대한민국의 영토는 한반도와 그 부속도서로 한다.
자유민주적 기본질서에 입각한 평화통일 국책연구기관, KINU
Korea Institute for National Unification

러북의 정보기관 협력과 한국 정부의 대응 방안

Online Series
2024. 04. 03. | CO 24-27

오 경 섭(기획조정실장)

세르게이 나리시킨 러시아 대외정보국(SVR) 국장이 3월 25~27일 평양을 방문했다. 나리시킨 국장과 리창대 국가보위상이 만났고, SVR 대표단과 국가보위성 간부들은 실무회담을 가졌다. 조선중앙통신은 "회담들에서는 조선반도와 러시아를 둘러싼 현 국제 및 지역 정세들에 대한 견해가 호상 통보되고 적대 세력들의 가증되는 정탐 모략 책동에 대처하여 협력을 더욱 강화하기 위한 실무적 문제들이 폭넓고 진지하게 토의됐다"고 보도했다. 회담 결과와 관련해서는 "시종 동지적이며 화기애애한 분위기 속에서 진행된 회담들에서는 제기된 문제들에 대해 완전한 견해 일치를 보았다"고 전했다.[1)]

조선중앙통신 보도는 러북 정보기관의 구체적인 협력 사안과 내용을 공개하지 않았다. 앞으로도 러북 정보기관은 어떤 국가를 대상으로, 어떤 영향력공작(influence operation)을, 어떻게 협력해서 실행하는지를 공개하지 않을 것이다. 그러나 이번 회담 결과 보도에서는 러북 정보기관 협력에 대한 몇 가지 중요한 정보를 제공한다. 첫째, 러북 정보기관은 국제 및 동북아 차원에서 적대세력들에 대한 영향력공작을 위한 협력을 진행할 것이다. SVR은 러시아 대통령 직속의 해외 첩보기관이고, 국가보위성도 해외 첩보를 다루기 때문이다. 둘째, 국제 및 동북아 차원에서 러북 정보기관이 맞설 적대세력은 미국, 한미동맹·미일동맹, 한미일 안보협력을 가리킨다. 셋째, 정보기관 간 협력은 미국, 한미동맹·미일동맹, 한미일 안보협력에 대응하기 위한 실무적 문제를 협의할 정도로 진전된 것으로 추정된다. 넷째, 협력의 목표는 국제 및 동북아 차원에서 적대세력인 미국의 국력과 국제적 영향력을 줄이고, 한미동

1) "로씨야련방 대외정보국대표단이 우리 나라를 방문하였다," 『조선중앙통신』, 2024.3.28.

맹·미일동맹과 한미일 안보협력의 균열을 만들어 와해시키는 것이다. 다섯째, 러북 정보기관은 사이버공간을 활용한 영향력공작을 실행하기 위해 협력할 것이다. 그동안 러북 정보기관은 사이버 영향력공작을 활발하게 진행했기 때문이다.

이 글은 그동안 러북 정보기관이 각각 국제사회를 상대로 실행한 사이버 영향력공작에 대한 분석을 기초로 양국 정보기관의 협력 방향을 살펴보고, 이에 대한 한국 정부의 대응 방안을 제시할 것이다.

사이버 영향력공작

EU 사이버안보국은 사이버위협의 주요 유형을 랜섬 웨어, 멀웨어, 사회공학, 데이터에 대한 위협, 서비스 거부, 인터넷 위협, 허위 정보와 잘못된 정보, 공급망 공격 등으로 구분한다.[2] 특정 국가가 적대국을 겨냥해서 실행하는 사이버위협은 영향력공작을 목표로 한다. 영향력공작은 인간의 인지에 영향을 미쳐 타국의 여론과 정책이 자국에 우호적으로 변하도록 정보의 유포와 메시지 전달을 통해 은밀하게 영향력을 행사하는 고도의 정보전이다.[3] 최근 각국의 영향력공작은 주로 사이버공간에서 진행된다. 사이버 영향력공작은 표적이 된 대중의 행태를 조정하거나 변화시키는 인지적 목적을 위한 자원의 배치를 의미한다.

사이버 영향력공작의 주 무대는 선거다. 러시아는 2016년 미국 대선에 개입했고, 중국은 2020년 미국 대선과 2019년과 2021년 캐나다 총선에 개입한 것으로 알려졌다. 사이버 선거 개입은 사이버 변조 작업과 사이버 영향력공작이 있다. 사이버 변조 작업은 국가의 선거 인프라를 조작하는 것이다. 선거 인프라 조작 유형은 투표 집계 결과를 변경할 목적으로 투표기를 조작하는 행위와 유권자의 투표를 차단하기 위해 유권자 등록 데이터베이스를 조작하는 행위로 구분한다. 선거에서 사이버 영향력공작 유형은 독싱 공작과 정보 공작으로 구분한다. 독싱 공작은 개인·조직·국가에 해를 끼칠 목적으로 비공개 정보를 해킹하여 공개 영역으로 유출하는 행위이다. 정보 공작은 새로 생성되거나 공개된 정보를 의도적으로 사용하여 표적이 된 대중을 위협·혼란 또는 호도하는 행위이다.[4]

---

2) ENISA, 『ENESA Therat Landscape 2023』 (2023) <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023> (검색일: 2024.3.30.), pp. 6~8.
3) Pascal Brangetto, Matthijs A. Veenendaal, "Influence Cyber Operations: The use of cyberattacks in support of Influence Operations," *2016 8th International Conference on Cyber Conflict,* (2016), p. 114; 최성규, "미국과 소련의 영향력 정보전," 『중앙SUNDAY』, 2024.3.9.~10.
4) Barrie Sander, "Democracy Under The Influence: Paradigms of State Responsibility for Cyber I

러시아의 사이버 영향력공작

러시아는 차세대 전쟁의 주전장인 사이버공간에 주목했다. 차세대 전쟁의 중요한 특징은 사이버공간에서 적 부대와 주민들의 사기를 무너뜨려 저항 의지를 붕괴시키기 위해 심리전과 정보전을 실행하는 것이었다. 러시아는 적대국에 대한 영향력공작에 정보전을 활용했다. 정보전의 중요성은 2013년 러시아 총참모장 게라시모프 독트린을 통해 알려졌다. 게라시모프는 정치적 목적을 달성하기 위해 군사적 수단과 함께 정치·외교·경제 등 비군사적 수단의 통합적 운영이 중요하다고 주장했다. 차세대 전쟁의 주요 전장은 영토적 경계선이 아니라 인간의 마음속에 존재한다고 생각했기 때문이다. 게라시모프는 비군사적 조치와 군사적 조치는 4:1의 비율로 수행하고, 군사적 조치 이외에 정보 공간을 제어하고 캠페인의 모든 측면에 대한 실시간 조정의 중요성을 강조했다.[5] 이후 러시아는 적대국을 대상으로 사이버 영향력공작을 활발하게 진행했다.

대표적인 사례는 2016년 미국 대선 개입이다. 러시아는 2016년 상트페테르부르크 소재 인터넷 리서치 에이전시가 수천 개의 소셜 미디어 계정을 만들어 친 트럼프, 반 클린턴 허위 정보, 가짜뉴스를 외부로 확산시켰다. 러시아 군사정보국은 민주당전국위원회(DNC)의 서버를 해킹해서 수천 개의 이메일을 다운로드했다. 러시아의 영향력공작은 거짓 핵티비스트 페르소나를 만들어 팔로워를 끌어모았고, 플랫폼 유출에서 플랫폼 간 유출이 이루어졌고, 언론인에게 연락해서 유출 내용을 홍보함으로써 매체 간 유출이 이루어졌다. 위키리크스는 러시아 조직에 연락해서 "당신이 지금 하는 것보다 훨씬 더 큰 영향을 미칠 것"이라고 주장하며 향후 유출을 대행하겠다고 제안함으로써 주요 인플루언서를 통한 유출이 이루어졌다.[6]

미국 민주당은 선거 운동이 뿌리째 흔들리고 당내 분열이 커졌다. 공식 대선 후보 선출을 앞둔 시점에 DNC가 힐러리 클린턴을 지지한다는 사실이 드러났고, 진보적 민주당원과 온건한 민주당원은 서로 등을 돌렸다. 트럼프 대통령의 선거 운동은 러시아의 공격보다는 해킹의

---

nfluence Operations on Elections," *Chinese Journal of International Law*, Volume 18, Issue 1, (2019), pp. 5~8.

5) 서현태, "대한민국의 하이브리드전 수행방안 연구: 게라시모프 독트린을 중심으로," 『韓國軍事學論集』, 제78호 제3권 (2022), pp. 151~154; Molly K. Mckew, "The Gerasimov Doctrine – It's Russia's new chaos theory of political warfare. And it's probably being used on you," *POLITICO MAGAZINE*, September/October 2017, <https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538/> (검색일: 2024.3.29.).

6) Ben Nimmo, "The Breakout Scale: Measuring the Impact of Influence Operation," *Brookings Institute*, (2020), p. 7., <https://www.brookings.edu/wp-content/uploads/2020/09/Nimmo_influence_operations_PDF.pdf> (검색일: 2024.3.29.); "인공지능과 선거개입," 『중앙일보』, 2023.12.21.

내용에 초점을 맞췄다. 두 주요 정당은 서로를 공격했고, 그 결과 미국 정치는 가장 양극화된 국면으로 치달았다. 러시아의 영향력공작은 미국 정치를 혼란에 빠트렸고, 미국 민주주의의 가장 중요한 2가지 제도인 선거와 언론에 영향력을 행사함으로써 공격의 목표를 성공적으로 달성했다.[7]

2017년 1월 미국 정보기관이 발표한 보고서에서는 블라디미르 푸틴 대통령이 "2016년 미국 대선을 겨냥한 영향력 캠페인을 지시했고, 그 일관된 목표는 미국의 민주주의 절차에 대한 대중의 신뢰를 약화시키고, 클린턴 장관을 폄하하며 그녀의 당선가능성과 대통령직에 해를 가했다"고 '높은 확신'으로 결론을 내렸다. 마이크 무어 전 CIA 국장 대행은 "9/11 테러에 버금가는 정치적 사건"이라고 밝혔다. 러시아의 사이버 영향력공작은 전 세계 정치지도자들에게 큰 경각심을 불러일으켰다. 이후 많은 국가가 자국 정치 시스템을 겨냥한 유사한 작전을 막기 위한 대응 방안을 마련했다.[8]

북한의 사이버 영향력공작

김정은은 사이버 전력을 핵·미사일에 이어 3대 전력으로 규정하고, 사이버공작에 주력할 것을 요구했다. 북한은 경제적·군사적·기술적으로 한국과 정면으로 경쟁할 수 없으므로 사이버공간을 통해 새로운 전장을 만들었다. 북한의 전략은 군사력을 제외한 경제적·기술적 분야에서 한국보다 강해지는 것을 목표로 하는 것이 아니고, 자신들과 동등해질 때까지 한국을 약화하는 것이다. 북한은 6천여 명(사이버공작 요원 1,700명, 지원 및 기술인력 4,300명)의 사이버요원을 두고 사이버공작을 진행한다. 사이버공작의 주요 거점은 중국 선양, 다롄, 광저우, 베이징, 내몽골 등이다. 북한은 무역회사 등으로 위장한 해외 사이버공작 거점을 만들고, 사이버 영향력공작을 진행한다.

북한의 주요 해킹조직은 정찰총국 121국 산하 조직으로 라자루스그룹(Lazarus Group), 블루노로프(BlueNorOff), 안다리엘(Andariel), 김수키(Kimsuky) 등이다. 라자루스그룹(2007년 구성)은 히든 코브라, ATP 38과 동일 조직으로 추정된다. 블루노로프(2014년 구성)는 약 1,700명 안팎의 규모이고, 금전적 이익을 얻을 수 있는 공격만 진행한다. 안다리

7) Alonso Bernal eds., "Cognitive Warfare: An Attack on Truth and Thought," *NATO Innovation Hub*, p. 16, <innovationhub-act.org/cognitive_warfare/> (검색일: 2024.3.29.).
8) Barrie Sander, "Democracy Under The Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections," p. 3.

엘(2016년 구성)은 약 1,600명 안팎의 규모이다. 김수키(2010년 구성)는 탈륨과 동일 조직으로 추정하고, MS가 2019년 인터넷 계정 도용 혐의로 미연방법원에 고소했다. 이 해킹그룹은 북한 정권의 글로벌 정보수집 임무를 담당하며, 일반적인 사회공학 전술, 스피어 피싱, 워터링 홀 공격 등을 사용해 피해자로부터 원하는 정보를 색출한다.[9]

북한의 사이버 공격 유형은 재정적 사이버공격(방글라데시은행 공격, 대만 극동국제은행 공격 등), 군사·정보 활동(한국 국방부 공격, 방위산업 공격 등), 이념·영향력공작(소니 픽쳐스 공격, 탈북자 공격 등), 파괴적인 공격(WannaCry 랜섬웨어 공격 등), 사이버 간첩교신(사이버 드보크) 등으로 구분한다.[10]

사이버 해킹은 평양이나 해외 거점에서 실시간으로 한국의 주요 국가기관망, 공공망, 상용 포털망 등에 접속해서 조직 동향, 관련 자료 등을 탐색하고, 정보를 수집한다. 대표적인 사이버해킹은 2014년 한수원 해킹, 2015년 서울메트로, SK그룹, 한진그룹, 2016년 인터파크, 국방데이터센터, KT그룹, 2017년 암호화폐거래소의 금융정보 해킹, 워너크라이 랜섬웨어 해킹, 2018년 평창 동계올림픽 개막식 사이버 공격, 암호화폐 거래소 빗썸 해킹, 2019년 암호화폐거래소 업비트 해킹, 2021년 서울대 병원 해킹 및 개인정보 유출 등이다.[11]

사이버테러는 D-DOS·VD-DOS(변형된 D-DOS) 공격기법을 개발했다. 북한은 2009년 61개국에 있는 586대의 공격 명령 서버를 이용해서 총 47개 사이트를 공격한 7.7 사이버 대란을 일으켰고, 2011년 3월3~5일 72개국 748대의 서버를 활용하여 국내 40여 개 공공망에 대한 D-DOS 공격을 감행했다. 북한은 2011년 4월 농협 전산망 해킹, 2013년 3.20 사이버공격, 6.25 사이버공격 등을 진행했다. 2013년 6.25 사이버공격은 방송사·신문사 서버 장비, 청와대·국무조정실 홈페이지 변조, 정부통합전산센터 D-DOS 공격, 경남일보 등 43개 민간기관 홈페이지 변조 등 총 69개 기관을 연쇄적으로 공격했다. 또한 북한은 300명 이상 댓글 전문요원으로 구성된 댓글팀을 운영한다. 댓글팀은 허위 정보와 역정보 등 가짜뉴스를 확산해서 여론을 왜곡하고, 남남갈등과 사회 혼란을 고조시킨다.[12]

9) 김보미·오일석, 『북한 사이버 위협의 특징과 대응방안: 김정은 시대를 중심으로』 (서울: 국가안보전략연구원, 2022), pp. 22~23.
10) Robert Potter, "Toward a Better Understanding of North Korea's Cyber Operations," *38NORTH*, August 5, 2019, <38north.org/2019/08/rpotter080519/> (Accessed March 30, 2024); 유동열, "북한의 사이버 위협 실태와 대응," 『전략연구』, 제84호 (2021.11), p. 26.
11) 유동열, 위의 글, pp. 16~17.
12) 김흥광, "북한의 정보전 전략과 그 수행방법," 『군사논단』, 제67호 (2011), p. 273; 유동열, 위의 글, p. 21.

사이버 외화벌이는 북한 사이버 공작팀의 핵심 임무이다. 사이버 공작팀은 사이버테러, 사이버 금전 탈취, 사이버도박, 게임프로그램 개발, 불법 사이버 도박회사 운영 등을 통해 연간 10억 달러 규모의 외화벌이를 진행한다. 북한은 2015년 12월부터 2019년 5월까지 최소 17개국의 금융기관과 암호화폐 거래소를 대상으로 35차례에 걸친 사이버 공격을 통해 최대 20억 달러를 탈취했다. 유엔 대북제재위원회는 2024년 3월 20일 전문가 패널 연례보고서에서 북한이 해킹, 사이버 공격 등 악의적 사이버 활동으로 전체 외화벌이의 약 50%를 조달했다는 유엔 회원국 보고 내용을 기술했다. 또한 대량살상무기 개발 프로그램 재원의 40%가 이 같은 불법적인 사이버 수단으로 조달됐다고 지적했다. 2023년 북한이 관여한 것으로 의심되는 가상화폐 탈취 사건 17건을 조사중이고, 탈취 규모는 총 7억 5천만 달러(약 1조원)에 달한다고 밝혔다. 2017~2023년 북한이 가상자산 관련 회사를 상대로 사이버 공격을 벌여 탈취한 금액이 약 30억 달러(약 4조원)로 추산되며, 이와 관련한 의심 사건 58건을 조사를 진행 중이라고 밝혔다.[13)]

사이버 간첩교신은 북한 상부선과 국내 간첩 사이에 외국계 이메일 계정을 개설해서 아이디와 패스워드를 공유하면서 음어화된 보고 내용과 지령 내용을 올려놓고 교신한다. 사이버 드보크는 2010년 적발된 간첩 한춘길 사건에서 등장했고, 2023년 1월 적발된 민주노총 간부 간첩 사건에서 사용됐다. 또한 북한은 2011년 왕재산간첩단 사건과 2021년 청주간첩단 사건에서 스테가노그라피 방식을 활용했다. 스테가노그라피 방식은 간첩 교신 수단으로 비밀메시지를 이미지·오디오·비디오 또는 텍스트 등 커버라 불리는 다른 미디어에 숨겨서 전송하는 첨단 과학적 기법이다.[14)]

러북 정보기관 협력 방향

러북 정보기관은 미국, 한미동맹·미일동맹, 한미일 안보협력의 약화를 목표로 한 사이버 영향력공작을 실행하기 위해 협력할 가능성이 있다. 러북은 공동의 적인 미국에 대한 사이버 영향력공작을 실행할 것으로 예상된다. 가장 중요한 목표는 미국의 국력과 국제적 영향력을 훼손하는 것이다. 사이버 영향력공작은 인종 갈등을 비롯한 미국의 고질적인 문제들을 들춰내 사회 갈등과 분열을 촉진함으로써 미국의 민주주의를 불안정하게 만드는 것이다. 또한 러북

13) “유엔 "北, 사이버탈취 6년간 4조원대…핵개발 재원의 40% 조달”,” 『연합뉴스』, 2024.3.21., <https://www.yna.co.kr/view/AKR20240320177800072?input=1195m> (검색일: 2024.3.22.).
14) 유동열, “북한의 사이버 위협 실태와 대응,” p. 23.

은 국제사회에서 미국의 지도력과 영향력을 훼손하기 위해 국제질서를 신냉전으로 규정하면서 강력한 반미연대를 구축하기 위한 사이버 영향력공작을 진행할 것이다. 우크라이나 전쟁, 북핵 문제, 이스라엘-팔레스타인 사태 등은 미 제국주의 패권 전략의 필연적인 산물이라고 주장하면서 미 제국주의를 무너뜨려야 한다고 반미국가를 비롯한 국제사회에 호소할 것이다.

러북은 한미동맹·미일동맹과 한미일 안보협력을 균열시키기 위한 사이버 영향력공작을 진행할 수 있다. 사이버 영향력공작의 이슈는 한미 동맹을 균열시키기 위해 방위비 분담금 문제를 활용할 수도 있고, 한일 갈등을 부추기기 위해 역사 문제나 독도 문제를 활용할 수도 있다. 또한 러시아는 북한의 사이버 외화벌이를 지원할 것으로 예상된다. 북한 해킹조직은 2021년부터 암호화폐 자금 세탁을 위해 가란텍스 등 다수의 러시아 암호화폐거래소를 이용한 것으로 알려졌다. 러시아는 북한의 사이버 외화벌이에 협조할 것이다.

러시아가 미국 대선에 개입한 사례를 볼 때, 러북은 독싱 공작과 정보 공작(허위정보와 가짜뉴스 유포)을 통해 2024년 미국 대선에 개입할 가능성이 있다. 대선 개입 목적은 러북에게 유리한 정치인의 대통령 당선을 돕고, 미국의 민주 절차에 대한 대중의 신뢰를 약화하는 것이다. 러북이 미 대선에 공동으로 개입한다면, 2027년 한국 대선에서 자국의 안보에 위협적인 후보를 낙선시키거나 자국에 우호적인 후보의 당선을 돕기 위한 사이버 영향력공작을 실행할 수도 있다는 것을 경계해야 한다.

러북은 북한의 핵보유국 승인과 대북제재 해제를 관철하기 위해 사이버 영향력공작을 진행할 수도 있다. 북한은 북핵 문제에 대한 한·미의 양보를 끌어내기 위해서 서해 NLL 수역 등에서 군사도발을 감행하거나 핵실험과 탄도미사일 실험을 진행할 것으로 예상된다. 러시아는 유엔안보리에서 북한의 핵 개발은 미국의 위협 때문이라고 주장하면서 대북제재 해제를 요구할 것이다. 러북의 사이버 영향력공작은 한국의 안보에 중대한 위협이다.

한국 정부 대응 방안

한국 정부는 북한과 북한을 지원하는 국가들이 사이버 영향력공작을 실행하기 위해 협력할 수 있다는 것을 고려해서 체계적·종합적 대응 방안을 마련해야 한다. 무엇보다도 한국 정부는 사이버안보법을 제정해야 한다. 사이버안보법은 합법적인 사이버위협 정보수집과 분석 등 체계적·지속적·효율적인 사이버안보 대응 방안을 규정해야 한다. 사이버안보법은 사이버안보 추진체계 정비, 기본계획과 실행계획 수립, 사전적 예방정책과 사후적 예방정책을 포함해야 한다.

한국 정부는 공공·민간·국방 등 분야별로 분산된 사이버위협 대응체계를 총괄하는 국가 차원의 컨트롤타워를 설립해야 한다. '사이버안보전략'은 '국가안보전략'에서 더 중요하게 다뤄야 한다. 2019년 수립된 "국가사이버안보전략"은 수정·보완해서 국가 사이버안보 발전 방안을 제시해야 한다. 국정원과 군은 사이버 심리전 조직을 창설해서 북한을 비롯한 적대국의 사이버 공격에 체계적으로 대응하고, 사이버 심리전을 수행할 수 있는 전문 인력을 체계적으로 양성해서 대북한 사이버 심리전을 수행해야 한다.

국정원 대공 수사권은 복원하는 방안을 검토해야 한다. 북한은 사이버 영향력공작을 통해 반국가 활동을 진행하는 지하당원 포섭, 자생적 테러범 양성 등 안보 위협을 높일 것이다. 북한은 궁극적으로 대한민국 파괴와 영토 편입을 추구하기 때문에 대남공작원들과 지하당을 통해 안보 체제를 흔들고, 정권 타도 등 국가 전복 활동을 진행할 것이다. 그러나 한국은 국정원 대공 수사권 폐지, 국가보안법 무력화, 인터넷 발달 등으로 인해 대남공작원과 북한에 포섭된 반국가 활동을 하는 지하당원이 사이버 영향력공작을 실행할 수 있는 환경이 획기적으로 개선됐다. 국정원은 국가 안보와 국익 보호를 위해 여러 가지 방법으로 정보를 수집하고 분석해야 한다. 경찰 단독 간첩 수사는 북한 및 해외정보망 부재, 노하우 부족 등 전문성 부족으로 인해 한계가 있다. 해외에서 북한 공작원들이 반국가 활동을 하는 지하당원을 포섭하는 장면을 채증할 수 있는 능력은 국정원의 전문적 정보 활동 영역이다. 정부는 북한의 사이버 영향력공작에 대응하기 위해서 국정원의 대공 수사 능력을 활용하고, 경찰의 대공 수사 역량도 획기적으로 증대시켜야 한다.

한미일 고위급 사이버협의체와 한미 전략적 사이버 안보협력 프레임워크는 대폭 강화해야 한다. 한국의 안보를 위협하는 적대세력의 사이버 영향력공작 대응은 한국의 독자적 대응만으로는 역부족이기 때문이다. 한미일은 캠프 데이비드 합의를 이행하기 위해 한미일 3국 간 고위급 사이버협의체를 신설해서 운영하고 있다. 한미일 고위급 사이버협의체는 북한과 적대세력의 사이버 영향력공작에 체계적으로 대응해야 한다. 한미는 2023년 4월 한미동맹 70주년을 계기로 '한미 전략적 사이버안보 협력 프레임 워크'를 발표했고, 정례적으로 한미 사이버정책협의회를 통해 사이버안보 협력을 강화하고 있다. 한국 정부는 사이버 범죄 수사를 위한 신속한 정보 공유, 사이버 침해 사고 대응 및 기술 협력을 위한 정부와 민간 간 인적교류 확대, 국방 분야 공동 사이버 훈련 발전, 가상자산 탈취 등 사이버 불법 활동 대응, 영향력공작 대응 등 한미 간 협력을 강화해야 한다. ⓒKINU 2024

※ 이 글의 내용은 집필자의 개인적 견해이며, 통일연구원의 공식적 견해가 아님을 밝힙니다.