독도재단 신진연구자 연구지원사업 연구용역 과제

하이브리드 전쟁과 독도 사이버 방어전략

- 러시아-우크라이나 정보심리전 사례를 중심으로 -

하 대 성

2023년 10월

경북대학교

목 차

I. 서 론: 전쟁의 진화 및 양상 변화

2022년 2월 24일 발생한 러시아-우크라이나 전쟁이 우리에게 주는 시사점은 무엇인가? 코로나 펜데믹 이후 세상은 많은 학자들이 예상한 데로 미중 패권경쟁의 심화와 세계화의 퇴보, 국가주의 부활을 가져왔다.[1] 코로나 펜데믹의 확산과 더불어 시작된 전쟁은 3일을 넘기지 못할 것이란 많은 군사 전문가들의 예상을 뒤엎고 1년이 지난 지금까지 격렬한 공방을 이어오고 있다. 심지어 저항을 넘어 반격작전을 감행하여 2014년 빼앗긴 크림반도까지 수복하겠다는 의지를 국제사회에 천명하고 있다.[2] 무엇이 이러한 결과를 가져오게 했는가? 러시아의 침략을 비판하며 군사적 지원을 이끈 우크라이나의 힘은 무엇인가? 전쟁전문가들의 관심사는 약소국이 강대국을 상대로 어떻게 전쟁의 주도권을 잡을 수 있었는가에 주목하고 있다. 국제사회의 여론을 이끌고 군사적 지원을 얻어낼 수 있었던 원인은 정보심리전에서의 승리다.[3]

국제정치적 시각에서 러시아-우크라이나 전쟁이 주는 시사점은 투키디데스 시대 이후로 변하지 않는 국제정치의 단면을 보여주고 있다는 점이다. 미국의 인도·태평양 전략과 중국의 일대일로전략의 경쟁은 동아시아에서 충돌을 불가피한 것으로 전망하고 있다.[4] 강대국의 영향력이 상존하는 한반도는 강대국들의 충돌로 전쟁과 평화가 공존할 수밖에 없는 지정학적 운명을 지니고 있다. 우리가 러시아-우크라이나 전쟁을 민감하게 인식해야 하는 이유이다. 강대국의 지배속성을 보여주는 국제정치 현실 속에 국제정치, 국제정세, 국제관계를 정확히 인식하고 이해할 수 있어야 한다. 그래야만 강대국을 활용하여 전쟁을 억제하고 평화를 지켜낼 수 있기 때문이다.

독도 문제는 세계 도서영유권 분쟁사례에 비추어 볼 때 경우에 따라서는 군사적 위기까지도 초래할 가능성이 있는 전형적인 도서영유권 분쟁의 특성을 지니고 있다.[5] 2019년 중국, 러시아 군용기가 한국의 방공식별구역(KADIZ)을 무단 침범한 것은 28회로 중국 군용기가 25차례, 러시아 군용기가 13차례였다. 일본은 러시아 군용기의 독도 영공침범 때 한국공군의 경고사격을 문제 삼아 이를 영공침범 행위로 보고 주권을 침해했다고 주장했다. 이를 계기로 자위대법 제84조에 기반을 두고 독도 상공에서

---

1) 김상배, 『미중 디지털 패권경쟁』, (서울: 한울, 2022), pp. 11-12.

2) "우크라, 8년전 빼앗긴 크림반도 곧 수복작전"...러, 핵무기 보복 시사", 조선일보(2022.08.19.), https://www.chosun.com/international/international_general/2022/08/18/RGFMW4O3V5E6JPZLUAS3Z6UVTI/(2023.03.12.)

3) 송태은, "러시아-우크라이나 전쟁의 정보심리전: 평가와 함의", 『주요국제문제분석』, Volume 2022, Issue 12(2022.), pp.1-2.

4) 정호섭, 『미중 패권경쟁과 해군력』, (서울: 박영사, 2021.), pp.369-376.

5) 하대성, "한국의 독도 위기관리와 DKD 모델", 『경북대학교 박사학위 논문』(2021.), p.18.

충돌이 발생하는 경우 항공자위대 전투기를 긴급발진시킬 가능성을 방위백서에 명시했다.[6] 결국, 일본은 독도해역에서 문제가 발생하면 군사적 행동을 하겠다는 도발적 표현을 명시한 것이다. 일본의 독도 영유권 주장이 구호가 아니라 군사적 실행 가능성을 내포했다는 점에서 직접적인 위협이다. 이미 동해 및 독도해역은 미국, 중국, 러시아, 일본의 전략적 군사적 각축장이 되고 있다. 우리는 이러한 위협에 대비한 대응방안이 없거나 있다고 하더라도 이런 위협을 예견하지 못했을 뿐만 아니라 기존의 대응책으로는 체계적이고 복합적인 대응이 불가하다는 것을 인식하고 있다. 이것이 러시아-우크라이나 전쟁에 주목하는 이유이다.

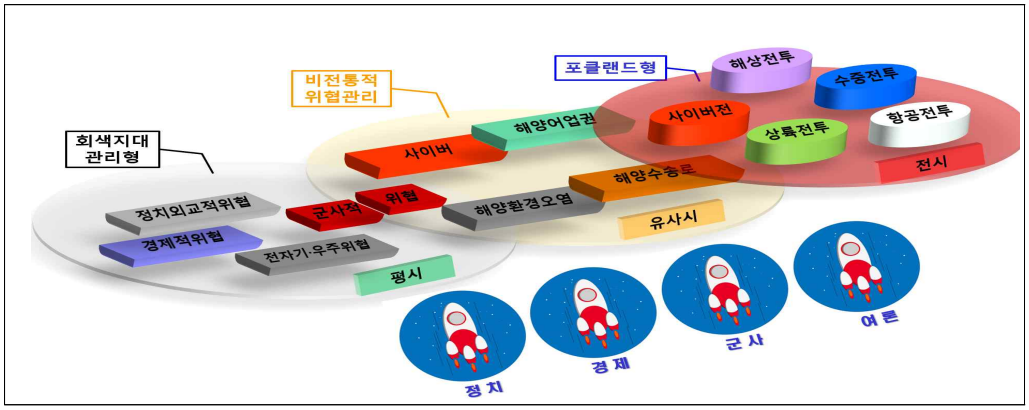
다윗과 골리앗의 싸움처럼 약자가 강자를 이겼을 때 주목한다. 우크라이나가 러시아를 상대로 벌인 정보심리전은 정보심리전의 대가인 러시아로부터 배운 처절한 학습효과에 기인한다.[7] 또한 서방과 IT기업, 해커집단, 일반 대중의 사이버 협공을 이끌어낼 수 있었기 때문이다. 반면 러시아가 펼친 정보심리전은 명분 없는 전쟁에 대한 국내외의 반발로 '특수군사적전'이란 명분은 전쟁의 실패요인으로 작용했다. 향후 벌어질 전쟁은 하이브리드 전쟁으로 대표된다. 전평시를 구분하지 않는 정보심리전이 하이브리드 전쟁의 요체이다. 정보심리전에 대한 효과적인 대응은 다양한 위협에 대비하고 전쟁을 미연에 방지할 수 있기 때문이다. 장차 독도 및 동해해역에서 벌어질 다양한 위협에 가장 효과적으로 대비할 수 있는 능력은 바로 정보심리전 역량에 있다는 것을 의미한다.

러시아-우크라이나 전쟁은 사이버 영역에서 벌어지는 정보심리전이 전쟁의 주도권을 달성할 수 있는 강력한 비대칭전력임을 입증하고 있다. 정보심리전은 전시 비무력적 군사활동으로 적국에 대한 정보 우위를 달성하고 의사결정에 혼선을 유발하며 적국의 전투 및 저항의지를 말살하여 전쟁의 주도권을 잡기 위한 중요한 전쟁수단이다.[8] 러시아-우크라이나 전쟁은 괄목한 ICT 기술이 전쟁 양상에 미치는 영향을 실감하게 했다. 새로운 기술이 접목된 안보환경은 우리가 상상하는 것보다 훨씬 빠르게 변화하며 공간의 제약을 좁혀가고 있다. 정보심리전의 핵심은 바로 디지털 프로파간다(digital propaganda) 활동이다.[9] 국제사회로부터 정치적 지지와 군사적 지원을 확보하기 위한 목적으로 전장 정보와 내러티브(narrative)를 유리하게 이용하여 사이버 전장에서 우위를 점하기 위한 군사적 활동으로 치열하게 전개되었다. 디지털 프로파간다 활동에는 초국가적으로 활동하는 익명의 해커집단과 IT기업, 일반 시민 등의 비국가행위자가 주요 행위자로 참가했다. 이는 우크라이나가 러시아의 정보심리전에

6) 앞의 논문. p.3.
7) 송태은, 위의 논문, pp.16-17.
8) 앞의 논문, p.1.
9) 정보심리전 핵심 선전

대항하여 펼친 반격 정보심리전이 효과적으로 작용할 수 있게 한 원동력이 되었다.

중국과 러시아, 일본은 강력한 국제여론을 동원해 평화가 이미 장착된 동아시아 독도해역에서 전쟁게임을 벌이고 있다. 독도 및 동해해역에서 벌어지고 있는 문제의 본질은 한국의 영토인 동해에서 벌어지고 있는 현실이며 효과적인 대응이 필요하다는 사실이다.



<그림 1> 한국형 독도방어 DKD 모델[10)]

〈그림 1〉한국형 독도방어 DKD 모델에서 보는 것처럼 회색지대 위협과 비전통적 위협, 군사적 위협 모두 사이버 위협이 존재한다. 하이브리드전은 평시, 유사시, 전시를 구분하지 않고 정치, 경제, 군사, 여론 제 분야에서 사이버 위협에 대비할 수 있어야만 위기를 효과적으로 관리할 수 있다는 것을 의미한다. 도발에 대한 가장 효과적인 대응은 러시아-우크라이나 전쟁사례에서 본 것처럼 디지털 프로파간다 활동을 통해 한국에 유리한 전장정보와 내러티브를 활용하는 것이다. 무력사용이나 직접적인 대응보다는 국제적인 여론을 유리하게 작용할 수 있는 정보심리전을 전개할 수 있는 능력과 대비가 필요하다.

이러한 배경에서 러시아-우크라이나 정보심리전 양상을 살펴보고 하이브리전 전쟁과 독도 사이버 위협요인을 분석하여 독도 사이버 방어전략을 구상해 보고자 한다.

본 연구에서 러시아-우크라이나 전쟁의 정보심리전 분석은 2022년 개전부터 2023년 2월까지 전쟁사례로 한정한다. 정보심리전의 승패는 개전 후 1년여 기간 동안 이미 결정되었기 때문에 구체적이고 상세한 분석은 선행연구들로 대신한다.

본 연구는 독도에 군사적 위기상황을 포함한 다양한 위협이 발생했을 경우 이에

10) 하대성, 위의 논문, p.243.

대응하고 위기를 관리하여 전쟁을 예방할 수 있는 독도 사이버 방어전략을 구축하는 것이다. 이를 위해 먼저 러시아-우크라이나 전쟁의 정보심리전 사례와 전세를 분석하여 결정적인 승리요인을 도출한다. 동해와 독도해역에서 영향력을 행사할 수 있는 중국, 러시아, 일본의 사이버전략과 능력을 법과 제도적인 측면, 사이버기술 확보 측면에서 알아보고 한국의 사이버전략과 역량을 비교해 보고자 한다. 2010년대부터 독도와 동해해역에서 발생한 다양한 위협사례에 대한 한국 정부의 대응실태 분석을 통해 우리가 가진 한계와 문제점을 살펴볼 것이다.

중국은 정보전을 가장 중요한 전쟁수단으로 간주한다. 특히 마오쩌뚱의 게릴라 전술이나 손자병법의 심리전처럼 전통적인 군사전략의 범주에 포함하여 다루고 있다. 열세한 전력으로 강력한 적을 상대로 싸우지 않고 이기는 전쟁전략을 수용하고 있는 것이다.

러시아는 하이브리드 전쟁 교리를 실제 전쟁에 적용하여 이론과 실제를 결합한 전쟁경험을 축적하고 있다. 에스토니아에 대한 사이버전(2007년), 조지아군에 대한 사이버전+군사력 투입(2008년), 크림반도 합병(2014년), 우크라이나 침공(2022년) 등을 통해 하이브리드 전쟁 교리를 적용한 수행능력이 진화하고 있다.

일본은 2014년 11월 '사이버 시큐리티 기본법'을 제정하고 급변하는 사이버 안보 환경에 대비하고 있다. 2015년에는 사이버 시큐리티전략을 마련하여 사이버 안보관련 최상위 지침서를 제정하였으며 2016년에는 외무성 산하 '사이버안전보장정책실'을 전담조직으로 편성하였다. 방위성은 2014년 '사이버 방위대'를 창설하고 미국의 사이버사령부를 모방한 통합부대 창설을 구상하였다. 2022년 3월 일본 방위성은 자위대 사이버방위대의 기능을 강화하여 약 540명 규모로 재편하고 사이버 공격수단을 개발하여 군사작전에 활용할 것이다.[11)]

이글의 Ⅱ장은 러시아-우크라이나 전쟁에서 디지털 프로파간다 활동을 이해할 수 있는 하이브리드 전쟁과 정보심리전의 개념에 대해 설명한다. Ⅲ장에서는 러시아-우크라이나 정보심리전 전략과 실제 적용사례를 사이버행위자 측면과 디지털 플랫폼의 무기화 측면에서 분석한다. 그리고 그러한 사례가 전세에 미친 영향을 조명하여 정보심리전의 요체를 확인할 것이다. Ⅳ장에는 먼저 동해와 독도 해역에서 영향력을 행사할 수 있는 미국, 중국, 러시아, 일본의 사이버전략과 능력을 법과 제도적인 측면, 사이버기술 확보 측면에서 알아보고 한국의 사이버전략을 비교 분석한다. 독도와 동해해역에서 벌어진 위협사례를 도출하여 한국의 사이버전략과 능력에 기반한 전평시 정보심리전의 독도 적용방안을 정책적 과제로 제시하고자 한다. 독도 사이버 방어전략

11) "일본 '자위대 사이버방위대' 설치...540 명 규모", 한국경제 TV(2022.03.17.), https://www.yna.co.kr/view/AKR20220317073200073(2023.05.12.)

은 동아시아에서 미국과 중국이 벌이는 패권경쟁 속에 장차 독도 및 동해해역에서 발생할 수 있는 다양한 위협과 영토분쟁을 효과적으로 관리하기 위한 사이버 정보심리전 역량을 키우는데 있다. 독도 사이버 방어전략을 통해 동아사아에서 약자인 한국이 강대국을 상대로 싸우지 않고 이길 수 있는 방책을 제공하여 한반도 및 동아시아에서 평화를 담보할 수 있어야 하기 때문이다.

Ⅱ. 하이브리드 전쟁과 정보심리전 개념 및 유형

1. 하이브리드 전쟁

모든 국가가 직면하고 있는 안보환경은 정보통신기술의 발달로 방패가 창을 따라가지 못하는 엄청난 속도로 빠르게 변화해 왔다. 제2차 세계대전에서는 비행기가 등장하여 전장을 땅과 바다에서 하늘로 확대시켰다.[12] 지금은 우주와 사이버 영역까지 확대되는 변화를 겪고 있다. 전쟁의 방식 또한 정보통신기술의 발달에 따라 진화되어왔다. 전쟁이라는 전통적인 고강도 군사적 도발보다 저강도 군사적 도발을 통해 군사적 정치적 목표를 달성하는 새로운 전략전술의 등장이다.[13] 회색지대 전략과 정보전, 미디어전, 심리전 등 다양한 수단을 동원한 하이브리드 전쟁 등이다.

회색지대 전략의 특징은 '살라미 전술'을 적용하여 상대방이 의도와 동기가 무엇인지 전혀 모르게 하여 전쟁으로 확산되지 않고 목표를 달성하는 것이다.[14] 또한 선제적 조치로 기정사실화(Fait Accompli)하여 상대방이 적절한 대응을 하지 못할 뿐 아니라 사전 대비책을 강구하지 않으면 전략적 의도와 목적을 안다하더라도 대응할 수 없기 때문이다. 그래서 회색지대 전략은 애매모호함(Ambiguity)과 점진주의(Gradualism)로 대표된다.[15] 대규모 군사 분쟁은 아니지만 제한적 물리력 사용과 함께 정보 조작, 정치 및 경제적 압박, 사이버전, 해양경비대 등 공권력을 동원하며 대리전도 수행된다.

회색지대 전략을 수행할 수 있는 의도와 능력을 갖춘 대표적인 국가는 중국과 러시아로 가짜뉴스로 대표되는 정보전과 심리전 등을 총체적으로 수행하고 있다. 중국

12) 데이비드 조던 외, 강창부 역, 『현대전의 이해』, (서울: 한울, 2014.), pp.111-113.
13) 앞의 책, p.26.
14) 홍규덕, "하이브리드 전쟁의 역설: 우크라이나 전쟁의 교훈", 『전략연구』, Volume 29, Issue 2(2022.), pp.55-57.
15) 양욱, "회색지대 분쟁 전략: 회색지대 분쟁의 개념과 군사적 함의", 「전략연구」 Volume 27, Issue 3, 2020. 11. pp. 12~14

은 ‘3전 교리’ 즉 심리전과 여론전, 법률전을 기반으로 회색지대 전략을 수행하고 있다. 사실을 조작하여 상대국의 사기를 저하시키고 국내외 여론에 영향력을 확대하고 있다. 현지에서는 문화교류 목적의 공자학원 등을 통해, 사이버 영역에서는 인터넷을 통해 사회 통합을 저해하고 행정력을 저하시키는데 주안을 둔다.[16)]

중국은 이미 우리나라를 대상으로 회색지대 전략을 적극적으로 수행해 왔다. 미국의 종말 고고도 지역방어 시스템(THAAD) 성주 배치를 빌미로 무역 보복을 한 것이 대표적이다, 서해 및 동해, 남중국해 등에서 해상민병대(Maritime Militia)와 불법조업 선단을 동원하여 어장을 황폐화하고 환경오염을 일으키는 사례는 기정사실화 되고 있으며 뚜렷한 대응책을 마련하지 못하는 실정이다.[17)]

중국은 영유권 행사를 위해 남중국해 일대에서 회색지대 전략을 사용하고 있다. 남중국해 일대 암초와 환초를 매립하여 인공섬을 만들고 영유권을 주장하고 있다. 영유권 주장을 위해 인공섬에 비행장과 항구를 건설하면서 대공미사일 포대 등 군사시설을 함께 건설하여 군대를 주둔시켰다. 회색지대 전략의 특징인 살라미 전술과 점진적 접근, 동기와 의도를 모호화 하고, 종국엔 기정사실화 하는 단계를 철저히 적용한 것이다.[18)]

러시아는 컴퓨터를 통한 접속 루트 조작, 대중의 여론을 조작하는 심리전으로 SNS와 AI 시스템을 활용한 허위사실 유포와 기만 전략을 집중적으로 수행하고 있다. 러시아는 우크라이나 동부 돈바스에서 전쟁이 시작되기 전 여론조작, 심리전, 전자전을 수행했다.

회색지대 전략은 전쟁으로 확산되지 않을 정도의 저강도 도발을 통해 점진적으로 목적을 달성하는데 반해 ‘하이브리드 전쟁(Hybrid War)’은 국가는 물론 반군이나 테러 집단 같은 비국가 단체들이 정규전과 함께 비정규전, 사이버전을 수행하는 새로운 형태의 전쟁 개념을 의미한다. 베트남 전쟁도 정규전과 비정규전이 동시에 치러졌지만, 북베트남의 정규전 부대와 비정규전 부대가 분리되어 ‘복합전(Compound War)’으로 정의한다. 정규전과 비정규전이 혼합된 하이브리드 전쟁은 정규전과 비정규전 부대의 구분이 없으며 동시에 수행된다. 그리고 평시에도 경제 제재, 사이버 공격, 선전과 기만, 그리고 가짜 뉴스를 동원한 정보전 등이 수행된다. 하이브리드 전쟁은 재래식 전쟁과 달리 영역과 공간의 구분이 없다. 특정 정부의 전복이나 영토를 병합,

---

16) 정삼만, “해양에서의 회색지대전략의 이론과 실제(Gray Zone Strategy in Maritime Arena : Theories and Practices)”, 한국해양전략연구소, Strategy21 통권 43호, Vol.21, No.1, 2018.06.01.

17) 하대성, 위의 논문, pp.202-203.

18) 조현덕, 이정태, “중국의 남중국해 영향력 확대를 위한 투트랙 전략-맞대응 및 회피전략을 중심으로”, 『대한정치학회보』 제29권 4호(2021.11.), pp. 120-121.

또는 상대국의 약점을 이용한 전략적 이익이 목표가 된다.[19]

하이브리드 전쟁의 기원은 2006년 7월 제2차 레바논 전쟁이다. 제2차 레바논 전쟁에 주목하는 이유는 비정규군인 헤즈볼라가 국가 수준의 정규전을 수행했다는 점이다. 이것이 하이브리드전의 기원이다. 헤즈볼라는 민간인 거주지역에 미사일 발사대를 설치하여 이스라엘 공군의 공격을 유도하여 많은 민간인 피해를 유도하였다. 정치적 목적을 위해 의도적으로 전쟁범죄 행위를 이용한 사례이다. 또한 지대함 미사일을 사용하여 이스라엘 해군 초계함 하니트(Hanit)를 격침시켜 하이브리드 전쟁의 개념을 정립하는 계기가 되었다.[20]

러시아는 제2차 레바논 전쟁을 통해 하이브리드 전쟁을 '신세대 전쟁(New Generation Warfare)'이란 이름의 교리로 정립했다. 현재 러시아의 총참모장인 발레리 게라시모프는 러시아의 하이브리드 전쟁 교리를 정립한 인물로 이를 '게라시모프 독트린'이라 부른다. 그는 2013년 발표한 논문에서 "선전포고 없이 이뤄지는 정치·경제·정보·기타 비군사적 조치를 현지 주민의 항의 잠재력과 결합시킨 비대칭적 군사행동"으로 정의했다. 2014년 크림반도 점령, 2022년 우크라이나 침공 등을 주도한 인물로 러시아의 정보심리전 수행능력과 역량을 가늠할 수 있을 것이다. 러시아가 하이브리드 전쟁에 나선 것은 냉전 붕괴 후 미국이 독보적 군사력 우위에 선 미국에 대항하기 위한 전략적 필요성 때문이다.

러시아는 하이브리드 전쟁 교리를 실제 전쟁에 적용하여 이론과 실제를 결합한 전쟁경험을 축적하고 있다. 에스토니아에 대한 사이버전(2007년), 조지아군에 대한 사이버전+군사력 투입(2008년), 크림반도 합병(2014년), 우크라이나 침공(2022년) 등을 통해 하이브리드 전쟁 교리를 적용한 수행능력이 진화하고 있다. 전쟁 수행방식은 전쟁 이전부터 민간해커를 동원하여 사전 연습 대상을 지정하여 정부 웹사이트에 대한 디도스 공격을 감행하고, 전쟁 이후에는 지휘체계 무력화에 중점을 둔다. 무력화한 정부 웹사이트를 통해 가짜 뉴스를 퍼 날라 정보심리전을 전개한다. 언론기관, 인터넷 서비스 회사, 통신사, 금융기관 등에 대한 사이버 공격으로 국민들의 일상을 마비시키면서 불안과 공포를 조장한다. 외부로부터의 인터넷과 통신을 차단하여 외국 정부와 해외 언론들은 해당 국가에서 벌어지는 상황을 알 수 없도록 만들었다. 사이버 공격으로 공격여건이 조성되면 군사력을 투입하여 손쉽게 전쟁목표를 달성한다.

2. 정보심리전 개념

---

19) 송승종, "러시아 하이브리드 전쟁의 이론과 실제", 『한국군사학논집』 Volume 73, Issue 1(2017.), pp. 69-71.

20) 육군군사연구소, "2014년 러시아의 우크라이나 개입", 2015., pp.10-17.

게라시모프독트린을 진일보시켰다고 평가받는 체키노프와 보그다노프(Chekinov and Bogdanov)는 '차세대 전쟁'에서 비군사적 수단 운영의 필요성과 전자전을 통한 정보우세를 매우 중요하게 다루고 있다.[21] 비군사적 수단으로 미디어, 종교조직, 문화단체, NGO, 해외로부터 자금지원을 받는 대중운동, 외국의 원조로 연구를 수행하는 학자들을 명시했다. 이들을 무력분쟁 이전부터 운영하여 협조된 공격에 활용해야 한다는 것이다. 전자전의 중요성을 강조하며 실제 공격이 이루어지기 이전에 강도 높은 선전선동을 전개하고, 적의 지휘통제통신 능력을 무력화해야 정보에서 우위를 점할 수 있다. 이를 통해 전자전은 전투작전의 중요한 형태로 부각된다.[22]

차세대 전쟁에서 주전장을 사이버 공간으로 전망한다. 사이버 공간에서 심리전과 정보전을 통해 군과 국민들의 사기를 떨어뜨려 저항의지를 말살하는 것이 대표적 특징이다. 특히 개전 단계에서의 중요성을 강조하고 있는데 개전 전 수개월에 걸쳐 외교, 경제, 이념, 심리·정보 등 제 분야 수단들을 통합하여 협조된 비군사적 공세를 요구한다. 또한 주민의 단결을 와해하고 중앙정부에 대한 불만을 고조시키며 군대의 사기를 떨어뜨리는 전방위적 선전선동캠페인을 전개한다. 대중적 기만과 뇌물을 이용하여 대상국 관료 및 군장교들을 포섭하여 침투한 비밀공작요원의 무기, 자금, 물자 등의 공급자 역할을 맡긴다. 비밀공작 요원들은 테러, 도발 감행 및 혼란과 불안정 조성 등을 위해 활동한다.

군사적 단계는 군사력이 투입되기 전 공격여건 조성을 위한 전자전과 군사력 투입으로 이루어진다. 공격여건 조성을 위한 전자전은 대규모 수색 및 전복(subversive) 임무와 전자 녹다운으로 대표된다. 수색 및 전복 임무는 군부대, 핵심시설 등 주요 핵심표적을 찾기 위해 가용한 모든 첩보수집 수단과 방법이 사용된다. 이어서 '전자 녹다운(electronic knockdown)'을 통해 정부 및 군을 무력화한다. 전자전을 통해 공격여건이 조성되면 장거리 포병, 정밀유도 미사일, 드론 및 자동화 무기를 통해 포병 및 항공작전 등의 군사공격이 이루어진다.

정보심리전, 전자전을 이용한 군사적 목표는 개전 초기단계에서 정부 및 군 통제소가 파괴되고 핵심 인프라가 심각한 피해를 당해 마비상태에 이르는 것이다. 마비상태에 이르면 적부대는 적시적절한 전개 및 배치가 불가능해진다. 군사공격을 통한 전쟁의 종결단계에서는 정규 지상군이 진입하여 잔여 저항지점을 고립하고 격멸한다.[23]

---

21) Chekinov, S. and S. Bogdanov. 2013. "The Nature and Content of a New-Generation War." Military Thought (October-December). p.17.

22) 체키노프와 보그다노프는 걸프전을 인류 최초의 차세대 전쟁으로 정의하고, 미국은 이미 선전선동을 목적으로 페이스북과 트위터 등을 통해 특화된 인터넷 '댓글부대(troll Farm)'를 동원하고 있다고 비난한다.

23) Chekinov, S. and S. Bogdanov. 앞의 논문. p.22.

이러한 차세대 전쟁의 모습은 2014년 크림반도, 2022년 우크라이나에서 벌어진 상황과 유사하다.

정보심리전(information & psychological warfare)은 상대국보다 많은 정보를 가지고 상대국에 불리한 정보를 주어 합리적인 판단을 내리지 못하게 함으로써 전쟁 의지를 말살하는 중요한 전쟁수단이다. 정보전(information warfare)을 통해 적보다 많은 정보를 획득하고, 정치전(political warfare)을 통해 상대국의 여론에 개입하여 자국에게 유리한 여론을 조성할 수 있어야 한다.

정보심리전이 군의 작전으로 수행될 때 정보작전(IO: information operations)과 심리작전(PSYO: psychological operations)으로 구분한다. 정보작전은 적에 대한 정보를 수집하거나 적에게 불리한 정보를 주어 합리적인 판단을 내리지 못하도록 유도하여 아군에게 유리한 상황을 조성하는 것이다. 심리전은 적의 사기를 꺾고 전쟁의지를 말살하며 아군의 사기와 결의를 높이는 전시 군사활동이다.[24]

전쟁에서 정보작전은 다른 군사수단에 비해 비용대 효과면에서 높은 가성비를 가지고 진입비용이 낮은 이점이 있다. 이는 전시와 평시의 구분을 모호하게 만들고 훨씬 더 위협적인 전쟁수단으로 진화해갈 것이다. 컴퓨터 네트워크에 대한 공격·방어·전과확대(exploitation), 전자전과 심리작전 등을 포함한다.[25]

정보작전은 의사결정에서의 오류를, 심리작전은 적에게 불리한 감정적 반응을 유도하는 것으로 완전히 구분할 수 없다. 작전목표를 공유하며 정보수집 활동이 긴밀하게 연결되어 유사하고 중첩된 부분이 많기 때문이다.

2014년 크림반도 침공, 2016년부터 진행된 미국과 유럽국가에 대한 선거 개입 등 러시아의 평시 정보심리전은 주목받아왔다. SNS에 허위조작정보를 유통하여 선거에 개입함으로써 가져온 파급효과를 실감했기 때문이다. 이러한 행위는 사이버공격으로 국가 주권을 침해하고 민주주의 제도를 공격하는 것이다.[26] 미중 패권경쟁이 가속화되고 정치체제, 이념 및 가치의 영역으로 확대되면서 더욱더 주목받고 있다.

특히 러시아-우크라이나 전쟁에 주목하는 이유는 역사상 가장 복잡한 형태의 정보심리전 양상을 보여주기 때문이다. 행위자 측면에서 서방의 IT기업, 국제적인 해커조직과 더불어 일반 시민들 조차 초국가 행위자로서 참여한 것이다. 이들은 사이버 심리전 공격에 참가하고, 일국에 유리하도록 여론을 만들어 감으로써 전쟁의 양상을 복

24) 송태은, “현대 전면전에서의 사이버전의 역할과 전개양상: 2022년 러시아-우크라이나 전쟁 사례”, 『국방연구』, Volume 65, Issue 3(2022.), pp.217-220.

25) 최근대, “중국의 반접근 지역거부(A2/AD) 전략에 대한 분석: 정보작전 수행역량 강화를 중심으로”, 『한국군사학논총』(2023.), p.40.

26) 하대성, “하이브리드 전쟁과 독도 사이버 방어전략”, 2023년 경북대학교 평화문제연구소 춘계 평화포럼 발표자료(2023.04.07.)

잡하게 만들고 있다.

3. 정보심리전의 유형

정보전은 지휘통제전, 첩보전, 전자전, 심리전, 해커전, 경제정보전, 사이버전 등 7가지 유형으로 구분한다.[27] 첫째, 지휘통제전은 지휘부에 대한 공격이다. 둘째, 첩보전은 전장 정보시스템을 구성하고 보호하며 필요 시 거부할 수 있어야 한다. 셋째, 전자전은 무선·전자 혹은 암호기술과 관련된 분야를 말한다. 넷째, 심리전은 상대국의 여론에 개입하기 위한 것이다. 다섯째, 해커전은 컴퓨터 시스템을 공격한다. 여섯째, 경제정보전은 경제적 우위를 점하기 위해 정보활동이다. 일곱째, 사이버전은 미래 전쟁으로 정의했다. 결국 정보전은 첨단 전자정보통신기술의 발달로 인해 구현되는 군사혁신 과정을 통해 나타난 개념이다. 따라서 정보전의 유형도 전자정보통신기술의 발전에 따라 변화되어갈 것이다.

정보작전에는 진짜정보, 허위정보와 허위조작정보 등이 있다. 허위정보는 예기치 않게 우연히 만들어진 잘못된 정보다. 허위조작정보는 누군가를 오도하기 위해 의도적으로 생산된 잘못된 정보다. 허위조작정보는 정확한 정보를 고의로 잘못된 맥락(wrong context)에 포함하여 메시지의 신뢰도를 높이는 방식으로 정보를 왜곡한다.[28] 이러한 여러 성격의 정보를 활용하는 정보작전은 다양한 전략적 효과를 가진다.

심리전의 대상은 상대국가와 대중이다. 특히 대중의 생각과 감정에 영향을 미치기 위한 선전선동과 심리작전을 이용한다. 심리전의 승패는 메세지에서 보여지는 내러티브의 공감력에 달려 있다.[29] 심리작전은 군사활동으로 평시, 전시, 우발사태(contingencies) 등 모든 상황에서 운용된다. 심리작전은 무력수단과 함께 사용되어 군사적 파괴력의 시너지 효과를 낸다.[30] 작전적 수준에서 심리작전은 전투 준비 차원에서 제한된 규모로 수행된다. 심리작전은 국가 프로파간다 활동으로 국가의 모든 공적 활동이 포함된다.[31]

지금 우리는 초연결(hyper-connected) 시대에 살고 있다. 초연결시대 정보심리전

---

27) Martin Libichi, “What is information Warfare?”, 『Strategic Forum』, No.28(1995.)

28) 송태훈, “세계전쟁 양상에 따른 정보작전(Imformation Operations) 변화 분석”, 『군사연구』(2020.) p253-255.

29) Joseph D. Celeski, “Psychological Operations—A Force Multiplier.” Special Air Warfare and the Secret War in Laos, Air University Press(2019) https://www.jstor.org/stable/pdf/resrep19555.19.pdf(검색일: 2023.7.10).

30) 송태훈, 앞의 논문, p267-269.

31) 이정하, “러시아 연방의 정보-심리작전과 제귀 통제(Reflexive Control)”, 『한국서양사연구회』, 제66권(2022.), pp.159-166.

은 인터넷과 SNS 등 사이버 공간을 통해 수행된다. 작전공간이 우주, 사이버 영역으로까지 확대됨에 따라 민간과 공적영역, 전쟁행위와 범죄행위, 작전과 비작전공간의 경계가 불명확하게 되었다. 정보심리전의 행위자 역시 영역간의 경계가 불명확해짐에 따라 국가 외에 다양한 행위자가 등장하고 있다.[32] 전평시 사이버 공간에서 다양한 비국가행위자가 정보심리전을 수행할 수 있게 된 것이다.

초연결 시대 정보커뮤니케이션 환경은 실시간 정보수집과 분석이 가능하다.[33] 이러한 정보커뮤니케이션 환경에서 수행되는 정보심리전은 과거와는 비교할 수 없을 정도의 강한 영향력과 파괴력이 지니고 있다.

오늘날 정보심리전의 특징을 살펴보면 첫째, 실시간 효과적인 정보의 전송이 가능하다. 지금 만든 정보는 첨단 인터넷과 SNS 등을 통해 실시간 발신할 수 있으며 수억 명의 사람이 받아볼 수 있다. 다양한 전장 정보운영 시스템(수집-탐지-생산-분석-공유)을 구축하고, 특정한 정보와 메시지를 특정 대중에게 보낼 수 있게 된 것이다. 정보심리전은 개인정보 및 공간정보 인프라, SNS 계정 데이터에 접근할 수 있는 능력이 중요한 변수이다.

둘째, 정보통신기기, 사물인터넷 등을 통해 정보커뮤니케이션 환경에 손쉽게 접근할 수 있다. 언제 어느 때라도 휴대폰과 컴퓨터, 자동차 등을 이용해 인터넷과 소셜미디어에 접속한다. 이러한 네트워크의 초연결성은 최적화된 여론 환경을 조성하여 언제든지 정보심리전을 쉽게 활성화할 수 있다. 따라서 나의 정보커뮤니케이션 채널은 확보하고 적의 정보커뮤니케이션 채널은 차단하는 것이 정보심리전에서 승패를 가늠한다.

세계 대중을 실시간 연결하는 최첨단 수단은 소셜미디어 플랫폼이다. 이들 플랫폼 대다수는 서구의 세계적인 IT기업이 독점하고 있다. 효과적인 정보심리전 수행을 위해서 이들 IT기업과의 공조는 필요조건이다. 이번 전쟁을 통해 세계를 연결하는 통신 네트워크 핵심 인프라 중 인공위성의 역할이 주목받고 있다. 원래 인공위성은 기후, 트래픽 상황 등에 따라 데이터 전송에 지장을 초래할 수 있다고 평가되었다.[34] 그러나 이번 러시아-우크라이나 전쟁에서 통신 인프라가 완전히 파괴된 우크라이나에 지

32) 송태은, 앞의 논문 참조

33) 오늘날 정보커뮤니케이션 환경은 정보통신기기, 각종 사물인터넷(Iot), 대규모 데이터를 저장하는 센서(sensor) 및 먼 거리에서 사람과 사물의 움직임을 정밀하게 탐지하고 인식할 수 있는 인공지능(Artificial Intelligence, AI) 기술을 탑재한 지능형 감시기술의 확산으로 실시간 정보수집과 분석이 가능하다.

34) Christian Bueger & Tobias Liebetrau, Jonas Franken, “Security threats to undersea communications cables and infrastructure –consequences for the EU.” IN-DEPTH ANALYSIS, European Parliament(2022). https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf(2023.07.02).

원된 서방의 위성 인터넷 서비스를 통해 인공위성 인터넷의 안보적 중요성이 크게 부각 되었기 때문이다.

셋째, 정보심리작전을 수행할 수 있는 행위자가 엄청나게 많아졌다는 것이다. 휴대폰, 컴퓨터의 보급과 정보커뮤니케이션 환경의 발달로 누구나 행위자가 될 수 있다는 측면에서 정보심리전의 기능과 영향력이 그 어느 때보다 강화되고 확대되었다. 정보심리전 수행주체가 IT기업, 민간 프로그래머, 초국적 해커조직 등으로 다양하게 확대되었다. 수행방식 또한 민간기업의 트롤팜(troll farm)[35]에 의한 대리공격과 직접 사이버 부대를 운영하는 방식을 두고 있다.[36]

SNS의 가짜계정인 '소셜봇(social bots)'을 이용한 사이버 심리전을 '로보트롤링(robo-trolling)' 혹은 디지털 프로파간다로 부른다. 이러한 AI 알고리즘 기술을 적용한 사이버 심리전은 상대국의 여론을 조작할 수 있을 정도의 가공할 만한 파괴력을 가지고 있다.

Ⅲ. 러시아-우크라이나 전쟁의 정보심리전 실제와 전세

1. 실제(사례)

가. 사이버전 행위자 차원

이번 사이버전 행위자는 국가 행위자, 비국가 행위자, 초국가 행위자 등이 참가하여 매우 다양하다. 특히 공격의 배후에서 국가를 지원하는 비국가 행위자, 참전국을 지원하는 비국가 행위자 등 다양한 배경에서 역할을 하고 있다.

러시아의 사이버전 특징을 살펴보면 첫째, 민간 해커그룹을 이용했다. 이는 기존에 러시아가 사용해온 방식이다. 둘째, 국제사회가 오랜 논의를 걸쳐 구축한 사이버 규범을 어겼다. 공격 제외대상인 에너지, 보건, 교육시설과 같은 비군사적 민간시설을 공격했다. 특히 병원과 학교, 난민 대피시설 등을 공격한 것이다.[37]

우크라이나도 미국을 동원해 러시아와 벨라루스를 공격했다. 미국이 우크라이나 사이버전의 대리세력으로서 사이버 공격과 방어, 사이버 정보작전을 수행하고 있다고

35) 민간기업에서 운영하는 악의적 댓글 부대로 고의로 선동적이고 도발적인 의견을 온라인 커뮤니티에 게시하여 분쟁과 혼란을 일으키는 조직을 말한다.

36) 허태회 외, "세계 주요 강대국들의 정보전 준비와 대응체계", 『국방연구』, Volume 49, Issue 1(2006.), pp.217-220.

37) 해커그룹의 사이버 공격 작전은 2022년 6월을 기준으로 할 때 약 240여개로 알려져 있으며 이는 언론을 통해 알려진 것보다 훨씬 큰 규모이다.

공개적으로 인정했다. 이는 우크라이나의 요청에 의해 수행된 집단적인 자기방어 조치로 직접적인 군사활동이 아니라고 언급했다.[38)]

중국과 벨라루스는 러시아를 지원하기 위해 우크라이나에 사이버 공격을 감행했다. 특히 중국 정부와 연계된 것으로 의심되는 해커조직은 전쟁 전부터 우크라이나 웹사이트를 공격했다. 개전 후에는 전 세계를 대상으로 하고 있으며 나토 회원국에 대한 공격은 116%로 급증했다. 이는 2022년 3월 14일에서 3월 20일까지 중국 주소 IP의 사이버 공격을 분석한 결과이다.

개전 후 9월 초까지 집계된 러시아의 공격은 1,600건 정도로 전쟁 전과 비교하면 112% 증가했다. 우크라이나 기업에 대한 사이버 공격은 매주 1,500건으로 개전 전과 비교할 때 25% 증가했다. 러시아의 공격은 사이버전 역사상 가장 규모가 크고 가장 오랫동안 지속되었다고 평가한다. 하지만 서방의 지원으로 러시아의 사이버 공격은 상당히 제한적으로 전개되었다. 개전 초 감행한 러시아의 디도스 공격의 파괴력이 크지 않으며 범위 또한 우크라이나 영토를 넘어서지 못하고 있다고 미국의 사이버 보안 회사가 밝혔다.

매우 흥미로운 것은 사이버전 역사상 가장 다양한 행위자들이 협공하여 사이버 심리전의 효과를 가져왔다는 것이다. 인터넷 해커들의 집단인 어나니머스(anonymous)는 러시아가 우크라이나를 침공한 날 사이버전 선전포고를 했다. 'IT Army of Ukraine'는 초국가 해커조직, 우크라이나 해커 등과 연대하여 디도스 공격을 수행했다. 다양한 해커조직의 사이버 협공은 러시아의 사이버 공격력을 적절히 제한하는 효과를 가져왔다.[39)]

해커조직의 사이버 공격은 민감정보 유출과 와이퍼 공격이다. 민감정보는 고위 관료와 주요 기관에 대한 정보, 러시아 군인들의 개인정보를 유출한 것이다. 특히 이들의 개인정보를 공개하고 전범 재판소에 넘길 것을 주장했다. 와이퍼 공격은 러시아 국방부 웹사이트를 디도스로 공격해 우크라이나의 선전선동 메시지가 프린터에서 출력되게 했다. 또 관영매체의 웹사이트 마비, 러시아 TV 채널에서 우크라이나 지지 메시지나 노래가 나오도록 만들었다.

이번 사이버전은 대리전의 양상을 띠면서 해커조직 간 사이버전도 진행되고 있다.

---

38) 2022년 6월 미 백악관 대변인 카린 장-피에르(Karine Jean-Pierre)는 우크라이나 사이버전에 대한 미국의 지원은 직접적인 군사활동을 하지 않는다는 약속을 위반한 것이 아니므로 러시아로부터 사이버 보복을 초래할 것으로 보지 않는다고 말했다.

39) "폭격·피란 실시간 중계…러·우크라 '틱톡 전쟁'," 조선일보(2022.03.02.) https://www.chosun.com/international/international_general/2022/03/02/L2V5AKOVMZE2FODNBDQLA357PM/?utm_source=naver&utm_medium=referral&utm_campaign=naver-news(2023.08.16.)

미국의 첩보기관 동맹인 파이브아이즈(Five Eyes)가 親 러시아 해커조직의 사이버 공격을 경고하자 어나니머스는 즉각 Killnet의 가담자 146명의 개인정보를 공개했다. 이 밖에도 어나니머스는 러시아의 400개 이상의 CCTV를 해킹하여 러시아 대중에게 반전 메시지를 송출했다. 러시아 시민들의 휴대폰에 반전문자 메시지를 보내고, 일반인들도 어나니머스 사이버작전에 참가할 수 있도록 프로그램을 개발해 송출했다.[40]

사이버 행위자 차원에서 비국가 행위자가 국가와 협력하여 사이버전에 가담하는 전례를 만들었다는 것은 매우 중요한 변화이다. 이러한 변화는 국제사회가 오랜 논의를 걸쳐 구축한 사이버 규범을 무력화하고 향후 사이버전에 대한 대응을 더욱더 어렵게 만들 것이다.

나. 디지털 플랫폼의 무기화

우크라이나는 러시아의 사이버 공격으로 파괴된 인터넷 인프라를 대신해 스타링크(Starlink) 위성 인터넷 서비스를 일론 머스크에게 요청했다. 일론 머스크에 의해 제공된 스타링크 위성 인터넷 서비스는 지금도 우크라이나 전역에서 인터넷 서비스를 지원하고 있다. 우크라이나는 스타링크 단말기 15,000대를 통해 하루 150,000명이 인터넷을 이용한다. 특히 우크라이나군은 스타링크 위성 인터넷 서비스가 지원되지 않는다면 군사작전을 수행할 수 없을 것이다. 정찰드론으로 표적을 식별하고 타격수단에 표적정보를 인계하여 정밀타격하는 표적탐지 및 타격체계는 스타링크 없이는 불가능하다. 또한 각 군을 연결하고 지휘하는 지휘통제통신시스템도 위성인터넷을 기반으로 운용되기 때문이다.[41]

2022년 4월 14일 모스크바함 침몰 사건은 러시아에 굴욕감을 준 심리전 효과를 낳았다. 사용된 무기체계는 넵튠(Neptune) 미사일로 이 또한 스타링크 시스템에 의해 운용되었다. 러시아는 스타링크에 대한 전파방해 공격을 시도했으나 스타링크는 코드를 수정하여 공격을 무력화시켰다. 스타링크라는 위성인터넷 운영 플랫폼의 중요성을 여실히 보여주고 있다.

정보심리전 수행을 위해 사이버 공간에서 플랫폼 확보는 필수적이다. 서방의 IT 기업들이 대다수 플랫폼을 독점하여 우크라이나에 불리한 전쟁정보와 내러티브 확산은 제한되었다. 반면 러시아에 불리한 전쟁정보와 내러티브는 확산되었다. 세계의 유명 SNS 플랫폼은 페이스북, 구글, 유뷰트, 틱톡 등이다. 이러한 매체가 러시아 관영매체의 기사를 차단했다. 서방의 IT 기업들은 우크라이나인이 사용하는 SNS 채널 네트워

40) 홍규덕, 앞의 논문, pp.63-66.

41) “WP 머스크의 스타링크 위성 인터넷, 우크라 생명줄”, 뉴시스(2023.09.20.), https://v.daum.net/v/20230920095914249(2023.09.25.)

크를 폐쇄했다. 러시아가 우크라이나와 국제사회에 보내는 정보심리전 메시지가 제한되어 정보심리전의 한계를 가져왔다.[42]

비트코인 채굴 3위인 러시아는 스위푸트(SWIFT: 국제은행간통신협회결제망)에서 차단되자 가상화폐를 전쟁자금으로 동원했다. 미 재무부 해외자산통제국은 즉각 러시아의 가상화폐와 연관된 회사와 개인을 제재명단에 올려 제재했다. 러시아와 우크라이나는 대체불가토큰(NFT)을 이용해 전쟁자금을 모금하는 등 블록체인 기술을 이용한 가상화폐 영역에서도 디지털 플랫폼 경쟁이 벌어졌다.

2. 전세

러시아의 정보심리전이 효과를 거두지 못한 가장 큰 이유는 '명분 없는 전쟁'을 수행한 데 대한 국제사회의 반발이다. 이는 과거 지속적으로 서방과 동유럽에서 반복한 러시아 내러티브의 기만성에 대한 학습효과에 기인한다. 또한 세계 IT 기업이 러시아發 담론이 국제사회에 확산되지 않도록 러시아 관영매체의 콘텐츠를 차단한 반면 우크라이나의 담론은 확산되도록 지원했기 때문이다.

반면 우크라이나는 2014년 러시아의 침공에 대한 학습효과로 인하여 효과적인 반격 내러티브를 시의적절하게 내보냈다. 젤렌스키 대통령은 이러한 내러티브를 효과적으로 프레이밍했고, 서방은 러시아의 군사정보를 우크라이나에 제공하여 우크라이나가 정보우위를 누릴 수 있게 하였다. 세계 IT기업이 우크라이나의 정보심리전 담론이 우세할 수 있도록 도왔고 우크라이나 시민들의 소셜미디어를 사용한 정보심리전 가담 등으로 러시아보다 성공적인 정보심리전을 이끌수 있었다.[43]

러시아-우크라이나 전쟁의 정보심리전이 전세에 미친 영향을 정리해보면 첫째, 러시아의 명분없는 전쟁에 대한 국내반발을 들 수 있다. 러시아 정부는 전쟁 목표와 명분을 군인들에게 제대로 제공하지 않은 채 전쟁을 개시함으로써 명령불복과 사기저하 문제를 지속적으로 노출하였다. 러시아는 국내 반전여론과 자국 군대의 반발을 무마하기 위해 펼친 정보심리전이 전쟁의 실패요인으로 작용하게된 것이다. 전쟁 초기 우크라이나 공격을 '특수 군사작전'이라고 주장함으로써 해외정보에 노출된 국민들을 설득하지 못한데 기인한다. 러시아 군인들은 명령이행을 거부하거나 무기를 고의적으로 파괴시키는 등 전쟁의 목적과 명분을 상실하고 사기가 심각하게 저하되는 결과를 가져왔다.

러시아는 전쟁의 절대 조건인 국내 대중의 전쟁지지 여론을 얻지 못했고, 대규모

---

42) 홍규덕, 앞의 논문 참조

43) "Truth is Another Front in Putin's War", *The New York Times,* March 20, 2022. https://www.nytimes.com/2022/03/20/world/asia/russia-putin-propaganda-media.html?partner=naver(2023.03.21.)

국내 반전시위가 일어나 소셜미디어의 국내 접속을 차단하고 언론을 검열하며 시위대를 탄압하게 되었다. 모스크바에서 3천 명이 넘는 러시아 시민이 체포되었고, 피터스버그에서도 2천 명 이상의 시민이 체포되었다.

둘째, 러시아 내러티브에 대한 학습효과에 대한 반감과 우크라이나 내러티브의 선전을 들 수 있다. 러시아의 내러티브에 대한 학습효과는 러시아의 정보심리전의 가장 큰 실패요인이다. 2016년 이후 서방을 대상으로 빈번하게 전개한 허위조작정보 활동을 통한 선거개입과 2014년 우크라이나 침공 이후 지속해온 우크라이나에 대한 심리전은 서방과 우크라이나로 하여금 러시아의 심리전 전술을 분석하고 연구하게 하였다. 러시아 관영매체의 보도나 러시아 정부의 주장은 정보로서의 가치를 상실한 것이다. 러시아 發 가짜뉴스가 고도의 설득기제를 통해 생산되고 유포되어도 우크라이나와 서방은 러시아의 정보 자체를 신뢰하지 않은 결과를 가져온 것이다.

디지털 공간의 영향공작 활동을 분석하는 워싱턴 DC 소재 조사기관 Omelas는 2월 24일 러시아가 우크라이나로 진입하면서부터 러시아 미디어의 영향공작이 목표청중(target audiences)을 견인하지 못했다고 분석했다. 러시아 관영매체는 소셜미디어에 12,300개의 콘텐츠를 게시하여 130만 명의 청중이 있었으나 서방 매체는 총 116,000개의 콘텐츠를 통해 4천4백8십만 명의 청중이 있었다. 이는 러시아가 영어 정보에 있어서 서방을 압도할 수 없었던 데 기인한다.

반면 우크라이나는 젤렌스키 대통령이 주도하고 우크라이나 시민들이 가세하여 반격 내러티브를 지속적으로 발신했고 전황에 대한 신속한 정보 제공을 통해 정보전에서도 우위를 누릴 수 있었다. '푸틴 vs. 민주주의의 대결', '작지만 강한 우크라이나', '용감하고 일치단결된 우크라이나 군과 시민', '거짓말쟁이 러시아'등의 공격적인 프레이밍을 지속적으로 내보냈다.[44]

셋째, 서방 IT 기업의 온라인 플랫폼 독점에 따른 결과이다. 이를 통해 러시아는 정보심리전을 제대로 전개하지 못하는 결과를 초래했다. 또한 러시아의 공격으로 통신이 파괴된 우크라이나는 일론 머스크(Elon Musk)의 스타링크(Starlink)와 미국 국제개발처(USAID)의 도움으로 우주인터넷 서비스를 제공받아 정보심리전을 전개할 수 있었다.

Facebook, Instagram, YouTube, TikTok과 같은 소셜미디어를 운영하는 Meta나 Google이 RT, Sputnik, TASS와 같은 러시아 관영매체를 차단했다. 또한 이들 매체의 미국내 직원들을 모두 해고하는 등 세계적 IT 기업들이 온라인 공간에서의 러

44) "Russia has the tanks and troops. Ukraine has zelensky," CNN. March 9, 2022. https://us.cnn.com/2022/03/09/opinions/volodymyr-zelensky-ukraine-message-house-of-commons-ghitis/index.html(2023.03.21.)

시아 發 내러티브 확산을 물리적으로 차단하는 조치를 취하였다. 우크라이나인을 대상으로 하는 Facebook, Instagram, Twitter, YouTube, Telegram, Odnoklassniki, VK 계정, 그룹, 페이지, 채널들의 네트워크가 모두 폐쇄되고 수상한 채널들도 삭제되었다.

EU도 러시아 관영매체의 콘텐츠 송출을 금지했다. 심지어 우크라이나 에이스 파일럿의 러시아 전투기 격추 영상이 허위조작정보로 알려졌음에도 불구하고 트위터사는 우크라이나 정부가 게시한 해당 영상과 우크라이나 전대통령 페트로 포로셴코(Poroshenko)가 게시한 2019년 국방부 영상에 오정보에 지정하는 “out of context” 플래그를 지정하지 않았다.[45)]

마지막으로 서방의 우크라이나 정보심리전 지원이다. 서방은 전쟁 시작 전부터 러시아의 민감한 전쟁정보를 선제적으로 노출하고 전쟁에 대한 내러티브를 장악하는 방식으로 러시아가 이번 전쟁의 내러티브를 정의하지(define) 못하게 막았다. 서방은 푸틴의 전쟁을 ‘실패하는 전쟁(a failing war)’의 이미지로 규정했고, 이러한 프레이밍은 우크라이나의 러시아에 대한 항전 의지를 증진시켜주는 효과를 가져왔다.

Ⅳ. 정보심리전의 독도 적용 및 방어전략

1. 한국의 정보심리전 전략과 대비태세

한국의 미래 정보전 대비 전략개념은 없다. 정보전 능력 측면에서 한국은 일본과 비슷하나 일본에 비교하여 훨씬 더 많은 사이버 침해사고와 범죄가 발생하고 있다. 특히 사이버테러 취약국으로 분류된 한국은 중국과 대만처럼 적극적인 대응과 대책 마련은 전무하다. 국방부, 국정원은 지속적으로 사이버테러나 가상적국으로부터의 사이버 위협에 대한 대응책 마련을 강조해 왔지만 구체적인 정보전 전략이 제시된 바 없다.[46)]

법·제도적 측면에서 살펴보면 2013년 4월 ‘국가 사이버안전 전략회의'를 개최하고 청와대, 국가정보원, 국방부 등 정부부처가 “국가 사이버안보 종합대책”을 수립하여 4대 실천전략을 채택하면서부터 시작되었다. 청와대가 'Conitrol Tower'를 맡고 국가정보원이 총괄적인 실무를 담당하며 관련 행정기관이 소관 업무 분야를 담당하는

45) “40대 격추도, 전사도 모두 허구...키이우의 유령은 없었다”, 연합뉴스(2022.05.03.), https://www.youtube.com/watch?v=Xd4bmdNq0Ck(2023.04.08.)

46) 이용석; 정경두, “러시아 대 우크라이나 사이버 전쟁의 교훈과 시사점”, 『국방정책연구』, Volume 137(2022.), pp.68-70.

국가적인 대응체계가 구축된 것이다.

사이버정보 공유를 위한 'Smart 협력체계' 구축, 국가 기반시설에 대한 사이버침해에 대응하기 위한 위기대응훈련, 국가기반시설에 대한 망 분리 운영, 사이버안보 전문가 양성사업 및 영제 교육원 설립을 추진하였다.[47)]

2014년 '초연결 Digital 혁명 선도국가' 실현 비전으로 '사물 인터넷 기본 계획'을 확정하였고, '초연결사회 도래에 따른 사물 인터넷 정보보호 로드맵' 발표 등이 이어졌다. 2015년에는 'K-ICT Security 발전전략'을 발표[48)]하고 "정보보호 산업의 진흥에 관한 법률"을 제정하였다.

2016년에는 "국민보호와 공공안전을 위한 테러방지법"을 제정하는 등 loT 사회에 대비하기 위한 법·제도적 노력을 꾸준히 진행하였다. 그러나 관련법들이 정보Service와 주요 기반시설 영역에만 제한적으로 적용되어 사이버공간 전체를 포괄할 수 없어 민·관·군 통합 사이버안보 추진을 위한 근거가 미흡했다.

정보보호 및 사이버전 대응 관련 법들은 개별 입법으로 사이버보안 활동에 혼란이 가중되어 정비가 필요했다. 정보보호 및 사이버전을 규율하기 위한 상위법을 제정하고 그 법에 따라 하위 관계법들을 제정하여 상하관계를 일치시키고 법률의 동일한 해석과 적용이 요구되었다.

2018년 12월 문재인 정부에서 처음으로 국가안보전략을 수립하고, 이를 근거로 2019년 4월 국가사이버안보전략을 발표하였다. 9월에는 사이버안보 관련 대한민국의 최상위 지침서인 국가사이버안보전략을 차질 없이 추진하기 위해 법부처 차원에서 이행할 국가사이버안보 기본계획을 확정했다. 정부는 사이버안보 6대 전략과제를 뒷받침하기 위해 기관별 실행계획을 18개 중점과제, 100개의 세부과제로 종합하고 2022년까지 단계적으로 추진할 계획이다.

---

47) 최영관, 조윤오 "우리나라 사이버 테러 실태 및 대용 방안에 관한 연구: 경찰 사이버보안 전문가를 대상으로", 『한국경찰학회보』, 19권(2017.), p. 210.

48) 미래창조과학부, "K-ICT 시큐리티 발전전략", https://www.kisa.or.krhoticenoticeVewsp!mode=view&p_No=4&b_No=4&d_No=1556(검색일: 2023.08.23.)

전략과제	중점과제	세부 과제수
국가 인프라 안전성 제고	❶국가 정보통신망 보안 강화 ❷주요정보통신기반시설 보안환경 개선 ❸차세대 보안 인프라 개발	24
사이버공격 대응 고도화	❹사이버공격 억지력 확보 ❺대규모 공격 대비태세 강화 ❻포괄적 능동적 수단 강구 ❼사이버범죄 대응역량 제고	28
협력 기반 거버넌스 정립	❽민관군 협력 체계 활성화 ❾범국가 정보공유체계 구축 및 활성화 ❿사이버안보 법적기반 강화	16
사이버보안 산업 성장	⓫사이버보안 투자 확대 ⓬보안 인력기술 경쟁력 강화 ⓭보안기업 성장환경 조성 ⓮공정경쟁 원칙 확립	14
사이버보안 문화 정착	⓯사이버보안 인식 제고 및 실천 강화 ⓰기본권과 사이버안보의 균형	9
국제협력 선도	⓱양다자간 협력체계 내실화 ⓲국제협력 리더십 확보	9
합 계	18	100

<표 1> 사이버안보 전략별 기본계획의 주요내용[49)]

기본계획의 주요내용을 살펴보면 첫째, ‘국가 핵심 인프라 안전성 제고’ 측면에서는 국가 정보통신망과 주요정보통신시설의 보안환경 개선으로 생존성과 복원력을 강화하고 안전하고 편리한 차세대 보안인프라를 개발·보급하여 국가 핵심 인프라의 안전성을 높이겠다는 전략이다.

둘째, ‘사이버공격 대응역량 고도화’의 경우 사이버공격을 사전에 효율적으로 억지하고 사고발생시 신속하고 능동적으로 대응할 수 있도록 민·관·군 합동 대응체계를 강화하는 등 사이버위협 대응역량을 지속적으로 고도화하겠다는 것이다.

셋째, ‘신뢰와 협력기반 거버넌스 정립’ 측면에서는 개인·기업·정부 간의 상호 신뢰

49) “국가사이버안보전략 기본계획 확정...18개 중점과제, 어떤 내용 담겼나”, 보안뉴스(2019.09.03.), https://www.boannews.com/media/view.asp?idx=82713(2023.09.11.)

와 협력을 바탕으로 국가 차원의 정보공유 시스템을 활성화하고 지자체, 중소기업, 정보보호지원센터 등과 협력하는 등 종합적인 사이버안보 거버넌스를 만들어나갈 방침이다.

넷째, '사이버보안 산업 성장기반 구축'을 위해서는 사이버안보의 핵심역량이 되는 기술, 인력 및 관련 산업의 경쟁력을 확보하기 위한 인력양성 프로그램, 연구개발 활동 등을 통해 혁신적인 보안산업 생태계를 만들겠다는 전략이다.

다섯째, '사이버보안 문화 정착'의 경우 국민 모두가 사이버안보 중요성을 인식하고 실천하며 정책 수행 과정에서 기본권을 존중받고 국민들의 참여와 신뢰를 보장할 수 있는 사이버보안 문화를 정착시킨다는 계획이다.

여섯째, '사이버안보 국제협력 선도'를 위해서는 다양한 국제협력을 통한 파트너십을 강화하고 국제규범 형성을 주도하는 등 사이버안보를 위한 국제협력을 내실화하겠다는 계획이 지난 번 발표된 6대 전략과제를 이행할 18개 중점과제에 포함됐다.

이를 통해 해킹, 정보 절취 등 증가하는 사이버위협에 대응하여 사이버 공간에서 국민이 안전하고 자유롭게 활동할 수 있는 환경이 마련될 수 있는 기반이 조성되었으나 "사이버안보기본법" 제정은 여전히 표류 중이다.

2023년 윤석열 정부는 국가사이버안보전략서를 발표하며 사이버전에 대한 대응 중심의 수세적 개념에서 탈피해 선제적·능동적 작전개념으로 발전시키고 우수한 사이버 전문인력을 육성할 수 있는 시스템을 시급히 발전시켜야 한다고 강조했다.[50] 그러나 역시 사이버안보기본법 제정과 함께 현재 통합방위법에 사이버안보 분야와 관련된 조항이 없어 법규 보완이 필요하다. 정부의 컨트롤타워 역할도 사이버안보 업무의 통제보다는 사이버안보 전략과 능력을 건설하는 것에 중점을 두어야 한다.

통합방위법 개정을 통해 국가 사이버 대응조직도 구성할 수 있어야 한다. 사이버작전사령부와 정부기관의 사이버 인력, 민간 보안인력 등을 포함하여 범국가사이버조직을 운용할 수 있어야 한다. 사이버예비전력을 지정하여 운용하는 방안도 포함되어야 한다. 사이버 통합방위사태 선포기준을 마련하고 단계별 자원 동원 및 대응체제를 구축해야 한다. 이들은 평시 사이버상황에 대한 정보공유와 합동훈련을 통해 즉응대응력을 유지할 수 있도록 법률에 명시해야 할 것이다.

국가정보원은 2020년 개정된 국가정보원법에 따라 사이버안보를 주된 직무로 명시하고 사이버범죄, 사이버테러, 사이버전 등에 대한 단계별 대응절차를 마련하고 있다. 이를 위해 NSC, 국정원, 국방부 및 정보통신부와 효율적인 업무분장과 기능 강화를 위해 체계적인 종합대응체계를 구축하고 있다.

---

50) "우리나라의 국가사이버안보전략, 사이버 보안 강대국 사례와 비교해보니", 보안뉴스 (2023.08.03.), https://www.boannews.com/media/view.asp?idx=120106

국방부는 현대 정보전의 중요성을 인식하고 정부의 대응태세보다는 진일보한 대응태세를 강구하고 있으나 미국이나 중국의 능력과 체계에는 미치지 못한다. 국방부는 사이버안보의 중요성을 반영하여 업무 소관부서를 조정했다. 사이버안보 정책업무를 기획조정실(정보화기획관에서 국방정책을 총괄하는 국방정책실(방위정책관)로 이관했다. 합참 역시 사이버 작전업무를 군사지원본부(사이버지휘통신참모부)에서 군사작전을 주도하는 작전본부(작전기획부)가 담당하도록 했다. 국방부, 합참 차원의 통합된 정보전 전담조직을 편성하고 전략개념과 교리 개발, 전문인력 양성이 요구된다.[51] 또적의 사이버침해를 사전에 방지하기 위하여 민·관·군은 유기적인 정보공유체계가 갖추어져 있어야 한다. 정보공유의 시기와 수준이 법률로 규율되어 있어야 국가 행위가 법 안정성을 갖게 된다.

사이버기술 확보 및 연구개발은 2000년 1월에 '국가보안기술연구소(NSR)'를 설립하면서 시작되었다. 이를 통해 사이버전에 대비하기 위한 국가급 연구개발 수행체제를 마련했다.

우리나라는 국가 및 공공기관에 대한 보안관제를 통해 사이버공격 탐지·차단체계를 운영한다.[52] '국가 사이버안전 Center'는 단위 및 부문 보안 관제 Center에게 사이버공격 탐지기술을 배포하고 국가안보에 위협이 되는 사이버 공격을 탐지·대응한다.

우리나라는 낮은 보안기술 경쟁력[53]을 갖고 있음에도 불구하고 새로운 보안기술을 확보하기 위한 R&D 투자는 미미하며, 정보보호 관련 인증제도의 도입 분야 등에서 미흡한 부분이 식별되고 있다.

국가차원의 사이버방호 역량 제고와 사이버전문 인력 양성을 위해 국가보안기술연구소 산하에 '사이버 안전훈련 Center'를 설치하여 정보보안 실무교육, 사이버위협 대응훈련 등을 하고 있다. '사이버보안 인재 Center는 실전형 사이버훈련장을 운영하여 매년 2,000여 명의 국가 사이버보안 인력을 양성하고 있다. 정보보호 인력 수급정책을 살펴보면 보안설계, 단말보안, 사이버협력보안 등 사회 제 기능을 망라한 융합보안 전문 인력의 수요는 증가하고 있으나 정책적인 반영은 미흡하다.

국외협력활동 측면에서 살펴보면 사이버침해는 공격자를 특정하기 어렵고 타국과의

---

51) "변재선 전 국군 사이버사령관, 사이버작전사령관에 전문가 보직시키고 사이버전 개념과 전략 장기간 연구해 발전시킬 연구집단 필요", 뉴스투데이(2023.06.27.), https://www.news2day.co.kr/article/20230627500126(2023.09.21.)

52) 보안관제는 각급 기관에서 수행하는 단위 보안관제 Center, 중앙행정기관에서 수행하는 부문 보안관제 Center(35개소), '국가 사이버안전 Center'에서 수행하는 국가 보안관제로 3단계 체계를 유지한다.

53) 국방기술품질원이 2016년 우리나라 사이버기술 수준을 평가한 결과 사이버감시정찰기술 74%, 사이버지휘통제기술 76%, 사이버방호 기술 80%, 사이버훈련 기술은 77%, 공통기반 기술 82%로 평가되었다.

협력이 필수적이기 때문에 긴밀하고도 적극적인 국제공조는 필요한 조치다. 한국은 '부다페스트협약'[54] 가입을 추진한 지 5년 만인 2023년 6월 유럽평의회로부터 정식 가입 초청서를 받았다. 협약 가입으로 디지털 증거 관련 국제 공조 수사 절차가 원활해지면 해외 거점을 둔 보이스피싱, 디지털성범죄, 랜섬웨어 공격 등 늘어나는 디지털 사이버 범죄 대응력이 강화될 것으로 판단된다. 국제공조가 가능해지면 조약 가입국 간의 긴밀하고 신속한 협조를 통해 사이버침해 공격자를 특정할 수 있게 된다.

2. 한반도 주변 강대국의 사이버전략과 능력

가. 미국

미국은 911테러 이후 2001년 "애국법(Patriot법)"이 제정되어 미국의 연방기관은 민간의 전화선, internet, 전자 Mail, Web Surfing 등 모든 전자통신에 대한 추적 권한을 가지게 되었다.[55] 더불어 국가안보 위험활동, 조직범죄, 누군가에 대한 살인, 중대하고 급박한 위험이 있는 경우 영장 없이도 전자감시를 할 수 있게 하였다. 2002년 애국법을 보완하기 위해 "공공안전과 사이버 보안강화법(The Public Safety and Cyber Security Enhancement Act of 2002)" 이 제정되었다.

2002년 11월 25일 두 법을 묶어 "국토안보법(The Homeland Security Act)"을 제정했다. 이 법은 사이버테러[56]를 포함한 모든 테러로부터 미국의 기반시설을 보호하기 위해 총 17편으로 구성되었고 2편에 사이버보안, 10편에 정보보안을 별도로 규정하고 있다. 같은 해에 정보보호 및 대테러 업무를 총괄하는 국토안보부를 창설하였다. 특히 미국은 사이버보안과 관련된 조항을 무려 50여개의 법률에 포함시키거나 직접 법률로 공포했다.

2011년 국방부에서 발표한 "사이버공간에서의 국방부 작전전략(Department of Defense Strategy for Operating in Cyberspace)"[57]은 5가지 전략적 주도권(Strategic Initiative)을 제시하고 있다.

첫째. 사이버공간을 새로운 작전영역으로 명확히 인식하여 사이버공간을 최대한 이용할 수 있도록 조직하고 훈련하며 장비를 확보한다. 둘째, 사이버보안을 강화하고 새로운 작전개념을 채용하여 국방부의 Network와 System을 보호하기 위한 안전한

54) 2001년 11월 23일 유럽평의회(COE : Coundl of Europe) 주도로 체결한 "사이버 범죄조약(The Convention on Cyber Crime)"으로 일명 'Budapest 협약(Budapest Convention)'이라고 한다.

55) 패트리어트법의 정식 명칭은 Uniting (and) Sitrengthening America (by) Providing Appropriate Tools Required (to) Intercept (and) Obstruct Terror Act of 2001이다.

56) 최영관, 조윤오 위의 논문 pp. 208-209.

57) 2010년 수립된 "국가안보전략"과 4년 주기로 수립되는 "국방검토보고서(QDR)"의 사이버안보 내용에 기초하여 사이버 공간에서의 국방부 작전전략을 발표했다.

사이버공간 상태를 확보한다. 셋째, 미 정부기관 및 기구는 민간부문과의 협력을 통해 범정부차원에서 총력적인 대응을 한다. 넷째, 전 세계가 그물망처럼 연결된 정보화 시대에 개별국가의 능력으로 사이버공격에 대응 한다는 것은 쉽지 않기 때문에 동맹국, 협력국 및 민간영역과의 협력을 강화한다. 이를 통해 집단적 자위권과 집단적 억지를 구현하고자 하고 있다. 다섯째. 사이버안보역량은 개인의 역량과 밀접한 관계를 갖고 있기 때문에 우수인력을 확보하고 첨단 ICT 기술을 따라가기 위하여 HW적인 측면과 SW적인 측면에서 진보된 기술을 신속히 반영함으로써 지속적인 장비 Upgrade를 한다는 것이다.

오바마 정부는 사이버작전과 사이버작전 수행을 위한 법적 기반을 마련한 정부로 평가받고 있다. 첫째, “사이버정보공유 보호법(CISPA : Cyber Intelligence Sharing and Protection Act, 2012. 4)”이다. 이 법은 공공및 민간이 사이버위협에 공동으로 대처하기 위해 정보공유 기반을 마련하고자 제정된 법이다. 둘째, “국가 사이버안보 보호법(NCSPA : National Cybersecurity Protection Act. 2014.12)”이다. 이 법은 국토안보부 산하에 국가 사이버안보 및 당신 통합센터를 설치하여 사이버 위협정보를 공유하는 중 연방정부와 민간의 접점 역할을 수행하기 위한 법이다. 셋째, “사이버보안 강화법(CEA : Cybersecurity Enhancement Act. 2014)”이다. 이 법은 사이버위험을 감소시키기 위한 표준 및 절차수립을 보장하는 공공•민간 협력체계를 마련하고 사이버 안보 관련 연구개발과 교육, 인력양성, 인식제고, 기술표준 등을 추진하기 위해 제정되었다. 넷째, “사이버보안 인력평가 법(CWAA : Cybersecurity Workforce Assessment Act, 2014)”이다. 이 법은 국토안보부의 사이버안보 인력의 역량을 평가할 수 있도록 기반을 마련하고, 사이버안보 인력확보 전략과 역량강화 전략 등을 추진하기 위해 제정하였다.

2015년 12월 18일에는 “사이버보안법 (Cyber security Act of 2015)”이 제정되어 효과적인 사이버보안 정보공유 체계를 구축하고, 민·관의 정보공유 활성화를 꾀했다.

2018년 9월 20일 “미국의 국가 사이버전략(National Cyber Strategy of the United States of America)”을 발표했다. 미국이 추구하는 사이버정책의 핵심목표는 첫째, 연방 Network 및 정보 보호 둘째, 중요 Infra 보호 셋째, 사이버범죄 퇴치 넷째, 사이버침해 보고 개선을 위한 구체적인 조치 강구이다. 사이버 위협에 대한 보호 우선순위는 첫째, 국가보안 둘째, 에너지 및 전력 셋째, 은행 및 금융 넷째, 보건 및 안전 다섯째, 통신 여섯째, 정보기술 일곱째, 운송이다.

이를 위해 먼저 미국의 번영을 촉진해야 한다. 활기찬 Digital 경제를 육성하고 미국의 독창성을 유지하며 사이버보안 인력을 개발하고 확보한다. 둘째, 힘을 통해 평

화를 유지한다. 책임 있는 국가 행동규범을 통해 사이버안정성을 강화하고 사이버공간에서 용납할 수 없는 행위에 대해 확실한 거부의사를 밝힌다. 셋째, 안전한 인터넷 공간에 대한 선구자적인 영향력을 유지한다. 개방적이고 신뢰할 수 있는 안전한 인터넷을 유지하며 국제 사이버역량을 구축한다.

미국은 사이버공간에서 미국의 우위를 지키면서, 국익의 안정을 해치거나 국익에 반하는 사이버공간에서의 행동을 파악, 대응, 교란, 저하, 억제한 것이다. 이를 위해 미국은 지구촌의 모든 국가들에 대하여 책임 있는 국가행동의 규범과 허용할 수 없는 사이버공간 행동의 속성을 파악하고 사이버공간에서 악의적인 행위자들에게 비용을 부과하여 미국의 사이버안정을 증진하겠다고 강조한다.

미국은 사이버공간에서도 물리적인 상황과 마찬가지로 영향력을 지속 증대할 것 이다. 미국은 인터넷의 개방성, 상호운영성, 보안, 신뢰성의 보존을 통해 미국의 이익을 강화한 것이며 이 목표를 달성하기 위해 전 지구적인 노력을 할 것이라고 천명하였다. 또한 Infra 및 유망 기술의 발달을 지원하고 국제적인 사이버역량을 구축하겠다고 하였다.

미 국가 사이버전략은 사이버공간을 지켜나가기 위해 미국의 Partner 국가들과 시민사회. 민간부문을 포함하는 여타 단체들과 협력하여 혁신, 개방, 효율을 높이는 정책을 수립하기로 하였다. internet Governance는 다중이해당사자(multi-Stakeholder) 모델을 지지하고 실체 없는 사이버보안 우려를 Digital 보호주의의 구실로 이용하는 것을 배격한다고 하였다. 미국은 또한 국제 Partner들의 사이버역량 구축에 최선을 다하여 Partner들의 국가 사이버보안 전략의 수립 및 집행. 사이버범죄 대치. 사이버보안기준 수립, 사이버위협으로부터의 중요 infra 보호를 지원하기로 하였다. Internet에서의 자유는 국가 사이버전략의 혁심 원칙이며 미국은 다양한 해외원조 Program을 통해 이를 촉진시키고 있다. 30개 국 정부로 구성된 자유 온라인 연합(Freedom Online Coalition)이 대표적 활동이다.[58)]

미국의 사이버전략은 일부 국가의 악의적 사이버활동에 대처하고 있으며 미국 및 미국의 Partner들에게 사이버피해를 끼치는 사이버 행동교란에 대해서는 반드시 대가를 치르도록 하겠다는 의지를 밝히고 있다. 이는 중국이 일대일로 정책으로 연선국가에 대한 사이버지원과 사이버공동체 구축을 통해 세력화하는 것을 경고한 것이다. 이를 위해 Partner 국가 및 동맹국과의 협력을 통해 국제법과 평화 시에 적용되는 책임 있는 국가행동에 대한 자발적인 비구속적 규범을 준수할 것을 요구한다. 또 악

58) 시민사회, 민간부문, 기타 이해당사자들과의 협력과 다자간 외교를 통해 Internet 자유를 발전시키기 위해 30개 국 정부가 연합하여 결성. 연합 회원들은 외교적 노력 을 조정하고 시민사회 및 민간부문과 긴밀히 협력하여 전 세계 Intemet 자유표현, 협회, 집회 및 개인정보보호의 기본 인권을 보호하기 위해 함께 노력하는 정부 단체이다.

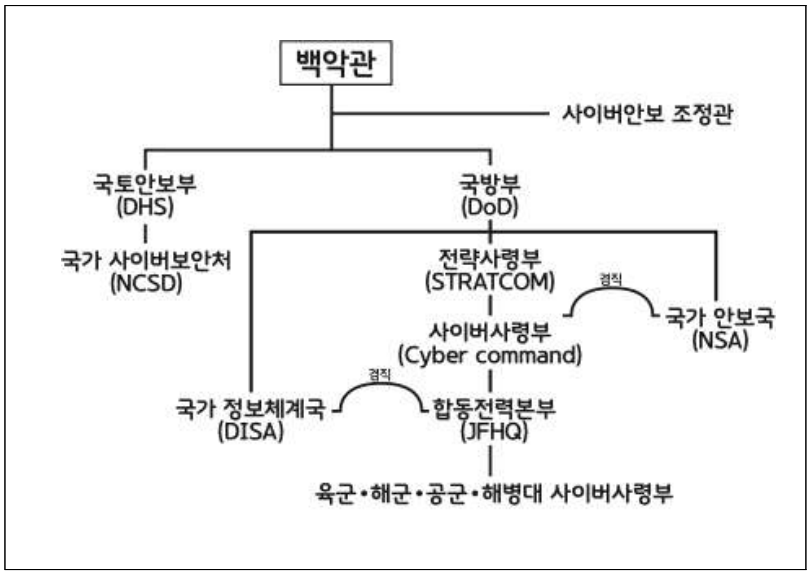
의적 사이버활동으로 인한 갈등의 위험을 줄일 수 있도록 실질적 신뢰구축 조치의 이행을 지원하겠다고 명시하고 있다.

미 국방부가 2011년 5월 발표한 “사이버보안을 위한 국제전략”에서 사이버공간에 대한 기본원칙을 확립[59]하고 국제적인 공조체제를 강화하는 계기를 마련했다. 7월 발표한 “사이버공간에서의 국방부 작전전략”에서는 사이버공간에서 적극적인 방어를 하겠다고 명시했다. 오바마대통령은 2013년 대통령 행정명령 20호[60]를 발령하여 국가기간망을 흔드는 사이버공격을 전쟁행위로 간주하고, 이러한 사건이 발생하면 경고없이 무력으로 대응한다는 방침을 밝혔다. 미 국방부는 2015년 4월에 “국방 사이버전략(The DoD Cyber Strategy)”을 통해 사이버공간을 기존 물리적인 공간과 동일하게 취급하여 물리적인 군사력도 사용하겠다는 구상을 발표하였다.

미국의 사이버전 역량 구축은 1990년대 냉전이 종식되면서 시작되었고, 사이버전 수행 중심기관은 미국국가안전보장국(NSA)이었다. 핵심임무는 컴퓨터네트워크작전(CNO)으로 어떤 상황에서도 정보우위를 점하는 것이다. 911 테러 이후 각 정보기관에 분산되어 있던 사이버전 수행기구를 정부기관 및 민간기관과 국방 분야로 구분하여 통합하였다. 정부기관 및 민간분야는 국가 사이버보안처(NCSD)로 통합하였고, 국방 분야는 전략사령부 예하의 사이버사령부로 통합하였다. <그림 2> 미국의 사이버전 수행기관에서 보는 것처럼 사이버안보 조정관을 통해 백악관으로부터 국토부와 국방부간의 유기적인 관계가 형성되도록 하였으며 각 군 사이버사령부까지 통합할 수 있도록 효율성에 주안을 두고 지휘관계를 구성하였다.

59) 사이버공간에 대한 기본원칙은 세 가지로 첫째, 기본적 자유권 (Fundamental Freedoms)의 보호 둘째, Privacy 셋째, 정보의 자유로운 흐름 (Free Flow of Information)이다.

60) 2012년 10월에 오바마대통령이 서명한 이 기밀지침은 2003년에 부시대통령이 서명한 기밀지침인 국가안보지침 (NSPD)-38을 대체하는 것으로 NSA분석관인 Edward Showden에 의해 2013년 6월에 공개되었다.



<그림 2> 미국의 사이버전 수행기관

나. 중국

중국의 사이버안보체계는 크게 3단계로 구분할 수 있다. 첫째, 정보화 도입 및 주력 시기로 1994년부터 2001년까지이다. 둘째, 정보보호, 정보System 안전 확보 중점추진 시기로 2002년부터 2012년까지이다. 셋째, 사이버공간 안보 강조시기로 2013년부터 현재까지이다.

정보보호 및 정보System 안전 확보는 후진타오주석의 지시에 의해 시작된다. 최초 계기는 2003년 3월 "국가 정보화 영도소조" 산하에 '국가 Network 및 정보안전 협조소조'를 설립하도록 지시하면서 부터이다. 협조소조는 2003년 8월 정보안전 보장업무 강화에 관한 의견을 '27호 문건'으로 제시하여 보호제도, 연구개발, 법제구축, 예산편성 등 관련근거를 마련하는 계기를 만들었다.[61]

후진타오주석의 지시에 의해 2006년 5월 "2006-2020년 국가 정보화 발전전략"을 발표하고, 국가 정보보호 체계구축 및 능력 강화방안을 제시한다. 2008년 3월에는 '공업정보화부'를 신설하여 국가 정보보호업무를 주관하도록 하였다. 이 과정에서 '국무원 정보화 판공실'을 해체하면서 부재한 Control Tower를 대신하기 위해 2011년

61) 주요 내용은 첫째, 정보안 전등급 보호제도 실시 둘째, 암호기술의 바탕위에 Network 신뢰 체계 마련 셋째, 정보보호기술의 연구 개발 강화, 정보보호 산업발전 추진 넷째, 정보보호와 관련된 법제 구축, 표준화 System 마련 다섯째, 정보보호 예산은 정보화 예산과 함께 편성 등이다.

5월 “국가 Internet 정보판공실”을 설립하게 된다.

중국의 사이버공간 안보는 사이버전에 대비하고, 정보보호보다 Network 안전을 강조하고 있는 것이 특징이다. 이는 중국사회 전반에 절친 정보화의 가속화, 중국의 Internet기술 낙후, 중국의 Network 관리체계의 문제, 미국 등 사이버 대국과의 경쟁 문제, Edward Snowden 사건으로 중국 지도부 사이버안전 위기감이 고조된 때문이다. 시진핑주석은 2014년 2월 “중앙 사이버안전 및 정보화 영도소조”를 설립하고 획기적인 통합·집권형 사이버 안보체제 구축을 꾀한다. 2014년 4월에는 “총체적 국가안보관”을 발표하면서 '사이버 안전'이 국가안보의 중요한 요소로 등장하게 된다.

시진핑주석이 중앙 국가안전위원회 1차 회의에서 처음 사용한 '총체적 국가안보관'이란 개념은 내부로부터의 안보위협에 많은 경계심을 드러내고 있다. 이후 개최된 “중국공산당 제18기 중앙위원회 제4차 전체회의(18기 4중 전회)”에서 핵심 표제어는 '의법치국(依法治國)'이었다. 이를 배경으로 중국의 사이버안보 관련 법·제도가 확립되기 시작했다.[62] 2015년 7월 '국가안전법'을 제정하였고, 2016년 11월 '사이버안보법'을 제정하여 2017년 6월부터 시행하였다.

‘사이버안보법'은 첫째, 국가의 총체적 국가안전관을 실행하는 중요한 조치이며 둘째, 중국이 직면한 엄중한 사이버 안전의 위험에 대응하고 인민들의 절실한 이익을 지키기 위한 것이라고 설명하고 있다. 이 법은 총 7장 79개 조문으로 구성되어 있다. 주요내용은 첫째. 총칙에서 국가 사이버안보 전략을 수립하고 Network의 안전관리체제를 구축한다. 둘째, 3장에서 Network 운영안전을 보장하기 위해 Network 안전등급 보호제도를 시행하고 Internet 실명제를 법제화 한다. 셋째, 주요 정보기반 시설의 운영보안을 위해 보안심사를 의무화 하고 개인정보와 Data는 중국 내 저장을 원칙으로 한다. 넷째, 4장에서 Network 정보 안전을 위해 Network 운영자의 개인정보 수집절차와 유관기관 보고 의무화를 규정하였다. 다섯째, 경보 및 긴급대응 을 위하여 Network 보안 Monitoring 정보 및 긴급 대응체제를 구축하도록 하였다.

2017년 6월에는 “Network 안전 법(網絡安全法)”을 시행하여 통신, 방송 등 일련의 전파 Service를 제공하는 기반정보 Network와 전력·물·가스 공급망, 금융·의료·사회보장 등 국민생활과 밀접한 중요업계의 정보 System, 군사 Network, 시(市)급 이상의 국가기관 정무 Web site, Service 이용자 수가 많은 Network Service 제공자 및 관리자의 Network System 등을 핵심 정보 Infra로 정하고 이에 대한 사이버규율 체계를 규정하였다.

---

62) 중국은 4중 전회를 계기로 당면 사회문제에 대한 법률을 체계적으로 제정하였고 법률 정비를 통해 반부패 운동이 안정적이고 지속적으로 이어질 수 있도록 했으며 사이버와 관련된 법률도 정비되기 시작한 것이라고 평가할 수 있다.

중국의 사이버전략은 공격적이다. 2008년 이후 Network전과 전자전을 결합하여 Internet 폭탄 등의 공격수단과 전자기 엄폐물 등의 방어수단으로 구성되는 “망전일체전(網電一體戰) 전략”을 수립하였다. 방호용 사이버무기체계로 Windows로 대표되는 미국 운영체제로부터 종속되지 않기 위해 '기린'이라는 독자적인 운영체계를 개발하여 사이버공격에 대한 방어망을 구축하였다. 2007년부터 중국 정부기관과 군, 보안업체들에게 보안상 이유로 '기린'을 사용하도록 통제했다. 중국에서 판매되는 Dell PC의 42%에 '우분투 기린'을 설치하도록 하였다.

중국은 사이버공격무기체계의 독자적인 개발과 운용 능력을 확보하고 있다. 중국산 Router 등의 기술을 확보하고 중간자 “역 추적 악성 공격무기체계(Great Cannon, 萬里大砲)”등을 개발했다. 중국은 통합 Network 전자전(NEW Integrated Network Electronic Warfare)전략을 수립하고 ICT 기초에 관한 인력확보, 논문, 응용분야에 대한 기반역량이 갖추어져 사이버전 핵심기술에 대한 완전한 자립이 가능한 국가로 평가된다.[63]

중국의 사이버공격은 이미 알려진 사례도 많을 뿐만 아니라 사이버공격 실행능력 면에서도 세계 최고 수준임이 입증되고 있다. 국가 차원의 사이버부대를 직접 운영[64] 하고 있으며 전 세계 모든 국가에 대한 해킹 및 정보수집 활동을 감행하고 있다.

중국은 경쟁국인 미국의 사이버방어체계를 무력화 시킬 수 있는 사이버기술을 보유하고 있으며 전 세계에서 가장 많은 악성Code를 개발하고 공격을 수행할 수 있는 인력, 예산 및 기술력을 보유하고 있는 것으로 알려져 있다. 2007년 이후로 중국은 인민해방군 예하의 사이버공격 및 방어를 위한 대책수립에 투자를 아끼지 않고 있으며 총참모부 사이버사령부 예하에 상세 임무가 알려지지 않은 '61398부대' 등을 운영하고 있다.

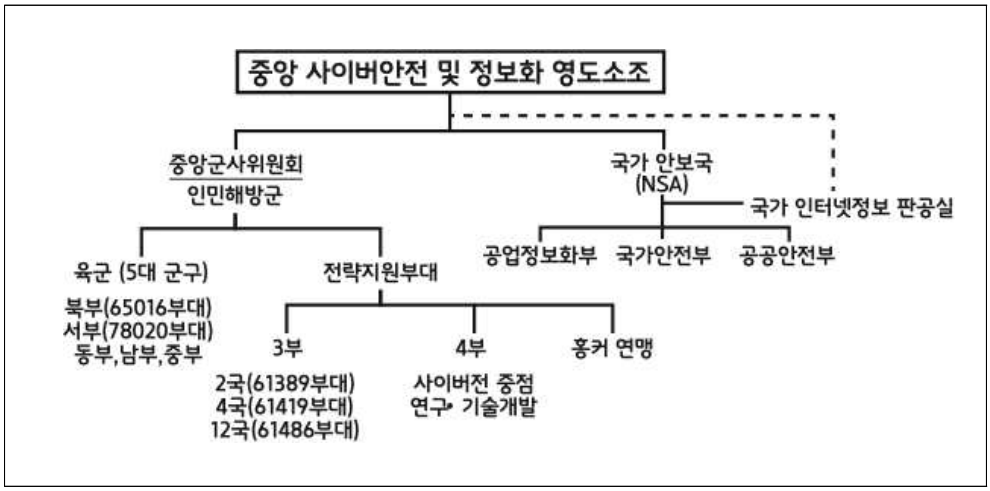
중국 사이버무기체계의 특징은 첫째, 특수한 Internet 구조를 기반으로 한 독자적인 자산이 존재한다는 것이다. 중국 Internet은 국가통제 하에 있으며 1998년부터 운영된 중국의 Digital 공안체계인 Great Firewall을 기반으로 공격을 수행하는 Great Cannon을 보유하고 있다. 둘째, 사이버무기체계의 정보수집용과 공격용의 경계가 불분명하다. 중국 사이버작전 조직의 특성상 민·군 경계가 불분명하며 악성 Code를 통해 개인정보 유출 등의 비군사적 작전과 국가차원의 정보수집, 능동대응 등 군사적 작전을 병행한다. 셋째, 강력한 Internet 통제정책을 통해 자국 내 감시정

63) “中, 만리대포로 홍콩시위 지휘 사이트 집중 공격”, 뉴시스(2019.12.06.), https://newsis.com/view/?id=NISX20191206_0000852792&fbclid=IwAR2XhLh4YLgqeVMRK-fTXgVQQZSZ8ZXbIkeldZfOpT081cjM0hJ8w-Crp7c(2023.09.21.,)

64) 2009년 미국 내 34개 IT 기업을 공격 한 ‘Operation Aurora’의 배후가 중국이라고 Microsoft사에서 발표하였을 정도로 국가 차원의 사이버부대를 운용하고 있다.

찰이 가능하다는 점을 들 수 있다.

<그림 3> 중국의 사이버전 수행기관은 '중앙 사이버안전 및 정보화 영도소조'에서 총괄하며 전략지원부대에서 전자전과 사이버전을 담당한다. 전략지원부대 3부는 평시 정보수집과 유사시 사이버공격을 담당하는 부대로 알려져 있다. 현재까지 확인된 바에 의하면 전략지원부대 2국 (61398부대)은 미국과 캐나다를 대상으로 정치, 경제, 군사정보를 수집하며, 4국(61419부대)은 한국과 일본을 대상으로 정보 수집을 하고, 12국 (61486부대)은 미국과 유럽의 신호정보를 집중 수집하여 산업기밀을 생산하고 있다. 전략지원부대 4부는 1990년에 설립되었으며 전자전과 Network 공격 등 사이버전을 중점적으로 연구하고 있으며 사이버무기체계와 관련된 기술을 전담 개발하고 있다.



<그림 3> 중국의 사이버전 수행기관

다. 러시아

러시아는 1996년 3월에 제정된 “컴퓨터 정보영역에서의 범죄에 관한 법(Crimes in the Sphere of Computer Information)]”에 비인가 컴퓨터정보에의 접근, 부당한 컴퓨터 Program의 제작·사용·배포, 컴퓨터 System 또는 Network 운영규칙의 위반 등 사이버범죄 대응을 위한 사안들이 포함되어 있다.

이러한 형사법적인 규정은 타인의 사이버정보에 대한 불법적인 접근과 유해한 컴퓨터 Program의 제작·사용·유포 등의 범죄를 처벌하는 법적인 근거가 되고 있으며 컴퓨터 System 및 Network 운용 규정에도 적용되고 있다. 러시아는 1995년에 전화, Internet 통신에 대한 FSB의 감청을 허용하는 법을 제정하였고, 이를 위해 1996년

운영적 조사활동을 위한 시스템(SORM; System for Operative Investigative Activities)-1, 1998년에 SORM-2를 설립하였다. 정보통신부장관은 2000년 “130호 명령(전화기, 휴대폰, 무선통신, 무선호출망에서의 조사활동을 보장하는 기술적 수단의 도입)”을 법제화 했다. 2014년에는 SORM-3의 감청기능을 지원하기 위한 요구사항을 발령하고 2015년에는 SORM-3에 대응하는 장비들을 설치하였다.

이외의 사이버 안보와 관련하여 러시아가 원용하고 있는 법은 2006년 7월에 발효된 러시아 연방법인 “정보, 정보기술 및 정보보호법”이다. 이 법은 각 기관이 정보체계를 구축할 때에 보안대책을 구비하고 접근이 통제된 정보에 대해서는 비밀성을 지키며 동시에 적절한 정보 접근을 구현하기 위한 기술적, 법률적 조치들을 담고 있다. 그러나 러시아는 아직도 독립된 '사이버기본법' 없이 정부의 정보보안 Doctrine으로 대체하고 있다.[65]

러시아는 사이버전과 관련하여 공식적인 문서를 발표한 적이 없다. 그러나 2000년 9월에 “러시아연방 정보보안 Doctrine (Doctrine of the Information Security of the Russian Federation)”을 발표하고 Internet 정책을 국가안보의 주요 의제로 간주한다고 선포하면서 개인의 권리도 제한할 수 있다는 내용을 포함하였다.[66] 2007년 4월 러시아 해커들이 감행한 에스토니아의 전산망에 대한 사이버공격으로 Paradigm이 전환되었다는 것을 증명했다.

2016년 12월 승인된 “신 정보보안 Doctrine(President of the Russian Federation, 2016)”에서 주변국이 군사적 목적으로 러시아의 정보 Infra에 대한 영향력 확대를 추구하는 것'에 대한 우려를 나타냈다. 이 Doctrine은 사이버심리전에 대해 적시하며 이에 대한 후속 문건이나 법률을 제정하는 데 중요한 기반을 제공할 것이다.

러시아의 사이버전 수행기관은 연방보안국(FSB)[67]가 사이버전 전담조직인 Alpha부대를 통해 통신감청과 국가통신을 관리하는 임무를 수행하며 사이버안보 관련기관을 총괄하고 있다. FSB는 국가기밀을 포함한 중요정보의 통제와 예방조치. 관련기관에 대한 보안기술과 암호 Service를 제공한다. 예하조직으로는 정보보안센터, 침해사고대응팀, 국가 사이버범죄 조정본부 등이 있다.

러시아는 세계 최초로 2002년 해커부대를 창설하여 사이버전문인력의 양성과 기술개발에 노력해 왔다. 특히 물리적인 전쟁 수단으로 사이버공격작전을 수행했다. 2008

---

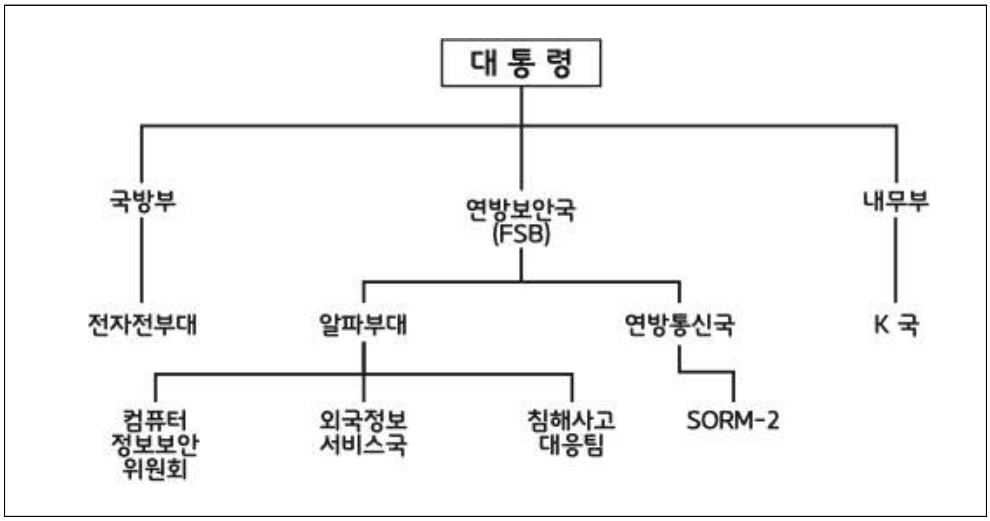
65) 김상배, “세계 주요국의 사이버 안보 전략: 비교 국가전략론의 시각”, 『국제 지역연구』, 제3권 (2017.), pp.67-108.

66) 위의 논문 참조

67) https://terms.naver.com/entry.naver?docId=645843&cid=43124&categoryId=43124,(검색일: 2023.8.23)

년 8월 조지아와의 전쟁에서 사이버공격작전의 요망효과를 달성하지 못하자 러시아군에 해커기능을 강화한 사이버전 전담 부대가 창설되었다. 이후 다양한 분쟁에 개입하며 상당한 수준의 사이버 공격역량을 갖추게 되었다. 특히 에스토니아, 조지아, 키르키스스탄, 우크라이나, 미국 등을 대상으로 사이버공격을 통해 공격역량을 확보했다.

러시아는 독자적으로 현존하는 모든 무기제계의 개발이 가능한 기술을 보유한 국가이며, 미국과 기술경쟁력 면에서 비교가 가능한 국가라고 할 수 있다. 러시아는 사이버전에서 승리를 거두기 위하여 공격과 방어수단을 총체적으로 개발하는 방향으로 사이버전 전략을 추진하면서 사이버무기체계의 개발 Program의 중요성을 강조하고 있다. <그림 4>는 러시아의 사이버전 수행기관이다.



<그림 4> 러시아의 사이버전 수행기관

라. 일본

일본은 1997년 9월부터 관방성을 중심으로 사이버전에 대비하기 시작했다. 정부, 산업시설에 대한 사이버위협이 증가함에 따라 "대규모 산업설비·Network 보안대책위원회"를 설립한다.[68] 1999년 9월부터는 국가전복 등을 꾀하는 컴퓨터 Network 부정접근을 근절하기 위하여 관방성·방위성·경찰청·금융감독청 등 13개 부처가 참석하는 "정보보안 관계 성·청 국장회의"를 설립하였다.[69] 2000년 2월부터는 정부 차원의 대

68) 다른 국가의 사례, 사이버테러 조직의 동향, 사이버대응 체제, 보호대책의 조사와 분석을 통해 사이버전을 연구하였다.

69) 해커대책 등 정보통신 기반 정비에 관한 행동계획을 수립하고 시행하는 협의기구이다.

응체제를 구축하기 위해 국장급회의체인 ‘정보보안대책 추진회의’, 정부와 민간 간 정책협의를 위한 학자·보안전문가·중요 민간시설의 대표자로 구성된 '정보보안부회'를 신설하였다. 2000년 12월에는 ‘사이버테러 대책에 관한 특별 행동계획'을 발표하고 내각 관방을 중심으로 관·민의 긴밀한 협력을 천명했다. 민간 주요 Infra 사업자와 지방자치단체는 자율적인 대책 강구를 주문했다.[70]

전수방위(專守防衛)를 국방의 기본방침으로하는 일본은 2005년 각의에서 결정된 4가지 유형[71]에 포함되지 않는 사이버위협에 대한 대응은 법적 근거가 없다. 이러한 문제점을 인식하고 2010년 방위계획대강을 통해 사이버 공격에 대한 위험을 안보 당면과제로 제시한다. “사이버 공격에 대한 대응태세 및 대응능력을 종합적으로 강화한다”는 방침이다. 2012년 9월 방위성은 “방위성·자위대에 의한 사이버공간의 안정적·효과적 이용을 위해”라는 제목의 지침을 발표했다. 방위성은 무력침공을 위한 공격여건조성작전으로 사이버공격이 발생했을 때 자위권을 발동해야 한다는 의지를 표현한 것이다.

사이버위협에 대한 국가적 대책마련은 2012년 아베내각이 등장하면서 구제화 되기 시작했다. 2013년 12월 국가안전보장전략, 2013 방위계획대강, 중기방위력정비계획을 발표하면서 사이버공간에 대한 위협을 국가안보상의 과제로 제시한다. 2013년 방위계획대강은 사이버 공간의 안정적 이용을 확보하는 대응방안으로 상시감시태세 구축, 침해사고 발생 시 피해 최소화, 신속한 피해복구 등을 제시하며 통합기동방위력 구축을 기본개념으로 제시했다.

2018년 발표한 新방위계획대강은 일본 방위에 있어 우주·사이버·전자파 등과 같은 첨단 군사영역에서의 방위력 강화가 ‘사활적으로 중요’하다는 인식이 반영되었다. 중국, 북한의 군사적 위협에 대한 대응과 더불어 안보환경의 질적 변화에 대한 대응역량 강화가 일본 방위력 강화의 핵심영역으로 급부상했음을 의미한다. 이를 위해 다차원통합방위력 구축을 기본개념으로 제시하였다.

사이버 영역에 대한 대처능력 강화를 위해 유사시 사이버 반격능력 보유와 사이버공간에서의 자위대의 역할을 확대하겠다고 선언한 것이 특징이다.[72] 이는 2018년 국가안전보장회의(NSC)에서 제시한 ‘적극적 사이버 방어개념’을 채택한 것이다.[73] 단,

---

70) 김재광 등, “일본의 사이버위기 관련 법제의 현황과 전망”, 『법학논중』, 제33권(2009.), pp.43-50.

71) 2005년 각의에서 결정된 무력공격사태는 ①선박 및 항공기에 의한 착륙 및 상륙침공, ②게릴라 및 특수부대에 의한 공격, ③탄도미사일 공격, ④항공공격 등이다.

72) 일본에 대한 공격 시 우주·사이버·전자파 영역을 활용하여 공격을 저지·배제한다고 명시하여 유사시 자위대가 적의 정보통신 및 네트워크를 공격하는 사이버 반격능력을 보유하겠다는 점을 명확히 하고 있다.

73) 2018년 “사이버시큐리티전략안”이 작성될 당시 국가안전보장회의(NSC)가 제시한 개념으로

사이버 공격과 자위권 발동에 대한 일본 내 법적 논의가 제대로 이루어지지 않은 상태에서 진행되었다는 한계는 있다. 이러한 일본의 사이버 반격능력 보유는 미일안보조약에 의한 억지력에 더 이상 의존하지 않겠다는 뜻으로 풀이된다.

일본은 사이버보안 분야 기본법 제정 전까지 정보화 분야의 기본법인 “고도 정보통신 Network 사회형성 기본법(2000)”에 근거하여 정책을 시행했다. 도쿄올림픽 개최가 확정되자 이를 계기로 사이버보안 기본법 개정의 필요성을 느끼게 되었다. 2014년 11월 사이버안보를 위한 사이버보안의 기본이념과 국가 책무를 명확히 한 “사이버보안기본법”을 제정한다. 이 법은 사이버 보안 강화를 위한 다양한 조치들을 규정하고 있다.[74] 이를 통해 범국가적 사이버 보안을 추진하기 위한 법적 근거를 마련했다. 사이버보안을 강화하기 위한 활동의 투명성을 확보하여 국민들도 참여할 수 있도록 하였고, 사이버보안을 위한 국제협력에도 적극 참여 할 수 있도록 하였다.[75]

일본의 사이버전 수행조직은 2005년 내각 관방에 '정보보안 Center'와 '정보보안 정책회의'를 설치하여 정부 각 부처의 사이버방위 역량을 ' 정보보안 Center'가 조정하도록 하였다. 정부기관과 방위사업체를 대상으로 한 사이버공격에 대응하기 위하여 경시청에 '사이버 Force Center'와 ' 생활안전국'을 설치하여 사이버대응을 총괄하도록 하였다. 또한 같은 해 각 군 자위대에 사이버전 담당 System 방호대를 창설하였고, 2008년 7월에는 160여명 규모의 '자위대 지휘통신 System'로 확대하였다. 2015년 1월에는 내각 산하에 사이버보안센터 (NISC)를 설치하여 사이버공격을 담당하도록 하였다.

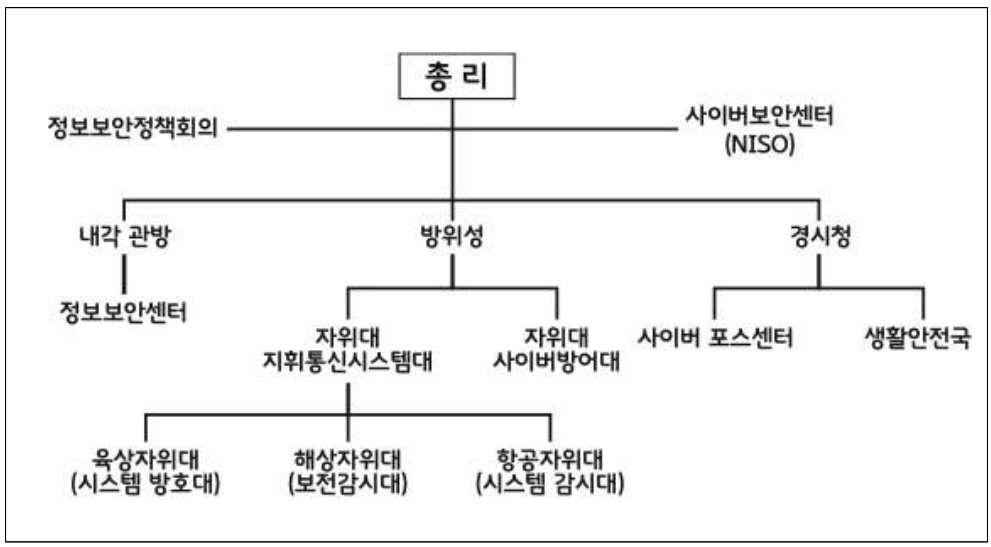
2014년 3월 자위대에 창설된 ‘사이버방위대’는 자위대지휘통신시스템대 산하에 90명 규모로 편성되어 방위성 및 자위대의 컴퓨터 시스템 상황에 대한 24시간 감시태세 및 침해사고 발생 시의 긴급 대응체제를 갖추게 되었다. 또 육해공 각 자위대가 개별적으로 실시해 오던 정보수집 및 대원 훈련 등의 임무를 일원화 하게 되었다.

공격조짐을 포착하여 유사시로 판단되면 사이버 공격을 받기 전에 상대의 능력을 상실케 하거나 저하시킨다는 의미의 ‘적극적 사이버방어’ 개념이다.

74) 첫째, 사이버보안을 '전자적 방식, 자기적 방식, 기타 사람의 지각으로는 인식할 수 없는 방식으로 기록되거나 발신, 전송 또는 수신되는 정보의 누설, 멸실 또는 훼손방지 및 그 밖의 정보의 이전관리를 위한 필요 조치와 정보 System 및 정보통신 Network의 안전성·신뢰성의 확보를 위하여 필요한 조치가 강구되고 그 상태가 적절하게 유지 관리되는 것'이라고 규정하였다. 둘째, “사이버보안기본법”이 추구하는 기본이념을 제시하고 있다. 셋째, 사이버 관련 국가의 법률적 주체들에게 기본책무를 요구하고 있다. 넷째, 사이버보안 전략의 수립을 위한 정부의 임무는 사이버보안에 관한 시책을 종합적이고 효과적으로 추진하기 위해 사이버보안 기본계획을 수립하며 사이버보안 수행을 위한 예산을 확보하도록 하였다. 다섯째, 내각 관방장관이 본부장이 되는 '사이버보안전략본부'를 내각에 설치하였다. 여섯째, '사이버보안전략본부'의 대외 협력관계를 명시하였다.

75) 박상돈, “일본 사이버안보법에 대한 고찰 : 한국의 사이버안보법제도 정비에 대한 시사점을 중심으로”, 『경희법학』, 제50권(2015.), pp.161-165.

2022년 3월 일본 방위성은 자위대 사이버방위대의 기능을 강화하여 약 540명 규모로 재편했다고 보도했다.[76] 임무는 사이버 공격 대처, 사이버 전문인력 양성, 실전적 훈련 지원, 정보통신 네트워크 관리·운영 등이다. 일본은 우주와 사이버, 전자파 등 3개 분야를 방위력 정비의 핵심축으로 삼고 있다. 향후 사이버방위대는 사이버방어를 넘는 공격수단을 개발하여 군사작전의 일부로 사이버전을 활용할 것이다. <그림 5>는 일본의 사이버전 수행기관이다.



<그림 5> 일본의 사이버전 수행기관

자위대는 사이버전 역량을 확보하기 위하여 사이버요격 무기체계 (Virus형)를 개발한 바 있고, 2015년에는 미국과 사이버공격에 대한 방위조약을 체결하였다. 사이버전에 대비하기 위해 매년 약 5,000억 원 이상을 집행하는 등 정부예산을 과감히 투자하고 있으며, 방위성 지원 하 후지쯔에서 사이버공격자를 추적하여 파괴하는 멀웨어(Malware)[77]를 제작한 바 있다. 방위성은 중장기적으로 사이버공격 대책에 대한 기획입안을 담당하는 '사이버기획조정관'을 신설하고 다른 나라에서 발생한 사이버 공격에 대한 정보를 수집, 분석하기 위해 정보본부에 전담요원을 배치하였다. 또한 사이버전 선진국들의 기술을 대거 도입하여 자체 사이버무기체계 개발 System을 구축

76) "일본 '자위대 사이버방위대' 설치...540명 규모", 한국경제TV(2022.03.17.)

77) 멀웨어는 위협행위자가 조직이나 개인을 혼란에 빠뜨리기 위해 배포하는 악성 소프트웨어이다. 이메일에 첨부되거나 사기성 링크에 포함되며 광고에 숨겨져 있거나 다양한 인터넷 사이트에 대기하고 있다. 멀웨어의 최종 목표는 컴퓨터와 네트워크에 피해를 주거나 악용하는 것이며 데이터나 돈을 훔치는 것이다.

운영하고 있다.

3. 사이버 위협요인과 독도 방어전략

가. 사이버 위협요인

사이버위협의 유형은 사이버해킹, 사이버범죄, 사이버테러, 사이버분쟁, 사이버전쟁 등으로 구분된다. 사이버공간에서의 다양한 사이버위협들이 정치사회적인 효과를 유발하면서 개인 간의 사이버분쟁을 벗어나 국가 간의 사이버전쟁으로 확대될 수 있다는 것이 가능한 시나리오가 되었다. 이것은 정치적으로 동기화된 단순한 사이버위협이 대규모 군사작전을 유발시킬 수 있다는 의미이기도 하다.

국가정보원은 '2022년 사이버안보 위협 주요 특징 및 내년 전망'을 발표했다.[78] 2023년 사이버안보 위협의 주요 특징은 3가지로 특정했다. 첫째, 국내 해킹 피해가 지난해보다 5.6% 감소했다는 사실이다. 이는 국제사회의 사이버억지 조치가 이어지고 우리 정부의 대응이 강화된 결과로 보고 있다. 해킹 수단은 안보부처와 연구기관을 사칭하는 해킹메일이었으며 IT 솔루션의 보안 취약점 악용 공격도 빈번하게 발생했다.

둘째, 국가 배후 해킹조직은 국내 외교·안보 현안 및 첨단기술을 절취하는 공격이 지속되고 있다는 점이다. 주로 북한의 정보 절취 공격과 국제적 경쟁력이 있는 방산·원전·정찰자산 등의 첨단 산업기술 절취 행위가 늘어나고 있다.

셋째는, 국가간 사이버분쟁 및 랜섬웨어로 인한 글로벌 안보 불안감이 고조되고 있다. '러시아-우크라이나 전쟁'에 이어 '중국-대만'과 중동지역 갈등에서도 디도스 공격 등 다양한 사이버 분쟁이 발생하고 있다. 코스타리카 정부는 범죄조직의 랜섬웨어 공격으로 국가비상사태를 선포했고, 영국과 프랑스의 공공 의료 서비스가 차질을 빚는 등 랜섬웨어가 국가안보에 영향을 주기도 했다고 분석했다.

국가정보원이 선정한 2023년 사이버안보 위협은 5가지로 먼저 첨단기술·안보현안 절취 목적의 사이버첩보 활동이 심화될 것으로 전망한다. 북한과 중국 등 국가 배후 해킹조직은 원자력·우주·반도체·방산 관련 첨단기술과 함께 한국·미국의 대북정책과 방위 전략 해킹을 지속하고 있다.

둘째, 사회 혼란 목적의 해킹 가능성 우려다. 지난 10월에 발생한 IDC 화재사고의 파급력을 학습한 해킹조직이 사회 혼란을 노리고 주요 기반 시스템에 대한 파괴적 사이버 공격을 자행할 가능성이 있다.

셋째, 공공·기업 대상 랜섬웨어 피해 확산 등 사이버 금융범죄가 빈발하고 있다.

78) "2023년 사이버 위협 전망 TOP 5", 아웃소싱타임스(2022.12.12.), http://www.outsourcing.co.kr/news/articleView.html?idxno=95471(2023.08.12.)

글로벌 경제위기 아래 중소 병원·플랫폼 기업을 노린 랜섬웨어 유포와 데이터 공개 협박, 탈중앙화 가상자산(DeFi) 및 오픈뱅킹 등 신 금융 서비스를 공략하고 있다.

넷째, 용역업체·클라우드 등 민간 서비스를 악용한 공급망 해킹이 지속되고 있다. 전산 용역업체를 해킹해 절취한 계정정보·소스코드를 고객사 침투 단서로 악용하거나 공공에 확대 중인 민간 클라우드의 보안취약점을 집중 공격한다.

다섯째, 사이버억지 정책 회피 목적의 다양한 해킹수법이 출현하고 있다는 점이다. 디지털 추적을 회피하기 위해 다크웹, 방탄호스팅 서버 이용이 일상화되고 타 조직의 악성코드를 모방하거나 인공지능 기술을 적용한 해킹도구가 등장하고 있다.

독도와 동해해역을 사이에 두고 벌어지는 한·일간 갈등은 회색지대에서 물리적·사이버 공간에서 저강도 분쟁의 형태로 나타나고 있다. 물리적 사실을 왜곡, 조작하여 사이버분쟁으로 발전하기 때문에 국가 간 사이버전쟁으로 확대되지 않도록 대비해야 한다. 예를 들면 회색지대 전략이 사용되는 모든 영역 즉 정치, 경제, 군사적 활동 등에서 명확한 인식과 대비책이 강구되어 있어야 한다.

첫 번째 사례는 위안부 판결이다.[79] 위안부 판결은 회색지대의 전략 중에서도 정치적 강압이 보다 강하게 나타난다. 이것은 위안부 판결이 한일 관계의 악화와 외교관계에 대한 우려를 형성해 국내정치의 분열을 초래하거나 외교활동에 제한을 줄 수 있다.

두 번째 사례는 강제징용 판결로부터 시작된 한국과 일본 간의 무역 갈등이다.[80] 여기에서는 정치적 강압도 작동하지만 경제적 강압이 보다 두드러진다. 강제징용 판결에 대한 보복으로 일본의 수출 제한이라는 경제적 강압이 한국의 불매운동, 관광금지 등의 일본에 대한 새로운 경제적 강압을 재생산해 양국의 경제적 손실을 만들어냈다.

세 번째 사례는 일본해상자위대 초계기의 근접비행 사건이다.[81] 이것은 군사적 활동을 중심으로 회색지대 전략이 나타나는 사례이다. 직접적인 군사적 충돌은 아니지만 레이더의 활용, 근접비행과 관련한 군사적 마찰이 정치적, 외교적 상황에 영향을 미치고 있는 사례로 볼 수 있다. 회색지대 전략을 보려주는 한·일간의 갈등 사례는 향후 독도/다케시마 분쟁에서 정치적 강압, 경제적 강압, 군사적 활동 등의 전략이 복합적으로 적용될 수 있다.

---

79) "文 정부의 안보...오답만 선택하는 공부 못하는 학생", 뉴데일리(2021.02.03.), https://www.newdaily.co.kr/site/data/html/2021/02/02/2021020200096.html(2023.08.21.)

80) 최은미, "강제동원문제를 둘러싼 한일갈등의 전개와 향후 전망", 『주요국제문제분석』, 제31호(2019), pp.3-15.

81) "軍 '日초계기 경고음 증거 못 돼, 교묘한 가공' 정면 반박", 뉴시스(2019.01.22.), https://newsis.com/view/?id=NISX20190122_0000537667&cID=10301&pID=10300(2021.03.19)

한·일간의 독도/다케시마 분쟁은 사실상 샌프란시스코조약 이후 이승만 라인을 선언한 1953년부터 시작되었고, 그 이후 수면 아래에서 갈등의 소지가 지속되었다. 독도를 둘러싼 한일 간의 전략적 경쟁은 보다 복잡한 성격으로 전개될 수 있다. 독도는 심각한 군사적 충돌과 같은 전쟁의 상황이 아니지만 영유권과 관련해 한일 양국 간에 분쟁의 소지가 있는 모호한 영역이다. 또한 외교부나 외무성이 정부의 입장을 대변하고 있기 때문에 행위의 주체를 국가로 볼 수 있다. 그리고 장기간에 걸쳐 지속적으로 영유권 주장과 이에 대한 항의를 반복하고 있다는 점에서 사이버분쟁의 위협에 대한 대비가 요구된다.

나. 독도 방어전략

한국의 디지털 환경과 사이버보안 여건은 양호하다. 그러나 사이버침해 위협 발생 시 공격의 주체를 특정하거나 피해를 최소화할 수 있는 능력과 태세는 미흡하다. 독도와 동해해역에서 벌어지는 모든 위협은 복합적으로 작용한다. 하나의 위협에 그치지 않고 최종 정치적 목적을 달성하기 위해 연계할 것이다.

러시아-우크라이나 전쟁의 정보심리전 사례를 통해 사이버영역에서 정보전과 심리전이 운용되는 특징을 살펴보았다. 향후 사이버전은 매우 다양한 행위자가 참가할 것이기 때문에 이러한 다양한 행위자를 평시부터 관리해야 한다는 점이다. 두 번째는 디지털 플랫폼을 장악하는 자가 정보심리전에서 승리할 수 있다는 점이다. 이미 플랫폼을 선점한 서방 국가 및 IT기업들과 국제적인 협력을 강화해 나가야 한다.

이번 전쟁의 승패는 정보심리전의 우위에서 결정되었다. 앞서 Ⅲ장에서 우크라이나가 정보심리전의 우위를 점할 수 있었던 이유를 도출하였다. 먼저 전쟁의 명분이다. 명분 없는 전쟁의 문제를 지적하여 여론을 조성했다. 둘째, 정보심리전이 발신하는 내러티브의 대결이다. 러시아가 발신하는 가짜뉴스는 이미 학습을 통해 신뢰하지 않게 되었다. 반면 우크라이나는 철저한 대비를 통해 적시적절한 반격 내러티브를 발신하여 러시아와 내러티브 대결에서 우위를 점했다. 셋째, 서방 IT기업의 플랫폼 독점이 러시아의 정보심리전 효과를 차단했다. 또 스타링크 인터넷 시스템을 지원받아 우크라이나는 디지털 플랫폼을 유지할 수 있었다. 마지막으로 서방국가의 지원이다. 전쟁정보를 공유하고 민감정보를 노출하여 러시아의 가짜뉴스를 신뢰하지 않도록 만든 것이다.

러시아-우크라이나 전쟁에서 도출한 정보심리전의 특징적 요소를 한국과 주변 강대국의 사이버전략과 능력에 대비하여 분석한 결과를 토대로 사이버 독도 방어전략을 제시하면 다음과 같다.

첫째, 사이버전 대비 관련 법령체계의 정비 및 기본법 제정이다. 정보보호 및 사이

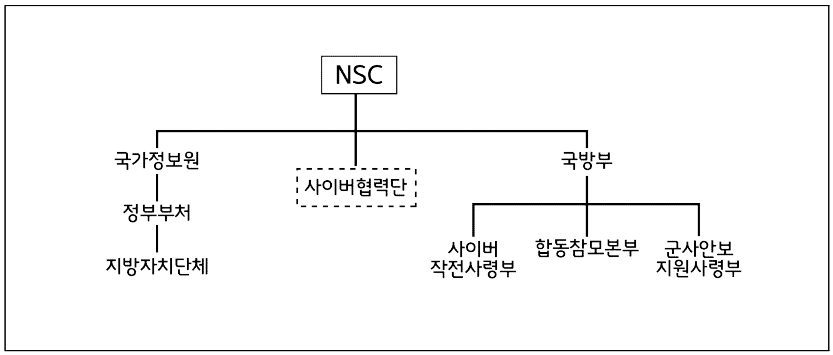
버전 관련 법들이 개별 입법되어 상호 연계 및 상하관계가 정립되지 않아 동일한 법률의 해석을 기대할 수 없다. 다행히 문재인 정부에서 처음으로 국가사이버안보전략과 국가사이버안보기본계획을 확정하여 정책으로 추진할 수 있는 근거를 마련했다.

윤석열 정부는 국가사이버안보전략서를 발표하고 사이버전 대응을 선제적이고 능동적인 작전개념으로 바꾸라고 주문했다. 그러나 법적 근거 없이는 사이버침해와 공격에 대응하는 전력과 노력을 통합할 수 있는 컨트롤타워를 둘 수 없고 효과적으로 대응할 수 없다. 2006년 17대 국회에서부터 사이버보안법이 발의되고 있으나 정치적 고려 등을 이유로 폐기되고 있다. 사이버기술의 급속한 발전으로 대응법 제정이 따라가지 못하는 것이 현실이다. 따라서 매 사안마다 대응법을 제정하기보다 사이버안보법을 기본법으로 제정하여 국가적 지향방향을 설정하는 것이 필요하다. 기본법을 통해 법의 해석과 유추에서도 일관성 있는 적용이 가능해 진다.

사이버안보를 국가가 모두 책임질 수 있는 범위를 벗어났다. 이번 전쟁의 특징에서 본 것처럼 다양한 사이버전 행위자를 통합할 수 있어야 한다. 사이버 관련 이해당사자들과 행정기관들이 모두 포함된 거버넌스를 구축할 수 있는 법적 근거가 필요한 것이다. 이 법안에 반대하는 사람들은 사이버위기 관리와 조사활동을 위해 희생될 수 있는 국민의 기본권 침해를 우려한다. 따라서 컨트롤타워를 맡는 기관에 대한 법률적인 통제와 국회와 사법부의 견제장치를 요한다.

사이버보안법을 시행하고 총괄하는 조직은 위에 열거한 긍·부정적인 측면을 모두 충족할 수 있어야 한다. 이를 위해 국가안전보장회의 통제하에 두어야 한다. 현재 시스템은 사이버공격 대상이 누구인지에 따라 대응기관이 달라져 통합된 대응이 불가하다. 예를 들면 공공분야는 국가정보원이 군 관련 분야는 국방부에서 하고 조사는 경찰이 맡는 식이다. 사이버전을 수행하는 기관의 체계를 일원화하고 책임의 한계를 명시할 수 있게 조직을 편성해야 한다.

한국의 사이번전 수행조직(안)은 <그림 6>에서 보는 것과 같이 국가안전보장회의(NSC)에서 국가정보원과 국방부를 통해 전평시 사이버전 수행기관을 조정·통제하도록 한다. 또한 사이버협력단을 두어 민·관·군 협의체로 운영하면서 정보공유 및 국제적 공조와 협력체계를 구축한다. 국가정보원은 전·평시 정부 기관과 지방자치단체의 사이버조직과 역량을 조정·통제하고 국민의 기본권 침해가 발생하지 않도록 세부적인 법적 제도적 장치를 마련한다. 국방부는 전평시 사이버전의 핵심전력으로 사이버작전사령부와 군사안보지원사령부를 통해 연구개발, 전문인력 양성, 정보기술 등을 확보할 수 있어야 한다. 합동참모본부를 통해 사이버전을 통합방위작전의 핵심영역으로 구분하여 육해공군의 전력과 역량을 보호하고 대응할 수 있는 체계를 구축해야 할 것이다.

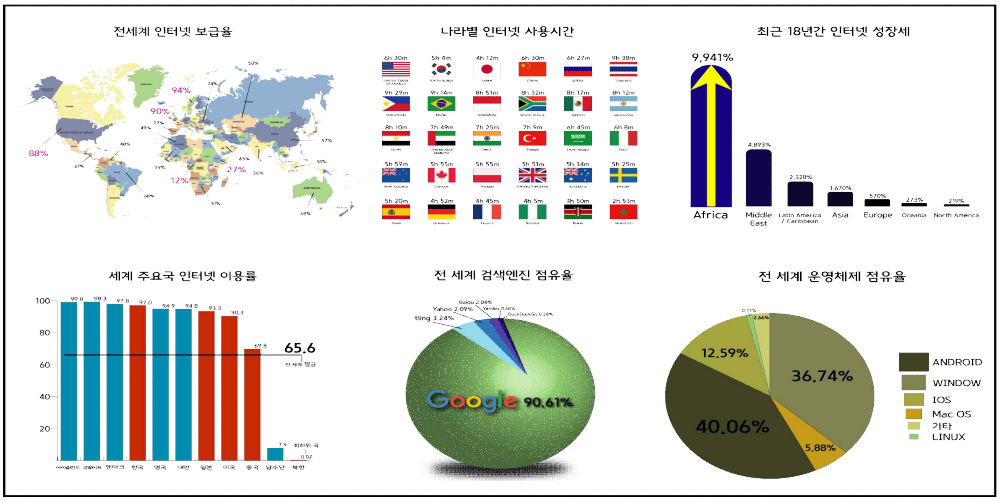


<그림 6> 한국의 사이버전 수행조직(안)

통합방위법은 물리적으로 적의 침투 및 도발이 발생한 지역 또는 위협에 물리적으로 대응하기 위한 것이다. 사이버공간에서 발생하는 불법적인 사이버 정보수집활동이나 사이버공격에 대한 대응은 제한된다. 이를 위해 통합방위작전의 영역에 사이버공간을 포함하고, 사이버영역에서 군의 역할과 기능을 명확히 보장해야 한다. 사이버전을 총력전으로 수행하기 위해 사이버사태에 대한 대응조직 편성을 명시해야 한다. 또 사이버 대비태세를 유지하기 위한 민관군 통합 사이버무기체계 연구개발, 인력확보 및 교육훈련 등의 내용을 규정해야 한다.

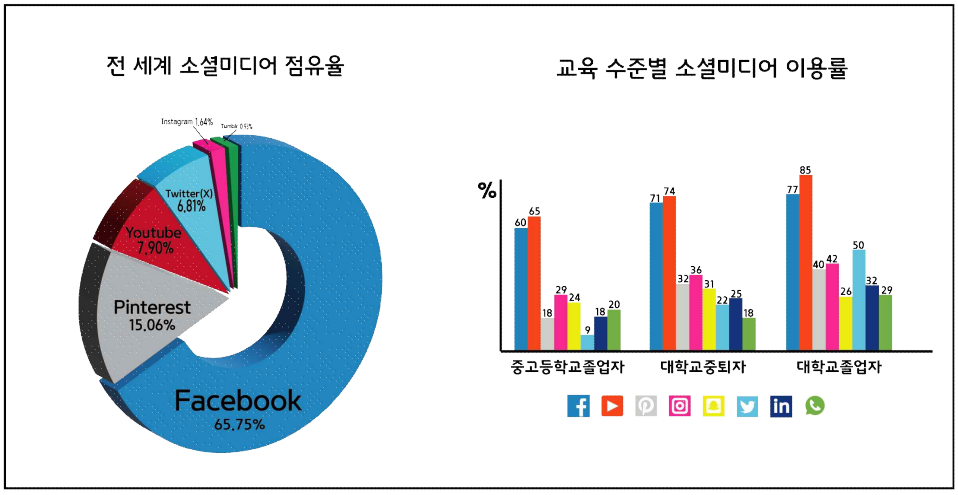
둘째, SNS를 활용한 독도 홍보전략을 수립하여 평시부터 메시지의 내러티브를 확보할 수 있어야 한다. 나라별로 일일 인터넷 사용시간은 태국인이 9시간 38분을 온라인에서 보내고 미국인은 웹서핑에 6시간 30분을 보내는 것으로 나타났다. 한국인은 5시간을 웹서핑에 보낸다. 인터넷 이용률은 서방국가가 90% 이상으로 세계 평균은 65.6%이다. 인터넷 성장세를 보면 아프리카는 18년 간 10,000% 성장했으며 북미는 219% 성장했다. 인터넷 보급률을 살펴보면 북미, 북유럽, 서유럽은 90%에 달하며 중앙 아프리카와 동부 아프리카는 20% 미만이다.

이러한 인터넷 보급률을 기준으로 전 세계에서 가장 인기 있는 운영체제는 안드로이드로 40.6%를 그다음은 윈도우가 36.7%를 차지했다. 검색엔진은 구글이 90.6%로 가장 많은 사람이 사용하고 있다.



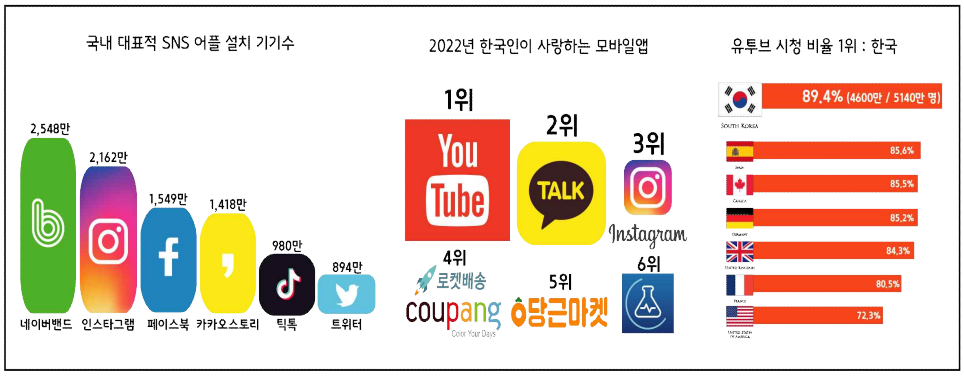
<그림 7> 인터넷 사용 트렌드

소셜미디어 트렌드를 분석해 보면 소셜네트워크(SNS)는 전 세계인들이 모이는 소통의 장이다. 많은 기업에서 SNS를 도입하여 마케팅이나 인재 채용의 수단으로 활용하며 업무 환경에 SNS를 도입해 생산성을 높이는 경우도 있다. SNS 중 가장 많은 사용자를 보유하는 것은 페이스북이다. 현재 10억 명이 사용하고 있는 것으로 분석된다. 소셜 미디어 사용율은 연령대가 높아짐에 따라 낮아지고 교육수준이 높을수록 많이 사용한다. 이는 교육을 많이 받은 사람이 컴퓨터, 네트워킹, 마케팅 관련 직업에 많이 종사하기 때문인 것으로 분석된다.



<그림 8> 소셜미디어 트렌드

한국인이 가장 많이 사용하는 모바일앱은 유튜브이며 2위는 카카오톡, 3위는 인스타그램이다. 카카톡은 월 평균 4,690만 명이 유튜브는 4,498만 명이 이용했다. 대표적인 SNS의 모바일앱 설치기기 수는 네이버 밴드 설치자 수가 1위로 2,548만 명이며 인스타그램은 2,162만 명으로 2위이다. 특히 한국인의 유튜브 시청 비율은 세계 1위로 전 국민의 90%인 4,700만 명이 시청했다.



<그림 9> 한국인 소셜미디어 트렌드

MZ세대는 SNS를 정보 전달 창구가 아니라 관계를 만들어 나가는 공간으로 인식한다. 따라서 독도 홍보컨텐츠는 SNS를 통해 평시부터 관리되어야 한다. 특히 한국인이 가장 많이 애용하는 유튜브와 인스타그램, 카카오채널을 이용하여 홍보하는 전략을 강구해야 할 것이다. 세계인들을 위해서는 가장 선호하는 페이스북과 유튜브를 이용해 홍보하는 전략이 필요하다.

셋째, 정보기술의 확보와 연구개발 역량의 확보이다. 이번 전쟁에서 사용한 사이버 무기체계는 고도의 기술적 집약체이다. 러시아가 사이버 공격에 와이퍼 악성 코드와 디도스·문자스팸 등을 사용했다. 와이퍼란 컴퓨터에 침입할 경우 저장공간 내 모든 데이터를 삭제하는 유형의 악성 소프트웨어를 말한다. 미국 IT보안업체 멘티언트의 제이미 콜리어 컨설턴트는 와이퍼 공격 외에도 국방부와 최대 상업은행 프라이밧뱅크에 디도스 공격이 가해진 것을 확인했다고 밝혔다. 사이버 무기체계는 연구개발을 통해 대응기술을 확보할 수 있다. 따라서 사이버 무기체계에 대한 연구를 수행할 연구기관과 연구인력, 국가적 노력이 동반되어야 할 것이다. 이를 위해 민·관·군 연구소를 연계하여 연구를 전담할 수 있는 국가급 연구소 운영을 통해 사이버능력을 확보해 나가야 한다.

넷째, 사이버 전문인력 육성과 교육훈련 체계확보이다. 인원을 육성, 확보하고 교육훈련을 체계화해야 한다. 사이버전은 총력적으로 다양한 사이버전 행위자가 참가한다. 따라서 사이버군 뿐만아니라 민간 정보보호 인력의 관리가 요구된다. 여기에는 화이트 해커 육성도 포함된다. 이를 위해 사이버예비군 제도를 적극 활용할 수 있어야겠다. 통합방위법에 사이버예비군을 명시하여 평시부터 관리하고 예비군 훈련을 통해 사이버전 능력을 키우고 유지할 수 있는 체계를 만들어야 한다. 또한 평시부터 민간 사이버 역량을 통합할 수 있는 다양한 거버넌스 형태를 강구하여 사이버전 수행조직에서 관리 및 유지 할 수 있도록 체계를 정립해야 한다. 유사시 사이버 총력전이 가능하도록 전문인력을 육성하고 교육훈련에 주안을 두어야 한다.

다섯째, 국제협력 체계의 구축이다. 2023년 한국은 부다페스트협약에 가입 초청을 받아 사이버 국제협력의 기초를 만들었다. 사이버침해는 국제공조 필요성이 날로 커지는 만큼 타국과의 협력이 필수적이다. 경찰은 지난 2020년 'n번방' 사건 당시 부다페스트협약 미가입국으로 수사에 어려움을 겪었다. 정부는 협약 가입을 통해 전세계 인프라를 활용해 사이버 범죄에 대응하겠단 방침이다. 우리나라의 사이버범죄협약 가입 추진은 안전하고 평화로운 사이버공간 구축을 위한 국제사회의 노력에 적극 참여한다는 의미가 있다. 이를 통해 최첨단 사이버범죄 수사기법과 사이버 대응 선진 모델을 구축하는 계기로 만들어야 한다.

Ⅴ. 결론

지금까지 러시아-우크라이나 정보심리전 전략과 실제 적용사례를 사이버행위자 측면과 디지털 플랫폼의 무기화 측면에서 살펴보았다. 그리고 동해와 독도 해역에서 영향력을 행사할 수 있는 미국, 중국, 러시아, 일본의 사이버전략과 능력을 법과 제도적인 측면, 사이버기술 확보 측면에서 알아보고 한국의 사이버전략을 비교 분석했다.

한국의 사이버전 준비태세는 매우 미흡하다. 법과 제도적인 면에서 사이버기본법이 제정되지 않았고 사이버전 수행조직도 민·관·군 모든 자원을 통제할 컨트롤타워가 없는 실정이다. 러시아-우크라이나 전쟁사례를 통해 정보심리전은 효과대비 진입비용이 가장 낮은 전쟁수단임이 입증되었다. 우크라이나는 러시아와의 정보심리전에서 우위를 점할 수 있었기에 초기전쟁에서 공격을 효과적으로 막아낼 수 있었다.

사이버전 위협에 대한 대응능력을 갖추기 위해서는 첫째, 사이버보안 의식과 정보인프라에 대한 보호역량이 필요하다. 인터넷 침해사건의 경우 다른 국가들보다 유독 한국이 가장 피해가 심한 이유는 국민 개개인의 보안의식이 희박하기 때문이다. 충분한 보안의식이 없는 상태에서 해킹에 무방비로 노출되어 있는 것이 현실이다.

둘째, 정보전과 사이버테러 공격에 대비한 민관군 대응역량을 총괄하고 결집시킬 수 있는 종합대응체계가 마련이다. 사이버 문제에 대한 관련 부처별 책임과 권한이 불분명하고 모호하여 위기시 신속한 대응능력과 기동성이 떨어진다.

셋째, 선진정보강국들과의 협력체계 구축이 요구된다. 사이버공격이나 사이버테러가 해외에서 발생하여 외국 사이버위협 대응기구와 국제협력을 강화하여 민간 및 정부차원에서 신속하고 효과적으로 대응할 수 있어야 한다. 이와 더불어 심층적인 협력체제로 발전하기 위해서는 사회협력 저변을 확대하고 다양화시켜 나가는 것이 필요하다.

넷째, 정보전 강대국들의 대응방향이나 대책을 따른 것도 중요하지만 미래 정보주권 선점을 위해 독자적인 마스트플랜과 전략이 필요하다. 정보전 상황에서 독자적인 정보안보 강화 전략과 마스트플랜을 준비하고 구체적인 로드맵과 추진전략을 수립해야 한다. 그렇지 않으면 머지않은 장래에 사이버공격과 사이버테러로 인한 국가적 위기를 초래하게 될 것이다.

독도 사이버 방어능력은 한국의 사이버전략과 대응능력에 기초한다. 한국의 사이버전략과 능력을 강화하기 위한 대책을 다음과 같이 제안한다.

첫째, 사이버안보법을 기본법으로 제정하여 사이버전에 대비한 국가적 지향방향을 설정해야 한다. 사이버침해와 공격에 효과적으로 대응할 수 있는 자원과 노력의 통합 근거가 되기 때문이다. 사이버기술의 발전에 맞추어 대응법률을 일일이 제정할 수 없

기 때문에 기본법 제정을 통해 법의 해석과 일관성 있는 적용을 가능하게 해야 한다. 통합방위법은 통합방위작전 영역에 사이버공간을 명시하여 사이버전에서 군의 역할과 기능을 정의해야 한다. 이를 위해 사이버 대응조직을 편성하고 연구개발, 인력확보, 교육훈련 방법을 규정해야 한다.

둘째, SNS를 활용한 독도 홍보전략으로 평시부터 정보심리전에 대비해야 한다. 세계인이 가장 많이 사용하는 페이스북과 유튜브에 독도 홍보 계정을 개설하고 컨텐츠를 개발하여 홍보한다. 국내에서는 한국인이 가장 많이 사용하는 유튜브와 인스타그램, 카카오채널에 계정을 개설하여 컨텐츠를 올려 메시지의 내러티브를 확보한다.

셋째, 사이버무기계 개발을 위한 기술과 연구개발 역량을 확보한다. 와이퍼, 디도스 등 악성 코드는 매우 강력한 공격수단으로 피해가 크며 대응이 어렵다. 꾸준한 연구개발을 통해 사이버기술 능력을 확보하는 것이 중요하다. 따라서 국가적 차원에서 민관군 연구소를 연계하고 연구인력을 통합할 수 있는 국가급 연구소 설립이 요구된다.

넷째, 사이버 전문인력의 육성이다. 사이버전은 총력전이다. 전문인력의 양성은 꾸준한 훈련과 관리가 필요하다. 통합방위법에 사이버예비군 제도를 만들어 평시부터 민간 사이버 역량을 유지 및 관리할 수 있어야 한다. 이를 통해 민관군 통합 사이버 인력 관리가 이루어져야 한다.

다섯째, 부다페스트협약 가입을 통해 국제협력 체계를 구축하는 것이다. 사이버침해에 대한 분석과 대응은 타국과의 협력이 필수적이다. 이를 통해 선진 사이버범죄 수사기법을 배우고 대응모델을 도입하여 사이버공간에서 안전하고 평화로운 이용 환경을 구축하는 것이 필요하다.(끝)

참고문헌

군사연구소, 『2014년 러시아의 우크라이나 개입』, 2015.

김상배, 『미중 디지털 패권경쟁』, 서울: 한울, 2022.

_____, 『버추얼 창과 그물망 방패』, 서울: 한울, 2018.

김선래 외,『미중러 전략경쟁과 우크라이나 전쟁』, 다해, 2022.

데이비드 조던 외, 강창부 역, 『현대전의 이해』, 서울: 한울, 2014.

정호섭, 『미중 패권경쟁과 해군력』, 서울: 박영사, 2021.

조너선 E.힐먼, 박선령 역, 『디지털 실크로드』, ㈜로크미디어, 2022.

알렉스 캘리니코스 외,『우크라이나 전쟁』, 책갈피, 2022.

이홍균, 『일본의 해양전략과 21세기 동북아 안보』, 한국해양전략연구소, 2002.

폴 케네디 저, 이일수·김남석·황건 공역, 『강대국의 흥망』, 서울: 한국경제신문사, 1989.

한용섭 외,『미·일·중·러의 군사전략』, 서울: 한울, 2018.

B. H. 리델하트, 황규만한경구 역,『현대육군의 개혁』, 일조각, 2001.

김상배, “세계 주요국의 사이버 안보 전략: 비교 국가전략론의 시각”, 『국제 지역연구』, 제3권(2017.)

김재광 등, “일본의 사이버위기 관련 법제의 현황과 전망”, 『법학논총』, 제33권(2009.)

박상돈, “일본 사이버안보법에 대한 고찰 : 한국의 사이버안보법제도 정비에 대한 시사점을 중심으로”, 『경희법학』, 제50권(2015.)

송승종, “러시아 하이브리드 전쟁의 이론과 실제”, 『한국군사학논집』 Volume 73, Issue 1(2017.)

송태은, “현대 전면전에서의 사이버전의 역할과 전개양상: 2022년 러시아-우크라이나 전쟁 사례”, 『국방연구』, Volume 65, Issue 3(2022.)

_____, “러시아-우크라이나 전쟁의 정보심리전: 평가와 함의”, 주요국제문제분석(2022.)

송태훈, “세계전쟁 양상에 따른 정보작전(Imformation Operations) 변화 분석”, 『군사연

양욱, “회색지대 분쟁 전략: 회색지대 분쟁의 개념과 군사적 함의”, 「전략연구」 Volume 27, Issue 3(2020.)

이정하, “러시아 연방의 정보-심리작전과 제귀 통제(Reflexive Control)”, 『한국서양사연구회』, 제66권(2022.)

이용석; 정경두, “러시아 대 우크라이나 사이버 전쟁의 교훈과 시사점”, 『국방정책연구』, Volume 137(2022.)

정삼만, “해양에서의 회색지대전략의 이론과 실제(Gray Zone Strategy in Maritime Arena : Theories and Practices)”, 『Strategy 21』, 통권 43호, Vol.21, No.1(2018.)

조현덕, 이정태, “중국의 남중국해 영향력 확대를 위한 투트랙 전략-맞대응 및 회피전략을 중심으로”, 『대한정치학회보』 제29권 4호(2021.11.)

최근대, “중국의 반접근 지역거부(A2/AD) 전략에 대한 분석: 정보작전 수행역량 강화를 중심으로”, 『한국군사학논총』(2023.)

최영관, 조윤오 “우리나라 사이버 테러 실태 및 대용 방안에 관한 연구: 경찰 사이버보안 전문가를 대상으로”, 『한국경찰학회보』, 19권(2017.)

최은미, “강제동원문제를 둘러싼 한일갈등의 전개와 향후 전망”, 『주요국제문제분석』, 제31호(2019.)

하대성, “한국의 독도 위기관리 DKD 모델”, 경북대학교 대학원 박사학위 논문(2021.)

_____, 이정태, “독도의 전략적 가치와 독도방어 전략의 특수성”, 『대한정치학회보』 제30집 3호(2022.)

_____, “하이브리드 전쟁과 독도 사이버 방어전략”, 2023년 경북대학교 평화문제연구소 춘계 평화포럼 발표자료(2023.04.07.)

허태회 외, “세계 주요 강대국들의 정보전 준비와 대응체계”, 『국방연구』, Volume 49, Issue 1(2006.)

홍규덕, “하이브리드 전쟁의 역설: 우크라이나 전쟁의 교훈”, 『전략연구』, Volume 29, Issue 2(2022.)

Chekinov, S. and S. Bogdanov. 2013. “The Nature and Content of a New-Generation War.” Military Thought (October-December)

Christian Bueger & Tobias Liebetrau, Jonas Franken, “Security threats to undersea communications cables and infrastructure - consequences for the EU.” IN-DEPTH ANALYSIS, European Parliament(2022)

Joseph D. Celeski, “Psychological Operations－A Force Multiplier.” Special Air Warfare and the Secret War in Laos, Air University Press(2019)

Martin Libicki, “What is information Warfare?”, 『Strategic Forum』, No.28(1995.)