아 산 정 책 연 구 원

이슈브리프

No. 2025-27

이재명 정부의 사이버 안보 법·전략에 대한 제언

신소현

연구위원

2025-08-28

2013년 에드워드 조지프 스노든(Edward Joseph Snowden)의 폭로로 전 세계는 미국의 NSA(National Security Agency)와 영국의 GCHQ(Government Communications Headquarters) 등이 해외에 소재한 외국인에 대해 전자통신 등의 감시를 하였음을 알게 됐다. 기본적으로 다른 국가의 네트워크와 시스템에 접근하거나 외국인을 대상으로 정보를 수집하는 것은 주권 및 인권 침해적 요소를 동반한다. 그러나 전 세계가 사이버 공간을 통해 초연결(Hyper-connected)된 사회에서 온라인을 통한 정보 수집은 피할 수 없는 현실이 되었다. 국가 배후 해킹 조직이나 외국의 정보기관, 국제 범죄 조직이나 테러 단체 등이 해킹 등 소프트웨어 수단을 이용하여 국가 안보를 위협하는 상황에 맞서기 위해서 국가들은 수사 및 정보기관이 온라인 해외 정보 수집을 할 수 있도록 국내법으로 뒷받침했다. 그래야 디지털 민주주의 국가로서 해외 정보 수집을 담당하는 오퍼레이터들이 법적 근거에 기해 임무를 수행하게 할 수 있고, 적절한 통제 장치를 마련하여 필요한 범위에서만 수집을 하도록 감독할 수 있으며, 국가 간 분쟁시 이들을 보호할 수 있는 근거도 마련되기 때문이다. 반대로 우리의 사이버 공간에 외세가 악성 영향을 끼쳐 안보의 위협이 되는 경우도 있다. 온라인을 통한 정보 조작은 단독으로 또는 오프라인의 휴민트(Human Intelligence, HUMINT) 활동과 결합하여 국내 정보 환경을 오염시키고 개입을 하므로, 이들에 대한 규제

및 대응 근거를 법적으로 마련할 필요가 있다. 현재 우리 법제에서 해외 정보 수집은 대통령령인 사이버안보업무규정에 일부 규정되어 있으나 체계상 맞지 않고 통제 장치가 미비하다. 온라인 정보 조작을 통한 해외 개입의 경우에는 적절한 국내 법령이 없다. 사이버 안보(보안) 관련 정부 거버넌스 구축 및 위협 대응 조치 등을 포괄하여 제정하려던 사이버 안보 관련 기본법 제정은 2006년 첫 발의 후 계속 실패했다. 국가 사이버 안보에 관한 정책 방향이나 기본 원칙 등을 포괄적으로 규정하는 기본법 제정은 오히려 부처 간 거버넌스 갈등으로 이어져 지난 20년간 소모적 논쟁을 불러왔다. 해외 정보 수집 관련 사항은 사이버안보업무규정이 아닌 국가정보원법의 개정을 통해 정비하고, 해외 개입 관련 사항은 신법(新法)을 제정하는 것이 바람직하다.

다른 한편으로 국가사이버안보전략의 적절한 갱신을 통해 더딘 입법을 보완하고 체계적인 국가 사이버 안보 강화를 도모할 수 있다. 이전 전략 실행의 성과와 문제점에 대한 검토를 거쳐 새로운 안보 환경의 변화를 반영한 새 전략이 필요하다. 기존의 국가 전략이 구체성이 떨어진다는 지적을 받아온 만큼, 사이버안보기본계획의 내용을 상당 부분 포섭한 종합적이고 상세한 전략을 수립해야 한다. 또한 다중 이해관계자들의 참여도 확대하여 이재명 정부의 국가사이버안보전략을 공개해야 할 것이다.

I. 문제의 소재

사이버 위협은 물리적 피해가 없이도 충분히 심각한 국가 안보 차원의 문제를 야기한다. 흔히 알려진 디도스(Distributed Denial of Service, DDoS) 공격이나 랜섬웨어(Ransomware) 같은 사이버 공격은 직접 컴퓨터 시스템이나 네트워크에 침투하여 이루어지는 반면, 시스템에 직접 접근하지 않으면서 온라인 정보 조작 등을 통해 안보 위협을 일으키는 경우도 있다. 국가 안보는 크게 이 두 가지 유무형의 사이버 안보 위협 모두에 대응해야 한다. 직접 컴퓨터 시스템이나 네트워크에 침입하는 형식의 사이버 침해(cyber exploitation)라 해도 모두 알아챌 수 있는 것은 아니다. 과학기술 역량이 부족하면 공격이나 침해를 받았는지 영원히 모르고 넘어갈 수도 있다. 장래의 대규모 사이버 공격이나 물리적 충돌 이전에 혹은 테러나 조직 범죄를 일으키기 위해서도 사이버적 수단이 이용된다. 이러한 사이버 침해를 미리 혹은 즉시 알아채고, 역으로 추적하여 무력화시킬 수 있으면 더 큰 피해를 막을 수 있다. 이를 위해 중요한 것이 사이버 정보 수집, 특히 해외 정보 수집이다.

허위조작정보를 유포하는 등 온라인에서 정보 조작을 통해 다른 국가의 여론 형성이나 정책 결정에 개입하는 외세의 악성 영향력 활동(개입)도 위협적이다. 해외 정보 수집이 국가 안보에 위해가 되는 사이버 위협에 대응하기 위해 밖으로 나가는 것이라면, 해외 개입 대응은 우리 사이버 공간 안으로 들어온 사이버 위협을 다루는 것이다. 두 경우 모두 국가 사이버 안보를 위해 대응해야 하지만, 동시에 오남용의 우려가 있어 반드시 법률을 통해 위임하고 적절한 통제장치를 마련해야 한다.

국가 사이버 안보의 전반적인 밑그림을 제시하는 것이 국가사이버안보전략이다. 문재인 정권에서 첫 국가사이버안보전략을 발표한 이래, 윤석열 정부 역시 전략을 발표했다. 지난 전략들에 대한 간략한 분석을 바탕으로 세 번째 이재명 정부의 국가사이버안보전략을 위한 제언을 한다.

II. 정보 수집 및 해외 개입 관련 법제 정비

1. 해외 정보 수집 법제의 정비

(1) 국제적 대응 동향

국가 배후 해킹 조직이나 외국의 정보기관, 국제 범죄 조직이나 테러 단체 등이 해킹 등 소프트웨어 수단을 이용하여 우리 안보를 위협하는 것에 대응하기 위해 정보기관은 은밀히 추적할 필요가 있다. 그런데 원칙적으로 다른 국가의 네트워크와 시스템에 접근하거나 외국인의 디바이스에 연결하는 것은 주권 및 인권 침해의 요소가 있는 불법행위이다. 우리나라 정보통신망법에서도 수집을 위한 해킹 프로그램을 설치하고 사용하는 행위는 금지된다. 그럼에도 불구하고 각국의 정보기관이나 군, 경찰 등은 해외를 상대로 한 온라인 정보 수집을 할 필요가 있고, 또 하고 있다. 디지털 민주주의 진영의 국가들은 이를 위해 국내법적으로 근거 법령을 만들고 대외에 공개하며, 정보 수집 및 조회 사유를 제한하고, 사전 허가 혹은 사후 검토를 위한 통제 장치나 감독 기관을 운영하고 있다.

미국의 「Foreign Intelligence Surveillance Act(FISA)」, 영국의 「Investigatory Power Act(IPA)」, 호주의 「The Telecommunications and Other Legislation Amendment Act

2018(The Assistance and Access Act)」, 캐나다의「Communications Security Establishment Act」등이 그 예이다. 이 밖에 네덜란드, 스웨덴, 노르웨이 등도 관련 법을 제·개정했다.[1] 이들 국가는 모두 해외 정보 수집을 하고 필요한 경우 상대에 대한 무력화 조치를 취할 수 있는 권한을 부여함과 동시에, 오남용을 방지하기 위한 통제 장치를 두고 있다. 행정부 내부에서 특별 영장을 청구하거나 대통령의 허가를 득하는 등의 사전 통제 장치를 마련하고, 사후에는 의회나 특별 기관에 보고하는 의무를 부여하며 때로는 특별 심사를 거치는 등 사후적 감독 절차를 마련하고 있다.[2]

일본 역시, 2025년 5월 해외 정보 수집을 포함한 사이버 안보 역량 강화를 미국, 유럽 등 주요국 수준 이상으로 강화하기 위한 신법과 정비법을 의회에서 통과시켰고, 2027년 전면 시행할 예정이다.[3] 흔히 'Active Cyber Defence Law'라고 불리는 이 법제는「중요 전자계산기 부정행위로 인한 피해방지 법안」(신법)과「동법 시행에 따른 관계법령 정비법안」(정비법)의[4] 크게 두 갈래로 구성된다. "신법은 주요기반 사업자와 정부 간 민관협력 강화, 사이버 공격 실태 파악을 위한 통신정보 이용에 관하여 규정하고, 정비법은 경찰 및 자위대의 사이버 공격 무해화 조치, 사이버 안보 거버넌스 정비 등을 규정한다."[5] 그동안 신중한 태도를 견지하던 일본이 능동적인 해외 사이버 정보 수집과 무력화 조치에 대한 근거법을 마련하고, 경찰과 자위대가 '접근 확인 및 무해화 조치'를 실시할 수 있는 요건과 절차를 구체화하고 역할을 분배하며, 독립기관을 설치하여 이를 승인 및 사후 통보하는 제도를 도입했다.[6]

(2) 現 사이버안보업무규정(대통령령)의 문제점

2024년 3월 5일 국정원은 사이버안보업무규정(대통령령 제34287호)을 일부 개정했다. 개정된 사이버안보업무규정은 '사이버안보정보 업무'에 "사이버안보 관련 정보의 수집·작성·배포 업무 수행에 관련된 조치로서 국가 안보와 국익에 반하는 북한, 외국 및 외국인·외국단체·초국가행위자 또는 이와 연계된 내국인의 활동을 확인·견제·차단하고 국민의 안전을 보호하기 위하여 취하는 대응조치"를 포함시켰다(제3조 1항 나). 이 대응조치를 실행하기 위해 "국가정보원장은 국가 안보와 국익에 반하는 국제 및 국가 배후 해킹 조직 등의 활동을 선제적으로 확인·견제·차단하기 위하여 국외 및 북한 소재 거점을 대상으로 추적, 무력화 등 필요한 조치를 할 수 있다"는 규정을 신설했다(제6조의2 3항). 이는 앞서 말한 해외 정보 수집을 할 수 있는 근거가 된다. 여기서 중요한 것은 '선제적

무력화 조치'까지 대응조치가 가능하다는 것과 '연계된 내국인의 활동'도 대상이 될 수 있다는 점이다. 선제적 무력화 조치란 사이버 안보 위협의 실행 이전이라도 국정원장이 합리적인 근거가 있다고 판단하면 미리 해킹 프로그램 등을 활용해 목표 대상의 시스템에 침투하여 향후에 예상되는 위협을 방해하거나 제거하겠다는 것이다.

신설된 사이버안보업무규정 내용은 지난 제21대 국회(2020–2024)에서 김병기 의원이 대표 발의했던 「국가사이버안보법안」에 있었던 '사이버안보위해자 추적 조치'의 내용을 상당 부분 반영한 것이다. 그러나 임기 만료로 폐기된 김병기 의원안에서는 사이버안보위해자 추적을 위해 '대통령의 승인'을 얻어 국외 또는 북한에 보관 중인 사이버안보위협디지털 정보를 수집하거나 사이버안보 위협행위를 '무력화'시키는 조치를 하도록 설계했었다. 그리고 추적 과정에서 어떠한 경우에도 사이버안보 위협과 무관한 국민의 법익을 침해해서는 안 된다는 조항도 있었다. 그러나 현 업무규정은 이러한 내용 없이 선제적 추적과 무력화 조치가 가능하도록 했다. 즉, 상위 법률인 국정원법에 있는 직무 규정(제4조 제1항 1호 마 및 3호) 외에는 어떠한 상세한 절차나 내용 및 견제 장치에 대한 법률의 규정 없이, '선제적인 무력화 조치'를 '내국인'을 상대로도 시행할 수 있도록 대통령령으로 규정한 것이다.

예측에 기반한 선제적 조치로서 때로는 우리 국민을 대상으로 할 수도 있는 선제적 무력화 조치에는 법원의 허가나 대통령의 승인처럼 합리적인 근거에 기해 선제적 조치가 필요한지를 판단하는 절차 및 사후 보고·검토 절차 등과 같은 오남용 통제 장치가 필요하다. 그런데 현재 업무규정에는 이 내용이 없다. 더욱이, 헌법 제37조 제2항은 국민의 기본권을 침해할 우려가 있는 입법을 할 때에는 반드시 법률로써 정해야 하는 법률유보(法律留保)의 원칙을 규정한다. 국정원법 직무 조항의 위임을 받더라도 그 내용과 범위는 예측 가능하고 명백해야 한다(명확성의 원칙). 정리하면, 현 업무규정상의 선제적 무력화 조치 관련 조항은 내용적으로는 적절한 오남용 통제 장치를 누락하고 있고, 형식적으로는 명백하고 체계 정합적인 법률적 근거에 기반하고 있지 않다. 이는 해당 임무를 실행하는 요원들이 합당한 법적 보호를 받기 위해서라도 개선되어야 한다. 따라서 현 사이버안보업무규정 제6조의2 등의 내용을 보강하여 상위 법령인 국정원법에 담는 개정이 필요하다. 그래야 다른 선진 유사입장국가들과 비슷한 수준의 입법이 된다.

(3) 사이버안보기본법이[7] 아닌 국가정보원법 개정을 통한 해결

2005년 대통령 훈령인 「국가사이버안전관리규정」을 통해 처음으로 국가 사이버 안보 체계를 마련한 이래, 최초로 제17대 국회(2004–2008)에 입법 발의 후, 제22대 현 국회(2024–2028)에 이르기까지 매번 사이버 안보 관련 기본법의 입법 시도가 있었다. 제21대에서는 정보위원회 소관으로 국민의힘 조태용 의원이 「사이버안보기본법안」(2020.06)을 대표 발의했고, [8] 더불어민주당 김병기 의원이 「국가사이버안보법안」(2022.02)을 대표 발의했으며, [9] 이어서 과학기술정보방송통신위원회 소관으로 더불어민주당 윤영찬 의원이 「사이버보안 기본법안」(2022.03)을 대표 발의했다.[10] 그러나 모두 임기 만료 폐기됐다. 그리고 2025년 7월 11일, 국회 정보위원회 소관으로 다시 「국가사이버안보법안」이 국민의힘 유용원 의원에 의해 대표 발의되어 계류 중이다.[11]

약 20년에 걸쳐 명칭과 내용을 조금씩 바꾸어가며 여러 차례 발의되었음에도 사이버 안보 관련 기본법이 여전히 통과되지 못한 데에는 여러 복합적인 요인이 작용했다. 사이버 안보(보안)의 주도권을 둘러싼 정부 부처 간의 대립, 사이버 정보 수집이 자칫 사찰이나 감시로 이어질지도 모른다는 불안과 불신, 그리고 사이버 안보를 국가 및 국제 안보의 큰 흐름 속에서 바라보지 못한 태도 등이 그 주요한 이유로 꼽힌다. 무엇보다 국민의 입장에서 볼 때, 기본법이든 개별 관련법의 개정이든 그 형식은 그다지 중요치 않다. 기본법 형식의 채택은 입법자의 선택에 달린 것이지 필수적인 것도 아니고, 기본법이 관련 개별법보다 체계상 우위에 있는 것도 아니다. 기본법 담론은 오히려 정부 부처 간 소관 사항에 대한 주도권 확보를 위한 거버넌스 싸움이라고 볼 수도 있다. 따라서 실질적으로 사이버 안보를 튼튼히 한다는 관점에서 모든 사안에 접근해야 하며, 사이버 안보 기본법 제정을 둘러싼 소모적 논쟁을 끝내야 한다.

사이버 공간의 특성에 맞게 정보기관이 정보 수집 역량과 전문성을 발휘할 수 있도록 뒷받침하는 사항 중 법률로 규정해야 하는 것은 국정원법을 개정하면 된다. 직무 조항을 보완하고 오남용 통제 장치 조항을 신설하면 된다. 사이버 위협 대응은 고도로 축적된 정보 역량과 실전화된 대응 기술이 요구되는 작업이다. 국제적인 테러 단체의 움직임이나 핵심 기반 시설에 대한 사이버 공격의 징후 혹은 국가 핵심 산업 기술에 대한 탈취 등 다양한 루트의 사이버 위협이 탐지되면 관련 정보 파악을 위해 역추적 등 사이버 활동을 해야 한다. 그러나 그간의 입법 미비로 당장 오퍼레이션을 할 수 없었던 정보기관의 고충도 이해할 만하다. 그래도 우리의 사이버 안보 법제와 정책, 전략이 실시간으로 국제 사회와 공유되는 시대에 시행령으로 해외 정보 수집의 법적 근거를 삼아서는 안 된다.

2. 해외 개입 대응 법제의 정비

(1) 국제적 대응 동향

해외 정보 수집이 국가 안보에 위해가 되는 사이버 위협에 대응하기 위해 밖으로 나가는 것이라면, 해외 개입 대응은 우리 사이버 공간 안으로 들어온 사이버 위협을 다루는 것이다. 해외조작정보 및 개입(Foreign Information Manipulation and Interference, FIMI)은 EU 가 정립한 개념으로 허위조작정보를 포함하여 폭넓게 일어나는 외세의 온라인 영향력 활동을 의미한다. 온라인 정보 조작을 통한 개입이 주로 문제되지만, 고전적인 간첩 활동(spying)을 하는 휴민트와 결합되면 더 큰 위협이 된다. 실제 호주는 온라인과 오프라인을 구별하지 않고 '해외 개입'(Foreign Interference)이라는 하나의 개념으로 포섭해 입법화했다. 앞서 지적한 바와 같이, 입법 형식은 입법자가 결단할 문제이지만, 입법의 필요와 요구는 주권자 및 국제 안보 환경에 달린 문제이다. 해외 정보 조작 및 개입에 대한 대응을 위한 법제의 정비가 필요하다.

미국은 해외악성영향(Foreign Malign Influence, FMI)이라는 개념을 정립하고, 외국의 악성 영향력 활동에 대응하기 위한 권한의 위임과 담당 기관(FMIC)의 신설 및 유관 부처와의 협력, 민주적 통제 방안까지 입법했다.[12] 영국도 2019년 허위조작정보대응반(CDU) 설치 후, 2023년 11월 명칭을 변경하여 국가안보온라인정보팀(NSOIT)을 운영하고 있다. 그리고 국가안보법2023 및 온라인안전법 등의 입법 조치를 통해 규율하고 있다. 프랑스 역시, 법령 제2021-922 호에 기해 디지털외세개입방지국(VIGINUM)이 총리실 직속 산하 국방 및 국가안보사무국(SGDSN) 소속으로 설립되어 2021년 7월부터 활동하고 있다. 동시에 고도의 자격을 갖춘 전문가로 구성된 '윤리과학위원회'(CES)를 두어 개인 데이터의 상담, 수집 및 사용에 대한 허가와 이행 조건을 모니터링하고, 디지털외세개입방지국의 운영을 감독한다. 독일이나 일본도 해외 정보 조작에 대응하기 위한 방안을 마련하고 있다.

그러나 우리나라는 해외 발 정보 조작과 그를 이용한 외국 정부의 개입 활동에 대응할 수 있는 법제가 정확히 없다. 정확한 수권 조항을 입법하지 않고 모호한 기존 조항을 활용해 정부 기관의 위임 범위를 늘려 활동하는 것은 장기적 관점에서 오히려 해롭다. 국내 정보

환경을 보호하고 정보 온전성(information integrity) 확보를 통해 국내의 민주적 절차를 수호하는 일은 헌법적으로 명백하고 정당한 법제 설계를 통해 이루어져야 한다.

(2) 간첩 행위와의 유기적 연결

위에서 본 국가들이 법률적으로 정확한 수권 조항을 신설하고, 담당 기관을 만들며, 감독·통제 장치를 설계한 이유는 그만큼 온라인 정보 조작을 통한 해외 개입 행위를 감시하고 방어하는 것이 어렵고 미묘한 임무이기 때문이다. 온라인에서 내국인의 개인적인 일탈인지 외세의 권한 없는 조직적인 행위(Collaborated Inauthentic Behaviors, CIB)인지를 식별하여 후속 조치를 취하는 것은, 일견 모니터링이라는 이름 아래 검열하고 사찰하는 것이 아닌가 하는 의심을 갖게 할 수 있다. 사이버 공간에서 순식간에 국경을 넘어 벌어진 정보 조작을 추적해서 규명하는 일은 기술적, 법적 지원 없이는 힘들다. 그런 측면에서 오프라인의 휴민트와 연결된 증거를 보여주는 일은 더욱 값지고 중요하다. 특히, 자금의 흐름을 추적하고 대리인(proxy)을 조사하여 후속 조치를 취하려면, 간첩죄를 비롯한 관련 법령의 정비도 함께 이루어져야 한다.

최근 2025년 4월 필리핀 상원의원 프란시스 토렌티노(Francis Tolentino)는 주 마닐라 중국 대사관이 마닐라 소재 홍보 회사와의 계약을 통해 온라인에서 중국에 유리한 여론 조성을 위한 목적으로 댓글 부대(troll farms)를 이용한 조직적인 개입 활동을 지시했다며, 금융 거래 내역과 함께 폭로했다.[13] 실제로 주 필리핀 중국 대사는 이에 대해 제대로 반박하지 못했다.[14] 독일에서도 원내 의원 등이 러시아로부터 자금 지원을 비롯한 광범위한 개입에 노출되었음이 보도된 바 있고,[15] 유럽의회에서도 해당 의원의 특권을 면제하는 등 절차가 진행 중이다.[16] 이처럼 새로이 등장하는 현상을 포섭하기 위하여 형법상 간첩죄 및 관련 범죄 조항들을 재정비하고, 해외 정보 조작 및 개입 등을 규율할 새로운 법을 제정할 필요가 있다.

III. 국가사이버안보전략의 실질적 강화

1. 국가사이버안보전략 평가 및 국제적 동향

우리나라의 최초 국가사이버안보전략은 2019년 4월 공개됐다. 주요 유사입장국가들과 비교하여 대략 10년 정도 늦은 첫 발간이었다. 디지털 강국의 전략이나 입법 그리고 정부의

입장 및 정책 방향은 늘 국제 사회의 관심 대상이다. 특히, 사이버 안보 분야의 정부 정책 문서들은 유엔을 포함한 다양한 국제 기구나 비정부기구 플랫폼에서 거의 실시간으로 공유된다.[17] 이에 실전 사이버 보안을 잘 하는 것만큼이나 법제와 전략, 정책 분야의 정보 공유 및 국제적 소통도 중요하다.

2024년 2월 개정된 국가사이버안보전략이 발표됐다. 국가 전략의 개정을 위해서는 이전 전략의 실천 상황과 효과 등을 검토하는 리뷰 작업이 선행되어야 한다. 영국 정부는 매번 리뷰 보고서를 낸 이후 국가 전략을 갱신하고, 호주도 전략 개정을 위해 이해관계자들의 의견을 수렴하는 제도 등을 둔다. 반면, 한국의 사이버안보전략은 그 작성 과정이 공개되지 않고 폭넓은 이해관계자의 의견 수렴 절차도 거치지 않는다. 특히, 전략의 개정을 위해서는 종합적인 검토 작업과 그에 따른 평가와 반성 및 변화된 안보 환경을 반영하는 토론 과정이 필요하다.

2024년 국가사이버안보전략은 미국 하버드 대학교 케네디 스쿨 벨퍼 센터가 조사·연구한 Cybersecurity Strategy Scorecard 에서 조사 대상 7개국(미국, 영국, 독일, 호주, 일본, 싱가포르 및 한국) 중 최하위를 기록했다. 해당 분석은 'Protecting People and Infrastructure', 'Generating Capacity', 'Building Partnerships', 'Codifying Roles and Responsibilities', 'Communicating Clear Policy'의 총 5개 분야에서 이루어졌는데, 한국의 전략은 대체적으로 구체성이 떨어지고 실질적 정책을 제시하지 못한 것으로 평가받았다. '사이버안보기본계획'의 추가적인 세부 사항을 고려해도 여전히 일관되게 세부 내용이 부족하다는 평가는 뼈아프다. 글로벌 동맹과의 파트너십 심화 및 사이버 공간 규범 관련 부분은 비교적 높은 점수를 받았지만, 산업계, 시민사회나 지방정부 등 국가 사이버 안보 계획에서 중요한 행위자들이 누락되고 책임성과 성과 평가 측면에서 다른 국가 전략들에 비해 뒤처져 있다는 지적이다.[18]

이는 상대적으로 늦은 국가 전략의 출발에, 제대로 된 리뷰와 소통 절차를 거치지 않고 전략을 갱신한 탓도 크다고 본다. 동일한 기관에서 실시한 기술 관련 사이버 안보 역량 평가에서는 상대적으로 좋은 평가를 받은 데 비해,[19] 전략, 법제, 정책 분야에서는 확연히 뒤처지는 모양새다.

2. 국가사이버안보전략의 상세화를 통한 실행능력 강화

이재명 정부는 빠르게 변화하는 사이버 안보 환경과 위협 등을 적절하게 반영하고 대비한 국가사이버안보전략을 수립해야 한다. 공약집에 따르면, 사이버 안보 분야의 공약은 '국민생활안전 및 재난대응' 분야에서 모두 '사이버 보안'이라는 용어만을 사용하고 있으며, 국가 안보 및 국제 안보 측면에서의 논의는 보이지 않는다.[20] 국내적 차원에서의 사이버 보안 확충, 대응체계 고도화 및 법제도 마련도 당연히 중요하지만, 초스피드로 초연결된 사이버 공간의 특성을 따른 국제적 차원의 고려도 중요하다.

현행 국가사이버안보전략 – 사이버안보기본계획 – 사이버안보시행계획으로 이어지는 구조에서 시행계획은 공개되지 않는다는 맹점이 있다. 벨퍼 센터 평가에서 전략과 기본계획까지 다 살펴보더라도 구체성이 떨어진다는 지적을 보면, 시행계획 단에 각 부처별로 많은 국가 사이버 안보 정책 및 실행 방안이 담겨 있을 것으로 예상된다. 최소한 기본계획 단의 내용을 전략으로 끌어올려 좀 더 종합적이고(holistic approach) 상세한 새 전략이 나올 필요가 있고, 시행계획에서 정말 기밀로 해야 할 사항이 아니라면 기본계획으로 공개하는 것이 바람직하다. 다른 유사입장국가들의 전략에 공통적으로 나타나는 중소기업에 대한 사이버 보안 지원, 디지털 경제 활성화 방안, 사이버 안보 정보공유 플랫폼 마련, 첨단 기술 선도를 위한 지원 방안, 사이버 안보 영역의 다중 이해관계자들의 참여 보장 및 확대, 관련 인력 육성 제도 및 프로그램 등 보다 다양한 사이버 안보 관련 분야들에 대한 상세한 목표 설정과 실행 로드맵이 차기 국가 전략에서 공개되길 바란다. 이런 사항들이 각 부처별 시행계획에 이미 포함되어 있을 가능성이 크지만, 구체적인 정보 공개 없이는 목표하는 국가 전략을 사회가 제대로 공유하기 힘들 것이다. 사이버 안보 관련 정책 내용의 상세화 및 확대된 정보 공유가 필요하다.

V. 결론

사이버 위협은 물리적 피해가 없이도 충분히 심각한 국가 안보 차원의 문제를 야기한다. 이미 각국은 여러 방식으로 국가 사이버 안보 법제를 정비하고 사이버 공간을 통한 정보 수집 역량 등을 고취하는 경쟁을 하고 있다. 기술력의 발전 못지않게 법과 제도의 정비를

통해 효율적인 거버넌스를 구축하고, 실제 오퍼레이션을 뒷받침하는 것도 중요하다. 이는 기본법 제정이 아니더라도 국정원법의 개정이나 신법 제정을 통해서도 입법적으로 해결할 수 있다. 국가사이버안보전략 부문은 이제까지 국가안보실 소관이었다. 국가 안보 컨트롤 타워로서 국가 및 국제 안보 차원의 종합적인 관점에서 좀 더 발전되고 상세한 국가사이버안보전략을 수립해야 한다. 실용성(practicality)과 연속성(continuity)을 중시하는 이재명 정부가 AI 산업이나 사이버 보안 분야뿐만 아니라 이와 함께 모두 연동되어 있는 국가 사이버 안보의 법제 및 전략 정비에도 힘쓰길 고대한다.

저자

신소현 박사는 아산정책연구원의 외교안보센터의 연구위원이다. 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 국내규범의 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.

[1] 김창섭, 윤상필, 이상진, '해외정보기관의 디지털정보 수집 법제도 분석 – 4 개 중견국의 사례를 중심으로' 국가전략 제 29 권 제 1 호 (2023) 147-176.

[2] 김창섭,「안보 목적의 온라인 정보수집 활용을 위한 법·기술적 수행방안」박사학위논문 (고려대학교 2022)

[3] JIJI, 'Japan Enacts Active Cyberdefense Law' *the Japan times* (16 May 2025) <https://www.japantimes.co.jp/news/2025/05/16/japan/politics/cyber-bill-enactment/> accessed 20 May 2025.

[4] 내각관방, サイバー安全保障に関する取組（能動的サイバー防御の実現に向けた検討など）(사이버 안보에 관한 대처 (능동적 사이버 방어 실현을 위한 검토 등)) <https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/index.html> accessed 20 May 2025.

[5] KISA, 2025 년 1 분기 인터넷·정보보호 법제동향 44.

[6] Ibid 44, 49.

[7] 기본법'이란 "정책입법・프로그램법으로서의 기능과 성격을 가지는 독특한 입법 형식, 즉 정책의 이념이나 기본이 되는 사항을 정하고, 그에 의거하여 시책을 추진하거나 제도의 정비를 도모하는 입법 유형"으로서 "여러 법령에서 규정하고 있는 사항에 대한 기본 원칙이나 정책 방향 등을 규정하는 경우에는「○○ 기본법」이라는 표현을 사용한다. (김현준, '기본법의 정체성 문제와 이른바 행정기본법 명명의 오류', 법조 제 68 권 제 4 호 (2019) 15-16; 법제처,「법령입안심사기준」(2021) 723)

[8] 국회의안정보시스템 [2101220] 사이버안보 기본법안(조태용의원 등 27 인) <https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_S2C0I0T6E3Q0C1X7W4E3I0B7S5Z7Z9>

[9] 국회의안정보시스템 [2113145] 국가사이버안보법안(김병기의원 등 13 인) <https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_P2I1J1H0N0V6U1T8K5N5C5E2H8A6B0>

[10] 국회의안정보시스템 [2113670] 사이버보안 기본법안(윤영찬의원 등 12 인) <https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_T2B1W1I1M1F7U1Z8F2R2A4I5D8L6X9>

[11] 국회의안정보시스템 [2211450] 국가사이버안보법안(유용원의원 등 10 인) <https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_U2Q5P0P7N1O0N1N6V4V7U3S4T3R5S0>

[12] 50 U.S.C. §3059: Foreign Malign Influence Center (2023 년 11 월 26 일 발효)

[13] Senate of Philippines, Tolentino Exposes Link Chinese Embassy and Troll Farms (Press Release 24 April 2025) <https://web.senate.gov.ph/press_release/2025/0424_tolentino1.asp>

[14] Mara Cepeda, 'Manila Accuses Beijing of 'Sinister' Campaign to Sway Midterms, Push South China Sea Narratives' *The Strait Times* (25 April 2025) <https://www.straitstimes.com/asia/se-asia/manila-accuses-beijing-of-sinister-campaign-to-sway-midterms-push-south-china-sea-narratives> accessed 27 April 2025.

[15] Maik Baumgärtner, Markus Becker, Jörg Diehl, Martin Knobbe, Timo Lehmann, Ann-Katrin Müller, Sven Röbel, Marcel Rosenbach, Fidelius Schmid, Wolf Wiedmann-Schmidt und Steffen Winter, 'How the AfD Became the Long Arm of Russia and China' *SPIGEL International* (1 May 2024) <https://www.spiegel.de/international/germany/afd-spionageaffaere-russland-und-china-im-fokus-neue-enthuellungen-belasten-die-partei-1714480876-a-a1c05e64-b6bc-4c6b-844e-a78a32ec4f91> accessed 17 July 2025.

[16] European Parliament, Report on the Request for Waiver of the Immunity of Petr Bystron (A10-0077/2025) < https://www.europarl.europa.eu/doceo/document/A-10-2025-0077_EN.html#_section3>

[17] UNIDIR, Cyber Policy Portal <https://cyberpolicyportal.org/>; NATO CCDCOE, Applicability of International Law <https://cyberlaw.ccdcoe.org/wiki/Applicability_of_international_law>

[18] Harvard Kennedy School Belfer Center for Science and International Affairs, Cybersecurity Strategy Scorecard <https://www.belfercenter.org/research-analysis/cybersecurity-strategy-scorecard>

[19] Harvard Kennedy School Belfer Center for Science and International Affairs, National Cyber Power Index 2022 <https://www.belfercenter.org/publication/national-cyber-power-index-2022>

[20] 더불어민주당, [제 21 대 대통령선거 더불어민주당 정책공약집] 이제부터 진짜 대한민국: 회복·성장·행복으로 국민통합 <https://theminjoo.kr/main/sub/news/view.php?sno=0&brd=188&post=1212023&search=> 98-99.