issue BRIEF

2024-04

한국의 디지털 민주주의 수호를 위한 제언:
허위조작정보(Disinformation)와 외국의 영향력 활동에 대한 대응

신소현 부연구위원
아산정책연구원
2024.01.31.

2016년 영국의 브렉시트(Brexit) 국민투표와 미국의 대통령 선거에 대한 러시아의 온라인 영향력 공작 및 그 효과가 밝혀진 이후, 민주주의 국가들은 권위주의 국가가 사이버공간을 활용하여 벌이는 여론 조작이나 선거 개입이 실질적인 국가안보의 위협이 될 수 있음을 경험하였다. 2023년 11월 국가사이버안보센터(National Cyber Security Center, NCSC)가 발표한 '중국의 언론사 위장 웹사이트를 악용한 영향력 활동' 보고서를 통해 한국에서도 비슷한 중국의 영향력 활동이 수행되고 있음을 확인했다. 언론의 자유 및 표현의 자유와 같은 국제인권법과 헌법상의 기본적 인권을 존중하면서 민주주의 체제를 수호하여야 하는 국가들은 디지털 권위주의[1] 체제의 국가들이 거리낌없이 행하는 전략적인 영향력 공작에 대응하기가 쉽지 않다. 따라서 디지털 민주주의를 수호하기 위한 유사입장국가들(like-minded states) 간 협력과 정보 공유가 더욱 중요하다. 미국과 유럽연합(European Union, EU)을 비롯한 다른 민주주의 국가들과 비교하여 한국은 외국의 영향력 활동에 대한 대응 준비에 상대적으로 뒤쳐져 있는 것이 사실이다. 이는 2013년 국가정보원과 국군 사이버사령부가 '온라인 여론 조작 사건(소위 댓글사건)'으로 유죄 판결을 받음으로써 국내 여론 조작 가능성에 대한 지나친 우려로 외국의 영향력 활동에 대한 논의 자체가 터부시되어 온 탓이 크다. 그러나 한국을 둘러싼 디지털 권위주의 체제 국가들의 위협이 한층 크게 다가온 지금, 더 이상 한국의 디지털 민주주의 수호를 위한 대비에 주저할 수 없다. 미국은 법률로 FMI(Foreign Malign Influence)라는 개념을 수립하고 외국의 영향력 활동의 정의와 기능, 담당 부서와 유관 부처 및 민주적 통제 방안까지 모두 규정하고 있다. EU는 FIMI(Foreign Information Manipulation and Interference)라는 개념을 정립하고

허위조작정보를 포함하여 광범위하게 이루어지는 외국의 온라인 영향력 활동에 대한 대응을 EU의 대외관계를 총괄하고 '공동외교안보정책(Common Foreign and Security Policy, CFSP)'을 추진하는 EEAS(European External Action Service)가 담당하면서 동시에 회원국들의 적절한 대응을 주문하고 있다. 영국과 프랑스, 독일 역시 유사한 자국의 대응 체제를 마련하고 있다. 우리도 다른 유사입장국가들의 사례를 분석하고 한국의 실정에 맞는 외국의 영향력 활동에 대한 대응 체제 구축을 하여야 한다.

1. 일상 생활에 침투한 외국의 영향력 활동

2023년 10월 한국과 중국의 항저우 아시안게임 8강전 축구 대결에 대한 '다음'(Daum) 포털 사이트 응원 섹션에서 중국에 대한 응원이 90%에 육박한 일을 두고 이것이 중국인들이 한 것인지를 두고 일어난 논란이 정치권까지 이어진 적이 있다.[2] 이 논란과 관련한 모든 기술적, 정치적 공방을 배제하고 일단 이러한 논란이 일어났다는 사실은 이미 한국인들이 중국의 영향력 공작 혹은 중국이 한국의 인터넷에 개입한다는 사실을 인식하고 있음을 보여준다. 이어 2023년 11월 13일 국가사이버안보센터가 발표한 '중국의 언론사 위장 웹사이트를 악용한 영향력 활동' 보고서는 이미 한국을 대상으로 한 '외국의 영향 작전(influence operation)'이 현실에서 벌어지고 있음을 국가기관과 민간의 기술기업들이 협력하여 밝혀낸 좋은 사례이다.[3] 2016년 브렉시트 국민투표와 미국 대선에 러시아가 온라인에서 영향작전을 통해 영국과 미국의 여론 형성에 관여하고 선거에 개입했다는 사실이 드러난 이후, 이러한 외국의 영향력 활동은 전 세계적으로 국가들이 우려하는 공통의 사이버위협이 되었다.

구소련 붕괴 이후 냉전이 종식되고 세계화를 거치면서 민주주의와 권위주의 체제의 경쟁은 민주주의 승리로 마무리된 듯 보였다. 정보통신기술의 발달이 우리에게 준 새로운 장(場)인 사이버공간에서는 개인에서 국가에 이르는 다양한 행위자들이 초국경성과 익명성을 바탕으로 모두 연결되고, 그들이 상호작용하는 속도는 초고속이므로 사이버공간에서

벌어지는 일들은 인류가 이전에 경험하지 못한 속도와 범위의 전파력과 파급 효과를 자랑한다.[4]

반면, 첨단 정보통신 및 인공지능 기술 등은 권위주의 체제 국가가 자국 국민의 표현의 자유와 언론의 자유 및 공론의 장에서 이루어지는 자유로운 의사소통을 차단하거나 검열하는 가장 좋은 수단으로 활용된다. 예를 들어, 권위주의 정부는 도처에 깔린 수많은 CCTV를 이용해 국민들의 이동과 회합을 추적하고 개인의 이동통신 수단(모바일 폰, 태블릿 등)을 이용하여 알고 싶은 개인의 일상을 복원할 수도 있으며, 때로는 그들의 생물학적 정보(얼굴인식, 지문, 홍채, 음성 등)를 무차별적으로 수집하여 활용한다. 이러한 검열과 대량감시는 권위주의 체제를 공고하게 하는 동시에, 권위주의 국가가 민주주의 국가를 상대로 영향을 끼치려는 활동을 용이하게 한다. 국내에서 활용하고 고도화시킨 기술과 전략 전술을 민주주의 체제를 상대로 활용하는 경우, 민주주의 국가들은 사이버공간에서도 동일하게 보장되는 디지털 인권, 개인의 프라이버시, 개인정보보호, 표현의 자유 및 언론의 자유를 모두 지키면서 동시에 대응 혹은 방어를 할 수밖에 없다. 이러한 비대칭성이 사이버공간을 무대로 한 디지털 민주주의와 권위주의의 체제 대결 양상을 다시금 불러왔다.

사이버공간에서 혹은 사이버공간을 매개로(in or through cyberspace) 이루어지는 외국의 영향력 활동에 대한 전 지구적인 공통의 인식과 그에 대한 대응방안 모색에 있어서 한국은 사실 뒤쳐져 있다. 이에 본 글에서는 우리나라와 입장을 같이 하는 민주주의 진영의 주요국들이 어떻게 외국의 영향력 활동에 대하여 대응하고 협력하고 있는지 간단히 살펴보고, 한국이 이러한 국제적 흐름을 따라잡기 위하여 어떤 정책 전환을 하여야 하는지에 대하여 검토한다.

2. 용어 정리 및 개념의 구조

우선, 그동안 '허위정보(misinformation)', '오정보(false information)', '가짜뉴스(fake news)' 등 여러 용어들과 혼용되어 온 허위조작정보(disinformation)의 개념을 먼저 정리할 필요가

있다. 영문상 'misinformation'과 'disinformation'은 다른 의미를 내포하고 있는데, 전자는 잘못된 정보가 의도와는 무관하게 무심코 퍼지게 된 것을 의미하고 후자는 잘못된 정보를 의도를 가지고 퍼뜨린 경우를 뜻한다.[5] 이때 그러한 '의도'를 가진 주체는 국가기관이나 기업, 개인 등 다양할 수 있다. 국어사전에서 '조작(造作)'이란 "어떤 일을 사실인 듯이 꾸며 만듦"이라 정의되어 있기 때문에[6] 허위를 사실인 듯이 꾸미는 것에 의도가 있어야 허위조작정보인 것으로 이해될 수 있으나, 앞서 살펴본 'disinformation'의 뜻에 비추어 이미 존재하는 허위정보나 오정보를 의도적으로 유포한 것도 허위조작정보에 해당한다고 본다. 다시 말해 '허위조작정보'는 그 유포의 고의성이 핵심이라 하겠다.

가짜뉴스는 보통 거짓, 즉 '뉴스 채널을 통해 뉴스의 형식으로 배포되는 고의적으로 거짓인 사실 진술'을 의미하는데 국제법적으로 아직 확정된 정의는 없다.[7] 가짜뉴스란 보통 뉴스의 형식을 취하면서 허위 내용을 포함하고 있는 경우를 이른다. 또한 가짜뉴스는 뉴스 미디어를 공격하거나 불법화하기 위한 도구로서 라벨링(labelling) 하는 용도로도 사용된다.[8] 결국, 가짜뉴스는 외국의 영향작전을 다루는 데 있어 극히 일부의 내용일 뿐 허위조작정보를 대체하여 쓸 수 있는 용어가 아니다. 더욱이 언론과 표현의 자유를 중시하는 민주주의 체제에서 허위조작정보나 영향작전과 구별 없이 뭉뚱그려 가짜뉴스라는 용어를 사용하는 것은 민주주의 자체에 대한 공격이 될 수 있으므로 사용해서는 안 된다. 따라서 국가안보적 관점에서 외국의 영향력 활동을 논할 때에는 가짜뉴스라는 용어를 쓰는 것은 자제해야 한다. 허위조작정보의 일부 유형으로서 외국이 만든 가짜뉴스가 활용될 수 있을 뿐이므로 외국의 영향력 활동을 모니터링하고 필요한 경우 조치를 취하고자 하는 정책 당국이 무분별하게 가짜뉴스라는 단어를 국내와 해외를 가리지 않고 사용하게 되면, 외국의 영향력 활동의 직접 대상이 되는 우리 국민들의 인식을 제고하고 설득하는 데 걸림돌로 작용할 수 있다. 가짜뉴스는 저널리즘 분야에서 주로 팩트체크(fact check)와 짝이 되는 용어로 이해하는 것이 좋다.

FIMI란 EU에서 내세우는 개념으로 허위조작정보를 포함하여 광범위하게 이루어지는 외국의 온라인 영향력 활동을 의미한다. 이는 민주주의 가치나 절차 및 정치적 과정을 위협하거나 부정적인 영향을 미칠 수 있으나 대부분은 불법이 아닌 행동 패턴으로서, 이러한

영향력 활동은 한 국가의 영토 안팎의 대리인(proxy)을 포함하여 국가 또는 비국가 행위자에 의해 의도적이고 조율된 방식으로 수행되기 때문에 그 성격상 '조작적(manipulative)'이다.[9] 다시 말해 모든 허위조작정보가 FIMI인 것도 아니고, FIMI 역시 허위조작정보만을 의미하지도 않는다.[10] FIMI는 주로 DISARM framework에 기반하여 분석되고 있는데,[11] 공격자(주로 국가)는 장기적인 계획을 갖고 성취하고자 하는 FIMI의 목적을 설정한다(campaigns). 이러한 캠페인은 특정한 목적을 가진 단기적인 여러 개의 사건(incidents) 단위로 구성되는데, 이는 사람들의 관점이나 감정 혹은 행동에 변화를 주고자 한다. 이러한 사건들은 목표로 삼은 사람이나 그룹의 믿음, 감정, 행동 등을 형성하는 이야기(narratives)를 만들어 내기 위하여 메시지나 이미지, 계정 및 그들 간의 네트워크 등의 기본적인 요소(artifacts)를 사용한다.[12]

FMI는 미국이 법률로 규정하고 있는 외국의 영향력 활동으로 그 법적 정의와 기능, 담당 부서와 유관 부처 및 민주적 통제 방안까지 모두 법에 규정되어 있다.[13] 그러나 현재로서는 2028년 12월 31일까지 일몰 규정[14] 방식으로 규정되어 있어 차후 연장될 가능성도 있고 다른 형태로 바뀔 가능성도 있다. 미국이 정의하는 FMI란 "외국 정부가 공개적 혹은 은밀한 수단을 통해, (a) 정치적, 군사적, 경제적 혹은 미국 내 선거를 포함하여 미국 정부, 주 정부 또는 지방 정부의 기타 정책이나 활동, 혹은 (b) 미국 내 여론에 영향을 미칠 목적으로 지시하거나 대신시키거나 실질적인 지원을 하여 수행되는 모든 적대적 노력"이다.[15] FMI에는 악성 행위자들이 퍼뜨리는 허위조작정보와 선전(propaganda)이 포함된다. 악성 행위자들은 의도적으로 여론을 속이고 영향을 미치며, 사회를 불안정하게 만들고, 정책, 선거, 사회 문제 등에 영향을 미치고, 세계적인 사건에 대한 공포를 심기 위하여 허위조작정보를 사용한다.

사이버공간에서 벌어지는 사이버공격 및 악의적 활동을 누가 어떤 방식으로 한 것인지에 대하여 명확하게 규명하는 것은 쉽지 않다. 순식간에 지구 반대편 어딘가에서 누군지 모를 행위자가 범한 사이버공격은 우리의 컴퓨터 네트워킹 시스템에 대한 피해를 넘어서 정책 결정자나 일반 대중의 인지(cognisance)에도 영향을 미쳐 민주적인 여론 형성과 선거 과정에 개입하는 수준까지 이를 수 있다. 악성 사이버 활동 행위자를 찾아내어

책임소재(accountability)를 가리는 일을 '귀속(attribution)'이라 하는데, 사이버공간에서 귀속의 문제는 물리적 공간보다 훨씬 복잡하고 어렵다.

귀속은 초기에는 기술적 귀속(technical attribution)과 법적 귀속(legal attribution)만을 논했으나, 현재는 정치적 귀속(political attribution)[16]까지 확장되었다. 기술적 귀속은 악성 사이버 활동의 기술적 요소들을 밝히는 것이다. 말웨어(malware)의 시그니처, 전술과 기술 및 과정(tactics, techniques, and procedures, TPP), 트래픽 등 구체적으로 사용된 기술적 요소들을 추적한다. 법적 귀속은 해당 악성 사이버 활동이 자연인이나 조직, 국가 기관 등 법적으로 어떤 주체에게 책임소재가 있는지 밝히는 것이다.[17] 국가의 경우에는 국제법에 위반되는 행위인지의 여부를 가려야 하고, 개인인 경우에는 그 개인이 속한 국적국가의 국내법이나 기타 관련된 규정들을 살펴야 한다. 정치적 귀속은 공적 귀속(public attribution)[18]이라고도 불리며 피해국이 악성 사이버 활동의 행위자 혹은 국가를 나름의 충분한 기술적, 법적 근거를 갖고 지목하는 것이다. 정치적 귀속은 피해국 입장에서 일종의 정치적 선택이고 의무 사항은 아니다. 기술적, 법적 귀속을 완성하게 되면 미국의 법무부가 다른 유관 부처들과 협력하여 관련된 자국민뿐만 아니라 해외에 거주하는 외국인을 직접 기소하는 경우처럼 단일 국가가 대응하는 경우도 있고,[19] 때로는 같은 피해를 입은 유사입장국가나 동맹국들끼리 연대하여 가해국을 국제적으로 공개 지목하고 사과를 요구하거나(naming and shaming)[20] 혹은 일정한 제재를[21] 가하는 등의 외교적 수단을 통해 정치적 귀속까지 마무리하기도 한다.

3. 외국의 정보 조작 및 영향력 활동에 대한 주요국 법제

러시아 트롤 팜(troll farm), 우마오당(五毛党)이라는 별칭으로 잘 알려진 중국의 인터넷 평론원(网络评论员) 등은 직접 국가가 조직하여 운영하거나 프록시 조직을 외부에 만들어 사실상 국가의 의도와 목적에 따라 운영된다.[22] 중국 공산당 통전(United Front; 统一战线)의 역할과 활동 방식은 중국이 영향작전에 있어 역사적인 노하우와 승리의 경험을 보유하고 있음을 잘 보여준다. 2023년 11월 개최된 G7회의에서도 회원국들은 허위조작정보라는

공통된 위협에 대한 우려와 그에 대한 대응 강조하면서 각국의 경험을 공유하였다.[23] 이하에서는 허위조작정보 등을 활용한 외국의 영향력 활동에 대하여 민주주의 진영의 미국, 영국, EU, 프랑스 및 독일이 어떻게 대응하고 있는지 간단히 살펴본다.

미국은 FMI 개념을 정립하고 ODNI(Office of the Director of National Intelligence) 산하에 FMIC(Foreign Malign Influence Center)를 설립하였다.[24] FMIC는 ODNI의 5개 센터 중 하나이다.[25] FMIC는 모든 정보 커뮤니티에서 외교 및 법집행 기능 부처까지 포함하여 분석가들 모집하여, 외국의 영향작전에 관하여 미국 정부가 보유하거나 획득한 모든 정보 및 다른 보고들에 접근하고, 이러한 정보 및 보고들을 분석하는 1차 조직으로서 연방 정부의 정책결정직위 및 의회에 외국의 악의적 영향에 대한 종합적인 평가(comprehensive assessments)와 지시 및 경고(indications and warnings)를 제공한다.[26] 당연히 해외 정보를 담당하는 CIA(Central Intelligence Agency) 및 NSA(National Security Agency)와 공조하며, 미국 국내 담당 유관기관인 FBI FITF(Federal Bureau of Investigation Foreign Influence Task Force), DHS(Department of Homeland Security), CISA(Cybersecurity & Infrastructure Security Agency), EAC(US Election Assistance Commission)와 정보를 공유하며 협력한다. 또한 매년 1회 이상 ODNI 수장의 지시에 따라, 의회정보위원회, 하원외교위원회 및 상원외교관계위원회에 외국의 악의적 영향에 대한 보고서를 제출하여야 한다.[27] 동 보고서에는 보고서가 다루는 기간과 (i) 센터의 가장 중요한 활동 및 (ii) 프라이버시 보호 및 시민의 자유와 관련된 권고를 포함하여 센터의 기능 수행 능력을 향상시키기 위한 입법 및 다른 조치들을 위하여 필요하다고 센터장이 결정한 권고사항이 포함되어야 한다.[28] 또한 미국 국무부(Department of State) 역시 국방수권법(National Defense Authorization Act, NDAA)에 기하여 GEC(Global Engagement Center)를 설치하고,[29] 미국과 동맹국 및 파트너 국가들의 정책, 안보, 안정을 해치거나 이에 영향을 끼치려는 외국 및 비국가행위자들의 선전 및 허위조작정보에 대해 연방 정부의 대응을 지휘, 조정, 조율, 통합하고 협력하는 역할을 한다. 특히 국무부는 외국이 허위조작정보와 선전을 활용하여 미국의 이익을 저해하려는 시도에 적극 대응하려는 유관부처 간 노력을 데이터에 기반하여 선도한다.

영국은 미국이나 EU와 달리 허위조작정보 용어를 그대로 쓰고 있다. 2019년 DCMS (Department for Digital, Culture, Media and Sport) 산하에 설립되었던 CDU(Counter-Disinformation Centre)는 2023년 2월 리시 수낙(Rishi Sunak) 총리가 정부 조직을 개편하여 DSIT(Department for Science, Innovation and Technology)에 속하게 되었다.[30] CDU의 목적은 허위조작정보 내러티브 및 인위적으로 정보환경을 조작하려는 시도를 이해하고 정부가 유해한 허위정보 혹은 허위조작정보의 범위와 그 도달을 파악하기 위한 것이다. 허위정보 및 허위조작정보를 반박하는 자료를 정부 소셜 미디어에 게재하거나 사실 확인을 위한 대중의 인식을 제고하는 한편, 소셜 미디어 업체들로 하여금 신뢰할 만한 정보 출처를 권장하고 그에 맞는 서비스 약관을 갱신하고 준수하도록 유도한다.[31] CDU는 공중보건과 공공안전 및 국가안보에 위협이 되는 맞춤형 허위조작정보, 예를 들어 COVID 19나 5G 기지국 관련 루머 및 우크라이나 전쟁 등에 대한 대응에 중점을 둔다. CDU의 주업무는 오픈 소스를 이용하여 대중에게 접근 가능한 데이터를 바탕으로 분석하는 것이 원칙이고, 절대 개인을 모니터하지 않으며, 모든 데이터는 비실명화(비식별화, anonymised)하여 분석하도록 한다.[32] 주요 소셜 미디어 플랫폼과 협업하여 그들의 서비스 약관을 점검하고 공신력 있는 정보를 유통하도록 유도하는데(유해 컨텐츠 판단이 주된 의무가 아님), (i) 컨텐츠가 공중보건, 공공안전 혹은 국가안보를 위협하고(a demonstrable risk), (ii) 플랫폼의 서비스 약관을 위반한 것으로 판단되는 경우, 정부가 직접 일정한 조치를 취할 것을 요구하지 않고 플랫폼이 독자적으로 자신들의 서비스 약관에 따라 어떤 조치를 취할 것인지 결정하도록 한다.[33] 표현의 자유 보장을 위하여 정치적 토의는 모니터링 하지 않고, 언론인, 정치인, 정당의 그 어떠한 컨텐츠도 소셜 미디어 플랫폼에 통보하지 않는다.[34] CDU는 내각 장관들에게 정기적으로 보고한다.

EU는 FIMI 관련 이슈를 EU의 대외관계를 총괄하고 '공동외교안보정책'을 추구하는 EEAS에서 관장한다. EEAS에 속한 'Strategic Communications, Task Forces and Information Analysis Division(STRAT.2)'은 EU의 공동 대응 및 각 회원국에 대한 가이드를 제시하는 역할을 수행하고, 'EUvsDisinfo' 프로젝트를 통하여 러시아와 중국의 정보조작활동에 대한 데일리 분석을 포함한 정보를 공유한다.[35] 또한 디지털서비스법(Digital Services Act, DSA)을 통하여 온라인 소셜 미디어 플랫폼 회사들에게 해당 플랫폼이 허위조작정보 및 선거 조작

등에 이용되지 않도록 위험 관리를 해야 하는 법적 의무를 부과하고 있다.[36] EU의 FIMI 대응은 외국의 영향력 활동에 대한 규제(disruption & regulation), 외교적 대응(diplomatic responses), 상황 인식 제고(situational awareness), 및 회복탄력성 강화(resilience building)로 크게 구성된다.[37]

프랑스는 EU의 대표적인 회원국으로서 총리 산하 SGDSN(General Secretariat for Defence and National Security) 내에 VIGINUM(Vigilance and Protection Service against Foreign Digital Interference)이 2021년부터 설립되어 활동하고 있다.[38] VIGINUM은 프랑스와 프랑스의 근본적인 이익에 해를 끼치려는 외국 행위자가 연루된 정보 조작 캠페인으로부터 디지털 공개 토론을 보호하는 임무를 수행한다. VIGINUM은 개인 데이터의 상담, 수집 및 사용에 대한 허가와 이행 조건을 모니터링할 책임이 있는 고도의 자격을 갖춘 사람으로 구성된 '윤리과학 위원회(Ethical and Scientific Committee, CES)'의 감독 아래 엄격한 법적, 윤리적 틀 내에서 운영된다.[39]

독일 정부 역시 외국의 영향력 활동으로 인한 안보 위협에 대한 우려를 표명한 바 있다.[40] 독일은 내무부(Bundesministerium des Innern, BMI)와 외교부(Auswärtiges Amt, AA)가 외국의 허위조작정보를 추적 및 분석하는 데 협력하고 대응책을 모색한다. 내무부 산하 연방정보국(Bundesnachrichtendienst, BND) 및 연방헌법수호청(Bundesamt für Verfassungsschutz, BfV)이 연계하여 주로 오픈 소스 정보 수집한다.

주요 민주주의 국가들의 대응 체계를 분석해 보면, 전 정부 차원의 협력 대응 체계 구축이 공통적이다. 또한 영국이나 EU를 제외하고는 정보기관이 속한 부처 내에 허위조작정보 및 외국의 영향력 활동 대응 부서가 속해 있다. 그러나 이는 정보기관의 독점적 임무가 절대 아니며, 그 임무의 특성상 외국으로부터 민주주의를 보호한다는 명분 아래 자칫 국내 민주주의에 대한 해악을 끼칠 우려도 크다. 이에 앞서 본 민주주의 국가들은 모두 외국의 영향력 활동에 대응하는 조직에 대한 민주적 통제 제도 구축하고 공개적이고 투명성이 보장된 임무 수행 방식을 강조하고 있다.

4. 한국의 현실 및 정책 제언

그동안 외국의 영향력 활동에 대하여 민주적이고 정당한 대응을 하기 위하여 주요 선진 민주주의 국가들은 위와 같은 노력을 경주해 온 반면, 한국의 현실은 한참이나 뒤쳐져 왔다. 가장 결정적인 요인은 2013년 국가정보원과 사이버사령부가 벌인 '온라인 여론조작사건'이 대법원 유죄판결을 받아 관련자들이 형사 처벌을 받았기 때문이다.[41] 이후, 한국 사회에서 외국의 온라인 영향 공작에 대한 논의 자체에 대한 터부가 존재했다는 사실은 부정하기 어렵다. 그러나 더 이상 지체한다면 이 또한 국가안보에 대한 임무해태 혹은 방기가 될 것이다. 왜냐하면 이상에서 살펴본 국가들이 한국이 당하는 해외 영향력 활동에 대하여 정보를 공유하고 공동 대응의 네트워크를 구축하고 싶어하기 때문이다. 러시아와 중국으로 대표되는 주요 권위주의 체제 국가들은 민주주의적인 제한이 없는 탓에 무차별적으로 사이버공간을 이용한 악성 영향력 활동을 전개하고 있다. 게다가 한국은 북한의 그러한 활동 역시 경계해야 한다.

외국의 영향력 활동에 대한 대응은 민주주의 체제를 수호한다는 명분으로 국내 민주주의 과정을 파괴할지도 모른다는 자체적인 모순을 방지해야 하는 어려운 문제를 원래부터 갖고 있다. 게다가 한국은 이미 주요 국가정보기관들이 직접 국내 민주주의 과정에 불법적으로 개입했던 전례가 확인된 바 있어 국민들을 설득하는데 한계가 있었다. 2023년 11월 국가사이버안보센터가 여러 국내 기업들과 공동으로 '중국의 언론사 위장 웹사이트를 악용한 영향력 활동' 보고서를 발표한 것은 주목할 만한 좋은 성과였다.[42] 해외 정보활동이라는 본연의 임무에 충실했을 뿐만 아니라 국내 기술기업과의 협업을 통해 얻은 결과로서 사이버 분야에서 특히 요구되는 민관협력(public private partnership, PPP)의 모범 사례이다. 그러나 그 가치에 비해 생각보다 오래 이슈가 되지 못한 점이 아쉬운데, 이는 국정원이라는 단일 기관의 이름 아래, 외국의 온라인 영향력 활동과는 다른 성격이지만 혼동하기 쉬운 기존의 대북 심리전(확성기 등)과 같은 다른 내용이 순차적으로 발신된 탓일 수 있다.

① 외국의 영향력 활동을 모니터링하는 별도의 기관 설립

미국이나 영국 등 복수의 정보기관을 가진 나라들과 달리 하나의 독점 정보기관인 국정원만 존재하는 우리나라의 현실에서, 기존의 사이버안보 및 정보 업무를 수행해 오던 국정원이 훨씬 광범위하게 민간 영역에서 일어나는 영향력 활동을 겸하여 모니터링하게 된다면, 여러 오해와 저항을 불러올 가능성이 있다. 동일 기관 내의 다른 부서가 각각 따로 수행한 활동과 수집한 정보라 하더라도 이것이 한 기관에 집중되어 동일한 이름 아래 외부로 메시지가 발신된다면 기관 내에서 정보가 오용될지도 모른다는 불필요한 오해를 받을 수 있기 때문이다. 더욱이 영향력 활동을 모니터링하고 대응하려면 대중을 향한 정보 공개(openness)가 필수적이고 민주주의 수호라는 명분을 위해서는 투명성(transparency)이 담보되어야 하는데, 이 두 가지 특성은 정보기관의 성격과 잘 맞지 않는 측면이 있다. 따라서 기존의 사이버안보센터보다는 별도의 기관을 설립하고 미국처럼 여러 관련 기관으로부터 분석관(analysist)을 뽑아 재배치하는 것이 좋겠다. 이 새로운 기관은 지속적으로 외국의 영향력 활동 모니터링 결과를 투명하게 국민들에게 공개함으로써 국민 인식을 제고함과 동시에 신뢰를 구축할 수 있다. 이 기관은 전정부적으로 유관 부처간 정보 공유의 허브가 되어 합동 분석 시스템을 만들어 협력적 대응 체계를 구축해야 한다. 특히 앞서 언급한대로 다른 민주주의 국가들과 네트워크를 구축하여 정보 공유 및 국제 협력을 추진하는 것도 중요하다.

② 민주적 통제를 위한 감독 장치 구비

한국 국민의 인지에 간섭하고 여론을 조작하기 위하여 말단까지 스며드는 외국의 영향력 활동을 감지한다는 것은 그만큼 사적 활동 영역에 대한 감시 혹은 침해의 가능성이 크다는 의미이기도 하다. 이를 위해서는 담당기관에 법률로 임무를 부여해야 할 뿐만 아니라 상시적인 민주적 통제를 받기 위한 감독 장치를 구비해야 한다. 프랑스의 CES와 같은 기능을 할 수 있는 별도의 위원회와 같은 기관이나 정기적인 국회 보고 및 검토와 같은 별도의 절차를 설계해야 한다. 역시 민간 영역의 시민사회나 학계도 함께 참여하는 협의체를 통해

투명성을 높이는 방안도 고려할 수 있다. 아니면 앞서 말한 별도의 모니터링 기관을 설립하는 단계에서부터 민간과의 협업 체계를 꾸리는 방안도 생각해 볼 수 있다.

③ 대국민 교육과 홍보

이쯤에서 근본적인 질문을 해보자. 왜 우리는 외국의 영향력 활동에 대응해야 하는가? 이는 외국 정부가 우리 국민들 혹은 정책 결정자들을 대상으로 의도적으로 잘못된 정보를 오랜 시간 노출시켜 결국 우리의 인지에 간섭하고 그들이 원하는 방향으로 내부 혼란이나 잘못된 의사결정을 유도하고자 하기 때문이다. 그렇다면 대응책만큼 중요한 것이 예방책이다. 한 번 왜곡된 집단적 인지를 되돌리는 것은 쉽지 않다. 따라서 외국의 영향공작에 시민들이 휘둘리지 않도록 하는 것이 더 중요하고 효율적일 수 있다. 그러므로 정보 수용자들의 '디지털 문해력(digital literacy)'과 '미디어 문해력(media literacy)'을 증진시켜 외국의 영향력 활동 위험이 항상 존재할 수 있다는 점을 꾸준히 알려줘야 한다. 국민들이 어떤 자극적인 정보를 접했을 때 즉각적으로 감정적인 반응을 하기보다는 차분하게 그 정보가 해외 세력이 발신한 의도된 허위조작정보일수도 있다는 가능성을 떠올리게 할 수 있다면, 그리하여 국민들이 스스로 팩트체크를 하려는 노력으로 나아갈 수 있다면, 이야말로 최상의 대응이 될 수 있다. 또한 국민들로부터 기본적인 신뢰를 받기 위하여 외국의 영향력 활동에 대한 대응은 지속적이고 일관된 대국민 메시지 발신이 중요하다. 외국의 악성 영향력 활동에 대한 지속적이고 일관된 정보 제공과 함께 국민들의 디지털·미디어 문해력 증진을 위한 정책을 균형 있게 추진함으로써 그만큼 국민의 신뢰를 획득할 수 있다.

이제 우리나라도 헌법과 국제인권법 기준을 준수하면서 어느 정도까지 어떤 방식으로 외국의 악성 영향력 활동에 대응할 것인지에 대한 본격적인 논의를 해야 한다. 앞서 본 주요 민주주의 국가들과 유사한 정부기관을 만들 것인지 아니면 한국의 실정을 고려한 다른 형태의 기구를 꾸릴 것인지 결정해야 한다. 그리고 전 정부 차원의 유관 부처간 협력 대응체계 구축, 합동 분석 및 국제적 협력 방안에 대한 고려와 함께 민주적 통제와 투명성 제고를 위한 기관 및 법제 정비도 해야 한다. 또한 시민사회와 학계를 포함한 폭넓은 의견

수렴과 민주적 과정을 통해 국민들의 인식을 제고하고 디지털 문해력을 증진하는 방안도 함께 수립해야 한다.

---

[1] '디지털 권위주의'는 중국과 러시아로 대변되는 독재나 권위주의 체제에서 디지털을 활용하여 국민과 정보를 통제하는 것을 의미하고, '디지털 민주주의'란 이와는 반대로 디지털 세상에서도 인권과 민주적 절차를 존중하면서 민주주의적 가치를 지키는 것을 말한다.

[2] 이가영, '축구 한중전, 中응원이 89%... 다음 포털서 벌어진 일', 『조선일보』(2023.10.02) <https://www.chosun.com/sports/sports_special/2023/10/02/T3DEH4XT2NA75K7K6TDR342BEA/>

[3] NCSC 합동분석협의체, 중국의 언론사 위장 웹사이트를 악용한 영향력 활동 (2023년 11월 13일) <https://www.ncsc.go.kr:4018/main/cop/bbs/selectBoardArticle.do?bbsId=SecurityAdvice_main&nttId=88028&menuNo=020000&subMenuNo=020200&thirdMenuNo=>

[4] 신소현, '사이버공간에서 국가의 적대적 허위조작정보 작전에 대한 규율' (2022) 28 국가전략 63.

[5] Dictionary. 2022. "Misinformation vs. Disinformation" <https://www.dictionary.com/e/misinformation-vs-disinformation-get-in formed-on-the-difference/>

[6] 네이버표준국어대사전<https://ko.dict.naver.com/#/entry/koko/fa47f6aa08fe 49bba9ec6dac02111c74>

[7] 국내에서 가짜뉴스 규제를 위하여 입법 논의하는 법적 정의는 별론으로 한다.

[8] Misinformation vs Disinformation: What are the differences between misinformation, disinformation, and fake news? <https://insights.taylorandfrancis.com/social-justice/misinformation-vs-disinformation/#?> (검색일: 2023.11.30)

[9] Nicolas Hénin, *FIMI: Towards a European Redefinition of Foreign Interference* (2023)

[10] Ibid. ("Not all disinformation is FIMI, and FIMI is not only disinformation.")

[11] https://disarmframework.herokuapp.com/

[12] Hadley Newman, *Foreign Information Manipulation and Interference Defence Standards: Test for Rapid Adoption of the Common Language and Framework 'DISARM'* (Hybrid CoE Research Report 2022) 15-16.

[13] 50 U.S.C. §3059: Foreign Malign Influence Center (2023년 11월 26일 발효)

[14] 일몰 규정이란 입법자가 정한 특정기한이 도래하면 법령의 전부나 일부의 효력이 별도의 조치를 취하지 않는 한 상실되도록 규정한 것이다.

[15] 50 U.S.C. §3059 (f)(2)

[16] Andraz Kastelic, *Non-Escalatory Attribution of International Cyber Incidents: Facts, International Law and Politics* (2022)

[17] Samuele Dominioni and Giacomo Persi Paoli, *A Taxonomy of Malicious ICT Incidents* (2022) 4.

[18] Christina Rupp and Alexandra Paulus, *Official Public Political Attribution of Cyber Operations: State of Play and Policy Options* (October 2023)

[19] US Department of Justice, *40 Officers of China's National Police Charged in Transnational Repression Schemes Targeting U.S. Residents* (Department of Justice 17 April 2023) <https://www.justice.gov/opa/pr/40-officers-china-s-national-police-charged-transnational-repression-schemes-targeting-us>

[20] Max Colchester, 'Heads of FBI, MI5 Issue Joint Warning on Chinese Spying', *The Wall Street Journal* (6 July 2022) CHINA <https://www.wsj.com/articles/heads-of-fbi-mi5-issue-joint-warning-on-chinese-spying-11657123280?tpl=cs> accessed 12 July 2022.

[21] Council of the European Union, *Cyber-attacks: Council extends sanctions regime until 18 May 2025* (16 May 2022)

[22] Jessikka Aro, *Putin's Trolls: On the Frontlines of Russia's Information War against the World* (2022)

[23] G7 2023 Hiroshima Summit, *Existing Practices against Disinformation (EPaD)* (日本 総務省 2023 日本総務省) <https://www.soumu.go.jp/main_content/000905620.pdf>

[24] 50 U.S.C. §3059 (a)

[25] 다른 4개의 센터는 NCTC(National Counterintelligence Center), NCSC(National Counterintelligence and Security Center), NCBC(National Counterproliferation and Biosecurity Center), and CTIIC(Cyber Threats Intelligence Integration Center)이다.

[26] 50 U.S.C. §3059 (b)

[27] 50 U.S.C. §3059 (d)(1)

[28] 50 U.S.C. §3059 (d)(2)

[29] NDAA for Fiscal Year 2019 SEC. 1284. [미 국무부의 기존 CSCC(Center for Strategic Counterterrorism Communications)를 발전시켜 임무를 확대한 것임)

[30] Cabinet Office and Innovation and Technology Department for Science, *Fact Sheet on the CDU and RRU* (9 June 2023) <https://www.gov.uk/government/news/fact-sheet-on-the-cdu-and-rru >

[31] Ibid.

[32] Ibid.

[33] Ibid.

[34] Ibid.

[35] https://euvsdisinfo.eu/

[36] DSA 제34조, 제35조

[37] EU FIMI Toolbox

[38] https://www.sgdsn.gouv.fr/publications/viginum-publication-du-premier-rapport-du-comite-ethique-et-scientifique

[39] VIGINUM, *VIGINUM YEAR #1* (SGDSN 2022)

[40] https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/disinformation/article-disinformation-hybrid-threat.html

[41] 대법원 판결 2017도14322(선고 2018. 4. 19); 대법원 판결 2019도11962(선고 2020. 3. 12)

[42] (NCSC 합동분석협의체) 중국의 언론사 위장 웹사이트를 악용한 영향력 활동 (2023년 11월 13일) <https://www.ncsc.go.kr:4018/main/cop/bbs/selectBoardArticle.do?bbsId=SecurityAdvice_main&nttId=88028&menuNo=020000&subMenuNo=020200&thirdMenuNo=>

신소현
외교안보센터

신소현 박사는 아산정책연구원의 외교안보센터의 부연구위원이다. 주요 연구 분야는 정보보호 기술을 비롯한 신기술 (인공지능, 우주기술, 양자컴퓨팅 등)의 발전으로 생겨난 새로운 공간인 사이버 공간과 우주 공간과 관련된 각 국제법 분야의 변화와 발전이다. 무력충돌, 군사, 무기, 사이버첩보 등의 전통안보 뿐만 아니라 경제, 재난, 환경 등 새로운 비전통 안보분야들을 국제 및 국가안보의 관점에서 분석하고 관련 국제 및 국내 규범의 형성과 변화 및 정책적 이슈들을 융합적으로 연구한다. 세종연구소 사이버안보센터 창립 멤버였으며 사이버안보포럼을 조직한 바 있고, 고려대학교 정보보호연구원 연구위원을 역임하였다. 최신 저작으로는 "사이버공간에서 국가의 적대적 허위조작정보 작전에 대한 규율", "우주안보와 국제법", "사이버 억지와 미국의 선제적 방어전략의 국제법적 검토" 등이 있다.