경제·인문사회연구회 협동연구 총서 19-43-03
주변국의 국경안보와 한반도 통일환경(3/3년차)

KINU 연구총서 19-29

주변국의 사이버 환경과 한반도 평화체제 구축

채재병 • 김일기 • 김상규 • 이상현

KINU 통일연구원

경제·인문사회연구회 협동연구 총서

“주변국의 국경안보와 한반도 통일환경”

1. 협동연구 총서 시리즈

협동연구 총서 일련번호	연구보고서명	연구기관
19-43-01	한반도 평화·번영 실현을 위한 국경 협력	통일연구원
19-43-02	한반도 접경국과의 초국경 관광·교통 협력	대외경제정책연구원
19-43-03	주변국의 사이버 환경과 한반도 평화체제 구축	한국국가정보학회

2. 참여연구진

연구기관		연구책임자	참여연구진
주관연구기관	통일연구원	현승수 연구위원 (총괄책임자)	오경섭 연구위원 이우태 부연구위원 나용우 부연구위원 김규륜 석좌연구위원 이승열 입법조사관 (국회 입법조사처) 박성용 교수(전북대학교) 윤인주 부연구위원 (한국해양수산개발원)
협력연구기관	대외경제정책연구원	최장호 부연구위원	허재철 부연구위원 이정균 전문연구원 최유정 전문연구원 임소정 연구원
	한국국가정보학회	채재병 책임연구위원 (국가안보전략연구원)	김일기 책임연구위원 (국가안보전략연구원) 김상규 연구교수 (한양대학교 중국문제연구소) 이상현 객원연구위원 (제주평화연구원)

경제·인문사회연구회 협동연구 총서 19-43-03
주변국의 국경안보와 한반도 통일환경(3/3년차)

KINU 연구총서 19-29

주변국의 사이버 환경과 한반도 평화체제 구축

연구책임자
채재병 (국가안보전략연구원 책임연구위원)

공동연구자
김일기 (국가안보전략연구원 책임연구위원)
김상규 (한양대학교 중국문제연구소 연구교수)
이상현 (제주평화연구원 객원연구위원)

KINU 통일연구원

주변국의 사이버 환경과 한반도 평화체제 구축

주변국의 국경안보와 한반도 통일환경(3/3년차) KINU 연구총서 19-29

발 행 일	2019년 12월 30일
저 자	채재병, 김일기, 김상규, 이상현
발 행 인	임강택
발 행 처	통일연구원
편 집 인	평화연구실
등 록	제2-02361호 (97.4.23)
주 소	(06578) 서울시 서초구 반포대로 217 통일연구원
전 화	(대표) 02-2023-8000 (FAX) 02-2023-8296
홈 페 이 지	http://www.kinu.or.kr
기획·디자인	(주)에이치에이엔컴퍼니(02-2269-9917)
인 쇄 처	세일포커스(주) (02-2275-6894~6)
I S B N	978-89-8479-970-7 93340
가 격	8,500원

주변국의 사이버 환경과 한반도 평화체제 구축

본 보고서에 수록된 내용은 집필자의 개인적인 견해이며,
당 연구원의 공식적인 의견을 반영하는 것은 아닙니다.

차 례

표 차례

그림 차례

요 약

최근 한반도 정세변화에 따라 한반도 주변국들의 국경안보 실태와 이들 국가의 대한반도 국경협력 가능성 그리고 남북한 접경지대 협력에 대한 종합적인 분석을 통해 한반도 평화·번영 시대를 준비할 필요가 커졌다. 국경안보의 개념을 확대하여 정치 및 군사적 측면뿐 아니라 경제협력 및 교류를 통해서도 국경안보에 대비할 수 있다는 새로운 분석 틀을 제시하여 한반도 통일 및 통합 과정에서 나타날 수 있는 주변국과의 갈등을 미리 방지하고, 국경안보를 위한 다자적 협력 기반을 조성할 필요성이 생긴 것이다. 특히 사이버공간에서의 국가 간 주권과 관할, 경계에 대한 논의가 활발하며, 이를 둘러싼 한반도 주변 강대국인 미·일·중·러의 입장이 강화되는 추세이다. 이는 4차 산업혁명 시대에 필연적으로 제기될 사이버상의 주권 문제와 직결되며, 한국도 사이버 국경분쟁을 염두에 두고 적극적인 대응책 강구가 시급한 상황이 도래했다. 따라서 본 연구는 국경안보의 연장선상에서 남북한 및 미·일·중·러 주변국들의 사이버공간에 대한 인식, 전략, 국제협력 등 사이버환경을 살펴봄으로써 사이버영역에서의 한반도 평화체제 구축을 위한 전략과 과제를 제시한다.

국가안보 차원에서 국경안보가 논의되는 것과 마찬가지로 사이버안보도 국가안보 및 국경안보 차원에서 논의될 수 있는 것이다. 국경안보 차원에서의 사이버안보 논의는 사이버공간이라는 새로운 안보영역이 현실공간에서의 국경과 같은 접점을 포함하고 있으며 국경안보와의 상관성을 갖고 있다는 것이다. 물론 현실공간에서의 국경안보 개념은 사이버공간의 특수성으로 인해 그대로 적용될 수는 없으나 국경이 주권과 주권이 충돌하는 지점이라는 논리의 연장선상에서 보면 사이버공간에

서도 주권 충돌의 지점이 존재하므로 국경안보 개념의 확장을 통해 국경안보 차원에서의 사이버안보 논의가 가능한 것이다. 즉 사이버안보의 특성이 국경안보 개념의 확장과 사이버공간과의 연계를 설명해주고 동시에 사이버공간에서의 국경안보 개념 정립의 근거를 제공해주고 있다.

외교부에 따르면 한반도 평화체제는 남북한을 비롯한 관련국 상호간에 공식적으로 전쟁상태를 종식시킴으로써 법적·제도적 및 실질적으로 한반도에 공고한 평화가 보장되어 있는 상태를 의미한다.[1] 국경안보와 국경협력 문제는 사이버공간에서도 적용 가능하며 주변국의 국경안보와 한반도 통일 환경은 주변국의 사이버환경과 한반도 평화체제 구축과 일맥상통한다. 이에 따라 한반도 사이버 평화체제는 기존에 논의되고 있는 한반도 평화체제의 부분 또는 확장이라는 측면에서 접근하고 있다. 즉 한반도 평화체제를 위한 사이버공간 차원에서의 안보 레짐을 의미한다. 따라서 한반도 사이버 평화체제는 사이버공간에서의 한반도 평화를 보장하는 사이버안보 레짐을 형성하는 국내외적 법적, 제도적 장치들과 거버넌스로 구성된다. 특히 사이버공간에서의 거버넌스 구축을 위한 국제적인 협력과 국제규범의 형성에 방점이 주어진다.

국경안보 차원에서 사이버안보를 논의하기 위해 남북한 및 한반도 주변국들을 중심으로 사이버공간에서의 변화된 전략과 정책들을 검토하였다. 주변국 사이버안보정책의 공통적 요소는 첫째, 사이버안보가 국가안보 우선과제로 부상한 상황에서 단일부처가 감당할 수 없으므로 관련 기관 간 협력체제 개발을 진행하고 있다는 점이다. 둘째, 사이버 기술 발달을 통한 방어력 증강을 통해 억지력과 안전을 확보하고자 한다는 점이다. 셋째, 사이버 공간의 민간부문의 몫을 감안할 때 모든 정책결정에 기업, 시민사회, 기술자, 학자 등을 포괄하는 민·관 파트너십이 토대가 되고 있다는 점이다. 넷째, 모든 국가가 국제협력 강화에 중점을

1) 외교부, 「한반도평화체제」, 〈http://www.mofa.go.kr/www/wpge/m_3982/contents.do〉 (검색일: 2019.10.11.).

두고 있다는 점이다. 이에 따라 한국은 사이버공간에 대한 안전성 확보, 사이버공격에 대한 억지력 확보, 정보보안 정책의 성공적 추진을 위한 사이버안보 기반 조성, 국제 사이버협력 네트워크 확충 등을 사이버안보 전략의 추진방향으로 삼아야 할 것이다.

마지막으로 한반도 사이버 평화체제를 제안하고, 이를 구축하기 위해 주변국들의 사이버안보 정책 변화에 대한 대응을 통해 한반도 사이버안보 협력의 전략과 과제를 제시하였다. 또한 이 과정에서 새로운 규범의 확립과 경쟁에 대비한 정책을 수립하기 위해 불안정한 사이버공간의 확장과 이에 기초한 위기와 갈등을 해결할 수 있는 평화적 규범 수립에 관한 정책 방안도 제시하였다. 한반도 사이버 평화체제를 위해 국제사회와의 다양한 협력을 통해 사이버안보 국제협력 네트워크를 형성하고, 리더십을 구축하면서, 사이버공격을 감행하는 국가들의 불법행위를 국제사회 공동문제로 이슈화하고, 외교, 군사, 경제 등 국제공조를 통한 국제사회의 광범위한 제재 조치를 유도하는 것 등을 기본 전략으로 제시하였다. 국제 사이버 안보 파트너십을 강화하기 위해 다른 나라나 국제기구 등 국제사회와의 다양한 협력방안 강구하고, 사이버공격에 대한 억지력을 확보하기 위하여 미국, 일본, 중국, 러시아 등과 다자·양자간 국제협력을 강화함과 동시에 후발국들에 대해 사이버 선도국가로서의 역할을 수행하며, 중립적이고 보편타당한 사이버안보 국제규범 수립을 지원해야 할 것이다.

주제어: 사이버환경, 사이버안보, 국경안보, 한반도 평화체제, 한반도 사이버 평화체제

Abstract

The Cyber Environment of Neighboring Countries and the Establishment of Peace Regime on the Korean Peninsula

Chae, Jae Byung et al.

With the recent change in the situation on the Korean Peninsula, the need to prepare for the era of peace and prosperity on the Korean Peninsula has increased through a comprehensive analysis of the border security situation and the possibility of border cooperation of neighboring countries on the Korean Peninsula, and the border cooperation between the two Koreas. By presenting a new framework for analysis that can prepare for border security not only through political and military aspects but also through economic cooperation and exchanges by expanding the concept of border security, the government needs to prevent possible conflicts with neighboring countries in advance that may emerge in the process of reunification and integration of the Korean Peninsula and create a foundation for multilateral cooperation for border security. In particular, there are active discussions on sovereignty, jurisdiction and boundaries among countries in cyberspace, and the positions of the U.S.,

Japan, China and Russia, the neighboring powers on the Korean Peninsula, are intensifying. This is directly related to the issue of cyber sovereignty that will inevitably be raised in the era of the fourth industrial revolution, and South Korea is also in urgent need of an active countermeasure with cyber border disputes in mind. Therefore, this study presents strategies and tasks for establishing a peace regime on the Korean Peninsula in cyber territory by looking at cyber environments, including awareness, strategies, and international cooperation of the two Koreas, the U.S., Japan, China and Russia as an extension of border security.

Just as border security is discussed in terms of national security, cyber security is something that can be discussed in terms of national security and border security. The discussion on cyber security at the border security level is that the new security area, called cyberspace, includes border-like interfaces in real space and has a correlation with border security. Of course, the concept of border security in real space cannot be applied as it is due to the special nature of cyberspace, but in the extension of the logic that borders are a place where sovereignty collides with sovereignty, there is also a point of conflict in cyberspace, so the expansion of the concept of border security enables discussion of cyber security at the border security level. In other words, the nature of cyber security explains the expansion of the concept of border security and the linkage of cyberspace, while providing the basis for establishing the concept of border security in cyberspace.

According to the Ministry of Foreign Affairs(ROK), a peace regime on the Korean Peninsula refers to the establishment of peace that is solidly secured in legal, institutional and concrete terms by formally ending the state of war on the Korean Peninsula among the related countries with the two Koreas lying at the center. Border security and border cooperation issues can also be applied in cyberspace, and the neighboring countries' border security and reunification environment on the Korean Peninsula are in line with the cyber environment of neighboring countries and the establishment of a peace regime on the Korean Peninsula. Accordingly, the cyber peace regime on the Korean Peninsula is approached in terms of part or extension of the peace regime on the Korean Peninsula, which is currently under discussion. In other words, it means a security regime at the level of cyberspace for a peace regime on the Korean Peninsula. Thus, the cyber peace regime on the Korean Peninsula consists of domestic and international legal and institutional devices and governance that form a cyber security regime guaranteeing peace on the Korean Peninsula in cyberspace. In particular, the focus will be on the international cooperation and the formation of international norms for the establishment of governance in cyberspace

To discuss cyber security in terms of border security, we reviewed the changed strategies and policies in cyberspace, focusing on the two Koreas and neighboring countries of the Korean Peninsula. A common element of neighboring countries'

cyber security policies is that they are developing cooperation systems among related agencies because they cannot be afforded by a single ministry at a time when cyber security has emerged as a national security priority. Second, it wants to secure deterrence and safety by strengthening its defense capabilities through the development of cyber technologies. Third, given the private sector's share of cyberspace, the private–government partnership, which encompasses businesses, civil society, technicians and scholars, is laying the foundation for all policy decisions. Fourth, all countries are focusing on strengthening international cooperation. Accordingly, South Korea will have to use its cyber security strategy as a way to secure safety in cyberspace, secure deterrence against cyber attacks, create a cyber security base for successful implementation of information security policies, and expand international cyber cooperation networks.

Finally, it proposed a cyber peace regime on the Korean Peninsula and presented strategies and tasks for cooperation in cyber security on the Korean Peninsula by responding to changes in neighboring countries' cyber security policies to build it. In the process, to establish new norms and policies against competition, it also proposed policy measures on establishing peaceful norms to resolve crises and conflicts based on expanding unstable cyberspace. The basic strategy was to form a cyber security international cooperation network, establish leadership and launch cyber attacks through various cooperation with the

international community for the cyber peace regime on the Korean Peninsula, issue illegal acts by countries that carry out cyber attacks as a joint issue of the international community, and to induce widespread international sanctions through diplomatic, military and economic cooperation. In order to strengthen international cyber security partnership, the government should seek diverse cooperation measures with the international community, including other countries and international organizations, strengthen international cooperation between multilateral and bilateral countries, such as the U.S., Japan, China and Russia to secure deterrence against cyber attacks, play a role as a cyber leader in the late-start countries, and support the establishment of neutral and universal international cyber security norms.

Keywords: Cyber environment, Cyber security, Border security, Peace regime on the Korean Peninsula, Cyber peace regime on the Korean Peninsula

Ⅰ. 서론

최근 한반도 정세변화에 따라 한반도 주변국들의 국경안보 실태와 이들 국가의 대한반도 국경협력 가능성 그리고 남북한 접경지대 협력에 대한 종합적인 분석을 통해 한반도 평화·번영 시대를 준비할 필요가 커졌다. 국경안보의 개념을 확대하여 정치 및 군사적 측면뿐 아니라 경제 협력 및 교류를 통해서도 국경안보에 대비할 수 있다는 새로운 분석 틀을 제시하여 한반도 통일 및 통합 과정에서 나타날 수 있는 주변국과의 갈등을 미리 방지하고, 국경안보를 위한 다자 협력의 기반을 조성할 필요성이 생긴 것이다. 특히 사이버공간에서의 국가 간 주권과 관할, 경계에 대한 논의가 활발하며, 이를 둘러싼 한반도 주변 강대국인 미·일·중·러의 입장이 강화되는 추세이다. 이는 4차 산업혁명 시대에 필연적으로 제기될 사이버상의 주권 문제와 직결되며, 한국도 사이버 국경 분쟁을 염두에 두고 적극적인 대응책 강구가 시급한 상황이 도래했다.

주변국들의 국경협력 가능성은 사이버 영역에서도 동일하게 적용될 수 있다. 국경협력에 대한 정치경제적 관점에서 보는 초국경 거래의 증대는 사이버공간과 유사점을 갖는다. 또한 국경협력과 안보문제는 사이버공간에서 그대로 적용 가능하다. 국경분쟁의 평화적 해결을 통한 국경협력 개념 또한 사이버 위협과 갈등을 해소하는데 함의를 갖는다. 영토갈등과 국제분쟁, 국경안보와 국제협력, 국경협력과 한반도 통일이라는 세 가지 차원에서의 접근은 사이버공간에서도 마찬가지로 적용될 수 있다. 주변국의 국경안보와 한반도 통일 환경은 주변국의 사이버 환경과 한반도 평화체제 구축과 일맥상통한다. 또한 국경안보와 사이버안보 영역의 결합은 전통적 안보개념과 비전통 안보개념을 포괄하는 융합적 성격을 갖고 있다. 따라서 21세기 사이버공간에서의 국경과 주권 문제에 대한 선제적 대응이 요구된다.

과학기술과 정보통신의 발달로 초연결 사회가 도래하였다. 전통적 국경 개념의 붕괴와 확장은 소위 오프라인에서의 안보가 온라인 영역으로 전이되어 더욱 중요한 안보 문제를 야기하고 있다. 또한 한반도 주변의 정세 변화와 새로운 형태의 안보 상황이 출현하고 있다. 즉 남북한 및 북미 정상 회담 개최 등 한반도에는 새로운 평화의 분위기가 조성되고 있다. 그러나 미중 양국을 위시한 일본, 러시아 등 주변국들은 여전히 막후에서 치열한 국가이익 실현을 추구하고 있다. 특히, 전통 안보 영역 이외의 비전통 안보 영역인 사이버공간에 관한 규범 경쟁과 안보 체계 확립의 중요성에 초점을 맞추고 있다. 따라서 비전통 안보 영역인 사이버공간에서 새로운 차원의 안보 인식과 대응책 마련이 시급하다.

한반도의 평화 정착을 위해서는 전통 안보와는 별개의 시각에서 기존 형태와 다른 사이버 국경의 해체와 동 영역의 안보를 결합한 지속 가능한 평화통일 시대를 대비하여야 한다. 이에 사이버공간에 관한 분석은 물론 이해 당사국들의 행태에 대한 세밀한 분석을 통해 장기적이고 구체적인 전략과 대응책을 마련하는 것이 필요하다.

남북관계의 개선에도 불구하고 여전히 북한은 안보적인 측면에서 주시하고 경계해야 할 대상이다. 특히 남한과의 국력 비대칭 속에 북한이 주력하고 있는 사이버역량 강화와 이에 기초한 사이버공격과 테러 등 안보적 위기상황의 조성에 대한 방비는 필수 불가결하다. 또한 북한의 사이버공격이 중국에서 시작되거나 중국을 거치는 경우가 있으므로 이에 대한 대비도 철저히 할 필요가 있다.

미국은 2001년 9·11 테러를 기점으로 사이버안보를 일반적인 안보영역을 넘어 국가안보적 차원으로 체계화하며 관련 법·제도를 정비하기 시작했다. 사이버안보와 관련된 업무도 국방부, 국가안보국, 국토안보부, 연방수사국 등 다양한 조직에서 담당하고 있다. 국가 전

반에 걸쳐 사이버안보와 관련된 시스템을 구축하는데 막대한 예산을 투입하고, 사이버 전략 계획을 수립하여 사이버안보 태세에 대한 방비를 진행 중이다. 미국의 이러한 행보는 중국과 북한을 특정하여 경쟁과 갈등, 의심과 경계를 하는 행태와 아주 밀접하게 연결되어 있다.

일본은 2014년 제정한 사이버보안기본법을 통해 사이버안보 수행체계를 국가 차원에서 정비하는 한편, 2015년에는 향후 3년간의 정책 방향을 제시한 사이버 보안전략을 마련하였고, 2018년에는 이를 대신하는 새로운 사이버안보전략을 발표하였다. 자국을 서방 선진국의 일원으로 생각하는 일본은 외무성을 중심으로 적극적으로 국제적 논의에 참여하여 각국과의 사이버협력을 강화하고 사이버 규범을 형성하는 모습을 보이며, 특히 G7으로 대표되는 기본적 가치관을 공유하는 국가들과의 협력을 통해 사이버공간에 대한 규범 논의를 주도해 나가고 있다. 2018년 발표된 신방위대강에서는 일본 방위에 있어 사이버·우주·전자파 등과 같은 첨단 군사 분야에서의 방위력 강화가 사활적으로 중요하다고 명기하는 한편 적극적 사이버 방위를 내세워 사이버공격에 대한 반격권 행사를 인정함으로써, 전수방위의 허용한계를 넘어서는 듯한 공세적 대응에 나서고 있다. 이는 주변국의 측면에서 볼 때 자위대의 군사적 역할 확대와 관련된 민감한 부분이기 때문에 향후 일본의 법적 기반 검토과정을 예의 주시해 나가면서 이것이 한반도에 가져올 파장에 대한 검토와 대비가 필요하다.

중국은 그동안 선진국에 비해 사이버 영역의 기술적 발전 속도가 상대적으로 뒤처져 있었다. 그러나 시진핑(習近平) 집권 이후 사이버공간에 대한 중요성을 인식하고 사이버역량을 강화하는 데 집중하고 있다. 내부적으로 국내 정치의 안정성 유지를 위한 정책 설정

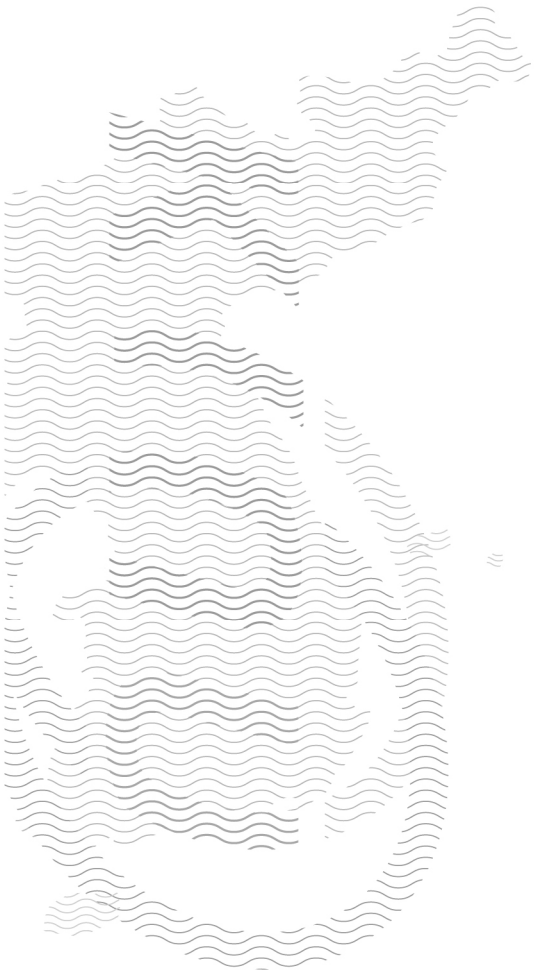
을 진행함과 동시에 대외적으로 서구사회와의 규범 경쟁 상황을 대비하는 전략까지 포괄하고 있다. 중국은 현재 미국을 중심으로 한 서구 국가들로부터 경계와 의심의 대상이 되고 있는데 이는 1990년대 초반 불거진 중국 위협론과 궤를 같이한다. 따라서 한국은 서구의 시각이 향후 중국의 사이버 영역에서의 행태와 어떤 상관성이 있을지 정확하게 진단하고 분석할 필요가 있다.

러시아는 사이버공간을 주권이 미치는 전략영역으로 인식하기 때문에 가상공간에서 생성·유통되는 정보에 대한 국가의 영향력을 보장받으려 하고 대외적으로는 사이버공간을 국가의 이익과 영향력을 확대하는 수단으로 적극적으로 활용하고 있다. 러시아는 사이버공간의 핵심요소를 정보가 생성·유통되는 공간으로 인식하고 있다. 따라서 무분별한 정보에 대한 관리 및 통제 기제가 필요한 정보 주권을 강조하게 될 수밖에 없다. 사이버공간에서 정보의 자유로운 유통을 강조하는 서구 중심적 인식과 공공안전을 우선해 정보 주권을 강조하는 러시아의 인식은 정면으로 배치되고 있다.

따라서 본 연구는 국경안보의 연장선상에서 남북한 및 미·일·중·러 주변국들의 사이버공간에 대한 인식, 전략, 국제협력 등 사이버 환경을 살펴봄으로써 사이버영역에서의 한반도 평화체제 구축을 위한 전략과 과제를 제시하고자 한다. 이를 위해 2장에서는 국경안보 개념의 확장과 사이버공간에서의 주권 개념을 통해 국경안보와 사이버공간의 연계성을 살펴본다. 3장과 4장에서는 한반도 주변국의 사이버 영역에 관한 발전과 전략 분석을 위해 남북한 및 미·일·중·러를 중심으로 사이버공간에서의 새로운 전략과 발전방안을 추적, 관찰한다. 5장에서는 한반도 사이버안보 협력의 전략과 과제를 모색하기 위해 주변국들의 사이버안보 정책 변화에 대한 대응을 살펴보고, 한반도 사이버 평화체제를 제안한다. 또한 이 과정에서 새로운

규범의 확립과 경쟁에 대비한 정책을 수립하기 위해 불안정한 사이버공간의 확장과 이에 기초한 위기와 갈등을 해결할 수 있는 평화적 규범 수립에 관한 정책 방안도 제시한다. 이를 통해 본 연구는 통일한국의 주권 공간 확대를 위한 선도적 연구로서, 글로벌 차원에서 우리의 통일 기반 구축뿐만 아니라 평화·번영의 한반도 형성에도, 기여할 수 있을 것이다.

Ⅱ. 국경안보와 사이버공간



1. 국경안보 개념의 확장과 사이버공간

가. 사이버공간의 정의와 인식

현재 사이버공간은 매우 다양한 형태로 이해되고 또 개념화되고 있으며, 여전히 많은 논의가 진행되고 있다. 사이버공간의 특징은 보통 다음과 같다. 첫째, 현실의 공간이 처음부터 주어진 것이었다면 사이버공간은 물질적이면서 동시에 비물질적인 성격을 갖는 인간의 창조물이다. 둘째, 사이버공간은 인류가 지금까지 경험하지 못했고 또 예측하기 힘든 방식으로 진화하고 있다. 셋째, 사이버공간은 단지 하나의 공간으로만 존재하는 것이 아닌 현실 세계와 중첩되어 있고 또 상호작용한다. 넷째, 사이버공간의 행위자는 국가를 비롯하여 개인, 기업 등 다양하며 이들은 각각 또는 동시적으로 상호작용하면서도 물리적으로는 실체를 갖지 않는다. 다섯째, 모든 사회가 고유한 질서가 있듯이 사이버공간도 기존 현실 사회의 중추 기능을 그대로 나타내는 질서를 보유하고 있다. 따라서 이러한 특징들로 인해 사이버공간을 정의하거나 이해하기 위해서는 기술적 문제뿐만 아니라 정치, 경제, 사회, 문화적 문제도 함께 이해해야 한다. 그런데 사이버공간이 현실 세계와 같이 정치, 경제, 사회, 문화 등 인류의 삶의 문제와 밀접히 연결 또는 중첩되면서 하나의 권력 공간으로서 변화하기 시작했다.

사이버공간은 영토, 영공, 영해, 우주와 마찬가지로 새로운 안보 위협이자 기회의 공간이 되고 있다. 그러나 본질적으로 사이버공간은 그 추상성으로 인해 명확하게 개념을 정의하기는 어렵다. 사이버공간에 대한 주요 선진 국가 및 국제기구의 정의들은 이러한 문제를 잘 나타낸다. 대표적으로 미국의 2011년 「사이버공간정책검토」에서

사이버공간은 '정보기술기반시설의 상호의존적인 네트워크'로 정의된다.[2] 한편 북대서양조약기구(North Atlantic Treaty Organization: NATO)의 '탈린 매뉴얼'에 따르면, 사이버공간은 '물리적, 비물리적 요소를 통해 만들어진 컴퓨터 네트워크를 통하여 컴퓨터와 전자적 스펙트럼을 이용한 정보의 변경·저장·교류로 특징지어지는 환경'이다.[3] 또한 '국제전기통신연합(International Telecommunication Union: ITU)'에 따르면, 사이버공간은 '인터넷·컴퓨터 네트워크·전기통신에 직·간접적으로 연결된 시스템 및 서비스'로 정의된다.[4] 요컨대 사이버공간은 물리적 제약과 관계없이 네트워크상에 구축된 가상의 공간이다. 개인, 사회, 국가 전반에 연결된 정보 인프라와 실제 생활에 사용되는 모든 정보를 포괄한다.

각 국가 및 국제기구들의 사이버공간 정의에서 보았듯이 사이버공간 개념과 관련하여 사이버공간과 현실세계의 경계에 있어서의 모호성으로 인해 사이버공간을 가상공간 영역으로 제한할 것인지 아니면 물질적 기반을 포함하여 사이버공간으로 정의할 것인지 하는 문제가 제기된다. 즉 사이버안보의 대상이 전자적 수단에 의한 정보통신망 공격에 한정되는 것이 아니라 네트워크와 정보통신 시스템, 그리고 이를 통해 처리되는 정보와 이를 기반으로 형성되는 사회적 관계까지 전반적으로 포함시킬지 하는 문제이다. 사이버공간의 의미를 폭

2) White House, "Cyberspace Policy Review," 2011, 〈https://obamawhitehouse.archives.gov/assets/documents/Cyberspace_Policy_Review_final.pdf〉 (Accessed April 3, 2013), p. 1.

3) Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare: prepared by the International Group of Experts at the invitation of the NATO Cooperative Defence Centre of Excellence* (Cambridge: Cambridge University Press, 2013), p. 258.

4) ITU, "National Cybersecurity Strategy Guide," 2011, 〈http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf〉 (Accessed October 11, 2019), p. 5.

넓게 해석할 경우 정보통신기반시설에 대한 물리적인 공격은 그 자체로 사이버공간에 대한 직접적인 침해가 되기 때문에 사이버안보의 필수적인 구성요소가 된다. 반면에 사이버공간의 의미를 좁게 볼 경우에는 이러한 물질적 기반에 대한 침해는 물리적 공격에 따라 나타나는 결과로서 간접적으로 사이버공간의 안전을 위협하는 것이 되어 이에 대한 대응조치까지도 사이버안보의 구성요소로 포함시킬 것인지 하는 문제가 발생하기 때문에 논란의 여지가 있다. 실제로는 사이버공간을 가상공간으로 제한하여 규정하는 국가들조차도 정보통신기반시설에 대한 물리적 공격이 사이버공간의 안전을 침해하는 것으로 간주하여 이에 대한 예방 및 대응조치를 요구하고 있는 상황이다. 결국 이는 사이버공간이 가상공간과 현실공간과의 통합으로 간주되어야 한다는 점을 보여주고 있는 것이다.[5)]

사실상 사이버공간은 현실공간과 별개로 존재하고 있는 것이 아니라 물질적 기반시설과 단말기 등을 통하여 연결되어 있다. 사이버공간은 인터넷을 중심으로 하는 컴퓨터 및 네트워크를 기반으로 하여 형성된 가상의 정보 처리 공간이므로 사이버공간은 물질적 실체 여부에 관계없이 컴퓨터 및 정보통신망을 통하여 정보를 처리할 수 있는 모든 네트워크와 시스템을 포함하고 있다.[6)] 사이버공간은 현실공간과 명확히 구별되지 않을 뿐만 아니라 현실의 일상생활 영역과도 점차 일치해가고 있다. 즉 사이버공간은 가상공간인 동시에 현실공간의 일부가 되어 가고 있으므로 현실세계와 유기적으로 연결된 개념인 것이다. 이 경우 사이버안보는 정보통신기반시설에 대한 위협과 정보통신기반시설을 바탕으로 형성된 네트워크 및 정보통신시스템에 대한 위협으로부터 이들의 안전을 보장하는 조치와 행동

5) 채재병, “안보환경의 변화와 사이버안보,”『정치·정보연구』, 제16권 2호 (2013), p. 182.

6) 위의 글, p. 182.

으로 규정될 수 있다.[7]

이를 따르면 사이버공간에 대한 침해는 좁게는 사이버공간에 대한 직접적 침해와 사이버공간의 원활한 작동을 가능하게 하는 기반시설에 대한 침해로 구성되는 간접적 침해로 구분할 수 있다.[8] 또한 사이버공간에 대한 침해는 전자적 수단에 의한 사이버공격에 국한되지 않고 기타 물리적 수단에 의한 침해 역시 포함한다.[9] 구체적으로 직접적 침해에는 사이버공격은 물론 정보통신설비에 대한 물리적 공격이 포함된다.[10] 간접적 침해는 사이버공간을 지탱하는 주요 정보통신기반시설 또는 관련된 일반적인 사회기반시설에 대한 공격의 결과로 발생하는 위협을 지칭한다.[11] 예를 들어, 주요 정보통신기반시설의 범위에는 케이블·라우터 등의 전산설비만을 포함시킬 수도 있지만 이들의 작동을 가능하게 하는 전력시설 등의 시설 역시 포함시킬 수 있는데, 이들은 직접적으로 사이버공간을 구성하지는 않지만 이들에 대한 침해는 사이버공간의 안전에 대한 결정적 위협이 될 수 있다는 점에서 사이버안보의 대상이 된다는 것이다.[12]

이처럼 사이버공간에 대한 정의는 논쟁적이며 여전히 국제적으로 합의를 이루지 못한 상태이다. 하지만 분명한 건 현실 세계와 사이버공간이라는 가상 세계의 경계가 무너지고 있으며 나아가 그 상호의 존성도 높아지고 있다는 것이다. 따라서 이는 그만큼 사이버 위협에 대한 취약성이 더 증대되었다는 것, 즉 사이버안보의 중요성이 더 커졌다는 것을 의미한다.

---

7) 위의 글, p. 182.
8) 위의 글, pp. 182~183.
9) 위의 글, p. 183.
10) 위의 글, p. 183.
11) 위의 글, p. 183.
12) 위의 글, p. 183.

국제정치에서 주목하는 영역 갈등, 분쟁과 평화는 사이버공간에서도 존재한다. 또한 사이버공간에서의 제도화의 가능성도 진행되고 있다. 국경갈등과 마찬가지로 사이버 갈등도 심화되고 있다. 주변국도 동일한 상황에 놓여있으며 사이버공간에서의 통일 환경 구축을 위한 노력도 필요하다. 이번에 공표된 '국가사이버안보전략'에 따르면, 사이버 억지를 통한 '한반도 사이버 평화체제'[13] 구축을 목표로 추진되고 있다. 이미 국제사회는 4세대 전쟁 시기에 진입했으며 일본의 경우 육·해·공·우주·사이버 영역에서의 방어체제 구축을 시도하고 있고, 중국도 마찬가지로 육·해·공·천·전 개념을 통해 5개 영역에서의 방어체제를 구축하고 있다. 즉 국가안보 차원에서 국경안보가 논의되는 것과 마찬가지로 사이버안보도 국가안보 및 국경안보 차원에서 논의될 수 있는 것이다. 다음으로 국경안보 차원에서의 사이버안보 논의를 국경안보 개념의 확장이라는 측면에서 살펴본다.

나. 국경안보 개념의 확장

국경안보는 국가주권과 그 영향력을 지금처럼 유지하거나 보다 더 확장하기 위한 포괄적인 전략의 일환으로 단순한 국경관리의 차원을 넘어서는 것이다. 국경안보는 육·해·공에서의 국경 관련 위협들에 대한 억제와 안전보장 및 육상, 항만, 공항 등 모든 국경 출입 지역의 안전 강화를 의미한다. 더 나아가 인접국과의 분쟁 방지 및 해소, 국경 지역의 발전과 안정을 위한 군사·경제적 정책을 모두 포괄하고 있다. 유럽안보협력기구(Organization for Security and

13) '한반도 사이버 평화체제'는 아직 확정된 개념은 아니며, 본 연구에서는 한반도 평화체제의 부분 또는 확장이라는 측면에서 사이버공간에서의 한반도 평화를 위한 하나의 레짐으로 이해한다. 따라서 여기에는 한반도와 주변국들의 사이버공간에서의 국제협력과 규범에 방점이 주어진다.

Co-operation in Europe: OSCE)의 국경안보 및 관리 상황을 살펴보면, 2005년 류블랴나에서 개최된 각료이사회에서 유럽안보협력기구 국경안보 및 관리개념을 채택하였다. 이는 유럽안보협력기구 회원국 간에 발생하는 합법적인 국경활동을 촉진시키고 회원국의 국경안보 및 국경관리 능력을 제고하기 위한 것이었다. 주로 우즈베키스탄, 투르크메니스탄, 타지키스탄 등 중앙아시아의 유럽안보협력기구 회원국에서 대아프가니스탄 마약밀매 근절 등 국경 통제 사업으로 진행되고 있다.

국경이라는 현실공간은 기술을 매개로 현실보다도 더 현실과 배접해 있는 가상현실의 공간과 결합하여 인류 전반에 걸친 새로운 공간 네트워크를 구현해내고 있다. 불가분의 두 공간은 확장된 공간의 크기보다도 더 큰 갈등과 위기의 가능성을 내포하고 있는 것이다. 다시 말해 국경안보 차원에서의 사이버안보 논의는 사이버공간이라는 새로운 안보영역이 현실공간에서의 국경과 같은 접점을 포함하고 있으며 국경안보와의 상관성을 갖고 있다. 물론 현실공간에서의 국경안보 개념은 사이버공간의 특수성으로 인해 그대로 적용될 수는 없으나 국경이 주권과 주권이 충돌하는 지점이라는 논리의 연장선상에서 보면 사이버공간에서도 주권 충돌의 지점이 존재하므로 국경안보 개념의 확장을 통해 국경안보 차원에서의 사이버안보 논의가 가능한 것이다.

이와 같은 국경안보 개념의 확장은 최근 나타나고 있는 안보개념 변화와 일맥상통한다. 안보개념 변화의 시작은 국제사회에 냉전이 종식된 이후 안보에 대한 변화된 인식으로부터 비롯되었다고 할 수 있다. 이러한 안보인식의 변화는 다음과 같은 세 가지 측면에서 살펴볼 수 있다. 첫째, 안보의 대상 즉 위협의 주체가 무엇인지, 무엇으로부터 안전을 보장해야 하는 것이냐에 대한 인식의 변화이고, 둘째, 안보

의 내용 즉 위협으로부터 보호되어야 할 영역이 무엇이고 어디까지냐에 대한 인식의 변화이고, 셋째, 안보의 추구방법 즉 위협의 방지와 대처를 위한 방법 및 수단이 무엇이냐에 대한 인식의 변화이다. 이 세 가지 측면을 구체적으로 살펴보면, 안보의 대상이라는 측면에서는 외부의 적으로부터 주권과 영토, 국민의 생명과 재산, 국가이익 등에 대한 보호라는 과거의 국가 중심적 시각에서 기근, 질병, 환경오염, 마약밀매, 테러리즘, 종족갈등 등 초국가적인 성격의 위협으로부터의 보호로 변화했다. 안보의 내용이라는 측면에서는 이러한 초국가적인 성격으로 인해 물리적인 힘을 사용하는 군사적 안보에 더해 이외에도 경제안보, 사회안보, 환경안보, 인간안보 등을 모두 포함하는 포괄안보로 인식이 변화했다. 안보의 추구방법이라는 측면에서는 위협에 대처하기 위한 각 국가별 또는 동맹 체제를 통한 힘에 의존한 안보에서 초국가적인 위협에 대응하는데 필수적인 관계국들 간에 협력하는 협력안보로 변화했다. 요컨대 국가 중심적이고 군사력에 의존하는 전통적인 안보로부터 초국가적이며 비군사적인 요소까지 포함하는 비전통적인 안보로 변화한 것이다.[14]

이는 냉전 이후 국제사회에서 냉전으로 인해 드러나지 않던 종교·인종·문화·영토·자원 등을 둘러싼 국가 간 분쟁이 표출되면서 테러의 확산, 국제적인 범죄의 증가, 난민의 발생, 환경문제의 등장, 대량살상무기의 확산 등과 같은 초국가적인 위협요인들이 크게 나타났기 때문이다. 그리고 이같이 국제안보환경의 변화로 새로운 사회적 문제들이 국가안보를 위협하고 있는 상황에서는 이에 부합하는 포괄안보개념이 크게 요구되었던 것이다.[15] 이에 따라 냉전 이후 국

14) 채재병, "국제테러리즘과 군사적 대응," 『국제정치논총』, 44집 2호 (2004), pp. 59~60.

15) Richard N. Haas, "Paradigm Lost," *Foreign Affairs*, vol. 74, no. 1 (1995), pp. 43~58.

제사회에는 전통적인 군사문제 외에 자원·생태·무역·경제·사회·테러리즘·초국가적 범죄·환경·인도주의 등을 대상으로 하는 포괄안보가 주요 안보개념으로 자리 잡게 되었다.[16] 즉 냉전기의 안보개념이 군사방위와 유사한 의미의 군사적인 차원에서의 외부적 위협에 대한 대응이었다면, 냉전 이후에는 여기에 더해 경제·자원·환경·사회문제 등 비군사적인 요소들을 포괄하는 개념으로 변화한 것이다.[17] 이제 안보는 일반적으로 정부의 책임으로 인식되면서 국가 및 시민의 핵심적 가치가 대내외로부터 위협받는 상황을 방지하여 심리적으로 뿐만 아니라 물리적으로도 안전을 유지하는 것으로 인식되었다.[18]

포괄안보 개념은 통상 전통적인 군사안보와 비군사안보적 요소를 포괄하여 종합적으로 안보정책을 추진해야 한다는 점에서 비전통적인 안보개념으로 간주된다. 다시 말해 포괄안보는 군사안보와 비군사안보 간의 적절한 조화를 통해 안보정책목표를 효과적으로 달성하고자 하는 것이다.[19] 이러한 포괄안보 개념을 통해 안보의 범위나 영역은 크게 확대되었고 이제 안보는 개인·지역·체제와 밀접히 연계되어 정치와 군사뿐만 아니라 사회·경제·환경 등 각 분야를 포괄하지 않고서는 전혀 이해할 수 없는 개념이 되었다.[20] 그러나 이와

16) Carolyn M. Stephenson, "New Approaches to International Peacemaking in the Post-Cold War World," in *Peace & World Security Studies: A Curriculum Guide*, ed. Michael T. Klare (Boulder: Lynne Rienner Publisher, 1994), p. 18.

17) Kanti Baipai, "The Idea of Human Security," *International Studies*, vol. 40, no. 3 (2003), p. 223.

18) Robert Mandel, *The Changing Face of National Security: A Conceptual Analysis* (Connecticut: Greenwood Press, 1994), pp. 18~19.

19) 채재병, "국제테러리즘과 군사적 대응," p. 60.

20) Barry Buzan, *People, States, and Fear: An Agenda for International Security Studies in the Post-Cold War Era* (Colorado: Lynne Rienner Publisher, 1991), p. 363.

같은 안보개념의 변화는 동시에 안보의 개념 및 목표를 더욱 불투명하게 만들었다고 할 수 있다. 즉, 위협의 주체가 다양화되고 위협요인 또한 다양한 분야로 확대됨에 따라 어떤 대상에 대해 어떻게 대응하고 어떤 분야에 더욱 중점을 두어 안보목표를 설정해야 할지가 훨씬 더 복잡해지고 모호해진 것이다.[21] 사실상 국경안보 개념도 이와 같은 안보 개념의 변화에 토대를 두고 있다.

사이버안보도 이러한 범주에서 출발하고 있다. 사이버위협은 냉전 종식 이후 안보개념의 변화 속에서 비약적인 정보통신기술의 발전에 기인하여 부각된 새로운 안보위협이라고 할 수 있다. 실제로 지금까지 사이버안보에 대한 논의는 이상에서 언급한 안보개념 논의 과정에 따라 유사한 경로를 통해 전개되어왔다. 안보의 대상, 내용, 추구방법 측면에서의 변화 양상이 사이버안보의 양상과 거의 일치하고 있는 점 때문이다. 또한 사이버위협은 테러리즘과 사실상 거의 흡사한 속성을 갖고 있다. 테러리즘과 마찬가지로 공격과 방어에 있어 비대칭성을 갖고 있다는 점이 가장 두드러진 특징이다. 이것이 처음 사이버위협이 발생했을 때 사이버테러라고 안보이슈화 되었고 아직까지도 포괄적인 테러리즘의 영역에서 사이버위협이 주로 다루어지고 있는 이유이기도 하다. 그리고 사이버위협, 즉 사이버공격의 주체가 개인·집단·국가 등으로 다양하고 그로 인한 피해가 매우 크다는 것도 상당히 유사한 점이다. 따라서 지금까지 사이버위협에 대한 논의는 그 유사성으로 인해 주로 테러리즘의 영역에서 사이버테러라는 개념을 통해 주로 논의되어 온 것이 사실이다. 그러나 앞으로 사이버안보에 관한 논의는 새로운 방향에서 전개될 가능성이 매우 크다. 왜냐하면 사이버안보는 가상공간이라는 영역을 갖고 있어 기존에 논의되는 안보영역과는 완전히 별개의 새로운 영역이기 때문

21) 채재병, "국제테러리즘과 군사적 대응," p. 61.

이다. 또한 사이버안보라는 문제는 국가안보적 차원에서 다루어져야 하고, 그 대처방법이나 수단에 있어서도 군사적 수단과 비군사적 수단이 같이 사용되어야 하고, 이를 효과적으로 구사하기 위해서는 국제적인 협력도 해야 한다는 점에서 안보개념의 확대와 그로 인한 안보개념의 재정립이라는 측면에서 접근해야 한다고 할 수 있다.[22] 이러한 사이버안보의 특성이 국경안보 개념의 확장과 사이버공간과의 연계를 설명해주고 동시에 사이버공간에서의 국경안보 개념 정립의 근거를 제공해주는 것이다. 앞서 언급했듯이 사이버공간에서의 국경안보 개념의 적용이 똑같을 수는 없으나 안보개념의 재정립이라는 측면에서 보면 사이버공간과 국경안보의 상관성 도출이 가능한 것이다.

2. 사이버공간에서의 주권

주권 개념의 발달은 개별 국가들 간의 상이한 이해관계를 조정하고 안정적인 국제관계를 유지하는 데에 필수적이다. 유럽연합(European Union: EU)의 출현은 주권 개념의 적극적인 확대와 국내외적 이슈들에 대한 탈주권적 해석이 선택적 사안들에 의해 이루어짐으로써 가능했다. 탈냉전적 국제정치 상황은 국가들로 하여금 그들이 인식하고 있는 주권의 개념적 구성에 대해 고민하게 했다. 중국의 부상에 대비한 미국의 헤게모니 프로젝트 조정, 미일동맹의 새로운 도약, '하나의 중국(One China Policy)'을 바라보는 각 국의

22) Joseph S. Nye Jr., "Power and National Security in Cyberspace," in *America's Cyber Future: Security and Prosperity in the Information Age*, vol. Ⅱ, ed. Kristin M. Lord (Washington D.C.: Center for a New American Security, 2011), p. 9.

입장 등의 사례들에서 알 수 있듯이 국제관계의 가변적 요인들은 국가들 간의 안정적인 국제관계 출현을 절실히 요구하고 있는 시점이다.

주권은 규범적 요인과 실천적 요인을 동시에 갖고 있는 역사적 산물이다.[23] 주권은 권력, 합법성, 질서, 권위 등과 같은 정치적 개념들로 이루어져 있으며 정치적 결사체인 국가의 출현과 함께 발전하였다.[24] 국제정치학적으로 주권은 '국제사회를 구성하는 자격의 부여'로 이해할 수 있는데 그렇다면 국가들에게 주권개념의 내재화와 현실적 체험은 곧 국제사회로의 편입의 역사와 과정을 의미한다.

주권이 가지는 가장 대표적인 웨스트팔리안(Westphalian)적 전통인 '대내적 대중성(internal popularity)'과 '대외적 합법성(external jurisdiction)'은 시간적·공간적 차원에서 다양한 사건들을 통해 개념적 발달을 촉진시켜왔다.[25] 세계화적 현상들의 심화로 인해 주권의 개념적 변화가 예상되는 오늘날의 시점에서 보면 주권개념의 역사적 변천, 동서양 간 적용의 차이, 국제사회에 투영된 유형 등이 중요하다. 안정적인 국제관계의 창출을 위해서는 국제적인 수준에서의 제도화가 이루어지고 국가들 간의 다양한 이슈들을 논의할 수 있는 초국가적인 제도들의 등장이 필수적이다.

주권의 개념화 작업은 역사적 변천을 경험하였다. 역사적 변천은 국가기구의 강화와 국제사회의 확산이라는 두 개의 작동원리가 상호작용하면서 구체화되었다. 주권 연구자들은 이러한 구체화를 대내적 주권의 확보와 대외적 주권의 확보로 이해한다.[26] 대내적 주권

---

23) Joseph A. Camilleri and Jim Falk, *The End of Sovereignty?* (Aldershot: Edward Elgar, 1992), p. 12.

24) Jens Bartelson, *Genealogy of Sovereignty* (Cambridge: Cambridge University Press, 1995), pp. 53~87.

25) Stephen D. Krasner, *Sovereignty: Organized Hypocrisy* (Princeton: Princeton University Press, 1999), pp. 3~10.

이 경험성과 대중성을 바탕으로 한 얻어지는 지위로서의 의미를 강조한다면, 대외적 주권은 국제질서 속에서 합법성과 독립성을 강조하는 주어지는 지위로서의 의미를 가진다. 이런 연유에서 전자는 경험적 주권으로 그리고 후자는 합법적 주권으로 이해되면서 각각 독립적인 이론적 정체성을 확보하게 되었다.

주권 개념의 정착은 국가 기구의 확대와 자본주의 세계질서의 확대로 압축된다. 유럽 국가들 사이에서 국제적, 법적 질서의 기초를 제공한 웨스트팔리아조약(Treaties of Westphalia)이 등장한 이후 세력균형을 위해서 주권이 침해를 당하는 경우도 있었고, 또 때로는 주권을 대신하는 새로운 개념을 만들기 위한 지적 노력이 있었던 것도 사실이지만, 궁극적으로 유럽은 물론 전 세계적으로 국가들에게 부여된 절대적인 세속적 권위를 상호 인정함으로써 주권 개념은 국제사회의 다양한 현상들을 설명하는 핵심 담론으로 기능하였다. 역사적 경험의 산물로서 주권은 국제사회의 구성적 특성을 결정하는 주요 요인으로 작용하였다.[27)]

탈냉전기적 주요 전쟁의 성격을 규정하고, 전쟁 발생의 핵심적인 원인들이 가지는 안보부재(insecurity)의 제공이 웨스트팔리아적 주권 개념의 확보로는 설명될 수 없다는 전제하에 새로운 주권 개념의 인식론적 토대에 대한 분석이 요구된다. 탈냉전기 전쟁의 유형과 원인은 전통적인 주권국가의 정체성과 국제안보 확보의 근거인 소위 '절대적 주권(Absolute Sovereignty)'으로는 이론적인 포착이 불

---

26) Walter C. Opello and Stephen J. Rosow, *The Nation-State and Global Order: A Historical Introduction to Contemporary Politics* (Boulder, CO: Rienner, 1999), pp. 1~13.

27) Samuel J. Barkin and Bruce Cronin, "The State and the Nation: Changing Norms and the Rules of Sovereignty," *International Organization*, vol. 48, no. 1 (1994) p. 108; Thomas J. Biersteker and Cynthia Weber, eds., *State Sovereignty as Social Construct* (Cambridge: Cambridge University Press, 1996), p. 11.

가능하다. 웨스트팔리아 체제는 주권을 중심축으로 한 국제관계의 근대성을 정착시킨 인류사적 상징성을 가짐과 동시에 국내 영역과 국제 영역의 분리를 통한 독자적인 차별성을 부여하였다. 주권의 존재론(ontology)에 대한 이론화는 무정부상태를 중심으로 이루어졌다. 무정부상태의 역사적 모델은 서구의 주권국가체제였고, 주권국가의 형성과정은 역사적 경험에서 알 수 있듯이 무수히 많은 다양한 형태의 전쟁을 통한 대중적 합의의 확보과정이다.[28] 따라서 근대 국제질서체제하에서의 전쟁 수행이 가지는 일차적인 함의는 웨스트팔리아적 주권개념의 실천이라는 차원에서 이해할 수 있다. 하지만 현실과 이론의 영역 모두에서 웨스트팔리아적 주권개념은 도전 받고 있으며 이러한 현상은 소위 '세계화'로 불리어지는 탈냉전기에 들어 더욱 가시화되고 있다.

웨스트팔리아적 주권은 영토(territory), 인구(population), 권위(authority), 인정(recognition)을 핵심 구성요소로 포함하면서, 사법적 독립권, 대외적 배타성, 대내적 권위의 인정, 상호의존적 규제 등의 형태로 주권 실현의 근거를 확보하였다.[29] 탈냉전적 국제관계는 이러한 전통에 커다란 변화를 가져왔다. 전통적으로 전쟁의 발생을 포함한 국제사회의 안보부재를 야기하는 위협요인들은 이러한 주권의 정체성이 얼마나 침해받느냐의 문제로 환원된다.[30] 탈냉전기적 국제질서의 등장은 주권과 전쟁간의 이러한 인과관계에 대한 전면적인 재수정을 요구하고 있다. 새로운 인종, 테러, 종교, 레짐 붕괴, 빈곤, 인권, 대량살상무기 등으로 대표되는 새로운 안보위협

---

28) Charles Tilly, *Coercion, Capital and European States AD 990–1900* (Oxford: Basil Blackwell, 1990). pp. 20~28.

29) Stephen D. Krasner, *Sovereignty: Organized Hypocrisy*, pp. 3~10.

30) J. G. Ruggie, "Territoriality and Beyond: Problematizing Modernity in International Relations," *International Organization*, vol. 47, no. 2 (1993). pp. 139~174.

의 등장은 필연적으로 웨스트팔리아적 주권개념의 변화와 이의 결과로서 새로운 전쟁 발발 요인들을 제공하고 있는 현실이다.

주권과 안보는 국제관계 연구를 지배해온 가장 핵심적인 개념적 지표들이다. 웨스트팔리아적 개념에 의거하면 주권은 영토와 인정이 정당화되고, 특정한 영토에 한정해서 사회통합을 이루어낼 수 있는 정치적 통제, 권위체의 존재를 의미하는 권위, 그리고 인구의 완비를 의미한다. 이러한 전통은 근대국제체제의 완성 및 발전을 규준하는 근간으로 작동하였다. 다시 말해 국제관계의 근대성은 정치적 지배에 있어서 독특한 영토성으로 규정될 수 있다. 자본주의적 성장을 가장 효율적으로 견인할 수 있었던 국가라는 지배형태는 일정한 공간적 영역의 통제에 기초하였고 그 공간의 부족에서 야기하는 권위의 보충은 국제사회의 확산을 통해 이루어졌던 것이다.[31]

모든 전쟁의 성격에는 주권에 대한 개별 국가의 대내적 합의의 전통이 있었고 동시에 국제관계적 차원에서의 대외적 인정의 규범이 있었다. 근대국제체제 형성 이후 이것을 웨스트팔리아적 주권 개념으로 이해한다. 현실과 이론으로서의 웨스트팔리아 주권은 모두 도전 받고 있다. 경제단위로서의 국가, 개인의 정체성을 독점하는 국가, 안보를 제공하는 주체로서 국가의 능력, 전 지구적 문제에 있어서 국가의 윤리적 책임, 제한된 영토 내의 민주주의 존속 가능성 등 기존의 국내-국제, 정치-경제 구분, 전통적인 안보와 국제법 개념으로는 충분히 설명할 수 없는 변화들이 발생하고 있기 때문이다.[32]

웨스트팔리아적 주권이 가지는 가장 중요한 함의는 국민을 전제로

---

31) Jens Bartelson, *Genealogy of Sovereignty*. pp. 53~87.

32) Ian Clark, "Beyond the Great Divide: Globalization and the Theory of International Relations," *Review of International Studies*, vol. 24, no. 3 (1998); Claire Cutler, "Critical Reflections on the Westphalian Assumptions of International Law and Organization: A Crisis of Legitimacy," *Review of International Studies*, vol. 27, no. 1 (2001), pp. 133~150.

하여 일정한 정치체의 경계 내에서 효율적인 통제를 할 수 있는 공적 권위체의 능력과 국내의 공식적인 정치적 권위조직을 의미하고, 이를 전제로 한 국제관계의 대외적 배타성의 원리가 상호 인정되는 관행이다. 이런 관점에서 보자면 웨스트팔리아적 주권 개념의 충실한 해석은 절대적 주권에 대한 상호 보장인 셈이다. 세계화적 국제관계로 압축되는 오늘날 국제사회의 관행으로 보자면 이러한 주권 개념은 소위 웨스트팔리아적 족쇄로 볼 수 있다. 생태적 환경 보존의 문제, 국제 금융의 관리, 지구적 자본주의의 안정성 확보, 유럽에서의 주권 통합을 위한 실험 등으로 표현되는 오늘날 국제사회의 주요 현안들은 명백히 서구 근대국제체제의 역사적 정체성을 확보해주었던 웨스트팔리아 주권 개념의 변화를 의미하기 때문이다.

안보는 위협의 부재를 의미한다.[33] 근대국제체제 특히 전후 냉전기 국제질서에서 위협의 부재는 웨스트팔리아적 주권 개념의 존중을 전제로 하였다. 전쟁수행과 관련한 대내적 합의는 전통적 주권 개념의 파괴에서 일차적인 정당성을 확보하였고, 그것이 국제사회에 반영되는 과정도 개별 주권에 대한 대내적 질서와 대외적 독립성에 대한 인정을 근거로 한다. 따라서 국제안보 확보를 위한 국제사회의 가장 중요한 합의는 주권에 대한 존중이라고 볼 수 있을 것이다. 하지만 탈냉전기 국제안보는 이러한 합의에 근본적인 변화를 가능케 한다. 즉, 웨스트팔리아적 주권 개념에 근본적인 변화가 야기되고 있다면, 그것은 결과적으로 주권 개념이 국제안보적 차원에서 구체화되는 실천양식의 변화를 의미하고 동시에 전쟁 발발의 요인 및 개별 사회구성원들과 국제사회가 정당화하는 전쟁 수행의 근거도 변화하는 것이다.

---

33) Barry Buzan, *People, States, and Fear: An Agenda for International Security Studies in the Post-Cold War Era,* p. 7.

국제안보를 위협하는 안보부재는 인종, 빈곤, 종교, 대내적 권위의 부재, 석유자원 등 다양한 차원으로 나타나고 있다. 이러한 현상들은 소위 세계화적 변화의 원인일 수도 있고 동시에 결과로서 평가할 수도 있을 것이다. 문제는 탈냉전기적 공간에서 발생한 전쟁의 원인들은 웨스트팔리아적 관점에서 설명하자면 주권의 대외적 독립성에 대한 실질적 부정을 전제로 하고 있다는 점이다. 웨스트팔리아적 주권 개념은 근대국제질서를 규준함은 물론 이러한 규준을 바탕으로 한 국제안보에 대한 합의의 주요한 근간을 이루었다.

이러한 주권개념이 사이버공간에서도 통용되는가? 그리고 사이버공간에서의 주권 개념이 국경안보에서의 주권 개념과 어떠한 공통점과 차이점이 있는가? 이에 대한 답을 하기 위해서는 앞서 설명한 포괄안보 차원과 안보개념의 확장이라는 측면에서 국경안보와 사이버안보를 살펴볼 필요가 있다. 일반적으로 사이버안보란 사이버공간을 사이버공격으로부터 보호하는 것이라고 할 수 있다. 따라서 사이버공간에 대한 다양한 주체와 수단을 통한 공격으로부터 국가와 국민을 보호하기 위한 즉 사이버공간을 안정적으로 유지하고 방어하기 위한 수단들의 총합이라고 할 수 있다. 그런데 현실적으로 사이버안보 개념을 논의하는 것은 매우 어렵다. 왜냐하면 사이버라는 용어가 매우 추상적인 개념이라 현실세계에 적용하기가 쉽지 않기 때문이다. 실제로 사이버라는 용어는 컴퓨터나 인터넷 등의 정보통신기술과 이를 기반으로 하는 정보통신망, 그리고 이를 통해 구현되는 가상공간과 관련된 모든 것을 의미한다. 이러한 사이버의 추상적인 성격은 사이버공간과 현실세계의 경계를 매우 모호하게 만들었다. 그리고 이러한 모호성은 사이버공간에 대한 규정도 어렵게 만들고 있다. 현재 사이버공간이 무엇을 지칭하는지에 대한 명확한 정의는 존재하지 않는다.[34] 따라서 사이버공간에 대한 정의도 명확하지

않은 상태에서 이와 관련된 사이버안보 개념을 논한다는 것이 얼마나 어려운지는 자명한 사실이다.

앞서 언급한대로 사이버안보의 개념에 대한 국제적 합의는 도출되지 않고 있으며, 개별국가나 국제기구들은 사이버안보에 관해 상이한 개념들을 제시하고 있다.[35] 또한 각국은 자국의 안보전략상 사이버안보 및 관련 개념들에 대한 구체적인 정의를 제시하지 않고 있기도 하다.[36] 다만 각국 사이버안보 전략의 구체적인 범위와 내용들을 살펴보면, 사이버안보의 개념을 기존의 정보통신망보호, 정보보호, 정보통신기술안전 등의 특정 영역에 대한 보호라는 개념에서 탈피하여 사이버공간의 개념을 보다 폭넓게 도입함으로써 그 안보대상을 확장하고 있다는 사실을 파악할 수 있다. 즉 사이버안보 개념을 국가차원의 사이버공간에 대한 직·간접적 위협으로부터 국가 사이버공간의 안전을 확보하는 행동 및 조치로 규정한다고 할 수 있다. 지금까지 사이버공간의 안전은 정보통신망과 이를 통해 처리되는 정보, 또는 정보시스템의 보호에 중점을 두고 있었다.[37] 예를 들어 유럽연합에서 기존에 사용해 온 '네트워크와 정보시스템의 보호'라는 개념이나 미국에서 사용된 '정보보호'의 개념은 한국의 정보보호와 유사하게 정보 및 정보시스템의 보호를 목적으로 하는 조치였다.[38]

이와 관련하여 최근의 추세는 포괄적인 사이버안보의 개념이 나타나고 있다고 할 수 있다. 정보통신망 보호, 정보보호 등에 비하여 사이버안보는 좀 더 폭넓은 범위를 규정하는 방향으로 발전하고 있

34) 채재병, "안보환경의 변화와 사이버안보," pp. 180~181.

35) 위의 글, p. 184.

36) ENISA, *National Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace* (Heraklion: ENISA, 2012), p. 5.

37) 채재병, "안보환경의 변화와 사이버안보," p. 185.

38) 채재병, "국제테러리즘과 군사적 대응," p. 185.

다.[39] 사이버공간의 안전을 위해서는 정보보호가 필수적이고 핵심적인 부분을 차지하는 것이 사실이지만 좀 더 포괄적으로 정보 및 정보통신망의 안전이 사이버안보를 구성하는 중요한 핵심요소라고 할 수 있다.[40] 그리고 사이버안보를 일정한 상태의 개념으로 규정하기 보다는 적극적인 행위의 개념으로 규정함으로써 국제적으로는 대체로 사이버안보를 적극적 행위를 수반하는 개념으로 보고 있다.[41]

포괄적인 사이버안보의 개념은 그 대상 측면에서 정보의 안전성 보장에 중점을 둔 기존의 정보보호 또는 정보보안과 구별되어 현실세계에서와 마찬가지로 사이버공간에서의 안전을 보장하는데 초점을 맞춘다. 즉 사이버공간이 하나의 독립된 영역이라기보다는 현실공간을 수직적·수평적으로 연결해주는 역할을 하기 때문에 사이버공간의 안보는 필연적으로 기존의 정보보호 내지 정보보안보다는 확장된 개념이 될 수밖에 없다. 기존의 정보보호 개념이 정보 자체의 안전성, 즉 정보의 비밀성·무결성·이용가능성을 보장하기 위한 조치라는 의미라고 한다면 정보통신망의 보호도 마찬가지의 조치가 취해져야 한다는 의미이다.[42] 즉 사이버안보의 대상은 사이버공간에서 이용·저장·전송되는 정보뿐 아니라 사이버공간 자체에 대한 안전성을 보장하고자 하는 것이기 때문에 사이버공간을 지탱하는 토대는 물론 그 이용에 관한 전반이 포함되어야 한다는 것이다.[43]

국경안보에서의 주권은 앞에서 설명한 웨스트팔리아적 주권개념으로부터 출발하고 있다. 다만 국경안보가 국가주권과 그 영향력을

39) 위의 글, p. 185.
40) 위의 글, p. 185.
41) 위의 글, p. 185.
42) 위의 글, p. 186.
43) 위의 글, p. 186.

지금처럼 유지하거나 보다 더 확장하기 위한 포괄적인 전략의 일환으로 단순한 국경관리의 차원을 넘어선다는 점, 육·해·공에서의 국경 관련 위협들에 대한 억제와 안전보장 및 육상, 항만, 공항 등 모든 국경 출입 지역의 안전 강화를 의미한다는 점, 더 나아가 인접국과의 분쟁 방지 및 해소, 국경 지역의 발전과 안정을 위한 군사·경제적 정책을 모두 포괄하고 있다는 점에서 국경안보도 포괄안보차원에서 국가안보를 전개하고 있는 것이다. 다시 말해 국경안보에서의 주권개념은 안보개념의 확장으로 인한 웨스트팔리아적 주권개념의 변화를 내포하고 있는 것이다.

그리고 현실공간에서의 국경안보 개념이 사이버공간의 특수성으로 인해 그대로 적용될 수는 없지만 국경이 주권과 주권이 충돌하는 지점이라는 논리의 연장선상에서 사이버공간에서도 주권 충돌의 지점이 존재하고 사이버안보가 포괄적인 사이버안보 차원에서 국가안보를 전개하고 있다는 점에서 사이버공간에서의 주권개념도 국경안보에서의 주권개념과 일맥상통한다고 할 수 있다. 다시 말해 사이버공간에서의 주권개념과 국경안보에서의 주권개념은 주권의 정체성이라는 측면에서 별다른 차이를 보이지 않는다. 물론 사이버공간에서의 주권개념은 현실공간인 국경안보에서의 주권개념과 동일시하기 어려운 부분도 있다. 이는 사이버공간의 특수성에서 비롯되는데 우선 '사이버 국경은 존재하는가?'에 대한 문제이다. 사이버공간에서의 이러한 물리적 구분은 애매성과 모호성을 갖고 있다. 일단은 사이버공간에서 일어나는 일들은 눈에 보이지 않는다는 점이다. 그렇지만 사이버공간에서 일어나는 일들이 감지되지 않는 것은 아니다. 실제로 모든 사이버공간에서의 활동들은 결과적으로 현실세계로 귀결된다. 즉 사이버공간에서 주권과 주권이 충돌하는 지점으로서의 사이버 국경은 비록 그 특수성으로 인해 보이지 않고 특정되지

않지만 존재하는 것이다. 이런 측면에서 볼 때 주권의 정체성 차원에서 사이버공간의 주권개념과 국경안보에서의 주권개념은 사실상 동일하다고 할 수 있다.

Ⅲ. 사이버공간과 남북한

1. 한국

가. 사이버공간에 대한 인식 및 환경

(1) 사이버공간에 대한 인식

한국의 사이버공간에 대한 인식은 2019년 4월 3일 정부 수립 이후 최초로 수립·발표된 『국가사이버안보전략』에 잘 나타나 있다.[44] 첫째, 한국은 사이버공간을 국가운영의 핵심기반으로 인식하고 있다. 한국은 국가정보화를 통해 정보화 인프라를 구축하고 디지털 경제 확대 등 국가산업 성장과 혁신의 기반을 마련하고 경제·사회시스템을 비약적으로 발전시켰다. 또한, 행정기관을 중심으로 하는 정보화는 전자정부를 중심으로 행정의 효율성과 국민의 편의성을 크게 높였으며 국가운영의 핵심 경영시스템으로 자리 잡고 있다.[45] 이러한 국가정보화의 역할 덕분에 현재의 사이버공간은 국민의 일상생활, 기업의 경제 활동, 정부의 행정서비스 등에 있어 핵심기반으로 작용하고 있으며, 국민들은 사이버공간을 통해 삶의 지평을 확장하고 있다.

둘째, 한국의 사이버공간은 취약성이 증대하고 있다. 사이버공간에 대한 의존도가 높아지면서 사이버공간에 대한 위협도 함께 증가하고 있다. 악성 댓글, 스팸메일, 개인정보 유출, 금전적인 목적을 대상으로 하는 피싱(phising)이나 파밍(pharming)에 따른 개인적인 피해가 증가하고 있으며, 네트워크 보급에 따른 정보교환 및 공유로 인한 주요 기밀의 유출 가능성도 세계적 수준에 이르고 있다.[46] 그

44) 사이버공간에 대한 인식에 대해서는 국가안보실, 『국가사이버안보전략』 (서울: 국가안보실, 2019), pp. 2~7 참조.

45) 한국정보화진흥원, 『2018 국가정보화백서』 (서울: 한국정보화진흥원, 2018), pp. 2~3.

46) 국가정보원·미래창조과학부·방송통신위원회·안전행정부, 『2013 국가정보보호백서』

리고 최근 사물인터넷 기반의 융합기술이 가전·의료·공장이나 기반시설 등에 보급되면서 사이버공간에 대한 위협이 현실 공간으로 이어지고 있다.

셋째, 한국에 대한 사이버위협의 심각성이 증가하고 있다. 사이버위협의 주체는 개인이나 해커집단에서 범죄·테러 단체로 그리고 최근에는 국가 차원으로 확대되고 있다. 이는 최근의 사이버공격 양상이 기밀절취·금전취득에서 사회혼란 야기와 기반시설 마비·파괴 등 사이버테러의 형태로 나아가는 것과 일맥상통하고 있다.

넷째, 한국은 사이버공간에 대한 공격을 국가안보 차원에서 대응하고 있다. 최근 국가 간 정치·경제·군사적 분쟁은 사이버 공격으로 이어지고 있으며, 러시아의 우크라이나 침공에서 보듯이 물리적 공격 전후에 사이버 공격을 진행하는 사례가 발생하고 있다. 또한, 국가·테러단체 등의 개입으로 사이버 공격으로 인한 피해 규모와 심각성이 확대되어 국가안보에 대한 위협으로 대두되고 있다. 따라서 사이버공간에 대한 안보역량을 국가안보의 중요전력으로 인식하고 있으며, 사이버공격 역시 국가안보 차원에서 대응하고 있다.

(2) 사이버공간의 환경

한국은 2018년 UN(국제연합, United Nations)의 전자정부 발전지수 3위와 온라인 참여지수 1위, 2017년 국제전기통신연합 ICT(정보통신기술, Information and Communication Technology) 발전지수 2위를 차지하는 등 주요 정보통신지수에서 세계 최고의 수준을 보여주고 있다.[47] 또한, 초고속통신망(5G)을 선도적으로 구축하고 있으며, 2017년 7월 현재 인터넷 사용 인구는 4,528만 3천 명으로

(서울: 인터넷진흥원, 2013), p. 5.

47) 한국정보화진흥원, 『2018 국가정보화백서』, p. 308.

인구대비 90.3%에 달한다. 그리고 2018년 11월 현재 스마트폰 가입자 수는 약 5천 68만 명이며,[48] 보급률은 95%에 달하는 등 정보통신 인프라는 세계 최고 수준이다.[49] 이러한 정보통신 인프라를 바탕으로 현재 우리 사회는 산업, 행정, 국방 등 국가 전반으로 정보화가 확산되고 개인·기업·정부 등 모든 주체의 활동 기반이 사이버공간으로 확대되었다.[50]

한국의 정보화 진전과 사이버공간의 확대는 역설적으로 사이버 공격의 주요 대상 국가로 우리나라를 위치시키고 있다. 세계 최고 수준의 정보통신 인프라는 그만큼 우리의 사이버공간이 외부의 공격에 쉽게 노출될 수 있음을 의미한다. 한국에 대한 해킹·사이버 사기 등은 지속적으로 증가하고 있으며, 악성코드 유포와 DDoS 공격 등을 활용한 사이버 공격 역시 끊임없이 발생하고 있다. 한국을 대상으로 하는 사이버 공격은 개인과 기업을 넘어 공공기관과 국가기관으로까지 확대되고 있으며, 그 피해 규모와 파급효과는 점차 증가하고 있다.

한국은 사이버 공격으로 인해 피해 규모가 매년 늘어나고 있으며, 사이버공간의 확대에 따라 이메일은 물론 클라우드와 사물인터넷(Internet of Things: IoT) 등을 통한 사이버 공격도 급속도로 확대되고 있다.[51] 사이버 공격의 대상 역시 1·25 인터넷 대란(2003),

---

48) 위의 책, p. 548.

49) "한국 스마트폰 보유율 95%..세계 1위," 『연합뉴스』, 2019.2.6., 〈https://www.yna.co.kr/view/AKR20190206008200009〉 (검색일: 2019.7.19.).

50) 관계부처 합동, 『국가사이버안보 기본계획』 (세종: 과학기술정보통신부, 2019), p. 2.

51) SK인포섹은 이메일을 통한 사이버 공격은 올해 상반기 탐지된 악성메일 건수가 17만 1,400건으로 이미 작년 한 해 동안 탐지된 16만 3,387건을 넘어섰으며, 이런 추세라면 올해 약 34만 2,800건이 예상되어 작년의 2배, 2015년 6만 6,091건의 5배를 상회할 것으로 전망하고 있다. "AD서버 노린 사이버공격에 기업들 '휘청'," 『디지털타임스』, 2019.7.18., 〈http://www.dt.co.kr/contents.html?article_no=2019071802109931650002〉 (검색일: 2019.7.19.).

국가기관 시스템 공격(2004), 7·7 DDoS 공격(2009), 3·4 DDos 공격과 농협 전산망 마비(2011), 3·20 전산망 마비(2013), 한국수력원자력 내부문서 유출(2014), 서울메트로 해킹(2015), 국방부 해킹 사건(2016) 등 민·관·군 전 영역에 걸쳐 이루어지고 있다.

〈표 Ⅲ-1〉 주요 사이버공격 일지

일 시	주요 내용
2009.7.7.	• 청와대 등 정부기관 대상 DDoS공격
2011.3.4.	• 청와대·국정원 등 국가기관과 국민은행 등 금융기관, 네이버 등 국내 40개 사이트 대상 DDoS공격
2011.4.12.	• 농협 전산망 해킹으로 금융전산시스템 273대 파괴, 전산장애 발생
2011.11.	• 고려대 정보보호대학원 졸업생 이메일 계정 해킹
2012.6.9.	• 중앙일보 해킹
2013.3.20.	• KBS, MBC, YTN 등 방송사와 신한은행, 농협, 제주은행 등 금융기관 해킹
2013.6.25.	• 해킹과 DDoS 공격을 혼용하여 정부기관·언론사 등 69개 기관과 업체의 155대 서버 파괴 및 해당 사이트 접속 장애
2014.12.9.	• 해킹 / 사이버심리전(12/15), 한수원 원전 해킹
2014.12.24.	• 해킹/사이버 반달리즘, 소니 픽처스 엔터테인먼트사의 내부 전산망다운, 개봉영화 사전 유출로 1천억 원대 손실 발생
2015.10.	• 지하철 1~4호선 서버 해킹
2015.10.20.	• 국회를 비롯한 청와대, 외교부, 국방부, 통일부 등에 대한 해킹 시도
2016.1.6.	• 청와대 등 주요기관을 사칭하는 악성코드가 내장된 이메일 대량 유포 • 14년 12월 한수원 해킹 사건과 동일한 중국 랴오닝성 IP임이 밝혀짐
2016.5.3.~6.	• 인터파크 고객 1,030만 명 정보 해킹(북 정찰총국의 금전적 목적)
2016.12.12.	• 국방통합데이터센터(DIDC) 해킹
2017.5.12.	• 랜섬웨어(금전적 목적) • 구글과 러시아 카스퍼스키 랩은 '래저러스(Lazarus)'라는

일 시	주요 내용
	해킹집단과 유사성으로 미루어 북한을 배후로 지목

출처: 정영애, "사이버 위협과 사이버안보화의 문제, 그리고 적극적 사이버 평화," 『평화학연구』, 제18권 3호 (2017), p. 114.

특히 우리나라는 분단이라는 특수한 안보 상황으로 인해 사이버무기를 비대칭 전력으로 활용하는 북한으로부터의 위협에 노출되어 있다.[52] 사이버무기는 국가 간 경계가 불명확하고 공격 발원지 추적이 매우 어렵다는 점에서 전형적인 비대칭 전력 수단이며, 특히 북한의 사이버공격 능력은 매우 높은 수준으로 평가되고 있다.[53]

최근 미중·한일 갈등 등을 비롯한 동북아의 역내 갈등 심화 역시 사이버안보에 대한 위협으로 다가오고 있다. 아직 가시화되지는 않았으나, 우리의 사이버공간은 사이버위협의 주요 근원으로 식별되고 있는 중국으로부터의 사이버 공격 가능성에 노출되어 있다. 세계 최대의 해커 병력을 보유하고 있는 것으로 알려진 중국의 사이버전 수행능력과 행태는 최근 국제사회의 우려를 증가시키고 있다.[54] 나아가 중국 이외에도 국제적인 민간 해커집단의 위협 역시 매우 높게 나타나고 있으며, 향후 한국이 국제 테러조직에 의한 사이버 공격을 받게 될 위험성도 매우 높다고 볼 수 있다.[55]

---

52) 북한에 의해 이루어진 대표적인 대남 사이버 공격은 7·7(2009)·3·4(2011) DDoS 공격, '작계 5027' 유출(2009), 농협 전산망 파괴(2011년), 한국수력원자력 해킹(2014) 등이 있다.

53) 미국의 사이버 보안업체인 크라우드스트라이크(Crowdstrike)는 『2019 글로벌 위협보고(2019 Global Threat Report)』에서 북한의 사이버공격 능력이 러시아에 이어 세계 2위라고 밝히고 있다. "북한 사이버공격 능력 러시아에 이어 세계 2위," 『세계일보』, 2019.2.20., 〈https://news.v.daum.net/v/20190220092745850〉 (검색일: 2019.6.30.).

54) "중국 해커 병력 최대 5000명…심기 불편한 미국," 『중앙일보』, 2013.3.25., 〈https://news.joins.com/article/11026339〉 (검색일: 2019.6.30.); 시만텍에 의하면, 2012년 중국은 미국 다음으로 사이버공격이 빈번하게 시작된 공격 발원지 국가이다. Symantec, *Internet Security Threat Report 2013* (Tempe: Symantec, 2013), p. 8.

55) 채재병, "국제테러리즘과 군사적 대응," p. 180.

우리나라는 다른 나라에 비해 민·관·군 등 전 영역에서 정보통신기술에 대한 의존도가 월등히 높아 교통, 항공, 전력 등의 사회기반시설에 대한 사이버 공격이 이루어진다면 엄청난 사회적 혼란과 함께 국가재난 상태까지도 불러일으킬 수 있다. 또한, 최근 우리 사회의 사이버공간 확대에 따라 사이버 공격의 양상은 지능화·조직화 경향을 나타내고 있다. 인공지능 등 신기술을 활용한 공격이 증가하고 있으며 랜섬웨어와 같은 신종 위협이 끊임없이 발생하면서 국가안보에 대한 중대한 위협으로 다가오고 있다.

우리나라에 대한 사이버 공격의 증가에도 불구하고 사이버 공격에 대한 방어는 상당한 어려움을 겪고 있다. 사이버 공격은 공격징후를 사전에 파악하기 어렵고 민·관·군 등 모두를 공격대상으로 삼기 때문에 모든 공격에 대한 방어가 불가능하다. 그리고 최근의 급속한 정보통신기술의 발전을 보안기술이 따라가지 못하기 때문에 기존 방어체계의 한계를 뛰어넘는 사이버 공격에 대한 방어는 더욱 어렵다고 볼 수 있다. 세계 최고 수준의 정보통신기술 및 인프라와 함께 사이버 공격의 주요 대상인 오늘날 한국의 사이버공간 환경은 우리에게 국가안보의 새로운 도전영역으로 등장하고 있다.

나. 사이버안보 전략 및 추진체계

(1) 사이버안보 전략

한국의 사이버안보 전략은 그동안 주요 사이버 도발이 발생할 때마다 대책 마련 차원에서 이루어져 왔다. 한국의 사이버안보 전략은 「국가사이버위기 종합대책(2009)」, 「국가사이버안보 마스터플랜(2011)」, 「국가사이버안보 종합대책(2013)」 등을 거쳐 2019년 4월 「국가사이버안보전략」의 수립으로 나타났다. 「국가사이버안보전략」 수립 이

전의 시기에 수립된 사이버안보 전략들이 과제 중심의 액션플랜 성격을 띠고 있었다면, 「국가사이버안보전략」은 명실상부한 포괄적·종합적 사이버안보 전략이라고 평가할 수 있다.

〈표 Ⅲ-2〉 주요 사이버 공격별 정부의 종합대책

구분	정부대책 및 핵심내용
7/7 DDos	• 범정부 사이버위기 종합대책 – 대국민 언론 창구를 방통위로 일원화 – DDos 대피소 구축 및 대응장비 설치
3/4 DDos/농협 해킹	• 국가사이버안보 마스터플랜 – 민관군 사이버위협 합동 대응팀 구축, 운영 – 업무망–인터넷망 분리 및 외주업체 보안강화
3/20, 6/25 사이버테러	• 국가 사이버안보 종합대책 – 청와대 중심 사이버안보 컨트롤타워 정립 – 상황발생 시 청와대 및 국정원 동시 전파
한수원 해킹	• 국가 사이버안보 태세 강화 대책 – 국가안보실로 사이버안보 컨트롤타워 일원화 – 주요 정보통신 기반시설 보호체계 강화

출처: 윤오준 외, "사이버공격 대응분석을 통한 사이버안보 강화방안 연구," 『융합보안 논문지』, 제15권 4호 (2015), pp. 67~68.

국가안보실에서 수립·발표한 「국가사이버안보전략」은 국가안보전략의 부문 전략이며 사이버안보 정책의 최상위 지침 성격을 지니고 있다. 문재인 정부는 2018년 12월 발표한 「국가안보전략」의 '5大 과제' 중 하나로 '안전한 대한민국을 위한 국가위기관리체계 강화'를 제시하였으며, 이의 실현을 위해 '사이버안보 위협 대응능력 강화'를 세부과제로 제시하고 있다.[56] 이러한 차원에서 사이버안보

56) 문재인 정부의 '국가안보전략 5大 과제'는 ① 한반도 비핵화 및 항구적 평화정착 추진, ② 지속 가능한 남북관계 발전 및 공동·번영 실현, ③ 한미동맹 기반 위에 우리 주도의 방위역량 강화, ④ '국민'과 '국익 중심의 실용외교 추구, ⑤ 안전한 대한민국을 위한 국가위기관리체계 강화이다. 문재인 정부의 「국가안보전략」에 대해서는 국가안보실, 『문재인 정부의 국가안보전략』 (서울: 국가안보실, 2018), pp. 35~109 참조.

에 대한 국가차원의 포괄적인 중·장기 정책방향을 제시하는 「국가사이버안보전략」을 수립·시행한 것으로 볼 수 있다.

「국가사이버안보전략」은 수립배경, 비전 및 목표, 전략과제, 이행방안 등 4개의 장으로 구성되어 있다.[57] 「국가사이버안보전략」의 비전은 "자유롭고 안전한 사이버공간을 구현하여 국가안보와 경제발전을 뒷받침하고 국제 평화에 기여"하는 것이며, 이를 달성하기 위해 '3대 목표'와 '3대 원칙'을 제시하고 있다. '3대 목표'는 국가 주요기능의 안정적 수행, 사이버공격에 빈틈없는 대응, 튼튼한 사이버안보 기반 구축이며, '3대 원칙'은 국민 기본권과 사이버안보의 조화, 법치주의 기반 안보활동 전개, 참여와 협력의 수행체계 구축이다.[58] 그리고 한국의 사이버안보 비전과 목표를 달성하기 위한 전략과제로는 국가 핵심 인프라 안전성 제고, 사이버공격 대응역량 고도화, 신뢰와 협력 기반 거버넌스 정립, 사이버보안 산업 성장기반 구축, 사이버보안 문화 정착, 사이버안보 국제협력 선도 등 '6대 과제'를 제시하고 있다.[59]

정부는 「국가사이버안보전략」의 구체적인 추진을 위해 2019년 9월 「국가 사이버안보 기본계획」을 수립·발표하였다.[60] 정부는 「국가사이버안보전략」과 「국가 사이버안보 기본계획」의 성실한 시행을 위해 부처별로 「국가 사이버안보 시행계획」을 수립·추진할 것을 밝

57) 「국가사이버안보전략」의 주요 내용에 대해서는 국가안보실, 『국가사이버안보전략』, pp. 11~23 참조.

58) '3대 목표'와 '3대 원칙'에 대해서는 위의 책, p. 12 참조.

59) 전략과제에 대해서는 위의 책, pp. 13~23 참조.

60) 정부는 국가 사이버안보에 대한 위협이 증가함에 따라 과학기술정보통신부, 국정원, 국방부 등 9개 기관 합동으로 정부, 기업 및 개인 모두가 참여하여 사이버보안을 강화하기 위한 체계적인 실행 방안을 마련하였다고 밝히고 있다. 관계부처 합동, "국가사이버안보 강화를 위한 이행방안 확정-「국가사이버전략」 후속으로 기본계획 마련·시행," 『보도자료』,(2019.9.3.)., 〈https://msit.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=2170038〉 (검색일: 2019.9.20.).

히고 있으며, 이는 각 부처에 국가 사이버안보에 대한 책임성을 부여하는 한편, 법제도, 정책 등 추진과제의 실천력을 제고하기 위한 조치로 볼 수 있다.[61] 현재 한국의 국가 사이버안보 전략체계는 「국가사이버안보전략」-「국가 사이버안보 기본계획」-「국가 사이버안보 시행계획」으로 이루어져 있다. 「국가 사이버안보 기본계획」은 '6대 전략과제'를 뒷받침하기 위한 18개 중점과제와 100개의 세부과제를 제시하고 있으며, 2022년까지 단계적으로 추진될 예정이다.

〈표 Ⅲ-3〉 「사이버안보 전략별 기본계획」의 주요내용

전략과제	중점과제	세부 과제 수
국가 인프라 안전성 제고	• 국가 정보통신망 보안 강화 • 주요정보통신기반시설 보안환경 개선 • 차세대 보안 인프라 개발	24
사이버공격 대응 고도화	• 사이버공격 억지력 확보 • 대규모 공격 대비태세 강화 • 포괄적·능동적 수단 강구 • 사이버범죄 대응역량 제고	28
협력 기반 거버넌스 정립	• 민·관·군 협력체계 활성화 • 범국가 정보공유체계 구축 및 활성화 • 사이버안보 법적기반 강화	16
사이버보안 산업 성장	• 사이버보안 투자 확대 • 보안 인력·기술 경쟁력 강화 • 보안기업 성장환경 조성 • 공정경쟁 원칙 확립	14
사이버보안 문화 정착	• 사이버보안 인식 제고 및 실천 강화 • 기본권과 사이버안보의 균형	9
국제협력 선도	• 양·다자간 협력체계 내실화 • 국제협력 리더십 확보	9
합계	18	100

출처: 관계부처 합동, "국가사이버안보 강화를 위한 이행방안 확정-「국가사이버전략」 후속으로 기본계획 마련·시행," 『보도자료』, (2019.9.3.), 〈https://msit.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=2170038〉 (검색일: 2019.9.20.).

61) 관계부처 합동, 『국가사이버안보 기본계획』, p. 11.

(2) 사이버안보 추진체계

우리나라는 2005년 1월 대통령 훈령으로 「국가사이버안전관리규정」을 제정하면서 국가안보 차원에서 사이버위협에 대한 대응을 추진하기 시작하였다. 현재 한국의 국가사이버안보 추진체계는 청와대 국가안보실을 컨트롤타워로 국가정보원, 과학기술정보통신부, 국방부가 각각 공공분야, 민간분야, 국방분야를 담당하는 민·관·군 종합 대응체계로 구축되어 있다.

국가안보실은 사이버안보 컨트롤타워로서 사이버정보비서관을 두고 있으며, 체계적인 사이버안보 수행체계 정립·발전, 사이버공간의 안전한 보호 및 사이버전 수행능력 확보 등 국가 사이버안보 수행체계 강화를 통하여 선진국 수준의 사이버안보 대응역량 강화를 추진하고 있다.[62] 또한, 「국가사이버안보전략」을 수립·시행하고 있으며 민·관·군의 사이버안보 협력체계 활성화를 위한 법·제도의 지속적 개선, 사이버위협 예방 및 대응능력 강화, 국제협력 활성화 등을 추진하고 있다.

국가정보원은 국가·공공기관에 대한 사이버공격을 예방·대응하는 업무를 수행하고 있다. 국가정보원은 2004년 2월 출범한 '국가사이버안전센터(National Cyber Security Center: NCSC)'를 중심으로 중앙행정기관과 공공기관의 사이버위협 정보를 체계적이고 효율적으로 배포·공유하기 위하여 2015년 '국가사이버위협 정보공유시스템'을 구축하여 운영하는 등 사이버위협 정보의 허브 역할을 수행하고 있다.[63] 국가기관과 공공기관에 사이버공격이 발생하면 각급 기관은 국

62) 국가정보원·과학기술정보통신부·행정안전부·방송통신위원회·금융위원회, 『2019 국가정보보호백서』 (서울: 한국인터넷진흥원, 2019), p. 55. 사이버정보비서관은 2018년 8월 기존의 정보융합비서관과 사이버안보비서관을 통합한 직제이며, 사이버안보비서관은 2015년 4월 사이버안보에 관한 대통령의 직무를 효율적으로 보좌하기 위하여 신설되었다.

가정보원 국가사이버안전센터에 최초 상황보고를 하고 있다.

국방부는 사이버공간에서 사이버 작전 시행을 위해 '사이버작전사령부'를 두고 있다. 사이버작전사령부는 2010년 1월 '사이버사령부'로 출범하였으며 창설 당시에는 국방정보본부 예하에 있었으나 「국방개혁 307계획」에 따라 2011년 9월 국방부장관 직할부대가 되었다. 사이버작전사령부는 국방분야의 사이버안보를 담당하고 있으며, 사이버작전의 계획 및 시행, 사이버작전과 관련된 사이버보안 활동, 사이버작전에 필요한 체계 개발 및 구축, 사이버작전에 필요한 전문 인력의 육성 및 교육훈련, 사이버작전 유관기관 사이의 정보공유 및 협조체계 구축, 사이버작전과 관련된 위협 정보의 수집·분석 및 활용, 그밖에 사이버작전과 관련된 사항 등의 임무를 수행하고 있다.[64]

과학기술정보통신부는 민간분야 침해사고 예방·대응체계의 구축·운영, 민간분야 주요 정보통신기반시설의 지정 권고 및 취약점 분석·평가, 전자인증, 정보보호산업 및 정보보호 인력 관련 주요 정책 수립·추진 등 민간분야 정보보호에 관한 업무를 수행하고 있다.[65] 과학기술정보통신부는 국내 인터넷 이상모니터링과 홈페이지 악성코드 감염 등 민간부문에 대한 사이버공격에 예방·대응하기 위해 노력하고 있다.

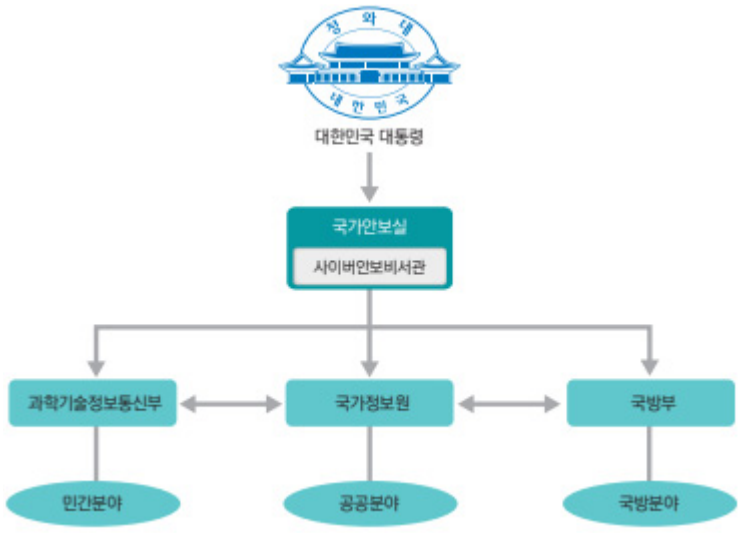
---

63) 위의 책, p. 57.

64) 법제처, 「사이버작전사령부령(2019.2.26 전부개정)」, 〈http://www.law.go.kr/lsInfoP.do?lsiSeq=207865&efYd=20190226#0000〉 (검색일: 2019.9.17.).

65) 국가정보원·과학기술정보통신부·행정안전부·방송통신위원회·금융위원회, 『2018 국가정보보호백서』 (서울: 인터넷진흥원, 2018), p. 57.

〈그림 Ⅲ-1〉 국가 사이버안보 추진체계



출처: 국가정보원·과학기술정보통신부·방송통신위원회·행정안전부·금융위원회, 『2018 국가정보보호백서』 (서울: 한국인터넷진흥원, 2018), p. 52.

국가정보원, 국방부, 과학기술정보통신부 이외에도 사이버안보 관련 국가기관은 행정안전부, 방송통신위원회, 금융위원회, 개인정보보호위원회 등이 있다. 또한, 전문기관은 한국인터넷진흥원, 국가보안기술연구소, 금융보안원, 한국지역정보개발원, 한국전자통신연구원 등이 있다. 이들 기관의 주요 기능 및 역할은 〈표 Ⅲ-4〉와 같다.

〈표 Ⅲ-4〉 정보보호 관련 국가기관 및 전문기관 현황

구분	명칭	주요 기능 및 역할
국가기관	국가안보실	사이버안보 수행체계를 일원화하여 사이버안보에 관한 대통령의 직무를 효율적으로 보좌하고 컨트롤타워 역할을 수행
	국가정보원	안보를 위협하는 사이버공격에 관한 정보를 수집·작성·배포하고, 국가·공공기관 대상 사이버공격 예방·대응 업무를 수행하며, 공공분야 정보통신기반시설 보호업무를 총괄
	과학기술정보통신부	민간 정보보호·전자인증·정보보호산업 관련 정책 수립 및 주요정보통신기반시설 지정권고, 민간 침해사고 예방·대응체계 구축·운영 등 민간분야 정보보호 및 정보보호산업 업무를 총괄
	행정안전부	전자정부 정보보호 및 개인정보보호 정책 업무를 수행
	방송통신위원회	정보통신서비스 및 방송 관련 개인정보보호 정책 업무를 수행
	금융위원회	전자금융 거래 이용자 보호와 전자금융 분야의 정보보안정책 수립 및 제도 개선 업무를 수행
	개인정보보호위원회	개인정보보호에 관한 사항을 심의·의결하고, 개인정보보호 기본계획을 수립하며, 개인정보 분쟁조정위원회를 운영
전문기관	한국인터넷진흥원	민간 사이버 침해사고 예방 및 대응, 개인정보보호 및 피해 대응, 정보보호산업 및 인력양성, 정보보호 대국민서비스, 국가도메인 서비스, 불법스팸 관련 고충처리 등을 수행
	국가보안기술연구소	공공 분야 사이버안전 연구·개발, 국가 암호기술 연구, 각종 정보보안기술 개발과 관련 기반 구축 및 지원, 국내외 정보보호 정책 연구, 전문교육과정 운영, 정보보호제품 인증 등을 수행
	금융보안원	금융 정보공유·분석센터 운영, 금융권 침해사고 대응, 전자금융 분야 취약점 분석·평가, 금융회사 자율보안 지원, 금융보안 교육 등을 수행
	한국지역정보개발원	지방자치단체 정보보호 인프라 강화, 지방자치 분야 사이버침해대응지원센터 및 정보공유·분석센터 운영 등을 수행
	한국전자통신연구원	민간분야 정보보호 기술 개발 및 보급 등을 수행

출처: 국가정보원·과학기술정보통신부·행정안전부·방송통신위원회·금융위원회, 『2019 국가정보보호백서』 (서울: 한국인터넷진흥원, 2019), p. 54.

다. 사이버 국제협력

국제사회의 사이버안보 논의는 UN, 경제협력개발기구(Organization for Economic Cooperation and Development: OECD), G8, 국제형사경찰기구(International Criminal Police Organization: INTERPOL) 등 국제기구와 국제협의체를 중심으로 진행되고 있다.[66] 특히 UN은 국제사회에서의 사이버안보 논의를 주도하고 있으며, 국제전기통신연합, UN 군축사무소(UN Office of Disarmament), UN 정부전문가그룹(Group of Governmental Experts on Information Security: GGE), UN 마약·범죄사무소(UN Office of Drug and Crimes) 등이 중심을 이루고 있다.

사이버안보의 지역협력은 지역 국제기구와 지역안보협력기구의 두 차원에서 진행되고 있다. 지역기구는 EU, 동남아국가연합(Association of South-East Asian Nations: ASEAN), 아시아태평양경제협력체(Asia-Pacific Economic Cooperation: APEC) 등이 있으며, 지역안보협력기구로는 북대서양조약기구, 유럽안보협력기구 등이 대표적이다.[67] 한편, 개별국가 간 양자 협력은 사이버 관련 이슈 중 하나로 사이버안보를 다루는 경향이 높으며, 국가 차원의 협력 이외에도 민간 차원의 다자간 국제협력 역시 중요한 역할을 수행하고 있다.

한국의 사이버안보 국제협력은 국제사회의 사이버안보 논의와 유사하게 UN 정보안보정부전문가그룹 참여, 양자 및 삼자협력, 아세안지역 협력, 세계 사이버스페이스총회 등을 중심으로 추진하고 있

66) 남상열, "사이버공간에 대한 국제적 논의와 2013년 서울 총회에의 시사점," 〈http://www.kisdi.re.kr/kisdi/fp/kr/board/selectSingleBoard.do?cmd=selectSingleBoard&boardId=GPK_COLUMN&seq=27337&reStep=36299&ctx=_〉(검색일: 2019.9.17.)

67) 장규현·임종인, "국제 사이버보안협력 현황과 함의: 국제안보와 UN GGE 권고안을 중심으로," 『정보통신방송정책』. 제26권 5호 (2014), p. 27.

다.[68] 한국은 유엔에서 사이버안보 규범을 논의하는 UN 정보안보 정부전문가그룹에 2004년 출범 이후 현재까지 총 4차례 참여하였다.[69] UN 군축·국제안보위원회는 2004년부터 국제안보 차원에서의 사이버안보 문제를 논의하기 위해 GGE 회의를 진행해 오고 있다. GGE는 사이버공간에 적용 가능한 국제법 및 규범 마련을 위한 논의를 진행해 오고 있으며, 제6차 UN 정보안보 GGE가 구성될 예정이다.

한국은 양자 및 삼자협력을 통한 사이버안보 국제협력에도 적극적으로 참여하고 있다. 한국은 한미동맹 차원에서 미국과 사이버안보의 비전을 공유하고 사이버안보협력 채널의 제도화를 추진하고 있다. 한미 간 사이버안보 논의는 정상회담과 사이버정책협의회를 통해 이루어지고 있으며, 2014년 4월 한미정상회담에서 양국은 사이버공간에서의 개방성, 상호운용 가능성, 안정성, 신뢰성을 지향하는 비전을 제시하였다.[70] 그리고 2015년 10월의 한미정상회담에서는 포괄적 동맹관계 구축영역에 사이버안보가 포함된다는 것을 천명하였다. 한미 사이버정책협의회는 2012년 출범한 이후 총 5회[71]의 회의를 통해 한미 간 사이버정책을 협의하고 있다. 한국은 미국 이외에도 영국, 일본, 러시아, EU, 호주, 인도, 중국, 사우디, 체코, 독일, 폴란드 및 NATO와 양자 사이버정책협의회를 개최하고 있으며, 일본·중국과는 삼자 사이버정책협의회를 그리고 미국·일본과는 삼자 사이버대화를 진행하고 있다.[72]

---

68) 한국의 사이버안보 국제협력 현황에 대해서는 외교부, "글로벌 안보협력 개요," 〈http://www.mofa.go.kr/www/wpge/m_3991/contents.do〉 (검색일: 2019.10.5.) 참조.

69) 우리나라는 제1차(2004~2005년), 제2차(2009~2010년), 제4차(2014~2015년), 제5차(2016~2017년)에 참여하였다.

70) 김상배, "사이버안보의 주변4강과 한국-세력망의 구조와 중견국의 전략," 『국제정치논총』, 57권 1호 (2017), p. 123.

71) 1차(2012.9), 2차(2013), 3차(2014), 4차(2016), 5차(2018) 회의가 개최되었다.

한국은 아세안지역과의 사이버안보 협력을 아세안지역포럼(ASEAN Regional Forum: ARF)을 중심으로 추진하고 있다. ARF는 사이버안보 이슈를 중시하는 대표적인 지역다자안보체로 대테러·초국가적범죄 회의(ISM on CTTC)를 통해 3대 중점 협력분야 중 하나로 사이버안보 이슈를 논의하고 있다. ARF는 사이버테러리즘 세미나, 사이버공간 대리행위자에 관한 워크숍, 사이버침해 대응 워크숍, 사이버공간 신뢰구축조치 세미나 등 사이버안보 논의를 적극적으로 진행하고 있다.[73] 한국은 2012년 9월 사이버공간 신뢰구축조치 세미나를 개최하였으며, 2013~2015년에 걸친 사이버안보 워크숍에 지속적으로 참여하면서 아세안 차원의 사이버안보 규범 마련에 적극적으로 참여하고 있다.

ARF는 회원국 간 사이버안보 분야의 신뢰구축, 분쟁방지, 상호이해 촉진을 위해 2015년 8월 ARF 외교장관 회담에서 사이버안보 작업계획을 채택하였다. 그리고 2018년 1월 본격적으로 ARF내 사이버분야 신뢰구축조치 논의를 위한 연구그룹이 조직되어 2018년 4월, 2019년 1월, 2019년 3월 등 총 4차례에 걸쳐 회의가 진행되었으며, 우리 정부도 적극적으로 참여하였다.

세계 사이버스페이스총회는 개방되고 안전한 사이버공간을 구축하기 위한 국제사회의 행동의제 개발과 관련 협력을 촉진하기 위해 출범하였으며, 전 세계 100여개 국가와 국제기구, 기업, 시민사회단체 등이 참여하고 있다. 사이버스페이스총회는 사이버테러, 사이버범죄, 국제안보 등을 비롯한 사이버안보가 주요 의제로 다루어지고 있다. 우리나라는 2011년 런던, 2012년 부다페스트에 이어 제3차 사이버스페이스총회를 2013년 서울에서 개최하였다. 이 회의에서 우

72) 외교부, "글로벌 안보협력 개요."

73) 장규현·임종인, "국제 사이버보안협력 현황과 함의: 국제안보와 UN GGE 권고안을 중심으로," p. 29.

리나라는 '개도국 역량강화'를 의제로 제안하였으며, 개도국의 관심과 지지 확보를 통해 총회 사상 최초로 결과 문서를 도출하는 등의 성과를 거두었다. 2015년 헤이그 총회에서는 전임 의장국으로서 국제규범 논의와 신뢰구축 노력의 병행 필요성 등을 주장하였으며, 2017년 인도 총회에서 초국경적 사이버위협이 기술적 차원을 넘어선 외교적 문제임을 강조하였다.[74]

2. 북한

가. 사이버공간에 대한 인식 및 환경

(1) 사이버공간에 대한 인식

미국 국방부는 2010년 『4개년 국방검토 보고서(Quadrennial Defense Review 2010)』에서 사이버공간을 처음으로 육·해·공 및 우주와 함께 제5의 전장으로 규정하였다.[75] 북한 역시 사이버공간을 전략적으로 중요성이 매우 높은 새로운 전장[76]으로 인식하고 있으며, 비대칭 전력으로 사이버 전력을 적극적으로 활용하고 있다. 북한은 군사전략과 국가안보 전략에 사이버 작전을 결합시키고 있

74) 외교부, "글로벌 안보협력 개요."

75) U.S. Department of Defense, "*Quadrennial Defense Review Report,*" 〈https://dod.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf〉 (Accessed September 17, 2019), p. 9; U.S. Department of Defense, "*DoD Strategy for Operating in Cyberspace,*" 〈https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf〉 (검색일: 2019.9.17.), p. 5.

76) 북한의 『로동신문』은 "여러 나라가 싸이버공간을 륙지와 해상, 공중, 우주와 나란히 5번째 전장으로 규정했다"고 하면서 각국의 사이버전쟁 사례를 소개하고 사이버공간의 안전을 보장하는 것이 중요해지고 있다고 주장했다. "국가간 대결장으로 되여가는 싸이버공간," 『로동신문』, 2019.7.16.

으며, 사이버작전을 위한 전력은 북한의 핵심 전력이자 국가적 목표를 달성할 수 있는 전략무기로 받아들이고 있다.[77]

북한은 사이버 작전을 군사전략의 중요한 핵심 부분으로 간주하고 있다. 북한은 인민군대의 3대 수단으로 사이버테러, 핵, 미사일을 제시하고 있으며, 사이버 무기는 핵, 생화학무기와 함께 3대 비대칭 무기이며 사이버 전력은 핵, 게릴라전과 함께 3대 비대칭 전력으로 간주하고 있다.[78]

북한은 2003년 걸프전, 즉, '사막의 폭풍 작전' 이후 본격적으로 사이버전에 관심을 기울이기 시작하였다. 김정일은 이라크 전쟁 이후 군 수뇌부들에게 "지금까지의 전쟁이 알(총탄, 포탄 등) 전쟁, 기름전쟁이었다면 앞으로 21세기 전쟁은 정보전"[79]이라고 강조하면서 사이버전에 대한 중요성을 강조하였다. 그리고 군사지휘관들에 대한 첨단 정보기술 교육 진행, 어린영재들과 미림대학 출신들로 조직된 전문사이버전 부대들의 조직개편을 통해 정보전 전투능력 구비 등의 조치를 취하였다.

김정은 역시 사이버공간의 중요성을 인식하고 사이버 공격과 사이버 전력의 중요성을 지속적으로 강조하고 있다.

77) 임종인 외, "북한의 사이버전력 현황과 한국의 국가적 대응전략," 『국방정책연구』, 제29권 제4호 (2013), p. 15

78) 위의 글, p. 15.

79) 김흥광, "북한의 사이버정보 실태," 『북한』, 5월호 (2005), p. 32.

〈표 Ⅲ-5〉 김정일·김정은 사이버 관련 교시 내용

구분		교시내용
김정일	사이버공간의 중요성 강조	• 인터넷은 국가보안법이 무력화되는 특별한 공간이다. • 남한당국이 통제할 수 없는 공간이다(2003.7). • 남한 내 인터넷을 적극 활용하라.
	사이버공격의 중요성 강조	• 사이버공격은 원자탄이고 인터넷은 총이다. • 21세기 전쟁은 정보전쟁이다. 현대전은 전자전이다. • 전자전에 따라 현대전의 승패가 좌우된다.
	사이버전력의 강화 강조	• 더 많은 정보전사를 양성하라. • 사이버부대는 나의 별동대이자 작전 예비전력이다.
김정은	사이버공격의 중요성 강조	• 사이버전은 핵, 미사일과 함께 인민군대의 무자비한 타격능력을 담보하는 만능의 보검이다. (김정은 2013년 8월 정찰총국 군간부들에게)
	사이버전력의 중요성 강조	• 강력한 정보통신 기술, 정찰총국과 같은 용맹한(사이버) 전사들만 있으면 그 어떤 제재도 뚫을 수 있고, 강성국가 건설도 문제없다. (김정은 2013년 4월 7일 정찰총국 해커부대 방문시)
	사이버거점 장악과 무력화 지시	• 적들의 사이버 거점들을 일순에 장악하고 무력화 할 수 있는 만반의 준비를 갖추라(김정은 2014년 6월 28일 정찰총국 사이버부대인 121국 비공개 방문시).
	전략사이버사령부 창설 지시	• 김정은 2012년 북한군 총참모부 정찰총국 산하기구 110호 연구소를 방문해 '전략사이버사령부 창설' 지시 – 2014년 북한 사이버전력 최대 6000명: 이들은 직접적인 해킹을 기획하는 정찰총국 예하 병력 1200명, 기술지원 인력 1800명, 정찰총국 외 유관조직에 산재된 사이버 요원이 3000명 정도 – 사이버 영재는 중학교 시절 조기 발굴해 매년 300명씩 사이버전사로 집중 양성
	사이버 인력 확보 지시	• 각 도의 제1중학교에서 유능한 컴퓨터 전문가를 양성하라 지시(2009.10.).

출처: 김윤영, "북한의 대남 사이버공작 대응 방안 연구," 『치안정책연구』, 제30권 2호 (2016), pp. 247~248.

북한은 사이버공간을 "제도적 기반과 정규군을 가진 일본군과 맞서 싸우던 항일빨치산의 투쟁무대"와 동일시하면서 "북한군의 정보모략전, 해킹, 사이버심리전, 대남공작은 북한이 아닌 제3국에서 벌

어지기 때문에 적에게 노출될 위험이 적고, 반면에 적대국은 인터넷이 제도화되고 공개되어 있기 때문에 드러난 공격위험을 가지고 있는 더없이 유리한 작전공간"으로 인식하고 있다.[80] 이러한 북한의 사이버공간에 대한 인식은 사이버방어보다는 사이버공격을 중시하는 경향으로 나아가게 하는 요인으로 작용하고 있다.

(2) 사이버공간의 환경

북한은 사이버공간을 매우 폐쇄적인 체제로 운영하고 있다. 사이버공간은 '열린 공간'으로서 시간과 장소를 가리지 않고 접근할 수 있는 특징을 지니고 있다. 그러나 북한은 대내적으로는 인트라넷을 그리고 대외적으로는 인터넷을 사용함으로써 사이버공간의 분리와 폐쇄성을 통한 안정화를 추진하고 있다.

북한의 사이버공간은 열악한 정보통신 인프라로 인해 상당히 낙후되어 있다고 볼 수 있다. 1990년대 중반 이후 북한당국이 정보통신망 확충에 관심을 가지면서 인프라 구축을 추진했지만, 평양을 제외한 다른 지역의 인프라 수준은 여전히 낮은 수준을 벗어나지 못하고 있다.

북한 사이버공간의 기본구조 특징은 네크워크 보안 수준을 높이기 위한 분리구축 및 운용이라고 할 수 있다. 인터넷 부분에서는 글로벌 인터넷과 국가 인트라넷으로 이원화하고 있으며, 이동통신 부분은 내국인용, 외국인용, VIP용으로 삼원화하여 분리구축·운용하고 있다.[81] 북한의 인터넷-인트라넷의 이원화 분리구축 정책은 국가안보에 중점을 둔 독특한 사이버 전략의 결과물로 볼 수 있다. 북

80) 김흥광, "북한의 사이버테러 정보전 능력과 사이버보안 대책 제언," (국가 산업기술유출 대응 콘퍼런스, 2010), p. 5.

81) 고경민·김일기·나용우, 『김정은 시대 북한의 정보통신 전략에 관한 연구』 (서울: 통일부, 2017), p. 23.

한은 사이버공간의 발전과 체제 위협 그리고 인터넷 개방과 통제라는 딜레마 상황을 극복하는 전략으로 '선(先)통제 후(後)활용'이라는 방어적 전략을 선택하였으며, 이 결과 인터넷과 인트라넷의 분리구축으로 나타났다.[82]

북한은 기관별로 다양한 인트라넷을 두고 있으며, 일반기관과 주민을 위한 '광명망'과 이와 분리된 '방패망'(국가보위성), '성새망'(인민보안성), '금별망'(군) 등을 운용하고 있다. 대부분의 북한 주민과 기관이 사용하는 대표적 인트라넷인 '광명망'은 평양과 평성을 중심으로 각 도청 소재지에 지역센터가 구축되어 있으며, 중소도시들은 가까운 지역센터에서 방사형으로 연결되어 있다.[83]

북한의 글로벌 인터넷과의 연결은 중국 단둥과 신의주를 연결하는 광통신망을 통해 중국의 차이나텔레콤으로부터 회선을 할당받은 중국 IP를 통해 이루어지고 있으며, 중국의 필터링 정책에 따라 여과된 인터넷 콘텐츠에만 접근할 수 있다.[84] 북한 내부에서의 외부로 통하는 인터넷 사용은 소수에 의해 독점·통제되고 있으며, 월드뱅크는 북한의 인터넷 이용자 수는 인구대비 0%로 세계 최저수준이며 실제 이용자들은 정부에서 신뢰할 수 있는 간부급 인원 수백 정도일 것으로 보고 있다.[85] 북한의 낙후된 정보통신 인프라와 낮은 인터넷 이용률 등 사이버공간의 낙후성은 오히려 사이버 공격에 대한 방어 측면에서는 매우 유리한 전략적 입지를 제공하는 역설적 현상을 나타내고 있다.

---

82) 고경민, "북한의 IT 딜레마와 이중전략-인터넷 정책과 소트트웨어 산업정책을 중심으로," 『정보화정책』, 제14권 제4호 (2007), p. 153.

83) 고경민·김일기·나용우, 『김정은 시대 북한의 정보통신 전략에 관한 연구』, p. 24.

84) Opennet Initiative, "Country Profile: North Korea," 〈https://opennet.net/research/profiles/north-korea〉 (검색일: 2019.6.15.), p. 1.

85) 임종인 외, "북한의 사이버전력 현황과 한국의 국가적 대응전략," p. 22.

나. 사이버안보 전략 및 추진체계

(1) 사이버안보 전략

북한은 당과 국가 차원에서 사이버안보 전략을 수립·발표하지 않고 있으며, 사이버안보 전략과 관련된 공식문서나 언론 보도 역시 알려진 바가 없다. 다만, 북한은 사이버공간의 폐쇄성으로 인하여 사이버 위협에 대한 방어보다는 오히려 공격에 초점을 두고 있다는 정도만 알려져 있다.

북한은 1990년대 말 사이버전 전법, 심리전 전법, 경제정보획득 전법 등 북한만의 독특하고도 다양한 정보전 전법들을 발전시켜 왔으며, 이러한 사이버 전략은 중국 군사교리인 점혈전략[86]과 사이버 전법[87]을 벤치마킹했다고 알려져 있다.[88] 또한, 북한 영토 내에서는 사이버 공격작전을 수행하지 않는 등의 사이버 교전규칙도 마련한 것으로 알려져 있다.[89] 한편, 북한의 사이버 공격전술은 사이버 공격작전 계획이 수립되면 사이버 부대원들이 중국의 안전가옥으로 이동한 후 프록시 서버를 가동하여 공격근원지를 숨기면서 수백 명

86) 점혈전략이란 상대편 정보시스템의 약점과 급소 부위의 혈(穴)을 눌러 전체를 마비시킴으로써 최대의 효과를 추구하는 것을 의미한다. "북의 복합도발 경보! EMP전자탄을 아는가?"『뉴데일리』, 2013.3.26., 〈http://www.newdaily.co.kr/site/data/html/2013/03/26/2013032600019.html〉(검색일: 2019.6.15.).

87) 사이버전법은 前饋潛伏法(전쟁 발발 전 바이러스를 적 컴퓨터에 잠복·은폐), 臨機預置法(전쟁 전날 바이러스를 적 컴퓨터나 무기에 장착), 間接攻擊法(바이러스를 전원, 출력, 온도제어시스템 등 보조시스템에 침투), 接口輸入法(컴퓨터 인터페이스를 통해 바이러스 침투 후 본 시스템으로 확산), 探測攻擊法(공장에서 컴퓨터를 생산할 때 발생하는 자기장을 활용해 바이러스를 침투시키거나 또는 간접자장을 만들어 컴퓨터를 혼란케 함) 등이다. "북한 사이버전법은 중국의 점혈전쟁술 모방한 것,"『중앙일보』, 2009.7.10., 〈https://news.joins.com/article/3681383〉(검색일: 2019.6.15.).

88) 임종인 외, "북한의 사이버전력 현황과 한국의 국가적 대응전략," pp. 28~29.

89) "북한 사이버 부대 귀순자, 3·20을 말하다,"『전자신문』, 2013.5.14., 〈http://m.etnews.com/201305130282?obj=Tzo4OiJzdGRDbGFzcyI6Mjp7czo3OiJyZWZlcmVyIjtOO3M6NzoiZm9yd2FyZCI7czoxMzoid2ViIHRvIG1vYmlsZSI7fQ%3D%3D〉(검색일: 2019.6.15.).

이 하나의 목표물에 대해 공격을 수행한 후 작전이 완료되면 북한으로 돌아가는 순으로 이루어지고 있다.[90]

북한은 사이버안보 전략의 한 축으로 사이버공간을 대남혁명전략 실현을 위한 장으로 활용하고 있다.[91] 북한은 대남정보기구별로 사이버 전담부서를 운영하고 있으며, 사이버공작 기술 개발, 사이버전 담요원 양성, 사이버공작 실행 등으로 세분화, 전문화, 다각화하여 운영하고 있다. 그리고 대남심리전 도구로 웹사이트와 함께 SNS를 적극적으로 활용하고 있으며, 북한의 영화, 음악, 소설, 문헌 등을 집중 전파하는 '사이버 문화심리전'을 강화하고 있다. 북한은 '전 사회의 김일성·김정일주의화'라는 한반도의 공산화를 위해 오프라인(offline)과 병행하여 온라인(online)공간인 사이버공간을 통해 사이버테러, 사이버 간첩교신, 사이버전 등을 수행하고 있다.[92]

(2) 사이버안보 추진체계

북한의 사이버 공격을 수행하는 기구들은 당·정·군 산하에 각각 존재하고 있으며, 이들은 사이버테러, 사이버심리전, 사이버 간첩교신 등을 수행하는 사이버 작전 부대와 수행조직들을 두고 있다. 북한의 주요 사이버 공격기구들은 총참모부, 정찰총국, 통일전선부와 225국 소속에 산재하여 있다. 총참모부는 지휘자동화국과 적공국, 정찰총국은 사이버전 지도국(121국), 노동당은 통일전선부와 225국 산하에 사이버전담부서를 두고 있다.[93]

---

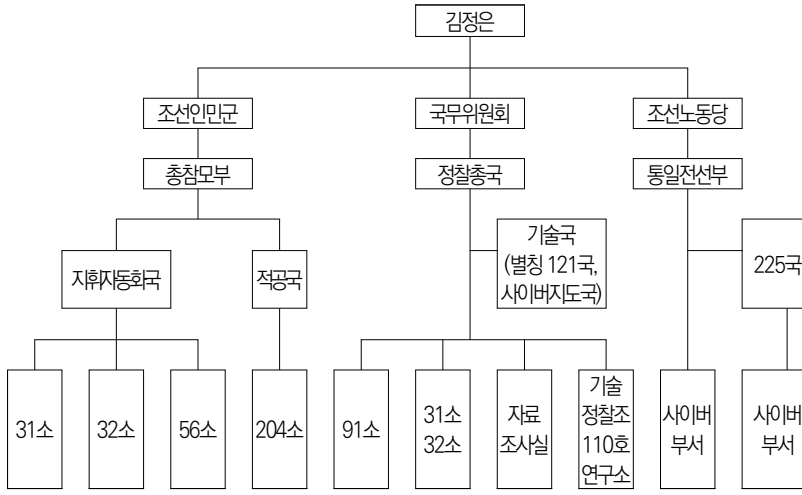
90) 임종인 외, "북한의 사이버전력 현황과 한국의 국가적 대응전략," p. 29.

91) 유동열, "북한의 대남 사이버위협 실태와 대책," (국가안보전략연구소 학술회의자료, 2014), p. 32.

92) 이에 대해서는 유동열, 『사이버공간과 국가안보』 (서울: 북앤피플, 2012), pp. 52~54 참조.

93) 북한의 사이버 공격기구들에 대해서는 위의 책, pp. 47~55; 유동열(2014), "북한의 대남 사이버위협 실태와 대책," pp. 24~27; 임종인 외, "북한의 사이버전력 현황과

〈그림 Ⅲ-2〉 북한의 사이버안보 기구도



출처: 임종인 외, 『사이버위협 시나리오 개발 및 대응방안 연구』 (서울: 합동참모본부, 2014), p. 59; "북한 군사지휘 및 사이버부대 기구도," 『연합뉴스』, 2013.4.10. 〈https://www.yna.co.kr/view/GYH20130410001000044?section=search〉 (검색일: 2019.9.20.) 참조하여 수정보완

북한 사이버 공격기구의 구체적인 기능과 역할은 다음과 같다.

한국의 국가적 대응전략," pp. 25~26; "북한 군사지휘 및 사이버부대 기구도," 『연합뉴스』, 2013.4.10., (https://www.yna.co.kr/view/GYH20130410001000044?section=search) (검색일: 2019.9.20.) 참조.

〈표 Ⅲ-6〉 북한 사이버공격 기구의 기능과 역할

담당부서		기능과 역할
조선인민군	총참모부	• 사이버전사 양성, 연구(지휘자동화 대학 등) • 한국군 대상 사이버심리전 실행(적공국 204소) • 군지휘통신 교란, 사이버전 실행(지휘자동화국)
국무위원회	정찰총국	• 사이버공작 요원 양성, 연구(모란봉대학) • 대남정치, 군사정보 해킹, 사이버공작 실행(기술정찰조, 110연구소) • 전담요원 해외파견, 사이버테러 등 공작수행 • 대남사이버심리전(역정보, 허위정부 유포 등) • 해커부대(91소)
조선노동당	통일전선부	• 대남 사이버심리전 전담 • 140여개 웹사이트(구국전선, 우리민족끼리 등) 운영 • 트위터 등 활용 SNS공작 • 여론조작 댓글팀 운영 허위정보, 사회교란 시도
	225국	• 한국 내 전략정보 수집 • 사이버 드보크, 사이버 간첩교신

출처: 유동열, "북한의 대남 사이버위협 실태와 대책," (국가안보전략연구소 학술회의자료, 2014), p. 26.

북한은 정찰총국 소속 사이버연구소를 중심으로 '사이버사령부'를 창설했으며, 국방위원회(현재 국무위원회)와 노동당 산하에 1,700여 명으로 구성된 7곳의 해킹조직을 두고 있다.[94] 북한의 주요 해킹조직들은 정찰총국 산하의 제3국(제3기술정찰국)과 110호 연구소 소속으로 알려져 있다.[95] 미국 재무부 해외자산통제국(Office of

94) "김정은 "사이버전은 만능의 보검" 3대 전쟁수단 운용," 『중앙일보』, 2013.11.5., 〈https://news.joins.com/article/13048072〉 (검색일: 2019.9.17.); 김흥광(전 북한공산대학 교수)은 북한이 "정찰총국 121국을 종전 연대급 전력에서 사단급 전력으로 증강"시켰으며, "121국의 병력은 2015년쯤 약 3,000명으로 두 배로 늘었고, 사이버전 병력수는 거의 7,000명에 달한다"며 "500명 규모의 204사이버심리전부대가 최근 들어 1,000명 수준으로 증설됐다"고 밝히고 있다. "北정찰총국 사이버전력 7,000명 육박," 『문화일보』, 2019.6.25., 〈http://www.munhwa.com/news/view.html?no=2019062501070609312001〉 (검색일: 2019.6.30.).

95) "美재무부, 북미실무협상 재개 전망 속 北 해킹그룹 3곳 제재," 『연합뉴스』, 2019.9.14., 〈https://www.yna.co.kr/view/AKR20190913039153071〉 (검색일: 2019.9.30.).

Foreign Assets Control: OFAC)은 '라자루스 그룹(Lazarus Group)'[96], '블루노로프(Bluenoroff)'[97], '안다리엘(Andariel)'[98]로 칭해온 북한의 3개 해킹그룹을 제재하면서, "이들은 미국과 유엔의 제재대상이자 북한의 중요 정보당국인 정찰총국의 통제를 받고 있다"고 밝혔다.[99]

북한 해킹조직들의 목표대상은 금융기관과 외교·안보기관에 집중되어 있으며, 금전적 이득과 외교·안보 정보 절취에 목적을 두고 있다. 세계 각국의 금융기관 공격에는 '레비린스 천리마'와 '스타더스트 천리마'가 그리고 외교·안보 정보 취득에는 '벨벳 천리마'와 '리커세이 천리마'가 투입되고 있다.[100] 북한의 스타더스트 천리마는 지난해 멕시코, 코스타리카, 칠레, 아르헨티나 등 남미 지역의 금융기관 해킹을 통한 자금 절취 활동을 집중적으로 전개했다.

북한은 사이버안보 기구와 해커조직에서 활용할 수 있는 사이버 인력을 양성하기 위해 많은 노력을 기울여 왔다. 북한의 사이버 전문인력 양성은 소학교부터 시작하고 있다. 북한은 소학교 재학 중인

---

96) 라자루스 그룹은 2007년 초 조직되어 2014년 소니픽처스 해킹, 2016년 방글라데시 중앙은행 해킹, 2017년 워너크라임 랜섬웨어 공격 등을 수행했다. 산하조직으로 미로천리마(APT37), 침묵천리마, 별똥천리마, 물수제비 천리마 등이 있다. "北 해킹 전사들의 조직명은 '천리마'…하부조직 주특기 명확," 『중앙일보』, 2018.2.21., 〈https://news.joins.com/article/22385751〉 (검색일: 2019.8.10.).

97) 블루노로프는 2014년 초 포착되었으며, 외국 금융기관 공격을 통한 불법적 수입 확보를 통해 부분적으로 핵무기와 탄도미사일 프로그램 증강을 지원하기 위해 외국 금융기관에서 11억 달러 탈취를 시도했고 방글라데시와 인도, 멕시코, 파키스탄, 필리핀, 한국, 대만 등 11개국 16개 기관에서 작전을 수행했다.

98) 안다리엘은 2015년 포착되었으며, 한국 정부와 인프라 시설을 겨냥한 공격을 수행하고 있다.

99) 이들 3대 해킹그룹은 2017년 1월~2018년 9월 사이에 5개 가상화폐거래소를 해킹해 5억 7천 100만 달러의 가상화폐를 탈취한 것으로 알려져 있다. "美, 北 3대 해킹그룹 정조준…적나라한 해킹실태·정체 드러나," 『연합뉴스』, 2019.9.14., 〈https://www.yna.co.kr/view/AKR20190914003600072〉, (검색일: 2019.9.30.).

100) "북한 사이버 공격 능력 러시아에 이어 세계 2위," 『세계일보』, 2019.2.20., 〈https://news.v.daum.net/v/20190220092745850〉 (검색일: 2019.6.30.).

학생들을 선발하여 평양 제1·2(고등)중학교 및 지방 영재학교 등의 '컴퓨터전문반'에 입학시키고 있다. 그리고 이들 학교에서 우수학생들을 선발하여 IT전문대학인 김일성종합대학의 컴퓨터과학대학, 김책공업종합대학의 정보기술대학, 평양컴퓨터기술대학, 함흥컴퓨터기술대학 등에서 사이버 전문가로 양성하고 있다. IT전문대학을 졸업한 정예학생들은 사이버공작 전문양성기관인 김일성군사종합대학,[101] 지휘자동화대학(일명 미림대학, 현 김일정치군사대학),[102] 모란봉대학[103] 등을 통해 사이버 전사로 양성된다.

사이버 연구기관으로는 국방과학원 산하의 정보전 연구중심, 미림대학의 정보전 연구센터(110호 연구소), 제2경제위원회 연구개발부서들이 등이 있으며, 이들은 상호협조하에 정보전의 수행에 필요한 각종 무기체계와 기술기재를 연구·개발하고 있다.[104]

북한은 2019년 37개 대학에 정보보안학과, 나노재료공학과, 로봇공학과 등 정보화와 첨단과학 분야의 학과를 신설하고 4월부터 교육과정을 시행하고 있다.[105] 이 중 정보보안학과는 사이버보안 학과로 볼 수 있으며 해킹인력 양성과도 밀접한 연관이 있는 것으로 보인다.

---

101) 총참모부 소속으로 1986년 5년제 전산과정을 신설하여 매년 1,000여 명의 사이버전사를 양성하고 있으며, 평양 만경대 구역에 있다.

102) 김정일 지시로 1986년 평양 미림동에 설립되어 일명 '미림대학'의 별칭으로 불려지다가, 2000년 '조선인민군 지휘자동화대학'에서 '김일정치군사대학(조선인민군 144부대)'으로 명칭이 변경되었다. 기본과정인 학부는 5년제로 매년 120여 명의 졸업생을 배출하고 있으며 대학원에 해당하는 연구과정은 3년제로 운영되고 있다. 학생들은 졸업 후 정찰총국 산하 사이버전지도국인 '121국' 등에 배치된다.

103) 정찰총국 소속으로 1997년 당 작전부(현 정찰총국 작전국)에 신설되었으며 전산정보처리, 암호해독, 해킹 등의 전문가를 양성하는 사이버공작 양성부서이다. 학제는 5년제이며 매년 30여 명의 신입생을 선발하고 입학 당시부터 인민군 '중위' 계급을 부여하고 있다.

104) 김흥광(2010), "북한의 사이버테러 정보전 능력과 사이버보안 대책 제언," p. 4.

105) "교육체계가 완비되고 있다,"『로동신문』, 2019.9.3.

다. 사이버공격 유형과 공격·방어능력

(1) 사이버공격 유형

북한의 사이버공격 유형은 크게 사이버 정보수집, 사이버심리전, 사이버테러, 사이버범죄, 사이버전 등으로 분류할 수 있다.[106] 사이버 정보수집은 주요 국가기관망, 공공망, 상용포탈망에 접속하여 광범위한 정보를 수집하고, 해킹 등을 통해 개인정보 및 특정정보를 대량으로 빼가는 공작 전개를 의미한다. 과거 국방과학연구소(Agency for Defense Development: ADD)의 컴퓨터 3,000여 대가 해킹당하여 군사기밀 2급 및 3급으로 분류된 보고서가 최소 수십 건에서 최대 수백 건 유출되었다.[107] 또한, 2016년에는 북한의 기습도발이나 전면전이 발생했을 경우를 대비한 한미 작전계획인 '작계 5027'의 일부가 유출된 것으로 밝혀졌다.[108] 2000년 이후 정보수집과 절취를 위해 청와대와 국회를 비롯한 정부 부처, 한국원자력연구원과 산업기술시험원 등 연구소, 그리고 신문과 방송 등 언론사들에 대한 북한의 해킹이 지속되고 있다.

사이버심리전은 대남 심리전 차원에서 북한이 운영하는 직영사이트와 해외 친북사이트를 활용하여 허위정보 및 역정보 등을 확산시키는 여론전을 의미한다.[109] 대남 사이버심리전은 통일전선부에서

106) 북한의 사이버안보위협 유형에 대해서는 윤규식, "북한의 사이버전 능력과 위협 전망," 『군사논단』, 제68호 (2011), pp. 69~70; 유동열, "북한의 대남 사이버위협 실태와 대책," pp. 27~32; 조성렬, "북한의 사이버전 능력과 대남 사이버위협 평가," 『북한연구학회보』, 제17권 제2호 (2013), p. 131 참조.

107) "국방과학硏 해킹… 軍기밀 수백건 유출," 『동아일보』, 2014.4.10., 〈http://www.donga.com/news/article/all/20140410/62408737/1〉 (검색일 : 2018.6.10.).

108) "북 해킹으로 작전계획 5027 유출 확인," 『중앙일보』, 2017.4.3., 〈https://news.joins.com/article/21436124〉 (검색일: 2019.9.7.).

109) 대남 심리전에 대해서는 유동열, "북한의 대남 사이버위협 실태와 대책," pp. 28~29 참조.

주도하고 있으며, 북한의 해외 개설 인터넷사이트는 구국전선(반제민전 홈페이지), 우리민족끼리(조평통 홈페이지), 조선중앙통신, 류경, 조선인포뱅크, 김일성방송대학, 백두넷 등 140여개에 달하며, 직영사이트는 노동신문 등 12개이다. 북한은 인터넷뿐만 아니라 페이스북, 트위터, 유튜브 등 SNS를 활용한 대남심리전을 지속하고 있다. 특히 통일전선전부와 정찰총국은 이른바 '댓글팀'을 운용하며 우리사회 내부에 조작된 정보와 여론을 확산시켜 국론분열과 사회교란을 시도하고 있다. 또한, 공개게시판, 토론방 등에 의도적으로 정부기관과 주요인사 등에 관한 악성루머를 유포하여 곤경에 빠뜨리는 'Flame 기법'도 활용하고 있다.

북한의 사이버테러는 DDos(DDos) 공격과 해킹 등을 통해 이루어지고 있다.[110] 북한은 2009년 7·7 DDos 공격을 시작으로 농협 전산망 마비(2011), 6·25 사이버 공격 및 3·20 사이버테러(2013), 한국수력원자력 해킹 및 청와대 사이버 공격(2014), 서울메트로 해킹 사건(2015) 등 지속적인 대남 사이버 공격을 지속하고 있다. 북한은 금융기관 전산망 해킹 및 공공망에 대한 DDos 공격과 주요 기반시설에 대한 사이버테러를 통해 우리 사회에 혼란을 가져오려는 시도를 지속하고 있다.

또한, 북한은 금전탈취 목적의 사이버범죄 역시 시도하고 있다. 『유엔안보리 전문가 패널 전문가 보고서』(2019.8.5.)는 북한이 2015년 12월~2019년 5월까지 최소 17개국의 금융기관과 가상화폐 거래소를 대상으로 35차례에 걸친 사이버 공격을 통해 최대 20억 달러(약 2조 4천억 원)를 탈취한 혐의가 있다고 밝혔다.[111] 그리고

110) 위의 글, pp. 30~31; 조성렬, 북한의 사이버전 능력과 대남 사이버위협 평가, p. 131 참조.

111) "北, 가상화폐 거래소 등 사이버 공격으로 2조원대 탈취 혐의," 『연합뉴스』, 2019.8.5., 〈https://www.yna.co.kr/view/AKR20190805011200073〉 (검색일: 2019.9.30.).

최근에는 가상화폐 거래소를 노린 공격이 두드러지고 있으며, 2017년 이후로만 북한 소행으로 추정되는 15건의 가상화폐 거래소 공격이 있었고, 이 가운데 10건은 한국의 거래소를 노린 것으로 밝히고 있다.

북한이 향후 사이버전을 감행하여 우리의 국가안보망과 군사망 무력화를 추진할 가능성도 있다. 북한군의 대표적 사이버전 공격수단으로는 러시아제를 개량한 'GPS 재머(Jammer)'와 현재 개발 중으로 알려진 '전자기 펄스(Electronic-Magnetic Pulse: EMP) 폭탄' 등이 있다.[112] 개량형 GPS 재머는 2010년 11월 23일 연평도 포격당시 우리 군의 대포병레이더(AN-TPQ) 작동을 방해하였으며, 2010년 12월 20일 연평부대의 해상사격 훈련 당시에는 무인정찰기(Unmanned Aerial Vehicle: UAV) 활동을 방해한 것으로 알려져 있다.[113]

(2) 사이버 공격·방어능력

북한의 사이버전 능력은 크게 공격과 방어로 나누어 구분할 수 있다. 북한의 사이버공격 능력은 미국 테크놀리틱스 연구소(Technolytics Institute) 케빈 콜만(Kevin Coleman)의 세계 10대 사이버전 능력 보유국에 대한 평가에서 나타나고 있다. 그는 북한의 사이버전 의지(Cyber Capabilities Intent)는 러시아에 이어 중국, 미국과 같은 세계 2위, 공격능력은 (Offensive Capabilities Rating)는 세계 6위, 사이버정보(Cyber Intelligence Rating)는 세계 7위로 평가하고 있다.[114] 미국 오바마(Obama) 대통령[115]과 헤리티지 재단은 사이버

112) 윤규식, "북한의 사이버전 능력과 위협 전망," p. 72.

113) 위의 글.

114) 케빈 콜만은 2009년도 세계 10대 사이버전 능력 보유국에 대해 미국(4.0), 중국

공격 능력에서 북한을 러시아나 중국, 이란보다 낮게 보고 있지만 위험한 수준으로 평가하고 있다.[116] 테크놀리틱스가 공개한 사이버 공격 능력 평가는 5점 만점을 기준으로 중국 4.2점, 러시아 4.0점, 이란은 3.4점, 북한 2.8점으로 나타나는 등 북한의 사이버공격 능력은 상당한 수준에 이르고 있다.[117]

미국의 사이버 보안업체인 크라우드스트라이크(Crowdstrike)는 2019년 2월 19일 '2019 글로벌 위협 보고(2019 Global Threat Report)'에서 미국의 주요 적대 국가들에 대한 사이버공격 능력을 평가하였으며, 북한의 사이버공격 능력을 러시아에 이어 세계 2위라고 발표했다.[118] 크라우드스트라이크는 사이버공격 능력을 해커가 목표물에 침투하는 속도를 기준으로 평가하였으며, 러시아 18분 49초, 북한 2시간 20분, 중국 4시간, 이란 5시간 9분 등의 순으로 나타났다. 북한의 사이버공격 능력에 대한 정확한 평가는 현재로서는 매우 어렵다고 볼 수 있다. 다만, 방글라데시 중앙은행 전산망 해킹,[119] 한

(4.0), 러시아(3.9), 인도(3.7), 이란(3.6), 북한(3.6), 일본(3.6), 이스라엘(3.6), 한국(3.2), 파키스탄(3.1)로 종합점수를 부여하고 있다. Kevin Coleman, "The Weaponry and Strategies of Digital Conflict," (*Proceedings of the 5th International Conference on Information Warfare and Security*, April 2010), p. 498 재인용: 조성렬, "북한의 사이버전 능력과 대남 사이버위협 평가," p. 133.

115) "Obama ranks N.Korea cyber capabilities as not so good," Bizcommunity, February 18, 2015 〈https://www.bizcommunity.com/Article/224/16/124630.html〉 (Accessed July 14, 2019); Dakota L. Wood ed., Index of US military Strength, Assessing America's Ability to Provide for the Common Defense (Washington D.C.: The Heritage Foundation, 2015) 재인용: 서형준·김인중, "북한의 사이버테러 실태와 능력분석을 통한 향후 활동 진단,"『국가정보연구』, 제8권 1호 (2015), p. 126.

116) Dakota L. Wood, *Ibid*.

117) 서형준·김인중, "북한의 사이버테러 실태와 능력분석을 통한 향후 활동 진단,"『국가정보연구』, 제8권 1호 (2015), p. 127.

118) "북한 사이버 공격 능력 러시아에 이어 세계 2위,"『세계일보』, 2019.2.20., 〈https://news.v.daum.net/v/20190220092745850〉 (검색일: 2019.6.30.).

119) 2016년 2월, 방글라데시 중앙은행이 뉴욕 연방준비은행에 예치하고 있던 1억 100만 달러(한화 약 1,167억원)를 도둑맞은 사건으로 국가 차원에서 사이버 공격을 통해

국수력원자력 대외비 문서 유출,[120] 소니 픽쳐스 해킹,[121] 3·20 전산 대란,[122] 농협 전산망 마비 사태[123] 등 '5대 해킹 사건'[124]을 통해 볼 때 상당한 수준에 이른 것만은 분명한 것으로 보인다.

북한의 사이버방어 능력은 방화벽이나 백신 등 보안소프트웨어 개발에 대해서는 알려져 있지만, 실질적인 방어능력과 관련된 발표나 자료는 현재까지 알려진 내용이 없다.[125] 그동안 북한의 사이버공간에 대한 공격은 많지 않았으며, 공격의 대부분은 국내 사이트가 아닌 해외에서 운영하는 웹사이트들에 대한 공격들이었으며 현재까지 '광명'을 비롯한 내부 인트라넷의 공격사례는 알려지지 않고 있다. 미국 정보기관들조차도 북한의 내부 인트라넷을 공격하는데 어려움을 겪고 있으며, 미국 국가안보국이 운영하는 해킹 전문팀인 '맞춤형 접속 작전팀(TAO)'도 북한 내부의 네트워크 해킹에는 실패했다.[126]

은행털이를 한 최초의 사례로 알려져 있다. 이 사건 조사결과 소니 픽쳐스 해킹을 주도한 라자러스(Lazarus) 그룹의 흔적이 발견되었다. 미국 재무부 해외자산통제국(OFAC)은 블루노로프와 라자루스 그룹이 협력했다고 설명했다.

120) 2014년 12월, '원전반대그룹'을 자칭하는 해커가 블로그와 트위터를 통해 한국수력원자력의 내부 자료를 유출하였으며, 유출자료에는 국내 원자력발전소의 설계도를 비롯하여 청와대, 국방부, 국정원 문서라고 주장하는 자료까지 공개되었다. 검찰은 해커 추정 인물이 북한 정찰총국 해커의 주무대인 중국 선양(瀋陽)시를 비롯한 특정 지역에서 접속했다고 발표했다.

121) 2014년 11월, 북한 김정은 노동당 위원장을 희화화한 영화 '인터뷰'를 제작한 소니 픽쳐스의 내부 자료가 유출된 사건이다. 제임스 코미 당시 FBI 국장은 북한이 소니 픽쳐스 해킹에 연관됐다는 결정적인 증거를 확인했다고 발표했다.

122) 2013년 3월 20일, KBS, MBC, YTN을 비롯한 방송사와 신한은행과 농협을 비롯한 금융기관에서 3만2천 대에 달하는 컴퓨터의 하드디스크가 파괴된 사건이다. 정부·민간 합동대응팀은 북한의 소행으로 적어도 8개월 이전부터 공격을 준비했다고 발표했다.

123) 2011년 4월 12일, 농협의 전산망 해킹으로 사흘 가까이 금융서비스가 중단된 사건이다. 검찰은 농협의 서버를 관리하는 업체 직원의 노트북이 북한 정찰총국이 배포한 악성코드에 감염되면서 농협 전산망을 공격했다고 발표했다.

124) 이에 대해서는 『BBC NEWS 코리아』, 2017.10.12., 〈https://www.bbc.com/korean/news-41584327〉 (검색일: 2019.6.30.) 참조.

125) 임종인 외, "북한의 사이버전력 현황과 한국의 국가적 대응전략," p. 20.

126) "전 세계 컴퓨터망 해킹한 NSA도 북한은 손 못대," 『조선일보』, 2013.10.26., 〈http:

북한이 운영하는 사이트에 대한 대표적인 공격으로는 2013년 4월과 5월 우리민족끼리와 조선의 소리에 대한 국제해킹조직 어나니머스(Anonymous)의 공격을 들 수 있다. 그리고 6월 25일에는 우리민족끼리(uriminzokkiri.com), 고려항공(airkoryo.com.kp), 벗(friend.com.kp), 노동신문(rodong.rep.kp), 평양산업대학(business-school-pyongyang.org), 여명(ryomyong.com), 노소텍(nosotek.com), 내나라(naenara.com.kp) 등에 대한 해킹공격이 이루어졌다.[127] 해킹 공격을 받은 주요 사이트들은 북한이 대외 홍보용으로 활용하고 있지만, 북한의 사이버공간 방어능력이 공격에 비해 취약함을 보여주는 사례로 볼 수 있다.

현재 북한의 해외 사이트들은 이용자가 적고 서버 규모가 작아 해킹에 대한 기본지식을 갖춘 5명 이상의 해커들에 의한 DDos 공격으로도 무력화될 수준이다.[128] 그러나 해킹공격을 받은 웹사이트가 대부분 북한의 홍보용 해외 사이트들이며, 북한의 내부망인 광명망이 건재함을 고려할 때 북한의 방어능력을 평가절하 하기에는 시기상조라고 볼 수 있다.[129] 오히려 북한은 해외 사이트들에 대한 사이버 공격을 통해 북한 스스로가 피해국임을 선전하고 이를 북한이 시도하고 있는 사이버 공격에 대한 정당성 논리로 활용하고 있다.

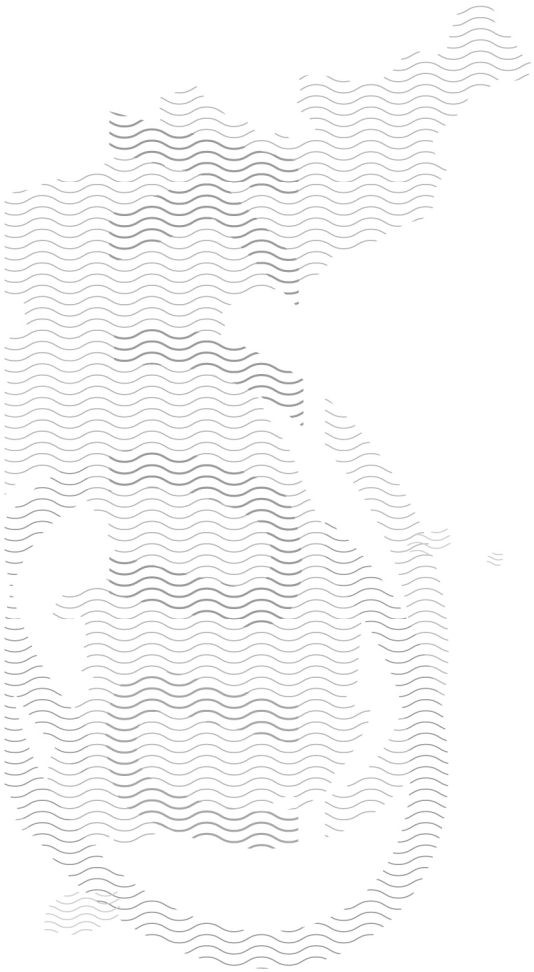
//news.chosun.com/site/data/html_dir/2013/10/26/2013102600341.html〉 (검색일: 2019.6.30.).

127) 조성렬, "북한의 사이버전 능력과 대남 사이버위협 평가," p. 130.

128) "6·25 남북 사이버전 어나니머스 주장 해커 실체는?"『머니투데이』, 2013.6.25., 〈https://news.mt.co.kr/mtview.php?no=2013062516471457890〉 (검색일: 2019.6.30.).

129) 임종인 외, "북한의 사이버전력 현황과 한국의 국가적 대응전략," pp. 20~21.

Ⅳ. 주변국의 사이버안보 환경과 한반도



1. 미국

가. 사이버공간에 대한 인식 및 환경

세계 IT 산업과 기술을 선도해 온 미국은 세계 유수의 정보 인프라를 구축하고 있으며, 정부와 민간 영역 또한 정보 인프라에 대한 의존도가 높기 때문에 외부로부터의 사이버 공격에 매우 취약한 국가 중 하나이다.[130] 또 한편으로 미국은 세계에서 가장 막강한 사이버 공격 능력을 보유한 나라이면서 사이버 반격 능력은 이에 미치지 못하는 것이 현실이기 때문에[131] 지금까지 외부의 적대세력들로부터 수많은 사이버 공격에 노출되어 왔다. 재래식 군사력에서 미국의 열세에 있는 국가들의 입장에서는 비용에 비해 효과적일 뿐만 아니라 은밀한 공격이 가능하고 추적이 어렵다는 이점을 활용하여 미국에 대한 비대칭적 공격을 강화하고 있는 것이다.

21세기에 들어와 발생한 대표적인 사례로는 2003년 중국으로 의심되는 침입자가 록히드 마틴사(Lockheed Martin Corporation), NASA(National Aeronautics and Space Administration, 미국항공우주국) 등을 공격한 타이탄 레인(Titan Rain)사건, 이용자의 컴퓨터 입력을 등록하는 스팸 메일이 방위산업관계자 등에게 발송된 포이즌 아이비(Poison Ivy)사건, 2009년 북한으로 의심되는 세력이 미국의 독립기념일에 미국의 연방정부 사이트 및 민간기업 사이트에 대한 DDos 공격을 감행한 인디펜던스 사건(한국에선 7·7 DDos 대란), 2014년 북한으로 의심되는 세력에 의한 소니 픽처스(Sony Pictures) 해킹 사건, 2015년 중국 정보기관에 의해 미국 정부 인사

130) 차정미, "미중 사이버 군사력 경쟁과 북한 위협의 부상," 김상배 편, 『사이버안보의 국가전략 2.0』 (서울: 사회평론 아카데미, 2019), p. 222.

131) 데이비드 E. 생어 지음, 정혜윤 옮김, 『퍼펙트 웨폰』 (서울: 미래의 창, 2019), p. 13.

관리청의 컴퓨터에서 2100만 명이 넘는 정부 인사들의 정보가 유출된 해킹 사건, 2016년 대선 러시아로 추정되는 해커집단에 의해 당시 민주당 지도부 인사 100명의 이메일이 해킹 당한 사건 등이 있다. 이 외에도 미국 정부는 2017년 미국 IT기업으로부터 5억 건 이상의 개인정보를 유출시킨 사건의 주범으로 러시아연방보안청(Federal Security Bureau: FSB) 요원 2명을 포함한 4명의 해커를 기소하였으며, 2018년에는 중국국가안전부와 연계된 해커 집단 APT10이 미국 기업으로부터 방위, 우주, 항공, 자원 개발과 관련된 정보를 유출시켰다고 발표하였다.

한편, 미국의 정보공동체의 컨트롤 타워 역할을 하는 국가정보장(Director of National Intelligence: DNI) 제도가 만들어진 이후 국가정보장은 매년 『세계 위협 평가(Worldwide Threat Assessment)』라는 연례 보고서를 연방의회에 제출하고 있다. 2000년대 중반까지만 하더라도 이 보고서에 나오는 국가안보 관련 가장 중요한 사안은 테러리즘과 관련된 것들이었다. 그러나 2010년대에 들어 핵심기반시설에 대한 사이버 공격 등 다양한 종류의 사이버 공격은 테러리즘을 제치고 미국의 국가안보에 가장 큰 위협으로 등장하였다.

예를 들자면, 2018년 2월 다니엘 코트(Daniel R. Coats) 미 국가정보장이 상원특별정보위원회(Senate Select Committee on Intelligence)에 보고한 연차 보고서 『전세계 위협 평가(Worldwide Threat Assessment)』는 미국에 대한 사이버위협의 주체로 러시아, 중국, 이란 및 북한을 명시하였다.[132] 구체적으로 살펴보면 러시아는 미국 및 동맹국의 핵

132) Daniel R. Coats, "Worldwide Threat Assessment of the US Intelligence Community," pp. 5~7, 〈https://www.intelligence.senate.gov/sites/default/files/documents/os-dcoats-021318.PDF〉 (Accessed June 20, 2019) 참고로 중국, 러시아, 이란 및 북한의 사이버 공격의 양상과 이에 대한 트럼프 행정부의 대응과 관련해서는 김상배, "트럼프 행정부의 사이버안보전략: 국가지원 해킹에 대한 복합지정학적 대응," 『국제지역연구』, 제27권 제4호 (2018) pp. 10~18.

심기반시설에 대한 정찰을 계속함과 더불어 사이버 첩보를 얻기 위해 미국과 NATO 동맹국을 표적으로 삼고 있다는 점, 중국의 경우 국가안보상의 우선사항으로 사이버첩보를 실시함과 더불어 사이버 공격능력을 향상시키고 있다는 점, 이란은 첩보 및 향후 사이버공격 준비를 위해 미국 및 미국의 서방 동맹국들에 대한 침투활동을 계속적으로 실시하고 있다는 점, 북한의 경우 금전획득, 정부수집 그리고 한국과 미국에 대한 공격을 실시하기 위해 사이버활동을 이용한다는 점을 예로 들고 있다.

이러한 인식은 같은 해 9월 미 국방부가 발표한 국방부 사이버 전략(DoD Cyber Strategy)에도 반영되었다. 이 전략에서는 미국의 정부 및 민간조직으로부터 기밀정보를 절취하고, 미국의 군사적 우위와 경제 활력을 저하시키려 하고 있다고 중국을 평가하는 한편, 러시아에 대해서는 사이버공간을 이용한 정보공작 활동으로 미국 국민들에게 영향을 미치고 미국의 민주주의적 절차를 위협하고 있다는 인식을 보였다. 한편, 올해 1월 미 상원 특별정보위원회에 보고된 전세계위협평가는 미국에 대한 최대의 위협으로 선거 개입과 사이버 공격, 스파이 행위를 명시하고 있다.[133] 보고서는 "우리는 모든 적대국 및 전략적 경쟁상대가 미국의 정책에 영향을 미치기 위해, 사이버공간에서의 스파이행위, 사이버 공격, 영향력 강화를 전개해 갈 것"이란 전망을 내놓았다. 이와 관련하여 보고서는 중국과 러시아를 미국의 핵심기반시설에 대한 최대의 잠재적 공격자로 지목한 뒤 이들 두 나라는 수 일 또는 수 주간의 혼란을 일으킬 능력을 보유하고 있음을 밝히고 있다. 또 보고서는 러시아가 미국을 대상으로 활발한 사이버 첩보활동을 벌이고 있으며, 2016년 대통령선거 때

133) Daniel R. Coats, "Worldwide Threat Assessment of the US Intelligence Community," pp. 5~6. 참고로 중국, 러시아, 이란 및 북한의 사이버 공격의 양상과 이에 대한 트럼프 행정부의 대응과 관련해서는 위의 글, pp. 10~18.

와 같이 다가오는 2020년 대통령 선거 때도 사이버 공격을 통한 선거 개입을 해 올 가능성이 있다고 지적하고 있다.

이에 더해 보고서는 사이버 첩보활동과 관련하여 중국을 미국의 경쟁상대로 지목하고 있으며, 중국의 IT기업이 미국에 대한 스파이 활동에 동원되고 있다는 시각을 제시하고 있다. 이는 미국이 최근 미중 무역 분쟁 과정에서 중국의 통신장비 기업인 화웨이에 대한 제재조치를 발동한 이유를 설명해 주는 대목이라 하겠다.

나. 사이버안보 전략 및 추진체계

〈표 Ⅳ-1〉 미국의 사이버안보 관련 주요 전략과 행정명령

주요 전략 및 행정명령	발표시기	작성 부처
The Comprehensive National Cybersecurity Initiative	2008.1.	백악관
Cyberspace Policy Review	2009.5.	백악관
International Strategy for Cyberspace	2011.5.	백악관
Department of Defense Strategy for Operating in Cyberspace	2011.7.	국방부
Executive Order 13636 “Improving Critical Infrastructure Cybersecurity”	2013.2.	백악관
The Department of Defense Cyber Strategy	2015.4.	국방부
Executive Order 13800 “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure”	2017.5.	백악관
National Defense Strategy	2018.1.	국방부
National Cyber Strategy	2018.9.	백악관

출처: 저자 작성

(1) 오바마 행정부의 사이버안보 전략

미국에서 사이버안보는 부시(George W. Bush) 행정부 말기에 들어서부터 미국의 국가안보에 있어 최우선 사항으로 간주되기 시작하

였다. 이러한 인식은 2008년 '국가사이버안보 종합계획(The Comprehensive National Cybersecurity Initiative: CNCI)'으로 구체화되었는데, 미국은 포괄적인 사이버안보 전략인 CNCI를 마련함으로써 사이버안보 정책의 토대를 다지게 되었다.[134] 부시 행정부의 뒤를 이어 탄생한 오바마 행정부는 사이버안보정책에 대한 재검토를 60일에 걸쳐 실시하도록 지시한 뒤 이를 기반으로 새로운 전략문서를 마련하였는데, 이것이 2009년 5월 발표된 '사이버공간정책리뷰(Cyberspace Policy Review: CPR)'이다.[135] CPR은 새롭게 출범한 오바마 정부가 실시하고자 하는 10개의 단기행동계획과 14개의 중기행동계획을 제시하고 있는데, 10개의 단기행동계획의 경우 지금의 미국의 사이버안보정책에 대폭 반영되었다는 점에서 주목할 필요가 있다.[136] 이 보고서를 토대로 2009년 6월에는 미 전략사령부(U.S. Strategic Command: USSTRATCOM) 산하에 사이버군(USCYBERCOM)이 창설되어 국가안보국(National Security Agency: NSA) 장관인 키스 알렉산더(Keith Alexander)가 초대 사령관을 겸임하게 되었다. 같은 해 12월에는 연방정부 부처의 컨트롤 타워 역할을 하는 사이버안보조정관(Cybersecurity Coordinator)이라는 직책이 백악관 내에 신설되어 하워드 슈미트(Howard Schmidt)가 초대 조정관에 임명되었다. 이에 더해

134) White House, "The Comprehensive National Cybersecurity Initiative," 〈https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-034.pdf〉 (Accessed June 20, 2019).

135) White House, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," 〈https://www.energy.gov/sites/prod/files/cioprod/documents/Cyberspace_Policy_Review_final.pdf〉 (Accessed June 20, 2019).

136) CPR에서 제시한 10개의 단기행동 계획은 다음과 같다. ① 사이버안보 정책을 통괄하는 부처 창설, ② 국가안보정책과 사이버정책 재검토, ③ 연방정부내의 사이버안보에 관한 평가기준 마련, ④ NSC의 사이버안보 담당국에 의한 프라이버시 인권 담당자 지명, ⑤ 사이버안보 관련 우선과제에 대한 부처횡단적인 메커니즘 구축, ⑥ 사이버안보에 관한 교육 및 계몽, ⑦ 사이버안보 관련 국제연대 강화, ⑧ 사이버안보 사업에 대한 대응능력 강화 및 민관연대 강화, ⑨ 사이버안보에 관한 연구개발 추진, ⑩ 프라이버시 인권에 대응한 사이버안보 강화.

2010년 2월에 발표된 4개년 국방전략재검토(Quadrennial Defense review: QDR) 보고서에는 육·해·공·우주에 이은 제5의 작전영역으로 사이버공간이 명확하게 제시되었다.[137] 더불어 2011년 7월에는 '국방부 사이버공간전략(Department of Defense Strategy for Operating in Cyberspace)'이라는 명칭의 사이버전략이 국방부 최초로 발표되었는데, 여기에는 필요하다면 사이버 공격에 의한 보복을 실시할 뿐만 아니라 재래식 전력의 행사도 마다하지 않겠다는 방침이 천명되었다.

한편 오바마 정부는 2013년 2월 핵심 기반시설의 사이버안보 강화를 위한 대통령령을 발동하여 민관영역의 정보공유제체구축을 위한 작업을 국토안보부, 국방부, 및 미국국립표준기술원(National Institute of Standards and Technology: NIST)등에 지시하였다. 국가의 핵심기반시설인 사이버 환경 유지에 대해 민간의 핵심기반시설 사업자들 간의 사이버안보에 관한 정보공유를 강화하고 협력하여 리스크 대응의 표준화를 진행하는 방침을 제시한 것은 주목할 대목이다. 앞서 언급한 CPR과 더불어 미연방정부는 이 대통령령을 선포함으로써 사이버안보 정책의 토대를 마련하게 되었다.[138]

2011년에 이어 두 번째로 발표된 2015년 국방부사이버전략(DoD Cyber Strategy)에는 ① 국방부의 네트워크, 시스템 정보 방어, ② 사이버 공격에 의한 심각한 결과로부터 미국의 국토와 권익 보호, ③ 군사작전 지원을 위한 통합적인 사이버 능력 제공 등 3가지가 사이버공간에서의 국방부의 중요한 임무로 규정되었고, 이러한 사이버 능력에는 적국 군사시스템 파괴를 목적으로 한 사이버 작전(Cyber Operation)도 포함된다는 점이 명시되었다.[139]

---

137) U.S. Department of Defense, "Quadrennial Defense Review," 〈http://www.defense.gov/qdr/〉 (Accessed September 12, 2019).

138) 田村賢吾, "サイバーセキュリティ対策–人材対策を中心に," 『損保総研レポート』, 第122号 (2018), p. 14.

(2) 트럼프 행정부의 사이버안보 전략

트럼프 행정부 들어 발표된 최초의 사이버안보 관련 정책조치는 수 차례의 수정과정을 거쳐 2017년 5월 트럼프 대통령이 서명한 미국 연방정부의 「네트워크 및 핵심기반시설 사업자의 사이버안보 강화에 관한 행정명령(Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infra-structure)」이다.[140] 먼저 이 행정명령은 3가지 핵심 사항으로 ① 연방정부의 네트워크에 관한 사이버안보, ② 핵심 기반시설에 관한 사이버안보, ③ 국가/국민을 위한 사이버안보에 대한 기술과 더불어 각각의 연방정부 기관의 장에 대해 대통령에 대한 보고서를 기한 내에 제출할 것을 지시하는 내용을 담고 있다. 이러한 행정명령의 내용은 오바마 행정부가 추진해 온 사이버안보 정책에 대한 이탈이나 180도 전환을 의미하지는 않지만, ① 연방정부기관장에 대한 직접적인 사이버안보 위협 관리책임 부여, ② 높은 위협에 처해 있는 핵심 기반시설 방호 및 사이버 침해사고 대책 강화, ③ 국제연대 및 미래 사이버안보 인재육성 중시 등의 개선책을 제시하고 있다는 점은 평가할 만하다.[141]

2017년 12월에는 트럼프 행정부 최초의 「국가안보전략」(National Secruity Strategy: NSS)이 발표되었다.[142] 이 보고서는 '미국 제

---

139) U.S. Department of Defense, "The DoD Cyber Strategy," pp. 4~5, 〈https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf〉 (Accessed September 20, 2019).

140) White House, "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," 〈https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/〉 (Accessed September 14, 2019)

141) 中沢潔, "トランプ政権におけるサイバーセキュリティ政策の現状" 『JETRO』, 2017.9, pp. 1~2.

142) White House, "National Security Strategy 2017," 〈https://www.whitehouse.g

일주의(America First)'의 관점에서 미국의 핵심이익을 ① 미국 국민, 미국 영토, 그리고 삶의 방식 보호(Protect the American People, the Homeland, and the Way of Life), ② 미국의 번영 촉진(Promote American Prosperity), ③ 힘을 통한 평화 보존(Preserve Peace Through Strength), ④ 미국의 영향력 확대(Advance American Influence) 등 4가지로 규정하였고, 이 네 가지 축을 중심으로 미국이 취해야 할 전략들을 구체적으로 제시하였다. 이 보고서는 또한 '힘을 통한 평화(peace through strength)'를 이룩하기 위해 군사, 핵무기, 우주, 사이버, 정보 등의 영역에서의 역량을 강화하겠다는 점을 천명하고 있다.

특히 사이버안보와 관련한 대목에서는 국가들이 사이버 능력을 외부에 대해 영향력을 행사하는 수단으로 간주한다는 점 및 사이버 공격이 현대전의 중요한 특징이 되었다는 점을 지적한 뒤, 미국에 대해 사이버 공격을 감행하는 상대방을 억지, 방어하고 때에 따라서는 반격에 나설 수도 있다는 점을 명확히 하고 있다. 그리고 이를 위한 대응 방안으로 ① 사이버 공격 특정 및 신속대응능력 개선, ② 미국 정부의 재산, 핵심기반시설, 정보 등을 보호하기 위한 사이버 수단 및 전문지식 향상, ③ 필요에 따라 적에 대해 사이버 작전을 실시할 수 있도록 미국 정부 권한 및 절차의 통합개선 등을 도모하는 전략방침을 제시한다.

이에 더해 "사이버범죄를 저지른 범죄자를 두둔하는 국가에게 책임을 지게 한다", "현저하게 악의적인 사이버활동을 전개하는 외국 정부, 범죄자 등에 대해 신속하고도 값비싼 대가를 지불하게 한다", "책임소재(attribution)에 대한 분석능력을 향상시킨다" 등의 표현

---

ov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf〉 (Accessed September 12, 2019).

이 반영된 점도 눈여겨 볼 대목이다. 이와 관련하여 일본의 사이버안보 전문가이자 총무성의 총합통신기반국장인 다니와키 야스히코(谷脇康彦)는 트럼프 행정부 들어 미국의 사이버안보 정책에서 '책임부과(assigned responsibility) 억지전략' 이 보다 강화되고 있는 것으로 평가한다.[143]

2018년 2월에는 미국 핵정책의 근간이라 할 수 있는 『핵태세 검토보고서(Nuclear Posture Review)』가 8년 만에 미 국방부에 의해 발표되었다.[144] 이 보고서는 적의 핵공격이 없더라도 핵무기 선제사용이 가능하고, 저강도의 소형핵무기 개발도 추진한다는 내용을 담고 있어 중국과 러시아의 반발을 가져왔다. 그러나 이보다 더 충격적인 것은 "사이버 무기로 전력망, 통신망, 수도 시설 등 미국의 핵심 기반시설을 위협하는 나라들에게 국가안보 차원에서 핵무기로 대응하는 방안까지도 고려할 것"이라는 내용이 포함되었다는 것이다.[145]

이 보고서를 필두로 트럼프 행정부의 사이버안보 정책은 악의적인 사이버 공격에 대해 이전보다 훨씬 더 공격적인 성향을 드러내게 된다. 대표적인 사례가 2018년 9월 트럼프 대통령이 서명한 행정명령과 국방부가 4년 만에 발표한 「국방부 사이버전략」(DoD Cyber Strategy)이다. 오바마 행정부 시기에는 미 국방부가 사이버 공격을 수행할 경우에는 연방정부 부처들로부터 사전 승인을 받도록 되어

---

143) 谷脇康彦, 『サイバーセキュリティ』 (東京 : 岩波新書, 2018), pp. 135~136. 참고로 '책임부과 억지전략'이란 공격자를 특정하여 경제적 제재나 외교적 제재를 가함으로써 사이버공격이 큰 대가를 치르게 되는 상황을 연출하고 이를 통해 공격을 단념시키는 것이다. 사이버 억지전략과 관련해서는 장노순·한인택, "사이버안보의 쟁점과 연구 경향," 『국제정치논총』, 제53집 3호 (2013), pp. 594~599을 참조.

144) Office of the Secretary of Defense, "Nuclear Posture Review," 〈https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF〉 (Accessed September 18, 2019).

145) 데이비드 E. 생어, 『퍼펙트 웨폰』, p. 6.

있었지만, 이 행정명령이 채택됨으로써 국방부를 비롯한 정부기관들은 외국의 적들에 대한 사이버 공격에 보다 많은 권한을 가지게 되었다.[146]

국방부가 발표한 새로운 「국방부 사이버전략」(DoD Cyber Strategy) 또한 공세적인 사이버안보 정책을 반영하고 있다.[147] 2015년 전략에 이은 2018년 전략은 미국이 중국·러시아와 장기적인 경쟁관계에 돌입하였다는 점, 그리고 중러 양국은 사이버공간에서의 활동을 통해 경쟁을 확대시킴으로 인해 미국과 그 동맹국 및 우호국에 대한 전략적 위협요인이 되고 있다는 점을 지적한 뒤, 이에 대한 대응방안으로 ① 사이버 군의 역량강화 가속, ② 악의적인 사이버활동에 대한 대항·억지를 위한 방위, ③ 동맹국 및 우호국과의 협력촉진과 같은 접근법을 제시하였다.

대통령 행정명령과 국방부 사이버 전략과 더불어 같은 해 9월 20일에는 새로운 「국가사이버전략(National Cyber Strategy)」도 발표되었다.[148] 이 보고서는 2017년에 작성된 국가안보전략과 마찬가지로 미국의 핵심이익을 ① 미국 국민, 미국 영토, 그리고 삶의 방식 보호(Protect the American People, the Homeland, and the Way of Life), ② 미국의 번영 촉진(Promote American Prosperity), ③ 힘을 통한 평화 보존(Preserve Peace Through Strength), ④ 미국의 영향력 확대(Advance American Influence) 등 4가지로 규정하고, 이 네 가지 축을 중심으로 미국이 취해야 할 사이버안보 전략들을 구체

146) 김상배, "국가사이버안보전략 화급하다," 『디지털 타임스』, 2018.10.15., 〈http://www.dt.co.kr/contents.html?article_no=2018101602102269640001〉 (검색일: 2019.9.18.).

147) 防衛省, 『令和元年国防白書』 (東京：日経印刷, 2019), p. 171.

148) White House, "National Cybersecurity Strategy," 〈https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf〉 (Accessed September 30, 2019).

적으로 제시하고 있다. 이 보고서의 핵심은 ① 연방정부의 네트워크와 핵심기반시설 보호, ② 디지털경제의 번영, ③ 사이버억지 이니셔티브 개시, ④ 개방적이고 상호 운용적이며 안전하고 신뢰할 수 있는 인터넷 유지 등을 언급하고 있다는 점이다.

(3) 사이버안보 추진체계

미국 연방정부의 사이버안보 추진체제를 보게 되면, 백악관의 국가안전보장회의 산하 사이버안보국(Cybersecurity Directorate), 국가정보장(Director of National Intelligence: DNI) 및 그 산하의 사이버위협 정보종합센터(Cyber Threat Intelligence Integration Center: CTIIC), 국토안보부(Department of Homeland Security: DHS)와 그 산하의 국가보호 프로그램총국(National Protection and Programs Directorate: NPPD)과 사이버안보통신통합센터(National Cybersecurity Communication Integration Center: NCCIC), 정보공유분석기구(Information Sharing and Analysis: ISAC) 및 US-CERT(United States Computer Emergency Readiness Team), 상무부(Department of Commerce: DOC) 산하의 국립표준기술원(National Institute of Standards and Technology: NIST), 국무부(Department of State: DoS) 산하의 사이버이슈 조정관실(Office of the Coordinator for Cyber Issues: S/CCI), 국방부(Department of Defense: DoD) 및 국방부 소관의 국가안보국, 사법부(Department of Justice: DoJ) 산하의 연방수사국(Federal Bureau of Investigation: FBI) 등의 조직이 각 분야별로 사이버안보 업무를 담당하고 있다.[149] 이를 도식화하면 〈그림 Ⅳ-1〉과 같으

149) 김상배, "트럼프 행정부의 사이버안보전략: 국가지원 해킹에 대한 복합지정학적 대응," pp. 19~20.

며, 미국의 사이버안보 관련 각각의 주요기관의 역할 및 임무는 다음과 같다.

먼저 백악관 국가안전보장회의(NSC) 산하의 사이버안보국은 대통령에 대한 정책자문의 역할을 수행한다.[150] 한 가지 특기할 점은 트럼프 행정부에 들어와 미국 연방정부 부처의 사이버안보 컨트롤타워 역할을 해 온 사이버안보조정관 제도가 2018년 5월 폐지되었다는 점이다. 사이버안보조정관 제도는 오바마 행정부 시절이던 2009년 5월에 설치되어 연방정부의 사이버안보 정책을 주도해 왔지만, 트럼프 행정부 하에서 폐지됨으로써 미국의 사이버안보 전략의 변화를 초래하고 있다.

국가정보장(Director of National Intelligence: DNI) 제도는 CIA, FBI, NSA와 같은 미국의 정보공동체(Intelligence Community)가 9·11테러를 미연에 방지하지 못하였다는 점과 2003년 이크라에 대한 침공 당시 이라크의 대량살상무기 보유에 대한 미국 정보공동체의 정보분석 오류에 대한 반성에서 비롯되었으며, 정보공동체의 통합과 효율적 운용을 위해 2004년 성립한 정보개혁 및 테러방지법(The Intelligence Reform and Terrorist Prevention Act of 2004)에 기초하여 마련되었다.[151] DNI는 중앙정보국을 비롯한 미국의 17개 정보기관의 컨트롤타워 역할을 하고 있으며, DNI 산하의 사이버위협정보종합센터(CTIIC)는 사이버안보 위협과 침해사고 등을 종합적으로 분석하여 유관기관에 대한 정보제공 역할을 한다.[152]

국토안보부는 연방정부내의 사이버안보 정책에 있어 중심적인 역

150) 김소정·양정윤, "미국과 중국의 사이버안보 전략과 한국의 안보정책에 대한 함의," 『국가안보와 전략』, 제17권 2호 (2018), pp. 6~7.

151) 小林良樹, 『インテリジェンスの基礎理論』 (東京 : 立花書房, 2014), pp. 210~214.

152) 신성호, "미국의 사이버안보 전략과 외교," 김상배 편, 『사이버안보의 국가전략』, (서울: 사회평론, 2018), p. 149.

할을 하고 있다. 국토안보부는 2001년에 발생한 9·11테러를 계기로 2002년에 신설된 조직으로 사이버안보를 비롯한 모든 위협으로부터 미국의 안전을 지켜내고자 하는 차원에서 조직되었다. 국토안보부에서 핵심기반시설의 안전과 위협에 대한 대처를 담당하는 것이 사이버·인프라보안청(Cybersecurity and Infrastructure Security Agency: CISA)이며, 사이버안보 위협에 대한 대처도 주요 임무 중 하나이다. CISA는 2018년 11월 16일 트럼프 대통령이 CISA관련 설립법안 서명을 통해 기존에 존재하던 국가보호·프로그램 총국(NPPD)이 승격하여 만들어진 것으로 CISA의 발족으로 모든 위협이나 리스크로부터 핵심기반시설을 방호하는 체제가 한층 강화되었다. CISA는 사이버 보안, 핵심기반시설보안, 응급 대응 담당 등 세 부서로 구성된다.[153] 국가사이버안보정보통합센터(NCCIC)는 핵심기반시설을 중심으로 한 사이버정보의 집약기관으로 '민관 정보공유'의 역할을 담당한다.[154] NCCIC의 산하에는 사이버침해사고 대응을 담당하는 US-CERT 및 산업제어시스템에 대한 사이버공격 정보를 수집하는 ISC-CERT(Industrial Control Systems Cyber Emergency Response Team)등이 있으며, 정보공유 분석센터(ISAC), 정보공유분석기구(ISAOs) 등의 기구로부터 사이버공격에 대한 정보를 수집 공유한다.[155] ISAOs는 사이버 위협에 대한 정보

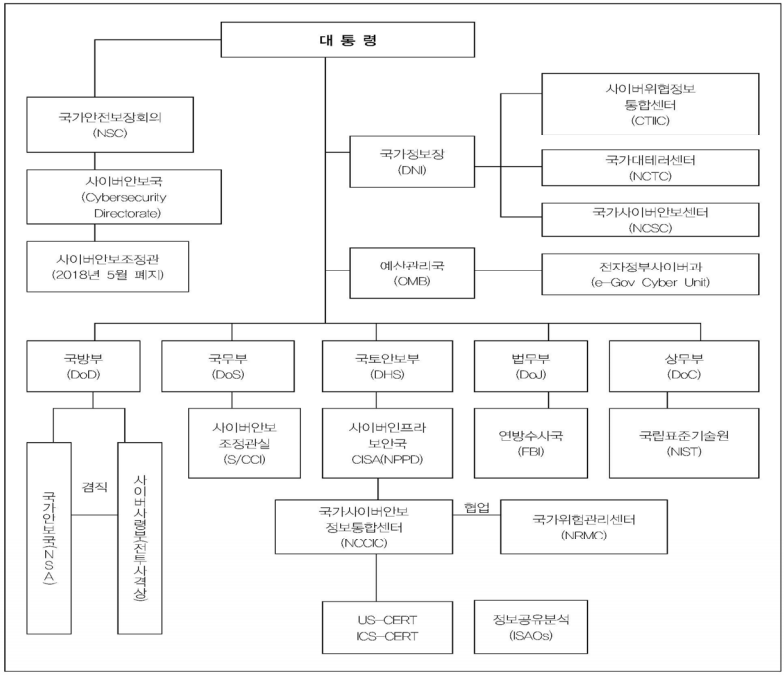
153) 김상배, "트럼프 행정부의 사이버안보전략: 국가지원 해킹에 대한 복합지정학적 대응," p. 24.

154) 2015년에 만들어진 사이버안보법(Cybersecurity Act of 2015)에 의하면 NCCIC는 연방정부와 민간기업간의 사이버안보 관련 정보의 창구역할을 담당하는 것으로 되어 있다. 笹川平和財団 安全保障事業グループ, 『サイバー空間の防衛力強化プロジェクト 製作提言: 日本にサイバーセキュリティ庁の設立を!』 2018.10, p. 15. 〈https://www.spf.org/global-data/20181029155951896.pdf〉 (검색일: 2019.10.5.).

155) 전완주, "미국의 사이버안보 수행체계 특징 및 시사점 고찰," 『신안보연구』, 통권 189호, (2016), pp. 33~36; 이동범·곽진, "미국 정부의 사이버 공격에 대한 보안전략," 『정보보호학회지』, 제24권 1호 (2014), pp. 18~19.

공유 및 분석을 실시하는 조직이다. ISAC가 금융, 에너지 등 핵심기반시설 분야마다 설립되어 있는데 반해, ISAOs는 ISAC가 조직되어 있지 않은 분야 및 ISAC의 멤버가 아닌 민간기업 등을 대상으로 하는 것이 특징이다.[156]

〈그림 Ⅳ-1〉 미국의 사이버안보 추진체계



출처: 김상배, "트럼프 행정부의 사이버안보전략: 국가지원 해킹에 대한 복합지정학적 대응," 『국제지역연구』, 제27권 제4호 (2018) p. 20을 참고로 재구성.

상무부(DoC) 산하의 국립표준기술원(NIST)은 미국에서 가장 오래된 물리과학연구소의 하나로 1901년에 설립되었다. NIST는 2013년 2월 12일 발표된 대통령령에 의해 핵심기반시설의 사이버 리스크를

156) 田村賢吾, "サイバーセキュリティ対策–人材対策を中心に," p. 16.

줄이기 위한 프레임워크를 구축하는 임무를 맡았으며, 이듬해인 2014년 2월「핵심기반시설의 사이버안보를 향상시키기 위한 프레임워크(Framework for Improving Critical Infrastructure Cybersecurity)」초판을 발표하였다.[157]

미 국무부(DoS)는 외교적 노력, 국제 관여 및 조정을 통해 국제사회에서 사이버공간과 관련한 미국의 국익을 증진시키는 역할을 수행하며 국제사이버 전략 작성을 담당한다. 국무부 산하의 사이버 이슈 조정관실(S/CCI)은 미국의 외교 정책, 국가 안보, 인권 및 경제 명령에 영향을 미치는 모든 국제 사이버 정책 이슈에 대한 외교적 대응을 전담하고 있다. 2011년에 설립된 S/CCI의 주도적 노력으로 국제 사이버 이슈가 외교 정책의 우선순위로 대두되었으며, 20개 이상의 국가에서 외교부 산하에 이와 유사한 전담부서를 설립하고 있다.[158]

미 국방부(DoD)의 사이버사령부(United States Cyber Command: USCYBERCOM)는 사이버공간에서의 작전 통괄 임무를 맡고 있으며, 사이버 사령부는 국방부의 정보환경을 운용 방위하는 '사이버방호부대', 국가차원의 위협으로부터 미국 방위를 지원하는 '사이버국가임무부대' 및 통합군이 실시하는 작전을 사이버 측면에서 지원하는 '사이버전투임무부대' 등으로 구성되어 있다.[159] 원래 사이버사령부는 오바마 정권 시기인 2009년 핵전력부대 통괄 및 미사일 방위를 담당하는 전략사령부(US Strategic Command) 산하에 신설되었지만, 2018년 5월 전략사령부와 동격인 통합사령부(United Command)로

157) 위의 글, p. 17.

158) U.S. Department of States, "About Us-Office of the Coordinator for Cyber Issues," 〈https://www.state.gov/about-us-office-of-the-coordinator-for-cyber-issues/〉 (Accessed September 20, 2019).

159) 防衛省, 『平成30年度防衛白書』 (東京 : 日経印刷, 2018), p. 204.

승격함으로써 사이버군 사령관은 다른 통합군 사령관과 마찬가지로 국방장관에 대해 직접 보고를 할 수 있게 되었다.

국방부 산하의 국가안보국(NSA)은 통신감청 등 신호정보(SIGINT)에 특화된 미국을 대표하는 정보기관 중 하나로 사이버공간에 대한 감시 및 정보수집활동 그리고 사이버 공격에 대한 대처에 있어 핵심적인 역할을 담당한다. NSA의 경우 냉전해체 이후 10여 년간 진영대립이 종식되고 외부로부터의 국가안보 위협이 사라지면서 정보기관의 존립자체가 의문시되고 조직의 예산과 활동이 대폭 축소되는 시기를 거치기도 했다. 그러나 2001년 발생한 9·11테러를 계기로 국가안보가 미국이 당면한 최우선 과제로 떠오르면서 NSA는 대규모 테러사태를 방지하기 위한 대책의 일환으로 사이버공간에 대한 감시활동을 주도하게 되었고, 급증하는 사이버 위협에 대한 대응 또한 이들의 활동영역으로 확대되었다. NSA의 장관은 미국 국방부 산하의 USCYBERCOM 사령관을 겸임하며, USCYBERCOM의 본부 또한 매릴랜드州의 포트 미드(Fort Meade)에 있는 NSA 본부에 위치한다.[160] 2013년 NSA의 계약사원이었던 에드워드 스노든(Edward Snowden)이 NSA를 비롯한 미국 정보기관의 비밀 통신감청 활동을 폭로함으로서 베일에 가려져 있던 사이버공간을 무대로 한 NSA의 통신감청 활동이 드러나기도 하였다. 2019년 10월에는 북한, 중국, 러시아 등 사이버안보 위협국에 대한 국가별 맞춤 대응을 위해 사이버안보국을 설치할 예정이다.[161]

법무부 산하의 연방수사국(FBI)은 범죄수사를 주된 임무로 하는 법집행기관이지만, 테러대책, 방첨과 같은 국가안보에 깊이 관여된

160) 2017년 8월 트럼프 대통령은 사이버사령부의 승격을 명령함과 동시에 국방장관에 대해 동 사령부의 NSA로부터의 분리 가능성에 대해서도 검토를 지시하였다고 한다. 中沢潔, “トランプ政権におけるサイバーセキュリティ政策の現状,” pp. 17~19.

161) 전채은, “미 NSA, 북해킹 막는 사이버보안부 10월 출범,”『동아일보』, 2019.9.6.

범죄 수사도 담당하며, 사이버 범죄 또한 중요 활동 영역 중 하나이다. NSA와 더불어 9·11테러 이후 그 기능이 강화되고 있는 정보기관 중 하나이기도 하다. 사이버범죄 수사는 FBI본부의 사이버범죄 부문이 통괄하며, 인터넷범죄고충센터(Internet Crime Complaint Center: IC3) 및 사이버액션팀(Cyber Action Team: CAT)과의 연대를 통해 컴퓨터와 네트워크에 대한 부정침입 수사에 우선적으로 대응하고 있다. IC3는 사이버상의 범죄행위 관련 피해 상황 및 관련 정보를 접수받아 FBI 등 관련기관에 통보하는 역할을 담당하며, CAT의 경우 FBI의 사이버 범죄 부문에 의해 설립된 사이버범죄 수사를 전담하는 특별 팀으로 수사관, 분석관 외에도 컴퓨터 감식 수사관과 악성코트 전문가가 수사에 참여한다.[162]

다. 사이버 국제협력

(1) 기본방침

미 국무부는 국제공조를 통한 국제교역과 상거래 지원, 국제안보 강화, 표현의 자유와 혁신을 촉진시키는 개방적이고 상호 운용적인 안전하고 신뢰할 수 있는 정보통신기반시설 촉진을 위한 미국 정부의 노력을 주도하고 있다.[163] 미국의 사이버 국제협력은 국무부의 소관사항이며 국무부는 국제사이버전략 작성을 담당한다. 이를 위해 미 국무부는 2011년 사이버이슈 조정관실(Office of the Coordinator for Cyber Issues: S/CCI)을 설치하여 사이버 국제협력을 효율적으

162) 이동범·곽진, "미국 정부의 사이버 공격에 대한 보안 전략," pp. 19~20.

163) U.S. Department of State, "Office of the Coordinator for Cyber Issues," 〈https://www.state.gov/bureaus-offices/bureaus-and-offices-reporting-directly-to-the-secretary/office-of-the-coordinator-for-cyber-issues/〉 (accessed september 20, 2019).

로 추진하고 있으며, 미국의 외교정책, 국가안보, 인권 및 경제에 영향을 미치는 모든 국제 사이버 정책 문제에 대한 외교적 대응을 전담하고 있다.

특히 국무부는 ① 사이버공간에서 미국이 만든 책임 있는 국가 행동 프레임 워크에 대한 수용 및 준수 촉진, ② 미국의 국익에 도움이 되고 미국의 가치를 증진시키는 개방적이고 상호 운용 가능하며 신뢰할 수 있고 안전한 사이버공간 구축 등 두 가지 정책목표 달성을 위해 마련된 2018년 국가사이버전략을 이행하는데 있어 선도적인 위치에 서 있다.[164]

미 국무부가 작성한 최초의 국제 사이버 전략은 2011년 5월에 발표된 「사이버공간을 위한 국제 전략(International Strategy for Cyberspace)」이다.[165] 이 전략은 2009년의 사이버공간 정책 검토에 규정된 단기행동계획 중 7번째 항목 "국제 사이버안보 레짐에서의 미국 정부의 대응 강화와 각종 이니셔티브를 실시하기 위한 국제적 파트너십 강화"에 기초하여 발표되었다. 2009년 보고서가 사이버안보 정책에서의 단기 및 중기 행동계획이 제시되었다면, 이 전략에서는 폭넓은 사이버문제에 대해 미국은 국제적 파트너와 협조하여 대응하기 위한 국제적 연대 방침을 제시한다는 국제 전략에 중점을 두고 있다.

이 전략의 핵심은 ① 자유로운 정보의 흐름을 존중한다는 원칙에 기초하여 혁신을 촉진함으로써 경제 활성화를 모색, ② 개방된 사이버공간에 대한 가치를 인정하는 국가와 상호운용성 있는 환경 구축

164) U.S. Department of State, "Key Topics- Office of the Coordinator for Cyber Issues," 〈https://www.state.gov/key-topics-office-of-the-coordinator-for-cyber-issues/〉 (accessed September 20, 2019).

165) White House, "International Strategy for Cyberspace," 〈https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf〉 (accessed September 20, 2019).

에 대한 합의 도출, ③ 사이버공간에서의 적대적인 행위에 대해서는 필요에 따라 사이버 공격에 대해서도 물리적인 대항조치가 가능 등으로 정리해 볼 수 있다.[166]

미 국무부의 기본 방침에 대한 검토는 이상으로 마치고, 이하에서는 국무부가 추진하는 구체적인 사이버 국제협력에 대해서 살펴보고자 한다. 2010년 이후 채택된 유엔 정보안보 정부전문가그룹(Group of Government Experts: GGE)의 최종보고서[167]에도 나타나 있듯이, 사이버 국제협력의 영역은 크게 양자 및 다자간 신뢰구축조치(Confidence Building Measures: CBMs) 실시, 개도국에 대한 역량강화(Capacity Building) 지원활동, 국제규범 확립을 위한 활동 등으로 나누어 볼 수 있다. 사이버공간에서의 신뢰구축 추진이란 국가 간의 사이버분쟁 예방을 위해 평시에 양자 또는 다자간 협력을 통해 투명성과 안정성을 확보하기 위한 노력을 추진해 나감을 의미한다. 다음으로 역량강화란 개도국의 사이버위협에 대한 취약성은 전 세계적인 위협이기 때문에 개도국의 역량구축 지원과 인재육성 등의 지원을 실시해 나간다는 것을 의미한다. 마지막으로 국제규범 확립이란 사이버안보 관련 국제규범이 확립되어 있지 않기 때문에 사이버공간에서의 국가 간의 관계를 규율하는 규범을 마련하기 위한 규범외교를 전개해나감을 의미한다. 이하에서는 이들 세 가지 영역을 중심으로 미국의 사이버 국제협력을 검토하도록 한다.

---

166) 持永大 · 村野正泰 · 土屋大洋,『サイバー空間を支配する者：21世紀の国家、組織、個人の戦略』(東京：日本経済新聞出版社, 2018), pp. 187~188.

167) The United Nations, Report of the Secreatry-General about the Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security: UN General Assembly A/65/201, 〈https://documents-dds-ny.un.org/doc/UNDOC/GEN/N10/469/57/PDF/N1046957.pdf?OpenElement〉(Accessed June 10, 2019).

(2) 양자 및 다자외교를 통한 신뢰구축 추진

미국은 2019년 현재 한국을 비롯하여 일본, 중국, 우크라이나, 에스토니아, 프랑스, 독일, 아르헨티나, 브라질, 칠레, 케냐 등 11개국과 양자 사이버 협의를 실시하는 한편으로 유럽연합(EU) 동남아국가연합(ASEAN) 등 지역기구와의 협력대화 추진은 물론 북대서양조약기구(NATO), 유럽안보협력기구(OSCE), 아세안지역협력포럼(ARF) 등 지역안보기구나 안보협의체와도 긴밀한 협력을 통해 신뢰구축을 추진하고 있다.[168]

〈표 Ⅳ-2〉 미국의 양자 및 다자간 사이버협의 개최실적(2017~2019)

연도	국가 및 회의명
2017	• 사이버 정책에 관한 미-아르헨티나 파트너십(4/27) • 사이버 및 디지털 경제 정책에 관한 미-케냐 파트너십 강화(6/27) • 제5차 미·일 사이버 대화(7/24) • 미-우크라이나 사이버안보대화(10/3) • 미·중 법집행 및 사이버안보 대화(10/3) • 제4차 미·EU 사이버 대화(11/15)
2018	• 미·불 사이버정책 관계 강화(2/9) • 미-브라질 사이버 및 인터넷 정책 양자협력(5/14) • 미·일 양자 사이버협의(6/21) • 제6차 미·일 사이버 대화(7/26) • 한·미·일 사이버안보 전문가 회의(7/27) • 제9차 인터넷 경제에 대한 미·일 정책협력대화(7/27) • 미-칠레 사이버 협의(9/18) • 제5차 미·EU 사이버 대화(10/16)
2019	• 제1차 미·독 사이버 대화(5/20) • 제6차 미·EU 사이버 대화(5/24) • 제3차 미-에스토니아 사이버 대화(6/7) • 제1차 미·아세안 사이버 정책 대화(10/3)

출처: 미 국무부 홈페이지를 참고하여 작성 * 괄호안 숫자는 개최일을 나타냄.

168) U.S. Department of States Home Page, "Remarks and Releases-Office of the Coordinator for Cyber Issues," 〈https://www.state.gov/remarks-and-releases-office-of-the-coordinator-for-cyber-issues/〉 (accessed September 20, 2019).

이 중 양자 간 사이버 협의 및 대화에서는 한국과 일본과의 대화 횟수가 눈에 띈다. 특히 일본과의 양자 간 사이버 협력은 사이버 대화뿐만 아니라 인터넷 경제에 대한 정책협력대화를 9차례에 걸쳐 실시하는 등 경제 분야에서의 협력을 강화하는 점도 눈여겨 볼 대목이다. 지역기구와의 사이버 협력에서는 EU와의 협력을 중시하고 있음을 알 수 있다. 더불어 2019년 10월 3일에는 싱가포르에서 아세안과 처음으로 미·아세안 사이버정책대화를 실시하여 미국과 아세안이 평화롭고 안전하며 회복 탄력적인 사이버공간에 대한 비전을 공유하고 파트너십을 형성하고 있음을 보여 주었다.[169]

(3) 국제규범 형성에 대한 대응

사이버공간에 대한 국제규범 확립 시도는 이제 막 시작되었다고 할 수 있는데, 미국은 국제사회에서의 사이버공간 관련 국제규범을 마련하고자 하는 움직임을 주도하고자 하며 이를 통해 미국이 추구하는 규범과 원칙 및 가치를 반영하고자 한다.[170]

사이버공간을 규율하는 국제적 규범 마련을 위한 움직임은 유엔 총회 제1위원회(군축 및 국제안보 담당)의 정보안보 정부전문가그룹(Group of Governmental Experts: GGE)회의를 비롯하여 북대서양조약기구(NATO)의 사이버방위협력센터(CCDCOE), 세계사이버스페이스총회, 유럽안보협력기구(OSCE), 상하이협력기구(SCO) 등에서 논의가 진행 중이다. 이들 중에서도 UN을 무대로 전개되는 정보안보 GGE의 활동은 국제사회가 당면한 사이버 국제협력의 방향

169) U.S. Department of States Media Note, "Co-Chairs' Statement on the Inaugural ASEAN-U.S. Cyber Policy Dialogue," (October 3, 2019), 〈https://www.state.gov/co-chairs-statement-on-the-inaugural-asean-u-s-cyber-policy-dialogue/〉 (accessed October 4, 2019).

170) 신성호, "미국의 사이버안보 전략과 외교," pp. 167~168.

성과 과제를 제시했다는 점에서 주목할만 하다. UN 정보안보 GGE는 사이버 위협의 심각성에 대처하기 위해 2004년 러시아의 제안으로 만들어진 것으로 지금까지 다섯 차례에 걸친 회의가 개최되었다. 당초 미국은 사이버공간 이용에 관한 국제규범 마련에 대해 소극적인 입장이었지만, 오바마 행정부 시기이던 2010년 이후부터 적극적으로 외교 교섭에 참여하게 된다. 그동안 회의는 미국을 중심으로 '정보의 자유로운 유통'과 '사이버공간에 대한 기존 국제법 적용'을 강조하는 서방 진영 국가들과 중국과 러시아 등 '국가주권에 기초한 국내통제 및 관리'를 우선시하는 비서방 국가들로 나뉘어 대립하는 형국을 보였다. 그럼에도 불구하고 미국은 UN 정보안보 GGE에서 2015년의 4차 회의 때까지 ① 국가는 정보통신기술(ICT) 이용에 있어 국가주권, 분쟁의 평화적 해결, 내정간섭금지와 같은 국제법의 기본원칙을 지켜야 한다는 점, ② 국제법에 규정되어 있는 국가가 준수해야 할 의무는 사이버공간에도 적용된다는 점, ③ 국가는 사이버공간에서 국제적 위법행위에 관여해서는 안 된다는 점, ④ 사이버공간에 대한 국제법 적용 및 규범 논의에서 유엔이 주도적 역할을 담당한다는 점 등 4가지 사항에 대해서 참여국 간 합의를 도출하는데 찬성하였다.[171] 이때까지 미국은 자유로운 정보의 흐름과 표현의 자유에 대한 억압을 우려하여 중러 양국이 주장하는 사이버공간에 대한 국가주권과 불간섭 원칙 인정에 대해 반대 입장을 취해 왔으나, 제4차 유엔 GGE에서는 이를 인정함으로써 새로운 대응책을 마련해야 할 것으로 간주되었다.

그러나 2016~2017년 전개된 제5차 회의에서는 국가들 간 첨예한 입장 차이로 인해 보고서 채택에 실패함으로써 사이버규범 모색을 위한 국가 간 사이버 국제협력은 한계에 봉착하였다. 다행히 2018년

171) 谷脇康彦, 『サイバーセキュリティ』, pp. 124~126.

개최된 제73차 유엔 총회에서는 제6차 유엔 정보안보 GGE 구성과 더불어 러시아가 제안한 모든 유엔 회원국에게 개방되는 '개방형 워킹그룹(Open-ended Working Group: OEWG)' 제안 결의안이 채택됨으로써 사이버안보 국제규범을 둘러싼 논의는 새로운 국면을 맞이하고 있다.

(4) 역량강화 지원

앞서 살펴본 사이버공간의 규범마련과 신뢰구축 활동에서 미국은 적극적인 모습을 보였지만, 개도국에 대한 역량강화 지원에는 다소 소극적인 모습을 보이고 있다.

물론 미국도 개도국에 대한 역량강화 사업을 실시하고 있다. 미국은 개도국에 대한 역량강화 지원을 위한 지역으로 아프리카를 중시한다. 2015년 7월 미아프리카군 사령부(AFRICOM)가 실시한 아프리카 출신 9개국 무관 연수, 2015년 7월 미국무부가 서아프리카국가를 대상으로 실시한 '사이버범죄대책 워크숍' 등이 대표적인 사례이다. 이 외에도 일본 및 호주 등과 동남아시아국가연합(ASEAN) 국가들의 사이버범죄 대책에 대해 공동으로 UNODC 등에 자금을 출자하고 있으며, 미주기구(OAS)의 회원국으로 국제적인 사이버안보 역량강화에도 관여하고 있다.[172] 이렇듯 미국은 역량강화 이념 자체에는 찬성하고 있으며, 관련 사업을 실시하고 있다. 그럼에도 불구하고 미국이 사이버 국제협력에서 가장 중시하는 것은 사이버공간에서의 국가의 행위를 규율하는 국제적 규범 확립이며, 역량 강화의 중요도는 국제적 규범확립이나 신뢰구축 조치에는 미치지 못한다. 다시 말해 미국은 개도국에 대한 역량강화를 어디까지나 사이버공

172) 村上啓, 「サイバー外交政策に関する研究-キャパシティビルディングを中心に-」 情報セキュリティ 大学院大学博士論文, (2018), pp. 91~93.

간의 국제규범 형성을 위한 전제로서 부수적인 시책에 지나지 않는다는 입장을 취하고 있다.

라. 한반도에 대한 함의

한국은 정보통신기술(ICT)의 발달로 세계 최초로 5G기술을 상용화 하는 등 자타가 공인하는 ICT 선진국이지만, 사이버 보안 기술은 미국이나 일본, 서유럽 국가 등 다른 사이버 선진국에 비해 뒤쳐져 있다는 평가를 받는 것이 현실이다. 이에 더해 북한으로부터 지속적인 사이버 위협에 처해 있는 한국에게 있어 사이버안보는 국가안보에 있어 필수 영역으로 자리매김하였다.

이러한 상황에서 문재인 정부는 2018년 12월 국가안보와 관련한 한국정부의 최상위 전략문서라고 할 수 있는 「국가안보전략」을 발표하였다. 그리고 이듬해인 2019년 4월에는 사이버안보 관련 기본방침을 제시한 「국가사이버안보전략」을 발표하였고, 같은 해 9월에는 중앙 관계부처 합동으로 보다 구체적인 내용들을 담은 「국가 사이버안보 기본계획」을 발표하였다.[173] 이처럼 정부 주도의 사이버안보 전략이 구체화되어 가는 과정에서 우리의 동맹국인 미국의 사이버안보가 한국에 주는 함의는 아래와 같이 두 가지 측면에서 검토할 수 있다.

먼저 2019년에 들어와 통상무역을 둘러싼 미국과 중국과의 갈등이 첨단 기술 패권 경쟁으로 확대되면서 한국은 미중 사이에서 선택을 강요받는 상황이 연출되고 있다. 문제의 발단은 미국이 국가안보

173) 관계부처 합동, "국가사이버안보 기본계획," 〈https://msit.go.kr/cms/www/m_con/news/report/__icsFiles/afieldfile/2019/09/03/(%EC%B0%B8%EA%B3%A0)%20%EA%B5%AD%EA%B0%80%20EC%82%AC%EC%9D%B4%EB%B2%84%EC%95%88%EB%B3%B4%20%EA%B8%B0%EB%B3%B8%EA%B3%84%ED%9A%8D.pdf〉 (검색일: 2019.9.9.).

상의 위협을 들어 중국의 통신장비 기업인 화웨이(Huawei)에 대한 제재에 착수한 것에서 비롯되었다. 영국과 호주, 뉴질랜드, 일본 등 동맹국들이 화웨이에 대한 제재에 동참을 선언하고 나선 상황에서 한국 정부는 전략적 모호성을 내세우며 미국과 중국 사이에서 고민에 빠진 것이다. 미국 국무부 대변인은 6월 13일 "한국이 5G 네트워크에 화웨이 통신장비를 쓸 경우 민감한 정보를 노출하지 않을 것"이라고 하여 동맹국인 한국과의 군사안보상의 정보공유를 제한할 수 있다는 뜻을 내비쳤다.[174] 이 문제와 관련해서는 "기본원칙은 동맹의 편에 서서 신중하게 접근해야"하되, "정치·외교적 영역에서는 동맹의 편에서 분명한 메시지를 전달하고, 실질적 선택에 있어서는 신중히 접근하는 게 필요하다"는 신범철 아산정책연구원 통일정책센터장의 지적에 귀 기울일 필요가 있다.[175]

둘째, 미국은 사이버 군사협력을 추진함에 있어 오프라인에서의 동맹의 틀을 온라인에서도 그대로 적용시키려는 정책을 추진 중에 있다. 미국은 2011년 「사이버공간의 국제 전략(International Strategy for Cyberspace)」이란 전략문서를 통해 외부로부터의 심각한 사이버 공격에 대해서는 집단적 자위권 행사도 마다하지 않겠다는 점을 선포한 이후 동맹국들과의 논의를 통해 동맹의 영역을 사이버공간으로의 확대하여 적용하려는 정책을 추진하고 있다. 미국은 북대서양조약기구(NATO)와 태평양안보조약(ANZUS) 가맹국인 오스트레일리아와의 협의를 통해 가맹국에 대한 사이버 공격이 집단적 자위권 행사의 대상이 된다는 점을 확인하였고, 미일 동맹 또한 2019년

174) 정효식, "미 국무부, '한국, 화웨이 쓰면 민감정보 공유 안한다'," 『중앙일보』, 2019.6.15., 〈https://news.joins.com/article/23497331〉 (검색일: 2019.9.9.).

175) 송병기, "홍일표 '화웨이 사태, 정부 손 놓고 있다' 화웨이 장비 사용 신중해야," 『쿠키뉴스』, 2019.6.18., 〈http://www.kukinews.com/news/article.html?no=673236〉 (검색일: 2019.9.10.).

4월 개최된 미일안보협의위원회에서 미일 안보조약이 규정하는 미국의 대일 방위의무가 사이버안보 영역에도 확대 적용된다는 데 합의함으로써 미래 첨단전에도 미일동맹이 굳건하다는 점을 확실히 하였다.

그러나 한국은 미중갈등을 의식하여 한미동맹을 미래 첨단전쟁에도 확대 적용시킬 것인지에 대한 논의를 발전시키지 못하고 있는 실정이다. 물론 한국 또한 지금까지 사이버 위협 정보 공유, 사이버범죄 수사공조, 구사적 사이버협력 심화 등 미국과의 동맹차원에서의 협력을 강화해왔다. 반면 한미동맹을 심화시켜 첨단 미래전쟁으로 확대 적용하는 문제에 대해서는 미중 패권 대립을 의식하여 적극론와 신중론으로 국론이 양분되는 상황이다. 한미동맹을 우선시하는 입장에서는 "사이버 군사 영역에서의 협력은 한미동맹의 큰 틀 속에서 하부구조로 들어가는 것이 비용측면에서 효과적"이며 외교적 압력으로부터도 자유로울 수 있다는 주장을 하는 반면,[176] 미중 간의 균형을 강조하는 입장에서는 "오프라인 한미동맹의 틀을 온라인의 한미관계에 그대로 적용하는 일에는 좀 더 신중히 접근할 필요가 있다"는 의견도 존재한다.[177] 이처럼 한미동맹을 사이버안보 등 첨단 미래 전쟁에 확대 적용하는 문제는 미중대립이 심화되는 동아시아 국제정세를 고려한다면 성급하게 결론을 내리기 보다는 보다 신중한 접근이 요구되는 전략과제라 하겠다.

176) 김상배 편, 『사이버안보의 국가전략』 (서울: 사회평론, 2017), p. 364.

177) 김상배, "국가사이버안보전략 화급하다," 『디지털 타임스』, 2018.10.15., 〈http://www.dt.co.kr/contents.html?article_no=2018101602102269640001〉 (검색일: 2019.9.18.).

2. 일본[178]

가. 사이버공간에 대한 인식 및 환경

일본의 경우 국가주도의 사이버 공격으로 인해 한국이 경험한 것과 같은 사이버 대란에 휩싸인 적은 없다. 그렇다고 해서 사이버공격의 무풍지대는 아니며 지금까지 크고 작은 사이버 위협에 노출되어 왔다. 2010년 이후의 일본 동향은 중앙 행정부처에 대한 사이버 공격은 물론 첨단기술 보유 민간 기업을 상대로 한 사이버 공격이 급증하는 추세이다. 2011년에는 일본 최대의 방위산업체인 미쓰비시 중공업의 기밀정보가 유출된 사건이 발생하였으며 2015년에는 일본연금기구가 보유하는 개인정보 125만여 건이 유출되는 사건이 발생하였다. 일본연금기구 관련 사건은 인명이나 물리적인 피해를 동반하지는 않았지만, 125만 건에 달하는 연급가입자의 개인정보가 사이버 공격에 의해 유출되었다는 점에서 일본 사회에 미친 충격은 컸다.[179] 2016년에는 방위정보통신기반(DII)이라고 하는 방위성과 자위대의 공동 운용 통신네트워크에 대한 부정침입 사건이 발생하여 내부정보 유출가능성이 언론을 통해 보도되기도 하였다.[180] 2018년에는 사이버공격에 의한 가상통화 절도사건이 연이어 발생하

178) 일본의 경우 통상적으로 '사이버시큐리티(サイバーセキュリティ)'라는 용어가 '사이버안보' 및 '사이버보안'을 의미하는 용어로 사용되고 있지만, 여기서는 편의상 '사이버시큐리티'를 '사이버안보'로 통일하였음을 밝혀 둔다.

179) 일본연금기구의 정보유출사건을 계기로 일본 정부는 2015년 9월 각의 결정이 이루어진 「사이버안보 전략」에서 사이버공격 피해에 대한 감시대상을 정부기관에서 독립행정법인 및 일부 특수법인으로까지 확대한다는 방침을 천명하였고, 이러한 방침은 2016년 기본법 개정으로 이어지게 된다. "マイナンバー制度対策も強化 新サイバー戦略を決定 政府、攻撃監視拡大へ,"『産経新聞』, 2015.9.4.

180) "陸自システムにサイバー攻撃, 情報流出か国家関与も 被害の全容不明," 『産経ニュース』, 2016.11.28., 〈https://www.sankei.com/affairs/news/161128/afr1611280003-n1.html〉 (검색일: 2019.6.6.).

여 수백억 엔의 재산피해가 발생한 것과 더불어 랜섬웨어 공격으로 교통기관의 일반업무 장애와 병원 등 의료기관에서 의료시스템 장애가 발생하기도 하였다.[181] 이런 한편으로 일본은 2020년에는 국제적 스포츠 이벤트인 도쿄 올림픽 및 장애인 패럴림픽 개최를 앞두고 있어, 올림픽의 성공적 개최와 행사의 원활한 운영을 위해 사이버공격에 대한 대책강화를 서두르고 있다.

2000년 이후 일본정부는 점증하는 사이버 위협에 대응하기 위해 각종 대책을 마련하여 왔는데, 2009년을 기점으로 그 대응양식에 있어 변화를 보이고 있다. 일본의 초기 대응은 주로 사이버 위협을 사이버공간에서 발생하는 범죄로 인식하여 정보보안이나 네트워크 보안을 강화하는 등 기술적인 차원의 대응이었다. 그러나 2009년 동맹국인 미국과 인접국인 한국에서 대규모 사이버 공격이 발생한 것을 계기로 사이버 공격을 기술적 차원을 넘어 국가안보에도 심각한 영향을 줄 수 있는 문제로 인식하게 되었다. 이러한 인식변화는 일본의 사이버안보 정책에도 반영되어, 이후에 책정되는 국가전략 문서에서 사이버안보는 국가안보 차원의 문제로 그 중요도가 한층 격상되게 된다.

한편, 2019년도 방위대강 책정을 한 달여 앞둔 2018년 11월 19일, 오노데라 이츠노리(小野寺五典) 전 방위상이 민간 NPO법인이 주최하는 안보 심포지움에서 '진정 필요한 방위력을 어떻게 구축할 것인가'라는 주제하에 기조연설을 하였다.[182] 오노데라 전 방위상은 2013년 방위대강 책정당시 방위대신으로 참여하였고, 2018년 시점

181) サイバーセキュリティ戦略本部, 『サイバーセキュリティ2019 (2018年度報告 · 2019年度計画』 2019.5.23., p. 15.

182) NPO法人 ネットジャーナリスト協会主催第19回安全保障シンポジウム, "真に必要な防衛力をどう構築するか," 2018.11.19., 〈http://anpo.netj.or.jp/content/symposium/2018_11/index.html〉 (검색일: 2019.9.9.).

에서 여당 방위대강 워킹팀 좌장을 맡는 등 일본 정부여당의 방위정책 형성과정에 깊이 관여하고 있었다는 점에서 그의 발언은 진지하고 무게감 있는 것이었다. 그는 먼저 '우크라이나에 대한 군사행동에서 보여진 러시아의 군사력을 어떻게 평가할 것인가?'는 주제로 개최된 2016년 4월 5일 미국 상원 군사위원회에 출석한 허버트 맥매스터(Herbert McMaster) 당시 육군 중장(이후 트럼프 정권하에서 국가안보보좌관 역임)의 발언에 주목한 뒤 일본이 처한 사이버 위협에 대해 언급하였는데, 요약하면 다음과 같다.

- 지금의 전쟁수행 양상은 예전의 우리가 알고 있는 방식과는 완전히 달라져 있다. 5년 전 방위계획 책정 당시 각국이 이러한 능력을 개발 중이라는 것에 대해서는 인식하고 있었다.
- 그러나 구체적으로 우크라이나에서 하이브리드전이 활용되고 크리미아가 지금의 상황에 처해져 있다. 일본의 주변국들도 당연히 이러한 능력을 보유하고 있다고 봐야 한다. 앞으로의 전쟁은 이러한 전투수행 방식으로 치러질 것이다.
- 이렇게 봤을 때 일본을 어떻게 방위해 나갈 것인가에 대해 근본적인 수정이 필요하다.
- 클로스 도메인 작전 능력을 향상해야 한다.
- 전수방위 국가인 일본의 경우 사이버공간의 공격, 반격, 자위권 발동 등에 대한 법 정비를 해야 한다.
- 그러나 세계에서 무엇이 공격, 전수방위, 자위권, 반격인지에 대한 정의가 불확정적이다.

요컨대, 오노데라 전 방위상은 2014년 러시아에 의한 우크라이나 공격당시 전자파 공격과 사이버 공격을 융합한 하이브리드 공격을

감행하였다는 점에서 현대 첨단전은 이전의 전쟁수행 방식과는 완전히 다른 것이며, 중국도 당연히 이러한 능력을 갖추고 있다고 봐야한다고 하여 사이버 위협 상대국인 중국에 대한 경각심을 드러내었다고 하겠다. 2018년 12월에는 중국의 관여가 의심되는 APT10이란 사이버 범죄 그룹에 대해 미국과 영국이 성명문을 발표하자, 일본 또한 이들 국가를 지지하는 외무보도관 담화를 발표하여 APT10이 일본의 민간기업, 학술기관 등을 대상으로 한 사이버 공격을 장기간에 걸쳐 감행해 왔다는 사실을 공개하였다.[183]

더불어 2019년 방위성이 발표한 방위백서를 보게 되면 사이버공간의 위협 동향에 대해 서술한 부분에서 미국의 정부기관이 발표한 보고서 등을 인용하여 중국, 러시아, 북한의 사이버 위협과 사이버 공격 사례를 소개하고 있다.[184] 사이버공간상에서의 위협은 그 국가가 처한 지정학적 위협과 밀접한 연관성이 있다는 점을 고려한다면 일본이 상정하는 사이버 위협 상대국은 중국, 러시아, 북한이라고 봐도 무난할 것이다.

그렇다면 일본은 어느 정도의 사이버역량을 보유하고 있을까? 여기에서는 호주전략정책연구원(Australian Strategic Policy Institute: ASPI) 산하의 국제사이버정책센터(International Cyber Policy Centre: ICPC)가 2014년 이후 매년 발표한 「아시아 태평양 지역의 사이버 역량(Cyber maturity in the Asia-Pacific Region)」이란 보고서를 통해 일본의 사이버안보 역량이 어느 정도 수준인지를 살펴보도록 한다.[185] 이 보고서는 '사이버 성숙도(cyber maturity)'란

183) 外務報道官談話, "中国を拠点とするAPT10といわれるグループによるサイバー攻撃について," 2018.12.21., 〈https://www.mofa.go.jp/mofaj/press/danwa/page4_004594.html〉 (검색일: 2019.10.10.).

184) 防衛省, 『防衛白書』 (東京 : 日経印刷, 2019), pp. 168~170.

185) Fergus Hanson, Tom Uren, Fergus Ryan, Michael Chi, Jack Viola and Eliza Chapman, "Cyber maturity in the Asia-Pacific Region 2017," (Australian Strategic

지표를 사용하여 아태지역 국가들의 사이버 역량을 평가한다.[186] 동 보고서에 따르면 사이버 성숙도는 거버넌스(governance), 금융 사이버범죄 대응(financial cybercrime enforcement), 군사 적용(military application), 디지털 경제 및 사업 (digital economy and business), 사회적 참여(social engagement)와 같은 항목들을 수치화하는 방식을 통해 도출된다.

〈표 Ⅳ-3〉을 통해 알 수 있듯이, 네 번째로 발표된 2017년 보고서에 따르면 일본은 호주와 함께 88점을 획득하여 조사대상 25개국 중 미국(91점)에 이은 공동 2위를 기록하였다.[187] 일본에 대한 전반적인 평가를 보게 되면 중장기 기본계획인 「사이버안보전략」 수립과 체계적인 이행, 그리고 사이버이슈에 대한 국민인식 증대 등이 호평을 받았다. 이와 더불어 일본이 사이버안보 관련 양자협의와 다자협의에 대한 적극적 참여와 개도국에 대한 역량강화지원을 지속적으로 추진하고 있다는 점 및 JPCERT/CC의 적극적이고도 인상적인 활동 또한 긍정적인 평가요인으로 작용하였다.[188]

Policy Institute, December 2017) 〈https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2017〉 (Accessed September 13, 2018).

186) 배선하, 박상돈, 김소정은 이 보고서에 대해 비판적인 시각을 보이고 있는데 "ASPI는 호주 국방부의 지원으로 설립된 국방안보 분야 정책연구소로 사이버 보안 분야에 대한 평가항목 선정 시 군의 역할에 대한 비중을 높게 책정하여, 군을 정부의 사이버 보안 조직의 일부가 아닌 독립적인 주체의 관점에서 평가"하고 있다는 점, 그리고 "연구개발 및 기술·표준·인증 관련한 평가항목이 없다"는 점을 지적한다. 배선하·박상돈·김소정, "국가 사이버보안 역량 평가를 위한 평가항목 연구," 『정보보호학회논문지』, 제25권 제5호 (2015), pp. 1297~1298.

187) 참고로 국제전기통신연합(ITU) 또한 법/제도, 기술, 조직, 역량 구축, 국제협력 등 5가지 항목을 기준으로 평가한 「글로벌사이버지수(Global Cybersecurity Index: GCI)」라는 보고서를 3년 단위로 발표하고 있는데, 2017년에 발표한 「GCI 보고서」에서 일본은 전 세계 193개국 중 11위를 차지하였고, 아시아태평양 지역에서는 싱가포르, 말레이시아, 호주에 이은 4위를 기록하였다. ITU, "Global Cybersecurity Index(GCI) 2017," 〈https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf〉, p. 59.

188) "Cyber maturity in the Asia-Pacific Region 2017," p. 43.

구체적으로 들어가 사이버성숙도 관련 11개 평가항목들을 세부적으로 들여다보면, 일본은 국제적 관여, 침해사고 대응 및 인터넷활용도의 측면에서 최고점인 10점을 받은 반면, 군사적용 항목에서는 7점을 받아 11개 항목 중 가장 낮은 평가를 받았음을 알 수 있다.[189]

국제적 관여와 관련해서는 제2차 일본-ASEAN 사이버범죄대화, 제2차 일본-인도 사이버협의, 제5차 미일사이버대화 등 다수의 양자대화를 개최하고, CSIRT(Computer Security Incident Response Team)의 국제적 연합체인 FIRST(Forum of Incident Response and Security Teams) 및 아시아태평양 컴퓨터 긴급대응팀(Asia Pacific Computer Emergency Resopnse Team: APCERT)에 적극적으로 참여하고 있는 점, 캄보디아, 인도네시아, 라오스, 미얀마, 필리핀, 베트남 등 ASEAN 6개국에 대해 사이버 방어훈련을 제공하고 개도국 역량강화를 위한 기본방침을 수립한 점, 그리고 이러한 모든 활동들이 외무성에 설치된 「사이버안전보장정책실」에 의해 효율적으로 추진되었다는 점이 긍정적인 평가의 요인으로 작용하였다.

다음으로 침해사고 대응과 관련해서는 일본이 평가대상국 중 가장 높은 평가를 받았는데, 이는 APCERT와 같은 국제 CSIRT 커뮤니티를 통한 연대활동 그리고 기술면에서의 정보발신, 역량구축지원 등과 같은 영역에서의 JPCERT/CC의 지속적인 노력이 반영된 결과라고 하겠다.[190] 인터넷 활용도의 경우 일본의 정보통신 시장이 세계에서 가장 발달한 곳 중 하나라는 점과 전체인구 중 92%가 인터넷을 사용한다는 점이 긍정적 평가로 이어졌다.

---

189) 이러한 경향은 ICPC가 보고서를 발간한 2014년부터 지속되는 양상을 보인다는 점에서 타국과 비교되는 일본 사이버안보 체제의 특성으로 봐도 무방하다는 것이 필자의 견해이다.

190) 아태지역 CSIRT의 동향 및 JPCERT/CC의 활동과 관련해서는 情報処理推進機構, 『情報セキュリティ白書』(東京: 情報処理推進機構, 2018), pp. 110~112 참조.

한편 이 보고서가 군사적용 항목에 대해서 낮은 평가를 받은 이유로는 2014년 사이버 방위대가 창설되긴 했지만, 그 활동 반경이 방위성 및 자위대의 컴퓨터시스템과 네트워크로 한정되며, 다른 정부기관 및 주요 인프라는 방어 대상에서 빠져있다는 점을 지적하고 있다. 실제로 사이버안보에 대한 일본의 군사적 대응체제가 충분한가에 대해서는 국내외를 막론하고 부정적인 견해가 지배적이다.[191] 예를 들면 정확한 규모는 알 수 없지만, 2018년을 기준으로 미국의 사이버 부대는 6000명, 세계최대규모의 사이버 부대를 보유한 중국은 10만 명, 북한의 사이버 부대는 7000명인 반면, 일본의 사이버방위대는 150명의 규모이기 때문에, 사이버공격에 대한 일본의 대응체제정비가 뒤쳐져 있다는 지적도 있다.[192] 그러나 사이버안보에 대한 일본의 군사적 대응은 평화헌법하에 전수방위를 국시로 삼아 온 전후 일본의 방위정책과 밀접히 연관된 문제이며, 사이버 공격과 자위권 발동에 대한 법적 기반 정비와도 관련된 문제이기 때문에 동북아 전반의 안보문제로까지 확대될 수 있는 민감한 이슈라고 하겠다.

191) 대표적으로는 미국의 사이버안보 전문가인 제임스 루이스(James Andrew Lewis)의 2015년 보고서를 참조. "U.S.-Japan Cooperation in Cybersecurity," A Report of the CSIS Strategic Technologies Program (November 2015), 〈https://www.csis.org/analysis/us-japan-cooperation-cybersecurity〉 (Accessed September 13, 2018).

192) "変わる脅威、自衛隊の変革迫る 宇宙・サイバーを挽回 新たな防衛大綱決定," 『日本経済新聞』 (2018.12.18.), p. 3.

〈표 Ⅳ-3〉 25개국 아태지역 국가들의 사이버 성숙도(2017)

순위	국가명	조직구조	입법규제	국제적 관여	침해사고대응	금융사이버범죄대응	군사적용	민관소통	디지털경제	대중인식	인터넷활용도	총점
1	미국	10	8	9	8	10	10	9	9	10	8	91
2	일본	9	8	10	10	8	7	8	9	9	10	88
2	호주	8	9	9	9	9	8	9	9	9	9	88
4	싱가포르	9	8	8	7	8	9	10	10	10	9	88
5	한국	8	9	8	8	8	9	9	9	9	10	87
6	뉴질랜드	8	8	8	8	7	6	9	10	9	9	80
7	말레이시아	7	8	8	8	6	7	7	8	6	8	73
8	중국	9	8	9	6	6	8	5	8	5	6	70
9	타이완	8	6	3	3	5	5	6	6	6	9	57
10	인도	7	5	8	5	4	3	6	7	8	3	56
11	브루나이	6	6	4	6	5	4	6	6	3	8	54
12	인도네시아	6	6	5	5	6	6	5	7	5	3	54
13	태국	7	6	5	5	5	5	4	6	6	5	54
14	베트남	6	7	5	6	5	3	5	6	4	6	53
15	필리핀	6	6	6	3	6	3	4	5	6	5	50
16	캄보디아	4	4	4	3	4	1	3	6	4	3	36
17	바누아투	5	4	5	1	2	0	7	4	4	3	35
18	방글라데시	4	3	3	3	4	1	4	4	5	2	33
19	라오스	4	4	3	4	1	1	4	3	3	3	30
20	파키스탄	3	4	2	1	4	4	5	3	2	2	30
21	미얀마	3	4	4	3	2	5	1	3	2	3	30
22	피지	2	4	4	0	4	1	2	3	4	5	29
23	파푸아뉴기니	4	4	4	1	1	1	2	1	5	1	24
24	북한	3	1	3	0	0	8	0	1	1	1	18
25	솔로몬제도	3	0	3	0	1	0	2	1	2	2	14

출처: "Cyber maturity in the Asia-Pacific Region 2017," pp. 100~101을 참조하여 재구성.

나. 일본의 사이버안보 전략과 추진체계[193]

(1) 일본의 사이버안보 전략

사이버안보에 관한 3년 단위의 중장기적 기본전략은 2005년 발족한 정책회의 시기부터 마련되었다. 2006년에 마련한 「제1차 정보보안 기본계획」, 2009년에 마련한 「제2차 정보보안 기본계획」에서 알 수 있듯이 처음에는 「정보보안 기본계획」이란 명칭이 사용되었다. 그러다가 민주당이 집권하던 2010년에는 「국민을 지키는 정보보안 전략」으로 바뀐 뒤 2012년 12월 재집권에 성공한 아베 정권 이후로는 「사이버안보전략」이란 명칭으로 정착되었다. 여기에서는 사이버안보 기본법에 제정된 이후에 마련된 「사이버안보전략 2015」(이하 2015년 전략)과 「사이버안보전략2018」(이하 2018년 전략)을 중심으로 그 내용과 특징을 살펴보겠다.

먼저 2015년 전략은 사이버안보 기본법이 시행된 이후에 책정된 최초의 전략으로 사이버안보 기본법을 토대로 하여 새롭게 출범한 전략본부와 내각 사이버안보 센터(NISC)의 주도하에 만들어졌다.[194] 이 전략은 2020년 도쿄올림픽·장애인 패럴림픽 개최, 그리고 2020년대 초반까지를 염두에 두고 향후 3년 정도의 기본적인 정책 방향성을 제시한 것이 골자라 하겠다. 2015년 전략은 도입부에서 사이버공간을 「무한가치를 산출하는 프론티어」로서의 인공공간이자 경제사회 활동의 기반으로 정의한다. 이에 더해 도입부에는 2015년 전략의 목적으로 자유·안전·공정한 사이버공간을 발전시켜, ① 경제사회의 활력향상과 지속 발전, ② 국민이 안전과 안심을 보장하는

193) 이 부분은 필자(이상현)의 논문 "일본의 사이버안보 수행체계와 전략," 『국가안보와 전략』, 제19권 1호 (2019)를 토대로 작성하였음을 밝혀둔다.

194) サイバーセキュリティ戦略本部, "サイバーセキュリティ戦略," 2015.9.4., 〈https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku.pdf〉 (검색일: 2019.1.20.).

사회실현, ③ 국제사회의 평화와 안정 및 국가 안보 기여 등 세 가지가 제시되어 있다.

본론에서는 앞에서 언급한 세 가지 목적을 달성하기 위한 정부의 대처방안들이 구체적으로 명시되어 있다. 2015년 전략에서 첫 번째 목적인 「경제사회의 활력향상과 지속 발전」과 관련해서는 사이버안보를 '비용'이 아닌 '투자'로 인식해야 한다는 점이 강조된다. 이와 더불어 경영층의 의식개혁이야 말로 안전·안심할 수 있는 고부가가치의 제품 및 서비스를 제공하고 신규 산업을 창출하기 위한 핵심 요소임을 지적한다.

두 번째 목적인 「국민의 안전과 안심을 보장하는 사회실현」에 대해서는 사이버위협에 대처하여 각 주체(개인·기업, 핵심 기반시설 사업자, 정부기관)들이 추진 또는 검토해야 할 사항들이 제시되어 있다. 주목할 점은 국민과 사회의 보호를 위하여 사이버범죄에 대한 수사능력 및 다양한 대처능력을 강화해야 한다는 내용이다. 핵심 기반시설은 기능이 저하되거나 정지할 경우 여러 분야에 걸쳐 사회에 커다란 영향을 미칠 수 있기 때문에 민관 모두가 매우 중점을 두고 보호해야 하는 분야라고 할 수 있다. 2015년 전략은 이와 관련하여 핵심 기반시설 분야의 범위 및 각 분야별 사업자 범위를 지속적으로 조정해 나가야 함을 강조한다. 참고로 2014년 정책회의에서는 정보통신 분야를 비롯하여 금융, 항공, 철도, 전력, 가스, 행정서비스, 의료, 수도, 물류, 화학, 크레딧, 석유 등 열세 가지 분야가 핵심 기반시설의 범위로 결정되었다.[195] 덧붙여서 정부기관 보호와 관련해서는 「정부기관 감시·즉응 조정팀」(Government Security Operation Coordination team: GSOC)의 감시 분석과 기능을 강화하고 이를 위하여 사이버안보 기본법의 개정을 검토할 필요성과 함께 정부기

195) 이상현, "일본의 사이버안보 수행체계와 전략," p. 139.

관에 대한 통일적인 기준 개정과 운용상황에 대한 감사 등 사이버 안보 강화에 대한 다양한 추진방안을 제시하고 있다.

세 번째 목적인 「국제사회의 평화와 안정 및 국가 안보 기여」에 대한 구체적 대응 방침은 사이버안보가 '위기관리' 그리고 '국가안보'와 밀접히 연관되어 있는 영역이라는 인식에 토대를 두고 있음을 알 수 있다. 구체적으로는 경찰과 자위대를 비롯한 여러 대처기관의 역량 강화를 목표로 하고 있으며, 사이버공간을 둘러싼 국제규범 형성에 적극 공헌, 개발도상국 대상 역량강화 지원에 대한 적극적 협력 추진, ASEAN과의 협력 강화, 동맹국 미국과의 긴밀한 연대 추진 등을 국제평화와 안정을 유지하기 위한 방안으로 두고 있다.

2015년 전략의 특징으로는 다음과 같이 세 가지를 지적해 볼 수 있다. 우선 다중이해당사자들의 자율성을 존중하여 사이버 공간에 대한 국가의 관리와 통제에 단호하게 반대한다는 점이다. 사이버공간의 국제규범을 둘러싼 국제적 논의는 크게 미국, 영국을 중심으로 한 서방진영과 중국, 러시아를 중심으로 한 비(非)서방 국가들이 대립하는 형국을 보이고 있다. 전자의 경우 정보의 자유로운 유통과 사이버공간에서의 표현의 자유가 존중되어야 한다는 입장인데 반해 후자는 사이버 공간은 국가가 나서서 통제와 관리를 해야 한다는 입장이다. 서방선진 7개국(G7) 회의의 회원국이자 '서방진영의 일원'이란 정체성을 가진 일본은 사이버 공간에 대한 정치권력의 감시와 통제에 반대하며 사이버공간에서의 표현의 자유와 정보교류의 자유가 담보되어야 한다는 입장이다.

둘째, 사이버공간에 대한 방첩기능을 강화해 나간다는 점을 명확히 밝혔다는 점이다. 최근 증폭되는 국제적 사이버 위협에 대한 사이버 선진국들의 대응을 보게 되면 사이버공간에 대한 국가 정보기관의 역할을 대폭 강화하고 있음을 알 수 있다.[196] 미국과 영국의

경우 신호정보(Signal Intelligence: SIGINT)를 담당하는 국가안보국(National Security Agency: NSA)과 정부통신본부(Government Communications Headquarters: GCHQ)가 사이버 안보 분야로 그 활동 영역을 확대하고 있으며, 이 외에도 러시아의 연방보안청(FSB), 중국의 국가안전부, 독일의 연방정보국(BND) 등의 정보기관이 사이버안보와 관련하여 중심적 역할을 담당하고 있다. 이처럼 미국, 영국 등 사이버안보 선진국들이 NSA, GCHQ와 같은 SIGINT 분야의 정보기관을 중심으로 사이버공간에 대한 정보역량을 강화해 가는데 비해 일본의 경우 2015년 전략이 발표될 때까지 사이버안보 체제에서의 정보기관의 역할과 위상은 베일에 가려져 있었다고 해도 과언이 아니다. 2014년 제정된 사이버 기본법에 기초한 사이버안보 수행체제를 보더라도 내각관방 산하의 NISC가 컨트롤 타워의 역할을 하고 있는 반면, 정보기관의 역할은 어디에서도 찾아볼 수 없었다. 하지만 2015년 전략에서는 "정부기관이 보유하는 기밀정보를 표적으로 한 사이버공격에 대처하기 위해 내각정보조사실 등 관계기관에서 사이버 방첩 관련 대응을 추진한다"고 하여, 적대적인 사이버 첩보활동에 대해서는 '내각정보조사실(Cabinet Intelligence and Research Organization: CIRO 이하 내조)'을 중심으로 사이버 방첩을 해 나갈 것임을 선언하였다. 사이버 방첩에 한정되기는 하지만 미국 CIA의 카운트 파트인 내조가 주체임을 명확히 함으로써 사이버공간에 대한 정보기관의 위상과 역할이 2015년 전략을 통해 드러나게 되었다.

196) 土屋大洋, "サイバーセキュリティとインテリジェンス機関—米英における技術変化のインパクト—," 『国際政治』, 第179号 (2015), pp. 50~53.

〈그림 Ⅳ-2〉 일본의 정보공동체

출처: 내각정보조사실 홈페이지를 참조하여 필자 작성[197]

세 번째 특징은 GSOC의 기능을 강화해 나간다는 방침이 제시되었다는 점이다. GSOC은 2008년 NISC 산하에 만들어진 조직으로 1년 365일 24시간 태세로 정부기구의 정보시스템에 대한 외부로부터의 사이버공격을 감시 분석하는 것이 주된 임무이다. 2015년 전략에 GSOC의 기능강화가 명시된 데에는 2015년 6월에 발생한 일본연금기구에 대한 사이버 공격 사건이 결정적인 역할을 하였다. 다시 말해서 일본연금기구의 개인정보 유출사건이 일어났을 때 연금기구가 감시 및 침해사고 조사 대상이 아니었기 때문에 침해사고에 신속하게 대응하지 못했다는 반성에서 비롯된 것이다. 2015년 전략은

197) 内閣官房ウェブページ, "内閣のインテリジェンス体制," 〈https://www.cas.go.jp/jp/gaiyou/jimu/jyouhoutyousa/taisei.html〉 (검색일: 2019.10.2.). 참고로 일본의 정보기관을 보게 되면 美 CIA의 카운터파트 역할을 담당하는 내각정보조사실(내각관방소속)을 중심으로 하여 외무성의 국제정보통괄관, 방위성의 정보본부(특히 정보본부내의 SIGINT를 담당하는 전파부가 미국 NSA의 카운트파트 역할을 담당), 경찰청의 경비국, 공안조사청 등이 정보공동체를 구성하고 있다.

GSOC이 실시하는 감시 및 진상규명 대상을 일본연금기구 등 일부 특수법인과 독립 행정법인으로 확대해야 한다고 지적함과 동시에 관련 기본법의 조속히 개정할 것을 촉구하였다. 이러한 노력은 2016년에 들어와 기본법 개정으로 이어졌다. 기본법 개정 결과 감시 및 원인규명 조사 대상범위는 기존의 중앙부처에서 독립행정법인과 전략본부가 지정한 법인(특수법인 및 인가법인)으로 확대되었다.

2018년 전략은 2015년 전략에 대한 개정을 통해 향후 3년간의 기본적인 정책방향성을 제시한 것이다.[198] 전략본부는 2018년 전략 수립과 관련하여 신(新)전략에 반영해야 할 주요 검토사항으로 ① 사이버공간의 미래상과 새로운 위협에 대한 예측, ② 2020년 도쿄 올림픽과 올림픽 이후를 대비한 체제정비, ③ 새롭게 대처해야 할 과제 선정과 대책의 조속한 실시 등 세 가지를 제시하였다.[199]

먼저 2018년 전략의 책정취지를 보게 되면 사이버공간의 미래상과 관련하여 'Society 5.0'란 개념이 등장한다.[200] 수렵사회, 농경사회, 공업사회, 정보사회를 거쳐서 도달하는 새로운 사회라 할 수 있는 Society 5.0은 '사이버공간과 현실공간이 고도로 융합되어 경제 발전과 사회적 과제를 해결해 나가는 인간중심의 사회'를 가리킨다. 원래 아베 정부의 다섯 번째 성장전략인 「미래투자전략 2017」에서 처음 등장한 것으로 아베 정부는 여기서 4차 산업혁명의 첨단기술이라 할 수 있는 IoT, 빅데이터, AI, 핀테크(Fintech) 등을 모든 산업이나 사회생활에 도입하여 국민들의 필요에 맞는 서비스를 제공하고, 사회적 과제를 해결해 나가는 사회를 지향해 나간다는 구상

198) サイバーセキュリティ戦略本部, "サイバーセキュリティ戦略," 2018.7. 27., 〈https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018.pdf〉 (검색일: 2019.10.2.).

199) サイバーセキュリティ戦略本部, "次期サイバーセキュリティ戦略の検討に当たっての基本的考え方," 2018.1.17.

200) Society 5.0이란 개념은 경단련(経団連)이 최초로 제안한 것으로 정부도 이에 공감하여 과학기술정책 등에 반영하고 있다.

을 밝히고 있다.[201] 요컨대 2018년 전략은 국가 성장전략이기도 한 Society 5.0을 사이버공간의 미래상으로 제시한 뒤 이의 성공적 실현을 위한 토대로 사이버공간의 지속적 발전과 안전이 필요하며, 사이버 위협의 확산과 증대에 대처하기 위해서도 사이버안보는 반드시 실현되어야 함을 강조한다.

2018년 전략은 ① 자유로운 정보 교류 보장, ② 법의 지배, ③ 개방성, ④ 자율성, ⑤ 다양한 주체 간 연대 등 2015년 전략에서 내건 다섯 가지 기본원칙을 계승하는 한편으로 3가지 전략목표를 중심으로 이를 달성하기 위한 구체적 대응 방안들을 제시하고 있는데, 이는 2015년 전략과 구성 및 체계 면에서 상당히 유사하다. 단, 특이점은 2020년 도쿄 올림픽 개최의 성공을 위한 전략들을 구체화한 점과 세 가지 전략 목표를 달성하기 위해 새롭게 대처해야 할 과제들이 추가된 점이다. 이러한 점들을 중심으로 2018년 전략을 검토해 보면 다음과 같은 특징들을 발견할 수 있다.

가장 큰 특징은 사이버 공격과 자위권 발동 여부에 대한 일본정부의 인식이 반영되어 있다는 것이다. 2018년 전략은 일본이 사이버공간에서도 유엔헌장을 비롯한 국제법이 적용된다는 종래 서방 선진국들의 입장과 동일하다는 인식을 밝히고 있으며, 2016년 G7 정상회의에서의 합의내용을 근거로 "일정한 경우 사이버 공격이 국제법상의 무력행사 또는 무력공격이 될 수 있다"고 하여 사이버 공격에 대한 개별 또는 집단 자위권 발동이 가능하다는 인식을 우회적으로 밝히고 있다.[202]

두 번째 특징은 사이버공격에 대한 억지력 강화 차원에서 사이버

---

201) 閣議決定, "未来投資戦略2017-Society5.0の実現に向けた改革," 2017.6.9., 〈https://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/miraitousi2017_t.pdf〉 (검색일: 2019.9.20.).

202) サイバーセキュリティ戦略本部, "サイバーセキュリティ戦略," p. 34.

공간에 대한 정보수집과 분석기능 강화를 선언하였다는 점이다.[203] 2015년 전략에서 사이버공간에 대한 방첩기능 강화를 선언하여 국가 정보기관인 '내조'를 중심으로 외국의 적대적인 사이버 활동에 대한 사이버 방첩활동을 추진해 나간다는 방침을 천명하였다는 점은 앞에서 살펴본 대로다. 2018년 전략에서는 이보다 한층 더 진화된 내용을 담고 있는데, "공격자에게 책임을 묻기 위해 사이버공격을 탐지·조사·분석하는 능력이 필요하다"고 하여 사이버공격의 진원지를 특정하기 위한 정보기관의 능력을 강화시키고 필요에 따라서는 제재를 취하겠다는 방침을 밝히고 있다. 이와 관련하여 미국의 인터넷 뉴스 매체인 인터셉트(The Intercept)가 2017년부터 2018년에 걸쳐 공개한 '스노든 일본 파일'은 2013년 무렵부터 내조와 방위본부 산하의 전파부(Directorate for Sinnals Intelligence: DFS)가 사이버공간에서의 정보수집 능력 강화를 위해 미(美) NSA와 긴밀한 협력을 추진해 온 정황을 보여주고 있다.[204] 이를 통해 사이버공간에서의 정보수집 및 분석능력 강화를 위한 일본 정보기관의 노력은 2018년 전략이 발표되기 이전부터 미국 정보기관의 협력하에 극비리로 추진되어 왔다는 사실을 유추해 볼 수 있다.

세 번째 특징은 국가안보를 위협하는 외부로부터의 사이버공격에 대한 대처방안으로 방위력·억지력·상황파악력을 강화해 나간다는 점을 명확히 하였다는 점이다. 구체적으로 살펴보게 되면 전반적인

203) 위의 글, p. 35.

204) 스노든 일본파일(Snowden Japan Files)은 2013년 NSA의 계약직원이던 에드워드 스노든(Edward Snowden)이 유출시킨 대량의 NSA 기밀문서 중 일본과 관련한 미공개 문서를 말한다. Ryan Gallagher, "Japan Made Secret Deals with The NSA That Expanded Global Surveillance," *The Intercept*, April 24, 2017, 〈https://theintercept.com/2017/04/24/japans-secret-deals-with-the-nsa-that-expand-global-surveillance/〉 (Accessed August 22, 2019); Ryan Gallagher, "The Untold Story of Japan's Secret Spy Agency," *The Intercept,* May 19, 2018, 〈https://theintercept.com/2018/05/19/japan-dfs-surveillance-agency/〉 (Accessed August 4, 2019).

조정역할은 내각관방산하에 설치된 국가안전보장회의(NSC)의 사무국인 국가안전보장국(NSS)이 담당하되, '방어'는 NISC를 중심으로 관련된 모든 기관, '억지'는 NISC, 국가안보국, 경찰청, 외무성, 방위성 등 대응조치를 담당하는 부처, 상황파악은 NSS, 내조, 경찰청, 법무성, 경제산업성, 방위성 등 정보수집과 조사를 담당하는 기관이 긴밀히 협력하여 추진해 나가되, 필요시에는 NSC에서 논의하고 결정할 수 있도록 하였다.

마지막으로 2018년 전략은 2020년 도쿄올림픽 행사기간에 발생할지 모를 사이버 침해사고에 대한 대응방안으로 '사이버안보 대처조정센터'를 구축한다는 방침을 제시하고 있다. 올림픽과 같은 대형 스포츠 행사의 경우 사이버 공격의 유인이 증가하기 마련인데, 〈표 Ⅳ-4〉에서 정리했듯이 이러한 경향은 2010년 이후 개최된 과거의 올림픽을 통해서도 살펴볼 수 있다.

〈표 Ⅳ-4〉 2010년 이후 치러진 올림픽에서의 사이버공격 피해 사례

대회	구체적인 공격 사례
2012년 런던올림픽	• 올림픽 공식 사이트에 대한 약 2억 건의 악의적인 접속 • 개막식 직전에 올림픽 경기장 전원에 대한 공격정보를 입수하여 필요한 조치를 실시
2016년 리오올림픽	• 올림픽 공식 사이트에 대한 집요한 사이버 공격 • 올림픽 관련 일부 조직 웹사이트의 내용 조작
2018년 평창올림픽	• 올림픽 준비 기간에 약 6억 건, 대회 기간 중에 약 550만 건의 사이버 공격 • 개막식 당시 사이버 공격으로 인해 일부 서비스가 이용 불가

출처: サイバーセキュリティ戦略本部,『サイバーセキュリティ2019 (2018年度報告・2019年度計画)』(2019.5.23.), p. 14.

(2) 일본의 사이버안보 추진체계

일본의 사이버안보 추진체계에서 핵심적 역할을 담당하는 것은 사이버안보 정책의 기본전략을 수립하는 '사이버안보 전략본부'와 기본전략의 입안 및 기타 민관영역의 통일적, 횡단적 사이버안보대책 추진관련 기획입안 및 종합조정을 실시하는 '내각 사이버안보 센터(NISC)'이다. 그리고 전략본부의 구성원인 경찰청, 방위성, 외무성, 총무성, 경제산업성 등 5개 중앙성청이 NISC와 협력하여 사이버안보 관련 업무를 수행해 오고 있다. 이를 도식으로 나타내면 〈그림 Ⅳ-3〉과 같다.

2014년에 제정된 사이버 기본법에 따르면 내각에 설치된 사이버안보 전략본부는 사이버안보와 관련된 기본전략을 수립하는 최고의 사결정기관이다.[205] 전략본부는 본부장과 부본부장을 각각 내각관방장관과 IT담당대신이 담당하며, 수상을 비롯하여 국가공안위원회 위원장, 방위상, 총무상, 외무상, 경제산업상 등이 임명하는 7명의 민간 고문들로 구성된다. 전략본부는 사이버안보 관련 중장기 계획인 「사이버안보전략」을 3년 단위로 수립하며 매년 다음 년도의 '연차계획'과 이전 년도의 '연차보고'를 작성하는데, 2018년부터는 연차계획과 연차보고를 하나로 엮은 보고서를 작성하고 있다. 또한 전략본부는 사이버 기본법이 규정한 바에 따라 사이버안보전략안을 작성함에 있어 IT종합전략본부 및 NSC의 의견을 청취하여야 하며, 사이버안보와 관련된 중요사항과 관련해서는 두 기관과 긴밀히 협력할 필요가 있다.

내각관방에 설치된 NISC는 앞에서 언급한 전략본부의 사무국 역

205) 村野正泰, "サイバーセキュリティに関する法律及び制度," 『情報通信技術の進展とサイバーセキュリティ (科学技術に関する調査プロジェクト2014)』 (東京：三菱総合研究所, 2015), pp. 158~159.

할을 하는 조직이다. 사이버 기본법에 따르면, NISC의 주된 업무는 ① 정책 기획과 부처간 업무조정, ② 정부부처의 정보시스템을 목표로 한 사이버 공격 감시 및 분석, ③ 사이버 침해사고에 대한 원인분석 및 대처 등 세 가지이다.[206] 또한 NISC는 범정부 조직인 「정부기관 감시·즉응 조정팀」(Government Security Operation Coordination team: GSOC)과 정보안보 긴급지원팀(Cyber incident Mobile Assistant Team: CYMAT)을 운영한다. 두 조직에 대해 개략적인 설명을 하자면, GSOC은 정부기관 정보시스템에 대한 부정 활동을 감시 및 분석하는 업무를 담당하며, CYMAT는 범정부 차원의 대응이 요구되는 중대한 침해사고에 대해 복구·피해확대 방지, 원인조사, 재발방지 등에 필요한 기술적 지원 및 조언을 담당한다.

다음으로 전략본부의 구성원인 경찰청, 방위성, 외무성, 총무성, 경제산업성 등 5개 중앙성청의 임무와 역할을 살펴보면 아래와 같다.

먼저 사이버범죄 및 테러를 담당하는 경찰청의 경우 종합적인 사이버안보대책 강화의 일환으로 경찰조직 내 컨트롤타워 역할을 담당하는 '장관관방 심의관' 및 '장관관방 참사관'을 설치하여 대처해 오고 있다. 이들은 주로 경찰청 내 사이버안보 관련 각종업무의 총괄 및 조정업무를 담당한다. 구체적으로는 △사이버안보 전략책정, △사이버공간 정세의 종합적 분석, △사이버공간 위협에 대한 종합적인 대처방안 책정, △범정부차원의 수사·기술 지원 조정, △수사관 등 인재육성에 관한 지침입안, △민간사업자, 외국기관 등과의 연락총괄 등의 업무를 수행한다.[207]

사이버 방위 분야를 담당하는 방위성은 2013년 부대신을 위원장으로 하는 '사이버정책 검토위원회'를 신설하여 국제협력, 인재양성

206) 이상현, "일본의 사이버안보 수행체계와 전략," p. 121.

207) 警察庁, 『警察白書』 (東京 : 警察庁, 2017), p. 134, 〈https://www.npa.go.jp/hakusyo/h29/pdf/pdf/07_dai3syo.pdf〉 (검색일: 2019.10.3.).

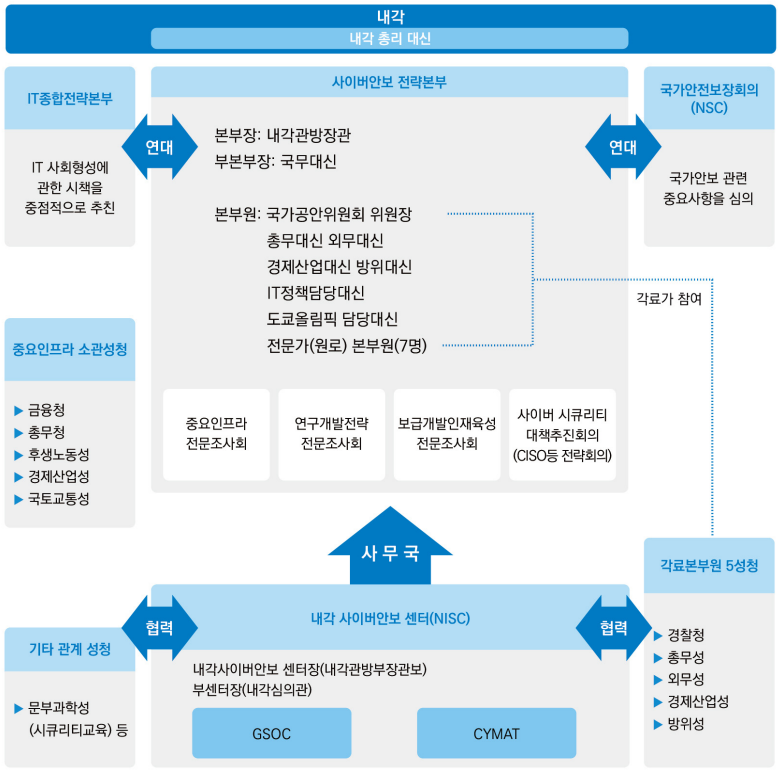
및 확보, 방위산업체와의 협력 등 사이버공격 위협에 대한 종합적인 검토를 실시하는 한편으로, 2014년에는 '자위대 지휘통신 시스템대' 산하에 24시간 태세로 방위성과 자위대의 통신 네트워크를 감시하는 '사이버방위대'를 신설하여 외부로부터의 사이버공격에 대한 대응책을 강화하고 있다.[208]

사이버 외교를 담당하는 외무성은 ① 국제적인 법의 지배 확립, ② 신뢰구축 추진, ③ 개도국에 대한 역량강화지원 등을 중심으로 사이버 외교를 추진하고 있다. 전담조직과 관련해서는 2016년 총합외교정책국(안전보장정책과)에 '사이버안전보장정책실'을 설치하였다가, 2019년 10월에는 새로운 전담조직으로 '신안전보장과제정책실'이 신설되었다. 외무성은 이들 조직을 통해 주요국과의 연대강화 및 사이버규범 확립을 위한 국제적 논의에 적극적으로 참여해 오고 있다.[209]

208) 防衛省, 『防衛白書』 (東京 : 日経印刷, 2019), p. 233.

209) 外務省報道発表, "総合外交政策局サイバー安全保障政策室の設置," 2016.7.12., 〈https://www.mofa.go.jp/mofaj/press/release/press4_003479.html〉 (검색일: 2019.10.3.).

〈그림 Ⅳ-3〉 일본의 사이버안보 추진체계



출처: サイバーセキュリティ戦略本部, 「サイバーセキュリティ戦略詳細の概要」 2018.7.27., 〈https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018-shousaigaiyou.pdf〉 (검색일: 2019.10.3.).

정보통신 분야를 소관하는 총무성은 사이버안보 추진체제의 강화를 위해 2018년 '사이버안보 통괄관'을 신설하는 한편으로 조직과 일반이용자에 초점을 맞춘 사이버안보 대책 강화 방안을 추진하고 있다.[210] 먼저 조직과 관련해서는 사이버공격에 대한 대처능력 향상을 위해 국가행정기관, 지방공공단체, 독립행정법인, 핵심 기반시

210) 総務省, 『情報通信白書』 (東京: 総務省, 2018), pp. 324~327., 〈http://www.soumu.go.jp/johotsusintokei/whitepaper/index.html〉 (검색일: 2019.10.3.).

설 사업자 등을 상대로 사이버 침해사고 발생 시의 대처요령을 습득하는 '실천적 사이버 방어연습(Cyber Defense Exercise with Recurrence: CYDER)'을 실시하고 있다.

경제산업 및 산업기술혁신 정책을 담당하는 경제산업성은 정보처리추진기구(Information-technology Promotion Agency: IPA) 및 일반사단법인인 'JPCERT 코디네이션 센터(Japan Computer Emergency Response Team Coordination Center: JPCERT/CC)'와의 협력을 통해 산업 분야의 사이버안보 관련 대응책을 마련하고 있다.[211] 그런 한편으로 사이버안보 감사제도 추진, 중요인프라 제어 시스템의 사이버안보 관련 연구개발을 추진하는 '제어시스템 시큐리티 센터(Control System Security Center: CSSC)'에 대한 지원도 담당한다.

다. 사이버 국제협력[212]

사이버 외교의 주무부서인 외무성은 업무의 효율적 추진을 위해 2016년 총합외교정책국 산하에 '사이버안전보장정책실'을 설치하였다가, 2019년 10월에는 '신안전보장과제정책실(Emerging Security Challenges Division)'을 설치하여 사이버 관련 업무를 전담시키고 있다.[213] 외무성 홈페이지에 따르면 일본은 2013년에 발표된 '국가

211) JPCERT/CC는 1996년에 설립된 일본을 대표하는 컴퓨터긴급대응팀(Computer Emergency Response team: CERT)으로 사이버침해사고에 대한 보고접수, 대응지원, 발생상황 파악 및 분석, 재발방지 대책 검토 및 조언 등의 업무를 기술적인 측면에서 실시한다. 情報処理推進機構, 『情報セキュリティ白書 2018』(東京 : 情報処理推進機構, 2018), pp. 110~112, 〈https://www.ipa.go.jp/security/publications/hakusyo/2018.html〉(검색일: 2019.10.3.).

212) 이 부분은 필자(이상현)의 논문 "사이버 위협에 대한 일본의 대응: 사이버 외교와 사이버 방위," 『국가전략』, 제25권 2호 (2019), pp. 96~103을 토대로 작성하였다.

213) 外務省報道発表, "総合外交政策局安全保障政策課の組織改編," 2019.10.1., 〈https://www.mofa.go.jp/mofaj/press/release/press4_007868.html〉(검색일: 2019.10.15.).

안전보장전략(NSS)'과 2015년에 발표된 '사이버안보전략'을 토대로 하여 ① 국제적인 법의 지배 확립, ② 신뢰구축(Confidence Building) 추진, ③ 개도국에 대한 역량강화(Capacity Building) 지원 등 세 가지 원칙을 중시하는 사이버 외교를 추진하고 있다.[214]

(1) 양자 및 다자외교를 통한 신뢰구축 추진

사이버 외교에서의 신뢰구축 추진이란 국가들 간 사이버 분쟁을 예방하기 위해 평시에 사이버안보 관련 투명성과 안정성 확보를 위한 노력을 전개하는 것을 의미한다. 익명성, 은밀성 등의 특성을 지니는 사이버 공격의 특성상 의도하지 않게 국가 간의 긴장이 고조될 수 있기 때문에 피해국과 공격 의심국 간의 우발적인 충돌을 방지하고 국가 간 신뢰를 조성한다는 측면에서 국가 간 정보교환, 정책대화, 교류가 중요하다는 인식에서 나온 것이다.[215] 〈표 Ⅳ-5〉를 통해 알 수 있듯이, 일본은 2019년 10월 현재 동맹국인 미국을 비롯하여 영국, 프랑스, 호주, 독일, 러시아, 인도, 한국, 이스라엘, 에스토니아, 우크라이나 등 11 개 국가와의 양자 사이버협의 또는 사이버 대화를 실시하는 한편으로, 유럽연합(EU), 동남아시아국가연합(ASEAN) 등 지역기구와의 사이버협의도 실시하고 있다.[216] 이 중 양자 사이버 협의는 2012년경 부터 자국의 관련 정책과 활동을 상대국에 소개

214) 外務省ウェブページ, "日本のサイバー外交," 作成日不明, 〈https://www.mofa.go.jp/mofaj/annai/page5_000250.html〉 (검색일: 2019.6.3.).

215) 신뢰구축과 관련해서는 土屋大洋, 『サイバーセキュリティと国際政治』 (東京 : 千倉書房, 2015), pp. 168~179; 土屋大洋 (2014), pp. 334~339. 참고로 신뢰구축은 냉전시기 전통안보 분야에서 등장한 개념이다.

216) 外務省 報道発表, "重要インフラのサイバーセキュリティに関する日米韓専門家会合の開催," 2016.12.20., 〈https://www.mofa.go.jp/mofaj/press/release/press4_004079.html〉 (검색일: 2019.7.5.); 外務省 報道発表, "サイバーセキュリティに関する日米韓専門家会合の開催」," 2018.7.30., 〈https://www.mofa.go.jp/mofaj/press/release/press4_006290.html〉 (검색일: 2019.7.6.).

하고 서로의 입장을 확인하는 수준에서 출발하였으며, 회를 거듭할수록 우호국 간 구체적인 양자 협력을 실시하는 방향으로 진화하고 있다.

〈표 Ⅳ-5〉 일본의 양자 간 사이버협의 개최실적(2012~2019)

연도	국가명
2012년	영국(1차), 인도(1차)
2013년	미국(1차)
2014년	미국(2차), EU(1차), 한국·중국(1차), 이스라엘(1차), 에스토니아(1차), 프랑스(1차), 영국(2차)
2015년	호주(1차), 러시아(1차), 미국(3차), 한국·중국(2차), 에스토니아(2차)
2016년	프랑스(2차), 이스라엘(2차), 미국(4차), 호주(2차), 독일(1차), 영국(3차), 한국(1차), 러시아(2차), 우크라이나(1차)
2017년	프랑스(3차), EU(2차), 에스토니아(3차), 한국·중국(3차), 미국(5차), 인도(2차), 이스라엘(3차), 호주(3차)
2018년	EU(3차), 영국(4차), 프랑스(4차), 미국(6차), 이스라엘(4차)
2019년	인도(3차), 호주(4차), EU(4차), 프랑스(5차), 미국(7차)

출처: 외무성 홈페이지 ※괄호 안 숫자는 양자협의의 회차를 나타냄.

(2) 국제 규범 형성에 대한 대응

일본은 서방선진국의 일원으로 유엔헌장을 포함한 기존 국제법이 사이버공간에도 적용된다는 입장을 취하고 있으며, 국제사회에서의 사이버공간에 대한 규범형성에 선도적으로 나서겠다는 의지를 가지고 기본적 가치관을 공유하는 국가들과의 협력 강화에 적극적으로 나서고 있다.

먼저 일본은 유엔총회 제1위원회 산하의 정부전문가그룹(GGE)과 사이버공간총회(GCCS) 참가를 통해 자신들의 입장을 발신하고 가치 공유국들과의 협력을 강화하는 등 국제규범 마련을 위한 국제사회의 논의에 적극적으로 참여하고 있다. 미국의 국제규범 형성에 대

한 대응에서도 살펴봤듯이, 유엔 GGE의 경우 2018년 개최된 제73차 유엔 총회에서 제6차 유엔 GGE의 구성과 더불어 러시아가 제안한 개방형 워킹 그룹(OEWG)제안 결의안이 채택되어 국제규범을 둘러싼 논의는 새로운 단계에 접어 들었다.[217] 2012년 제3차 유엔 GGE 참가 이래 국제규범 형성에 적극적인 역할을 하고자 하는 일본은 2019년 9월 9일부터 13일까지 4일간 뉴욕에서 개최된 제1차 개방형워킹그룹회의에서 OEWG가 지금까지의 유엔 GGE가 이룩한 성과에 입각하여 활동을 해 나가되, OEWG와 GGE가 대립관계를 형성하기 보다는 상호보완적인 역할을 해나가야 한다는 점을 강조하였다.[218]

한편, 일본은 유엔 GGE에서의 활동과 더불어 서방선진국들의 사교모임적 성격을 가진 서방선진 7개국(Group of Seven: G7) 회의를 사이버 외교의 공간으로 적극 활용하고 있다. 이와 관련하여 2016년 자국의 미에현(三重県) 이세시마(伊勢志摩)에서 열린 G7 정상회의에서 일본정부는 사이버안보 문제를 의제로 상정하여 공동성명 부속문서를 도출하는 등 적극적으로 대응하는 모습을 보였다. 일본 주도하에 체결된 사이버안보 관련 공동성명 부속문서에는 서구 선진 7개국의 합의사항으로 ① 유엔헌장을 포함한 국제법의 사이버 공간 적용 가능, ② 사이버공간의 악의적 이용에 대한 긴밀한 협력과 강력한 대응, ③ 올림픽 등 대형 국제 이벤트에 대한 사이버안보

217) OEWG는 국제안보 관련 정보 및 전기통신분야의 발전에 관해 유엔의 모든 회원국들이 참가할 수 있는 논의의 장으로 2019년 9월 첫 회의를 시작으로 총 3번의 회의를 통해 2020년 유엔총회에 보고서를 제출하도록 되어 있다. 이에 반해 제6차 유엔 GGE의 경우 25개국의 전문가들에 의한 전문적인 논의의 장으로 2019년 12월 제1차 회의를 시작으로 총 4번의 회의를 거쳐 2021년 유엔총회에 보고서를 제출하도록 되어 있다.

218) 外務省 報道発表, “第1回サイバーセキュリティに関する国連オープン・エンド作業部会会合の開催,” 2019.9.19., 〈https://www.mofa.go.jp/mofaj/press/release/press4_007809.html〉 (검색일: 2019.7.6.).

촉진 등의 내용이 포함되었다.[219] 2017년 4월 10일과 11일 양일간 이탈리아 루카(Lucca)에서 개최된 G7외상회의에서는 회의 종료후 「사이버공간에서의 책임있는 국가의 행동에 관한 G7선언」[220]이라는 문서가 채택 발표되었다.

(3) 개도국에 대한 역량강화지원

일본은 사이버공간의 특징상 일부 지역이나 국가의 대처능력 부족이 자국의 안보를 위협함은 물론 세계전체의 위험요인이 된다는 인식하에 개도국의 역량강화 지원에 앞장서고 있다. 주목할 점은 이전의 역량강화 사업이 경찰청, 총무성, 법무성, 외무성, 경제산업성, 방위성 등 관련 성청 단위로 전개되어 개도국에 대한 역량강화 지원사업이 분절화되는 경향이 있었기 때문에, 최근에는 전략적이고 효율적인 지원을 실시하고 효과를 극대화하기 위해 이들 간의 긴밀한 협력과 연대를 강조한다는 점이다.[221] 이를 위해 2016년 10월「사이버안보 분야 개발도상국에 대한 능력구축 지원」이라는 범정부차원의 기본방침을 마련하였으며, 이 방침에 따라 모든 정부부처가 하나가 되어 전략적이면서도 효율적인 지원을 위한 노력을 하고 있다.

일본의 역량강화 지원 사업은 개도국에 대한 양자 중심 대응과 다자무대를 중심으로 한 대응으로 나누어진다. 양자 중심 대응에서 눈에 띄는 것은 글로벌 파트너십 강화라는 측면에서 2009년부터 다양

219) "６つの付属文書 サイバーテロに対抗措置," 『日本経済新聞』, 2016.5.28.

220) 外務省ウェブページ, "サイバー空間における責任ある国家の行動に関するＧ７ルッカ)宣言," 2017.4.11., 〈https://www.mofa.go.jp/mofaj/files/000246366.pdf〉(검색일: 2019.7.6.).

221) 内閣サイバーセキュリティセンター · 警察庁 · 総務省 · 法務省 · 外務省 · 経済産業省 · 防衛省, "サイバーセキュリティ分野における開発途上国に対する能力構築支援基本方針) 概要," 2016.10., 〈https://www.mofa.go.jp/mofaj/files/000210150.pdf〉(검색일: 2019.6.15.).

한 연대 프로그램 실시를 통해 ASEAN 회원국들에 대한 역량강화 지원을 적극적으로 추진하고 있다는 점이다. 배후에는 일본 기업이 자동차산업 등 제조업체를 중심으로 동남아 각국에 진출하여 일본과 ASEAN 간의 경제적 유대관계가 긴밀한 상황에서, 향후 ASEAN 회원국들의 인터넷 보급률이 확대되어 간다고 가정했을 때, 이들의 열악한 사이버안보 환경이 일본에게 리스크 요인이 될 수 있다는 계산이 깔려 있다고 하겠다.[222] 일본의 ASEAN 회원국에 대한 역량강화 지원을 구체적으로 살펴보면 의식계발 및 중요 인프라 방호, 사이버 범죄대책, CSIRT(Computer Security Incident Response Team) 및 법집행기관의 능력강화 등의 지원을 실시하고 있다. 사이버범죄조약 체약국회의와 같은 다자외교 공간에서는 사이버범죄대책지원을 통해 사이버 공격 등의 범죄에 대한 대처·수사능력 향상을 통해 범죄를 억지하려는 노력을 하는 한편으로 사이버공간 이용에 관한 국제적 규범 마련 및 신뢰양성조치에 관한 개도국의 이해와 인식 공유를 위한 노력을 기울이고 있다.

(4) 양자 및 다자간 사이버 방위협력

일본은 사이버 공격에 대한 자체 방어역량을 강화를 서두르는 한편으로 동맹국인 미국과의 사이버 연대를 강화하는 방식으로 방위성과 자위대의 대응능력을 향상시키고 있다. 미일양국은 2011년 6월에 개최된 미일안보협의위원회(Security Consultative Committee: SCC)를 통해 처음으로 사이버안보 분야의 전략적 정책협의체 설치에 공감대를 형성하였다.[223] 양국 위원회는 공동발표문을 통해 "증

222) 谷脇康彦, "わが国のサイバーセキュリティ戦略," 『経済広報センターポケット・エディション・シリーズ』, no. 134 (2014), p. 22.

223) 日米安全保障協議委員会共同発表, "より深化し、拡大する日米同盟に向けて−50年間のパートナーシップの基礎の上に," 2011.6.11., 〈http://www.mod.go.jp/j/app

대하는 사이버 위협이 초래하는 과제에 미일 양국의 새로운 공동대처 방안에 대해 협의할 것을 결의하고, 양국 간 사이버안보 관련 전략적 정책협의체 수립을 환영하였다"는 점을 확인하였다. 이로부터 3년 뒤인 2014년에는 '미일사이버방위정책워킹그룹(Cyber Defense Policy Working Group: CDPWG)' 이라는 국방당국 간 실무레벨의 협의채널이 마련되었다. 양국은 이 협의채널을 통하여 ① 사이버 관련 정책 협의추진, ② 긴밀한 정보공유, ③ 사이버공격 대처를 위한 공동훈련 실시, ④ 전문가 육성 및 확보를 위한 협력과 관련된 실무협의를 실시하고 있다.[224]

이런 가운데 2019년 4월 미일 양국의 외교·국방장관이 참여하여 개최된 미일안보협의위원회(SCC)에서는 전쟁의 양상이 변화하고 있다는데 인식을 공유한 뒤 양국은 "일정한 경우에는 사이버 공격이 미일안보조약 제5조가 규정하는 무력공격에 해당할 수 있다는 점을 확인하였다"고 하여 미국의 대일방위 의무를 규정한 미일안보조약이 일본을 상대로 한 사이버 공격에도 적용될 수 있다는 데 인식을 같이 하였다.

한편, 일본은 사이버 방위 협력과 관련하여 동맹국 미국과의 연대강화와 더불어 중시하는 것이 NATO와의 협력강화이다. 일본은 NATO와 방위당국 간 사이버협의체인 '일-NATO 사이버 방위스텝 대화'를 매년 실시하고 있으며, NATO가 주최하는 '사이버방위연습(Cyber Coalition)'에도 옵서버를 파견하고 있다.[225] 이와 더불어 NATO의 사이버방위 관련 연구와 훈련을 실시하는 기구로 에스토니아의 주도로 설립된 사이버방위협력센터(Cooperative Cyber Defence

---

roach/anpo/kyougi/2011/06/js1_j.html〉(검색일: 2019.6.16.).

224) 防衛省, 『平成30年度版防衛白書』(東京 : 日経印刷. 2018), pp. 333~334.

225) 위의 글, p. 334.

Centre of Excellence: CCDCOE)와도 협력을 강화해 나가고 있다. 그리하여 아베 총리의 2018년 에스토니아 방문시에는 CCDCOE에 대한 일본 참가 승인이 이루어졌고, 같은 해 5월 오노데라(小野寺五典) 방위상이 방문하였을 때에는 방위성 직원의 CCDCOE 파견에도 합의하였다.[226] 이러한 행보에는 사이버전과 집단적 자위권 발동 여부에 대해 구체적인 법률 검토 필요성에 직면해 있는 일본정부의 고민이 담겨 있다. 다시 말해 이러한 행보의 배후에는 탈린 매뉴얼(Tallinn Manual)을 작성하는 등 사이버전 관련 국제규범 연구를 선도하는 CCDCOE와의 협력을 통해 국내의 사이버방위 관련 법률 논의를 심화시키려는 의도가 숨겨져 있는 것이다.

라. 한반도에 대한 함의[227]

앞서 살펴본 일본의 사이버안보가 한국에 주는 함의는 아래와 같이 세 가지 측면에서 검토해 볼 수 있다.

우선 일본 외무성의 경우 사이버외교의 효율적 추진을 위해 2016년 총합외교정책국 산하에 '사이버안보정책실'이라는 전담조직을 설치하고 2019년 10월에는 '신안전보장과제정책실'을 신설하였듯이, IT 선진국의 사이버외교를 효율적 추진을 위해서는 이를 전담하는 부서를 외교부에 신설할 필요가 있다는 점이다. 우리나라 외교부의 경우에는 국제기구국 산하의 국제안보과가 여러 업무 중 하나로 양자 및 다자간 사이버 협의 및 사이버 규범외교 실시와 같은 사이버외교 업무를 담당하고 있다. 그러나 2019년 9월 발표된 국가 사이버안보

226) 防衛省, "日エストニア防衛相会談（概要)," 2018.5.6., 〈http://www.mod.go.jp/j/approach/exchange/area/docs/2018/05/06_j-estonia_gaiyo.html〉 (검색일: 2019.6.16.).

227) 이 부분은 필자(이상현)의 논문 "사이버 위협에 대한 일본의 대응: 사이버 외교와 사이버 방위," 『국가전략』, 제25권 2호 (2019)를 토대로 작성하였다.

기본계획에서 '외교부 주관으로 사이버안보 분야 대외전략 수립을 위한 유관부처 간 정치적 논의를 위한 협의기구 운영'이 포함되는 등 향후 사이버안보 관련 업무가 지속적으로 증대될 것이 확실해지는 상황을 고려했을 때 사이버안보 업무를 효율적으로 추진하기 위한 새로운 전담 부서 신설은 반드시 검토되어야 한다.[228]

둘째, 일본이 사이버 규범외교를 추진함에 있어 서구선진국의 일원이라는 정체성을 토대로 G7회의를 활용하였듯이, 우리 또한 우리가 산파역할을 한 중견국 협의체인 믹타(MIKTA)를 다자공간을 무대로 한 사이버 규범외교를 추진함에 있어 적극 활용할 수 있다는 점이다. 미국과 영국을 중심으로 한 서방진영 사이버 강국 그리고 중국과 러시아로 대표되는 비(非)서방진영 사이버 강국들의 틈바구니 속에서 미들파워 국가들의 목소리를 반영한다는 차원에서 MIKTA는 유용한 협력체로 기능할 수 있다. 이를 위해서는 우선 중견국들만이 가지는 공통된 규범인식이 존재하는가에 대한 검토를 개시할 필요가 있다. 그리고 만약 이를 통해 공통된 규범인식을 도출할 수 있다면 한 단계 더 나아가 사이버안보를 MIKTA 회원국들 간의 중점협력이슈로 개발할 수도 있을 것이다.

마지막으로 역대최악이라는 수식어가 무색할 정도로 악화된 한일관계는 해결의 실마리를 찾지 못하고 있으며, 이러한 양국관계는 사이버안보 분야 양국 협력에도 악영향을 미치고 있다. 한일 사이버안보 협의는 2016년에 제1차 협의가 실시된 이후 3년이 지나도록 2차 후속협의를 위한 논의조차도 못하고 있는 실정이다. 그러나 2019년 현재 한일양국이 직면하고 있는 최악의 대립국면이 진정국면에 접어든다면 제2차 한일 사이버 대화는 조속히 개최되고 활성화 되어야 한다. 2018년 평창 동계 올림픽을 1년 여 앞둔 시점에서 개최된 제1

228) 관계부처 합동, 『국가 사이버 기본 계획』, 2019.9.3., p. 28.

차 한일 사이버안보 협의에서 올림픽의 성공적 개최를 위한 양국 간 사이버안보 협력방안이 주요 의제 중 하나였다는 점을 고려한다면, 2차 한일 사이버안보 협의는 한국이 경험한 평창올림픽 관련 정보를 일본과 공유하고 2020년 개최 예정인 도쿄올림픽의 성공적 개최를 위한 사이버 분야 협력방안이 논의되어야 한다. 사이버안보 분야에서의 양국 간 협력 재개는 대치국면에 처해있는 한일양국이 화해국면으로 나아가는 돌파구가 될 수 있을 것이다.

3. 중국

가. 사이버공간에 대한 인식 및 환경

중국의 사이버 영역 연구는 1990년대 초반부터 본격적으로 시작되었다. 중국의 사이버역량은 선진국과 비교하면 기술적인 측면이나 양적인 측면에서 발전 속도가 상당히 뒤처져 있었다. 중국 사이버 발전전략의 변화는 기본적으로 시대적 변화를 인식하고 그에 따라 대응하는 방식으로 설정한 것이라 할 수 있다. 하지만 그 정책의 특징과 방향이 단기적인 차원에서 접근하는 것이 아닌 장기적으로 집행해나갈 정책 인식에 기초한 목표와 방향성까지 내포하고 있다. 그 주요한 특징으로는 첫째, 기술의 중요성에 관한 인식 전환이다. 중국은 인터넷 기술 강국의 경험을 적극적으로 받아들이고 연구하여 중국 실정에 맞게 변용했다. 특히 미국의 정책 변화에 따라 제도적인 개혁을 시행하는 모습을 엿볼 수 있다. 일례로, 클린턴 정부는 1990년대 초반 미국은 경제적 측면에서 활용하기 위해 새로운 인터넷 정책을 수립한다. 대용량·고속 인터넷 정보유통시설을 구축하는 '국가정보기반구조 행동계획(정보고속도로, Information Highway)'이 바로 그것이

다. 같은 해 12월, 중국은 국가경제정보화연석회의 기구를 설립하여 정부 경제영역의 정보화 업무 리더와 조직을 통일하였다. 1994년 6월, 중국 정부는 '3금 공정(三金工程)에 관한 통지'를 발표한다. '3금 공정'은 금교공정(金桥工程), 금카드공정(金卡工程), 금관공정(金关工程)으로 나누어져 있는데, 첫째, 금교공정은 국가 공용 경제정보망을 구축하는 것이다. 국가 공용 경제정보망을 통해 각급 지도자와 관련 부처가 적시에, 정확한 관련 경제 정보와 국민경제 데이터를 국가에 적시에 제공하여, 거시적 경제 조절과 대책 수준을 향상하려는 프로젝트이다. 둘째, 금카드 공정은 금융 전산화 프로젝트로 정보 카드와 현금 카드의 이용 보급을 목표로 하는 통화 전자화 프로젝트이다. 신용카드를 보급하여 전자 결제 방식으로 화폐를 유통함으로써, 자금 이용률과 회전율을 높여 국가 금융기관 자금의 거시적 조정 능력을 향상하고자 한 프로젝트이다. 전자데이터교환기술(EDI)을 보급하고 대외무역 정보 관리 사업을 시행하기 위한 국가 대외 경제무역 정보망 프로젝트이다. 세관·경제 무역·금융·외환 관리·세무 등의 부서를 네트워크로 연결하고, 세관을 통과하는 수출입 무역 외환 결제 대금과 환급 세금을 전산화하여, 업무 처리의 정확성을 높이고 손실을 방지하기 위한 정책이다. 해당 정책은 인터넷 서비스를 통한 경제 발전과 사회관리 업무의 촉진을 모색한 것이었다. 결론적으로 1994년부터 1998년까지의 중국 네트워크 정책의 주요 목표는 사이버 기술력 강화와 이를 통한 안정적인 발전 시스템 구축에 있었다. 해당 시기의 주요 연구 주제 역시 대부분 인터넷 정보기술과 하드웨어 및 소프트웨어 등에 초점을 맞추고 있으며, 관련 자료를 보면 중국 정부의 인식과 정책 방향성을 명확하게 확인할 수 있다.

〈표 Ⅳ-6〉 장쩌민 시기 사이버 연구 주제 분석(상위 10위)

순위	연구 주제	편수	비율
1	인터넷 기술(互联网技术)	2,212	47.8%
2	정보 경제와 우정 경제(信息经济與邮政经济)	738	16.0%
3	컴퓨터 소프트웨어 및 컴퓨터 응용 (计算机软件及计算机应用)	378	8.2%
4	공업경제(工业经济)	281	6.1%
5	전신기술(电信技术)	213	4.6%
6	컴퓨터 하드웨어 기술(计算机硬件技术)	150	3.2%
7	무역경제(贸易经济)	98	2.1%
8	공안(公安)	76	1.6%
9	기업경제(企业经济)	72	1.6%
10	도서정보와 디지털 도서관(图书情报與数字图书馆)	61	1.3%

출처: 김상규, "중국의 사이버안보 정책 변화와 그 함의," 『현대중국연구』, 20권 4호, p 50.

이 같은 중국의 노력에도 불구하고 미국은 이미 전 세계 인터넷 시장을 선도하고 있었는데, Window 98이 출시되어 상용화하기 시작한 것이다. 하지만, 중국은 해당 분야에서 막 걸음마를 뗀 단계에 불과했다. 물론, 중국 내부에서도 인터넷 열풍이 불고 있었고, 중국 최초의 검색엔진인 SOHU의 창립을 비롯해 BAIDU, TENCENT 등 현재 중국 IT를 이끄는 대표적 인터넷 기업들이 창업하거나 설립하는 시도가 진행되고 있었다. 이 같은 변화 속에 중국 정부가 인터넷 영역에 관한 중요성을 인식, 국가 정보화 업무를 통합하여 효율성을 높이고 관련 정책의 시행과 관리를 담보하려고 한 의도를 볼 수 있다.

둘째, 사이버공간의 자주성과 혁신에 대한 인식이다. 중국은 기술 연구와 선진국 벤치마킹의 전략을 통해 기술 혁신과 독립의 두 가지 정책 목표를 추구하였다. 가장 특징적인 내용은 중국의 사이버 거버넌스 현실에 맞는 일련의 정책들을 추진했다는 것이다. 예를 들어, 공업부(정보산업부), 문화부, 교육부, 공안부 등 여러 부처가 중국

의 특색을 가진 관리정책을 수립하였다. 그중에서도 핵심은 '사이버 주권' 주장의 제기와 '사이버 보안법'의 시행이다. 해당 정책은 중국의 사이버 통치의 근본이념이 '자주'로 전환되었다는 것을 보여준다. 2010년 6월, 중국은 '중국 사이버 상황 백서'를 통해 사이버공간은 국가의 중요한 인프라이고, 역내 사이버공간은 중국의 주권 담당이 이루어지는 곳이라며 주권이 존중되고 지켜져야 한다고 주장하였다. 또한, 2014년 11월, 시진핑 정부는 제1차 세계사이버대회 축사를 통해 "중국은 세계 각국과 협력해 국제협력을 심화하고 사이버 주권을 존중하며 사이버안보를 보호하고 평화, 안전, 투명한 사이버 공간을 공동구축하겠다(中国愿意同世界各国携手努力，深化国际合作，尊重网络主权，维护网络安全，共同构建和平、安全、透明的网络空间)"고 천명하였다. 이후, 2016년 11월 17일, 중국은 "사이버 보안법"을 공포하였다. 해당 법은 중국이 사이버공간에 대해 어떻게 인식을 하는지 명확히 보여준다. 미국은 주로 컴퓨터시스템과 네트워크 등 인프라와 지적 재산권 같은 지식 정보자산의 안보 유지를 중요시하지만, 중국은 인터넷을 통해 유통되는 콘텐츠 등 정치·이념 차원의 안보 유지에 중점을 두고 있다.[229]

이 같은 정책 실행은 중국의 안보 인식과 궤를 같이한다. 특히, 정보안보는 중국 사이버 정책의 주요한 내용으로 네트워크 인프라의 구축, 네트워크 표준의 연구와 제정, 국제 네트워크와의 연결 등을 포함하고 있다. 중국은 단순히 공안업무뿐만 아니라 사이버공간에서 전파될 수 있는 유해정보와 불법적 내용의 콘텐츠 관리 조처를 시행하고 있다. 1999년 10월 발표된 '정보 네트워크를 통한 방송과 영화의 방송물 관리 강화에 관한 통고'는 부정적인 인터넷 콘텐츠

229) 김상배, "사이버안보의 복합지정학: 비대칭 전쟁의 국가전략과 과잉 안보담론의 경계," 『국제지역연구』, 24권 3호 (2015), p. 16.

전파에 대해 관리와 심사 인준 리스트를 하게 되어 있다. 해당 시기부터 사이버 정책의 안보개념은 이미 정치와 문화 방면으로 외연을 확장하고 있다는 것을 보여준다. 셋째, 사이버공간에 대한 안보 인식이다. 상술한 내용에서도 이미 언급하였지만, 사이버공간도 국가의 영토, 영해, 영공은 물론 우주 등 실체적인 현실의 공간과 마찬가지로 국가 주권을 적용할 수 있는 곳임을 명확히 하고 있다. 따라서, 사이버공간에 대한 주권 침해는 있을 수 없으며, 이를 수호하려는 일련의 법적, 제도적 조처와 행위는 국가안보 차원에서 당연한 국가 주권 행사의 권리라고 인식한다. 중국 사이버안보체제의 정책 기조는 '강한 정부, 약한 사회'로, 국가가 통제하는 사이버안보체제를 형성하고 있다. 이는 중국이 사이버공간에 대해 자주적으로 법적·제도적 시스템을 만들며 영향력을 확대하려는 의도를 보여준다. 중국이 사이버공간에 대한 국제사회의 규범 논의에도 적극적으로 개입하고 영향력을 행사하는 것도 이와 같은 맥락에서 이해할 수 있다.

나. 사이버안보 전략 및 추진체계

중국의 사이버 영역에 대한 인식은 사이버안보를 어떻게 구현할 것인지의 문제와도 직접 연결된다. 중국의 사이버안보체계는 앞서 설명한 인식 차원에 기초하고, 더불어 현실적인 여건에 맞는 정책 집행을 통해 차근차근 시행해나갔다. 1986년 2월, 중국은 국가경제정보센터(国家經濟信息中心)를 설립하면서 정보화 사업을 추진해 나간다. 해당 조직의 목표는 국가 정무의 정보화 시스템 구축과 선진 기술을 받아들여 기술력과 정보화 수준을 향상하는 것이다. 중국은 이를 시작으로 1990년대 초반부터 관련 조직을 구성하고 확대·개편하는 과정을 거친다. 1993년 3월, 중국 정부는 기계 전자공업부(机械电子工业部)를 분할, 전자공업부(电子工业部)로 재편하였다. 같

은 해 12월, 국무원은 부총리를 위원장으로 하는 '국가경제정보화연석회의'를 설립하고 국가 전산망과 정보안보에 관한 업무를 담당하게 하였다. 이어 1996년 4월, '국가경제정보화연석회의'를 국무원 '정보화 사업 영도 소조'로 바꾸었다. 또한, 1998년 3월에는 정보산업부를 구성하여 국무원 '정보화 업무영도 소조 판공실'을 '국가정보화판공실'로 확대 개편하였으며, 체신부(국가 체신국으로 변경)와 전자공업부를 통합하였다. 이와 동시에 같은 해 9월, 공안부는 '공안정보화 사업의 속도를 강화'하라는 중앙 지도부의 지시에 따라 공안부 '과기강경(科技强警)' 마스터플랜 체제를 채택하였다. 경제 문제와 사회의 변화에 발맞춰 범죄 해결과 관리의 효율성을 높이기 위한 '금순공정(전국공안정보화 프로젝트)'을 시작한 것이다. 이어 11월에는, 공안부가 '공안정보화사업인 금순공정 실시에 관한 요청'을 국무원에 보고하고 12월 국가계획위원회에 보낸다. 이듬해인 1999년 1월, 전국 공안청(국)장 회의에서 공안정보화사업인 금순공정을 전국적으로 본격적으로 가동하겠다고 공식 선언한다. 이 같은 일련의 조치들이 상당히 빠른 속도로 진행되었다는 것은 그만큼 정부가 관련 영역의 중요성과 시급성을 인식했다는 것으로 추론할 수 있다. 해당 정책은 기술력을 통해 공안시스템의 통합지휘와 신속대응, 작전 협조, 범죄 소탕 능력을 강화하는 것이다. 그 핵심은 공안통신네트워크와 컴퓨터 정보시스템으로 전국 공안종합업무통신망, 전국 위법범죄정보센터(CCIC), 전국 공안지휘 통제시스템 프로젝트, 전국 공공 사이버안보 모니터링센터의 구축이다. 이 같은 시스템의 구축은 전국 범죄정보센터를 중심으로 각 공안업무의 정보공유와 종합적으로 활용하여 각 공안업무에 강력한 정보지원의 실현을 목표로 한 것이다.

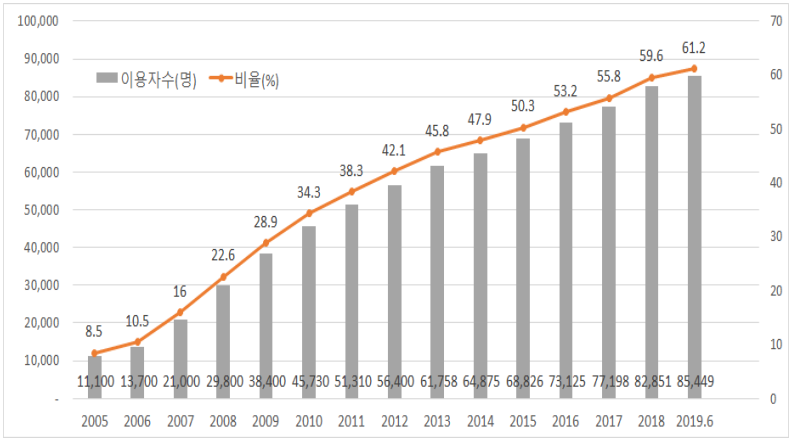
2000년대 초반부터 인터넷 보급이 점차 확대되면서 각 분야에 걸

쳐 정보화의 영향력이 급속하게 확대되었다. 이에 2000년 10월, 중국 공산당 15기 5중 전회에서 “정보 네트워크 안전보장 강화” 부분을 포함하여 정보화에 따른 정보 안전에 대해 당과 정부 차원에서 더욱 적극적인 정책에 관심을 두기 시작하였다.[230] 이 방침에 따라, 2001년 8월, 국가 정보화 영도 소조를 구성하고, 국무원 정보화 업무판공실을 설치하여 정보화 건설과 정보안보 업무영도 강화, 국가 정보화 발전전략의 심의, 거시정책과 중요한 의사결정을 종합적으로 조율하였다. 전문적인 인터넷 정보 관리와 의사결정기구의 출현은 중국이 독립적인 인터넷 거버넌스를 추구한다는 것을 의미한다. 2002년에는 국방 영역에서의 정보화 문제에 대해 공식적으로 언급한다. 즉, 국가 주권과 안보를 수호하기 위해서는 군사력의 불균형을 극복해야 하며, 이는 군 정보화에 기초하여 현대화를 이루어야 한다는 점을 강조하고 있다. 이후, 2008년 3월, 정보산업부는 폐지되고 공업과 정보화부·국무원 정보화 업무판공실과 국가발전과개혁위원회(华人民共和国国家发展和改革委员会: 발개위)의 공업업종 관리 직책을 수립하였다. 이후 국방과학 공업위원회 핵발전관리 직책을 제외하고 공신부로 통합하였다. 해당 정책의 목적은 인터넷과 정보사업의 다자관리 실태를 개혁하고 통합관리를 강화하기 위한 것이다. 그러나 공신부는 국무원에 소속된 부서이기 때문에 한계가 있었다. 기능, 직급, 부처 간 조율이 어렵고, 인터넷 거버넌스와 의사결정이 분산되어 원활한 정책 결정을 진행하기 어렵다는 문제점은 바뀌지 않았다. 2011년 이후 중국의 인터넷 영역은 인터넷과 경제, 정치, 사회발전 분야의 크로스오버가 급격히 진행되었고, 중국 인터넷 개인 사용자(네티즌) 수가 급증하고 휴대전화 인터넷 사용자가 점차 늘고 있었다.

230) 임병진, 『중국 사이버안보체계에 관한 연구』 (서울: 서울대학교, 2017), p. 31.

〈그림 Ⅳ-4〉 중국 인터넷 이용자 수 및 보급률

(단위: 만 명)



출처: 中國互聯網絡信息中心, “2019年 ‘中國互聯網絡發展狀況統計報告’,” 2019, p. 15, 〈http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201908/P020190830356787490958.pdf〉 (검색일: 2019.10.2.).

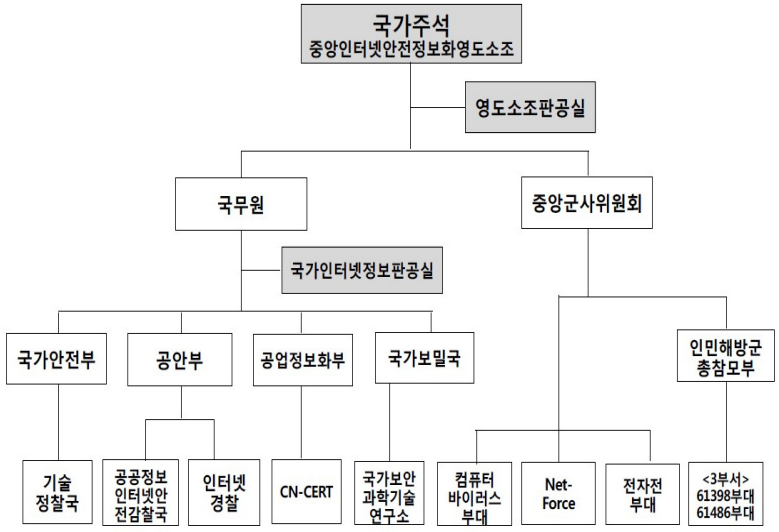
이에 2011년 5월, 중국 정부는 국가인터넷 정보사무실을 설립하였다. 해당 부서의 설립목적은 정보 네트워크의 관리를 한층 더 강화·보완하고, 사이버공간에 대한 통제 수준을 높여 온라인 여론을 감독하고 지도하기 위함이었다. 이때부터 중국의 인터넷 관리와 의사결정의 핵심 기제가 수립되었다. 이에 따라 공신부는 인터넷 산업에 대해 관리하고 관련 정책을 담당하는 데 집중하였고, 정보와 콘텐츠 관리 및 정책은 국가인터넷 정보사무소가 맡았다. 이외에도 사이버 범죄 예방 업무 등 사이버공간에 대한 관리 감독은 공안부가 담당하였다. 그러나 인터넷의 영역 간 융합이 급속도로 진행되면서 문제가 발생하였다. 정부가 사이버공간 관리에 관한 중요성을 인식한 만큼 국무원의 거의 모든 부처가 사이버 정책 결정에 관여하면서 여러 부서가 업무에 관여하게 되는 현상이 나타난 것이다. 중국 정부는 사이버공간 관리 능력 향상을 위한 사이버 의사결정기구의 획기적인

개편을 단행하였다. 2014년 2월, 중앙 사이버안보 및 정보화 영도 소조(국가 인터넷 정보 판공실, 약칭: 국신판)를 발족하였다. 해당 부서는 원래 국가 인터넷 정보 판공실이 국무원 신문판공실과 분리되어 독립된 것이다. 또한, 중국 공산당 중앙선전부(中国共产党中央宣传部: 선전부)·중화인민공화국 공업과 신식화부(中华人民共和国工业和信息化部, 약칭:공신부)·국신판, 중국외문출판발행사업국(中国外文出版发行事业局), 중국과학원(中国科学院) 등 정보 보안과 콘텐츠 관리 업무를 통합하여 최적의 조건을 갖춘 네트워크 관리와 협조기관을 편성하였다. 해당 기구는 같은 기간 성립한 국가안전위원회의 '중앙 전면 심화 개혁 영도 소조' 중 유일하게 업무 처리 실무부서를 만든다. 이 기관은 중앙기구 서열에 포함되었고, 국무원의 일반 조직구성 부문보다 상위의 기구가 되었다. 또한, 여타 인터넷 부서를 총괄하고 조정하는 권한을 부여하였다. 중국 정부가 안보 차원에서 사이버공간을 강력하고 엄격하게 관리하겠다는 의지를 보여주는 조치였다.

이와 같은 맥락에서 볼 때, 2016년 8월 발표한 '국가 사이버안보 표준화 업무에 관한 약간의 의견(关于加强国家网络安全标准化工作的若干意见)' 역시 사이버안보와 국가 업무네트워크를 포함해 인터넷 방화벽 구축 등 사이버 영역의 국가 운용체계를 효율적으로 관리·감독하겠다는 것이다. 사이버안보의 국가 표준화 사업 역시 중국 내 모든 시스템과 기관들을 하나의 네트워크로 연결해 활용할 수 있는 시스템을 구축하려는 목적을 보여준다. 이와 더불어, 2016년 11월에는 사이버 안전법을 발표하였다. 해당 법은 사이버공간의 주권 문제를 비롯해 그 전략과 목표, 법 적용 및 의무와 책임의 범위 등 아주 구체적이고 포괄적으로 구성되어 있다. 해당 시스템의 실현을 위한 중국 정부의 정책 행보는 정층설계, 전면적 조직 배치, 일괄

정책 추진, 구체적 감독 등으로 요약할 수 있으며, 그 명시적 조처는 2018년 3월, '중앙사이버안전 및 정보화 영도 소조'를 '중앙사이버안전 및 정보화위원회'로 격상한 것에서도 확인할 수 있다. 해당 분야의 중요 업무를 담당하는 '소조'가 '위원회'로 격상된 것은 장기적이고 안정적인 정책을 구현할 수 있다는 것을 의미한다. 이외에도 사이버공간의 안전과 이익을 위해 국가 전산망과 정보 안전관리센터를 공신부에서 떼어내 사이버안보와 정보화위원회의 업무로 나누어 최적화했다. 공신부는 전기통신망, 인터넷, 전용 통신망 건설, 조직을 책임지고, 통신업계의 기술 혁신과 발전에 초점을 맞추고 국가 전산망과 정보 안전관리센터 인프라 구축, 업무를 수행하게 된 것이다. 이 같은 일련의 조직 개편과 변화는 중국의 사이버 정책 결정은 물론 사이버 의사결정기구가 근본적인 문제 인식과 해결 방법을 찾기 위한 다양한 방법론을 고민하고 실질적으로 구현했다는 것을 보여준다.

〈그림 Ⅳ-5〉 중국의 사이버안보 추진체계



출처: 김상배, 세계주요국의 사이버안보 전략: 비교국가론적 시각, 『국제지역연구』, 26권 3호 (2017), p. 85.

결론적으로, 상술한 중국의 사이버안보체계 목표와 방향성은 다음의 2가지로 요약할 수 있다. 첫째, 중국의 네트워크 시스템과 기술 축적, 그리고 경제발전과 사회 안전망의 관리이다. 해당 영역은 사이버 금융 발전, 경제·사회 발전과 사회 거버넌스, 의료사회복지, 농촌농업발전, 인터넷 기반 건설, 당 업무 등 모든 영역을 망라한다. 특히나 최근 중국은 정부 기구를 간소화하고 상부 기관의 권한을 하부 기관으로 이양하는 '간정방권(简政放权)'에 의해 사회 거버넌스 모델의 전면적인 개혁이 추진되고 있다. 따라서 인터넷 기술과 경제사회 분야의 융합이 심화, 가속화하면서 인터넷과 사회 거버넌스에 대한 중국 정부의 관리 감독 역시 확대되는 시스템을 구축하는 방향으로 나가고 있다는 점을 확인할 수 있다. 둘째, 안보적인 차원에서

의 시스템 구축이다. 국내 차원에서의 사이버 영역에서의 안보 취약성에 대해 중국은 강력히 주장한다. 중국은 매월 중국 '국가 컴퓨터 네트워크 응급기술처리 협조센터(CNCERT, 이하 인터넷 응급센터)'가 '국가 정보보안 취약점 공유플랫폼(CNVD)'을 통해 협력업체(보안업체, 통신서비스업체, 통신기기 장비 업체)들과 CNCERT 지역센터, 개인(화이트해커)으로부터 접수한 사건형 정보보안 취약점들을 평가해 밝히고 있다.[231] 개인은 물론 정부 기관과 기업, 당의 업무 과정에서 발생하는 소프트웨어, 하드웨어, 정보시스템 등이 취약하다는 점을 강조한 것이다. 이는 중국이 사이버 영역에서의 문제를 국제사회와 어떻게 협의, 협력하느냐의 문제하고도 맞닿아 있다.

다. 사이버 국제협력

중국은 이제껏 사이버공간에서의 적극적인 행보를 하지 못했다. 중국의 기술력이나 시스템이 국제사회에서 선도적인 역할을 할 수 있는 역량이 안 됐기 때문이다. 따라서 선제적 정책 시행이나 연구를 진행한 것은 아닌 인터넷 후발주자로서 새로운 국내외적 상황 출현에 따른 사후 대응 방식을 선택했다.[232] 이 같은 측면에서 중국은 기술력을 강화하기 위해 계속 노력을 해왔고, 경제적인 성장에 기초하여 사이버 영역에서의 급속한 발전과 성장을 이루었다. 이 때문에 현재 사이버 영역에서 국제사회로부터, 특히 미국으로부터 사이버 공격, 해킹 등을 통해 미국의 정보를 탈취하고 있다는 의심을 받고 있다. 이는 5G 기술의 백도어(back door) 문제로까지 연결되어 미

231) "中 "누리꾼 절반 보안사건 겪어… 지난해 바이러스 감염기기 줄어"," 『보안뉴스』, 2019.3.13., 〈https://www.boannews.com/media/view.asp?idx=77783&kind=〉, (검색일: 2019.10.5.).

232) 김상규, "중국의 사이버안보 정책 변화와 그 함의," p. 9.

·중 무역 전쟁의 갈등 요인으로도 주목받았다. 이처럼 국제사회에서 중국이 갖는 사이버 영역에서의 전략과 행보는 긍정적이지 않다. 이유는 크게 두 가지로 요약할 수 있다. 중국의 사이버 영역에 대한 인식이 미국을 위시한 서방국가들과 다르다는 점과 중국의 기술력과 경제력이 점차 증가하면서 선진국들을 위협하는 수준에 이르렀다는 사실에 기인한다. 이는 국제사회에서 중국의 행보를 통해 충분히 확인할 수 있다. 2001년 12월 열린 유엔총회에서 중국은 국제표준화 기구 중 하나인 ITU 이니셔티브를 주도하였다. 또한, 정보사회 세계정상회의를 개최하며 홈그라운드 외교를 통한 영향력 확대를 꾀하였다. 물론 2003년 와이파이용 보안 프로토콜(WAPI)에 실패하긴 했지만, 사이버공간에서 중국의 행동반경을 넓히기 위한 표준화 수립 시도를 하는 등 국가적인 역량을 지속해서 쏟아부었다.

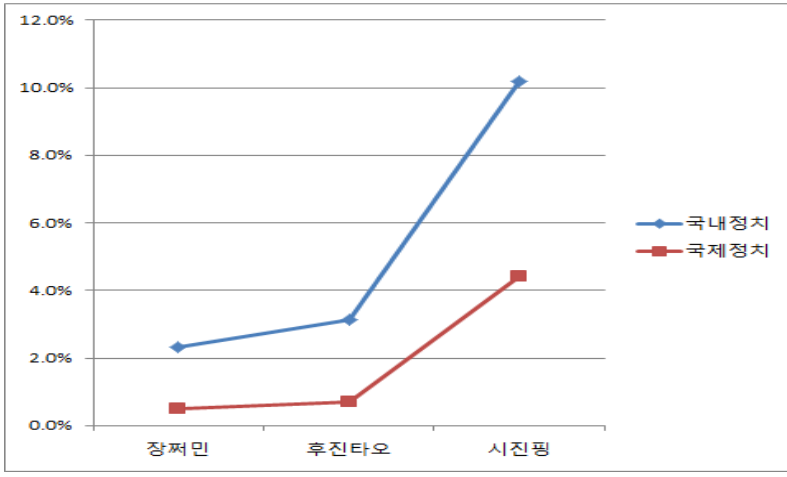
이외에도 중국은 중국국가인터넷정보판공실이 주최하는 세계 인터넷 대회(世界互联网大会, World Internet Conference: WIC)를 2014년부터 매년 저장성(浙江省) 우전(乌镇)에서 개최하고 있다. 매년 다른 주제를 표방하지만, 사이버 영역에서의 기본 입장은 대동소이하다. 다만, 중국이 지향하는 외교적 이념을 강조하고, 최신 기술을 선보이는 등 엑스포 형태의 방식을 차용하여 운용하고 있다.

중국은 국제 사이버공간 거버넌스의 시작을 위해 '정부 주도, 각 분야 참여'를 주장했다. 사이버공간에 대한 접근이 정부 주도의 방식으로 출발한다는 점에서 중국이 주장하는 사이버 국가 주권과 정보안보의 인식과 궤를 같이한다. 이 때문에 중국이 국제사회에서 선택할 수 있는 협력의 방식이 제한적이다. 그중 중국이 주도적인 역할을 집행하는 상하이협력기구는 중국이 국제사회에서 활용하는 사이버 협력의 플랫폼으로서 그 의미가 있다. 중국은 해당 기구를 통해 국제정보안보에 관한 논의를 수행하고 관련 성명과 계획 등을 채

택한다. 따라서 국제 협력공간의 의미보다는 중국과 인식을 공유하고 협력을 강화하기 위한 플랫폼으로 보는 것이 더 적절하다. 물론 가장 중요한 협력관계는 무엇보다 미국과의 관계 형성이다. 양국 간 인식의 차이는 있지만, 사이버공간이 갖는 중요성 때문에 시진핑과 오바마가 양국 정상 회담을 통해 사이버 해킹 중단 협약을 맺거나(2015년 9월), 중국 공안부장과 미국의 국토안보부 장관 사이에 고위급대화를 진행(2015년 12월)하여 사이버범죄 척결을 위한 인식을 같이하는 등 일정 부분 의미 있는 결과를 도출하기도 하였다. 또한, 2017년부터 미·중 외교·안보 대화를 통해 사이버안보에 관한 의견을 교환하고 있다. 그러나 여전히 해킹 문제로 인해 위반 여부로 갈등이 발생하고 있다. 하지만 중국은 민간의 문제로 치부하며 인식을 달리한다.

시진핑은 집권 이후 사이버공간에 대한 중요성을 인식하고 사이버역량을 강화하는 데 집중하였다. 그 방향은 내부적으로 국내 정치의 안정성 유지를 위한 정책 설정을 진행함과 동시에 대외적으로 서구사회와의 규범 경쟁 상황을 대비하는 전략까지 포괄하고 있다. (그림 Ⅳ-6, 표 Ⅳ-7)

〈그림 Ⅳ-6〉 중국 지도자 시기별 주요 정책 연구 문제



출처: 김상규, "중국의 사이버안보 정책 변화와 그 함의," 『현대중국연구』, 20권 4호, p. 61.

〈표 Ⅳ-7〉 시진핑 시기 사이버안보 주요 정책 연구 주제

순위	연구 주제	편수	비율
1	互联网技术	10,660	42.6%
2	信息经济與邮政经济	3,031	12.1%
3	计算机软件及计算机应用	1,685	6.7%
4	电信技术	1,349	5.4%
5	中国政治與国际政治	1,322	5.3%
6	公安	1,089	4.4%
7	行政法及地方法制	1,023	4.1%
8	工业经济	620	2.5%
9	金融	526	2.1%
10	行政学及国家行政管理	441	1.8%

출처: 김상규, "중국의 사이버안보 정책 변화와 그 함의," p. 58.

이 같은 정책 설정의 배경은 미국과의 경쟁 관계를 가장 많이 고려한 것이라고 할 수 있다. 하지만, 중국의 근본적 핵심이익이 침해되지 않는다면 경쟁 관계 속에서도 공동으로 대처해야 할 중대한 문

제가 발생한다면 상황에 따라 미국뿐 아니라 주변국들과도 협력관계를 형성해 나갈 것이다. 사이버공간이 바로 초연결 사회(hyper-connected society)의 전형이며 중국 역시 사이버공간의 안정적인 운용이 절실하기 때문이다.

라. 한반도에 대한 함의

중국의 사이버공간 담론은 향후 우리에게 다양한 형태로 영향을 끼치게 될 것이다. 따라서 중국의 사이버공간 변화를 하나씩 살펴봄으로써 우리에게 주는 함의는 무엇인지 정리할 필요가 있다. 첫째, 중국 내부에서 어떤 변화가 일어날지 확인하는 작업이다. 중국 내부에서는 사이버 정책의 안전성과 필요성이 끊임없이 확대되어, 미래에는 더욱 강화될 것이다. 현재는 주로 네트워크 기술과 정보안보 영역 등에 초점을 맞추고 있다. 하지만, 사이버공간의 중요성과 활용 등 중요성이 증대하고 있는 만큼, 향후 사이버 영역에서의 새로운 표준을 수립하는 방향으로 나갈 것이다. 사이버공간에서의 레짐 형성은 국제 인터넷 접속 표준, 기술, 안전에 관한 정책은 국가주도의 강력한 형태로 나타날 수밖에 없다. 중국의 경우 내부적 정치 요인에 의해 정보검열과 통제 등 사이버공간의 주권을 강조하며 국가안보 범주의 정책으로 이어지고 있다. 특히, 사이버 경제와 디지털 경제가 발전함에 따라, 경제안보와 정보안보 분야는 미래 사이버 정책의 가장 핵심 사안이 될 것이다. 중국은 이미 핀테크를 통한 금융 시장의 확장과 사용자 수가 세계 최대이다. 따라서 해당 분야에서의 기술 교류와 제도 협력은 중국 국내 금융 시장의 보안을 위해서라도 필요한 부분이다. 둘째, 중국의 사이버안보는 음란물, 폭력, 도박 등 사이버공간에서 발생할 수 있는 사회적 현상을 포괄하고 있다. 해당 현상의 증가는 네트워크 이용자의 급증과 더불어 폭발적으로 늘어

나고 있으며, 네트워크 보안환경을 심각하게 훼손하고 있다. 게다가 인적, 물적 교류가 증가하면서 온라인을 통한 금융 거래가 급증하고, 해킹을 통한 정보 유출로 인한 보이스피싱 등 2차 범죄 피해도 늘어나고 있다. 따라서 불법 정보와 유해물의 이동으로 일어날 수 있는 사이버공간에서의 사회적 안정이나 국가안보 위협에 대비하기 위해서는 현상을 세밀히 분석함과 동시에 중국과의 공조를 통해 안정적이고 구체적인 협력을 이어갈 수 있는 시스템의 확립이 필요하다.

4. 러시아

가. 사이버공간에 대한 인식 및 환경

러시아는 사이버공간에 대해 안보적 관점에서부터 여타 국가들과 다르게 인식한다. 바로 '사이버안보(cyber security)'를 '정보안보(information security)'로 일컫는다는 점이다. 정보안보는 정보공간에서 안전에 대한 위협이 없는 상태를 의미하며 '정보공간에서 의도되거나 혹은 의도하지 않은 위험에 대처하거나 이를 안전한 상황으로 회복하는 것'으로 정의한다. 러시아는 사이버공간을 컴퓨터상의 가상공간이라는 개념 속에 한정하지 않고 '정보공간(information sphere)'이라는 보다 광범위한 개념으로 확대하여 해석하고 있다. 2016년 12월 정보안보에 관한 정책 '신정보 안보 독트린(New Information Security Doctrine)'에서 "정보안보는 개인, 사회 및 국가를 내외부의 정보 위협으로부터 보호하는 상태이며, 헌법상의 인권 및 시민권을 보장하며, 시민들의 품위 있는 삶의 질, 주권, 영토보존 및 러시아연방의 영속성 있는 사회경제개발은 물론 국가의 방위와 안보를 보장한다"라고 명시하고 있다.[233] 이 같은 인식은

2000년대 탈 소비에트 공간에서 벌어진 색깔 혁명의 배후에 미국과 서방의 가치와 제도, 규범의 확산을 통한 세력확장의 의도가 숨어있다고 의심하여 심각한 안보위협으로 받아들이는 것에서도 명시적으로 드러난다.[234]

러시아는 사이버공간에서 유통되는 정보 자체가 안보에 대한 위협이라고 인식하기 때문에 정보의 자유로운 생산과 유통을 적극적으로 통제하려 한다. 사이버공간을 정보가 생성·유통되는 공간으로 인식하기 때문에 무분별한 정보를 관리하고 통제하기 위해서는 정보 주권이 가장 중요할 수밖에 없다. 러시아 역시 중국과 마찬가지로 국내 차원에서의 국가안보 문제와 연결 짓는다. 인터넷을 이용한 외부의 개입이 러시아 정부에 미칠 부정적인 영향이 크다는 인식에 기인한 것으로 볼 수 있다. 정부가 독점하고 통제해야 할 정보가 일반 대중 속에서 유통될 경우, 대중이 정부에 반감을 갖고 정부에 저항함으로써 국가안보를 위협할 수 있기 때문이다. 그도 그럴 것이 러시아는 냉전 붕괴, 소련 해체과정에서 서방국가들이 활용했던 민주주의 확산 전략을 이미 경험적으로 체득했다. 따라서 이러한 외부 정보의 자유로운 유통과 확산은 반드시 통제해야 할 대상으로 인식할 수밖에 없을 것이다. 러시아 당국이 사이버공간을 어떻게 생각하고 있는지를 살펴보면, 세계 사이버 영역 지배에 대한 그들의 접근방식에 대해 많은 것을 알 수 있다. 특히, 러시아의 사이버공간에 대한 인식은 국제관계 이론의 관점에서 가장 선명하게 읽어낼 수 있다. 바로 무정부 상태의 세계를 더욱 혼란스럽게 만든다는 신홉스주의적 시각이다.[235]

---

233) 김강무, "러시아의 사이버안보 전략에 대한 고찰," (2017년 한국국제정치학회 연례학술회의 자료집, 2017), p. 2.

234) 김상배 편, "제4장 버추얼 창 공격의 복합지정학," 『사이버 안보의 세계정치와 한국: 버추얼 창과 그물망 방패』 (서울: 한울아카데미, 2018), p. 307.

235) Julien Nocetti, "Contest and conquest: Russia and global internet governance," *International Affairs*, vol. 91, no. 1 (2015), p. 116.

러시아의 정책 설정 역시 이 같은 지점에서 시작한다. 러시아는 2000년 국가정보안보정책인 '정보안보 독트린(Information Security Doctrine)'을 발표했다. 해당 내용은 러시아 국가안보와 관련된 영역이 정치, 경제, 국방 이외에 정보영역에 이해 큰 영향을 받고 있다는 것을 지적하고 있다. 특히, 2008년 조지아, 2011년 리비아 사태가 서방의 선전 활동과 정보 공세에 의해 발생한 것으로 규정하고, 외부 정보의 유입이 얼마나 위험한 것인지에 대해 자각하여 정책을 수립하고 집행하였다. 실제로 2011년 '러시아 군사력의 정보공간에서의 활동에 관한 개념적 조망(Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space)', 2013년 '러시아의 국제정보안보 분야에서의 국가정책의 기본 원칙(Basic Principles for State Policy of the Russian Federation in the Field of International Information Security)' 등 관련 내용에서 정보안보의 중요성을 명확하게 드러내고 있다. 러시아 정부가 본격적으로 인터넷 규제를 체계화시킨 것은 인터넷 시민운동과 반정부 시위가 빈번하게 일어났던 2010년대 초반에 들어서다. 2012년 러시아 의회는 인터넷 규제 법안(Federal Law No.139-FZ)을 통과시켰다. 러시아 정부가 인터넷에 대한 규제를 강화하게 된 데에는 몇 가지 이유가 있는데, 2010년대 초반 인터넷을 통한 반정부 시위가 확산하였다는 내부적인 요인과 더불어 새로운 정보통신기술이 CIS권에 불러온 변화가 러시아에 새로운 위협 요소로 인식했기 때문이다. 2014년에는 개인 블로그에 대한 검열이 강화되었는데, 매일 3,000명 이상이 방문하는 블로그는 통신 정보기술 매스컴관리국의 미디어 관리 명단에 등록해야 하며, 또한 블로거의 개인 정보 공개를 의무화하였다. 이 외에도 러시아에서 운영되는 소셜 미디어 웹사이트들의 서버를 러시아에 설치 혹은 이전해

야 하며 최소 6개월 동안 모든 사용자의 데이터를 보관할 것을 의무화하였다.[236] 2014년 12월 발표한 〈러시아연방 군사 독트린〉에서는 이러한 인식이 군사적인 방면에서도 강하게 발현하고 있음을 보여준다. 해당 내용을 보면 정보전의 중요성을 분명하게 명시하고, 정보전이 국가안보와 군사전략에서 중요한 부분이라 지적하고 있다. 특정 국가가 정보와 통신을 정치적·군사적 목적으로 사용하는 것은 상대국의 주권과 영토적 완전성을 해치고 국제법을 위반할 뿐 아니라 국제평화와 안보를 위협하는 행위라고 강조한 것이다.[237] 2016년에는 기존의 반 테러법이 개정되면서 암호화된 SNS가 급진주의 세력 및 테러집단에 남용될 수 있는 점을 근거로 러시아에서 운영되는 모든 SNS의 암호 해독 자료를 정부에 제출하라는 연방 법령 '374-FZ'와 '375-FZ'를 통과시켰다. 이와 같은 요구에 텔레그램이 반발하자 정부는 텔레그램의 사용을 중단시켰으며, 아마존(Amazon)과 구글(Google) 등 IP 주소 1800만 개를 차단하였다. 그 결과 여러 웹사이트의 운영이 중단되고 온라인 쇼핑의 마비 사태가 오기도 하였다. 한편 개인 정보 관련 법령을 준수하지 않았다는 이유로 링크드인(LinkedIn)이 글로벌 SNS 중 처음으로 러시아에서 완전히 차단되기도 하였다.[238] 같은 해 발표된 '신정보안보 독트린(Information Security Doctrine)'에서는 이보다 더 명확한 위기의식을 드러낸다. '국방, 사회, 경제, 과학기술 및 교육 등 정보인프라에 대한 공격과 침해가 증대하고 있어 러시아의 주권을 약화하고, 영토보존을 훼손하며 정치적·사회적 안정을 침해하고 있다'고 지적한 것이다.[239]

---

236) 신보람, "루넷(RuNet)과 유라시아-넷(Eurasia-Net): 중앙아시아에서의 러시아 인터넷의 위상," 『중소연구』, 42권 2호 (2018), p. 357.

237) 장덕준, 러시아의 신안보 이슈, 『여시재』, 2017.12.6., 〈https://www.yeosijae.org/posts/356〉 (검색일: 2019.9.10.).

238) 신보람, "루넷(RuNet)과 유라시아-넷(Eurasia-Net): 중앙아시아에서의 러시아 인터넷의 위상," pp. 357~358.

러시아의 인식과 일련의 정책 설정은 모두 당시 국제사회에서 점차 고조되는 사이버 공격(대표적으로 스턱스넷 사건)이 군사적·안보적 성격과 결합함으로써 그 파괴성이 높아진 것에서 기인했다고 할 수 있다. 이 때문에 러시아는 사이버안보의 군사적 측면을 강조하며 정보전쟁이라는 개념으로 확대하여 사용한다. 이 개념 속에는 정보, 보안, 기만, 역정보, 전자전, 통신약화, 내비게이션 성능저하, 심리적 압박, 정보시스템 저하와 프로파간다가 모두 포함된다.[240] 기존의 전통적인 전쟁의 개념이 사이버공간에서의 위기의식과 결합하여 새로운 형태의 전쟁인식이 형성된 것이라고 볼 수 있다. 결국, 사이버공간에서 '정보의 자유로운 유통'을 강조하는 서구의 인식과 '정보 주권'을 강조하는 러시아와 중국은 사이버공간에서조차 서방국가들과 대립을 할 수밖에 없는 근본적인 요인이라 할 것이다.[241]

나. 사이버안보 전략 및 추진체계

러시아의 사이버안보는 정치·사회체제의 보호 즉 국가안보에 기초한 정보안보 정책을 전개하고 있다. 러시아는 기본적으로 미국과 서방국가의 사이버공간을 통한 가치와 규범, 제도의 확산이 정보의 수집, 생산, 유통에 기초해 이루어지고 있다는 사실에 경각심을 갖고 있다. 2011년 미국 CIA가 정보를 불법으로 수집한 '스노든 사건'을 비롯해 정보력을 활용한 국가전략의 집행은 러시아에 새로운 대응전략 수립에 박차를 가하게 된다. 이러한 정보안보 전략은 2015년 12월 31일 발표된 러시아 국가안보전략에 명시적으로 드러나 있다. 해당 전략은 국가안보 수호를 위한 중장기 전략방안을 포괄적으로

239) 김강무, 『러시아의 사이버안보 전략에 대한 고찰』, pp. 3~4.

240) 김상배, 『사이버 안보의 국가전략 2.0』, p. 318.

241) 신범식, "러시아의 사이버안보 전략," 『슬라브학보』, 제32권 1호 (2017), pp. 147~148.

제시하고 있다. 중점을 두고 있는 것은 역시 정보안보와 관련한 사항으로, 정보공간에서 국가 주권 강화 및 인터넷 거버넌스 시스템을 개선하겠다는 의지를 강력하게 표명하며 국가 정보통제권의 인정을 주장하고 있다. 러시아가 발표한 대부분 정보안보와 관련한 정책의 핵심내용은 국가의 안보를 수호하고 획득할 수 있는 이익과 손실 등 국가 전략목표의 주요 방향성이 나타나 있다. 러시아는 정보안보가 국가이익을 내포하고 있다고 본다. 즉, "정보의 자유로운 이용, 개인 정보보호, 민주주의 수호, 상호교류 확대, 역사적·정신적·도덕적 가치 보존의 창구로써 정보공간 이용, 주요정보기반시설 보호, 통신 네트워크의 안정성 및 지속성 보장, 전자 산업 및 정보보호 산업 발전, 연구개발 강화, 정보안보에 관한 국가 간 전략적 파트너십 강화, 국제기구 활동을 통한 정보공간에서의 국가 주권보장"이라고 인식하는 것이다.[242] 정보안보를 위협하는 요인으로는 테러, 극단주의, 근본주의 및 주변국의 정보인프라에 대한 군사적 영향력 강화 및 공격, 정보·심리전을 활용한 정치·사회불안 야기, 러시아에 대한 외국 언론의 편향적 보도, 러시아의 전통가치 폄훼, 개인 정보 침해 및 금융사기를 포함해 정보기술을 이용하여 러시아 및 동맹국의 주권 및 영토 보호의 완전성을 훼손하는 행위 등으로 규정하고 있다.

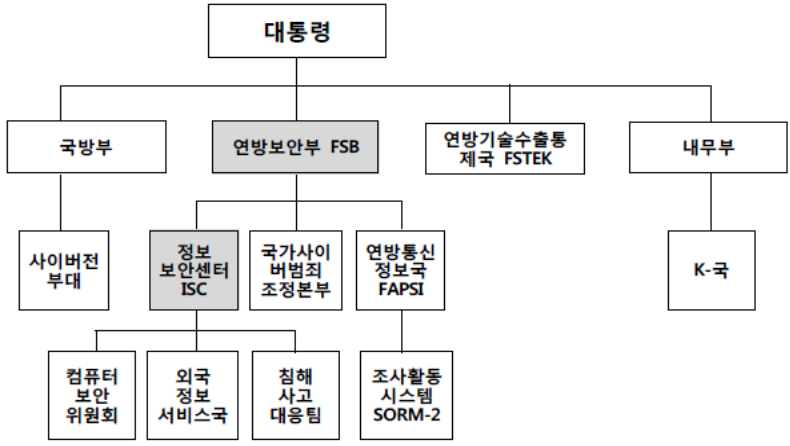
따라서 외부로부터 직간접적으로 침해당할 가능성을 사전에 차단하고 적극적으로 대응하는 전략을 수립하고 이에 따라 사이버안보를 수호하는 시스템을 구축하고 있다. 〈그림 Ⅳ-7〉은 러시아의 사이버안보 추진체계이다. 대통령 직속의 연방보안부(Federal Security Service: FSB)에서 정보보안 관련 기관을 직접 제어하고 있음을 보여준다. 푸틴 정부는 외부로부터의 위협이 이제는 사이버공간을 통

242) 양정윤·박상돈·김소정, "정보공간을 통한 러시아의 국가 영향력 확대 가능성 연구: 국가 사이버안보 역량 평가의 주요 지표를 중심으로," 『세계지역연구논총』, 제36집 2호 (2018), p. 148.

해 정교하게 침투한다고 인식하고 있어서 직접 사이버위협에 대한 대응책 마련을 강조하기도 한다. 물론, 푸틴의 안정적인 권력 유지를 위한 수단으로서의 의미도 내포하고 있음은 물론이다. 러시아 정보안보의 핵심 행위 주체인 연방보안부는 국가기밀과 중요 정보를 통제하고 예방 조치를 하는 것은 물론 주요 국가기관에 사이버 기술을 포함해 보안 업무를 제공한다. 특히 러시아 사이버위협 정보공유에 있어 중심 임무를 수행한다. 정보보안센터(ISC)는 통신보안 업무와 정보보호 시스템의 평가 및 인증을 총괄 조정하고, 침해사고대응팀의 운영과 공격 기술개발 등을 담당하고, 각급 정보를 수집하는 업무를 수행한다.[243] 연방통신정보국(FAPSI)은 인터넷 정보 조사시스템을 활용해 러시아 내부에서 유통되는 정보의 수집과 분석을 책임지고 있다.

243) 신범식, "러시아의 사이버안보 전략," p. 152.

〈그림 Ⅳ-7〉 러시아의 사이버안보 추진체계[244]



이 같은 배경에서 러시아는 서구의 사이버전(Cyber Warfare)과는 다른 정보전(Information Warfare)이라는 개념을 사용하며 관련 정책을 추진하고 있다.[245] 2014년 5월, 러시아는 군 지휘통신체계 보안을 위한 사이버전 전담부대의 창설을 결정했다. 사이버 부대의 창설은 그동안 국내적 위협에 대해 러시아 정부가 취했던 방어적 정책에서 벗어나 적극적이고 공세적인 정책으로 전환하게 된 것을 상징한다.[246] 이와 동시에 사이버공간에서의 포괄적인 전략 수립과 공세적인 대응을 하겠다는 의지의 표현이기도 하다. 러시아의 사이버군 창설은 향후 사이버 영역에서 임무 수행능력을 체계화하고 고도화하겠다는 것을 전제로 하고 있다. 러시아는 사이버공간에서 정

244) 김상배, "세계 주요국의 사이버 안보 전략: 비교 국가전략론의 시각," p. 89. 〈그림 5〉를 재인용.

245) 러시아는 컴퓨터네트워크 작전(computer network operations), 전자전(electronic warfare), 심리전(psychological operations), 정보작전(information operations)으로 구성된 포괄적 정보전(information warfare) 개념으로 확대했다. 김강무, "러시아의 사이버안보 전략에 대한 고찰," p. 3.

246) 신범식, "러시아의 사이버안보 전략," pp. 154~158.

보-기술전과 정보-심리전이라는 복합적인 형태의 전쟁을 수행한 경험이 있다. 2008년과 2014년, 조지아와 우크라이나에서 사이버 전쟁과 재래식 전쟁을 결합한 소위 '하이브리드 전쟁(Hybrid Warfare)'을 수행한 것이다. 러시아가 새로운 형태의 전쟁을 경험한 유일한 국가라는 점에서 의도하는 바를 어느 정도 추론해 낼 수 있다. 2008년 8월, 러시아와 조지아 간 분쟁은 사이버 기술을 전쟁에 사용함으로써 군사적 공세와 사이버 작전이 결합한 최초의 사례이다. 조지아의 경우 러시아에 의한 무력공격이 있기 이전부터, 그리고 양국 간 재래식 전쟁이 진행 중이던 당시에도 사이버공간에서의 위협 공격행위(DDoS)를 비롯한 통신 방해, 정보유출, 웹사이트 변조 등이 진행되었다.[247] 러시아의 사이버 능력은 미국 등 서방국가들과는 다른 체계로 발전해왔는데, 보안기술과 정보 부처를 중심으로 보안체계가 구축하는 등 이미 상당한 수준으로 발전한 것으로 알려져 있다.[248] 러시아는 전 세계적으로 군사적·정치적 목적의 사이버 활동을 적극적으로 전개하고 있다는 평가를 받고 있으며, '러시아 비지니스 네트워크(Russia Business Network: RBN)' 등 비정부(범죄, 애국적) 해커집단을 암묵적으로 활용해 사이버 능력을 강화하고 있다.

그러나, 러시아의 사이버 능력에 대한 서방의 일부 평가는 이와는 또 다르다. ITU에서 발표하는 '세계사이버안보지수(Global Cybersecurity Index, 〈표 Ⅳ-8〉)'에 따르면, 2018년 러시아의 사이버역량은 전체 26위로 세계 2위인 미국과 상당한 격차가 있다.

---

247) 김상배, "제4장 버추얼 창 공격의 복합지정학," 『사이버안보의 세계정치와 한국; 버추얼 창과 그물망 방패』, pp. 127~128.

248) 중국의 사이버 범죄/테러와 관련된 움직임이 지속하여 포착된 데 비해 러시아가 잘 포착되지 않는 것을 이를 증명하는 것이라는 평가도 있다. 신범식, "러시아의 사이버안보 전략," p. 140.

〈표 Ⅳ-8〉 2018년 ITU 세계사이버안보지수(Global Cybersecurity Index)[249]

국명	GCI 지수	법제	기술	조직	역량 구축	협력	순위
미국	0.926	0.2	0.184	0.2	0.191	0.151	2
러시아	0.836	0.197	0.162	0.177	0.166	0.135	26

출처: "2018 글로벌 사이버 시큐리티 인덱스," 〈https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf〉 (검색일: 2019.10.1.). 참고 저자 작성.

GCI 지수의 평가항목 중 러시아는 관련 법제, 기술, 조직, 역량구축, 협력 중 협력과 기술 항목이 비교적 낮은 수준으로 평가된다. 전체적인 역량을 평가하면 평균적인 지수가 낮게 나올 수 있다. 하지만, 실제로 러시아가 사이버군 창설을 비롯해 국제사회에서 보여준 사이버 공격 수행사례 등을 볼 때, 이미 미국에 버금가는 사이버 역량을 보유하고 있다는 평가를 받는다. 따라서, 사이버 영역에서 조직적인 체계를 갖추고 실제 활용하고 있다는 것은 러시아의 사이버역량이 지속해서 발전하고 있다는 방증이며, 이를 부정할 수는 없을 것이다.

다. 사이버 국제협력

러시아는 기본적으로 사이버안보와 관련한 국제협력의 주요 대상국으로 중국을 설정하고 있다. 이는 러시아 역시 중국과 마찬가지로 국제사회에서 국가 간의 협력에 대해 여타 국가들과 서로 다른 생각을 하고 있기 때문이다. 〈표 Ⅳ-9〉

249) 한국은 0.873으로 세계 15위, 북한은 0.020으로 세계 171위, 반면 중국은 0.828로 세계 27위를 기록했다. ITU, Global Cybersecurity Index, 2018, 〈https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf〉 (검색일: 2019.10.18.).

〈표 Ⅳ-9〉 러시아와 서방국가 비교[250]

	러시아 중심 SCO 진영	미국 중심 서방 진영
정보/ 사이버 안보 개념	정보기반시설과 정보 자체 등 국가안보 강조	정보의 자유로운 유통과 표현의 자유를 중시하며 정보 자체가 아닌 정보통신기반시설과 네트워크 보안에 집중
주요안건	범죄, 테러, 정보의 정치적·군사적 사용	인터넷 자유, 경제 협력, 지적 재산권 등
위협인식	정보 자체가 위협, 정보 무기, 정보전 등은 대량파괴, 인명 살상 무기와 같은 차원에서 논의 가능	범죄 차원의 무기와 국가안보 차원의 위협을 구분
국가 역할	정보공간에서의 국가 주권 강조	정보공간에 대한 민간의 역할 강조
정보공간의 핵심	정보안보(Information Security)	자율성(Autonomy)
Frame	국가 중심주의	초국가주의 / 다중이해당사자주의
국제규범	정보공간에 대한 기존 국제법 및 국제규범 이외의 새로운 국제규범의 필요성 역설	기존 국제법과 국제규범 적용 가능

출처: 장규현·임종인, "국제 사이버보안 협력 현황과 함의: 국제안보와 UN GGE 권고안을 중심으로," 『정보통신방송정책』 제26권 제5호(2014), p.33; 신범식(2017), 위의 글 p. 164를 재정리.

러시아는 SCO 진영의 일원으로 사이버안보의 개념과 주요안건, 위협인식, 국가 역학, 국제규범에 관한 전반적인 부문에서 서방국가들과 다른 태도를 견지하고 있다. 따라서, 국제사회에서 중국을 위시한 SCO 국가 이외에 적극적인 협력의 의지를 찾아보기 힘든 것이 사실이다. 이 때문에 미국을 중심으로 하는 서방국가들과의 대결 구도를 형성하는 것이 어쩌면 당연한 일일 수도 있다. 실제로, 러시아는 국가 중심적 관점에서, 사이버공간의 자유와 정보의 자유로운 흐름을 주장하는 미국의 교리는 패권주의인 미국이 다른 국가를 전복

250) 장규현·임종인, "국제 사이버보안 협력 현황과 함의: 국제안보와 UN GGE 권고안을 중심으로," 『정보통신방송정책』, 제26권 제5호 (2014), p. 33; 신범식, "러시아의 사이버안보 전략," p.164를 재정리.

시키고 그들 자신의 세계관과 가치로 침투하기 위해 사용하는 도구일 뿐이라는 입장이다.[251] 2013년 발표된 러시아의 정보안보에 관한 대표적인 국제정책문건인 '2020년 국제정보안보 정책 기본원칙'에서도 사이버위협을 국가 주권 및 영토적 완전성을 침해하는 행위로, 정보안보 목적을 주권을 침해하는 행위로부터 안정성을 보장하는 것으로 규정하고 있다.[252] 미국이 주장하는 국제사회에서의 사이버 행위 준칙은 러시아에 위협이 되는 행동이라고 보고 중국과의 연대를 통해 미국의 행위 준칙을 거부하고 있다.

두 나라 모두 중앙아시아 지역에서 안정을 도모하기 위해서는 분리주의, 테러주의, 극단주의를 척결해야 할 필요가 있고, 미국 및 서구 국가들의 영향력을 최소화하려는 공동의 이익을 갖고 있다.[253] 물론, 러시아의 이 같은 태도는 전략적인 행보로 볼 수 있으며, 같은 맥락에서 러시아가 지역적/소다자(小多者) 사이버 협력을 시도하고 있다는 점 또한 중요하게 분석해야 할 지점이다. 러시아는 같은 방향성을 가진 국가와의 협력을 강화하기 위해 독립국가연합(CIS), 상하이협력기구(SCO), 집단안보조약기구(CSTO) 등 우호적인 국가 및 국제기구와 국제적 사이버안보 관련 법체계를 구축하려 한다. CSTO 국가와는 정보안보 증진 체제의 구축을 위한 연합 행동 프로그램을 실행하고 있다. 또한, 브릭스(BRICS) 국가와 국제정보안보 협의를 하고, SCO 국가와는 협약을 체결하는 등 사이버 영역에서 발생하는 테러나 인터넷 통신망 해킹 문제를 논의하며 정부 간 협력을 적극적으로 확대하고 있다. 일례로, 러시아는 2015년 열린

---

251) Julien Nocetti, "Contest and conquest: Russia and gloabal internet governance," *international affairs*, vol. 91, no. 1 (2015), p. 115.

252) 김상배, 버추얼 창 공격의 복합지정학," 『사이버 안보의 세계정치와 한국; 버추얼 창과 그물망 방패』, p. 346.

253) 문수언, "상하이 협력기구(SCO)를 통하여 본 러시아와 중국 관계 : 러시아의 우려와 대응", 『사회과학 논총』, 13호 (2011), p. 14.

BRICS 및 SOC 정상회의에서 국제정보보안협약(Convention on International Information Security)을 제안하였고, 이후 좀 더 범위를 넓혀 유럽안보협력기구(OSCE)나 아세안지역안보포럼(ARF)의 사이버안보 관련 협의에도 적극적으로 참여하고 있다.[254]

하지만, 러시아는 안보협약의 도입과 UN GGE의 발전, ITU의 역할 강화를 강조하며, 유럽평의회(COE)나 나토 산하 사이버 방위협력센터(CCDCOE)가 주도하는 부다페스트 사이버 범죄협약과 탈린 매뉴얼에 대해서는 반대하고 있다. 이처럼 사이버안보 영역에서 미국을 위시한 서방국가들의 방향성과 러시아의 행보는 명확히 차이가 있어 협력이 이루어지기 쉽지 않은 것이다. 특히, 2016년, NATO가 사이버공간을 군사영역으로 인식함에 따라 러시아는 2020년까지 루넷(RuNet)이 세계 인터넷과 단절될 것이라고 선언했었다(RuNet 2020). 이는 사이버와 정보보안에 대한 현대 국제사회가 군국화되고 사이버상에서 군비경쟁이 시작되었다는 점을 시사한다.[255] 이 같은 상황은 온라인과 오프라인의 경계를 넘나들며 군사적 갈등이 발생할 수 있다는 사실을 보여준다. 결국, 사이버공간에 관한 양국의 인식 차이가 해결되지 않는 이상, 러시아와 서방국가들과의 대립은 불가피한 상황으로 흘러갈 것이 자명하다.

라. 한반도에 대한 함의

러시아는 새로운 안보위협에 대한 국가 차원의 인식 공유와 함께, 변화하는 환경을 활용해 자국의 국익을 극대화하기 위한 노력을 전개해왔다. 러시아는 한국과 이미 사이버안보협의회도 개최하고 있

254) 신범식, "러시아의 사이버안보 전략," pp. 161~162.

255) Mari Ristolainen, "Should 'RuNet 2020'Be Taken Seriously? Contradictory Views about Cyber Security Between Russia and the West," *Journal of information warfare*, vol. 16, no. 4 (2017), p. 8.

다. 사이버공간은 기회의 공간이자 동시에 새로운 위협의 공간으로서 국가들은 이에 적극적으로 대응해 왔다. 사이버공간은 근본적으로 정보의 자유로운 생산·유통·소비를 가능하게 한 정보통신기술의 혁명, 즉 기술적 차원에서 발생한 공간이다. 그러나 기술력의 부족으로 공간의 안정성이 담보되지 않은 상황에서 외부로부터의 정보 유입이 국가안보에 크게 위협되는 사례들이 발생하고 있다. 러시아 역시 이 같은 상황에 예의주시하고 대응책을 마련하고 있다. 따라서, 러시아는 서방국가들과는 다른 정보 주권을 강조하는 방식으로 정보공간을 안보적으로 중요한 공간으로 인식했고, 이 같은 인식에 동의하는 국가들을 중심으로 사이버공간의 질서를 주도적으로 수립하려고 시도하고 있다. 물론, 이 같은 행보의 의도는 자국의 안보는 물론 국익을 실현하기 위한 것이다.

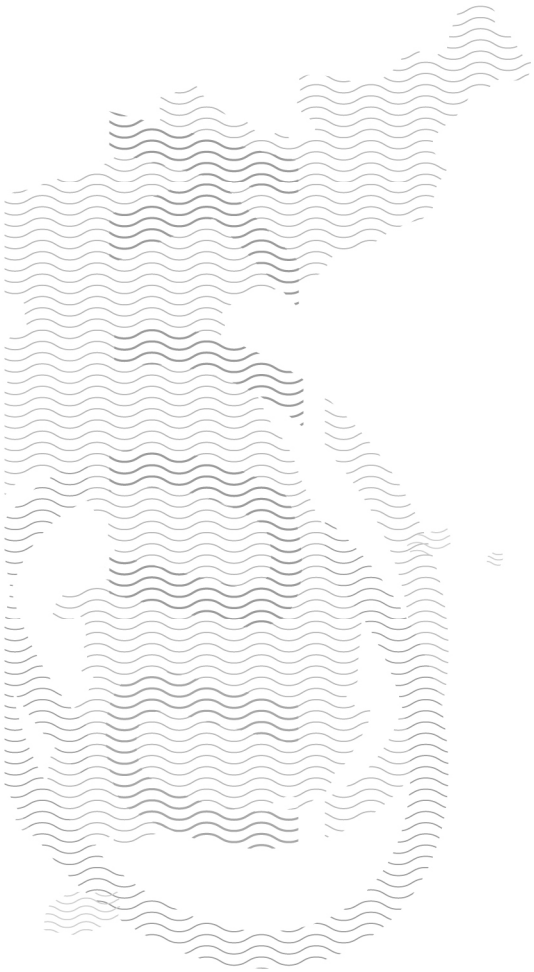
러시아는 사이버공간의 출현에 따른 위협들에 대응하기 위해 적극적으로 체계적인 법·제도 및 정책 추진체계를 구축해 왔다. 한국 역시 '국가 사이버안보 마스터플랜' 수립 이후 본격적으로 사이버안보 역량 강화를 추진하고 있다. 그러나 외부로부터 발생하는 사이버 공격은 지속해서 늘고 있다. '최근 5년간 정부 부처·광역자치단체에 대한 해킹 시도 자료'에 따르면 한국은행에 대한 사이버 공격 횟수는 2015년 38건에서 2018년 767건으로 3년 새 20배 이상 가까이 증가했다. 그중 러시아가 66건으로 두 번째로 많다. 사이버 공격은 출발지 정보제공자(IP)를 위조해 공격할 수가 있어 러시아의 공격이라고 단정할 수 없지만, 러시아를 거치는 경우라도 러시아와의 적극적인 협력이 필요하다.[256] 이 같은 점에서 한국과 러시아가 진행하고 있는 한-러 사이버안보협의회가 갖는 의미는 아주 크다. 한국과 러시

256) "공공금융 노리는 해커들…한은 겨냥 사이버공격 3년새 20배↑," 『연합뉴스』, 2019.10.8., 〈https://www.yna.co.kr/view/AKR20191007170900002?input=1195m〉 (검색일: 2019.10.9.).

아는 국제 사이버안보 환경 평가와 공동으로 대응할 수 있는 영역을 논의하고 더 나아가 러시아가 국제사회와의 협력에서 강조하는 유엔 등 다자협력 기구를 통한 국제무대에서의 사이버 규범, 신뢰구축조치(CBM) 및 역량 강화방안을 협의하고 있다.[257] 이외에도 한국은 사이버워킹그룹 등 사이버 영역의 교류 플랫폼을 활용하여 러시아와의 적극적인 협력과 정보교류를 통해 러시아와 우호적인 관계를 형성하고 사이버공간의 안전을 확보하는 노력을 기울여야 할 것이다.

257) 외교부, 제3차 한-러 사이버안보협의회 개최, 2019.2.1., 〈https://www.mofa.go.kr/www/brd/m_4080/view.do?seq=368978〉 (검색일: 2019.9.28.).

V. 한반도 사이버안보 협력: 전략과 과제



1. 주변국들의 사이버안보 정책 변화에 대한 대응

가. 미국

트럼프 행정부 들어 미국의 사이버안보 정책은 오바마 행정부 시절보다 훨씬 공격적인 성향을 보이고 있다. 대표적인 사례가 2018년 2월 발표된 '핵태세 검토보고서'에 사이버 무기로 미국의 핵심기반 시설을 공격하는 나라에 대해서는 국가안보 차원에서 핵무기로 대응하는 방안까지도 검토하겠다는 내용이 반영된 것이다. 이러한 공세적인 사이버 정책은 최근의 언론보도를 통해서도 확인해 볼 수 있다. NSA 국장이자 사이버사령부(USCYBERCOM) 사령관인 폴 나카소네(Paul Nakasone)는 2019년 4월 열린 어느 포럼에서 미국은 지난 10년간 적국의 사이버 공격에 대해 무기력했지만, 더는 방관하지 않을 것이라고 언급하였고, 6월 23일 미국의 NBC 방송은 전/현직 미국 관리들의 발언을 인용하여 미국의 사이버 부대가 적대국을 상대로 한 비밀 해킹 공격을 확대하고 있으며, 새로운 법적 권한을 부여받은 사이버 부대는 트럼프 행정부 출범 2년 동안 오바마 행정부 8년 동안 보다 더 많은 작전을 수행했음을 전했다.[258] 이러한 사이버상의 작전이 활발히 전개되는 배경에는 사이버사령부(USCYBERCOM)가 2018년 통합사령부로 승격한 점과 2019년 북한, 중국, 러시아 등 사이버안보 위협국에 대한 국가별 맞춤 대응을 위해 사이버안보국이 설치된 것과도 무관치 않을 것이다.

우리 또한 북한으로부터의 사이버 공격이 주된 사이버 위협요인이었던 시기를 지나 최근에는 중국, 러시아로부터의 사이버 공격이

258) 김성권, "미 사이버 부대 '적성국 공격 크게 늘려 트럼프 2년이 오바마 집권 8년보다 많아,"『뉴스투데이』, 2019.6.24., 〈http://www.news2day.co.kr/130313〉 (검색일: 2019.10.2.).

발생하는 등 사이버 공격의 진원지가 다변화되는 상황에 처해 있다. 뿐만 아니라 국가안보에 있어 사이버안보가 차지하는 비중이 점증하고 있는 현실을 감안한다면, 우리 또한 국방 사이버안보 역량을 대폭 강화하고 사이버 공격의 진원지를 특정하여 경제적 제재나 외교적 제재를 가하는 등의 책임부과 억지전략을 도입하는 것도 고려해 볼 수 있을 것이다.

다음으로 트럼프 행정부는 2018년 들어 자국의 민간기업에 대한 중국의 사이버공격이 계속해서 이루어지고 있다는 점을 강도 높게 비난하기 시작하였고, 정보기관인 중국국가안전부(MSS)와 관련이 있는 것으로 추정되는 해커 그룹 APT10과 중국기업을 기소하였다. 뿐만 아니라 국가안보상의 위협을 들어 중국의 통신장비 기업인 화웨이에 대한 제재에 착수하였고, 중국의 특정기업을 정부조달에서 배제할 것임을 결정하였다. 이는 미국 첨단 기술을 둘러싼 중국과의 패권대결을 선언한 것으로도 해석이 가능할 것이다. 이에 대해 영국과 호주, 뉴질랜드, 일본 등 동맹국들이 미국을 따라 화웨이에 대한 제재에 동참할 것임을 선언하고 나선 상황에서 한국 정부는 중국과의 관계악화를 우려하여 전략적 모호성을 내세우기에 바빴다. 이에 대해 미국 국무부 대변인은 한국이 5G 네트워크에 화웨이 통신 장비를 사용할 경우 민감한 정보를 공유하지 않을 것이라고 하여 한국과의 군사안보상의 정보 공유제한도 고려할 수 있다고 언급하며 불쾌감을 감추지 않았다.

안보는 미국, 경제는 중국인 딜레마 상황에서 한국은 어떠한 전략적 선택을 해야 하는가라는 문제는 비단 어제 오늘의 일이 아니며, 그 영역 또한 사이버안보 분야에 국한된 것이 아니다. 미국이 미일동맹을 사이버안보 분야로 확대하여 미래 첨단 전쟁에 대비하는 데 반해 한국이 한미동맹의 영역을 사이버안보 분야로 확장하는 데 대

해 주저하는 것도 이와 같은 맥락에서 해석할 수 있을 것이다. 미중 간의 신냉전이 단기전이 아닌 장기전으로 21세기 내내 고민해야 할 과제임을 고려한다면 성급한 결단이 필요한 사안이 아닌 것임은 명확해 보인다. 단 사이버 군사 영역에서의 협력은 한미동맹의 큰 틀 속에서 추진해 나가되, 사이버 범죄나 테러와 같은 비군사적인 영역에서는 중국과의 협력을 확대해 나가는 투 트랙(two-track) 전략은 참고의 여지가 있어 보인다.[259]

나. 일본[260]

우리는 2020년을 바라보는 이 시각에도 체계적인 사이버안보 추진체계 확립이란 해묵은 과제를 해결하지 못하고 있다. 요컨대 북한의 사이버 공격을 비롯한 국제적 사이버위협이 점증하는 상황임에도 불구하고 여전히 범정부차원의 국가사이버안보 기본법을 마련하지 못한 채 「국가사이버안전관리규정」, 「전자정부법」, 「국가정보화기본법」, 「정보통신기반보호법」 등과 같은 훈령과 분야별 개별법에 의존하고 있는 실정인 것이다. 이로 인해 법률 간 권한 충돌이 발생하고 책임소재 불명확 등의 문제점이 발생하고 있다.[261] 이러한 문제점을 해결코자 국회에서는 수차례에 걸쳐 의원입법 형태의 법안이 발의되었지만, 국가정보원의 위상 및 권한과 관련한 문제에 직면하여 의결에 이르지 못하거나 폐기되었다.[262]

---

259) 이와 관련해서는 한라대 장노순 교수의 발언에서 시사를 얻었다. 김상배 편, 『사이버안보의 국가전략』 (서울: 사회평론, 2017), pp. 363~368.

260) 이 부분은 필자(이상현)의 논문 "일본의 사이버안보 수행체계와 전략," 『국가안보와 전략』, 제19권 1호 (2019), pp. 146~148을 토대로 작성하였다.

261) 김상배, "제10장 사이버전략," 『2018 국가안보전략』 (서울: 국가안보전략원·동아시아연구원, 2017), p. 423.

262) 김도승, "국가 사이버안보의 법적 과제," 『미국헌법연구』, 제28권 2호 (2017), pp. 104~106.

사이버안보기본법 제정과 함께 시급한 과제로 남아 있던 것이 종합적이고 체계적인 국가사이버안보전략을 마련하는 것이었다. 정부는 사이버 대란이 발생할 때마다 「국가 사이버안보 마스터플랜」, 「국가 사이버안보 종합대책」, 「국가 사이버안보 태세 역량 강화방안」 등과 같은 대책을 내놓긴 했지만, 이들 방안들은 국가차원의 중장기적이고 종합적인 사이버전략으로 보기에는 미흡한 것들이었다. 다행히도 문재인 정부는 2019년 4월 사이버안보 기본방침을 제시한 「국가 사이버안보전략」을 그리고 9월에는 청와대, 국정원, 과학기술정보통신부, 외교부, 경찰청, 검찰청 등 중앙 관계 부처 합동으로 보다 구체적인 내용들을 담은 「국가 사이버안보 기본계획」을 발표한 점은 고무적이다.[263]

이러한 맥락에서 봤을 때 Ⅳ장에서 살펴본 일본의 사이버안보 추진체계 확립 과정은 우리에게 많은 점을 시사한다. 먼저 일본의 경우 사이버기본법을 제정하여 사이버안보 추진체계를 법제화한 뒤 범정부차원의 중장기적이고 종합적인 사이버안보전략을 수립한 반면, 문재인 정부는 국가사이버안보법이 국회에서 표류 중인 상황에서 국가사이버안보전략 수립을 우선적으로 추진하였다. 일본의 사례가 우리에게 의미하는 바는 향후 국회에서 논의가 예상되는 국가사이버안보법안에 국가사이버안보전략 관련 규정을 마련하여 이미 마련된 국가사이버안보전략의 법적 기반을 강화할 필요가 있다는 점이다. 다음으로 선진적인 사이버안보 기본법이 단기간에 성립되는 과정에서 일본 의회와 정부가 보여준 모습 또한 우리에게 시사하는 바가 크다. 일본의 여당과 야당은 국가안보가 걸린 문제에 대해서는 초당적으로 대처하여 긴밀히 협력하는 모습을 보여주었고, 중앙 정부 부처들도 긴밀한 의견조율을 통해 기본법이 조속히 실현되는 것에 기여하였다.

263) 관계부처 합동, 『국가 사이버안보 기본계획』.

다음으로 일본의 사이버안보 전략이 한반도 및 동북아 지역에 주는 함의에 대해서도 검토해 보고자 한다. 전수방위 원칙은 전후 일본의 방위정책을 대표하는 기본이념이며, 일본 정부는 사이버 공격에 대한 사이버 방위와 관련해서도 전수방위 원칙이 적용된다는 입장이다. 그러나 2018년 일본 국회에서의 여야 공방을 지켜보면 사이버 공격에 대해서도 전수방위 원칙이 적용된다는 정부의 입장에 반대 의견을 제시하는 의원들이 나오고 있으며,[264] 참고인 자격으로 출석한 사이버안보 전문가 또한 사이버공간에서 전수방위는 성립되지 않는다고 증언하고 있다.[265] 전후 일관되게 지켜 온 전수방위 원칙이 국경을 초월한 사이버 공격의 위협에 직면하여 붕괴될 위기에 처해 있는 것이다.

일본은 2018년 말에 채택된 신(新)방위대장에서 적극적 사이버 방위를 내세워 사이버 공격에 대한 반격권 행사를 인정하였다. 사이버 반격권 용인은 전수방위의 허용한계를 넘어서는 것으로 보일 수 있는 공세적인 대응이며, 주변국의 입장에서 볼 땐 자위대의 군사적 역할 확대와 관련된 민감한 부분이다. 뿐만 아니라, 2016년 이세시마 G7회의에서 사이버 공격에 대한 집단적 자위권 허용을 담은 문서 채택을 주도한 걸로 봤을 때, 일본은 안보환경의 질적 변화에 대응하고 미일동맹을 첨단 군사영역으로 확대·강화한다는 차원에서 사이버 공격에 대한 집단 자위권 추진을 인정하는 방향으로 나아갈 것으로 보인다. 따라서 우리의 입장에서는 사이버 공격과 자위권 발동에 관한 향후 일본 국내의 법적기반 검토과정을 예의 주시해 나가

264) 国会議事録検索システム,「参議院外交防衛委員会議録」第5号, 2018.11.29., 〈http://kokkai.ndl.go.jp/SENTAKU/sangiin/197/0059/19711290059005.pdf〉(검색일: 2019.7.11.).

265) 国会議事録検索システム,「参議院国際経済・外交に関する調査会議録」第1号, 2018.2.7., 〈http://kokkai.ndl.go.jp/SENTAKU/sangiin/196/0188/19602070188001.pdf〉(검색일: 2019.7.21.).

되, 이것이 한반도 및 동북아 안보에 가져올 파장에 대한 검토와 대비가 필요한 시점이라 하겠다.

다. 중국

중국의 사이버 정책 변화는 이전의 기술적인 분야에서 점차 안보적인 차원으로 전이하고 있다. 이는 기술의 진보와 더불어 경제적 영역에서의 역량을 구축하고, 이를 기초로 새로운 영역에서 자국의 영향력을 확대하려는 것과 궤를 같이한다. 시진핑 시기 중국의 사이버안보 관련 정책 변화는 강력한 지도력에 기반을 두어 정책을 시행하는 것과 연관이 있다. 사실, 중국 정부가 정보를 통제하고 사이버 안전에 더욱 치중하려는 의지는 2013년을 전후로 네트워크 안보와 정보화 발전 목표를 강력하게 추진하면서부터 드러나기 시작하였다.[266] 2014년, 시진핑은 당 중앙 사이버 안전 및 정보화 영도 소조(中央網絡安全和信息化領導小組)를 출범시켰다. 시진핑은 "정보화가 중화민족에 천재일우의 기회를 제공한다"라는 것과 "정보화 발전의 역사적 기회를 잡아야 한다"는 것을 강력하게 주장하였다. 더 나아가 사이버공간에서의 선전 활동, 사이버안보 보호, 정보기술의 혁신, 정보화를 통한 경제사회발전, 국민 통합, 사이버공간의 국제 거버넌스를 적극적으로 추진해야 한다는 점을 강조하였다.[267] 또한 "핵심기술은 국가의 보물"이라며 정보의 핵심기술을 통한 자주 혁신의 인터넷 강국 건설을 강조하며 네트워크의 관리 감독을 철저히 하겠다는 의지를 피력하였다.[268]

이 같은 의지는 군사적인 분야에도 투영되어 나타났다. 중국은 군

266) 김상규, "중국의 사이버 안보 정책 변화와 그 함의," p. 56.
267) 위의 글, p. 56.
268) 김상규, "중국의 사이버 안보 정책 변화와 그 함의," pp. 56~57.

사적인 차원에서도 사이버 영역에서의 정책 변화를 꾀하여, 2011년 사이버 공격 부대를 창설하였다. 해당 부대의 목적은 국가안보와 사이버 전쟁에서 공격의 주도권을 강화하는 것이다. 또한, 2015년 12월 전략지원부대를 창설하는데, 해당 부대는 정보, 기술정찰, 전자대항, 사이버 공격 방어, 심리전 등 5대 분야를 포괄하고 있다.[269] 이 같은 일련의 정책 시행은 군사 정보화에 관한 목표를 제시함과 동시에 조직구성을 통해 실제로 구현해가고 있다는 것을 보여준다. 또한 국제사회에서 중국이 나아가야 할 정책 방향성을 제시하는 것이다. 시진핑은 제16차 세계 인터넷 대회에서 "사이버공간은 인류가 함께 활동하는 공간으로 각국이 소통을 강화하고 공감대를 넓혀 협력을 심화시켜 사이버공간 운명공동체를 함께 구축해야 한다"고 주장하였다. 그 구체적인 내용으로는 첫째, 글로벌 네트워크 인프라의 구축 가속화 및 상호소통, 둘째, 온라인 문화교류 공유플랫폼을 건설과 상호감독, 셋째, 사이버 경제의 혁신적인 발전과 공동번영 넷째, 사이버안보 보장과 질서유지, 다섯째, 사이버 거버넌스 시스템 구축과 공평 정의 추구 등이다.[270]

중국은 현재 상하이 협력기구를 중심으로 사이버공간에서의 새로운 규범을 수립해야 한다고 주장하고 있다. 중국은 사이버상에서 유통되는 정치적 담론이나 이념적인 내용에 대한 조처를 중요하게 생각한다. 이 때문에 국제적으로는 사이버공간을 통해 발생할 수 있는 안보적인 이유로 자국 내 안정적인 정권유지를 위해 이를 관철하려고 한다. 그러나 동시에 미국과 중국의 기술격차가 줄어들면서 안보적인 차원이 아닌 경제적인 차원에서의 규범마저도 포괄한다. 중국은 현재 사물인터넷, AI와 빅데이터, 5G 등 중국이 선도하고 있는

269) 김상배 편, "제10장 사이버전략,"『2018 국가안보전략』, p. 237.

270) 新華網, 习近平就共同构建网络空间命运共同体提出5点主张, 2015.12.6., 〈www.xinhuanet.com//world/2015-12/16/c_128536396.htm〉 (검색일 : 2019.10.6.).

영역에서 공격적인 정책을 구현하고 있다. 실생활을 비롯한 산업 전반에 걸쳐 경제적 이익 실현을 넘어 중국의 사이버공간에서의 영향력을 강화해 나가고 있다. 이는 금융 산업에서의 핀테크 외에도 가전, 웨어러블 기기, 자율주행차 등 모든 영역을 망라하고 있다.

이 같은 점에서 중국의 사이버 정책 변화가 우리에게 주는 함의는 더욱 크다. 우선, 국제 차원에서의 함의이다. 지금 사이버공간은 국제사회에서 합의된 규범이 존재하지 않기 때문에 이를 둘러싼 이해당사국의 경쟁은 불가피할 것으로 보인다. 특히, 중국은 현재 최강대국 미국과 여러 면에서 경쟁 구도를 형성하고 있고, 사이버공간을 선점하고 선도할 수 있는 잠재적 패권의 가능성을 놓고 경쟁하고 있다. 향후 중국은 새로운 규범을 형성하는 과정에서 우리에게 중국의 규범을 따르도록 압박을 가할 가능성이 있다. 실제로, 5G 기술 도입 문제로 한 차례 미국과 중국 정부의 압력을 받았던 사례가 있다. 한국은 이제 사이버 영역에서조차 미·중 사이에서 더 많은 선택을 강요당하며 선택의 딜레마에 빠질 수 있다. 따라서, 선제적으로 여러 가능성에 대한 대응 매트릭스를 수립하여 사이버 영역에서의 위기관리 능력을 강화해야 할 것이다.

라. 러시아

러시아는 국가이익을 확대하고 국력을 전 세계적으로 투사하기 위해 노력하고 있다. 특히, 사이버공간을 새로운 전략 공간으로 활용하기 위해 가장 적극적으로 노력하는 국가 중 하나이다. 러시아는 21세기 들어 국가 차원에서 사이버와 관련된 다양한 정책, 전략 및 법제를 수립해 전개하고 있다. 러시아는 사이버공간을 주권이 미치는 전략영역으로 인식하기 때문에 가상공간에서 생성·유통되는 정보에 대한 국가의 영향력을 보장받으려 하고, 대외적으로는 사이버

공간을 국가의 이익과 영향력을 확대하는 수단으로 적극적으로 활용하고 있다. 사이버공간의 급격한 확장은 '국가성' 없는 자율적 정보통신기술의 발달에 의해서였지만, 그것을 관리 혹은 통제의 측면에서 본다면 사실상 미국 등 서방국가들이 주도해 왔다. 따라서, 인터넷 공간이 초국경적 성격을 지녔음에도 불구하고 미국의 영향력을 축소하려는 러시아, 중국 등과 사이버공간에서의 안보 경쟁이 치열할 수밖에 없다.

영토, 영해, 영공, 우주에 이은 소위 제5전장인 사이버공간 역시 그 공간의 주도권을 누가 잡느냐가 핵심이다. 사이버공간은 시공을 초월하고, 다양한 주체들이 은밀하고 자유롭게 활동할 수 있기에 소위 오프라인과 근본적인 차별성을 갖는다.[271] 따라서, 러시아는 정부의 권한을 극대화하여 이 같은 공간의 특성을 통제하여 적극적인 정책의 변화를 통해 새로운 공간에 대한 기회를 활용하려 한다. 따라서 러시아의 사이버공간에서의 새로운 정책 전개 역시 자국의 이익을 극대화하는 방향으로 변화할 것이다.

그렇다면 실제 러시아의 사이버 능력은 어느 수준인가? 미국 헤리티지 재단에서 발표하는 '미국 군사력지수(Index of U.S. Military Strength)'에 따르면, 미국의 사활적 이익에 고위협(high)이 되는 국가는 6개국으로, 러시아는 그중 한 국가이며, 구체적으로 러시아의 사이버 군사 능력이 가공할 만(formidable)하다고 평가하고 있다.

271) 나용우, "초연결융합시대와 사이버안보," 『Journal of North Korea Studies』, 제3권 2호 (고려대 공공정책연구소, 2017), pp. 31~34.

〈그림 Ⅴ-1〉 미국 사활적 이익에 위협을 주는 국가 및 위협 능력

	SEVERE	HIGH	ELEVATED	GUARDED	LOW
Russia		✓			
Iran		✓			
Middle East Terrorism		✓			
Af-Pak Terrorism		✓			
China		✓			
North Korea		✓			
OVERALL		✓			

	FORMIDABLE	GATHERING	CAPABLE	ASPIRATIONAL	MARGINAL
Russia	✓				
Iran		✓			
Middle East Terrorism			✓		
Af-Pak Terrorism			✓		
China	✓				
North Korea		✓			
OVERALL		✓			

출처: Heritage, 2020_Index Of US Military Strength_WEB, 2019.11., pp 11~12, 〈https://www.heritage.org/sites/default/files/2019-11/2020_IndexOfUSMilitaryStrength_WEB.pdf〉 참고하여 저자 재작성

미국은 사이버공간에서 러시아가 미국의 이익을 침해할 가능성과 역량에 대해 부정적으로 판단하고 있다. 실제로, 최근 러시아 내부에서는 사이버 영역에서의 새로운 인식과 정책 설정이 적극적으로 이루어지는 변화의 모습을 찾아볼 수 있다. 특히, 경제적인 영역에서 러시아의 이익 실현을 위한 행보를 보인다. 러시아는 지난 2014년부터 암호화폐를 규제하려 했고, 러시아 재무장관은 암호화폐의 사용부터 발행, 홍보까지 벌금을 부과하는 법안을 발표했다. 2015년, 러시아 정부는 비트코인 관련 웹사이트를 차단했고, 2016년에는 러시

아 재경부가 암호화폐 거래 금지 내용을 담은 법안 추진을 취소했다. 이어 2017년에는 비트코인 거래사이트를 차단·금지하고, 규제 시스템을 정비하려 했다. 그러나, 2018년 초부터 분위기가 반전되었는데, 러시아 정책 추진 기관들이 블록체인 및 암호화폐 관련법을 추진한 것이다. 러시아 정부는 그동안 반대해오던 블록체인 통화인 가상(암호)화폐에 대한 규제를 풀고 법률 제정을 진행했다. 2018년 1월, '디지털 금융자산 법'은 초안이 국회에 제출돼 3월부터 하원 의회에 의해 상정됐다. 결국, 2018년 5월, '디지털 금융자산 법(On digital financial assets)'과 '디지털 권리 법(On digital rights)'이 통과됐다.[272] 집권 여당인 통합러시아당은 정부의 이 같은 의지를 지지하고 있다. 2019년 3월 7일, 러시아 의회는 이 법안을 1차 독회(讀會)에서 찬성 334표, 반대 47표로 통과시켰다.[273] 러시아 정부의 태도 변화의 원인은 경제 상황이 좋지 않은 러시아로서는 블록체인 통화 흐름을 통해 러시아를 향한 서방의 경제제재를 우회할 수 있다는 판단을 한 것으로 보인다. 러시아는 미국을 위시한 서방국가가 러시아에 취하는 경제적 봉쇄 조치에 대응할 여력이 없다. 하지만, 이 같은 러시아의 긍정적인 조처는 새롭게 등장한 사이버공간의 속성을 잘 포착한 것에서 비롯된 것이라 하겠다. 사실, 러시아에 대한 경제제재 조치는 한 가지 목표가 아닌 다음과 같은 복합적인 목표가 존재한다고 볼 수 있다. 첫째, 군사적 능력을 직접 약화하거나 훼손하는 것이다. 둘째, 간접적인 목표로 대상 국가의 경제를 정체시켜 군사력 증대를 막아 군사력을 약화하게 만드는 것이다. 셋째, 무역 및 자본 그리고 금융 거래에 대해 규제를 시행하여 경제적으로 고사시키는 방법이다.[274] 이 세 가지 목적에 대해 우회하여 해결할

272) "러시아 블록체인 업계, 정부 시범사업 지원으로 순항," 『CCTV 뉴스』, (검색일: 2019.12.5.).

273) 위의 글.

수 있다는 전략적 선택이 2019년 4월부터는 블록체인 및 암호화폐 시범 사업을 시작하게 하고, 이를 위해 러시아 경제개발부는 모스크바를 포함한 4개 지역(모스크바, 칼루가, 칼리닌그라드, 페름 크라이)의 SEZ(특별경제구역)에서 스타트업 기업들이 블록체인 및 암호화폐 시스템 구축을 합법적으로 승인받을 수 있는 법도 추진한 것이다.[275]

그러나, 한편으로 이 같은 러시아의 정책 인식과 변화는 국제사회에서 사이버안보와 관련해 협력할 수 있는 여지가 생긴 것으로도 볼 수 있다. 사이버 영역의 금융 시스템을 활용하려는 것은 사이버 테러나 해킹 등에 노출될 위험성이 크기 때문에 국제사회와 공조할 가능성이 크며, 사이버 영역에서 추구하는 국가이익과 맞닿아 있는 것이다. 이 같은 측면에서 볼 때, 러시아 역시 국제사회와의 협력 의지가 존재한다는 방증이며, 필요성은 더욱더 증대될 가능성이 크다. 따라서, 한국 역시 관련 분야에서의 산업과 기술은 물론, 국제사회에서의 제도적 규범 형성에 적극적으로 참여할 수 있는 역량을 강화하고 사이버안보에서 다자적 입장을 견지하여 러시아와의 협력 관계를 강화해야 하는 방향으로 나아가야 할 것이다.

마. 시사점과 대응 방향

이상 살펴본 주변국 사이버안보 정책의 공통적 요소는 첫째, 관련 기관 간 협력체제 개발로 사이버안보가 국가안보 우선과제로 부상

274) 김상원, "경제제재와 러시아 경제의 변화", 한국외국어대학교, 『동유럽 발칸 연구』, 제43권 3호, pp. 155~156.

275) 한국자유총연맹, 학술 세미나 자료, 21세기판 철의 장막, 러시아 인터넷 '루넷(Runet)' 구축, 2019.4.10., 〈https://www.koreaff.or.kr/mybbs/bbs.html?mode=view&bbs_code=pds05&cate=&page=2&search=&keyword=&type=&bbs_no=2442〉(검색일: 2019.10.6.).

한 상황에서 단일부처가 감당할 수 없으므로 관련 기관 간 협력체제 개발을 진행하고 있다는 점이다. 둘째, 사이버 기술 발달을 통한 방어력 증강을 통해 억지력과 안전을 확보하고자 한다는 점이다. 셋째, 민·관 협력 강화로 사이버공간의 민간부문의 몫을 감안할 때 모든 정책결정에 기업, 시민사회, 기술자, 학자 등을 포괄하는 민·관 파트너십이 토대가 되고 있다는 점이다. 넷째, 국제협력 강화로 모든 국가가 국제협력 강화에 중점을 두고 있다는 점이다.

반면 각각의 국가 환경을 반영한 차이점으로 나타난 주변국 사이버안보 정책의 차별적 요소는 첫째, 주권에 대한 고려로 대내적으로는 전략적 차원에서 국방, 방첩 등에 대한 인식수준, 조직화 차원에서 외교, 정보, 군사부문의 협력수준, 운영차원에서 정보기관 참여수준에서의 차이이다. 대외적으로는 사이버공간의 개입방식, 신뢰구축방식에 대한 국제적 논의의 필요성에 대한 인식, 어떤 다자기구와의 협력필요를 언급하느냐, 동맹국 간 정보공유에 대한 입장에서의 차이이다. 둘째, 유연한 정책적 접근으로 일부 국가는 사이버공간의 경제활동을 활성화하기 위해 전략적 유연성을 강조하고 있는 반면 다른 국가는 사이버공간의 빠른 변화속도를 반영하기 위해서 정책적 유연성을 강조하는 차이이다. 셋째, 사이버공간의 경제적 측면의 중요성으로 경제발전을 위한 사이버공간의 중요성에 대해서는 모두 공감하는 가운데 일부 국가는 경제성장에 있어 높은 수준의 사이버안보 필요성을 강조하는 반면 다른 국가는 사이버안보산업 강화를 주요 정책으로 제시하는 차이이다. 넷째, 민관을 망라한 다양한 이해관계자가 포함된 협의체 운용으로 민관협력의 중요성에 대해서는 모두 공감하나 정책결정의 참여형식, 역할범위 등에서의 차이이다.

이상 주변국들의 사이버안보 정책을 검토해본 결과 나타나는 한

국의 대응전략에 있어서의 문제점은 첫째, 국가 안보차원에서의 사이버공격 총괄 대응 체계가 미흡하다는 점이다. 둘째, 새로운 안보 취약 요인들이 등장함에도 새로운 정보통신기술과 이에 적합한 보안기술의 발전이 병행되지 못하여 사이버공격에 대한 기존 방어 체계의 한계가 드러나면서 새로운 정보통신기술이 사이버공격에 노출되는 현상을 초래한다는 점이다. 셋째, 정보보안 의식 개선을 위한 정부차원의 노력이 미흡하여 대국민 홍보 및 교육이 부재하다는 점이다. 넷째, 사이버공격에 대응하는 국제 사이버협력 네트워크와 공조가 미흡하다는 점이다.

이에 따라 한국의 대응전략 방향은 첫째 사이버공간에 대한 안전성을 확보하는 것이 필요하다. 이를 위해 네트워크의 보호와 국가핵심시설의 안정성을 확보해야 한다. 즉 사이버공격에 대한 방어선을 구축하여 정부, 공공기관, 민간부문의 네트워크 취약성을 보완하고 예방능력을 증진한다.[276] 그리고 일원화된 사이버안보 추진 체계를 확립하여 국가 사이버안보 업무의 실질적인 총괄 조정 능력을 확보한다. 국가차원의 원활한 정보보안 사업 추진을 위해 별도의 정보보안 기금을 조성할 수 있는 법적 토대를 마련하고, 국가 사이버안보 대응 핵심 기술 개발을 위해 필요한 기술을 전담 개발할 수 있는 전담 연구 기관을 지정하여 안정적인 예산 지원 및 사업 추진을 한다. 국가 사이버안보 기술개발의 법적근거를 마련하기 위해 사이버안보 기본법을 제정하고 개별법들을 통·폐합한다. 정보통신기술 변화에 따른 사이버공격에 대한 대응을 보다 효과적으로 수행하기 위해 관련법들을 지속적으로 정비한다. 전략적으로 핵심 보안기술을 육성하는 등 사이버안보체계를 강화하고 사이버공격 대응능력을 향상시킬 수 있도록 관련법들을 정비한다.

276) 채재병, "안보환경의 변화와 사이버안보," p. 189.

둘째, 사이버공격에 대한 억지력을 확보하는 것이 필요하다. 사이버공격 능력 확보 및 공격 의지 무력화, 국제 공조 강화를 통해 사이버 억지력을 확보해야 한다. 이를 위해 사이버 방어능력을 강화하고 선제적 사이버 방어체제를 구축한다. 사이버공격 대응체계를 사전 예방 중심으로 전환하고, 사이버공격 수단이 다양화하는 데 따른 방어수단과 반격수단의 개발, 즉 공격능력 개발을 위한 사이버공격무기 개발, 사이버공격 대응기술 개발 등에 중점을 둔다. 국가 기능 혼란 및 마비를 목표로 지속적인 공격이 발생하는 환경에 따른 대응체계의 변화가 필요하다. 수동적 방어 형태에서 벗어나 선제적·적극적 방어로 전환할 필요가 있다. 현재까지 수행하고 있는 수세적 방어 전략으로는 진화하고 있는 공격 기술에 적절한 대응이 불가능하다. 기존 방어 중심에서 사이버공격 정보의 적극적 수집과 위해세력 적발 시스템 및 자원 무력화를 포함한 총괄 대응 체계를 확립한다. 미래 정보통신기술에서 필요한 정보보안 기술을 조기에 확보한다. 즉 미래 정보통신기술을 예측하고 보안취약점을 사전에 식별하여 이를 차단하기 위한 정보보안 기술의 조기 확보를 추진한다.

셋째, 정보보안 정책의 성공적 추진을 위한 사이버안보 기반을 조성하는 것이 필요하다. 국가·공공기관 사이버안보 의식을 강화하고 대국민 홍보를 통해 사회전반에 사이버안보 의식을 고취시켜야 한다. 국가 사이버안보는 전 국민의 사이버안보 의식에서 출발한다는 점에서 전 국민을 대상으로 하는 다양한 교육 및 홍보 프로그램을 개발하고, 사이버안보 의식 확산, 대국민 사이버안보 인식 및 저변 확대를 위해 정부 및 공공기관, 민간기업, 국민 등을 대상으로 사이버안보 의식 제고와 실천 활동을 강화한다. 상시 사이버공격 대응능력 강화 훈련을 실시하면서 민·관·군 합동 훈련의 정례화 및 체계화를 추진하고 실전적 훈련 프로그램으로 사이버안보 방위 훈련

의 실효성을 강화한다. 민·관·군 협력시스템을 강화하여 사이버안보 개념에 대한 인식 공유와 민·관·군 역할 정립을 통해 공동체 개념의 유기적 협력체제로 발전시킨다. 사이버공격과 관련된 이슈들과 각 기관별 시스템을 통합할 수 있는 국가차원의 정보공유 시스템을 구축하여 민·관·군 합동대응체계를 정립한다. 민·관·군 합동대응체계에 있어서 정보공유 개선은 효과적인 사이버안보의 핵심 요소이다. 사이버공격 대응을 위한 유관기관 통합훈련을 내실화하고 활성화한다. 유사시 사이버예비군으로 사용할 수 있는 사이버안보 전문 인력을 양성한다. 국가 사이버안보 강화를 위한 정보보안 핵심인재 양성 프로그램을 개발 및 시행함으로써 화이트해커 등 사이버안보 관련 인재육성을 강화한다. 사이버안보 인력 양성에 집중 투자하고 사이버안보 전문가 교육·양성 프로그램을 개발·지원한다.

넷째, 국제 사이버협력 네트워크를 확충하는 것이 필요하다. 이를 위해서 국제 사이버정보 공유체계를 구축하고, 사이버안보 국제규범화 및 국제 거버넌스에 주도적으로 참여할 필요가 있다.[277] 다만 국제규범 및 국제 거버넌스의 참여는 상이한 관점과 국가이익의 충돌이 존재하므로 각기 사안별로 별개의 차원에서 접근할 필요가 있다. 주요 국가들과 양자 및 다자간 사이버협력 확대 및 정보공유체계를 구축한다. 국제적 사이버공격 대응 합동훈련에 적극적으로 참여하고 활성화한다. 그리고 국제 사이버정보 공유체계를 통해 동맹국 간 정보교류를 활성화하고 이를 확대 발전시켜 우방국과의 사이버 동맹체제를 구축한다. 또한 정보 공유체계를 주변국으로 확대시켜 국제 사이버안보 공조체제를 구축, 강화한다. 전 세계적 사이버공격 피해 확산의 신속하고 효율적 대응을 위한 실무 중심의 국제적 협력관계를 주도하고 정보 획득력 및 글로벌 사이버안보 의사결정

277) 채재병, "안보환경의 변화와 사이버안보." p. 190.

에 대한 영향력 강화로 국제적 위상을 제고한다. 공공·민간분야 공조 강화 및 사이버 분야 중재자로서 국제협력을 확대한다. 이를 위해 사이버보안 취약 국가들에 대한 지원을 위해 사이버 공적개발원조를 시행한다. 사이버 후발국들을 견인함으로써 사이버안보 국제규범화에도 기여할 수 있을 것이다. 사이버안보는 기술의 우위에 따라 많이 좌우된다는 특성상 기술 후진국에 대한 기술적, 물적 지원이 필요하다. 네트워크로 연결된 상태에서 취약국의 안보수준 유지가 타국에 미치는 영향을 고려한다면 장기적으로 모든 조약 당사국이 일정 수준 이상의 기술적, 물적 수준을 유지할 필요가 있다. 이러한 지원은 정보통신기술 선·후진국 간의 정보격차를 줄이는데 기여하고 국제사이버공간 주도권 확보에도 도움이 될 것이다.

2. 한반도 사이버 평화체제

가. 사이버공간의 남북협력과 사이버 평화

오늘날 정보통신 기술의 발전에 따라 사이버공간이 전 세계적으로 확대되면서 국가안보 영역에서 사이버공간의 중요성이 더욱 중요해지고 있다. 사이버안보 위협은 비전통적 안보위협요인 중 가장 심각한 것으로 대두되고 있으며, 전력, 교통, 국방, 금융 등 사회기반시설의 정보통신기술과 통신망에 대한 의존도 증가는 사이버안보에 대한 중요성을 더욱 증대시키고 있다. 오늘날 사이버위협이 국가에 의해 주도되면서 사이버공간에 대한 중요성이 증대되고 있고, 국가안보 차원에서 사이버안보에 접근하려는 움직임이 강화되고 있다.

전 세계적인 정보통신기술 강국인 한국은 정보화의 진전에 따라 풍요로운 삶을 누려왔지만, 정보화가 진전될수록 사이버 공격에 노

출되기 쉬운 역기능도 역시 증가하고 있다. 한국에 대한 사이버 공격은 민간 차원뿐만 아니라 공공시설과 국가기관, 그리고 정당과 언론사 등 전 분야에 걸쳐 이루어지고 있다. 정보통신 강국임과 동시에 사이버 공격의 주요 대상 국가라는 역설적 사실은 우리에게 사이버 안보의 중요성을 다시 한 번 일깨워주고 있다.

우리는 남북 분단이라는 특수한 상황으로 인해 매우 강력한 사이버 전력을 가지고 있는 북한과 대치하고 있다. 그동안 북한은 우리의 사이버공간에 대해 수많은 공격들을 진행하여 왔다. 그러나 북한의 사이버공간 폐쇄성과 남북 간 정보화 수준의 격차로 우리의 대북 사이버 공격은 현실적으로 어려울 뿐만 아니라 설사 공격이 성공하더라도 상대적으로 약한 타격만이 가능할 뿐이다. 또한, 사이버공간을 둘러싼 한반도 주변국들의 다툼은 우리나라의 사이버공간에 대한 위험을 증가시키고 있다.

우리의 사이버공간에 대한 공격은 국가안보와 국익차원에서 중대한 위험과 막대한 손해를 발생시키고 있으며, 그동안 우리 정부는 한국의 사이버공간을 안전하게 지키기 위해 「국가사이버위기 종합대책(2009)」, 「국가사이버안보 마스터플랜(2011)」, 「국가사이버안보 종합대책(2013)」 등을 마련하여 왔다. 그리고 2019년 4월에는 국가차원에서 최초로 「국가사이버안보전략」의 수립·시행하고 있으며, 그 후속조치로 9월에 「국가 사이버안보 기본계획」을 수립·발표함으로써 구체적인 실행방안을 마련하고 있다.

「국가사이버안보전략」과 「국가 사이버안보 기본계획」은 우리의 사이버공간에 대한 위협을 효과적으로 방어할 수 있는 포괄적·종합적 계획이라고 볼 수 있다. 그러나 국경 없는 사이버공간의 특성을 고려할 때, 안보적 시각에 초점을 맞춘 사이버 전략이 '최선의 선택'일 수는 있지만 '최고의 선택'으로 보기는 어렵다.

사이버안보전략은 결국 사이버공간의 평화를 달성하는 것을 최종 목표로 하고 있다고 볼 수 있다.[278] 사이버안보의 목표가 사이버 평화이고, 사이버안보와 사이버 평화가 하나의 연속체라는 시각은 양자의 통합적이고 균형적인 접근의 아이디어를 제공하고 있다.[279] 사이버 평화의 시각에서 본다면 한반도의 사이버공간에 대한 평화가 우리의 국가사이버안보전략 목표가 될 것이다.

한반도는 2018년 「9월 평양공동선언」과 「9·19 군사합의서」를 통해 물리적 공간에서는 사실상의 남북불가침협정이자 실질적인 종전선언을 체결한 것으로 볼 수 있다. 군사합의서에 기반하여 2018년 11월 1일자로 한반도의 지상, 해상, 공중 모든 영역에서 적대행위가 중지되고 있으며, 초보적 단계의 운용적 군비통제가 시행되고 있다. 향후 남북 간 군사적 신뢰구축과 운용적 군비통제가 구조적 군비통제로 나아간다면 물리적 공간에서의 한반도 평화가 멀지 않아 우리 앞에 다가올 것으로 기대된다.

한반도의 물리적 공간과는 달리 사이버공간에서는 아직도 평화의 움직임은 보이지 않고 있다. 사이버공간에 대한 북한의 위협은 여전히 진행형이며, 당국 간 남북대화와 민간 차원의 교류협력 어느 곳에서도 사이버 평화에 대한 논의는 찾아보기 어렵다. 물론 북한의 사이버 공격에 대한 불인정[280]과 사이버공간의 문제가 남북 간 안보이슈로 등장한 시기가 오래되지 않았다는 점을 고려할 때 남북대화의 주제로 논의하기에는 시기상조라고도 볼 수 있다. 그러나 북한

278) Heather M. Roff, C*yber Peace: Cybersecurity Through the Lens of Positive Peace* (Washington, D.C.: New America, 2016), p. 10.

279) 정영애, "사이버 위협과 사이버안보화의 문제, 그리고 적극적 사이버 평화," p. 121.

280) "또 다시 북 해킹설 유포, 무엇을 노린 것인가," 『우리민족끼리』, 2015.8.14. 북한은 국내 한 대학병원 전산망 해킹이 '북한 소행'이라는 경찰청 발표에 "참을 수 없는 모독이고 엄중한 정치적 도발"이라고 반발하면서, 과거 농협 해킹 사건이나 언론사 및 금융기관에 대한 대규모 해킹 사건 역시 북한이 저지른 것이 아니라고 주장했다.

의 사이버 공격으로 인한 우리의 국익 훼손이 증가하고 있고, 최근 한반도의 평화 분위기가 무르익어감을 고려할 때 사이버공간에서의 '평화'를 논의하는 시점은 오히려 지금이 최적기라고 볼 수 있다.

사이버공간의 공격과 방어의 비대칭성과 우리나라에 비해 사이버 전력을 비대칭적 전력으로 운용하는 북한을 고려할 때, 남북 간 한반도 사이버공간에 대한 평화협정 또는 불가침협정 체결은 반드시 필요하다. 남북의 사이버안보협력은 '사이버공격을 통한 적대행위 금지 협약 체결'(사이버 평화협정)과 사이버안보 기술 공동연구 및 개발 등 크게 두 가지 방향에서 추진할 수 있다.[281] 남북 사이버 평화협정이 체결된다면 최소한 우리의 사이버공간에 대한 북한발 공격은 사라지거나 최소한에 그칠 것이며, 북한의 사이버공격을 억제하는 효과를 가져올 것이다. 그리고 사이버안보와 관련된 기술의 공동연구 및 개발이 이루어진다면 사이버공간에서의 남북협력이 이루어지는 효과를 가져올 것이며, 이는 한반도 사이버공간의 안전과 사이버를 통한 평화번영의 길로 나아갈 수 있는 토대를 제공할 것이다.

우리의 사이버안보 전략을 완성하기 위한 퍼즐의 완성은 한반도의 사이버공간에 대한 평화적 이용을 보장하는 '남북 사이버평화협정'이 될 것이다. 남북은 물리적 공간에서의 평화정착과 함께 사이버공간에서의 적대적 행위를 중지하고 평화적 이용을 통해 한반도 평화번영을 달성하기 위한 노력을 시작하여야 할 것이다.

나. 한반도 사이버 평화체제

한반도 평화체제는 남북한을 비롯한 관련국 상호 간에 공식적으로 전쟁상태를 종식시킴으로써 법적·제도적 및 실질적으로 한반도

281) 김호홍·오일석, "신안보 분야 남북협력 추진전략," 『신안보연구』, 통권 193호 (2018), p. 57.

에 공고한 평화가 보장되어 있는 상태를 의미한다.[282] 이에 따라 한반도 평화체제는 한반도의 평화를 확고히 하는 하나의 안보 레짐으로 규정되기도 한다. 이에 따라 한반도 사이버 평화체제는 기존에 논의되고 있는 한반도 평화체제의 부분 또는 확장이라는 측면에서 접근하고 있다. 즉 한반도 평화체제를 위한 사이버공간 차원에서의 안보 레짐을 의미한다. 따라서 한반도 사이버 평화체제는 사이버공간에서의 한반도 평화를 보장하는 사이버안보 레짐을 형성하는 국내외적 법적, 제도적 장치들과 거버넌스로 구성된다. 특히 사이버공간에서의 거버넌스 구축을 위한 국제적인 협력과 국제규범의 형성에 방점이 주어진다.

이는 사이버공간에서 구조적 평화체제를 구축하기 위한 노력이기도 하다. 즉, 사이버상의 인권과 경제적 이득 향유 등, 인간안보 측면에서 사이버안보 구축 방안인 것이다. 미래지향적 사이버안보 방안은 사이버공간의 각 주체들이 자유와 상호이익을 창출할 수 있는 자율적 통제체제를 통해 사이버위협을 최소화해야 한다. 이는 요한 갈퉁(Johan Galtung)이 말한 '적극적 평화(positive peace)' 구조의 구축을 통한 '평화구축(peacebuilding)'이라고 할 수 있다.[283] 이에 한국도 법·제도적 추진체계의 개선과 국내적 차원을 넘어서는 글로벌 거버넌스의 구축, 즉 사이버공간의 창의적이고 효과적인 국제규범과 국제레짐을 창출해야 할 필요가 있는 것이다.

한반도 사이버 평화체제의 의미를 구체적으로 확인해보기 위해서 우선 한반도를 둘러싼 사이버공간 실태에 대한 검토와 한반도 사이버 평화체제 구축을 위한 방안들을 살펴볼 필요가 있다. 한반도 사이

282) 외교부, 「한반도평화체제」, 〈http://www.mofa.go.kr/www/wpge/m_3982/contents.do〉 (검색일: 2019.10.11.).

283) 요한 갈퉁 지음, 이재봉 외 옮김, 『평화적 수단에 의한 평화』 (서울: 들녘, 2000). p. 200.

버 평화체제와 관련된 거버넌스 구축을 위한 국제협력과 국제규범 형성은 국제, 지역, 개별국가 차원에서의 국제공조를 통해 이루어지고 있다.

사이버안보 레짐 형성과 관련된 국제, 지역, 개별국가 차원에서의 국제공조를 살펴보면, 국제사회의 사이버안보 관련 국제공조 논의는 국제연합(UN), 경제협력개발기구(OECD), G8, 국제형사경찰기구(INTERPOL) 등 국제기구와 국제협의체를 중심으로 진행되고 있다. UN은 국제사회에서의 국제공조 논의를 주도하고 있으며, 국제전기통신연합(ITU), UN군축사무소(UN Office of Disarmament), UN 정부전문가그룹(GGE), UN 마약·범죄사무소(UN Office of Drug and Crimes) 등이 중심이다. 국제연합(UN) 이외의 국제공조는 경제협력개발기구(OECD)와 G8(Group of Eight)을 중심으로 추진되고 있다. 사이버안보 관련 지역별 공조는 지역 국제기구들을 중심으로 진행되고 있으며, 지역 기구와 지역안보협력기구의 두 차원에서 진행되고 있다. 지역기구는 유럽연합(EU), 동남아국가연합(ASEAN), APEC 등이 있으며, 지역안보협력기구로는 북대서양조약기구(NATO), 유럽안보협력기구(OSCE) 등이 대표적이다. 개별국가 간 양자 협력은 사이버 관련 이슈 중 하나로 사이버안보를 다루고 있다. 국가 차원의 협력 이외에도 민간 차원의 다자간 국제 협력 역시 중요한 역할을 수행하고 있다.

사이버안보 국제공조는 주로 정보통신기술과 사이버범죄 등 세부적 차원에 국한되어 국가안보 차원에서 사이버안보 문제를 포괄하지 못하는 한계를 보여주고 있다. 사이버안보 협력은 세계적 수준 보다는 지역적 차원 또는 개별국가 차원의 양자·다자관계에서 용이하다. 그러나 아태지역은 유럽과는 달리 사이버안보에 대한 공감대 형성이 저조하며 특히 동북아의 경우 국가 간 국제공조가 부족한 실정이다.

국제사회의 사이버안보 대립은 사이버 국제규범, 인터넷 거버넌스, 다자간 협력 모델 등을 중심으로, 미국·유럽 진영 vs 중국·러시아 등의 후발국가로 대별할 수 있다. 사이버안보 국제규범 형성을 둘러싼 대립은 미국과 유럽 중심의 '사이버범죄협약(부다페스트 협약)'과 러시아와 중국 중심의 '국제정보보안조약(안)' 등이 대립하고 있다. 양 진영은 정치적 타협을 통해 UN 'GGE 권고안(2013)'에서 사이버안보와 관련된 큰 틀에서의 원칙에 합의했으나, 세부적 분야의 적용문제와 관련하여 진영 간 갈등이 재발될 가능성이 상존하고 있다.

인터넷 거버넌스의 주체를 국제인터넷주소관리(ICANN)로 할 것인지, 아니면 국제사회의 모두가 동의할 수 있는 새로운 주체로 바꿀 것인지에 대해 각 국가들은 양분된 입장을 보이고 있다. 미국은 '국제인터넷주소관리'의 국제적 성격을 들어 현 체제 유지 입장인 반면, 러시아 및 중국 등 기타 국가들은 국제적인 합의에 의한 새로운 인터넷 거버넌스 구축을 주장하고 있다.

서방 진영 국가들의 사이버공간에 대한 논의는 다양한 이해관계 당사자들이 참여하는 '다자간 협력 모델'을 주장하고 있다. ICT 개발도상국이나 기타 국가들은 서방 진영의 국가와 기업이 주도하는 사이버공간 선점에 대해 우려를 표명하면서, 개발도상국들의 입장을 충분히 반영하지 않은 방안이라고 비판한다.

사이버 범죄 대응책 마련 및 처벌 대책과 관련하여 기존 국제법 적용 vs 신규 국제규범 창출의 두 입장으로 대별되고 있다. 기존의 국제법 체제를 적용하자는 서방 진영 국가들은 사이버범죄협약의 이행 확대를 주장하나, 중국과 러시아를 비롯한 일부 비서방 진영 국가들은 새로운 국제법의 설립과 적용을 주장하고 있다.

현재 한국은 국제-지역-개별 국가 차원에서 다양한 사이버안보

국제공조를 추진하고 있으나, 포괄적·중장기적 전략 및 방안 제시에는 미흡한 실정이다. 특히 한반도 주변국의 사이버공간 주도권 다툼, 북한의 대남 사이버공격 지속 등 한국의 안보상황과 경제·사회적 특수성 등을 고려하는 국제공조 방안 제시가 필요하다. 사이버안보 분야에서 국제기구 및 국제협의체, 지역협력기구, 개별 국가들과의 양자·다자간 공조를 병행하고, 국제공조는 양자·다자간 협력을 중심으로 지역수준, 세계수준을 병행하는 방향으로 추진해야 한다. 국제사회 논의도 GGE를 중심으로 참여하되 다양한 채널 협의를 지속해야 한다.

한반도 사이버 평화체제를 위한 기본 전략으로 국제사회와의 다양한 협력을 통해 사이버안보 국제협력 네트워크를 형성하고 리더십을 구축하고, 북한을 비롯한 사이버 도발을 자행하는 불량국가들의 불법행위를 국제사회 공동문제로 이슈화하고, 외교, 군사, 경제 등 국제공조를 통한 국제사회의 광범위한 제재 조치를 유도하는 것이다. 이를 위해서는 국제 사이버안보 파트너십을 강화해야 하는데, 첫째, 다른 나라나 국제기구 등 국제사회와의 다양한 협력방안 강구하고, 둘째, 사이버도발 억지력을 확보하기 위하여 미국, 일본을 비롯한 우방국들 및 중국, 러시아 등과 다자양자 간 국제협력 강화하고, 셋째, 후발국들에 대해 사이버 선도국가로서의 역할을 수행하며, 중립적이고 보편타당한 사이버안보 국제규범 수립을 지원해야 한다.

한반도 사이버 평화체제 구축을 위한 추진전략으로 첫째 글로벌 국제공조 차원에서 사이버안보 국제공조 확대·강화를 위해 UN GGE, ITU 전권회의, 세계 사이버 스페이스 총회 등 사이버안보 분야의 국제 거버넌스에 적극 참여한다. 기존 사이버안보 국제규범인 사이버범죄조약과 국제정보보안조약안의 참여는 유보적 태도의 중간자적 입장을 견지하는 가운데, 오히려 새로운 국제규범 창출 노력

에 관심을 기울이는 것이 바람직하다. UN GGE를 통한 사이버안보 국제규범 수립에 적극적인 참여를 지속적으로 추진하되, 사이버 분야의 역량 강화 지원을 우리의 선도적 역할을 확장, 사이버공간에서의 국제위법행위에 대한 국가책임, 사이버공격 발발 시 협력적 대응조치와 같은 사안들에 대한 논의를 중심으로 추진한다. 신규 국제규범 창출은 사이버공간의 핵심적 공통사항에 대한 국제사회의 공감대 형성으로부터 출발하여, 양자적 협력 → 국제적 공론화 → 다자적 협의체와 전담기구 구성 → 국제규범 정립 등의 순으로 단계적으로 추진한다. 주요 국가 간 양자 사이버 협력 및 국제기구 등과의 다자간 사이버 협력을 의미하는 '국제사이버 정보공유 체계'를 구축하여 동맹국간 정보교류를 활성화하고 이를 확대 발전시켜 우방국과의 '사이버 동맹체제'를 구축하고 사이버안보 관련 정보를 공유하여 향후 국제 사이버 정보의 '허브' 역할을 수행한다.

둘째, 동북아 지역 공조 차원에서 동북아 지역의 기존 사이버안보 국제공조 노력들은 외교적 차원의 접근이거나 기술적·사법공조 차원 분야에서 추진되었으며, ASEAN, ARF, SCO 등은 사이버안보 협력을 위한 포괄적인 기구로서는 적합하지 않다. 동북아 사이버안보 확보를 위해서는 양자협력보다는 다자가 참여하는 지역안보협의체가 효과적이며, 정책적 측면에서는 유럽네트워크보안청, 군사적 측면에서는 북대서양조약기구, 외교적 측면에서는 유럽안보협력기구의 활동을 벤치마킹하여 추진한다. 아세안+3, APEC, ARF 등 우리가 주도적으로 참여하고 있는 국제협력체를 중심으로 동북아의 집단적 사이버안보체제 구축을 추진한다. 나아가 한·중·일 사이버정책협의회에 미국, 러시아, 북한을 참여시켜 동북아의 사이버안보협력체로 발전시킨다.

셋째, 양자 및 다자 공조 차원에서 사이버안보 주요 관련국들인

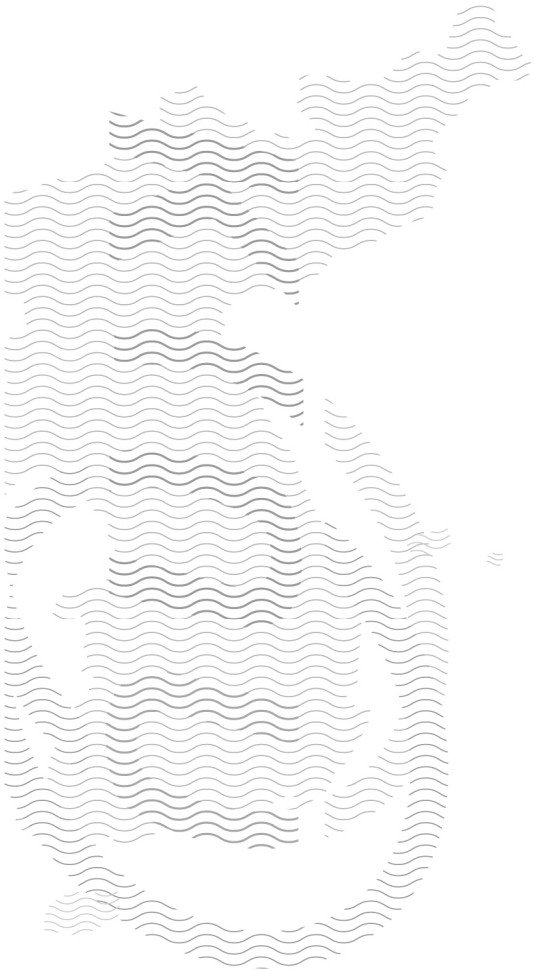
미국, 일본, 중국, 러시아 등을 비롯한 그 외의 다양한 국가들과 양자 또는 다자간 협력을 추진한다. 미국과는 동맹에 기반한 공조강화, 일본과는 정보협력 강화, 중국·러시아와는 신뢰구축 조치 형성 등을 추진한다. 한미 사이버 공조는 다른 분야의 동맹 수준으로 까지 강화할 필요성이 있으며 사이버 안보 핫라인 개설과 사이버 정보협의체 추진 등을 중점 추진한다. 한일 사이버 분야 정보협력 강화는 사이버정책협의체를 추진하고, 나아가, '한일 공동사이버센터'를 운영을 통해 정보인증 기준 정립과 공동 연구개발을 추진한다. 한일 '사이버분야 정보협력'을 통한 '한일 군사정보포괄협정'을 추진하되, 전반적인 한일 관계와 국민정서를 반영하여 추진한다. 한미일 군사정보공유협정에서 규정하고 있는 핵·미사일 정보공유에 사이버안보 분야를 추가하고, 향후 군사정보공유협정을 포괄적인 한미일 정보공동체로 발전시킨다. 한중·한러 사이버협력은 사이버 고위급 정책결정자들과의 핫라인 및 통신채널 확보를 추진 등 '신뢰구축조치(CBMs)' 형성을 중심으로 추진한다. 한중 사이버공조는 향후 사이버정책협의회를 발전시켜 사이버공조를 강화하고 사이버협력의 분야를 범죄·기술 분야를 넘어 안보분야로 확대시킨다. 한러 사이버공조는 러시아가 미중 양극체제를 다극체제로 변화시킬 수 전략적 가치를 고려, 전자정부나 민간분야 정보보안의 프로세스와 서비스와 같은 분야를 중심으로 추진한다. 러시아는 사이버전과는 달리 정부와 민간부분의 정보통신 및 정보보호관리체계가 낙후되어 있는 점을 고려한다.

넷째, 북한의 사이버 공격 억지를 위한 국제공조 차원에서 국제사회의 사이버안보 거버넌스에서 북한을 비롯한 사이버 불량국가들의 도발행위를 국제사회 공동문제로 이슈화, 외교·군사·경제 등 국제공조를 통한 국제사회의 광범위한 제재 조치를 유도한다. 사이버규

범 개발에 적극 참여하여 북한의 사이버공격에 대해 규제할 수 있는 원칙을 마련하되, 국제규범 형성 전까지는 국제전쟁법, 유엔헌장, 국가책임법 등의 국제법 적용에 대한 국제적 합의를 도출한다. 북한은 국제사이버 규범형성의 논의의 장으로 유도하여 사이버 공격의 억지 효과를 유도한다. 북한의 사이버공격에 대해 동북아안보협의체 또는 사이버안보 협의체에서 의제로 추진함으로써, 북한의 사이버 공격에 대해 방관하고 있는 중국의 견제효과도 얻을 수 있다. 나아가, 사이버 수사공조 및 협력을 추진하여 북한을 중국으로부터 분리시키는 외교적 노력도 병행한다.

다섯째, 국제협력을 위한 국내 법·제도 정비 차원에서 사이버 관련 법령을 보완하여 사이버업무수행체계를 지속적으로 정비하고, 국가 사이버안보 정책 의사결정의 일원화를 추진한다. 한반도 사이버 평화체제 구축에 주도적으로 나서기 위해서는 우리의 입장을 제대로 반영하는 사이버안보 원칙을 마련하여 다른 국가들을 설득할 수 있는 능력이 필요하다. 국가사이버안보전략 수립 이후 추진과제들을 통해 사이버안보에 대한 일관되고 체계적인 대응 논리나 외교전략을 추진한다. 사이버공격에 대처하기 위한 정부기관 상호 간의 통제와 조정이라는 기본법적 성격을 갖는 '국가사이버기본법'을 제정한다. 이를 통해 사이버안보 주무기관 설치, 사이버 공격 대응방안 등을 포함하며, 방어와 공격 양 측면을 모두 고려하여 동맹국, 민간, 학계, 시민사회 등과의 협력을 명문화한다.

Ⅵ. 결론



지금까지 국경안보의 연장선상에서 남북한 및 미·일·중·러 주변국들의 사이버공간에 대한 인식, 전략, 국제협력 등 사이버환경을 살펴보았다. 이를 토대로 한반도 통일 및 통합 과정에서 나타날 수 있는 주변국과의 갈등을 미리 방지하고, 국경안보를 위한 다자적 협력 기반을 조성하기 위해 사이버영역에서의 한반도 평화체제 구축을 위한 전략과 과제를 제시하였다.

먼저 한반도 주변국들의 국경안보 실태와 이들 국가의 대한반도 국경협력 가능성 그리고 남북한 접경지대 협력에 대한 종합적인 분석이 요구되는 시점에서 국경안보의 개념을 확대하여 정치 및 군사적 측면뿐 아니라 경제 협력 및 교류를 통해서도 국경안보에 대비할 수 있는 새로운 분석 틀을 제시하는 과정에서 4차 산업혁명 시대에 필연적으로 제기될 사이버상의 주권 문제와 한국의 사이버 국경안보 문제를 살펴보았다.

국경안보 차원에서의 사이버안보 논의는 사이버공간이라는 새로운 안보영역이 현실공간에서의 국경과 같은 접점을 포함하고 있으며 국경안보와의 상관성을 갖고 있다. 물론 현실공간에서의 국경안보 개념은 사이버공간의 특수성으로 인해 그대로 적용될 수는 없으나 국경이 주권과 주권이 충돌하는 지점이라는 논리의 연장선상에서 보면 사이버공간에서도 주권 충돌의 지점이 존재하므로 국경안보 개념의 확장을 통해 국경안보 차원에서의 사이버안보 논의가 가능하다. 또한 사이버안보의 특성이 국경안보 개념의 확장과 사이버공간과의 연계를 설명해주고 동시에 사이버공간에서의 국경안보 개념 정립의 근거를 제공해주고 있다.

국경안보와 국경협력 문제는 사이버공간에서도 적용 가능하며 주변국의 국경안보와 한반도 통일 환경은 주변국의 사이버환경과 한반도 평화체제 구축과 일맥상통한다. 따라서 한반도 사이버 평화체

제는 기존에 논의되고 있는 한반도 평화체제의 부분 또는 확장이라는 측면에서 접근할 수 있다. 즉 한반도 평화체제를 위한 사이버공간 차원에서의 안보 레짐을 의미하는 것이다. 따라서 한반도 사이버 평화체제는 사이버공간에서의 한반도 평화를 보장하는 사이버안보 레짐을 형성하는 국내외적 법적, 제도적 장치들과 거버넌스로 구성되고, 특히 사이버공간에서의 거버넌스 구축을 위한 국제적인 협력과 국제규범의 형성에 방점이 주어진다.

이어 한반도 사이버 평화체제에 대한 논의를 위해 다시 말해 국경안보 차원에서 사이버안보를 논의하기 위해 남북한 및 한반도 주변국들을 중심으로 사이버공간에서의 변화된 전략과 정책들을 검토하였다. 주변국 사이버안보 정책의 공통적 요소는 첫째, 관련 기관 간 협력체제 개발로 사이버안보가 국가안보 우선과제로 부상한 상황에서 단일부처가 감당할 수 없으므로 관련 기관 간 협력체제 개발을 진행하고 있다는 점이다. 둘째, 사이버 기술 발달을 통한 방어력 증강을 통해 억지력과 안전을 확보하고자 한다는 점이다. 셋째, 민·관 협력 강화로 사이버공간의 민간부문의 몫을 감안할 때 모든 정책결정에 기업, 시민사회, 기술자, 학자 등을 포괄하는 민·관 파트너십이 토대가 되고 있다는 점이다. 넷째, 국제협력 강화로 모든 국가가 국제협력 강화에 중점을 두고 있다는 점이다.

이에 따라 한국은 사이버공간에 대한 안전성 확보, 사이버공격에 대한 억지력 확보, 정보보안 정책의 성공적 추진을 위한 사이버안보 기반 조성, 국제 사이버협력 네트워크 확충 등을 사이버안보 전략의 추진방향으로 삼아야 할 것이다.

마지막으로 한반도 사이버 평화체제를 제안하고, 이를 구축하기 위해 주변국들의 사이버안보 정책 변화에 대한 대응을 통해 한반도 사이버안보 협력의 전략과 과제를 제시하였다. 또한 이 과정에서 새

로운 규범의 확립과 경쟁에 대비한 정책을 수립하기 위해 불안정한 사이버공간의 확장과 이에 기초한 위기와 갈등을 해결할 수 있는 평화적 규범 수립에 관한 정책 방안도 제시하였다.

한반도 사이버 평화체제와 관련된 거버넌스 구축을 위한 국제협력과 국제규범 형성은 국제, 지역, 개별국가 차원에서의 국제공조를 통해 이루어지고 있으며, 이에 따른 한반도 사이버 평화체제 구축을 위한 전략과 과제는 다음과 같다. 먼저 글로벌 국제공조 차원에서 사이버안보 국제공조 확대·강화를 위해 UN GGE, ITU 전권회의, 세계 사이버스페이스 총회 등 사이버안보 분야의 국제 거버넌스에 적극 참여한다. 둘째, 동북아 공조 차원에서 아세안+3, APEC, ARF 등 우리가 주도적으로 참여하고 있는 국제협력체를 중심으로 동북아의 집단적 사이버안보체제 구축을 추진하고, 나아가 남북한 및 미·일·중·러를 포함한 동북아 사이버안보협력체를 추진한다. 셋째, 양자 및 다자 공조 차원에서 사이버안보 주변국들인 미·일·중·러를 중심으로 그 외의 다양한 국가들과 양자 또는 다자간 협력을 추진한다.

사이버공간에서의 안보위협은 시공을 초월해 발생하기 때문에 불가측성과 더불어 정확한 근원지와 대상을 특정할 수 없다는 모호성을 가지고 있다. 특히, 국가안보적으로 첨예하게 대립하고 있는 동북아 지역에서의 강대국 간 경쟁과 갈등 구도는 공간의 제약을 받지 않는 사이버공간에서 더욱 빈번하게 발생할 가능성이 크다. 따라서 주변국의 사이버 관련 변화를 추적하고 분석하여 그에 적합한 대응책을 마련하는 것은 매우 중요하다.

사이버공간의 중요성이 증가하고 있으나, 주변국의 이해관계가 첨예하게 결부되어 있어 규범 설정에는 여전히 많은 시간이 필요하다. 결국 중요성과 불확실성이 공존하고 있는 사이버공간에서의 주

도권은 다양한 정보 수집을 통한 정확한 분석에 근거하여 실질적인 대응책을 마련하는데 중점을 두어야 한다. 따라서 주변국 간 협력을 수행하는 측면에서도 또한 새롭게 구성될 사이버공간의 규범 경쟁 차원에서도 주변국의 사이버공간에 관한 변화를 추적·관찰하여 우리에게 유효한 정보를 축적해야 한다. 이 같은 과정에서 사이버 국경 안보의 문제가 제기되는 것이며 이를 해결하기 위한 한반도 사이버 평화체제 구축이 요구되는 것이다. 향후 사이버공간에서의 한반도 평화는 현실공간에서의 한반도 평화와 번영을 가져오는 토대가 될 것이 명확하므로 이에 대한 보다 진전되고 적극적인 연구와 정책개발이 시급하다.

참고문헌

1. 단행본

국가안보실.『문재인 정부의 국가안보전략』. 고양: 다원디자인프린팅, 2018.

국가정보원·과학기술정보통신부·행정안전부·방송통신위원회·금융위원회.『2018 국가정보보호백서』. 서울: 한국인터넷진흥원, 2018.

_____.『2019 국가정보보호백서』. 서울: 한국인터넷진흥원, 2019.

국가정보원·미래창조부·방송통신위원회·안전행정부.『2013 국가정보보호백서』. 서울: 인터넷진흥원, 2013.

김상배.『세계주요국의 사이버안보 전략: 비교국가론적 시각』. 서울: 서울대학교 국제학 연구소, 2017.

_____.『사이버 안보의 국가전략』. 서울: 사회평론아카데미, 2019.

_____.『사이버안보의 세계정치와 한국; 버추얼 창과 그물망 방패』. 서울: 한울아카데미, 2018.

_____.『2018국가안보전략』. 서울: 국가안보전략연구원·동아시아연구원, 2017.

데이비드 E. 생어.『퍼펙트 웨폰』. 서울: 미래의 창, 2019.

신성호. "미국의 사이버안보 전략과 외교." 김상배 편.『사이버안보의 국가전략』. 서울: 사회평론, 2018.

유동열.『사이버공간과 국가안보』. 서울: 북앤피플, 2012.

이재봉 외 옮김, 요한 갈퉁(Johan Galtung).『평화적 수단에 의한 평화』. 서울: 들녘, 2000.

임병진. 『중국 사이버안보 체계에 관한 연구』. 서울: 서울대학교, 2017.

임종인 외. 『서울안보대화 사이버워킹그룹 운영방안』. 서울: 국방부, 2013.

차정미. "미중 사이버 군사력 경쟁과 북한 위협의 부상." 김상배 편. 『사이버안보의 국가전략 2.0』. 서울: 사회평론 아카데미, 2019.

Bartelson, Jorge. *A Genealogy of Sovereignty*. Cambridge: Cambridge University Press, 1995.

Biersteker, Thomas J. and Cynthia Weber. eds. *State Sovereignty as Social Construct*. Cambridge: Cambridge University Press, 1996.

Buzan, Barry. *People, States, and Fear: An Agenda for International Security Studies in the Post-Cold War Era*. Colorado: Lynne Rienner Publisher, 1991.

Camilleri, Joseph A. and Jim Falk. *The End of Sovereignty?* Aldershot: Edward Elgar, 1992.

Krasner, Stephen D. *Sovereignty: Organized Hypocrisy*. Princeton: Princeton University Press, 1999.

Mandel, Robert. *The Changing Face of National Security: A Conceptual Analysis*. Connecticut: Greenwood Press. 1994.

Opello, Walter C. & Stephen J. Rosow. *The Nation-State and Global Order: A Historical Introduction to Contemporary Politics*. Boulder, CO: Rienner, 1999.

Schmitt, Michael N. ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare: prepared by the*

International Group of Experts at the invitation of the NATO Cooperative Defence Centre of Excellence. Cambridge: Cambridge University Press, 2013.

Stephenson, Carolyn M. "New Approaches to International Peacemaking in the Post-Cold War World," in *Peace & World Security Studies: A Curriculum Guide*. edited by Michael T. Klare. Boulder: Lynne Rienner Publisher, 1994.

Tilly, Charles. *Coercion, Capital and European Sates AD 990-1900*. Oxford: Basil Blackwell, 1990.

警察庁.『警察白書』. 東京：警察庁, 2017.

小林良樹.『インテリジェンスの基礎理論』. 東京: 立花書房, 2014.

谷脇康彦.『サイバーセキュリティ』. 東京：岩波新書, 2018.

土屋大洋(編).『仮想戦争の終り』. 東京：角川角芸出版, 2014.

情報処理推進機構.『情報セキュリティ白書2018』. 東京：情報処理推進機構, 2018.

総務省.『情報通信白書』. 東京：総務省, 2018.

防衛省.『防衛白書』. 東京: 日経印刷, 2015.

_____.『平成30年度防衛白書』. 東京: 日経印刷, 2018.

_____.『令和元年国防白書』. 東京: 日経印刷, 2019.

持永大·村野正泰·土屋大洋.『サイバー空間を支配する者：21世紀の国家、組織、個人の戦略』. 東京: 日本経済新聞出版者, 2018.

2. 논문

고경민. "북한의 IT 딜레마와 이중전략-인터넷 정책과 소트웨어 산업 정책을 중심으로."『정보화정책』. 제14권 제4호, 2007.

김도승. "국가 사이버안보의 법적 과제."『미국헌법연구』. 제28권 2호,

2017.
김상규. “중국의 사이버안보 정책 변화와 그 함의.”『현대중국연구』. 20권 4호, 2019.
김상배. “사이버안보의 복합지정학: 비대칭 전쟁의 국가전략과 과잉 안보담론의 경계.”『국제지역연구』. 24권 3호, 2015.
_____. “사이버안보의 주변4강과 한국-세력망의 구조와 중견국의 전략.”『국제정치논총』. 57권 1호, 2017.
_____. “트럼프 행정부의 사이버안보전략: 국가지원 해킹에 대한 복합지정학적 대응.”『국제지역연구』. 제27권 제4호, 2018.
김상원. “경제제재와 러시아 경제의 변화.”『동유럽 발칸 연구』. 제43권 3호, 2019.
김소정·양정윤. “미국과 중국의 사이버안보 전략과 한국의 안보정책에 대한 함의.”『국가안보와 전략』. 제17권 2호, 2018.
김호홍·오일석. “신안보 분야 남북협력 추진전략.”『신안보연구』. 통권 193호, 2018.
김흥광. “북한의 사이버정보 실태.”『북한』. 5월호, 2005.
나용우. “초연결융합시대와 사이버안보.”『Journal of North Korea Studies』. 제3권 2호, 2017.
문수언. “상하이 협력기구(SCO)를 통하여 본 러시아와 중국 관계 : 러시아의 우려와 대응.”『사회과학 논총』. 13호, 2011.
배선하·박상돈·김소정. “국가 사이버보안 역량 평가를 위한 평가항목 연구.”『정보보호학회논문지』. 제25권 제5호, 2015.
서형준·김인중. “북한의 사이버테러 실태와 능력분석을 통한 향후 활동 진단.”『국가정보연구』. 제8권 1호, 2015.
신범식. “러시아의 사이버안보 전략.”『슬라브학보』. 제32권 1호, 2017.
신보람. “루넷(RuNet)과 유라시아-넷(Eurasia-Net): 중앙아시아에서의 러시아 인터넷의 위상.”『중소연구』. 42권 2호, 2018.

양정윤·박상돈·김소정. “정보공간을 통한 러시아의 국가 영향력 확대 가능성 연구: 국가 사이버안보 역량 평가의 주요 지표를 중심으로.”『세계지역연구논총』. 제36집 2호, 2018.

윤규식. “북한의 사이버전 능력과 위협 전망.”『군사논단』. 제68호, 2011.

이동범·곽진. “미국 정부의 사이버 공격에 대한 보안 전략.”『정보보호학회지』. 제24권 1호, 2014.

이상현. “일본의 사이버안보 수행체계와 전략.”『국가안보와 전략』. 제19권 1호, 2019.

_____. “사이버 위협에 대한 일본의 대응: 사이버 외교와 사이버 방위.”『국가전략』. 제25권 2호, 2019.

임종인·권유중·장규현·백승조. “북한의 사이버전력 현황과 한국의 국가적 대응전략.”『국방정책연구』. 제29권 제4호, 2013.

장규현·임종인. “국제 사이버보안협력 현황과 함의: 국제안보와 UN GGE 권고안을 중심으로.”『정보통신방송정책』. 제26권 5호, 2014.

장노순·한인택. “사이버안보의 쟁점과 연구 경향.”『국제정치논총』. 제53집 3호, 2013.

전완주. “미국의 사이버안보 수행체계 특징 및 시사점 고찰.”『신안보연구』. 통권 189호, 2016.

정영애. “사이버 위협과 사이버안보화의 문제, 그리고 적극적 사이버 평화.”『평화학연구』. 제18권 3호, 2017.

조성렬. “북한의 사이버전 능력과 대남 사이버위협 평가.”『북한연구학회보』. 제17권 제2호, 2013.

_____. “국제테러리즘과 군사적 대응.”『국제정치논총』. 44집 2호, 2004.

_____. “안보환경의 변화와 사이버안보.”『정치·정보연구』. 제16권 2호, 2013.

Baipai, Kanti. "The Idea of Human Security." *International Studies*. vol. 40, no. 3, 2003.

Barkin, Samuel J. and Bruce, Cronin. "The State and the Nation: Changing Norms and the Rules of Sovereignty." *International Organization*. vol. 48, no. 1, 1994.

Clark, Ian. "Beyond the Great Divide: Globalization and the Theory of International Relations." *Review of International Studies*. vol. 24, no. 3, 1998.

Cutler, Claire. "Critical Reflections on the Westphalian Assumptions of International Law and Organization: A Crisis of Legitimacy." *Review of International Studies*. vol. 27, no. 1, 2001.

Haas, Richard N. "Paradigm Lost." *Foreign Affairs*. vol. 74, no. 1, 1995.

Nocetti, Julien. "Contest and conquest: Russia and global internet governance." *International Affairs*. vol. 91, no. 1, 2015.

Nye Jr., Joseph S. "Power and National Security in Cyberspace," in Lord, Kristin M. & Sharp, Travis eds. *America's Cyber Future: Security and Prosperity in the Information Age,* vol. Ⅱ. Center for a New American Security. June, 2011.

Ristolainen, Mari. "Should 'RuNet 2020' Be Taken Seriously? Contradictory Views about Cyber Security Between Russia and the West." *Journal of information warfare*. vol. 16, no. 4, 2017.

Ruggie, J. G. "Territoriality and Beyond: Problematizing Modernity in International Relations," *International Organization*. vol. 47, no. 2, 1993.

川口貴久.「サイバー攻撃と自衛権：重要インフラ攻撃とグレーゾン−事態」.『グローバル・コモンズ（サイバー空間、宇宙、北極海）における日米同盟の新しい課題』. 東京：日本国際問題研究所, 2015.
谷脇康彦.“わが国のサイバーセキュリティ戦略.”『経済広報センターポケット・エ ディション・シリーズ』. no. 134, 2014.
田村賢吾.「サイバーセキュリティ対策−人材対策を中心に」.『損保総研レポート』. 第122号, 2018.
土屋大洋.“サイバーセキュリティとインテリジェンス機関―米英における技術変化のインパクト―.”『国際政治』. 第179号, 2015.
2019年 ‘中國互聯網絡發展狀況統計報告’
吴青熹.「习近平网络社会治理思想的三个维度」.『东南大学学报』. 第19卷 第6期, 2017.

3. 기타자료

『연합뉴스』.
『디지털타임스』.
『세계일보』.
『동아일보』.
『로동신문』.
『뉴데일리』.
『중앙일보』.
『전자신문』.
『문화일보』.
『조선일보』.
『머니투데이』.
『쿠키뉴스』.

『보안뉴스』.
『우리민족끼리』.
『CCTV 뉴스』.
고경민·김일기·나용우. 『김정은 시대 북한의 정보통신 전략에 관한 연구』. 통일부 정책연구용역 결과보고서. 2017.
김강무. "러시아의 사이버안보 전략에 대한 고찰." 〈2017년 한국국제정치학회 연례학술회의〉 자료집. 2017.
김흥광. "북한의 사이버테러 정보전 능력과 사이버보안 대책 제언." 한국사이버테러정보전학회·경기산업기술보안협의회, 『국가 산업기술유출 대응 콘퍼런스』, 2010.
관계부처 합동. 『국가사이버안보 기본계획』. 세종: 과학기술정보통신부. 2019.
국가안보실. 『국가사이버안보전략』. 서울: 청와대 국가안보실, 2019.
남상열. "사이버공간에 대한 국제적 논의와 2013년 서울 총회에의 시사점." 『전문가칼럼』 (진천: 정보통신정책연구원, 2012)
유동열. "북한의 대남 사이버위협 실태와 대책." 『사이버공간과 국가안보』. 국가안보전략연구소 학술회의자료집. 2014.
외교부. "글로벌 안보협력 개요."
장덕준. "러시아의 신안보 이슈."
한국정보화진흥원. 『2018 국가정보화백서』. 2018.

Coats. Daniel R. *Worldwide Threat Assessment of the US Intelligence Community*. 2018.
_____. *Worldwide Threat Assessment of the US Intelligence Community*. 2019.
ENISA. *National Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace*. 2012.

Gallagher, Ryan. "Japan Made Secret Deals with The NSA That Expanded Global Surveillance," *The Intercept*. 2017.

_____. "The Untold Story of Japan's Secret Spy Agency." *The Intercept*. 2018.

Godwin Ⅲ, James B. et al. *The Russian-U.S. Bilateral on Cybersecurity: Critical Terminology Foundation 2*. East West Institute and the Information Security Institute of Moscow State University. 2014.

Hanson, Fergus & Uren, Tom & Ryan, Fergus & Chi, Michael & Viola, Jack & Chapman, Eliza. *Cyber maturity in the Asia-Pacific Region 2017*. Australian Strategic Policy Institute. 2017.

ITU. *Global Cybersecurity Index(GCI)*. 2018.

___. *National Cybersecurity Strategy Guide*. 2011.

Lewis, James Andrew. "U.S.-Japan Cooperation in Cybersecurity." *A Report of the CSIS Strategic Technologies Program*. 2015.

Office of the Secreatry of Defense. "Nuclear Posture Reiview." 2018.

Opennet Initiative. "Country Profile: North Korea."

Roff, Heather M. *Cyber Peace: Cybersecurity Through the Lens of Positive Peace*. New America. 2016.

Symantec. *Internet Security Threat Report 2013*. vol. 18, Appendix. 2013.

Technolytics. "World War Ⅲ: A Cyber War has begun." 2007.

U.S. Department of Defense. Quadrennial Defense Review Report. 2010.

_____. *DoD Strategy for Operating in Cyber*

space. 2011.

_____. *The DoD Cyber Strategy*. April, 2015.

U.S. Department of States. "About Us-Office of the Coordinator for Cyber Issues"

_____. Media Note, "Co-Chairs' Statement on the Inaugural ASEAN-U.S. Cyber Policy Dialogue." 2019.

White House. "The Comprehensive National Cybersecurity Initiative." 2010.

_____. "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure." 2009.

_____. *Cyberspace Policy Review*. 2011.

_____. "National Security Strategy." 2017.

_____. *International Strategy for Cyberspace*. 2011.

_____. "National Cybersecurity Strategy." 2018.

_____. "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." 2017.

WIRES. *Obama ranks N.Korea cyber capabilities as not so good*. 2015.

中沢潔.「トランプ政権におけるサイバーセキュリティ政策の現状」. 『JETRO』. 2017年 9月.

최근 발간자료 안내

연구보고서

2017년도 연구보고서

〈연구총서〉

2017-01	북한인권 피해구제 방안과 과제 - 인도에 반한 죄를 중심으로 -	이규창 외	11,500원
2017-03	2017 남북통합에 대한 국민의식조사	박주화 외	12,000원
2017-04	통일 이후 통합방안: 민족주의와 편익을 넘어선 통일담론의 모색	이상신 외	8,500원
2017-05	대북·통일정책 관련 주요 쟁점과 정책추진방향	민태은 외	9,500원
2017-06	북한이탈주민의 교육, 복지, 그리고 시민권에 대한 인식	민태은 외	13,000원
2017-07	전환기 남북관계 발전 추진 방안	조한범 외	7,500원
2017-08	한반도 평화로드맵 실천전략	홍 민 외	7,000원
2017-09	북한 주민들의 복지와 시장화	임강택	8,000원
2017-10	한반도 평화체제 구상과 대북정책	정성윤 외	8,000원
2017-11	평양과 혜산, 두 도시 이야기: 북한 주민의 삶의 공간	조정아, 최은영	9,500원
2017-12	북중관계 주요분야별 현황 분석	임강택 외	12,000원
2017-13	트럼프 행정부 출범 이후 동아시아 전략환경 변화와 한국의 대응	김상기 외	11,000원
2017-14	동맹의 진화와 글로벌 파트너십	정구연 외	7,000원
2017-15	북한인권 정책환경 분석	한동호 외	7,500원
2017-16	북한 재난협력 방안과 과제	임예준, 이규창	9,000원
2017-17	김정은 시대 조선노동당의 조직과 기능: 정권 안정화 전략을 중심으로	박영자	13,000원
2017-18	김정은 정권 5년의 북한경제: 경제정책을 중심으로	홍제환	7,500원
2017-19	김정은 정권의 통치 테크놀로지와 문화정치	홍 민	6,000원
2017-20	김정은 정권의 핵전략과 대외·대남 전략	정성윤	6,500원
2017-21-01	뉴노멀 시대 미중 전략 경쟁관계와 한반도에의 함의(1부)	전병곤 외	9,500원
2017-21-02	뉴노멀 시대 미중 전략 경쟁관계와 한반도에의 함의(2부)	전병곤 외	9,500원
2017-22-01	주변국 국경안보: 이론과 실제	현승수 외	10,000원
2017-22-02	주변국 국경안보: 사례와 검증	현승수 외	9,500원
2017	사회권의 관점에서 본 북한인권	북한인권연구센터 편	13,500원

〈정책연구시리즈〉

2017-01	지속가능한 통일·대북정책: 환경 분석과 추진방향	이규창 외
2017-02	통일국민협약 추진방안	조한범, 이우태

2017-03 동서독 통일과정에서 서독정부의 대동독정책 연구 이상신 외
2017-04 대북제재 국면에서 남북교류협력 추진 방안 임강택, 홍제환
2017-05 평화와 번영의 한반도: 정책목표와 추진방향 이규창 외

〈Study Series〉

2017-01 Implications of North Korea's Nuclear Advancement and Response Measures Chung, Sung-Yoon et al.
2017-02 Study on Changing Trend of Human Rights Institution and Situation in North Korea Rim, Ye Joon et al.
2017-03 Advancement of Science and Technology and North Korea's Asymmetric Threat: Rise of Cyber Warfare and Unmanned Aerial Vehicle Chung, Kuyoun·Lee, Kitae
2017-04 Study on North Korean Defectors' Perception about Democracy and the Market Economy Kim, Soo-Am et al.

2018년도 연구보고서

〈연구총서〉

2018-01 평화의 심리학: 한국인의 평화인식 박주화 외 19,000원
2018-02 사회문화교류협력 및 인적 접촉 활성화 방안 이규창 외 14,000원
2018-03 남북관계 발전과 북한주민 의식 변화 성기영 외 10,500원
2018-04 국경협력의 가능성과 미래 이기태 외 9,000원
2018-05 북한과 주변국의 국경안보 이기태 외 8,000원
2018-06 중국 초국경 경제협력 연구: 통일 한반도 국경안보에 대한 시사점 현상백 외 12,000원
2018-07 KINU 통일의식조사 2018: 남북평화 시대의 통일의식 이상신 외 11,000원
2018-08 한반도 비핵·평화체제 구축과 남북관계 전략 조한범 외 8,000원
2018-09 북한의 주민 일탈과 법적 대응 박영자 외 11,500원
2018-10 '하나의 시장' 형성을 위한 시장친화적 남북경제협력방식의 모색 임강택 외 9,500원
2018-11 한반도 평화통일을 위한 글로벌 네트워크 전략 김진하 외 9,500원
2018-12 북한 민생 실태 및 협력 방안 홍제환 외 9,000원
2018-13 북핵위기와 북미 간 전략환경 인식 이우태 외 11,000원
2018-14 북한의 핵전략 분석 홍우택 외 6,500원
2018-15 제재 국면에서의 주민의 인권 도경옥 외 10,000원
2018-16 한반도 평화와 남북협력 종합연구(총괄보고서) 김상기 외 5,500원
2018-17 북핵 종합평가와 한반도 비핵화 촉진전략 정성윤 외 21,000원
2018-18 동북아 플러스 책임공동체 형성 방안 이기태 외 12,000원
2018-19 북한 변화 실태 연구: 시장화 종합 분석 홍 민 외 20,500원
2018-20 한반도 평화체제 구축과 한미관계 김상기 외 10,000원

2018-21 북한에서 국가-사회관계 양상 연구 한동호 외 14,000원
2018-22 김정은 시대 북한의 국가기구와 국가성 박영자 외 13,500원
2018-23 북한 군사경제 비대화의 원인과 실태 오경섭 외 12,000원
2018-24 한반도 평화번영과 남북중 협력방안 정은이 외 9,500원
2018-25 중국 시진핑 2기 지도부 구성과 대외정책 전망 신종호 8,500원
2018-26 2030 미중관계 시나리오와 한반도 신종호 외 12,000원

〈정책연구시리즈〉

2018-01 김정은 시대 북한 경제사회 8대 변화 박영자 외
2018-02 2018년 미국 중간선거 평가와 미국의 향후 대외정책 전망 민태은 외
2018-03 대북 제재 현황과 완화 전망 서보혁 외
2018-04 지자체 남북교류협력사업의 평가지표와 발전방향 나용우 외

〈Study Series〉

2018-01 The Implementation Strategy of the Establishment for Peaceful Community on the Korean Peninsula Hong, Min · Cho, Han-Bum · Park, Ihn-Hwi
2018-02 2017 Survey of Inter-Korean Integration Park, Juhwa · Rhee, Minkyu · Cho, Won-Bin
2018-03 North Korean Economy in the Kim Jong-un Regime Hong, Jea Hwan
2018-04 Peace Regime of the Korean Peninsula and North Korean Policy Chung, Sung-Yoon · Lee, Moo Chul · Lee, Soo-hyung
2018-05 Eight Changes in North Korean Economy and Society under the Kim Jong Un Regime Park, Young-Ja et al.

2019년도 연구보고서

〈연구총서〉

2019-01 트럼프 행정부의 안보전략과 한반도 평화체제의 전망: 미국의 적대국 관계정상화 사례와 한반도에 주는 시사점 이기태 외 8,000원
2019-02 남북관계 2023: 도전요인과 대북정책 추진방향 김갑식 외 17,500원
2019-03 한반도 평화협정의 법적 쟁점과 과제 도경옥, 안준형 8,500원
2019-04 한반도 평화체제 구축을 위한 국제협력 이재영, 김주리 8,000원
2019-05 화해협력 이론과 사례 그리고 한반도 서보혁 외 12,000원
2019-06 한반도 평화체제 구축을 위한 한중협력방안 이재영 외 11,500원
2019-07 북한 여성의 일상생활과 젠더정치 조정아 외 11,000원
2019-08 북한 변화의 변수와 경로: '핵문제'와 '개혁·개방'의 조합을 중심으로 박영자 외 11,000원
2019-09 남북연합 연구: 이론적 논의와 해외사례를 중심으로 이무철 외 15,000원

2019-10 뉴노멀시대 미중관계 변화와 한국의 대북·통일전략 신종호 외 18,000원
2019-11 남북한 인도협력 방안과 과제: 인도·개발·평화의 트리플 넥서스 홍석훈 외 9,000원
2019-12 남북 사회문화교류 활성화를 위한 교류거버넌스 구축방안: 체육교류를 중심으로 이우태 외 9,000원
2019-13 분권형 대북정책 추진 전략과 실천과제: 대북교류협력정책의 지속가능성 제고 방안을 중심으로 나용우 외 10,000원
2019-14 북한 외교정책: 정책패턴과 북핵외교 사례분석 김진하 외 10,000원
2019-15 김정은 정권 핵심집단 구성과 권력 동학 오경섭 외 9,500원
2019-16 북한이탈주민 가치적응 실태연구: 지역사회통합 중심으로 김수경 외 7,500원
2019-17 변화하는 통일환경에 따른 대북·통일정책 개선과제: 신한반도체제 구상을 중심으로 조한범 외 14,500원
2019-18 남북교류협력 재개 과정에서의 신변안전 보호에 관한 연구 - 영사접견 기능의 제도화를 중심으로 - 이규창 외 11,500원
2019-19 국민과 함께하는 통일·대북 정책 이상신 외 24,000원
2019-20 한반도 평화와 남북 협력 종합연구 총론: 평화·경제·화해 협력 구상 서보혁 10,000원
2019-21 한반도 평화체제 관련 쟁점과 이행방안 서보혁 외 14,000원
2019-22 2019 한국인의 평화의식 박주화 외 19,000원
2019-22-01 평화의식 문항별 분석 박주화 18,500원
2019-22-02 평화의식 문항별 테이블 박주화 14,500원
2019-23 평화교육의 실태와 쟁점: 통일교육과의 접점을 중심으로 조정아 외 12,000원
2019-24 북한 실태 연구: 도시경제의 네트워크와 로지스틱스 홍 민 외 21,500원
2019-25 김정은 시대 서부 주요 도시의 기업현황 및 가동률 결정요인 분석 정은이 외 14,000원
2019-26 남북경협 발전 잠재력과 정책 과제 김석진, 홍제환 10,000원
2019-27 한반도 평화·번영 실현을 위한 국경 협력 현승수 외 14,000원
2019-28 한반도 접경국과의 초국경 관광·교통 협력 최장호 외 10,000원
2019-29 주변국의 사이버 환경과 한반도 평화체제 구축 채재병 외 8,500원
2019 제3세대 인권과 북한 인도협력연구실 편 16,500원

〈정책연구시리즈〉

2019-01 한반도 평화협정문 구상과 제안 김상기 외
2019-02 국제 전략환경의 변화와 한국의 신남방정책 이기태, 배정호
2019-03 국제 비교를 통해 본 북한의 생활수준 김석진, 홍제환
2019-04 급변하는 동북아 정세가 한국인의 주요 인접국가 인식에 미치는 영향: 한미동맹과 한일관계를 중심으로 이상신 외

〈Study Series〉

2019-01 North Koreans' Current Living Conditions Based on UNICEF Survey Results: With a Focus on the Status of Infant Nutrition Hong, Jea Hwan

2019-02 The Impact of Sanctions on the Enjoyment of Human Rights
Do, Kyung-ok · Baek, Sangme

2019-03 South Koreans' Perception on Peace: With a Focus on Peace, War, the Way Peace is Realized, and the Attitude for Inter-Korean Reconciliation
Kim, Kap-Sik · Park, Juhwa

KINU Insight

2017-01	북한의 핵·미사일 관련 주요 활동 분석	홍 민
2017-02	중국의 19차 당 대회 평가와 정책적 고려사항	전병곤
2017-03	북한 노동당 중앙위원회 제7기 제2차 전원회의 평가 및 권력구조 전망	박영자
2018-01	2018년 김정은 신년사 분석과 정세 전망	홍 민 외
2019-01	2019년 김정은 신년사 분석과 정세 전망	홍 민 외
2019-02	김정은 정권의 정보화 실태와 특징: ICT 부문을 중심으로	정은미
2019-03	미국의 INF조약 탈퇴 의미와 트럼프 행정부의 군사·안보 전략에 대한 함의	김주리
2019-04	'우리 국가제일주의'의 문화예술적 표상과 시사점	이지순
2019-05	중국의 4차 산업혁명과 북한에 주는 함의	이재영
2019-06	한반도 국제정세의 역동성과 한국의 대응 방향	서보혁
2019-07	신한반도 체제 구상의 이해	조한범
2019-08	최근 한반도 정세 평가와 정책 과제	김갑식 외

북한인권백서

북한인권백서 2016	도경옥 외 18,000원
White Paper on Human Rights in North Korea 2016	도경옥 외 22,500원
북한인권백서 2017	도경옥 외 20,000원
White Paper on Human Rights in North Korea 2017	도경옥 외 24,500원
북한인권백서 2018	한동호 외 20,000원
White Paper on Human Rights in North Korea 2018	한동호 외 24,000원
북한인권백서 2019	김수경 외 20,000원
White Paper on Human Rights in North Korea 2019	김수경 외 24,500원

연례정세보고서

2016	통일환경 및 남북한 관계 전망 2016~2017	통일연구원
2017	통일환경 및 남북한 관계 전망 2017~2018	통일연구원
2018	2019 한반도 정세 전망	통일연구원

2019 2020 한반도 정세 전망 통일연구원

정기간행물

통일정책연구, 제25권 1호 (2016)	10,000원
International Journal of Korean Unification Studies, Vol. 25, No. 1 (2016)	10,000원
통일정책연구, 제25권 2호 (2016)	10,000원
International Journal of Korean Unification Studies, Vol. 25, No. 2 (2016)	10,000원
통일정책연구, 제26권 1호 (2017)	10,000원
International Journal of Korean Unification Studies, Vol. 26, No. 1 (2017)	10,000원
통일정책연구, 제26권 2호 (2017)	10,000원
International Journal of Korean Unification Studies, Vol. 26, No. 2 (2017)	10,000원
통일정책연구, 제27권 1호 (2018)	10,000원
International Journal of Korean Unification Studies, Vol. 27, No. 1 (2018)	10,000원
통일정책연구, 제27권 2호 (2018)	10,000원
International Journal of Korean Unification Studies, Vol. 27, No. 2 (2018)	10,000원
통일정책연구, 제28권 1호 (2019)	10,000원
International Journal of Korean Unification Studies, Vol. 28, No. 1 (2019)	10,000원
통일정책연구, 제28권 2호 (2019)	10,000원
International Journal of Korean Unification Studies, Vol. 28, No. 2 (2019)	10,000원

기타

2016	북한 내 고문 및 비인도적 처우	한동호 외
2016	Torture and Inhumane Treatment in North Korea	Han, Dong-ho et al.
2016	북한 여성·아동 인권 실태	도경옥 외
2016	Human Rights Situation of Women and Children in North Korea	Do, Kyung-ok et al.
2016	러시아 사할린 지역의 북한 노동자	이애리아 외
2017	북한 내 이동의 자유	한동호 외
2017	Freedom of Movement in North Korea	Han, Dong-ho et al.
2017	러시아 모스크바 및 상트페테르부르크 지역의 북한 노동자	이애리아 외
2018	한반도 평화체제 및 비핵화 관련 자료집	박주화, 윤혜령 53,500원
2018	북한의 건강권	이금순 외
2018	The Right to Health in North Korea	Lee, Keumsoon et al.
2018	미·중·일·러 한반도 정책 연구 네트워크 다이렉토리	김진하 외

통일연구원 定期會員 가입 안내

통일연구원은 민족공동체 실현을 위한 국민 역량을 축적하고 통일환경 변화에 적극적·주도적으로 대응할 수 있도록 통일문제에 관한 제반 사항을 전문적, 체계적으로 연구하고 있습니다. 본원의 연구성과에 관심이 있는 분들에게 보다 많은 정보와 자료를 제공하고자 연간 회원제를 운영하고 있습니다.

연간 회원에게는 간행물을 우편으로 우송해 드리며 각종 학술회의에 참석할 수 있는 혜택을 드립니다.

1. 회원 구분
   - 가) 학생회원: 대학 및 대학원생
   - 나) 일반회원: 학계나 사회기관소속 연구종사자
   - 다) 기관회원: 학술 및 연구단체 또는 도서관

2. 가입방법
   - 가) 회원 가입신청서 작성
   - 나) 신한은행 140-002-389681(예금주: 통일연구원)으로 계좌입금
   - 다) 연회비: 학생회원 7만원, 일반회원 10만원, 기관회원 20만원

3. 회원 특전
   - 가) 연구원이 주최하는 국제 및 국내학술회의 등 각종 연구행사에 초청
   - 나) 연구원이 발행하는 정기간행물인 『통일정책연구』, International Journal of Korean Unification Studies, 단행본 시리즈인 연구총서, 협동연구총서 등 우송
   - 다) 도서관에 소장된 도서 및 자료의 열람, 복사이용
   - 라) 통일연구원 발간자료 20% 할인된 가격에 구입

4. 회원가입 문의
   - 가) 주소: (06578) 서울시 서초구 반포대로 217 통일연구원 도서회원 담당자
   - 나) 전화: (02)2023-8009, FAX: (02)2023-8293, E-Mail: books@kinu.or.kr
   - 다) 홈페이지: http://www.kinu.or.kr

※ 가입기간 중 주소 변경 시에는 즉시 연락해 주시기 바랍니다.

회원가입신청서

* 표는 필수항목입니다.

신청자 성명* (입금자가 다를 경우 별도 표기)		소 속*		
간 행 물* 받 을 주 소	(우편번호 :) **※ 도로명 주소 기입必**			
연 락 처*	TEL		이메일	
이메일 서비스	수신 ( ) 수신거부 ( )			
회 원 구 분*	학생회원 ( ) 일반회원 ( ) 기관회원 ( )			

본인은 통일연구원의 연회원 가입을 신청합니다.

20 년 월 일 성 명 (인)

개인정보 이용 동의서

통일연구원은 개인정보보호법 등 관련 법령상의 개인정보보호 규정을 준수하며 개인정보 보호에 최선을 다하고 있습니다. 연구원은 다음과 같이 연구원 업무 수행에 반드시 필요한 범위 내에서 개인정보를 이용하는 데 동의를 받고자 합니다.

1. 개인정보의 수집·이용 목적: 도서회원 가입 신청 관리
2. 수집하려는 개인정보의 항목
   성명, 소속, 주소, 연락처, 회원구분
3. 개인정보의 보유 및 이용 기간: 입금일로부터 1년
   ※ 회원자격 갱신 시 개인정보 보유기간은 1년간 연장됩니다.
4. 동의를 거부할 권리 안내
   귀하는 위와 같은 개인정보를 제공하는 데 대한 동의를 거부할 권리가 있습니다. 그러나 **동의를 거부하실 경우 도서 회원 가입 및 발송이 원활히 이루어 질 수 없음을 알려 드립니다.**

20 년 월 일 성 명 (인)

※ 본 신청서 및 개인정보 이용 동의서를 보내주십시오.
(06578) 서울시 서초구 반포대로 217 통일연구원 도서회원 담당자앞
전화: (02)2023-8009, FAX: (02)2023-8293, E-Mail: books@kinu.or.kr
※ 온라인 신한은행 140-002-389681 (예금주: 통일연구원)

주변국의 사이버 환경과 한반도 평화체제 구축

KINU 통일연구원

값 8,500원
93340
9 788984 799707
ISBN 978-89-8479-970-7