전을 달성한다는 '1개 중심'과 정치체제를 유지한다는 '2개 기본점'이 이에 해당한다. 이러한 원칙을 사이버 영역에 적용할 경우 경제발전을 위한 정보화와 체제유지를 위한 사이버 안보 강화로 나타난다(차정미·박차오름, 2019: 287-293). 이와 유사하게 북한도 양자택일이 아닌 양자조합의 기치를 적용할 것으로 보이는데, 최근 김정은 체제에서 경제발전과 정보화의 상관관계를 전제한 '사회주의 강국 건설'의 강조가 이를 뒷받침한다. 즉 경제발전과 체제유지를 병행하겠다는 것으로, 중국과 유사한 논리로 관련된 인식과 전략이 도출된다는 것이다. 그러나 체제 특성상 북한의 위협인식이 중국보다 높을 수 있는데, 이러한 추정은 북한의 1인 지배체제와 중국의 일당 지배체제 간의 차이에 기인한다고 볼 수 있다. 그럼에도 중국의 사례는 북한에 일종의 지침서로 작용할 수 있는데, 중국 사례가 경제발전과 체제유지를 동시에 달성한 성공사례로 평가되기 때문이다(차정미·박차오름, 2019: 294-303). 따라서 두 국가의 사이버 안보

전략도 경제발전을 위한 정보화와 체제유지를 위한 사이버 안보 강화의 병행으로 구현되고 있다고 볼 수 있다. 같은 맥락에서 본 연구는 국가 정체성과 인식이 대외정책을 결정하는 데에 영향을 준다는 블룸(Bloom)과 이러한 정체성을 구체화했던 웬트(Wendt)의 문제의식을 결합해 중국의 사이버 안보전략을 분석하고, 이를 북한에 적용해 사이버 능력 현황과 사이버 안보전략을 전망해 보고자 한다.

웬트는 정체성을 설명하면서 유형 정체성(Type identity)과 역할 정체성(Role identity)을 언급했는데 전자는 체제 유형이나 국가의 구성에 근거한 것으로 민주주의 혹은 권위주의와 같은 정치체제 속성에 따른 정체성이며, 후자는 국가 간 상호작용에 따라 구성된 지위를 일컫는 것으로 국가관계에서 비롯된 역할 속성에 따른 정체성을 의미한다. 웬트는 이러한 정체성이 국가 행위를 결정하며, 국가안보와 연관된 국가이익 실현에도 영향을 미친다고 보았다(Wendt, 1999: 224-245). 웬트의 논리를 사이버 안보전략에 적용할 경우, 체제와 지위에 근거한 정체성이 사이버 안보전략에 반영되고 이를 통해 사이버 영역에서 국가이익을 달성하려는 것으로 볼 수 있다. 하지만 이러한 과정에서 단순하게 정체성만이 작동한다고 보기에는 무리가 있다. 왜냐하면 국가안보에 정체성이 주요 요소로 투영되고 발현되기는 하지만(Katzenstein, 1996: 499), 이와 더불어 행위자의 인식을 바탕으로 안보환경이 구성되기 때문이다(최종건, 2009: 95). 이러한 맥락에서 '① 국가 정체성이 위협받거나, ② 국가 정체성을 강화할 기회가 있을 때 이를 보호·강화하고자 정체성이 작동'한다는 블룸의 국가 정체성과 인식 간의 상관관계 설명은 본 연구에서도 유용하다. 정체성과 인식은 상호 간의 밀접한 연관성에 의해 작동되는 것이며, 특히 이러한 현상은 정책 수립에서 두드러지게 나타난다는 블룸의 주장을 보면 더욱 그러하다(Bloom, 1993: 76-103).

두 학자의 주장처럼 국가가 정체성과 인식에 근거해 행동한다고 가정하면, 정체성은 체제 속성에 따른 유형 정체성과 국가 지위에 따른 역할 정체성으로 구분되고, 대외환경에 대한 인식은 위협인식과 기회인식으로 나눌 수 있다. 또한 국가이익은 국가 정체성의 한 부분으로서 보호·강화해야 하기 때문에 정체성에 따른 인식은 유형 정체성과 위협인식(체제의 위협 최소화), 그리고 역할 정체성과 기회인식(지위의 기회 최대화)으로 구체화된다. 표 1에서 보듯이 정체성과 인식을 기준으로 4개로 분류가 가능하지만 웬트와 블룸의 이론적 교차지점과 사

표 1 정체성과 인식에 따른 상관관계 유형 분류

정체성 \ 인식	위협(최소화)	기회(최대화)
유형(체제)	체제의 위협 최소화	체제의 기회 최대화
역할(지위)	지위의 위협 최소화	지위의 기회 최대화

출처: Bloom(1993), Wendt(1999)를 바탕으로 유형화.

이버 안보전략이라는 특성[7]을 고려하면 앞서 서술했듯이 체제에 대한 위협을 최소화하고 지위에 대한 기회를 최대화(음영표시)하는 상관관계 접근이 적합하다.

정체성과 인식의 상호작용에 초점을 둔 이러한 유형 분류는 구성주의적 관점(Eriksson and Giacomello, 2007: 19)에 기초한 것으로 사이버 안보전략에 대한 표면적 이해에만 그치는 것이 아닌, 보다 본질적인 이해를 위해 '관념변수'에 주목하는 의의가 있다. 특히 국가 간 사이버 안보의 개념과 담론에 대한 합의가 어려운 현실에서(Chang, 2014: 29; 김상규, 2019: 45; 김상배, 2015: 16; 채재병, 2013: 183), 개별국가의 인식과 담론 분석이 체제 단위에서의 분석과 전망에 중요한 기초연구라는 대목은 구성주의적 접근의 필요성을 방증한다(차정미, 2018: 4). 무엇보다 중국의 사이버 안보전략을 정체성과 인식을 바탕으로 해석해 북한의 향후 사이버 안보전략에 적용하는 것은 권위주의 체제의 특수성과 보편성을 동시에 고려하는 의미가 있다.

7 사이버 안보전략은 ① 물리적 국경을 초월한 공간 ② 공격주체의 신원(국가/비국가 행위자) 확인의 어려움 ③ 방대한 공격영역으로 집약되는 사이버 공간의 특성(조화순·김민제, 2016: 78)에 기인해 사이버 공격으로부터 체제를 수호하고 이를 바탕으로 지위를 확대하고자 하는 메커니즘을 따른다. 관련된 실제 사례로 러시아는 2000년대 서방(西方)의 가치, 제도, 규범 확산을 체제전복의 기도로 간주했다. 이는 '게라시모프 독트린'이라는 전략인식의 변화를 통한 2014년 5월 사이버전 전담부대 창설 결정으로 이어졌는데(윤민우, 2018: 271), 기저에는 러시아의 '체제의 위협 최소화'가 내포되어 있다. 미국은 포괄적 사이버 역량강화를 통해 주요 경쟁자인 러시아, 중국에 대한 패권적 지위를 유지하는 것을 목표로 하며(윤민우, 2018: 274-275), 기저에는 미국의 '지위의 기회 최대화'가 내포되어 있다.

III. 중국의 사이버 안보전략

시진핑은 사이버 영역에서의 발전과 관리가 동시에 이뤄져야 함을 강조함으로써 사이버 공간의 기회와 위협의 양면성에 대한 인식을 드러냈다(国家互联网信息办公室, 2019a). '국가사이버공간안전전략(国家网络空间安全战略, 이하 안전전략)'이라는 중국 최초의 사이버 안보전략은 이러한 인식이 구체화된 결과물이다. 이에 대해 앞 장에서 설명한 분석 틀을 바탕으로 공식 문헌에서 나타나는 중국의 정체성과 인식을 분석하고자 한다.

1. 유형 정체성과 위협인식 기반

다른 나라와 구별되는 중국 체제의 독특한 특성은 '중국특색(Chineseness)'으로 지칭된다. 이는 과거 중국의 역사적 굴욕과 국가 자존심의 손상이 단순한 묘사에 그치지 않고, 전략적 현실에 대한 중국의 인식에서 강한 요소로 작용함에 따라 나타난 결과다. 즉 국가주권 회복과 국가 통합이라는 목표 달성을 위해 국가 정체성이 발현되었고, 국내외적인 취약성 극복이라는 안보 과제는 중국의 생존과도 연계된다고 인식한 것이다(Nathan and Scobell, 2015: 31-33).

결국 정체성과 인식은 중국의 사이버 안보[8]에도 적용되는데, 중국은 사이버 안보가 곧 국가안보이며 당(黨)의 통치에 대한 위협 완화를 위한 수단으로 인식한다. 이는 국가안보를 위한 정책결정 및 이행에 대한 통제를 정당화하는 의미다(Chang, 2014: 12). 이러한 인식은 중국 체제를 굳건히 함으로써 당의 영도를 확고히 유지하는 것으로 연결되며, 정치·사회적 안정 확보까지 이어지게 된다. 이를 위해 사이버 공간에서는 대내적으로 정보 통제와 관리, 대외적으로 주권 확립이 핵심 요소가 될 수밖에 없는 것이다(조현석 외, 2017: 97). 요약하면, '중국 특색의 사회주의'를 강조하는 중국이 '공산당 영도의 사회주의체제'를 최우선 안보대상으로 삼고자 한다는 것이다(차정미, 2018: 17). 즉 사이버 안보전략에서 중국

8 중국은 사이버 안보를 'information security(信息安全)' 혹은 'network security(网络安全)'라는 단어로 표현한다. 관련 내용에 대해서는 Chang(2014: 13-14); 조윤영·정종필(2016: 156) 참고.

의 유형 정체성은 공산당 영도의 사회주의 체제이며, 이와 관련된 위협인식은 체제에 대한 대내외 위협에 기인한다. 이러한 유형 정체성과 위협인식은 '체제의 위협 최소화'로 귀결된다.

2016년에 발표된 중국의 '안전전략'의 세부 내용을 통해 보다 구체화된 유형 정체성과 위협인식을 확인할 수 있다(国家互联网信息办公室, 2016). 우선, 전문(前文)에서 정보기술과 사이버 공간의 발달이 새로운 안보 위협과 도전을 초래할 수 있으며 사이버 안보가 국가안보에 직결됨을 언급했다. 중국은 사이버 안보 유지가 당 전략의 충분한 이행과 개혁의 수단으로서 중요하다고 인식하는 것이다. 1장에서는 심각한 도전으로 사이버 침투로 인한 정치적 안보위협을 가장 먼저 꼽았으며 경제·문화·사회적 안보위협이 뒤를 이었는데, 정치체제에 대한 위협인식을 우선적으로 하고 있음을 보여 주는 대목이다. 이는 기술적 위협을 강조하는 서구의 사이버 안보 인식과 달리 이데올로기적 위협에 방점을 두는 것으로(김진용, 2018: 175), 정치적 측면에서 당 지배의 지속과 국내 정치·사회적 안정이라는 목표를 추구(조현석 외, 2017: 97)하는 것과도 일맥상통한다. 특히 당은 '체제의 위협 최소화' 일환에서 정치·경제·군사적 영역의 사이버 안보전략을 관할하는 기구로 새로운 영도소조[9]를 출범시킴으로써 일원화된 통합 지도체제의 완성으로 대응했다(조윤영·정종필, 2016: 159-160). 이와 같은 당의 대응은 '안전전략'을 통해 더욱 구체화되었는데, 위협인식으로부터 유형 정체성을 수호하려는 목적을 명문화(明文化)한 것이다.

또한 2장에서 전략의 목표로 제시하는 평화(和平)·안보(安全)·개방(开放)·협력(合作)·질서(有序) 역시 '체제의 위협 최소화'의 맥락을 전제하고 사이버 공간(특히 내부적)에 대한 제한과 통제 등의 관리(治理)를 지속적으로 강조한 것으로 볼 수 있다. 이는 사이버 공간에서의 위협이 상존한다고 보는 관점으로 체제에 대한 위협을 선제적으로 관리해야 할 필요성이 반영된 것이다. 3장에서는 사이버 공간을 '통제'할 수 있는 주권을 주장하면서 이에 대한 '보호'를 핵심 개념으로 제시하는데 핵심은 '체제의 위협 최소화'에 있으며, 중국이 주창하는 주권 확립의

9 중국의 영도소조란 당의 정책 결정이나 정책 집행 과정에서 다양한 조직·집단의 참여와 상호 협의를 제도적으로 보장하기 위한 일종의 '관계기관 협의체'를 의미한다(서진영, 2006: 80-81).

기저에도 이 논리가 동일하게 내재되어 있다. 4장에서 제시된 전략적 임무로 사이버 영역에서의 주권·국가안보·사회 기반시설 등의 보호 역시 3장의 논리가 확장되어 제시된다. 이러한 논리는 중국의 유형 정체성과 위협인식이 결합된 것으로 최근 '사이버 안보 위협정보발표 관리방법(网络安全威胁信息发布管理办法)'도 이를 뒷받침한다. 즉 사이버 안보 위협정보 관리를 위한 13개의 조항은 궁극적으로 사이버 안보 관련 규범화와 효율적인 대응을 목적으로 한다(国家互联网信息办公室, 2019c). 이는 자국의 사이버 안보 강화를 위한 것으로 위협정보에 관한 법률이나 규제의 부재에 기인한다는 언급을 통해서도 뒷받침된다(国家互联网信息办公室, 2019d). 이러한 일련의 사례들은 앞서 논의한 '안전전략'에서의 유형 정체성과 위협인식이 강화된 것으로 사이버 공간의 위협 요소들을 사전에 예방하고 통제하려는 목적으로 해석할 수 있다.

종합해 보면, 사이버 안보전략에서 중국의 유형 정체성은 위협인식과 밀접하게 연관되어 궁극적으로 공산당이 주도하는 체제유지를 목적으로 한다. 여기서 위협인식 바탕의 체제유지라는 목적은 다른 국가 사례와 유사한 보편성을 보이지만, 공산당 주도의 강한 통제에서는 중국의 특수성이 나타난다. 이는 시진핑 체제에 들어 이전 체제보다 공격적인 양상으로 변모하는데, 핵심은 중국이 국내정치의 안정적 국정 운영을 가장 최우선 정책 목표로 상정하기 때문에 사이버 영역에서 관련 문제들이 국가 위기로 확대되는 것을 우려한다는 점이다(김상규, 2019: 59-60). 이러한 우려는 중국으로 하여금 대내적으로는 국내정치적 안정과 대외적으로는 주권 확립 차원에서 사이버 영역의 '통제'에 집중하도록 함으로써 '체제의 위협 최소화'를 실현하려는 것으로 볼 수 있다.

2. 역할 정체성과 기회인식 기반

중국의 경제발전은 1차적으로 내부성장을 가능하게 했고 세계경제에서 존재감을 드러내는 동력이 되었다. 1978년의 개혁개방이 중요한 시초가 된 것인데, 경제발전을 위한 인식 전환은 정보화를 위한 교류협력과 육성정책에 대한 적극적인 벤치마킹으로 이어졌다. 이를 토대로 급속한 발전이 이뤄졌는데, 당이 경제발전을 위한 핵심 동력으로 정보화를 인식한 결과다. 특히 '중국몽(中国梦)' 실

현과 관련해 사이버 공간을 발전시키는 것이 이를 달성하는 핵심 수단이 된다는 기회인식을 바탕으로 관련된 지원을 아끼지 않고 있다(차정미·박차오름, 2019: 290-291). 이와 같은 경제발전에 대한 집중은 중국의 중요한 목표[10]인데, 이를 실현하는 수단으로 정보화를 강조한다. 중국에게 '정보화(信息化)'는 정보통신기술(ICT) 산업과 관련 요소의 개발을 통해 산업사회를 정보사회로 현대화하고 변화시키는 것을 목표로 하는 일종의 '체계'를 의미한다(Chang, 2014: 13). 정보혁명이라고도 일컬어지는 정보화는 당의 주도가 핵심으로 당은 정보화의 창시자, 후원자, 관리자로 언급되기도 한다. 이를 통해 당은 정책 집행의 강점과 신뢰성을 확보하는 효과도 얻는데, 경제발전의 지속은 정치적 정당성의 유지와 연관된다. 즉 당의 운명은 연간 국내총생산(GDP)의 성장률에 달려 있다고 해도 과언이 아니며, 경제적 요인은 항상 안정된 지배구조를 위해 필요한 전제라고 언급되기도 한다(Wu, 2007: 145-146).

나아가 경제발전을 위한 정보화는 궁극적으로 체제유지와도 연결되며, 둘은 모순적 관계가 아닌 순환적 관계에 해당한다. 경제발전을 통해 정치적 정당성을 획득해 체제유지를 공고히 할 수 있고, 안정적 체제에서 경제발전에 더욱 집중할 수 있다. 이러한 측면에서 중국의 사이버 안보전략은 대내적 차원이 포함된 중국적 특성이 배어 있다(Chang, 2014: 21; 김상규, 2019: 60; 조현석 외, 2017: 93-94). 이는 '안전전략'이 발표되기 전부터 구체화되었는데 당의 권력 연장이라는 목표와 내부 안정 유지, 사회정치적 불안 억제, 경제성장 촉진이라는 목표에 의해 사이버 안보전략이 추진되었다. 이 중 지속적인 경제성장 보장과 국내 사이버 범죄 활동억제라는 두 가지 하위목표는 중국의 전략이 경제발전과 체제유지를 핵심으로 하고 있음을 의미한다(Chang, 2014: 21-23). 이러한 전제를 바탕으로 중국이 사이버 안보를 경제발전과 불가분의 관계로 인식함을 확인할 수 있다. 시진핑의 "사이버 안보와 정보화는 양 날개이자 양 축"이며 "정보화 없이는 현대화도 없다."라는 발언(新华网 14/02/27)은 이를 대변한다. 역할 정체성과 기회인식으로 해석하면 국제사회에서 '중국몽' 실현이 전자에, '정보화를 통한 경제발전'이 후자

10 중국의 경제발전은 '1개 중심 2개 기본점 원칙'에서 '1개 중심'에 해당하는 것으로 가장 중요한 개념으로 강조된다. 관련 내용에 대해서는 차정미·박차오름(2019: 287-290) 참고.

에 해당한다고 볼 수 있다.

'안전전략'에서 더욱 구체화된 역할 정체성과 기회인식을 확인할 수 있는데(国家互联网信息办公室, 2016), 1장의 중대한 기회에서 중국은 경제발전의 새로운 동력으로 사이버 공간을 인식하고 있다. 이는 관련 기술의 발달을 통한 새로운 공간의 형성으로 문화적 번영, 사회적 통치, 교류·협력, 그리고 국가주권의 확장이 가능하게 되었기 때문이다. 따라서 중국은 기회와 도전이 공존하나 기회가 더 크다는 인식하에 체계적인 발전과 관리를 통한 적극적인 활용으로 사이버 공간의 잠재력을 극대화하고자 한다. 3장에서는 경제발전을 위한 정보화와 사이버 안보의 연관성에 대해 명확하게 언급하는데, "안보가 발전의 전제조건인 동시에 발전이 안보의 근간"이며 "발전하지 않는 것은 심대한 위험"이기 때문에 "정보화 없이는 사이버 안보가 불가능하고 기존의 안보마저 상실될 것"으로 보고 있다. 이는 앞서 언급한 시진핑의 인식에서 더 나아가 경제발전과 사이버 안보의 상관관계를 더욱 명확히 한 것이다.

4장에서는 사이버 안보를 위한 전략적 임무로서 사이버 문화 공고화, 사이버 통치체계 개선, 그리고 국제적 협력 강화를 제시하는데 이는 궁극적으로 '일대일로(一带一路)' 건설 촉진을 목적으로 한다. 일대일로 가입국에 대한 중국의 막강한 디지털 영향력 행사는 이러한 목적이 현실에서 구체화된 것으로 중국판 GPS인 베이더우(北斗·북두)위성항법 시스템 실시, 화웨이의 5G 통신망 지원 및 해외 데이터 센터 개설, 알리바바의 블록체인 송금 서비스 운영 등이 이에 해당한다(곽예지, 2019). 물론 이러한 사례들이 사이버 안보와 직결되는 것은 아니지만 일대일로 건설의 기반을 확대, 강화하는 측면에서 유의미하다. 미국 사이버 보안회사 크라우드스트라이크(CrowdStrike)가 최근 발표한 '2020 글로벌 위협 보고(2020 Global Threat Report)' 역시 동일한 맥락에서 중국 사이버 안보의 전략적 임무를 분석했다. 디지털 실크로드를 발전시키려는 중국의 구상이 디지털 연결을 확대, 강화로 나타나는데 국경을 초월한 다양한 인프라 구축이 이에 해당한다고 본 것이다(CrowdStrike, 2020: 56). 중국은 자신이 주도하는 질서와 규범을 정보화와 결합해 세계적으로 확대하려는 명확한 의도를 가지고 있으며, 이는 역할 정체성과 기회인식이라는 상관관계 속에서 '지위의 기회 최대화'라는 목표로 사이버 안보전략에도 구현되고 있다고 볼 수 있다.

‘안전전략’에 반영된 역할 정체성과 기회인식은 최근 공업·정보화부가 발표한 ‘사이버안보 산업발전 촉진 지도의견(关于促进网络安全产业发展的指导意见)’에서 더욱 구체화된다(国家互联网信息办公室, 2019b). 해당 문건의 서두에서 발전 이념에 기초한 사이버 안보를 강조하고 있으며, 관련 산업의 규모와 환경이 이전에 비해 개선되었으나 더욱 발전시키는 것이 목적임을 밝혔다. 이를 위한 인프라와 지원 환경을 한층 견고히 함으로써 2025년까지 연간 수입으로 20억 위안, 총 산업 규모로 2,000억 위안을 초과하는 목표를 제시했다. 이러한 중국의 역할 정체성과 기회인식은 궁극적으로 ‘중국몽’의 실현과 확장으로 이해할 수 있다. 또한 중국은 이를 사이버 안보전략과 연계해 추진함으로써 관련 산업을 더욱 발전시키고자 하는 의도를 지니고 있으며, 사이버 영역에서의 ‘지위의 기회 최대화’를 실현하고자 한다.

요약컨대, 사이버 안보전략에서 중국의 역할 정체성은 국제사회에서의 ‘중국몽’ 실현으로 집약되는데 자신의 지위를 격상하려는 목적으로 일대일로를 사이버 공간에서 확대하려는 모습으로 나타났다. 동시에 기회인식으로서 정보화를 통한 사이버 공간 발전으로 구체화되어 ‘안전전략’에 반영되었던 것이다.

IV. 북한에의 적용

1. 북한의 사이버 능력 현황

그동안 북한은 자신의 체제를 대내외, 특히 외부의 위협으로부터 수호하고자 사활을 걸어왔다. 냉전 종식 이후 국제환경의 급변으로 북한의 위협인식은 최고조에 이르렀으며, 고립은 더욱 심화됐다(Kim, 2011: 106-107). 북한은 국가안보와 군사안보를 동일시한 가운데 ① 직면한 위협을 군사사상에 따라 의미를 부여하는 군사우위의 원칙과 ② 외부에 의지하지 않고 자신의 생존은 스스로 지키겠다는 자기의존의 원칙, 그리고 ③ 생존을 위해서는 외부의 간섭과 제약에 구애받지 않고 위협대상에 대해 모험적 행위도 독자적으로 결정하고 행사한다는 행동자유의 원칙에 따라 생존전략을 구현해 왔다. 또한 이러한 원칙은 ① ‘외부 의

존을 통한 생존 보장'의 외적 균형보다는 '위협에 맞서 스스로의 힘으로 대항할 수 있는 국방력 강화'의 내적 균형 강화, ② 미국의 핵위협으로부터 자위·실존적 억지 수단으로서 핵무기 개발과 핵전략의 수립, ③ 군사전략으로서의 공세적 억지전략의 수립과 시행으로 이어졌다(부승찬, 2017: 6-20).

북한의 이러한 생존전략은 사이버 영역에서도 동일하게 적용되었고, 앞서 살펴본 유형 정체성과 위협인식에 연계되어 구현됐다. 북한의 유형 정체성은 최고지도자 중심의 1인 지배체제로, 김정은 체제 초반의 '핵·경제력 병진노선'에서 2018년 '사회주의 경제건설 총력 집중 노선'으로의 전환(로동신문 18/04/21)에도 불구하고 유형 정체성과 위협인식은 일관되게 나타난다. 집권 초기 김정은의 "사이버전은 핵, 미사일과 함께 인민군대의 무자비한 타격 능력을 담보하는 만능의 보검"(문동희, 2019)이라는 발언은 사이버 공간을 전쟁터와 유사한 개념으로 인식하는 것이다. 나아가 '체제의 위협 최소화'의 방편으로 자기역량 강화라는 북한의 특수성 역시 나타난다. 북한은 2013년경부터 사이버 해킹 조직을 신설하고, 재편하기 시작했으며 전문성 제고와 임무 세분화를 목적으로 자금과 인력을 집중해 오고 있다(목용재, 2017). 또한 최근 북한의 백신 소프트웨어에 최초로 랜섬웨어(ransomware)[11] 방지 기능이 탑재된 것은 내부에서 이로 인한 피해가 발생하고 있거나, 높아진 위협인식에 근거한 것으로 유추할 수 있다(강진규, 2019b).

이러한 유형 정체성과 위협인식은 공격능력과 밀접하게 연계되어 있다. 물론 전통적 안보와는 다른 사이버 영역의 특성과 환경으로 사이버 안보 능력을 명확하게 파악하는 데는 어려움이 따른다. 그럼에도 불구하고 다수의 연구는 공통적으로 북한의 사이버 공격능력이 세계적 수준이라고 평가한다(김인수·KMARMA, 2015; 김홍광, 2011; 임종인 외, 2014; 황지환, 2017). 구체적으로 해킹을 위해 네트워크에 침투하는 시간을 기준으로 북한은 러시아에 이어 세계 2위로 평가됐으며, 이를 뒷받침하는 사이버전 인력은 2013년에 비해 2배 이상 증가한 6,800여 명으로

11 몸값을 뜻하는 Ransom과 컴퓨터 프로그램의 총칭인 Software가 합쳐진 컴퓨터 악성 프로그램의 일종으로, 공격자가 피해자에게 금전(암호화폐)을 요구하는 사이버 범죄다. 2016년은 전 세계 개인과 기업을 대상으로 랜섬웨어 기반의 대규모 공격이 이뤄져 '랜섬웨어 공격의 해(the year of ransomware attacks)'로 불리기도 한다(Encyclopædia Britannica, 2016).

표 2 5개국 사이버 능력 종합평가[12] (단위: 점)

요소 / 국가	사이버 공격	사이버 방어	사이버 의존도[13]	총계
북한	2	7	9	18
러시아	7	4	5	16
중국	5	6	4	15
이란	4	3	5	12
미국	8	1	2	11

출처: Clarke and Knake(2010: 73)을 바탕으로 재구성.

파악되었다(국기연, 2019; 오택성, 2019). 이러한 세계적 수준의 공격능력은 표 2의 사이버 능력 종합평가에서는 5개국 중 가장 낮은 점수로 나타났는데(음영표시), 북한의 공격능력이 대상 국가들 중 가장 낮은 것을 의미하기보다는 사이버 공격에서 개인이 아닌 조직 차원으로 활동해 공격 행위자를 포착해 내기 어렵다는 것을 의미한다(지다겸, 2020). 또한 북한은 다른 국가들에 비해 사이버 방어와 사이버 의존도 점수가 높게 나타난다. 이는 북한이 폐쇄적 시스템을 통해 사이버 영역에 대한 방어에 치중한 결과로 해석할 수 있다.

유형 정체성과 위협인식뿐만 아니라 사이버 영역에서 북한의 역할 정체성과 기회인식도 상존하는데, 이는 김정은이 강조하는 '정보화를 통한 지식경제로의 전환'의 방편으로 과학기술 발전 사업을 적극적으로 추진함으로써 경제강국 건설을 목표로 하는 데에서 확인된다(로동신문 19/04/12). 다시 말해, 사이버 영역을 활용해 경제발전을 도모함으로써 궁극적으로 자신의 지위를 정상화하려는 것으로 해석이 가능하다. 이러한 기저에는 경제발전을 이루기 위한 기회의 장(場)으로 사이버 영역을 인식하는 보편성이 작동하는데, 앞서 살펴본 중국의 인식과도 유사하다. 최근 경제적 측면에 중점을 둔 북한의 사이버 활동(CrowdStrike,

12 해당 평가는 별도의 가중치 없는 각 요소별 점수의 총합으로, 연구자들의 국가별 평가 점수에 따른 것이다(Clarke and Knake, 2010: 73).

13 해당 요소는 국가의 중요한 인프라가 네트워크 시스템에 의존하는 정도를 의미하며, 점수가 높을수록 유선 연결이 적게 이뤄진, 즉 연결성이 약한 국가임을 뜻한다(Clarke and Knake, 2010: 72-74).

2020: 45-46)은 이러한 역할 정체성과 기회인식을 뒷받침한다.

2. 북한의 사이버 안보전략 전망

향후 북한 사이버 안보전략의 핵심은 역할 정체성과 기회인식에 달려 있다. 북한은 중국과 마찬가지로 기회인식에 따라 사이버 영역을 활용한 경제발전을 추구한다. 물론 1인 지배체제의 북한과 일당 지배체제의 중국의 역할 정체성과 기회인식은 동일하지 않다. 앞서 살펴보았듯이 중국은 고도화된 경제를 바탕으로 자국의 국제적 영향력을 확대하고자 하는 반면, 북한은 국제적 고립의 지속으로 경제발전을 통한 지위 정상화라는 당면과제를 해결하기 위한 수단으로 사이버 영역에 주목하기 때문이다. 크라우드스트라이크의 최근 연구에서 주목한 북한의 재정과 가상화폐 영역의 특화(CrowdStrike, 2020: 47)는 대북제재의 영향에 따른 것으로, 북한의 '지위의 기회 최대화' 맥락을 뒷받침하는 동시에 '디지털 경제'로의 전환을 모색하는 북한의 최근 행보를 고려할 때 향후 사이버 안보전략을 전망하는 데에도 중요한 준거가 된다.

북한은 김정은의 "전당적으로, 전국가적으로 과학기술을 중시하는 기풍을 철저히 세워야 한다."는 지시에 따라 "과학기술이 사회경제발전을 좌우하는 과학기술의 시대에서 과학기술중시를 국풍으로 확립하여 최단 기간 내에 나라의 과학기술을 세계적 수준으로 올려 세워야 할 무겁고도 영예로운 임무"이므로, "과학과 기술에 의거하여 정치와 경제, 군사와 문화의 모든 분야에서 세계를 압도할 것"임을 강조한다(리홍수, 2019). 또한 북한이 "과학기술중시를 국풍으로 확립하기 위해서는 근본적으로 수자(디지털)화가 수반되어야한다."라고 지속적으로 강조하는 점을 고려할 때, 디지털 중시가 곧 과학기술중시라는 인식을 확인할 수 있다. 나아가, 다양한 해외 사례를 여러 차례 언급함으로써 과학기술의 발전과 전략 전환이 국제적 추세임을 강조한다. 뿐만 아니라 이를 주제로 대내적인 '전국정보화성과전람회'를 개최하고, 관련 사항을 『로동신문』에서 지속적으로 보도하는 것은 정보기술 발전을 통해 디지털 경제를 국가적 차원으로 확대하려는 전략적 인식으로 보인다(강진규, 2019a).

이에 따라 북한은 중국의 정보화를 통한 경제발전 전략을 주목하고 있다(리

철혁, 2019). 이는 정보화가 경제발전을 이루는 데에 필수조건이며 경제발전이 곧 대내외의 변화로 이어진다는 인식에 의한 것이다. 북한은 정보화를 통한 경제발전 추구라는 기회인식을 바탕으로 국가전략을 '디지털 경제'로 전환해 지위의 정상화, 즉 역할 정체성을 강화하고자 하고 있다. 다시 말해, 권위주의 체제유지와 경제발전을 병행하는 빅데이터 역설(Big Data Paradox)로 북한은 정치적 생존과 경제적 번영을 이루고자 하는 것이다(김용호, 2018: 143-144). 나아가, 이는 사이버 안보에서도 유사한 방식으로 작용할 것이다. 본격적인 국가전략의 전환을 고려할 때, 기회인식에 따른 역할 정체성의 정상화로 향할 가능성이 크다.[14] 최근 강조되고 있는 경제발전을 위한 정보화가 사상 다음으로 중요하다는 인식이 이를 뒷받침한다. 즉 "경제사업에서 제기되는 모든 문제를 과학기술에 의거하여 풀어나가며 생산과 건설을 과학화하기 위하여 적극 노력"할 것을 강조한 김정은의 발언(장은경, 2019)은 정보화를 통해 경제발전을 가속화하겠다는 의지이며 궁극적으로 지위 정상화를 목표로 하는 것이다.

물론 이러한 인식과 더불어 유형 정체성과 위협인식 역시 작동할 것이다. 특히 기술적 측면에서 위협인식에 직결되는 불안정을 사전에 예방하고자 국가 주도의 명확한 통제를 병행할 것이다. 또한 현재 북한의 인터넷 정책과 유사한 모습으로 기본적인 정보통신 산업체계와 연결은 가능하나, 대중의 접근은 통제하는 기조가 유지될 것이다(차정미·박차오름, 2019: 298). 전자는 내부 인트라넷인 '광명망'을 통한 국가 주도의 정보화이며 후자 역시 이와 연계된 '붉은 별' 운영체제를 비롯한 인프라를 의미한다. 즉 체제유지를 전제한 경제발전의 병행이 사이버 안보전략에도 적용될 수 있는 것이다.

이를 종합해 보면, 향후 북한의 사이버 안보전략은 최고지도자 중심의 1인 지배체제라는 유형 정체성을 수호하고자 하는 인식과 경제발전을 통한 지위 정상화라는 역할 정체성을 강화하고자 하는 인식이 동시에 구현되는 방향으로 전개될 가능성이 높다. 중국과 비교할 때, 북한의 경우 고립과 대북제재의 지속이라

14 북한의 지위 정상화는 '지위의 기회 최대화'의 맥락에서 도출된 것으로, 사회주의 강국 혹은 과학기술 강국 등의 지향점과도 연계된다. 핵심은 북한이 기회인식을 바탕으로 자신의 역할 정체성을 회복·강화하고자 사이버 영역을 활용할 가능성이 크다는 것이다.

는 외부 환경에서 중국보다 높은 위협인식이 나타날 것으로 예상된다. 이러한 상황에서 북한은 지위 정상화의 수단으로서 사이버 활동을 지속 강화할 것으로 보이는데, 이 역시 중국보다 높은 기회인식에 따른 것이다. 물론 중국처럼 국제적 영향력 확대가 아닌 고립된 환경에서 지위를 정상화시키려는 것을 의미한다. 이러한 북한의 특수성을 전제로 거시적인 관점에서 '체제의 위협 최소화'와 '지위의 기회 최대화'라는 중국과의 유사성이 향후 북한의 사이버 안보전략에 좀 더 높은 수준으로 반영될 것으로 전망된다.

V. 결론

정체성과 인식은 구체적으로 유형 정체성과 위협인식에 따른 '체제의 위협 최소화'와 역할 정체성과 기회인식에 따른 '지위의 기회 최대화'로 나눠볼 수 있다. 이에 따라 본 연구는 사이버 안보전략에 당국의 정체성과 인식이 반영된다는 전제로 중국의 '안전전략'을 해석하고 북한에 적용했다. 연구 결과로서 중국은 '체제의 위협 최소화'와 '지위의 기회 최대화'라는 목적하에 사이버 안보전략을 구현하고 있다는 사실을 확인했고, 이를 북한에 적용해 봄으로써 향후 북한의 사이버 안보전략이 어떻게 구체화될 것인지를 전망해 보았다.

유형 정체성과 위협인식 측면에서 중국과 북한 간에는 '체제의 위협 최소화'를 추구하는 공통점이 존재하나, 최소화의 정도는 일당 지배체제인 중국보다 1인 지배체제를 유지하는 북한의 경우가 두드러질 것이다. 중국은 공산당 영도의 사회주의 체제라는 유형 정체성과 관련된 위협인식을 '안전전략'에서 구체화하고 있으며, 북한은 최고지도자 중심의 1인 지배체제라는 유형 정체성과 관련된 위협인식을 근간으로 사이버 안보전략을 구체화해 나갈 것으로 보인다. 역할 정체성과 기회인식의 측면에서도 두 국가 모두 '지위의 기회 최대화'를 추구하는 공통점을 보인다. 중국의 경우 '안전전략'에서 경제발전의 새로운 동력으로 사이버 공간을 인식하고 '중국몽'이라는 역할 정체성을 실현하고자 한다면, 최근 '사회주의 경제건설 총력 집중 노선'으로의 전환을 선언한 북한은 중국의 정보화에 따른 경제발전을 예의주시하면서도 대북제재라는 제한적인 상황에서 지

위 정상화를 위한 수단으로 사이버 활동을 강화할 것으로 예상된다.

특히 북한의 사이버 안보전략은 중국보다 높은 수준의 '체제의 위협 최소화'와 '지위의 기회 최대화'로 구현될 것이다. 다시 말해, 북한은 양자를 동시에 추구하겠지만 '사회주의 경제건설 총력 집중 노선'으로의 국가전략 전환을 선언한 김정은 체제에서는 후자에 무게를 둔 사이버 안보전략이 구체화될 것이다. 대북제재가 지속되고 있는 현 시점에서 개혁개방 없이 경제발전을 달성하려면 사이버 영역을 적극적으로 활용해야 하기 때문이다. 하노이 회담 이후 미국과 외교관계가 냉각됨에 따라 북한은 빠른 시일 내에 제재 완화가 어렵다고 판단할 것이고, 이와 관련해 향후 가상화폐 거래소에 대한 사이버 공격이 예상된다는 분석은 이를 방증하는 대목이다(CrowdStrike, 2020: 50). 이러한 맥락에서 북한은 사이버 영역을 통해 자신의 지위를 정상화하려는 역할 정체성과 기회인식을 발현시켜 나가고자 할 것이다. 이는 정체성과 인식을 중심으로 중국과 북한의 사례를 분석한 결과로서 구성주의적 관점에 따른 것이다. 서두에 언급했듯이 정체성과 인식이 주관성에 근거하기 때문에 명확한 인과관계를 보이기 어려운 것이 사실이다. 그럼에도 불구하고, '관념변수'에 주목한 본 연구는 중국의 사이버 안보에 관한 정체성과 인식을 연계해 두 가지 측면에서 고찰하고 이를 북한에 적용함으로써 향후 사이버 안보전략을 구체화했다는 점에서 그 의미를 찾을 수 있다.

투고일: 2019년 12월 15일 | 심사일: 2020년 6월 14일 | 게재확정일: 2020년 7월 27일

참고문헌

강진규. 2019a. "북한, 수자경제 국가 전략화 할 것인가." 『NK경제』(12월 2일). https://www.nkeconomy.com/news/articleView.html?idxno=2308(검색일: 2020. 4. 1).

_____. 2019b. "북한, 백신SW에 처음으로 랜섬웨어 방지 기능 탑재." 『NK경제』(12월 11일). https://www.nkeconomy.com/news/articleView.html?idxno=2359(검색일: 2020. 4. 1).

곽예지. 2019. ""中, 일대일로에 '디지털 실크로드' 구축"…美와 경쟁 치열해진다." 『아주경제』(10월 21일). https://www.ajunews.com/view/20191021105454694(검색

일: 2020. 5. 1).
국가안보실. 2019.『국가사이버안보전략』.
국기연. 2019. “[단독] 북한 사이버 공격 능력 러시아에 이어 세계 2위.”『세계일보』(2월 20일). https://www.segye.com/newsView/20190220000578(검색일: 2020. 5. 1).
김관옥. 2015. “미중 사이버패권경쟁의 이론적 접근.”『대한정치학회보』23집 2호, 231-255.
김광명. 2019. “《새로운 전선》으로 되고있는 싸이버공간.”『로동신문』(10월 12일). 6면.
김상규. 2019. “중국의 사이버 안보 정책 변화와 그 함의.”『현대중국연구』20권 4호, 41-67.
김상배. 2015. “사이버 안보의 복합지정학: 비대칭 전쟁의 국가전략과 과잉 안보담론의 경계.”『국제·지역연구』24권 3호, 1-40.
_____. 2017. “세계 주요국의 사이버 안보 전략: 비교 국가전략론의 시각.”『국제·지역연구』26권 3호, 67-108.
김용호. 2018. “김정은의 신외교와 독재자의 딜레마(Dictator’s Dilemma), 그리고 빅데이터 역설(Big Data Paradox).”『한국과 국제정치』34권 4호, 123-151.
김인수·KMARMA. 2015. “북한 사이버전 수행능력의 평가와 전망.”『통일정책연구』24권 1호, 117-148.
김진용. 2018. “시진핑 시기 중국의 사이버 안보 부상과 취약성.”『국방연구』61권 3호, 155-182.
김흥광. 2011. “특별기고: 북한의 정보전 전략과 그 수행방법.”『군사논단』67호, 263-284.
로동신문. 2018. “조선로동당 중앙위원회 제7기 제3차전원회의 진행 조선로동당 위원장 김정은동지께서 병진로선의 위대한 승리를 긍지높이 선언하시고 당의 새로운 전략적로선을 제시하시였다.”(4월 21일). 1면.
_____. 2019. “국가적투자를 효과적으로 리용하여 나라의 과학기술발전사업을 목적지향성있게 추진하겠다.”(4월 12일). 7면.
리철혁. 2019. “수자경제의 발전을 지향하는 국제사회.”『로동신문』(6월 24일). 6면.
리홍수. 2019. “과학기술중시를 국풍으로 확립해나가는것은 우리 혁명발전의 중요한 요구.” http://www.ryongnamsan.edu.kp/univ/ko/research/articles/c12706a7c6e8d6476c3d2b6ae0042a82(검색일: 2020. 4. 1).
리효진. 2019. “국가간 대결장으로 되여가는 싸이버공간.”『로동신문』(7월 16일). 6면.
목용재. 2017. “김정은 집권 이후 신설된 북 해킹조직 6개.”『자유아시아방송』(11월 22

일). https://www.rfa.org/korean/in_focus/ne-my-11222017102238.html(검색일: 2020. 3. 30).

문동희. 2019. "'만능의 보검' 北사이버 전사, 암호화폐부터 군사기밀까지 노린다." 『DAILY NK』(9월 16일). https://www.dailynk.com/만능의-보검-北사이버-전사-암호화폐부터-군사기밀(검색일: 2020. 3. 30).

부승찬. 2017. "약소국 북한의 생존전략: 원칙과 구현방식." 『국방연구』 60권 2호, 1-26.

서진영. 2006. 『21세기 중국 외교정책: '부강한 중국'과 한반도』. 폴리테이아.

오택성. 2019. "북한 사이버 공격 능력 세계 최상위…정예요원 7천명." 『VOA NEWS』(8월 16일). https://www.voakorea.com/korea/korea-politics/5043950(검색일: 2020. 5. 1).

윤민우. 2018. "사이버 공간의 특성과 사이버 테러리즘, 그리고 사이버 안보전략의 변화." 『가천법학』 11권 4호, 253-286.

이근욱. 2009. "자유주의 이론과 안보: 모순된 조합인가 새로운 가능성인가?" 『국제정치논총』 49집 5호, 33-53.

이동선. 2009. "21세기 국제안보와 관련한 현실주의 패러다임의 적실성." 『국제정치논총』 49집 5호, 55-80.

임종인·권유중·장규현·백승조. 2014. "북한의 사이버전력 현황과 한국의 국가적 대응전략." 『국방정책연구』 29권 4호, 9-45.

장노순·한인택. 2013. "사이버안보의 쟁점과 연구 경향." 『국제정치논총』 53집 3호, 579-618.

장은경. 2019. "필수적인 제2의 실력." 『로동신문』(12월 1일). 1면.

조윤영·정종필. 2016. "사이버안보(cybersecurity)를 위한 중국의 전략: 국내 정책 변화와 국제사회에서의 경쟁과 협력을 중심으로." 『21세기정치학회보』 26권 4호, 151-177.

조현석·이은미·김동욱. 2017. "중국의 사이버 안보전략 연구의 통합적 접근." 『한국위기관리논집』 13권 7호, 89-107.

조화순·김민제. 2016. "사이버공간의 안보화와 글로벌 거버넌스의 한계." 『정보사회와 미디어』 17권 2호, 77-98.

지다겸. 2020. "미, 북한 사이버 공격 기소·제재 6건…기술 정교함, 영향력 비해 미비." 『VOA NEWS』(4월 23일). https://www.voakorea.com/korea/korea-politics/us-dprk-hacking(검색일: 2020. 5. 1).

차정미. 2018. "중국 특색의 '사이버 안보'담론과 전략, 제도 분석." 『국가안보와 전략』 18

권 1호, 1-43.

_____. 2019. “미중 사이버 군사력 경쟁과 북한 사이버 위협의 부상: 한국 사이버안보에의 함의.”『통일연구』23권 1호, 43-93.

차정미·박차오름. 2019. “중국 ‘1개 중심 2개 기본점 원칙’의 인터넷 발전전략과 북한에의 적용.”『아세아연구』62권 3호, 277-311.

채재병. 2013. “안보환경의 변화와 사이버안보.”『정치·정보연구』16권 2호, 171-193.

최종건. 2009. “안보학과 구성주의: 인식론적 공헌도를 중심으로.”『국제정치논총』49집 5호, 81-100.

황지환. 2017. “북한의 사이버 안보 전략과 한반도: 비대칭적, 비전통적 갈등의 확산.”『동서연구』29권 1호, 139-159.

国家互联网信息办公室. 2016. “《国家网络空间安全战略》全文.” http://www.cac.gov.cn/2016-12/27/c_1120195926.htm(검색일: 2020. 3. 27).

_____. 2019a. “习近平“4·19”讲话三周年: 牢牢抓住重要历史机遇.” http://www.cac.gov.cn/2019-04/19/c_1124389264.htm(검색일: 2020. 3. 30).

_____. 2019b. “工业和信息化部公开征求对《关于促进网络安全产业发展的指导意见(征求意见稿)》的意见.” http://www.cac.gov.cn/2019-09/27/c_1571114011459248.htm(검색일: 2020. 5. 5).

_____. 2019c. “国家互联网信息办公室关于《网络安全威胁信息发布管理办法(征求意见稿)》公开征求意见的通知.” http://www.cac.gov.cn/2019-11/20/c_1575785387932969.htm(검색일: 2020. 5. 5).

_____. 2019d. “国家互联网信息办公室有关负责人就《网络安全威胁信息发布管理办法(征求意见稿)》答记者问.” http://www.cac.gov.cn/2019-11/20/c_1575785388360559.htm(검색일: 2020. 5. 5).

新华网. 2014. “习近平: 把我国从网络大国建设成为网络强国.”(2月27日). http://www.xinhuanet.com/politics/2014-02/27/c_119538788.htm(검색일: 2020. 3. 27).

Akdag, Yavuz. 2019. “The Likelihood of Cyberwar between the United States and China: A Neorealism and Power Transition Theory Perspective.” *Journal of Chinese Political Science* 24(2), 225-247.

Austin, Greg. 2016. “Middle Powers and Cyber-Enabled Warfare: The Imperative of Collective Security.” The 18th IDSA Asian Security Conference. New Delhi. February.

Bloom, William. 1993. *Personal Identity, National Identity and International*

Relations. Cambridge: Cambridge University Press.

Burton, Joe. 2015. "NATO's Cyber Defence: Strategic Challenges and Institutional Adaptation." *Defence Studies* 15(4), 297-319.

Carr, Madeline. 2016. "Crossed Wires: International Cooperation on Cyber Security." *Interstate-Journal of International Affairs* 2015/2016(2), 2-13.

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

Ciolan, Ionela Maria. 2014. "Defining Cybersecurity as The Security Issue of The Twenty First Century: A Constructivist Approach." *Revista de Administratie Publica si Politici Sociale* 12(1), 120-136.

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

CrowdStrike. 2020. *2020 GLOBAL THREAT REPORT*. https://www.crowdstrike.com/resources/reports/2020-crowdstrike-global-threat-report(검색일: 2020. 5. 5).

Encyclopædia Britannica. 2016. "Ransomware." https://www.britannica.com/topic/Ransomware-2078176(검색일: 2020. 4. 5).

Eriksson, Johan and Giampiero Giacomello, eds. 2007. *International Relations and Security in the Digital Age*. Abingdon: Routledge.

Eriksson, Johan and Giampiero Giacomello. 2014. "International Relations, Cybersecurity, and Content Analysis: A Constructivist Approach." In Maximilian Mayer, Mariana Carpes, and Ruth Knoblich, eds. *The Global Politics of Science and Technology Vol. 2: Perspectives, Cases and Methods*. Berlin, Heidelberg: Springer.

Geddes, Barbara, Joseph Wright, and Erica Frantz. 2018. *How Dictatorships Work: Power, Personalization, and Collapse*. Cambridge: Cambridge University Press.

Hjortdal, Magnus. 2011. "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence." *Journal of Strategic Security* 4(2), 1-24.

Katzenstein, Peter J., ed. 1996. *The Culture of National Security: Norms and Identity in World Politics*. New York: Columbia University Press.

Kiggins, Ryan. 2012. "US identity, Security, and Governance of the Internet." In Sean S. Costigan and Jake Perry, eds. *Cyberspaces and Global Affairs*. Farnham:

Ashgate.

Kim, Yongho. 2011. *North Korean Foreign Policy: Security Dilemma and Succession*. Lanham, Maryland: Lexington Books.

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

Nathan, Andrew J. and Andrew Scobell. 2015. *China's Search for Security*. Chichester, New York: Columbia University Press.

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

Simons, Hans. 2014. "Consensual Hallucinations: The Politics of Identity in Dutch Cyber Security Policy." M.A. Diss., Radboud University Nijmegen.

Swaine, Michael D. 2013. "Chinese Views on Cybersecurity in Foreign Relations." *China Leadership Monitor* 42, 1-27.

The White House. 2018. *National Cyber Strategy*. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf(검색일: 2020. 4. 2).

Wendt, Alexander. 1999. *Social Theory of International Politics*. Cambridge: Cambridge University Press.

Wu, Xu. 2007. *Chinese Cyber Nationalism: Evolution, Characteristics, and Implications*. Lanham, Maryland: Lexington Books.

아시아리뷰 제10권 제1호(통권 19호), 2020

Abstract

China's Cyber Security Strategy and Its Application to North Korea: Identity and Perception

Chaorum Park Yonsei University
Seungchan Boo Yonsei University

This research aims to analyze China's cyber security strategy based on identity and perception, and apply it to North Korea to predict how the North Korea's cyber security strategy will take shape in the future.

Specifically, China's cyber security strategy can be classified into "minimization of regime threat," founded on type identity and threat perception and "maximization of opportunity for status," rested on role identity and opportunity perception. Underlying this, we suggested the direction of North Korea's cyber security strategy.

The analysis shows that both China and North Korea seek "minimization of regime threat," but China is shaping its cyber security strategy predicated on the threat perception related to type identity of the Communist Party's socialist regime, while North Korea is expected to shape its cyber security strategy based on type identity centered on their personal leader.

In terms of role identity and opportunity perception, both sides seek "maximization of opportunity for status," but China recognizes cyberspace as a new drive of economic development that could realize its role identity as the "China dream." On the other hand, North Korea, which recently announced its shift to "all-out focus on socialist economic construction," is expected to strengthen its cyber activities as a means to normalize its status under the limited circumstances of sanctions while keeping a close eye on

China's economic development following its informatization.

Keywords | China, North Korea, Cyber Security Strategy, Identity, Perception