러시아의
사이버 안보전략

2024

한국사이버안보학회
KACS

한국사이버안보학회 워킹페이퍼 24호
발간일: 2024년 8월 25일

윤민우 (가천대학교)

Ⅰ. 머리말

정보통신기술의 빠른 발전과 네트워크 사회의 등장으로 인해 사이버 공간은 의미 있는 실체적 전략공간으로 자리매김하였다. 특히 사이버 공간은 전쟁과 평화의 시기적 구분이 애매모호한 특성을 가진 다영역전쟁(multi-dimensional warfare) 환경에서 땅, 바다, 하늘, 우주 등의 물리적 공간과 인간의 인지-의식(cognition-perception) 영역 등 다른 공간 또는 영역들을 이어주는 전략적 연결통로로서의 중요한 가치를 지닌다. 따라서 사이버 공간을 누가 지배할 것인가에 따라 강대국들의 패권투쟁의 결과가 주요하게 영향을 받을 수 있다. 이 때문에 오늘날과 미래의 안보환경에서 미국, 러시아, 중국, EU(European Union) 등 강대국들의 국가안보전략에서 사이버 안보전략이 차지하는 비중은 날로 커지고 있다.

오늘날 전, 평시를 막론하고 수행되는 사이버 에스피오나지(espionage), 사이버 인지전, 사이버 테러, 또는 사이버 전쟁 등과 같은 각종 사이버 공간을 통한 위협들은 심각한 안보문제로 등장했다. 이는 분명하고 실존하는 위협이다. 이 같은 사이버 안보의 중요성을 감안할 때, 해외 주요 강대국들의 사이버 안보전략을 살펴보고, 분석·평가해보는 것은 의미가 있다. 이런 맥락에서 이 글은 해외 주요 사이버 안보 강대국들 가운데 러시아의 사이버 안보전략을 들여다볼 것이다.

러시아의 사이버 안보역량은 세계적으로 매우 높은 수준인 것으로 평가된다. 러시아는 대략 2000년경부터 국가차원에서 사이버 안보전략을 마련하고 발전시켜오고 있으며 이와 연계하여 정책, 전략, 법령, 추진체계 등을 구축하고 운용해 오고 있다.[1] 러시아의 사이버 역량 및 군사력은 현재 매우 높은 수준으로 평가되고 있다. 하버드 대학교 벨퍼 센터의 국가 사이버 역량 인덱스 2022에 따르면,[2] 2022년 현재, 러시아의 총체적인 사이버 국력은 미국(1위)과 중국(2위)에 이어 3위에 랭크된 것으로 나타났다. 특히 러시아는 총체적인 사이버 국력 평가에 포함된 8개 세부 항목들 가운데 사이버 안보역량과 직접 관련된 사이버 공격능력과 정보통제 부문에서 미국에 이어 2위를 차지했다.[3] 이밖에도 대체로 러시아의 해킹 등 사이버 공격능력과 선거개입, 영향력 공작 등과 같은 사이버 인지전 역량은 매우 높은 수준인 것으로 평가되고 있다. 실제로 러시아는 현재진행형인 러시아-우크라이나 전쟁에서 탁월하고 공격적인 해킹과 멀웨어 등의 사이버 기술공격 역량과 가짜뉴스, 허위조작정보 등의 영향력 공작 능력을 보여주고 있다. 이 같은 점들

1) 양정윤·박상돈·김소정. 2018. “정보공간을 통한 러시아의 국가 영향력 확대 가능성 연구: 국가 사이버안보 역량 평가의 주요 지표를 중심으로.” 『세계지역연구논총』, 36집, 2호, p. 134.
2) Julia Voo, Irfan Hemani, and Daniel Cassidy, “National Cyber Power Index 2022,” Report, September 2022, Harvard Kennedy School, Belfer Center for Science and International Affairs.
3) pp. 9-12.

을 고려하면 러시아의 사이버 안보전략을 살펴보고 그 특성들을 분석, 평가해보는 것은 주요한 의미가 있다.

Ⅱ. 러시아의 사이버 안보 개념과 인식

러시아의 사이버 안보에 대한 접근은 러시아의 지정학적 사고가 그대로 투영되어 있다. 러시아의 사이버 안보에 깔린 가장 근본적인 인식론은 러시아와 러시아 인근 지역을 독자적인 러시아/유라시아 문명(Russian/Eurasian civilization) 공간으로 보는 것이다. 이러한 인식론에 기초하여 사이버 전쟁은 미국이 이끄는 대서양 문명(Atlantic civilization)으로부터 초래되는 정보적 적대행위(informational aggression)이며 러시아의 사이버 안보는 이에 대한 대응행동이라고 이해된다. 이와 같은 러시아의 사이버 안보에 대한 개념과 인식은 러시아의 지정학적 사고 및 전략과 긴밀하게 연계되어 있다.[4)]

러시아는 인터넷을 미국 및 서방과는 다르게 인식한다. 미국과 서방은 인터넷을 정보와 개인의 연결성(connectivity), 공유(sharing), 그리고 개방성(openness)에 의해 작동되는 하나의 전일적인 공간으로 인식한다.[5)] 하지만 러시아는 이러한 미국-서방의 인식에 반대한다. 러시아는 글로벌 인터넷을 미국이 일방적으로 기술적, 문화적, 정신적으로 지배하는 공간으로 인식한다. 따라서 이러한 미국 주도의 글로벌 인터넷으로부터 러시아 부분(segment)을 따로 떼어내어 러시아 국가의 통제아래 러시아의 주권이 작동하는 독립된 공간으로 구축하고 싶어 한다. 러시아는 이를 '디지털 주권(digital sovereignty)'이라고 정의하며 국가는 디지털 환경에서 지정학적 국가이익을 독립적으로 결정하기 위한 권리와 능력을 가져야 한다고 주장한다.[6)] 러시아는 이러한 디지털 주권개념에 따라 글로벌 인터넷 공간은 독립적으로 격리된(self-contained) 각각의 디지털 주권의 영역으로 분할되어야 하며 각각의 격리된 사이버 영역(cyber domain)내에서 국가의 배타적 주권과 다른 국가나 외부 행위자로부터의 불간섭의 원칙이 지켜져야 한다고 주장한다.[7)]

러시아는 사이버 안보의 위협을 디지털 주권공간에 대한 위협으로 인식한다. 이 같은 사이버 안보의 개념에는 해킹, 디도스, 멀웨어 등과 같은 물리적, 기술적 침해뿐만 아니라 러시아의 문화적, 정신적, 그리고 도덕적 가치를 위협하는 정보내용도 포함된다. 이것이 사이버 안보에 대한 인식에서 미국-서방의 그것과 차별되는 지점이다. 러시아는 정보의 내용(content)을 미국-서방과는 달리 사이버 안보 위협으로 인식한다. 러시아에서는 이러한 정보의 내용과 관련된 위협이 "사

4) J. Darczewska, "The anatomy of Russian information warfare: The Crimean operation, a case study." *Point of View*, No. 42, OSW(Osrodek Studiow Wschodnich) Center for Eastern Studies, Warsaw, (May 2014). p. 5.

5) M. Ristolainen, "Should 'RuNet 2020' be taken seriously? Contradictory views about cybersecurity between Russia and the West." in J. Kukkola, M. Ristolainen, and J-P. Nikkarila eds. Game Changer Structural transformation of cyberspace. Puolustusvoimien tutkimuslaitoksen julkaisuja 10 (Finnish Defence Research Agency Publications 10), Finnish Defence Research Agency (2017), p. 8.

6) J-P. Nikkarila and M. Ristolainen, "'RuNet 2020' - Deploying traditional elements of combat power in cyberspace?" in J. Kukkola, M. Ristolainen, and J-P. Nikkarila eds. Game Changer Structural transformation of cyberspace. Puolustusvoimien tutkimuslaitoksen julkaisuja 10 (Finnish Defence Research Agency Publications 10), Finnish Defence Research Agency (2017), pp. 30-31.

7) J. Kukkola, J-P. Nikkarila, and M. Ristolainen, "Asymmetric frontlines of cyber battlefields," in J. Kukkola, M. Ristolainen, and J-P. Nikkarila eds. Game Changer Structural transformation of cyberspace. Puolustusvoimien tutkimuslaitoksen julkaisuja 10 (Finnish Defence Research Agency Publications 10), Finnish Defence Research Agency (2017), p. 77.

회적-인도적 영역에 영향을 미치기 위한 정보내용의 사용위협"으로 표현된다.

이 같은 기조에 따라 러시아는 사이버 안보의 위협을 정보-기술(information-technology)과 정보-심리(information-psychology) 구분하여 양자를 모두 정보안보(information security)의 위협으로 통합적, 전일적(holistic)으로 인식한다. 정보기술은 주로 악성코드(hostile code)를 활용한 하드웨어나 소프트웨어 또는 네트워크 기반설비에 대한 물리적 공격위협을 의미한다. 반면 정보심리는 대중들의 도덕과 인식에 대해 공격하는 작전을 의미하며 아랍의 봄(Arab Spring), 오렌지 혁명(Orange Revolution), 그리고 소련의 붕괴 등과 같은 사례가 여기에 포함한다. 러시아는 정보의 내용과 관련된 위협을 정보-심리의 영역에 속하는 것으로 이해하면서 인터넷 상에서의 적대적이거나 파괴적인 정보의 내용 역시 주요한 정보안보의 위협으로 받아들인다.[8)]

러시아는 사이버 안보를 이해함에 있어 전쟁과 평화를 시기적으로 이분법적으로 구분되는 개념이 아니라 일련의 연속된 스펙트럼 상의 어떤 단계 또는 상태로 인식한다. 러시아는 평화-전쟁 스펙트럼을 4개의 하위유형으로 구분한다. 이는 ① 평화적 공존, ② 이해관계의 갈등 또는 자연적 경쟁, ③ 무장충돌, 그리고 ④ 전쟁(a full-scale war)이다. 러시아의 개념으로 전쟁은 어떤 특정 시기에 국한된 의미가 아니며 단계적으로 이해갈등과 충돌이 격화되어 가는 과정이다.[9)] 사이버 공격-방어는 "이해관계의 갈등 또는 자연적 경쟁", "무장충돌", 그리고 "전쟁"의 단계 모두에서 국가 행위자의 전략-전술적 의지(will)나 이해(interest)를 관철하고 목표(objective)를 달성하기 위한 주요한 수단(means)이 된다. 전면전 이전의 단계인 "② 이해관계의 갈등 또는 자연적 경쟁"과 "③ 무장충돌"의 단계들에서의 사이버 공격행위들은 사이버 범죄, 핵티비즘, 사이버 테러, 사이버 간첩(또는 사이버 스파이)활동 등으로 나타난다. 사이버전(cyberwarfare)은 본격적인 전쟁개시 직전의 단계에서 예비공격 또는 선도공격으로 사용되거나 물리적 또는 키네틱 전쟁과 함께 수행된다. 2022년 러시아-우크라이나 전쟁발발 직전에 우크라이나 정보통신망을 상대로 전개된 사이버-기술 공격과 전면전 수행과정에서 관찰되는 사이버-기술 공격과 사이버 영향력 공작 등은 이 같은 전쟁 단계에서의 사이버전 수행의 대표적인 사례들이다.[10)]

러시아의 이 같은 사이버 안보개념과 인식에 주요한 토대가 되는 것은 게라시모프의 제안들이다. 이에 따라, 러시아는 전통적인 피와 폭력을 동반한 물리적 폭력충돌을 넘어 사이버 심리전과 사이버 기술공격, 외교적 압박과 경제적 위협, 그리고 테러리즘과 같은 비전쟁적 방식(Невоенный метод)을 적극적으로 새로운 전쟁개념의 범주에 포함시키고 있다. 사이버 공격을 포함한 여러 비군사적 방법과 전통적 군사적 방법의 적절한 비율은 4:1 정도가 적절한 것으로 제시된다. 게라시모프 제안에 따르면, 오늘날 전쟁의 게임규칙(rules of war)은 바뀌고 있으며, 비군사적 수단이 군사적 수단보다 더 효과적이다.[11)]

이 같은 게라시모프의 제안들을 요약하면, 다음과 같은 몇 가지 핵심 포인트들이 식별될 수 있다. 첫째, 갈등에는 점차적으로 더 많은 정보와 다른 비군사적 수단들이 포함된다. 둘째, 비밀작전과 비정규부대가 오늘날의 전쟁에서 점차 더 중요해지고 있다. 셋째, 전략적(strategic), 작전적(operational), 전술적(tactical) 수준들 사이의 구분과 공격과 방어의 작전들의 구분이 사라지고 있다. 넷째, 정보무기는 적의 이점에 대응하는 비대칭적 작전을 가능하게 해주고 적 영토의

8) S. A. Medvedev, "Offense-Defense theory analysis of Russian cyber capability." Thesis, Naval Postgraduate School, Monterey, California (2015), p. 47.
9) Nikkarila and Ristolainen, "RuNet 2020-Deploying traditional elements of combat power in cyberspace?" p. 194.
10) 윤민우·김은영, 모든전쟁: 인지전, 정보전, 사이버전, 그리고 미래전쟁에 대한 전략이야기 (서울: 박영사, 2023), p. 109.
11) Ibid, p. 95.

전반에 걸친 저항전선의 형성을 가능하게 해준다. 다섯째, 정보전쟁은 적의 전투능력을 떨어뜨리는 기회를 만들어낸다. 사이버 기술공격 및 사이버 영향력 공작은 여기서 매우 핵심적인 비군사적 활동을 구성한다. 그것은 전략적이면서 동시에 작전적이고 전술적인 성격을 갖는다. 또한 그와 같은 사이버 공격의 주체는 군과 정보기관뿐만 아니라 민간부문을 모두 포함한다. 이런 측면에서 전투원과 비전투원 간의 전통적인 구분은 그 의미가 퇴색된다.[12)]

Ⅲ. 러시아의 국가 사이버 안보 기본전략

러시아의 국가 사이버 안보 기본전략의 가장 근간이 되는 것은 러시아의 철학적 인식론, 문명사적 자기이해, 그리고 지정학적 인식이다. 이를 바탕으로 러시아의 국가안보전략이 구성되며, 이 국가안보전략은 다시 정보안보(information security)전략의 근간이 된다. 러시아의 사이버 안보 기본전략은 이 정보안보전략의 한 부문에 해당한다. 앞서 언급한 바대로 러시아는 정보안보를 사이버 안보와 오프라인에서의 방송, 라디오, 신문, 저널, 도서 등 전통적인 커뮤니케이션 채널들을 함께 아우르는 개념으로 이해한다. 따라서 사이버-기술과 사이버-심리를 포함하는 사이버 안보는 당연히 정보안보의 개념 안에 포함되어 이해된다. 이 같은 러시아의 국가 사이버 안보 기본전략과 관련된 주요한 상위수준의 인식론과 전략들을 자세히 소개하면 다음과 같다.

첫째, 러시아의 가장 최상위의 국가안보전략을 구성하는 근간이 되는 것은 러시아의 철학적 인식론과 문명사적 자기이해이다. 푸틴 러시아는 이반 일린(Ivan Ilyin), 니콜라이 베르댜예프(Nicolai Berdyaev), 블라디미르 세르게예비치 솔로비요프(Vladimir Sergeevich Solovyov)와 같은 여러 국가주의자-유라시아주의자들의 정치철학의 영향을 받았다. 역사적으로 '러시아 정체성', '단 하나의 슬로바키아 국가건설', '러시아 정교' 등 서구의 합리주의나 지성주의와 구별되는 러시아적 사상과 역사관, 국가관은 러시아의 역사를 따라 존재해 왔다고 이들은 인식한다. 이러한 영향을 받은 푸틴의 철학, 이념, 러시아에 대한 인식을 의미하는 핵심 키워드들은 다음과 같다. 그것들은 국가사회주의(national socialism), 나쉬즘(Nashism), 러시아 민족영토회복주의(Russia irredentism) (과거 러시아 제국과 소비에트 연방영토의 회복을 의미하는), 역사수정주의(historical revisionism), 굴욕적 역사, 반서구주의, 그리고 반미주의(Anti-Americanism) 등이다.[13)]

푸틴에 대한 포린어페어스(Foreign Affair)의 평가는 다음과 같다. "...푸틴은 메시아적 러시아 국가주의자이며 유라시아니스트이다. 그의 끊임없는 역사적 영감은 키예프 루스 때로 되돌아간다..." 이런 맥락에서 보면 오늘날 러시아-우크라이나 전쟁은 푸틴에게는 '러시아 주의'나 '슬로바키아 국가관'에 기반을 둔 천년 이상 지속되는 전쟁의 한 챕터에 해당한다. 푸틴은 이러한 사상과 철학에 기반을 두고 러시아인들에게 깊이 뿌리내린 러시아 정교식 도덕관과 러시아의 정체성을 복원하고 찬양함으로서 권위주의적 중앙정부에 의한 지배를 정당화하려고 기도한다.[14)] 이와 함께 푸틴은 구소련연방 국가들과 그 외 러시아의 전략적 이익이 걸린 모든 지역에서 러시아의 국익을 수호하는 것이 러시아의 사명이라고 주장한다.[15)] 결국 이렇게 볼 때 푸틴이 그리는 러시

12) 윤민우, "사이버 공간에서의 심리적 침해행위와 러시아 사이버 전략의 동향," 한국범죄심리연구, 14(2) (2018), p. 96, 100.
13) 윤민우·김은영, 모든전쟁: 인지전, 정보전, 사이버전, 그리고 미래전쟁에 대한 전략이야기, pp. 446-450.
14) Ibid.
15) Ibid.

아 미래비전은 서구국가들과는 문화, 종교, 정신적으로 차별화된 러시아적 정체성 위에 글로벌 강대국의 한 축으로 과거 러시아 제국과 구소련의 영토를 회복한 신러시아 제국을 건설하는 것이다.

둘째, 러시아의 국가안보전략은 러시아의 지정학적 인식과도 관련이 있다. 2000년 푸틴 정권의 출범을 기점으로 러시아는 지속적으로 강한국가(Superpower)를 재건하고 미국 주도의 단극질서를 다극질서로 바꾸려고 시도해왔다. 그리고 그러한 다극질서에서 러시아가 주도하는 세력공간(sphere of influence)을 확보하고자 노력해왔다. 이러한 러시아 주도의 세력 공간은 러시아 연방을 포함하여 근외지역(Near Abroad)으로 정의하는 이전 소비에트 연방에 속했던 주변국가들을 포함하는 지리적 범위에 해당한다. 러시아는 미국과 서방의 세력침투로부터 이 러시아의 세력공간을 방어하고 재건하는 것이 지난 20년 넘게 푸틴 정권의 지정학적 전략의 핵심이었다. 최근 2022년 러시아-우크라이나 전쟁 역시 이러한 맥락의 연장선상에 있다. 이와 같은 러시아의 국가안보전략에 깔린 가장 근본적인 인식론은 러시아와 러시아 인근 지역을 독자적인 러시아/유라시아 문명(Russian/Eurasian civilization) 공간으로 보는 것이다. 이러한 인식론에 기초하여 물리적 및 사이버 공간에서의 사이버 안보를 포함하는 정보-군사충돌은 미국이 이끄는 대서양 문명(Atlantic civilization)으로부터 초래되는 적대행위(aggression)에 대한 러시아의 당연한 대응행동으로 정의된다.[16)]

셋째, 이 같은 철학적 인식론, 문명사적 자기이해, 그리고 지정학적 인식을 기반으로 러시아의 국가안보전략이 구성되었다. 러시아는 2015년 12월에 대통령령 683호로 발표된 러시아 국가안보전략 2020(Стратéгия национальной безопасности Российской Федерации 2020)에서 국가안보 수호를 위한 포괄적 중·장기 전략방안을 제시하였다. 이는 러시아의 중·장기적 국가전략 목표를 나타냄과 동시에 푸틴 정부의 미래구상과 위험평가 등에 대한 시각을 보여준다. 전략에서는 러시아가 대외 위협에 능동적이고 적극적으로 대처할 것이며, 국제사회에서 러시아의 지위를 강화하는 한편 국민의 삶의 질 개선을 위해 노력할 것임을 밝힌다. 이 같은 메시지가 향하는 지향점은 유라시아 공간에서 러시아 세계질서(the Russian world order)를 구축하고 이에 대한 미국-나토로부터의 위협을 공세적 방어(offensive defense)로 억제하는 것이다. 또한 미국 주도의 단극질서를 미국과 러시아, 그리고 중국 등의 강대국들이 각각의 권역으로 분할하는 다극질서로 변화하려고 지향한다.

최근 2021년 6월 2일에 러시아 연방의 새로운 국가안보전략(Стратéгия национальной безопасности Российской Федерации)이 발표되었다. 이는 러시아가 1997년에 처음 국가안보전략을 발표한 이후로 5번째 국가안보전략이다. 새로운 국가안보전략에서도 러시아의 국제질서에 대한 인식은 이전 전략서와 마찬가지로 변함없이 계속되었다. 러시아는 단극질서를 거부하며, 다극질서를 지향한다. 2015년 국가안보전략 2020과 다른 유일한 점은 이전 문서에는 “다극세계(multipolar world)”라고 표현한 것을 새로운 문건에서는 “다중심세계(polycentric world)”라고 표현한다. 하지만 결국 이 둘은 같은 의미로 이해할 수 있다. 새로운 전략서에서도 러시아는 스스로를 다중심세계의 한 축을 담당하는 강대국이자 글로벌 리더로 스스로를 인식한다. 동시에 미국과 서방에 대해 매우 적대적인 태도를 견지하고 있다. 특히 2015년 전략서와는 달리 새로운 전략서에서는 더 이상 EU와 미국 등과 어떤 종류의 협력이 가능할 것이라고 여기지 않고 있다. 이는 매우 주목할 만한 변화이다.[17)]

16) J. Darczewska, “The anatomy of Russian information warfare: The Crimean operation, a case study.” *Point of View*, No. 42, OSW(Osrodek Studiow Wschodnich) Center for Eastern Studies, Warsaw, (May 2014). pp. 5-6.

특히 새로운 전략서는 러시아 사이버 안보전략과 관련된 중요한 내용을 담고 있다. 러시아는 초국가 정보통신 기업들이 러시아에 대한 서방의 핵심 무기 가운데 하나라고 인식한다. 이에 따라 러시아는 이들 국제 소셜네트워크(특히 페이스북이나 트위트 등)에 대한 적극적인 프로파간다를 시작했다. 러시아는 파괴적인 정보-심리 영향력으로부터 러시아 사회를 보호하고 러시아의 안전한 정보공간을 발전시킬 것을 강조하고 있다. 이 같은 새로운 전략서에 담긴 러시아의 기조는 국제 소셜네트워크가 러시아 대중들에게 미치는 영향력에 대해 심각하게 고려하고 있다는 것을 알려준다.[18)]

반면 서방과 자유주의의 가치들은 러시아의 허위조작정보(disinformation)와 프로파간다의 타깃이 되고 있다. 러시아는 서구와 자유주의 가치들이 타락의 길로 들어섰다는 것을 입증하고, 서구가 전통적인 가치들에 대항해 싸우고 있다는 사실을 보여주며, 전통적인 가치들의 유일한 수호자가 러시아 자신이라는 사실을 제시한다는 목표를 가지고 있다. 2015년 전략서에서 러시아는 이 같은 정신적이고(spiritual) 도덕적인(moral) 가치들을 특히 강조했는데 새로운 전략서에서는 이를 더욱 강조하고 있다.[19)] 이 같은 맥락에서 러시아의 새로운 전략서에서는 사이버 안보전략과 관련해서 특히 정보-심리 측면에 상당한 비중을 두고 있다고 평가할 수 있다.

러시아의 정보안보전략은 국가안보전략의 하위단위의 세부실행전략에 해당한다. 앞서 언급한 대로 러시아는 사이버 안보(cyber security)를 정보안보(information security)로 이해한다. 따라서 러시아의 사이버 안보전략은 정보안보전략에 담겨 있다. 러시아의 정보안보전략은 상위의 국가안보전략의 기조에 따라 정보안보에 관하여 정보공간에서 국가주권강화 및 인터넷 거버넌스 체계를 개선할 것에 대한 의지를 표방하고, 국가의 정보통제권 인정을 주장한다. 러시아의 정보안보에 관한 기본전략의 세부사항은 다음과 같다. ① 러시아 국가안보전략은 국가안보의 위협요소로 첨단기술을 활용한 불법행위 및 정보전을 명시하였으며, 국가안보 과제에 정보안보를 포함시켰다. ② 전 세계적으로 증가하는 정보 및 정보통신기술을 이용한 분쟁에 대한 우려를 표명하였다. ③ 국가안보를 저해하는 요소로 정보기술, 통신, 고도화된 기술 활용을 통한 불법 활동을 명시하였다. ④ 정보안보 확보 노력으로 공공안전을 저해하는 파시즘, 극단주의, 테러주의, 분리주의 운동에 정보통신 기술 활용가능성을 제시하였다. ⑤ 국민의 삶의 질 증진 및 국가기관에 대한 위협 감소 방안으로 정보 통신기반시설을 발전시키고, 국민의 사회적·경제적·정신적 활동과 관련된 정보 및 정보통신기술에 대한 접근성을 강화할 것을 지적하였다. ⑥ 경제안보 위협요소로 정보기반시설의 취약성을 지적하였다. ⑦ 국가안보 확보를 위한 노력의 일환으로 국제 정보안보체제 형성 노력에 참여할 것과 러시아의 전통과 정신적 가치를 수호하기 위해 인터넷 매체 등을 통한 외국의 문화 유입에 대한 방어 태세를 강화할 것임을 명시하였다(양정윤 외, 2018, pp. 146-147).

이와 같은 러시아의 정보안보 기본전략은 다음과 같은 특성을 갖는다. 먼저 방어적 속성이 강조되어 있다. 이는 미국-서방의 패권적인 문명적, 정보적 영향으로부터 러시아의 독자적인 문명권을 보존하고 방어해야 한다는 시각이 깔려있음을 의미한다. 다음으로 러시아인들은 정보전쟁을 정보무기로서의 정보 자원을 통제하기 위해 특별한 수단을 사용함으로서 정보공간 내에서 서로 다른 국가들에 의해 채택되는 다른 문명적 시스템들 사이의 경쟁의 한 부분으로 대중의 의식에 영향을 미치는 것으로 이해한다는 점이다. 그들은 따라서 군사와 비군사적 서열(order)[20)]과 기

17) Giorgi Bilanishvili, “On the New National Security Strategy of the Russian Federation,” Security Review, Rondeli Foundation, https://gfsis.org.ge/publications/view/3011
18) Ibid.
19) Ibid.
20) 서열은 전투서열을 의미한다.

술적(사이버공간)이고 사회적인(정보공간) 서열(order)을 혼합하여 사용한다.[21] 즉, 바꾸어 말하면 APT와 멀웨어 공격 같은 기술적 해킹공격과 영향력 공작(influence operation)과 같은 정보심리 공격을 함께 통합적으로 운용한다. 이와 같은 전형적인 사례는 2016년 러시아의 미국대선 개입사례이다.[22]

Ⅳ. 사이버 안보 추진전략

러시아의 사이버 안보 추진전략은 국가 사이버 안보 기본전략에 따라 미국-서방과는 다른 독특한 특성을 가진 두 개의 핵심기조로 구현된다. 먼저 러시아는 앞서 언급한 대로 미국-서방의 하이브리드전이나 사이버전보다는 정보전쟁(information war) 또는 정보충돌(information confrontation)의 개념으로 접근한다. 러시아의 시각에서는 정보전쟁은 사이버 공간, 오프라인에서의 정보통신, 그리고 대중의 심리 및 여론 등을 모두 포함하는 공간에서의 충돌 또는 공격-방어이다. 따라서 러시아는 사이버 상에서의 악성 코드와 같은 물리적, 기술적 침해뿐만 아니라 러시아의 문화적, 정신적, 그리고 도덕적 가치를 위협하는 정보내용 역시 전쟁 또는 충돌의 대상으로 인식한다. 이와 함께, 러시아는 앞서 언급한대로 이 같은 전쟁 또는 충돌은 2022년 2월 발발한 러시아-우크라이나 전쟁과 같이 전통적인 의미에서의 전쟁(a full-scale war) 상태에서만 나타나지 않으며 전면전 이전의 상태에서 상시적으로 정보전쟁 또는 정보충돌이 수행될 수 있다고 본다. 이 같은 러시아의 인식은 평화-전쟁의 시기적 혼재성 또는 통합성에 기초하여 군사부문에서의 통합적 정보전쟁 추진전략으로 나타난다.

다음으로 러시아는 사이버 공간을 러시아의 배타적인 주권공간으로 인식한다. 이 같은 러시아의 사이버 공간에 대한 접근에는 러시아의 지정학적 사고가 그대로 투영되어 있다. 러시아는 글로벌 인터넷을 미국이 일방적으로 기술적, 문화적, 정신적으로 지배하는 공간으로 인식한다. 따라서 러시아는 미국 주도의 글로벌 인터넷으로부터 러시아 부분(segment)을 따로 떼어내어 러시아 국가의 통제아래 러시아의 주권이 작동하는 독립된 공간으로 구축하고 싶어 한다. 러시아는 이를 “디지털 주권(digital sovereignty)이라는 개념으로 정의하며 국가는 사이버 공간에서도 배타적이고 독점적인 디지털 주권과 통제권을 갖는다고 주장한다. 러시아가 이해하는 주권의 개념은 미국-서방과는 다르다. 러시아의 주권에는 이념, 가치, 체제, 문화, 정신, 교육, 종교적 가치 등의 배타적 독자성과 국가에 의한 통제도 포함된다. 이는 배타적인 독자문명공간으로서의 미국-서방과 구별되는 러시아 세계의 지정학적 인식이 사이버 공간에 그대로 투영된 것이다. 이 같은 러시아의 사이버 공간에 대한 인식에 따라 러시아는 자신들의 인터넷망을 글로벌 인터넷망으로부터 분리하여 주권의 개념에 따라 국가가 통제하는 공간으로 구축하려는 목표를 가지고 있으며 이를 위한 추진전략을 실행하고 있다. 러시아의 비군사부분 사이버 안보 추진전략은 주로 이와 같은 러시아의 독자적 인터넷망 구축과 이에 대한 국가통제의 강화에 초점이 맞추어져 있다.

1. 군사부문

21) Darczewska, “The anatomy of Russian information warfare: The Crimean operation, a case study,” p. 12.
22) 윤민우·김은영, 모든전쟁: 인지전, 정보전, 사이버전, 그리고 미래전쟁에 대한 전략이야기, pp. 434-435.

러시아는 이 같은 “정보전쟁” 개념인식에 따라 전, 평시를 막론하고 사이버작전을 수행하고 있다. 이 같은 정보전쟁은 우크라이나 사례에서 보듯 본격적인 군사적 침공 직전단계나 전쟁수행 과정에서 적대국 정보통신망에 대한 사이버 기술공격과 허위조작정보 유포 형태로 나타나기도 하며, 선거개입, 여론조작과 영향력 공작, 해킹을 통한 사이버 스파이 활동 등과 같은 다양한 평시 사이버 작전의 모습으로 나타나기도 한다. 이 같은 정보전쟁 전략수행의 핵심 컨트롤타워는 러시아 연방군이나 정보기관들이다. 이 같은 국가기관들은 책임 부인성(deniability)를 위해 다양한 민간 해커들과 핵티비스트들과 같은 비국가 행위자들을 은밀히 지휘통제, 지원, 사주하여 사이버 작전을 수행한다.[23)]

러시아의 정보전쟁 수행 추진전략은 미래전에서의 전략목표달성을 위해서는 비군사적 수단의 비중과 역할이 증대할 것이며, 이에 정보전쟁이 결정적인 역할을 할 것이라는 인식에 따라 마련되었다. 러시아는 정보전쟁을 통해 적국의 지휘통제와 정보통신 시스템, 의사결정 과정과 시스템, 국가 핵심기반시설, 여론 등을 교란, 파괴함으로서 적국의 정부, 군, 민간의 전쟁수행 의지와 역량을 약화 제거시킴으로서 전쟁을 승리로 가져가는 결정적 기반을 조성하는 것을 전략목표로 한다. 이 같은 러시아의 군사 사이버 추진전략의 목표는 물리적, 기능(논리)적, 인지(심리)적 효과를 모두 포함한다. 물리적 목적은 적국의 정보통신 네트워크를 직접적으로 파괴하거나 손상 또는 기능 조작을 유도하는 등 적국의 지휘통제 및 정보통신 시스템과 핵심기반시설 자체의 불능, 손상, 혼란, 기능저하를 유도하는 것이다. 기능(논리)적 목적은 적국의 논리 네트워크와 정보통신의 기밀성, 무결성, 가용성 등 정보보호 핵심목표에 대한 부정적 영향을 미침으로써 적국의 원활한 정보소통과 의사결정 과정을 지연, 방해하는 것이다. 인지(심리)적 목적은 적국 지도부, 군, 일반대중의 인지능력, 의사결정 및 심리반응 등에 부정적 영향을 미침으로써 전쟁 수행을 위한 심리적 기반을 교란-파괴하는 것이다.[24)]

러시아의 정보전쟁은 국가차원의 연방군과 정보기관들의 사이버 부대들은 물론 다양한 민간 또는 비국가행위자들이 최대한 동원, 활용되어 수행된다. 이와 같은 러시아 정보전쟁 수행의 가장 주요한 실행 컨트롤타워는 연방보안국(FSB), 연방군 총참모부 정보총국(GRU), 그리고 대외정보국(SVR)이다. 각각의 기관과 사이버 작전 수행의 핵심 부서 또는 부대들을 살펴보면 다음과 같다.[25)]

먼저 연방보안국은 해킹과 같은 사이버 기술공격과 정보심리전 또는 영향력 공작의 수행을 위한 핵심 부서이다. 이와 같은 비밀작전은 FSB의 정보안보센터(FSB’s Center for Information Security)에 의해 수행된다. 정보안보센터는 다양한 사이버 범죄자들과 해커들을 이용하여 비밀공작을 수행한다.[26)] 한편 연방보안국의 TSRRSS(Electronic Surveillance of Communication) 센터는 사이버 및 신호정보(SIGINT) 부문에서 임무를 수행하며 전자통신(electronic communications)의 인터셉션, 암호해독, 그리고 처리를 수행한다.[27)]

러시아 연방군의 사이버 작전의 핵심 기관은 정보총국(GRU)이다. 런던과 브뤼셀의 사이버 안보전문가들에 따르면,[28)] 정보총국은 해외에서의 공세적 정보전쟁(또는 충돌) 수행에 있어서의 가

23) 윤민우·김은영, “어나니머스 등 국제해킹조직의 핵티비즘 분석연구,” 2022년 12월 정보세계정치학회 연구보고서, p. 81.
24) 장세호, “러-우 전쟁 과정에서 나타난 러시아 사이버 공격 양상과 한국 사이버 안보에의 함의,” 한국사이버안보학회 2023 추계학술회의, 2023년 10월 11일.
25) 윤민우·김은영, “어나니머스 등 국제해킹조직의 핵티비즘 분석연구,” p. 81.
26) T. Maurer and G. Hinck, “Russia: Information Security Meets Cyber Security,” In F. Rugge. ed., Confronting an “Axis of Cyber.” (Milano, It: Ledizioni LediPublishing, 2018) p. 46.
27) Wolf Pack. “Supplement to the 2012/3 South African Cyber Threat Barometer: Russia Case Study Report,” (2019), www.wolfpackrisk.com

장 핵심적인 기관으로 평가된다. 정보총국은 연방보안국과 서로 영역이 중첩되며 경쟁관계에 있다. 대체로 러시아 국내 보안방첩에서는 FSB가 해외 정보공작과 비밀전쟁 수행에서는 GRU가 좀 더 상대적으로 우위에 있는 것으로 알려져 있다.[29] 정보총국은 특히 러시아의 군사전략 독트린에 따라 정보전쟁 또는 정보충돌의 수행을 위해 공격(offense)과 방어(defense)의 임무를 수행한다. GRU는 러시아에서 가장 큰 규모의 해외정보기관으로 알려져 있으며 가장 위험하고 복잡하며 중요한 국익이 걸려있는 작전들을 수행한다. GRU는 선거개입과 해킹, 정보-심리작전 등과 같은 해외에서의 공세적 러시아 정보전쟁(또는 충돌)의 가장 위협적이고 핵심적인 기관이다.[30] GRU는 암호기술 및 솔류션에 관한 최고의 기술 실행력을 보유한 것으로 알려져 있으며 FSB등과 공조하여 활동한다.[31] GRU는 FSB와 마찬가지로 해커들과 사이버범죄자들을 프록시로 활용하는 비밀작전(Covert Operation)을 수행한다.

GRU 산하에 사이버 작전 수행과 관련된 부대들은 다음과 같다. 우선 GRU는 15개의 국(directorates)으로 구성되어 있으며, 이는 지역별 4개국과 임무별 11개국으로 나뉜다. 이 가운데 사이버 공격-방어는 12국(Twelfth Directorate)이 핵심 부서인 것으로 판단된다.[32] 또한 GRU 산하 소속 부대 가운데 사이버 공격-방어와 관련된 임무를 수행하는 부대로는 Unit 54777, Unit 26165, Unit 74455 등이 있다. 54777부대는 72특수임무센터(72nd Special Service Center)로도 불리며, GRU의 가장 주된 심리전 수행부대이다. 이 부대의 위장조직으로는 InfoRos와 Institute of the Russian Diaspora 등이 있다. 26165부대는 Fancy Bear, STRONTIUM, 또는 APT28로도 알려져 있는 사이버 작전/해킹그룹이다. 74455부대는 Sandworm Team 또는 Main Center for Technologies로도 알려져 있다. 이 부대는 DC Leaks와 Guccifer 2.0 등과 같은 여러 다른 가짜 아이덴티티(fictitious identities)를 사용하며 맥시멈 정치적 충격/효과를 위해 위키리크스(Wikileaks)와 협조하면서 정치적으로 민감한 사이버 해킹을 통해 훔친 자료들을 공개한다. 이 부대는 2017년 NotPetya 공격과 함께 2018년 평창동계올림픽 사이버 공격에도 관여하였다.[33]

해외 정보활동(intelligence)이나 공작(covert operation)을 주로 하는 민간 국가정보기관인 대외정보국(SVR) 역시 사이버 정보활동 및 공작 임무를 수행한다. SVR은 과거 KGB의 1국(First Chief Directorate)이 담당하던 해외정보(Foreign intelligence)의 책임과 권한을 승계한 기관이다.[34] 또한 2003년 FAPSI가 해체되면서 FAPSI의 통신(communication)과 정보(information)에 관련된 정보안보 관련 책임의 일부를 승계 받았다.[35] SVR은 해외정보안보활동, 인간정보(HUMINT), 사이버 및 신호정보(SIGINT) 분야의 대외협력 업무를 담당하고 있으며 전략정보를 수집하며 해외 정보보호 및 통신시스템 구축에 관한 역할을 수행한다.[36] SVR은 업무수행을 위해 FSB와 다른 행정부 수사기관들과 마찬가지로 통신운용자들(communication operators)과 인

28) 인터뷰 자료
29) ITU(International Telecommunication Union), “Cyberwellness Profile Russian Federation,” ITU 웹사이트. (2016), http://www.itu.int/md/D14-SG02.RGQ-C-0143/en
30) 인터뷰 자료
31) 양정윤 외., “정보공간을 통한 러시아의 국가 영향력 확대 가능성 연구: 국가 사이버안보 역량 평가의 주요 지표를 중심으로,” pp. 140-141.
32) Andrew S. Bowen, “Russian Military Intelligence: Background and Issues for Congress,” Congressional Research Service R46616, (24 November 2020), p. 4.
33) GRU, https://en.wikipedia.org/wiki/GRU#cite_note-50
34) McCauley, Bandits, Gangsters and the Mafia, p. 406.
35) 양정윤 외., “정보공간을 통한 러시아의 국가 영향력 확대 가능성 연구: 국가 사이버안보 역량 평가의 주요 지표를 중심으로,” p. 140.
36) Ibid.

터넷 운용자들(internet operators)로부터 정보통신 관련 정보를 요청할 수 있으며 다른 정부기관들로부터 데이터베이스와 정보시스템을 요청할 권한이 있다(ICNL, 2016).[37] 네덜란드 정보부(Dutch General Intelligence and Security Service: AIVD)는 2016년 미국 대선에 개입했던 러시아 해킹 조직인 Cozy Bear가 FSB와 연계된 것이 아니라 SVR에 의해 지휘통제를 받았다고 주장했다. 미국의 민간 사이버보안회사인 CrowdStrike 역시 이와 같은 네덜란드 정보부의 추론에 동의했다.[38]

FSB, GRU, SVR 등은 해커들과 범죄자들, 그리고 애국적 핵티비스트들과 같은 민간 프록시(proxies) 병력들과 연계되어 있다. 이와 같은 민간 프록시들은 사이버 작전들(cyber operations)에 동원된다.[39] RBN(Russian Business Network) 등은 이러한 프록시의 사례에 해당한다. 프록시를 이용하는 이유는 비용-효과의 측면과 익명성과 러시아 정부의 책임 부인성(deniability)를 높이기 때문이다.[40] CyberBerkut라는 해커그룹은 2014년 우크라이나 선거 기반시설에 대한 공격으로 알려졌다.[41] 트롤팜(troll farm)이라고 불리는 IRA(Internet Research Agency) 역시 프록시 행위자에 해당한다. IRA는 러시아 정부로부터 금전적 지원을 받고 허위조작정보, 영향력 공작 등에 동원되는 민간회사로 알려져 있다.[42] 러시아-우크라이나 전쟁에서도 이와 같은 러시아 연방군 및 정보기관들과 해커들, 핵티비스트들의 연계가 관찰된다. 멀웨어와 피싱(phishing), DDoS 등으로 우크라이나 주요 타깃들에 대한 전방위적 사이버 공격을 감행했던[43] Sandworm은 GRU의 74455부대와 연계됐던 것으로 알려졌다.[44] 러시아 민간해커들은 미국과 다른 42개국의 100개 이상의 기관들의 네트워크에 침투하였고, 대용량 데이터를 절취했다.[45] 이와 함께, 정보심리전을 수행하는 익명의 친러시아 애국적 핵티비스트들은 소셜미디어에서의 여론과 내러티브 담론을 주도하기 위해 입증하거나 진위여부를 가리기 어려운 스크린샷(screenshots)과 문건들(caches of documents), 뉴스들을 포스팅했다.[46] 상트 페쩨르부르크에 위치한 러시아 인터넷 트롤들은 러시아의 우크라이나 침공을 지지하는 여론을 온라인에서 적극적으로 유포, 확산시켰으며, IRA의 트롤팩토리(troll factory)는 친크레믈린 내러티브를 유포, 확장시키는 활동을 특히 인스타그램과 유튜브, 그리고 틱톡 등에서 활발히 전개하였다. 이 가운데 핵심적인 역할이 “Cyber Front Z”라고 불리는 텔레그램 채널에 의해 수행되었다. 이와 같은 러

37) ICNL(The International Center for Not-for-Profit Law), “Overview of the Package of Changes into a number of Laws of the Russian Federation Designed to Provide for Additional Measures to Counteract Terrorism.”
38) SOCRadar, “APT Profile: Coza Bear/APT29,” November 16, 2021, https://socradar.io/apt-profile-cozy-bear-apt29/
39) Maurer and Hinck, “Russia: Information Security Meets Cyber Security,” p. 47.
40) Connell and Vogler, “Russia’s Approach to Cyber Warfare,” p. 11.
41) Connell and Vogler, “Russia’s Approach to Cyber Warfare,” pp. 23-24.
42) 송태은, “디지털 허위조작정보의 확산 동향과 미국과 유럽의 대응,” 주요국제문제분석 2020-13, 국립외교원 외교안보연구소, pp. 22-23.
43) James A. Lewis, “Cyber War and Ukraine,” CSIS(Center for Strategic & International Studies) Report, June 2022. https://www.csis.org/analysis/cyber-war-and-ukraine; James Pearson and Christopher Bing, “The cyber war between Ukraine and Russia: An overview,” Reuters, May 10, 2022. https://www.reuters.com/world/europe/factbox-the-cyber-war-between-ukraine-russia-2022-05-10/
44) Andy Greenberg, “Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine,” WIRED, April 12, 2022, https://www.wired.com/story/sandworm-russia-ukraine-blackout-gru/
45) Maggie Miller, “Russian hackers targeting U.S., other Ukraine allies,” POLITICO, June 22, 2022. https://www.politico.com/news/2022/06/22/russian-hackers-target-u-s-00041342
46) Pearson and Bing, “The cyber war between Ukraine and Russia: An overview.”

시아 트롤팜들은 “애국적 활동(patriotic activity)”으로 우크라이나에서의 “특별 군사 작전(Special Military Operation)”을 지원하는 업무를 위해 임금을 받고 고용된 인력들로 알려졌다.[47] IRA 이외에도 MediaSintez, NovInfo, Nevskiy News, Economy Today, National News, Federal News Agency, and International News Agency 등의 다수의 민간 참여자가 조직적으로 동원되었으며, 이들의 배후에는 러시아 연방군 또는 정보기관이 있었던 것으로 파악되었다.[48]

2. 비군사부문

러시아의 비군사부문 사이버 안보 추진전략은 “디지털 주권” 개념에 기초해 미국이 지배하는 글로벌 인터넷 공간과 분리-격리된 러시아의 배타적 인터넷 공간의 구축에 초점이 맞추어져 있다. 이는 사이버 안보전략임과 동시에 러시아의 과학기술 및 경제산업발전전략의 일환으로 추진된다. 이 같은 러시아의 비군사부문 사이버 추진전략은 러시아 국내에서의 보안방첩의 핵심 기관인 연방보안국과 함께 디지털발전통신언론부(Ministry of Digital Development, Communications and Mass Media of the Russian Federation: Mincomsvyaz)가 주도하고 있다. 이 같은 러시아의 독자적 국가통제 인터넷망 구축 추진전략을 간략히 살펴보면 다음과 같다.[49]

먼저, “정보 사회 국가프로그램 2011-2020”은 디지털발전통신언론부와 경제개발부에 의해 추진되었다. 이 프로그램은 정보자원에 대한 동등한 접근, 디지털 콘텐츠의 발전, 혁신적 기술의 도입, 그리고 정보안보에 대한 정부규제의 획기적 개선을 통해 정보와 통신기술의 혜택을 이용하는 기회를 개인들과 기업들에게 제공하는 것을 목표로 한다. 이 프로그램은 6개의 하위 프로그램으로 구성되어 있다. 이러한 하위 프로그램들은 ① 삶의 질과 비즈니스 활동의 조건 개선, ② E 정부와 효과적인 국가 거버넌스, ③ 정보 통신 기술을 위한 러시아 시장의 발전, ④ 디지털 갭을 연결하고 정보사회의 기초 기반시설(infrastructure)을 건설하기, ⑤ 정보사회에서의 보안, ⑥ 디지털 콘텐츠의 개발과 러시아 문화적 유산 보존 등이다.[50]

다음으로 러시아의 글로벌 인터넷망과 격리된 독자적 국가 인터넷망 구축사업인 RuNet 관련 세부 추진 전략들은 다음과 같다. 2016년에 Minkomsvyaz는 러시아 핵심 인터넷 기반시설 보호를 위한 “정보사회(Information Society)” 프로그램의 새로운 지침을 추가 배포하였다. 그 내용은 RuNet의 외부네트워크 의존성을 제거하는 것과 국가의 완전한 통제를 보장하는 것을 담고 있다. 2016년 6월부터는 RuNet을 글로벌 인터넷으로부터 단절시키기 위한 세부적인 기술 계획이 논의되었다. MSK-IX는 RuNet 백업 포메이션을 연구하기 시작했다. 2016년 여름에 Minkomsvyaz는 RuNet을 글로벌 인터넷으로부터 2020년까지 단절될 것이라고 선언했다. 이는 9월 모스크바 시와 지역정부, 국가 미디어 회사인 Rossiya Segodnya에서 오라클 데이터베이스가 공개출처 소프트웨어인 PostgreSQL로 교체되었다. 10월에는 러시아 군사 인터넷이 완전히

47) Staff and agencies, “Troll factory’ spreading Russian pro-war lies online, says UK,” The Guardian, May 1, 2022. https://www.theguardian.com/world/2022/may/01/troll-factory-spreading-russian-pro-war-lies-online-says-uk
48) Ibid.
49) 윤민우, “러시아 사이버 안보의 국내적 기반과 체제,” 신범식·윤민우·김규철·서동주 지음 러시아의 사이버 안보 (서울: 사회평론아카데미, 2021), pp. 102-113.
50) 신범식, “러시아 사이버 안보의 개념과 원칙,” 신범식·윤민우·김규철·서동주 지음 러시아의 사이버 안보 (서울: 사회평론아카데미, 2021), pp. 47-49.

작동하고 있다고 선언되었다. 2016년 10월 Minkomsvyaz는 자동 시스템(autonomous system), 인터넷의 러시아 국가 부분의 기반시설(infrastructure of the Russian national segment of the Internet), 그리고 러시아의 관점에서 national .ru 와 .pф 영역(zone) 도메인 네임 등록(domain name registrar)과 같은 기본 인터넷 기반시설 개념을 정의하는 새로운 법률 초안을 발표했다.[51]

한편 디지털 경제발전 프로그램 관련 세부추진 전략들은 다음과 같다. 2017년 3월에는 디지털 경제발전 프로그램 추진을 위한 IWG(Inter-agency Working Group)가 구성되었다. 8월에는 디지털 경제프로그램 수행을 관리하기 위한 도구로서 삶의 질과 비즈니스 조건(Quality of Life and Business Conditions)을 증진시키기 위한 IT의 사용에 관한 정부위원회(Government Commission)의 디지털 경제에 관한 분과위원회(Subcommittee)가 설치됐다. 이와 함께, 디지털 경제 발전을 위한 새로운 단계가 2018년 5월 대통령 명령(Presidential Decree) 과 함께 추진되었다. 이 명령은 2024년까지 국가 사회-경제적 발전의 목표와 집중지표들을 정의했다. 이 명령에 따라 2024년까지 디지털 경제 발전의 국내 비용이 2017년과 비교하여 3배 이상 증가해야 하며, 대용량 데이터의 하이 스피드(high-speed) 전송, 처리, 저장을 위한 안정적이고 안전한 정보(information)와 원격통신(telecommunication) 기반시설이 모든 조직들과 가구들이 접근할 수 있도록 구축되어야 하고, 정부당국과 지방정부, 그리고 조직들이 국내산 소프트웨어를 주로 사용해야 한다. 그러한 국가 프로그램의 발전은 승인된 디지털 경제 프로그램과 액션플랜에 그 근거를 둔 Minkomsvyaz에 의해 주도된다.[52]

마지막으로 매일 매일의 사이버 보안관리와 관련된 규제, 감시와 연구개발 세부정책들은 다음과 같다. 2012년 Minkomsvyaz는 “깨끗한 인터넷(Clean Internet)” 프로젝트를 추인했다. 이에 따라 “안전한 인터넷 연맹(Safe Internet League)”이 만들어지고 인터넷 감시활동을 수행한다. 이 밖에 러시아의 공무원들은 임의대로 법원명령 없이 인터넷 자료들을 쉽게 폐쇄할 수 있으며, 경제적이고 도적적인 이유로 인터넷 검열을 도입하고 인터넷으로부터 유해한 내용들을 제거할 수 있고, 필요하다면 전체 웹사이트들을 폐쇄하는 것이 쉽고 완전히 합법적이다. 이와 관련하여 통신업자들(무바일 폰 서비스 공급자들과 같은)과 인터넷 서비스 공급자들은 모든 사용자들의 모든 통신과 활동들을 기록하고 저장하도록 요구된다. 한편, 러시아는 사이버 공간을 감시하는 소프트웨어에 투자하며, 사이버 범죄에 대한 소프트웨어와 기술을 발전시키는데 있어 세계에서 선도적이다.[53]

한편 연방보안국(FSB)는 이 같은 Minkomsvyaz가 주도하는 러시아 독자 인터넷망 구축사업과 국가통제에 사실상의 컨트롤타워로서의 역할을 수행한다. FSB는 러시아 인터넷 망에 대한 컴퓨터 침해사건 대응, 감시와 정보, 수사 및 법집행, 국가핵심기반시설보호 등의 사이버 보안방첩 임무를 수행할 뿐만 아니라 기술개발과 산업생산에서 규제와 면허 업무를 수행한다. 또한 이와 함께 디지털 경제발전, RuNet 2020, 교육·연구·개발 등의 거의 모든 러시아 인터넷망 구축과 관련된 하드웨어, 부품, 장비, 소프트웨어, 프로그램, 기반설비 구축 등 거의 모든 부문에서 참여기관이거나 핵심 코디네이터이거나 선도기관이거나 컨트롤타워로서의 역할을 수행한다.[54]

51) Ibid, pp. 50-51.
52) Ibid, pp. 43-47.
53) K. Giles, “Russian cyber security: Concepts and current activity,” REP Roundtable Summary, 6 September 2012, Chatham House, London: UK.
54) 윤민우, “러시아 사이버 안보의 국내적 기반과 체제,” pp. 102-106.

Ⅴ. 맺음말

러시아의 사이버 안보전략은 러시아의 독특한 지정학적이고 전략적인 인식과 이해을 기반으로 한다. 러시아는 미국-서방의 지정학적, 경제적, 문화적, 정신적 침해와 세력 확장에 의해 포위되어 있다는 포위된 요새(besieged fortress)의 관념을 갖고 있다. 러시아는 이 때문에 글로벌 지정학적 지형을 미국 주도의 단극질서에서 러시아가 미국과 함께 또 다른 동등한 강대국 행위자로 받아들여지는 다극질서로 변화시키고자 노력한다.

러시아의 사이버 전략에는 이러한 러시아의 지정학적 사고가 그대로 투영되어 있다. 러시아는 글로벌 인터넷을 미국이 일방적으로 기술적, 문화적, 정신적으로 지배하는 공간으로 인식한다. 따라서 이러한 미국 주도의 글로벌 인터넷으로부터 러시아 부분(segment)을 따로 떼어내어 러시아 국가의 통제아래 러시아의 주권이 작동하는 독립된 공간으로 구축하고 싶어 한다. 러시아의 이와 같은 주권과 사이버 공간에 대한 인식은 근본적으로 미국-서방의 주권과 사이버 공간에 대한 인식과는 다르다. 러시아의 이와 같은 인식은 중국의 주권과 사이버 공간에 대한 인식과는 상당히 유사한 측면이 있다. 러시아와 중국의 이와 같은 사이버 공간 주권에 대한 이해는 글로벌 사이버 공간을 각국 정부가 배타적-독점적으로 통제하는 주권 영역으로 분할하고 서로의 영역에 대한 기술적, 문화적, 정신적 개입 또는 침해를 금지하자는 디지털 웨스트팔리아 원칙으로 나타난다.

러시아가 인식하는 이와 같은 사이버 주권공간에 대한 위협은 러시아의 시각에서는 악성 코드와 같은 물리적, 기술적 침해뿐만 아니라 러시아의 문화적, 정신적, 그리고 도덕적 가치를 위협하는 정보내용이 포함된다. 러시아는 이를 정보-기술과 정보-심리의 위협으로 구분하며 모두 정보충돌 또는 정보전쟁의 위협으로 인식한다. 러시아의 격리된 배타적 사이버 공간에 대한 방어는 외부로부터의 정보-기술과 정보-심리의 위협 모두를 의미한다.

또한 러시아는 정보전쟁 또는 정보충돌을 전쟁-평화의 시기가 혼재되어 있는 회색지대에서의 이해관계를 둘러싼 갈등, 충돌로 인식한다. 이 같은 새로운 형태의 전쟁에서 승리하기 위해 러시아는 전통적인 지정학적 군사전략인 공세적 방어(offensive-defense)원칙을 사이버 전략에도 그대로 적용하고 있다. 이 같은 러시아의 전략기조에 따라 정보기술과 정보심리를 통합하고 군사-정보기관-민간 부문을 통합한 입체적 통합적 형태로 사이버 군사전략을 추진하고 있다.

이와 함께 러시아는 미국-서방의 러시아 사이버 공간에 대한 기술적, 정신적 침해를 방어하기 위해 러시아의 독자적 인터넷 망을 구축하려고 시도하고 있다. 이를 위해 정보통신관련 과학기술 및 경제산업발전을 도모하고 있다. 동시에 여러 법령 및 제도와 정책들을 마련하여 사이버 공간에 대한 국가 통제를 강화하고 있다.

이처럼 러시아의 사이버 안보전략은 러시아의 유라시아 문명으로서의 독특한 자기인식과 철학, 가치관, 세계관을 담고 있으며, 이를 구체화한 국가안보전략의 기반위에 세워져 있다. 또한 이 같은 사이버 안보전략은 정보전쟁 수행과 독자적 러시아 인터넷망 구축이라는 구체적 추진전략으로 구현되고 있다. 이 같은 러시아 사이버 안보전략은 적어도 2000년 이후로 지난 20여 년간 꾸준히 지속적으로 일관되게 추진되어 오고 있다.

〈참고문헌〉

송태은 (2020). “디지털 허위조작정보의 확산 동향과 미국과 유럽의 대응.” 주요국제문제분석 2020-13, 국립외교원 외교안보연구소, pp. 22-23.

신범식 (2021). “러시아 사이버 안보의 개념과 원칙.” 신범식·윤민우·김규철·서동주 지음 러시아의 사이버 안보, 서울: 사회평론아카데미.

양정윤·박상돈·김소정 (2018). “정보공간을 통한 러시아의 국가 영향력 확대 가능성 연구: 국가 사이버안보 역량 평가의 주요 지표를 중심으로.” 세계지역연구논총, 36집, 2호.

윤민우 (2018). “사이버 공간에서의 심리적 침해행위와 러시아 사이버 전략의 동향.” 한국범죄심리연구, 14(2), p. 96, 100.

윤민우(2021). “러시아 사이버 안보의 국내적 기반과 체제.” 신범식·윤민우·김규철·서동주 지음 러시아의 사이버 안보, 서울: 사회평론아카데미.

윤민우·김은영 (2022). “어나니머스 등 국제해킹조직의 핵티비즘 분석연구.” 2022년 12월 정보세계정치학회 연구보고서.

윤민우·김은영 (2023). “모든전쟁: 인지전, 정보전, 사이버전, 그리고 미래전쟁에 대한 전략이야기.” 서울: 박영사

장세호 (2023.10.11). “러-우 전쟁 과정에서 나타난 러시아 사이버 공격 양상과 한국 사이버 안보에의 함의.” 한국사이버안보학회 2023 추계학술회의.

Bilanishvili, G. (2021). “On the New National Security Strategy of the Russian Federation.” Security Review, Rondeli Foundation. Available at https://gfsis.org.ge/publications/view/3011.

Bowen, A. S. (2020). “Russian Military Intelligence: Background and Issues for Congress.” Congressional Research Service R46616, p. 4.

Connell, M. & Vogler, S. (2017). “Russia’s Approach to Cyber Warfare.” CNA.

Darczewska, J. (2014). “The anatomy of Russian information warfare: The Crimean operation, a case study.” Point of View, No. 42, OSW(Osrodek Studiow Wschodnich) Center for Eastern Studies, Warsaw.

Giles, K. (6 September 2012). “Russian cyber security: Concepts and current activity.” REP Roundtable Summary, Chatham House, London: UK.

Greenberg, A. (April 12, 2022). “Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine.” WIRED. Available at https://www.wired.com/story/sandworm-russia-ukraine-blackout-gru/.

GRU. (2023). Available at https://en.wikipedia.org/wiki/GRU#cite_note-50.

ICNL(The International Center for Not-for-Profit Law). (2016). “Overview of the Package of Changes into a number of Laws of the Russian Federation Designed to Provide for Additional Measures to Counteract Terrorism.” ICNL.

ITU(International Telecommunication Union). (2016). “Cyberwellness Profile Russian Federation.” ITU 웹사이트. Available at http://www.itu.int/md/D14-SG02.RGQ-C-0143/en.

Kukkola, J., Nikkarila, J-P. & Ristolainen, M. (2017). “Asymmetric frontlines of cyber

battlefields." in J. Kukkola, M. Ristolainen, and J-P. Nikkarila eds. Game Changer Structural transformation of cyberspace. Puolustusvoimien tutkimuslaitoksen julkaisuja 10 (Finnish Defence Research Agency Publications 10), Finnish Defence Research Agency, p. 77.

Lewis, J. A. (2022). "Cyber War and Ukraine." CSIS(Center for Strategic & International Studies) Report. Available at https://www.csis.org/analysis/cyber-war-and-ukraine.

Maurer, T. and Hinck, G. (2018). "Russia: Information Security Meets Cyber Security," In F. Rugge. ed., Confronting an "Axis of Cyber." Milano, It: Ledizioni LediPublishing.

McCauley, M. (2001). "Bandits, Gangsters and the Mafia." Routledge, p. 406.

Medvedev, S. A. (2015). "Offense-Defense theory analysis of Russian cyber capability." Thesis, Naval Postgraduate School, Monterey, California, p. 47.

Miller, M. (June 22, 2022). "Russian hackers targeting U.S., other Ukraine allies." POLITICO. Available at https://www.politico.com/news/2022/06/22/russian-hackers-target-u-s-00041342

Nikkarila, J-P. & Ristolainen, M. (2017). "'RuNet 2020' - Deploying traditional elements of combat power in cyberspace?" in J. Kukkola, M. Ristolainen, and J-P. Nikkarila eds. Game Changer Structural transformation of cyberspace. Puolustusvoimien tutkimuslaitoksen julkaisuja 10 (Finnish Defence Research Agency Publications 10), Finnish Defence Research Agency.

Pack, W. (2019). "Supplement to the 2012/3 South African Cyber Threat Barometer: Russia Case Study Report." Available at www.wolfpackrisk.com.

Pearson, J. & Bing, C. (May 10, 2022). "The cyber war between Ukraine and Russia: An overview." Reuters. Available at https://www.reuters.com/world/europe/factbox-the-cyber-war-between-ukraine-russia-2022-05-10/.

Ristolainen, M. (2017). "Should 'RuNet 2020' be taken seriously? Contradictory views about cybersecurity between Russia and the West." in J. Kukkola, M. Ristolainen, and J-P. Nikkarila eds. Game Changer Structural transformation of cyberspace. Puolustusvoimien tutkimuslaitoksen julkaisuja 10 (Finnish Defence Research Agency Publications 10), Finnish Defence Research Agency, p. 8.

SOCRadar. (November 16, 2021). "APT Profile: Coza Bear/APT29." SCORadar. Available at https://socradar.io/apt-profile-cozy-bear-apt29/

Staff and agencies. (May 1, 2022). "Troll factory' spreading Russian pro-war lies online, says UK." The Guardian. Available at https://www.theguardian.com/world/2022/may/01/troll-factory-spreading-russian-pro-war-lies-online-says-uk.

Voo, J., Hemani, I. & Cassidy, D. (2022). "National Cyber Power Index 2022." Report, September 2022, Harvard Kennedy School, Belfer Center for Science and International Affairs.

이 글의 내용은 필자 개인의 견해이며
한국사이버안보학회의 공식 입장이 아닙니다.