국가전략연구위원회 이슈브리핑 14호 (발간일: 2023.11.01.)

러시아의 사이버 안보전략[1)]

윤민우 (가천대학교)[2)]

1. 머리말

오늘날과 미래의 안보환경에서 미국, 러시아, 중국, EU(European Union) 등 강대국들의 국가안보전략에서 사이버 안보전략이 차지하는 비중은 날로 커지고 있다. 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.[3)] 러시아의 사이버 역량 및 군사력은 현재 매우 높은 수준으로 평가되고 있다. 하버드 대학교 벨퍼 센터의 국가 사이버 역량 인덱스 2022에 따르면,[4)] 2022년 현재, 러시아의 총체적인 사이버 국력은 미국(1위)과 중국(2위)에 이어 3위에 랭크된 것으로 나타났다. 특히 러시아는 총체적인 사이버

1) 이 글은 2023년 10월 25일 제5차 국가전략포럼에서 발표된 발표문을 수정보완한 것이다.
2) 가천대학교 교수, 국제정치학·형사사법학 박사
3) 양정윤·박상돈·김소정. 2018. "정보공간을 통한 러시아의 국가 영향력 확대 가능성 연구: 국가 사이버안보 역량 평가의 주요 지표를 중심으로." 『세계지역연구논총』, 36집, 2호, p. 134.
4) 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.

국력 평가에 포함된 8개 세부 항목들 가운데 사이버 안보역량과 직접 관련된 사이버 공격 능력과 정보통제 부문에서 미국에 이어 2위를 차지했다.[5] 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 점들을 고려하면 러시아의 사이버 안보전략을 살펴보고 그 특성들을 분석, 평가해보는 것은 주요한 의미가 있다.

2. 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.[6]

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.[7] 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 러시아 국가의 통제아래 러시아의 주권이 작동하는 독립된 공간으로 구축하고 싶어 한다. 러시아는 이를 '디지털 주권(digital sovereignty)'이라고 정의하며 국가는 디지털 환경에서 지정학적 국가 이익을 독립적으로 결정하기 위한 권리와 능력을 가져야 한다고 주장한다.[8]

---

5) pp. 9-12.

6) 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.

7) 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.

8) 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.

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.[9)]

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 "사회적-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.[10)]

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.[11)] 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 단계

---

9) 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.

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

11) Nikkarila and Ristolainen, "RuNet 2020-Deploying traditional elements of combat power in cyberspace?" p. 194.

인 "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.[12]

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.[13]

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 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.[14]

3. 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

12) 윤민우·김은영, 모든전쟁: 인지전, 정보전, 사이버전, 그리고 미래전쟁에 대한 전략이야기 (서울: 박영사, 2023), p. 109.
13) Ibid, p. 95.
14) 윤민우, "사이버 공간에서의 심리적 침해행위와 러시아 사이버 전략의 동향," 한국범죄심리연구, 14(2) (2018), p. 96, 100.

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.[15]

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 '러시아주의'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.[16] 이와 함께 푸틴은 구소련연방 국가들과 그 외 러시아의 전략적 이익이 걸린 모든 지역에서 러시아의 국익을 수호하는 것이 러시아의 사명이라고 주장한다.[17] 결국 이렇게 볼 때 푸틴이 그리는 러시아 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 미국주도의 단극질서를 다극질서로 바꾸려고 시도해왔다. 그리고 그러한 다극질서에서 러시아가

15) 윤민우·김은영, 모든전쟁: 인지전, 정보전, 사이버전, 그리고 미래전쟁에 대한 전략이야기, pp. 446-450.
16) Ibid.
17) Ibid.

주도하는 세력 공간(sphere of influence)을 확보하고자 노력해왔다. 이러한 러시아 주도의 세력 공간은 러시아 연방을 포함하여 근외지역(Near Abroad)으로 정의하는 이전 소비에트 연방에 속했던 주변 국가들을 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.[18)]

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.[19)]

---

18) 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.

19) Giorgi Bilanishvili, "On the New National Security Strategy of the Russian Federation," Security

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.[20]

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.[21] 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 속

Review, Rondeli Foundation, https://gfsis.org.ge/publications/view/3011

20) Ibid.

21) Ibid.

성이 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)[22]과 기술적(사이버공간)이고 사회적인(정보공간) 서열(order)을 혼합하여 사용한다.[23] 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 미국대선개입사례이다.[24]

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.

22) 서열은 전투서열을 의미한다.
23) Darczewska, "The anatomy of Russian information warfare: The Crimean operation, a case study," p. 12.
24) 윤민우·김은영, 모든전쟁: 인지전, 정보전, 사이버전, 그리고 미래전쟁에 대한 전략이야기, pp. 434-435.