No. 67

IIRI Online Series

코로나-19 시대의 사이버 안보

임 종 인

고려대학교 정보보호대학원 교수

2020. 5. 25

일민국제관계연구원
Ilmin International Relations Institute

코로나-19 시대의 사이버안보

임 종 인 | 고려대 정보보호대학원 교수

코로나-19로 인한 글로벌 팬데믹 위기는 인류의 삶을 크게 바꿔놓고 있다. 온라인 쇼핑이 급증하는 등 소비 환경이 변화하고 있고, 재택근무가 본격화되는 등 업무 환경이 변화하고 있으며, 화상회의 및 원격수업이 확산되는 등 소통과 교육의 방식도 변화하고 있다. 안전성 문제로 우려되던 전자투표, 원격진료 도입 논의도 본격화되고 있다. 코로나 시대의 인류는 대부분의 시간을 타인과의 직접 대면을 최소화하면서 온라인에서 보내고 있다. 이러한 비대면, 비접촉 생활방식은 이후 포스트 코로나 시대의 '뉴노멀(New Normal)'로 우리의 일상에 계속 자리 잡게 될 것으로 예상된다.

문제는 인류의 온라인으로의 이동이 오프라인의 위험을 감소시키는 반면, 온라인에서의 위험을 증가시킨다는 점이다. 개인적 삶과 사회적 활동의 많은 영역들이 사이버공간으로 들어오면서 이를 겨냥한 범죄와 테러, 스파이 활동도 사이버공간으로 빠르게 이동하고 있다. 확장된 온라인 활동과 늘어난 트래픽 양은 사이버 범죄자들과 사이버 스파이들의 먹잇감이 되고 있다. 또한, 코로나-19 위기는 사이버 공격자들이 활동하기 좋은 최선의 조건을 제공한다. 높은 청년 실업률은 이들의 사이버범죄 가담 가능성을 높여주고, 경기침체로 인한 국가들의 글로벌 양극화 현상은 일부 개발도상국들을 북한처럼 국가적 차원의 사이버범죄 활동에 나서도록 만들 수도 있다.

이미 코로나 시대의 사이버 위험에 대한 많은 경고들이 있어 왔는데, EU 집행위원회는 북한 등 22개국을 코로나-19 위기 이후 조심해야 할 대상으로 선정하고 사이버해킹이나 금융 질서 교란에 대처해야 한다고 발표했다. 미국 정부는 지난 4월 북한의 사이버해킹 시도가 미국과 국제사회, 특히 국제 금융체제에 위협이 되고 있다고 지적했으며, 유럽중앙은행은 은행들에게 코로나 시대에 증가하는 사이버공격에 대비하라고 경고한 바 있다. 실제로 세계 곳곳에서 코로나-19로 인한 사회 혼란을 악용하는 사이버공격들이 등장하고 있다. 안전이 검증되지 않은 줌(Zoom)과 같은 원격회의 소프트웨어는 시민들의 개인정보와 기업 및 국가 기밀을 노출시켰고, 사람들의 공포심을 이용한 스미싱과 가짜뉴스들도 지속적으로 증가하고 있다. 3월에는 체코의 대학병원이 랜섬웨어 공격을 받아 병원 전체가 마비되기도 했다.

코로나-19 위기는 인류 공동의 위협에 대한 국가 간 협력의 장이 되기보다는 보호주의 경향을 강화하고 미·중 간 갈등과 패권 경쟁을 심화시키는 계기가 되고 있다. 이러한 배경 하에 사이버수단을 활용한 국가 간 첩보전과 심리전은 더욱 증가하고 있다. 미국 FBI는 코로나-19에 관한 가짜정보를 전파하는 1만 개 이상의 트위터 계정이 중국 정부와 연관되어 있다고 발표했다. 또한, 화웨이 사태로 대표되는 미·중 간 최첨단 IT 기술전쟁도 지속될 것으로 예상된다. 이미 중국은 코로나-19 위기를 자국 내 5G망 구축 및 해외 진출을 통한 디지털 실크로드 개척 기회로 전략적으로 활용하려 하고 있고, 이를 통해 개발도상국에서의 기술 리더십을 확보하려 하고 있다.

백신 개발이 국가경쟁력과 글로벌 리더십 강화를 위한 새로운 기술전쟁의 장이 되면서, 타국 백신 연구기관을 대상으로 백신 개발 정보를 빼내려는 사이버첩보 활동도 본격화되고 있다. 로이터(Reuters)는 코로나 연구데이터가 모든 해커의 우선순위 표적이 되었다고 보도했고, 미국 정부는 중국 공산당 등 외국 정보기관에 의한 미국 백신 해킹시도가 예상된다고 발표했다. 영국 전문가들은 적대국들이 코로나 바이러스 연구를 훔치기 위해 영국 대학과 연구시설을 해킹하려 하고 있다고 경고하고

있다. 미국 FBI는 중국 연계 해커들의 미국 코로나 연구기관 대상 활동을 조사하고 있다고 발표하기도 했다.

포스트 코로나 시대에는 국가첩보 활동과 군사 활동도 언택트(untact) 상황에 맞춰 변화할 것이다. 국가 간 사이버첩보는 보다 더 일상화할 것이며, 국가적 목표 달성을 위한 저강도 도발로서의 사이버군사 활동도 증가할 것으로 예상된다. 미국의 사이버공간 솔라리움 위원회(Cyberspace Solarium Commission)는 코로나-19 위기 와중인 지난 3월 미국의 국익을 겨냥한 사이버공격에 대응하기 위해 선제 방어(Defend Forward) 및 지속적 교전(Persistent Engagement)을 포함한 다층적 사이버 억지전략을 골자로 한 새로운 사이버안보 전략의 큰 그림을 발표했다.

우리도 당면 코로나-19 위기와 다가올 포스트 코로나 시대에 주요 사이버 표적이 될 수 있음을 인식하고 포스트 코로나 시대의 사이버위협 환경에 대비한 새로운 사이버안보 전략을 수립하고 선제적으로 대응해나가야 한다. 이미 코로나 시대 북한의 사이버공격에 대한 여러 국가들의 경고가 있었고, 우리가 북한의 핵심 표적이 될 가능성은 높다. 중국과 서방 국가들과의 기술전쟁 와중에 서방 국가들의 공급망에 포함된 삼성전자 등 우리 기술업체들이 공격당할 위험성도 존재한다. 지금 이 순간 코로나 백신을 연구 중인 우리 바이오 제약기업들이 공격당하고 있을지도 모른다.

모든 위기는 동시에 기회이기도 하다. 언택트 환경에서 전 세계적으로 보안의 중요성은 더욱 높아지고, 포스트 코로나 시대의 슬기로운 비대면 생활을 위해 온라인 보안은 필수가 될 것이다. 코로나-19 위기를 통해 국민들은 자신이 사회의 안전을 유지하는 핵심 주체임을 자각하게 되었고, 자기를 보호하는 동시에 타인을 보호하기 위해 불편을 감수하고 마스크를 썼던 경험은 포스트 코로나 시대의 온라인 환경에서 나와 타인의 정보를 보호하기 위해 불편을 감수하고 보안수칙을 준수하는 노력으로 이어질 수 있다. 자발적인 시민의 역능 중심의 건강한 사이버 안보체계가 구축될 계기가 마련되고 있다.

또 하나 간과할 수 없는 점은 코로나-19 위기 시대 미·중 갈등으로 인해 국제 리더십이 부재한 상황 속에서 사이버보안 분야의 새로운 연대와 규범의 맹아들이 생겨나고 있다는 것이다. 유럽 사이버보안 조직들은 의료기관에 대한 사이버위협 공동대응을 위한 연대 캠페인을 벌였고, 금융기관들은 코로나 시대 사이버위협으로부터 국제 금융시스템을 보호하기 위한 국제기구 구축 논의를 시작했다.

방역 선진국이자 디지털 강국인 우리가 이러한 새로운 연대와 규범 노력을 선도할 필요가 있다. 우리는 코로나 방역에 이어 포스트 코로나 시대 글로벌 사이버 문제 해결을 위해 실질적인 리더십을 발휘함으로써 오프라인-온라인을 아우르는 안전 선진국으로 세계적 위상을 정립하고, 이를 포스트 코로나 시대의 신흥 글로벌 IT-보안 시장을 개척하기 위한 기회로 활용해야 한다. 또한, 안전 선진국 위상을 최근 발표된 디지털 뉴딜 정책과 전략적으로 결합하여 일자리 창출과 국부 창출을 동시에 이끌어 내야 한다. 현명하게 코로나 시대 사이버 위기를 극복하고 포스트 코로나 시대를 국가 부흥의 기회로 만들기 위한 지혜와 실천이 필요한 때이다.

/끝/

저자 소개

임종인 교수는 대한민국의 대표적인 사이버보안, 정보보호 분야 전문가이다. 임종인 교수는 2015년 대통령 안보특별보좌관을 역임하는 등 사이버보안 전문가로 다양한 활동을 하고 있다. 그는 현재 고려대학교 정보보호대학원과 사이버국방학과 교수로 재직중이며, 이를 각각 2000년과 2011년에 직접 설립했다. 고려대학교 수학과에서 학사, 석사, 박사를 받았으며, 1986년 고려대학교 교수로 부임했다. 임 교수는 2007년 8월부터 2019년 8월까지 대검찰청 디지털수사자문위원회 자문위원장을 역임하였으며, 한국정보보호학회장, 대통령 직속 개인정보보호위원회 위원 등을 역임하는 등 다양한 자문활동을 해오고 있다. 임종인 교수는 2012년 제1회 정보보호의 날 행사에서 대통령 홍조근정훈장을 수상한 바 있다.(Email: jilim@korea.ac.kr)