국제정치이론적 접근을 통한 한일 사이버 외교안보 협력방안 연구

최은아*

<목차>

요지

본 연구는 국제정치이론인 신현실주의(Neo-Realism)와 신자유주의(Neo-Liberalism), 구성주의(Constructivism) 이론적 논의를 통해 한일 양국의 외교·안보 전략에 관한 접근법을 제시하여 공통으로 직면하고 있는 사이버 안보위협 이슈와 그에 대한 대응 및 협력 프로세스를 해설하고자 하였다. 이론적 시각을 바탕으로 한일 사이버안보 협력방안을 도출함으로써 이를 통해 한일관계 발전에 기여하는 것에 연구 목적이 있다. 국제사회에서 사이버안보위협이 증가함에 따라 사이버공간에서도 서방 대 비(非)서방 진영의 대결 구도가 가열되고 있다. 서방 국가들은 동맹국과 우호국, 국제기구 등을 활용하여 사이버위협에 적극 대처하고 국제협력을 추진 중이다. 한국과 일본은 북한의 핵·미사일 위협 외에도 사이버 피해 사례를 공유할 수 있는 부분이 있다. 양국은 사이버 안보위협 이슈를 공유하고 능동적 협력을 통해 전략적 파트너십을 발휘해야 한다. 미국 주도의 인도-태평양 전략(Indo-Pacific Strategy)에 따라 일본, 호주, 인도 등 인태지역 주요 국가들이 안보연대를 구축하고 있는 상황에서, 한일 사이버 외교안보 협력은 글로벌 패권경쟁에서 두각을 보이고 향후 한미일 3국의 전략적 협력 강화에도 기여될 수 있을 것이다. 따라서 사이버 양자·다자협력을 추진하면서 위협억제, 전략적 가치 향상, 한일관계 개선을 두루 꾀해야 할 것이다.

주제어: 국가안보, 사이버 외교안보, 한일협력, 사이버 위협, 국제정치이론

* 성균관대학교 일반대학원 정치외교학전공 박사수료.
성균관대학교 글로벌미래전략연구소 연구원.

1. 서론

본 연구는 국제정치이론인 신현실주의(Neo-Realism)와 신자유주의(Neo-Liberalism), 구성주의(Constructivism) 이론적 논의를 통해 한국과 일본의 외교·안보 전략에 관한 접근법을 제시하여, 양국이 공통으로 직면하고 있는 사이버 안보위협 이슈와 그에 대한 대응 및 협력이 어떻게 이루어지고 있는지를 풀어가고자 하였다. 그리고 이론적 시각을 반영하여 한일 사이버안보 협력방안을 도출함으로써 이를 통해 한일관계 개선과 발전에 기여하는 데 연구 목적이 있다.

국가안보전략의 가장 기초는 국가가 처한 대내외적 위협을 파악하는 것이다. 신현실주의, 신자유주의 이론은 국제정치에서 힘(power)의 균형에 따라 나타나는 국가별 대내외적 위협과 의도, 전략과 대응방식을 해설하는 데에 적합하다. 특히 종국에는 위협을 공유하고 있는 한국과 일본이 공동으로 대응 및 협력하도록 방향성을 제시한다는 점에서 한일관계를 풀어가는 해법을 도출할 수 있다. 구성주의 이론적 시각에서도 한일 국민 간 과거사 갈등으로 인해 부정적인 상호인식과 협력이 제한되는 문제를 해결하기 위해서 지속적인 교류와 협력을 통해 미래지향적 정체성을 형성해야 한다는 방향성을 제시할 수 있다.

지금까지 한일 안보협력은 제한적으로 그리고 미국이 중재하는 구도로 이루어져 왔다. 1965년 수교 이후 한일관계는 강제징용 문제, 위안부 문제, 독도 분쟁 등 과거사 현안을 두고 정부별 입장 차를 나타내며 대립과 갈등이 누적돼왔다. 따라서 경제·사회 분야의 협력은 가능할지라도 민감한 안보적 차원의 협력 체제를 구축하기 어려운 상황이 지속되어 온 것이다. 그러나 나날이 심각해지는 북한의 핵무기 개발, 미사일 위협에 한일 양국은 공동대응의 필요성을 인식하게 되었다. 이에 이명박 정부에서 대북 핵·미사일 정보 공유가 가능한 최초의 군사협정인 한일 군사정보보호협정(韓日秘密軍事情報保護協定, GSOMIA)을 추진하였고, 이후 2016년 박근혜 정부에서 동 협정이 체결되었다. GSOMIA는 한일 양국이 자국 안보위협을 해소하기 위한 상호 필연적 의지를 확인함과 동시에 한일관계 개선에도 일정 기여되었다고 평가된다. 그러나 이러한 군사협력의 물꼬는 지난 문재인 정부에서 강제징용 대법원판결 문제와 맞물려 수출 통제, GSOMIA 파기 논란으로 이어지며 다시 수면 아래로 가라앉았다.

국제환경의 패러다임이 급변하고 신(新)아시아 안보 질서가 세워지는 상황에서 한일 양국이 이제는 고정적인 구도를 탈피해야 할 것으로 보인다. 한일 간 안보 분야에서의 신뢰는 지난 2018년 '레이더 조사(照射)-초계기 저공비행' 갈등 이후 좀처럼 회복되지 못하고 있다.[1] 한국은 일본과의 관계에서 과거사 문제

에 발목 잡히지 않고 안보를 따로 논의하는 일명 투트랙 전략을 해법으로 삼아 왔다. 미중 갈등이 고조된 현재 한국이 대외적 위협에 선제적으로 대응하고 글로벌 패권경쟁 구도에 유리한 지위를 선점하기 위해서는 일본과의 안보협력이 불가피하다. 특히 몇 년간 경색되었던 한일관계가 2022년 윤석열 정부 출범 이래로 일본 정부와의 외교·안보 협력에 열린 자세를 취하는 가운데 양국 관계개선 가능성의 기회를 열어가고 있다. 2022년 4월 한일정책협의 대표단이 일본에 파견되어 기시다 후미오 일본 총리를 비롯한 50여 명의 정계, 경제계, 학계, 언론계 주요 인사들과 공식 면담 일정을 소화하였고, 한일관계 개선의 의지와 당위에 대한 공감대를 형성하면서 개선을 위해 무엇보다 인적교류 확대가 중요하다는데 인식을 같이했다.[2] 이러한 흐름을 이어가면서 양국은 유의미한 안보협력의 기회를 엿볼 수 있을 것이다.

양국이 공통 안보위협 이슈를 인식하고 기민하게 대처하는 등 전략적 파트너십을 발휘하는데 효과적인 의제 중 하나가 사이버안보 분야이다. 국제사회에서 사이버안보위협이 증가함에 따라 사이버공간에서도 서방 대 비(非)서방 진영의 대결 구도가 가열되고 있다. 이 가운데, 한국과 일본은 북한의 핵·미사일 위협 외에도 사이버 위협과 피해 사례를 공유할 수 있는 부분이 있다. 사이버안보 대응 차원에서 서방 국가들은 동맹국과 우호국, 국제기구 등을 활용하여 위협에 적극적으로 대처하고 안보협력을 추진 중이다. 여기서 한일 양국이 사이버 위협에 대처하고 선제적으로 대응하면서 국제협력 중심으로 제도적 협력을 우선하고 있는 현상은 국제정치이론을 적용하여 유용한 해설을 도출할 수 있다.

2장에서는 한일협력, 사이버 안보협력 등에 관한 선행연구들을 검토하고, 분석의 틀을 제시하여 국제정치이론적 논의를 통해 한국과 일본의 외교·안보 전략에 관한 접근법을 구체적으로 살펴본다. 3장에서는 한일 사이버 외교·안보 협력 방안을 1) 위협 증가에 따른 선제적 대응, 2) 가치·규범 및 국제협력을 활용한 사이버 외교, 3) 미래지향적 정체성 형성을 위한 사이버 교류와 협력 세 가지 방면에서 제시한다. 마지막 장에서는 결론을 통해 연구 내용 요약과 연구가 지니는 의의와 한계를 정리한다.

---

1) 최은미, “기시다-바이든 미일정상회담 이후 일본의 대외전략과 한일관계에의 함의,”『이슈브리프』 2022-19, p. 9.

2) 박미영·권지원, “한일정책협의단 “한일관계 개선 ‘선택 아닌 당위’ 공감대”,” 『뉴시스』 2022.04.28. https://newsis.com/view/?id=NISX20220428_0001852599(검색일: 2022.07.14.)

2. 국제정치이론적 논의

2.1 선행연구 검토

한일 안보협력 연구는 군사협력과 한일 간 동맹 가능성 주제로 주요 논의가 진행되어왔다. 연구자들은 역사문제 등으로 인한 한일관계 진전의 한계에도 불구하고 협력의 가능성을 크게 평가하고 있는데, 그 동기로 북핵위협과 중국의 패권적 부상을 꼽았다. 다만, 동맹 형성으로 인한 이익보다 위험이 클 경우 동맹이 체결되지 않을 가능성을 염두해 동맹이 아닌 전략적으로 공조해야 한다는 입장이며, 이에 한미일 삼각 안보협력체제 형성의 필요성을 제기하는 연구들이 다수 있었다.[3)]

한미동맹을 매개로 한 한일관계 형성을 살펴본 남창희(2009)는 일본의 안보 역할의 확대가 한국에게 위협이 되지 않을 것이며 한미일 삼각 안보협력체제의 틀 내에서 한일 간 군사협력이 가능하다고 보았다. 박휘락(2018)은 한국과 일본 간의 안보협력이 제대로 추진되지 않는 원인을 구심요소와 원심요소로 구분하여 전자는 공통위협, 상호이익, 신뢰성을, 후자는 국제정치와 국민 여론을 선정하여 분석하였다. 원심요소 중에서 국제정치는 구심요소로도 이어질 수 있는 양방향적 요소로 해석되었으며, 국민 여론 요소의 경우 과거사와 독도 문제 작용 등은 향후 북핵위협이 증대되는 상황에서 정부가 적극적으로 필요성을 설득해나갈 경우 약화 될 것이라고 평가하였다.

일본의 안보전략과 정책 연구는 국제관계에 따라 일본의 대외 위협 인식이 어떻게 변화해 왔는지 분석하는 데 초점을 두고 있다.[4)] 구조현실주의(신현실주의)와 자유주의 이론을 조합해 일본의 위협 인식 변화와 대응방식을 설명한 노리 카타기리(Nori Katagiri)는 일본의 중국으로부터의 위협 인식이 커지고 있으며 특히 중국의 군사 현대화와 사이버 공격은 심각한 국가안보 위협이라고 지적하였다.[5)]

사이버 분야에서도 안보환경과 위협 인식 변화에 따른 일본의 사이버안보 전략

---

3) Taehyo Kim and Brad Glosserman ed, *The Future of U.S.-Korea-Japan Relations: Balancing Values and Interests* (Washington D.C.: Center for Strategic and International Studies. 2004); 남창희, "한미동맹과 미일동맹의 동조화와 한일안보협력," 『한일군사문화연구』 Vol.8 (2009); 박휘락, "북핵 고도화 시대 한일 안보협력 - 실태 그리고 구심요소와 원심요소 -," 『한일군사문화연구』 25권 0호 (2018); 박철희, "한일 갈등의 심화와 한일안보협력의 미래," 『한국국가전략』 4권 2호 (2019).

4) 권태환, "최근 일본의 안보정책 변화와 향후 전망: 미중 대립과 북한 비핵화를 중심으로," 『한국국가전략』 3(3), 8 (2018); 최해옥, "글로벌 기술패권에 대응하는 일본의 전략 및 시사점," 『STEPI Insight』 2021-10.

5) Nori Katagiri, "Between Structural Realism and Liberalism Japan's Threat Perception and Response," *International Studies Perspectives*, 19 (2018).

과 정책을 분석하는 연구가 꾸준히 진행되고 있다.[6] 이승주(2017)는 군사안보와 사이버안보의 연계 관점에서 일본의 사이버 안보전략을 분석하였으며, 박성호(2022)는 전통적 안보 기조인 양자주의와 비전통 안보 기조인 다자주의 측면에서 일본의 사이버안보 전략을 고찰하였다. 그러나 전통안보 관점에서 위협 주체와 공격 유형을 구체화하고 그에 따른 협력 유인을 제시한 것에 비해, 양국이 설정 가능한 사이버 위협의 주체와 공통되는 사이버 공격 유형에는 어떤 것이 있는지에 관한 세부 논의는 부족한 것으로 보인다.

정리하면, 기존 선행연구들은 전통안보와 군사안보 영역에서 한일관계를 진단하고 개선방안을 도출해왔다면, 최근 시도되는 논의들은 신안보 영역을 포괄 의제 범위에 두고 전략과 정책 내용을 분석하는 방식으로 진행되고 있다. 한일협력을 저해하는 역사문제, 과거사 갈등 등으로 비롯된 양국의 부정적 국민여론과 감정은 쉽게 해결될 수 없는 장기적 요인으로 다뤄지고 있으며, 정부의 '투트랙' 전략을 통해 이러한 요인과 외교·안보를 분리, 대응해야 한다는 주장이 대체적이었다. 한편, 신안보 영역에서 한일협력 프로세스를 다룬 연구가 미진한 상황에서, 북한과 중국 등의 사이버 위협 빈도가 증가하고 있으며 정교한 사이버 공격으로 인해 국가적 피해가 큰 내용을 반영하여 실질적인 협력의 필요성을 도출할 수 있을 것으로 보인다.

2.2 분석의 틀

한일 사이버 외교·안보 협력이 어떤 조건에서 가능할 것인지를 살펴보기 위해 다음 분석의 틀을 설정하였다. 먼저, 신현실주의에서는 협력 요인을 권력, 이익, 위협(인식)으로 설정하였다. 다음으로, 신자유주의에서는 가치, 제도, 경제를 협력 요인으로 설정하였고, 마지막으로, 구성주의에서는 규범, 정체성을 협력 요인으로 설정해 세 이론의 가정들이 어떻게 한일협력의 구체화를 이루는지 대응 및 협력 프로세스를 살펴보았다.

---

6) 민경식, "초연결 사회를 대비한 일본의 사이버보안 정책 동향," 『주간기술동향』 2016.4.13. (2016); 이승주, "일본 사이버안보 전략의 변화 : 사이버 안보의 전통 안보화와 전통 안보의 사이버 안보화," 『국가안보와 전략』 17(1), 65(2017); 이상현, "사이버 위협에 대한 일본의 대응: 사이버 외교와 사이버 방위," 『국가전략』 25(2), 88(2019); 이상현, "일본의 사이버안보 수행체계와 전략," 『국가안보와 전략』 19(1), 73(2019); 박성호, "일본의 사이버 안보전략 - 양자주의의 강화인가 다자주의로의 전환인가 -," 『일본학』 제56집(2022.4).

<표1> 국제정치이론적 접근을 위한 분석틀

국제정치이론	외교·안보 협력 요인	가정
신현실주의	- 권력 - 이익 - 위협(인식)	국가는 안보를 위해 위협적인 국가에 대항하며, 그 수단으로 동맹 또는 연합을 형성하여 세력균형을 유지한다.
신자유주의	- 가치 - 제도 - 경제	자유주의적 국제제도와 민주주의 가치, 규범을 확산하는 외교수단을 통해 평화와 번영이 극대화될 수 있다.
구성주의	- 규범 - 정체성	국가 간 교류와 협력을 통해 간주관성이 형성되고, 국가 정체성이 변화하면서 평화를 유지할 수 있다.

출처: 국제정치이론의 대표 변수와 가정을 선택하여 저자가 정리, 작성.

2.3 국제정치이론적 접근

아시아-태평양 지역은 미국, 러시아, 중국이라는 굵직한 군사대국의 이해가 집중되어 있다. 다만, 국제테러조직의 주요 공격 거점인 유럽과 중동지역 국가들에 비하면 국제테러 위협은 상대적으로 덜하다. 이에 한반도 역내를 둘러싸고 한국과 일본은 러시아, 중국, 북한에 대한 대외적 위협을 공유하고 있다. 국제정치학의 큰 패러다임인 현실주의 이론은 개별 국가 상위에 어떠한 중앙권위체도 없는 국제체제의 구조적 무정부 상태에서 나타나는 국제정치의 변화를 설명한다. 국제정치에서 국가행위자가 추구하는 최종 가치는 생존이다. 신현실주의에 따르면 국가는 자신의 안전을 궁극적 가치로 여기기 때문에, 모든 국가는 '안보(security)'를 극대화하기 위해 노력한다. 그리고 이를 달성하기 위한 수단으로서 '권력(power)'을 추구한다. 강대국들이 안보경쟁을 벌이는 가운데 한국과 일본은 역내 지정학적 갈등이 국가 생존에 직간접적으로 영향을 미치게 되므로 자국의 안전보장 문제에 민감할 수밖에 없다.

일본의 대외적 위협 우선순위와 그 대응은 미소 냉전을 전후하여 힘의 균형이 변화함에 따라 달라져 왔다. 신현실주의자 케네스 월츠(Kenneth N. Waltz)는 국가 행동을 '상대적 힘의 배분(distribution of relative power)'이라는 독립변수로 분석한다. 한 국가의 힘이 증가하는 경우에 주변 국가들은 세력균형(balance of power)을 유지하기 위해 부상하는 국가에 대항한다.[7] 1990년대 냉전 종식과 함께 소련 해체로 위협이 약화되면서 일본은 러시아를 상대로 이전보다 국방비를

7) 이근욱, 『왈츠 이후 국제정치이론의 변화와 발전』(파주:한울 아카데미, 2009), p. 39.

덜 지출할 수 있었다.[8] 하지만 2000년대부터 중국이 세계 2위 경제대국으로 급부상하며 국제무대에서 정치·경제적 영향력을 확대해가자, 러시아와 북한보다도 중국을 아태 지역에서 힘의 불균형을 초래할 큰 위협으로 인식하게 되었다.

중국과 장기간 센카쿠/댜오위다오(Senkaku/Diaoyu) 영토분쟁으로 대립이 격화되어 온 일본은 대(對)중국 견제전략을 세우고 동북아 지역안보 대결 구도를 조직화하는 방향으로 안보전략을 수립하게 되었다. 그러나 일본이 자체적으로 내부 군사력을 강화하기보다 미국의 핵우산과 동맹국의 신뢰 구축으로 조용히 억지력을 높이며, 동시에 중국과 경제·무역 협력을 유지해온 점은 자유주의 시각에서 설명이 유용할 수 있다. 신현실주의는 모든 국가가 위협과 분쟁을 중심으로 협력하기 어려우며 협력하더라도 배반의 가능성이 있음을 주장하지만, 신자유주의는 복합 상호의존성에 따라 협력의 지속이 가능하다고 본다. 나이(Joseph Nye)와 함께 국가 간 상호의존의 중요성을 강조했던 로버트 코헤인(Robert O. Keohane)은 현실주의자들과 달리, 무정부 상태에서도 국제레짐 또는 국제제도를 통해서 국가들이 협력을 도출해낼 수 있다고 주장하였다. 복합 상호의존의 핵심적 특징은 국가 간 무력의 사용이나 위협의 비효율성에 대한 근거있는 기대들이다. 이러한 기대는 무력사용의 위협을 비합법화시키는 관례나 레짐에 대한 지지를 창출하는 데 도움을 준다.[9]

일본은 동아시아 지역 내 평화와 번영을 위한 기회를 늘리기 위해 민주주의, 경제적 상호의존성, 국제기구 참여 등 다양한 수단을 동원해왔다. 대립과 갈등이 지속해온 역사, 외교·안보 이슈를 뒤로하고 한중일 3국 간 경제교류를 통해 무역·투자 협력을 증진해온 것 역시 불안정한 경제적 상호의존성을 해결해가면서 외교적 의존도를 높여 역내 평화를 유지하려는 기조로 볼 수 있다. 제도와 규범을 통한 협력과 이를 통한 국제레짐 형성, 궁극적인 평화 달성이 가능하다고 보는 신자유주의 패러다임에서 특히 한일협력의 필요성이 강조된다. 신자유주의 입장에서 국제사회에 형성된 서방 대 비서방 국가 간 대립은 권위주의 대 민주주의 체제의 상이성에 따라 나타나는 진영 대결 구도이다. 일본은 반전(反戰)과 평화에 대한 대외적 이미지를 강조하면서 국제사회에서 규범과 법치를 중심으로 한 리더십을 보여주고 있다. 미일동맹과 한미동맹은 민주주의, 법치주의 가치와 규범 확산을 토대로 한 국제사회의 평화와 번영 추구라는 각 정부의 뚜렷한 방향성을 제시하고 있다. 신자유주의는 한일 양국 간 공유하는 자유민주 헌법과 인권, 시장경제 제도와 가치를

8) Nori Katagiri(2018), *op. cit.*, p. 327.

9) Robert O. Keohane, "Neoliberal Institutionalism: A Perspective on World Politics," *International Institutions and State Power: Essays in International Relations Theory*, Boulder: Westview Press, 1989, ch.1(김우상 옮김), p. 245.

기반으로 협력과 신뢰가 축적될 수 있다고 기대한다.

신현실주의는 무정부적 질서(anarchic order)에 놓인 국가들이 외부의 위협에 대해 자구책(self-help)과 동맹의 조력(助力)을 총동원할 것을 주문한다.[10] 북한은 1990년대부터 핵무기 개발 시도와 탄도미사일 시험 발사, 괴선박 침투 등 도발 행위로 한반도 역내 긴장을 고조시키며 안보 위협요인을 증대시켜 왔다. 북한은 2022년에만 대륙간탄도미사일(ICBM) 8차례를 포함해 63차례나 탄도미사일을 발사했다.[11] 이에 한국과 일본은 미국과의 삼각구도 협력으로 북한 안보위협을 크게 평가하고 대응해왔다. 최근 두 차례 한미일 외교장관회담을 열고 공동성명을 발표(2022.05.28., 2022.09.22.)하여 북한의 탄도미사일, ICBM 도발을 규탄하고 북한의 비핵화 목표를 진전해가는 것의 중요성을 강조하였으며, 2016년 이래 6년 만에 성사된 한일 양국 국방차관 대면회의(2022.09.07.)를 통해 안보협력 강화를 위한 현안들을 논의하였다. 2022년 11월 13일 열린 캄보디아 프놈펜 한미일 정상회담에서는 '북한 미사일 경보 정보를 실시간으로 공유'하는 내용을 골자로 한 합의를 첫 3국 공동성명으로 채택하였다.[12]

적극적 다자주의 정책을 펼쳐온 중국은 2010년대부터 대국관계, 강군전략, 해양강국화로 요약되는 안보정책을 펴며 중국의 꿈 실현 목표를 드러냈다. 한일 양국은 중국의 공격적 부상에 따라 미국과의 양자 동맹을 바탕으로 군사·외교·안보·경제 분야에서 중국과 경쟁하고 있다. 일본은 미일동맹을 강화하고 군사협력을 필리핀, 인도, 호주로 넓히며 대(對)중국 동맹 전선을 구축해가고 있다. 부상하는 중국을 자국에 공격 의도가 있는 위협으로 인식한 주변 국가들이 적극적으로 동맹을 결성하는 양상은 스티븐 월트(Stephen M. Walt)가 동맹 형성에 있어서 경성권력(power) 만이 아닌 위협(threat)의 인식도 작용한다는 위협균형론(balance of threat)[13]의 이론적 근거가 된다.

신현실주의에서 세력균형론은 적대적 경쟁세력 간에 힘의 균형이 이루어져 있으면

---

10) 김태효, "신아시아 안보질서 2030: 패러다임 변화와 한국의 과제," 『신아세아』 26권 3호 (2019년, 가을), p. 67.

11) 신나리·신규진, "北미사일 발사 포착은 한국, 낙하땐 日… 실시간 공조 첫발," 『동아일보』 2022.11.26. https://www.donga.com/news/Politics/article/all/20221126/116695549/1(검색일: 2022.12.01).

12) 안석, "한미일 "北미사일 경보 실시간 공유"… 한일 지소미아 정상화한다," 『서울신문』 2022.11.14. https://www.seoul.co.kr/news/newsView.php?id=20221114003019 (검색일: 2022.11.22).

13) 월트는 위협을 판단하는 네 가지 요소로 총체적 국력, 지리적 인접성, 공격 능력, 공격 의도를 제시하였다. Stephen M. Walt, "Why Alliances Endure or Collapse," *Survival*, Vol. 39, No. 1 (Spring 1997), p. 158.

안정적으로 평화가 지속될 수 있다고 하였다. 여기서 힘의 균형을 어떻게 보느냐에 대해서는 현상유지적으로 안보를 극대화하는 방어적 현실주의와 현상타파적으로 안보를 극대화하는 공세적 현실주의로 구분될 수 있다. 현재 미국은 중국에 비해 상대적으로 큰 힘을 지키기 위해 쿼드(Quad), 오커스(AUKUS), 인도-태평양 경제 프레임워크(IPEF) 등을 이끌며 글로벌 동맹 네트워크를 재건하고 있다. 미국 입장에서는 자신이 상대적인 힘의 우위를 확보하고 유지하는 것을 균형이라고 보는 것이다. 이러한 흐름에서 미국과 일본의 협력이 전통안보 영역에서 비전통안보 영역으로 확대되는 기조 역시 미일동맹 강화를 통해 위협에 선제적으로 대응하고 자국 역량을 키워 안보를 극대화하는 행위로 설명된다.

미국, 유럽, 인도, 아세안 국가들은 국가별 인도-태평양 전략을 발표하며 인도-태평양 지역의 주요 의제인 번영과 안보를 구체화하고 있다. 일본은 2016년 케냐에서 열린 제6회 아프리카개발회의 기조연설을 통해 '자유롭고 열린 인도태평양(Free and Open Indo-Pacific, FOIP)'을 기치로 한 인도-태평양 전략 구상을 가장 먼저 발표하여 미국과 함께 인태전략을 주도하고 있다. 인태전략의 핵심은 공급망, 해양안보, 민주주의 및 인권이다. 중국을 배제한 글로벌 공급망 구축과 인도-태평양 지역에서의 군사적 우위 및 억지력 강화, 중국 견제를 위한 민주주의 연대, 인권과 노동 가치 중시, 투명하고 건전한 거버넌스 지원 등을 구체적인 내용으로 한다. 일본은 강력한 미일동맹과 FOIP 네트워크를 통해 안보를 강화하고 있으며, 동남아 지역 개발협력으로 역내 리더십 확대를 도모하고 있다. 이는 신자유주의 입장에서 자유시장과 개방성, 투명성을 기반으로 한 제도적 협력 장치를 통해서 민주주의 가치와 이념의 연대를 구축하는 것이라고 볼 수 있다.

한국 역시 미국 주도의 인태전략 중심으로 기존의 군사동맹을 경제·기술·공급망 동맹으로 확장하여 역내 영향력을 높여가고 있다. 문재인 정부까지는 직접 인태전략을 수립하는 대신 아세안·인도와 협력 강화 등에 초점을 둔 신남방정책을 추진하였으나, 윤석열 정부에서 2022년 5월 21일 한미 정상 공동성명을 통해 인도-태평양 전략 프레임워크를 수립한다고 발표하였다.[14] 인태지역 중심으로 전개되는 삼각협력, 소다자 협력 형태의 주요국 협력 가운데, 한국은 역내 우호 국가 이미지를 가지고 기술경쟁력이 높은 핵심 파트너로서 역할을 하고 있다.

일본과 한국은 글로벌 기술패권에 대응하기 위해 자유민주주의, 시장경제, 법과 제도 기반의 질서 등 가치 중심으로 협력을 강화할 수 있다. 디지털 부문은 국가

14) 대통령실, "[전문] 한·미 정상 공동성명," 『대한민국 정책브리핑』 2022.05.21. https://www.korea.kr/news/policyNewsView.do?newsId=148901846(검색일: 2022.06.14).

간 데이터 흐름 촉진, 첨단 ICT 기술 투자·공유, 사이버보안 인프라 구축, 민·관·군 사이버 기술협력 등을 내용으로 하여 민감하지 않은 수준에서 주요 협력의제로 강조되고 있다. 이미 일본은 글로벌 기술패권에 민감하게 반응하여 정부차원의 빠른 대응전략을 제시하였으며, '디지털청'을 설립함으로서 정부주도의 디지털화를 추진하고 있다.[15] 한미, 미일 간 협력 강화를 추진하는 분야가 미중 경쟁 분야와 겹치는 부분이 있어 향후에도 미중 대립이 격화하는 가운데 한미일 3국은 동맹 및 우호협력 관계를 전략적으로 강화하는 방향으로 협력을 이루어갈 것으로 보인다.

한편, 구성주의 이론에 의하면 국가 간 교류와 협력이 이루어지는 가운데 간주관성이 형성되고, 이를 통해 상호 연관성을 바탕으로 국가 정체성이 변화하며 평화를 유지할 수 있다.[16] 한일관계는 2019년 무역갈등과 지소미아 논란으로 급격히 나빠졌으나, 양국 국민의 상호인식은 2021년부터 꾸준히 개선되고 있다. 동아시아연구원(EAI)과 겐론NPO가 실시한 '제9회 한일 국민 상호인식조사'에서, 한국과 일본의 상대국에 대한 호감도가 반등한 이유는 장기 교착상태에 피로감을 느끼고 안보, 경제 사안 등에서 상호 협력의 필요성을 느끼기 때문이라고 분석되었다.[17] 2022년 발표된 일본의 '외교 여론 조사' 보고서에 따르면, 한국에 친근감을 느끼냐는 질문에 '친숙하다고 느낀다'라고 답한 사람의 비율이 45.9%로, 이전 조사 결과(37.0%)에 비해 증가했으며, 향후 한일관계의 발전이 양국과 아태지역에 중요하다고 생각하느냐는 질문에 '중요하다고 생각한다'라고 답한 사람의 비율이 68%였다.[18] 한일관계의 실질적인 개선과 협력을 원하는 여론이 증가하고 있다고 볼 수 있는 것이다.

---

15) 최해옥, "글로벌 기술패권에 대응하는 일본의 전략 및 시사점," 『STEPI Insight』 제280호(2021.10.18.), p. 4.

16) Alexander Wendt, "Anarchy Is What States Make of It: The Social Construction of Power Politics," *International Organization* 46(1992).

17) 미래지향적 협력관계를 이루어가면 역사문제도 해결될 것이란 전망도 2020년(24.5%)과 비교하여 2021년(38.1%)에는 늘어났다. 동아시아연구원, "[EAI] 국문 보도자료_제9회 한일미래대화(2021)," p. 1, 3. 2021.09.27. https://www.eai.or.kr/new/ko/etc/data_view.asp?intSeq=20884&board=kor_poll&keyword_option=&keyword=&more=(검색일: 2023.02.20).

18) PRIME MINISTER'S OFFICE, "外交に関する世論調査 (令和4年10月調査)," 2023. https://survey.gov-online.go.jp/r04/r04-gaiko/2.html(검색일: 2023.02.20).

3. 한일 사이버 외교·안보 협력

앞선 이론적 논의를 통해 한국과 일본의 국가안보전략은 대외적 위협에 선제적으로 대응하고 법, 제도적 규범화를 통해 국제사회에서 질서 유지 및 평화 프로세스를 구축하는 방식으로 이행되고 있음을 알 수 있었다. 마찬가지로, 사이버 안보 위협 이슈에 관해서도 한국 정부와 일본 정부에서는 사이버 위협에 공세적으로 대응하면서 법과 규범적 가치를 강조하여 국제협력을 통해 갈등을 해결하려는 유사한 입장을 가진다. 본 장에서는 사이버안보 분야에 관한 한일 양국의 대응 기조와 외교·안보적 협력 내용을 살펴보고, 제시 가능한 협력방안을 도출하였다.

3.1 위협 증가에 따른 선제적 대응

한국과 일본은 사이버안보에 관한 기본법안 제정 유무에 차이를 보이나, 컨트롤타워 및 실무 체계는 유사하다. 먼저, 일본의 정교한 사이버안보 대응체계는 2014년 사이버안보기본법 제정을 기점으로 마련되었다. 기본법 시행에 맞춰 2015년 1월 관방장관이 주도하는 '사이버시큐리티전략본부'가 설치되었고, 산하에 사무국으로서 '내각사이버시큐리티센터(NISC)'가 설치되어 사이버 안보전략을 총괄·조정해왔다.[19] 한국은 기본법이 없는 대신 개별 법령에 따라 각 부처가 소관 분야에 대한 실질적인 사이버보안 업무를 수행해왔다. 2013~2016년도에 국가정보원에서 청와대로 컨트롤타워를 옮기는 지휘 개편과 권력 분산이 이루어졌고, 현재 국가안보실이 컨트롤타워를 맡고 국가정보원이 총괄·실무를 담당하고 있다. 과거 사이버안보 전략과 대책들이 사건과 사고 이후 후속 대처하는 성격으로 수립돼왔고, 기존 법체계로 급증하는 사이버안보 위협에 신속 대응이 어렵다는 지적이 줄곧 제기돼 옴에 따라, 현 윤석열 정부에서 법체계를 정비하고 국가차원의 대응으로 격상하기 위해 사이버안보기본법 제정을 추진하고 있다.

한국과 일본을 상대로 중국, 러시아, 북한 등은 은밀한 사이버 작전을 벌이거나 배후 해킹조직을 운영하며 활발히 사이버 공격을 감행해왔다. 2016년 일본『방위백서(防衛白書)』는 중국, 러시아, 북한이 일본의 핵심 기반시설을 상대로 한 사이버 공격을 벌이고 있으며, 기술적으로 더욱 교묘해지고 있다는 인식을 천명하였다(防衛省·自衛隊 2016).[20] 한국 역시 7.7 디도스 공격(2009), 3.4 디도스 공격(2011), 3.20 사이버 테러(2013), 한수원 해킹(2014), 국방 기밀탈취(2016) 등

19) 이상현, "일본의 사이버안보 수행체계와 전략,"『국가안보와 전략』제19권 1호(통권 73호), 2019, p. 118.
20) 김상배 외,『사이버 안보의 국가전략 3.0』(서울:사회평론아카데미, 2019), p. 69.

굵직한 사이버 공격피해를 북한으로부터 겪은 바 있다. 한국과 일본은 각각 북한의 ATM 해킹 공격피해 경험을 보유하고 있다. 바로 북한의 대표적인 사이버 공격 중 하나인 사이버 외화벌이 공격이다. 일본은 2016년 편의점 ATM 해킹 사건과 2018년 1월 일본 가상화폐거래소 해킹 사건을 겪은 바 있다. 두 사건은 모두 북한 소행으로 추정된다고 밝혀졌다. 북한은 2017년 3월 한국 ATM도 해킹했는데, 본 사건으로 23만 건의 전자금융거래정보가 유출되었다. 이밖에 북한은 한국의 가상화폐거래소를 상대로도 여러 차례 해킹을 시도한 바 있다.[21]

한국과 일본은 증가하는 사이버안보위협에 관하여 억지력 강화, 적극적 방어, 선제적 대응 등 보다 공세적인 입장을 표명하고 있다. 2022년 11월 일본 정부는 사이버 공격에 대한 방어를 지휘하는 사령탑을 내각관방에 신설하겠다고 발표했으며, 연말까지 국가안전보장 등 안보 관련 문서 개정을 통해 적극적인 사이버 방어 체제 도입 방침을 담을 전망이라고 밝혔다.[22] 새로 설립되는 사령탑 조직은 기존 NISC의 기능을 흡수하고 규모와 권한을 확대하여 '적극적 사이버 방어'를 주요 임무로 담당하게 된다. 뿐만 아니라, 사이버 방어능력을 획기적으로 강화하기 위해 현재 890명 수준인 사이버 방어인력 수를 5년간 대폭 늘려 약 22배인 2만 명으로 확충하는 방안을 검토중이라고 밝혔다.[23] 한국은 국방부가 오는 2027년까지 세계 방산 수출 점유율 5% 돌파해 세계 4대 방산 수출국으로 도약해가겠다는 포부를 드러내며, 미래 통신·사이버 분야에서도 미래 핵심기술을 선제적으로 확보할 계획이라고 발표했다.[24] 2022년 11월 국정원은 민관 공동대응과 협력을 위한 '국가사이버안보협력센터'를 개소하였으며, '차세대 국가 사이버 위협 정보공유시스템'을 개발해 현재 479개인 사이버위협 정보공유 대상을 2배 이상 확대할 계획이라고 밝혔다.[25]

---

21) 유동열, "[전문가 진단] 북한의 새 외화벌이 수단, 사이버 금전(암호화폐) 탈취," 『미래한국』 2019.09.02. http://www.futurekorea.co.kr/news/articleView.html?idxno=120536(검색일: 2022.06.14).

22) 김호준, "日, 사이버방어 사령탑 내각관방에 설치…민간 해커 기용도 검토," 『연합뉴스』 2022.11.01. https://www.yna.co.kr/view/AKR20221101059300073(검색일: 2022.11.20).

23) 박상현, "日정부, 사이버 방어인력 5년간 22배 확대 추진…"2만명 목표"," 『연합뉴스』 2022.12.05. https://www.yna.co.kr/view/AKR20221205124600073(검색일: 2022.12.06).

24) 서현우, "[윤 대통령 주관 '방산수출전략회의'] 2027년까지 세계 4대 방산수출국 도약," 『국방일보』 2022.11.24. https://kookbang.dema.mil.kr/newsWeb/20221125/10/BBSMSTR_000000010021/view.do(검색일: 2022.12.06).

25) 국가사이버안보센터, "국가정보원, 민관 공동대응 위한 '국가사이버안보협력센터' 개소," 2022.11.30. https://www.ncsc.go.kr:4018/main/cop/bbs/selectBoardArticle.do?bbsId=Notification_main&nttId=14075&menuNo=010000&subMenuNo=010300&thirdMenuNo=#LI

국제무대에서 한일 양국은 미국과의 양자동맹 중심으로 사이버 외교·안보 협력을 강화하고 있다. 미일 양국의 외교·국방 장관이 양국의 안보를 논의하는 미일안보협의위원회는 2015년 4월 워싱턴 회의에서 우주, 사이버 영역으로 협력 강화를 합의하였으며, 2019년에는 일본에 대한 사이버 공격 역시 「미일상호협력 및 안전보장조약(日本国とアメリカ合衆国との間の相互協力及び安全保障条約)」 제5조 적용 대상임을 확인하였다.[26] 한국은 2022년 5월 열린 한미 정상회담에서 확장억제를 위한 공조 메커니즘으로서 한미 외교·국방(2+2) 고위급 확장억제전략협의체(EDSCG) 조기 재가동에 합의하였다. 그리고 우주·사이버 협력 강화 등을 통해 한미 연합방위태세를 더욱 강화하기로 합의하여 확장억제 범위에 사이버 영역까지 전략적으로 포함하였음을 알 수 있다.[27] 비슷한 시기 열린 미일 정상회담에서 기시다 총리는 방위비를 증액하겠다는 입장을 표명했는데, 향후 미일동맹의 일체화 및 글로벌화를 통해 사이버 영역에까지 방위력을 강화하여 방위협력의 진전을 이루겠다는 의지로 풀이된다.

경제안보, 첨단기술 이슈를 통한 전략적 소통이 강조되고 있는 상황에서, 양국은 대외적 위협정보 공유체계를 강화할 수 있는 프로세스를 마련하여 사이버 위협에 대응해가야 할 것이다. GSOMIA 체계를 통해 사이버위협 정보공유 확대를 시작으로, 북한 사이버 위협을 조기 식별하고 신속히 정보 공유하는 정형화된 프로세스를 구축해야 한다. 특히 향후 빈번해질 북한의 사이버 외화벌이 공격을 중대한 안보위협 사안으로 상정해야 할 것이다.

또한, 한국과 일본은 동남아시아 해양을 공유하고 있음에 양 국가의 사이버안보에 심각한 피해가 초래될 수 있는 위협으로 통신안보 위협이 있다. 지난 2011년 일본 동북 지방과 인접한 태평양 해저에서 발생한 지진(東日本大地震, 동일본 대지진)으로 일본과 연결된 해저케이블이 손상되어 우리도 유튜브나 구글 등 해외사이트 연결에 심각한 지장을 경험한 바 있다.[28] 해저케이블은 자연재해뿐만 아니라 인위적 파손이나 도청에 취약하다. 이러한 점을 이용해 해저케이블을 타겟으로 한 정보활동이 발생하고 있음을 유의하여 양국은 이에 관한 공동대응 인식이 필요할 것으로 보인다. 나아가 통신안보에 대한 중요도를 높이고 해저케이블 통신망

NK(검색일: 2022.12.01).

26) 박명희, “미일 안보협의위원회(2+2) 주요 내용과 시사점,”『이슈와 논점』 제1816호, 2021.04.08.

27) 외교부, “한미정상회담 주요성과,” https://www.mofa.go.kr/www/wpge/m_24812/contents.do(검색일: 2022.08.11).

28) 최정현, “핵잠수함·해저케이블과 스파이 특수전의 해저 삼각안보,”『KIMS Periscope』 제165호, 2019.07.21.

을 지키기 위한 논의를 시작으로 예상되는 사이버 위협에 선제적으로 대응해가야 할 것이다.

3.2 가치·규범 및 국제협력을 활용한 사이버 외교

일본은 최신 개정된 2021년 사이버 안보전략을 통해 정보의 자유로운 유통, 법치주의, 개방성, 자율성, 다자 간 협력이라는 기본원칙에 입각한 '자유롭고 공정하며 안전한 사이버공간 구현' 확보를 목표로 하며, ①사회-경제적 활력과 지속가능한 발전, ②안전한 디지털 사회 구현, ③국제사회의 평화 및 안정성과 일본의 국가안보에 기여한다는 정책 방향을 강조하였다.[29] 특히 전략에 중국, 러시아, 북한을 주요 사이버 공격 행위자로 언급한 부분은 개정 이전의 전략과 가장 큰 차이를 보인다. 해당 국가들이 군(軍)을 비롯한 기구를 통해 사이버 능력을 향상하고 있음에 따라, 미국과 일본을 비롯한 우방국들은 상호 공유하는 핵심 가치의 수호를 위해 사이버 대응 능력을 향상해야 함을 강력하게 천명한다.[30]

한국은 2019년 최초 발표한 「국가사이버안보전략」을 통해 증가하는 사이버위협에 대응역량을 강화하고 국제협력을 강화하는 등 기본 방향과 비전, 목표를 제시하였다. 신뢰 기반의 사이버안보정책을 추진하기 위한 3대 기본원칙으로 ①국민 기본권과 사이버안보의 조화, ②법치주의 기반 안보 활동 전개, ③참여와 협력 수행체계 구축 등을 마련하였다. 또한, 6대 전략과제 중 하나로 사이버안보 국제규범 형성과 국제협력을 선도하여 사이버안보 선도국가로서의 리더십을 확대한다는 내용을 담고 있다. 이에 사이버안보 국제협력 선도 전략의 주요 내용으로 '양·다자간 협력체계 내실화', '국제협력 리더십 확보'가 제시되었다.[31] 임종득 국가안보실 2차장은 "사이버공격의 배후를 규명하고 관련 제재조치에도 적극적으로 동참하는 등 사이버공간에서 악의적 행위자의 활동에 상응하는 대가를 치르게 할 것"이라며 "주요국과 사이버안보동맹 체결을 검토 중인데 사이버상호방어 개념을 명문화해 국제연대를 강화하고 동맹국과 공동대응하는 방어체계를 마련하고자 한다"고 말했다.[32]

---

29) 박성호, "일본의 사이버 안보전략 - 양자주의의 강화인가 다자주의로의 전환인가? -,"『일본학』 제56집(2022.4), p. 162.
30) 위의 논문. p. 171.
31) 청와대 국가안보실, "국가 사이버안보 전략," 『대한민국 정책브리핑』 2019.04.03. https://www.korea.kr/archive/expDocView.do?docId=38501(검색일: 2022.08.11).
32) 강진규, "국가안보실, 사이버안보 컨트롤타워 맡는다," 『NK경제』 2022.09.20. http://www.nkeconomy.com/news/articleView.html?idxno=10868(검색일: 2022.09.24).

양국은 2016년 10월 열렸던 한일 사이버정책협의회와 같은 양자협력을 재개하여 평화와 번영 목적으로 사이버 외교를 지속해갈 수 있다. 특히 한국은 한미동맹이 강조하는 사이버 적대세력 억지, 사이버공간에서의 여타 국제안보 현안에 관한 협력 등을 일본과의 협력에도 투사하여, 한미일 삼각 사이버안보 공조체제가 마련될 수 있도록 중첩적인 정책안들을 만들어가야 할 것이다.

한편, 국제 사이버범죄에 관한 신속한 국제공조 수사 체계를 통해서도 양국의 협력 프로세스가 가동될 기회가 높아질 것으로 보인다. 윤석열 정부는 사이버범죄에 관한 국제공조 프로세스인 부다페스트 협약 가입을 추진하고 있으며, 이에 유럽평의회에 협약 가입의향서를 제출한 상태다. 동 협약은 인태지역 주요국들인 미국, 일본, 호주 등 67개국이 이미 가입하고 있다. 한국은 가입 이후 공조를 통해 국제 사이버범죄와 사건, 사고 대응에 효율성을 높임으로써 일본과 국제사회 전반의 동맹·우호국 대상으로 협력과 신뢰 의지를 높일 수 있다.

다자협력으로는 NATO 사이버방위센터(CCDCOE)와의 협력을 통해 사이버안보 국제 네트워크를 강화하면서 한국과 일본이 함께 발언권을 키워나갈 것을 기대할 수 있다. 일본은 NATO와 방위당국간 사이버협의체인 「일-NATO 사이버 방위스탭 대화」를 매년 실시하고, NATO가 주최하는 사이버방위연습에도 옵서버를 파견하는 등 운용면에서의 협력도 염두에 둔 대응을 해나가고 있다.[33] 2022년 5월 아시아 최초로 CCDCOE의 정회원이 된 한국은 CCDCOE의 각종 회의, 사이버 방위연습 등에 참가해온 일본과 함께 국제 사이버 규범, 제도 형성을 주도해갈 수 있다.

한일 양국은 아세안 지역 국가들을 활용하는 차원에서도 교류·협력 추진이 가능하다. 아세안은 아태지역 사이버 협력이라는 차원에서 아세안 지역안보포럼(ARF)이라는 아태지역 프레임을 활용하는 동시에 아세안+3의 동남아시아와 동북아시아를 합한 프레임에서 중요한 축을 담당한다.[34] 한국 국방부 장관은 제9차 아세안 확대 국방장관회의(ADMM-Plus)에 참석하여 아세안 중심성에 입각해 다차원적인 국방협력을 발전시킬 것이라는 이행계획 목표를 제시하면서 7개 분과위원회 중 사이버안보 분과위원회를 두어 다자협력 활성화에 기여하겠다는 의지를 전한 바 있다.[35] 일찍이 아세안과 사이버 협력에 적극적인 일본이 역내 영향력을 높여온 상황에서, 한국도 아세안과 다

33) 이상현, “사이버 위협에 대한 일본의 대응: 사이버 외교와 사이버 방위,” 『국가전략』 2019년 제25권 2호, p. 110.

34) 김상배, “제9장 한국의 사이버 안보 전략과 외교,” 『사이버 안보의 국가전략』 (서울:사회평론아카데미, 2017), p. 328.

35) 서현우, “한·아세안 다차원적 국방협력 목표·이행계획 천명,” 『국방일보』 2022.11.24. https://kookbang.dema.mil.kr/newsWeb/20221125/9/BBSMSTR_000000010021/view.do(검색일: 2022.12.06).

자협력을 추진하여 역내 한미일 영향력을 높여가야 할 것이다.[36]

<표2> 한일 사이버 외교·안보 전략

구분	대한민국	일본
안보	- 사이버 억지력 제고 - 전략 목표: ① 국민 기본권과 사이버안보의 조화 ② 법치주의 기반 안보 활동 전개 ③ 참여와 협력 수행체계 구축	- 적극적 사이버 방어 - 전략 목표: ① 디지털 전환과 사이버 안보 강화 ② 상호 연결/연계성이 증대되는 사이버공간의 안보 강화 ③ 일본의 국가안보 강화
외교	- 한미 사이버 안보 협력 강화 - 주요국과 사이버안보동맹 고려, 공동대응 방어체계 구축	- 미일 동맹에 기반한 사이버 능력 강화 - 미일 안전보장조약에 사이버 영역을 포함하여 사이버 방어력 확대

출처: 한국과 일본의 정부 발간 보고서, 발표자료 내용 일부를 참고하여 저자가 재구성.

3.3 미래지향적 정체성 형성을 위한 사이버 교류와 협력

구성주의 이론은 한국과 일본이 과거 침략과 식민지 역사에 대한 기억을 반복하며 양국관계의 갈등과 긴장을 초래하는 것에서 벗어나야 하고, 양국관계를 개선하기 위해서 대중문화, 스포츠, 인적교류 등을 통해 미래지향적 정체성 형성이 필요하다고 진단한다. 이러한 맥락에서 사이버 협력 및 교류는 양국 관계개선에 디딤돌 역할을 할 수 있다. '2017년 아시아-태평양 지역의 사이버 성숙도'(Cyber Maturity in the Asia-Pacific Region 2017) 보고서에서 일본의 사이버 성숙도는 총점 88점(2위)이며, 한국은 총점 86.8점(5위)으로 양국 모두 높은 평가를 받았다.[37] 대중의 인식 항목에서도 양국이 높은 점수를 유지하고 있다. 일본은 소니픽처스사, 일본 연금서비스, 워너크라이, Not Petya 랜섬웨어 등 해킹 사건들을 비

36) 일본과 아세안의 사이버 보안 정책협력회의는 2009년부터 시작되었는데, 국장급이 참석하는 '고위급정책회의'와 과장급 및 실무담당자를 대상으로 하는 '네트워크보안 워크숍'과 '정보보호 훈련'으로 나누어 개최되고 있다. 특히 2013년 9월에는 사이버보안에 관한 장관급회의가 개최되어 사이버 공격에 대한 공동대응을 위한 합의문이 발표된 바 있다. 아세안과 일본은 사이버 공격의 위협에 공동으로 대처하기 위해, 공격을 예지하거나 바이러스 감염을 탐지해 경고를 울리는 시스템을 연계 개발한다는 내용을 골자로 한 공동성명도 발표했다. 김상배(2017), 앞의 책.

37) Fergus Hanson et al., "Cyber Maturity in the Asia Pacific Region 2017," Australian Strategic Policy Institute(ASPI) (2017). 2017.12.12. https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2017(검색일: 2023.02.18).

롯해 사이버 이슈에 관한 대중, 기업, 정부의 관심이 여전히 높으며, 한국 역시 한국인터넷진흥원(KISA)과 언론 보도를 통해 사이버보안 이슈를 국민에게 신속히 전달하고 있다.[38] 양국은 사이버 기술, R&D, 인적 교류를 적극적으로 확대·추진하여 개인-기업-정부 연계 차원에서 꾸준히 교류할 필요가 있다. 대중의 사이버 이슈에 관한 높은 관심을 활용해 양국이 교류와 협력을 높인다면 긴장과 갈등을 일정 완화하는 효과가 있을 것이다.

4. 결론

본 연구에서는 국제정치적으로 미중 패권경쟁이 가속화되는 가운데 한국과 일본이 동맹 네트워크 중심으로 군사·외교·안보·경제 전방위에 걸쳐 진영 간 연대를 구축하고 있는 현상을 신현실주의와 신자유주의, 구성주의 이론적 논의를 통해 살펴보았다. 미국이 주도하고 있는 인도-태평양 전략은 민주주의 국가들의 결집과 연대를 공고히 하는 주요 동력이 되어왔으며, 이에 한국과 일본은 자국의 안보전략이 추구하는 선제적 대응 기조에 맞춰 인태지역 역내 국가들과 상호 중첩되는 안보위협 이슈를 논의하며 협력을 모색하고 있다. 한일 양국은 북한의 핵·미사일, 중국의 부상에 따른 전방위적 압박 등 안보위협에 대응하기 위해 전략적으로 협력 범위를 넓혀가는 상황이다.

한일 간 군사안보협력보다도 민감하지 않은 수준에서 사이버 외교·안보 협력의 기회는 더욱 확대될 것이다. 양국은 북핵위협과 북한·중국 문제 대응을 위해 안보협력이 중요하다는 인식을 공유해왔다. 그리고 이들 위협이 사이버 영역에서 투사되면서 발생하는 대외적 위협과 피해에 맞서 국가 차원에의 대응과 보호를 핵심 국가목표로 설정하여 안보협력 범위를 사이버공간으로 넓혀가고 있다. 사이버 협력은 전통안보와 연계되는 사안으로서 러시아, 중국, 북한의 사이버 위협에 대처하고 양자·다자협력을 통해 한일관계 개선을 끌어낼 수 있는 핵심의제다. 즉, 대외 사이버 위협억제라는 국가적 목표 설정과 추진을 통해 한일 양국의 전략적 협력 관계 발전을 도모할 수 있다.

한국과 일본은 사이버 위협행위자를 향한 대응과 안보 수호 의지에 최우선 목표가 있다는 점, 그리고 국가 사이버안보 전략에서 법치주의, 개방성, 자율성을 추구하고 있다는 점에서 매우 유사한 국가적 대응 기조를 보인다. 양국은 상대

38) *Ibid.* p. 44, p. 77.

적으로 민감도가 낮으면서도 글로벌 안보 차원에서 협력이 필요한 분야에서의 협력을 추진하며 단계적으로 신뢰를 쌓아가야 할 것이다.[39] 글로벌 기술패권을 둘러싸고 미국과 중국이 디지털, 사이버 부문에서 치열하게 경쟁을 벌이고 있는 만큼, 한국과 일본은 ICT 기술협력 중심으로 경제안보 차원에서 협력 범위를 넓혀갈 수 있다.

사이버 영역은 새로운 규칙을 마련하기 위해 국제적 대처가 주도되고 있는 공간이다. 한일 양국은 사이버공간에서 신뢰를 구축해나감과 동시에 민주주의와 시장경제, 인권과 규범적 가치를 공유하는 우호 파트너 국가들과 연대 기회를 넓힐 수 있다. 특히 아세안과의 사이버 다자협력을 통해서 인태지역 역내 영향력과 위상을 높일 수 있다. 한국과 일본이 자국 사이버 안보전략을 통해 국제규범 형성과 신뢰 구축에 대한 의지를 강조하고 있는 만큼, 사이버 외교 무대를 적극적으로 활용하고 양자·다자 안보협력을 추진함으로써 양국관계 개선 나아가 한미일 삼각 사이버안보 공조체제로의 발전을 기대할 수 있을 것이다.

마지막으로, 한일 국민 간 상호인식 개선 차원에서 사이버 이슈에 관한 교류와 협력을 높인다면 양국의 미래지향적 협력 관계 형성에 크게 도움 될 것이다. 과거사 갈등에도 불구하고 상호 협력을 원하는 양국 국민 여론이 높아지고 있으며, 사이버 분야에의 대중과 여론의 관심이 큰 점을 이용하여 사이버 분야에서 인적, 기술적 교류와 협력을 확대·추진하여 양국이 긍정적 상호인식을 가지도록 노력해야 할 것이다.

본 연구는 사이버안보라는 신안보 영역에서 한일 양국이 공유할 수 있는 공통 위협 주체와 위협 유형을 구체적으로 제시하여 그에 따른 대응과 협력방안을 모색하였다는 점에서 의의가 있으나, 국제정치이론을 거시적으로 적용하여 한일협력의 제약사항에 관한 논의가 다소 부족하다는 점에서 연구한계가 있다.

39) 최은미(2022), 앞의 논문.

참고문헌

1. 단행본

김상배 외(2017)『사이버 안보의 국가전략』서울:사회평론아카데미.

_____(2019)『사이버 안보의 국가전략 3.0』서울:사회평론아카데미.

박건영 외(2009) 『국제관계론강의2』 파주:한울 아카데미, Robert O. Keohane, "Neoliberal Institutionalism: A Perspective on World Politics," *International Institutions and State Power: Essays in International Relations Theory*, Boulder: Westview Press, 1989, ch.1(김우상 옮김).

이근욱(2009)『왈츠 이후 국제정치이론의 변화와 발전』파주:한울 아카데미.

Kim, Taehyo and Brad Glosserman ed(2004) *The Future of U.S.-Korea-Japan Relations: Balancing Values and Interests* (Washington D.C.: Center for Strategic and International Studies. 2004).

2. 논문

권태환(2018)「최근 일본의 안보정책 변화와 향후 전망: 미중 대립과 북한 비핵화를 중심으로」『한국국가전략』3(3), 8.

김태효(2019)「신아시아 안보질서 2030: 패러다임 변화와 한국의 과제」『신아세아』26권 3호.

남창희(2009)「한미동맹과 미일동맹의 동조화와 한일안보협력」『한일군사문화연구』Vol.8.

민경식(2016)「초연결 사회를 대비한 일본의 사이버보안 정책 동향」『주간기술동향』4.13.

박명희(2021)「미일 안보협의위원회(2+2) 주요 내용과 시사점」『이슈와 논점』제1816호.

박성호(2022)「일본의 사이버 안보전략 -양자주의의 강화인가 다자주의로의 전환인가?-」『일본학』제56집.

박철희(2019)「한일 갈등의 심화와 한일안보협력의 미래」『한국국가전략』4권 2호.

박휘락(2018)「북핵 고도화 시대 한일 안보협력 - 실태 그리고 구심요소와 원심요소 -」『한일군사문화연구』25권 0호.

이상현(2019)「일본의 사이버안보 수행체계와 전략」『국가안보와 전략』제19권 1호(통권73호).

_____(2019)「사이버 위협에 대한 일본의 대응: 사이버 외교와 사이버 방위」『국가전략』제25권 2호.

이승주(2017)「일본 사이버안보 전략의 변화: 사이버 안보의 전통 안보화와 전통 안보의 사이버 안보화」『국가안보와 전략』17(1), 65.

최은미(2022)「기시다-바이든 미일정상회담 이후 일본의 대외전략과 한일관계에의 함의」『이슈브리프』2022-19.

최정현(2019)「핵잠수함·해저케이블과 스파이 특수전의 해저 삼각안보」『KIMS Periscope』제165호, 07.21.

최해옥(2021)「글로벌 기술패권에 대응하는 일본의 전략 및 시사점」『STEPI Insight』제280호, 10.18.

Katagiri, Nori(2018) Between Structural Realism and Liberalism Japan's Threat Perception and Response, *International Studies Perspectives*, 19.

Walt, Stephen M(1997) Why Alliances Endure or Collapse, *Survival,* Vol.39, No.1.

Wendt, Alexander(1992) Anarchy Is What States Make of It: The Social Construction of Power Politics, *International Organization* 46.

3. 기사자료

강진규(2022) “국가안보실, 사이버안보 컨트롤타워 맡는다” 『NK경제』 09.20. http://www.nkeconomy.com/news/articleView.html?idxno=10868(검색일: 2022.09.24).

김호준(2022) “日, 사이버방어 사령탑 내각관방에 설치…민간 해커 기용도 검토”『연합뉴스』 11.01. https://www.yna.co.kr/view/AKR20221101059300073(검색일: 2022.11.20).

박미영·권지원(2022) “한일정책협의단 "한일관계 개선 '선택 아닌 당위' 공감대"”『뉴시스』. 04.28. https://newsis.com/view/?id=NISX20220428_0001852599(검색일: 2022.07.14).

박상현(2022) “日정부, 사이버 방어인력 5년간 22배 확대 추진…"2만명 목표"”『연합뉴스』 12.05. https://www.yna.co.kr/view/AKR20221205124600073(검색일: 2022.12.06).

서현우(2022) “[윤 대통령 주관 ‘방산수출전략회의’] 2027년까지 세계 4대 방산수출국 도약”『국방일보』 11.24. https://kookbang.dema.mil.kr/newsWeb/20221125/10/BBSMSTR_000000010021/view.do(검색일: 2022.12.06).

_____(2022) “한·아세안 다차원적 국방협력 목표·이행계획 천명”『국방일보』 11.24. https://kookbang.dema.mil.kr/newsWeb/20221125/9/BBSMSTR_000000010021/view.do(검색일: 2022.12.06).

신나리·신규진(2022) “北미사일 발사 포착은 한국, 낙하땐 日… 실시간 공조 첫발” 『동아일보』 11.26. https://www.donga.com/news/Politics/article/all/20221126/116695549/1(검색일: 2022.12.01).

유동열(2019) “[전문가 진단] 북한의 새 외화벌이 수단, 사이버 금전(암호화폐) 탈취”『미래한국』 09.02. http://www.futurekorea.co.kr/news/articleView.html?idxno=120536(검색일: 2022.06.14).

안석(2022) “한미일 “北미사일 경보 실시간 공유”… 한일 지소미아 정상화한다” 『서울신문』 11.14. https://www.seoul.co.kr/news/newsView.php?id=20221114003019(검색일: 2022.11.22).

4. 인터넷 자료

국가사이버안보센터(2022) “국가정보원, 민관 공동대응 위한 '국가사이버안보협력센터' 개소” 11.30. https://www.ncsc.go.kr:4018/main/cop/bbs/selectBoardArticle.do?bbsId=Notification_main&nttId=14075&menuNo=010000&subMenuNo=010300&thirdMenuNo=#LINK(검색일: 2022.12.01).

대통령실(2022) “[전문] 한·미 정상 공동성명” 『대한민국 정책브리핑』 05.21. https://www.korea.kr/news/policyNewsView.do?newsId=148901846(검색일: 2022.06.14).

동아시아연구원(2021) “[EAI] 국문 보도자료_제9회 한일미래대화(2021)” p. 1, 3. 09.27. https://www.eai.or.kr/new/ko/etc/data_view.asp?intSeq=20884&board=kor_poll&keyword_option=&keyword=&more=(검색일: 2023.02.20).

외교부(2022) “한미정상회담 주요성과” https://www.mofa.go.kr/www/wpge/m_24812/contents.do(검색일: 2022.08.11).
청와대 국가안보실(2019) “국가 사이버안보 전략” 『대한민국 정책브리핑』 04.03. https://www.korea.kr/archive/expDocView.do?docId=38501(검색일: 2022.08.11).
Fergus Hanson, Tom Uren, Fergus Ryan, Michael Chi, Jack Viola and Eliza Chapman(2017) “Cyber Maturity in the Asia Pacific Region 2017” Australian Strategic Policy Institute(ASPI) 12.12. https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2017(검색일: 2023.02.18).
PRIME MINISTER’S OFFICE(2023) “外交に関する世論調査 (令和4年10月調査)” https://survey.gov-online.go.jp/r04/r04-gaiko/2.html(검색일: 2023.02.20.).

접 수 일: 2022년 12월 9일
심사완료일: 2023년 2월 17일
게재확정일: 2023년 2월 17일

Abstract

A Study on Cyber Diplomacy and Security Cooperation between Korea-Japan through International Relations Theory Approach

Choi Eun Ah

This study examines an approach to the diplomatic and security strategies of Korea and Japan through theoretical discussions of Neo-Realism, Neo-Liberalism and Constructivism, which are international political theories. Then, I explained the cyber security threat issues commonly faced by the two countries and the response and cooperation process. The purpose of this study is to contribute to the development of Korea-Japan relations by deriving a cybersecurity cooperation plan between Korea and Japan based on a theorstical perspective. As cybersecurity threats increase in the international community, the confrontational structure between the West and the non-Western camps is intensifying in cyberspace as well. Western countries are actively coping with cyber threats and promoting international cooperation by utilizing allies, like-minded countries, and international organizations. In addition to North Korea's nuclear and missile threats, South Korea and Japan can share examples of cyber damage. The two countries should share security threat issues and demonstrate strategic partnership through active mutual assistance. Under the leadership of the US Indo-Pacific Strategy, major countries in the Indo-Pacific region, such as Japan, Australia, and India, are building a security alliance. Cybersecurity and diplomatic cooperation between Korea and Japan will stand out in the global competition for hegemony and contribute to strengthening strategic cooperation among South Korea, the US and Japan in the future. Therefore, South Korea should seek to deter threats, enhance strategic values, and improve South Korea-Japan relations while pursuing cyber bilateral and multilateral cooperation.

Keywords: National security, Cyber security/diplomacy, South Korea-Japan cooperation, cyber threats, international relations theory