Jeju Peace Institute 제주평화연구원

JPI PeaceNet

우크라이나에 대한 러시아의 사이버 공격: 특이성과 함의

김 소 정
국가안보전략연구원

단기간 내 패전할 것으로 예상되었던 우크라이나가 의외로 선전하고 국제적 지원도 받게 된 데에는 SNS의 역할이 지대하다. 전쟁 중임에도 불구하고 우크라이나가 SNS를 효과적으로 활용할 수 있게 된 주요한 원인은 에스토니아나 그루지아와의 전쟁에서와는 달리 우크라이나 전쟁에서 러시아가 사이버 공격을 통해 주요 핵심 기반시설을 파괴하지 못하였고 인터넷 통제권도 확보하지 못하였기 때문이다. 이 글에서는 우크라이나에 대한 러시아 사이버 공격의 특이성을 분석하고, 국가정책 수립과 국제규범 논의에 주는 함의를 논의한다.

사이버공간을 평화롭게 만들려는 각국의 노력은 오래전부터 시작되었다. 역사적으로 보면 미국보다 러시아가 그러한 노력에 더 적극적이어서, 일찍이 1980년대-1990년대에 러시아가 미국에게 인터넷과 사이버공간에서 정보전, 여론전, 심리전의 우려를 불식시키기 위한 규범을 제안한 적이 있다. 당시 러시아의 제안은 미국이 반대하여 무산되었다.

지금 우리가 목도하는 러시아의 행태는 과거 평화를 추구했던 러시아의 행태와 정반대이다. 현재 진행 중인 우크라이나, 그리고 그 이전의 에스토니아, 그루지아, 크림반도에 대한 공격 과정에서 잘 보여주듯이, 러시아는 인터넷과 사이버공간을 통해 여론전, 심리전을 적극적으로 수행했으며, 물리적 공격 이전에 주요 정보통신 기반시설에 대해 선제적으로 사이버공격을 가해 기반시설에 치명상을 입혔다. 또한 피해국 국민들의 정보 접속을 통제 및 차단하기 위해 인터넷 차단, 우회시킴으로써 효과적인 프로파간다와 오정보(misinformation)/허위정보(disinformation) 캠페인을 벌였다. 이는 결국 전쟁의 향방을 러시아에 유리하게 유도하여, 전쟁에서 러시아가 승리하는 데 크게 기여하였다.

러시아의 사이버 공격과정을 단계별로 단순화하면, 1) 러시아는 다양한 근거로 소련연방 해체 이후 독립된 국가들을 통합하여 소련연방을 복원하여야 하는 필요성을 주장하는 한편, 2) 독립된 국가들에 존재하는, 러시아에 심리적/정서적 유대감을 갖는 민족적 구성원들은 독립된 국가에서 분리독립을 요구하거나 정부에 대한 저항하는 등 반정부적으로 활동하며, 3) 러시아는 오정보(misinformation)/허위정보(disinformation) 캠페인을 통해 이들 세력이 부당한 대우를 받고 있거나 독립을 원한다는 점을 부각시키고, 4) 러시아에 우호적인 세력들이 받는 부당함을 해소하기 위해 러시아가 개입할 근거와 명분을 주는 사건을 직간접적으로 만들어내고, 5) 이를 계기로 독립국가에 개

입할 명분을 확보하고 갈등을 고조시킨 후, 6) 전면전 이전에 사이버공격을 통해 주요 기반시설 제어, 언론 통제, 인터넷 접속 통제 등을 선행하고, 7) 물리적 침공을 전개하고, 8) 진행 과정에서 독립국 국민들의 인터넷 접속, 언론 접속을 제한/오도하여 러시아에 유리한 내용만 공유되도록 하고, 9) 원하는 정치적 결과물을 얻어내는 과정을 거쳤다.

크림반도 침공을 예로 들면, 러시아는 우크라이나 국민들의 인터넷 접속 차단 이후 특정 부처 장관의 항복, 대통령의 망명 등의 허위사실을 고위층의 트위터로 전송하고 이것이 퍼지게 함으로써 국민들의 사기를 떨어뜨리고, 결과적으로 전쟁의지를 약화시켜 쉽게 승리를 거머쥐었다.

우크라이나에 대한 러시아의 사이버 공격

그런데, 이번 우크라이나 침공 과정에서 행해진 사이버공격에서는 기존 공격과 다른 면이 발견된다. 다른 단계에서는 거의 유사하게 진행되었으나, 6)에서 행해진 사이버공격의 결과가 그리 치명적이거나 전면적이지 않았다는 점, 8)의 과정에서 러시아가 절대적인 통제권을 확보하지 못했다는 점에서 차이가 있다.

상세히 살펴보자면 첫째로, 전면전 이전 러시아가 사이버공격을 감행했음에도 불구하고, 주요 핵심기반시설의 마비나 전산망 마비 등이 예전처럼 치명적인 수준으로 발생하지 않았다. 이점에 대해 전문가들은 그 이유를 여러가지로 추측하고 있다. 첫번째 가설은 우크라이나의 주요핵심기반시설을 유효적절하게 공격할 수 있는 정보를 러시아가 확보하지 못했었다는 의견이다. 즉, 정보수집 실패로 인해 러시아가 사이버공격의 효과적으로 전개할 수 있는 적절한 전략을 수립하지 못했다는 것이다. 두 번째 가설은 우크라이나의 주요핵심기반시설이 우크라이나를 되찾고자 했던 가장 강력한 이유였기 때문에 이를 무력화시켜 사용불능 상태가 되는 것은 전쟁을 일으킨 목적에 위배되기 때문이라는 의견이다. 세 번째 가설은 러시아의 사이버공격 역량이 높지 않거나, 우크라이나의 사이버방어 역량이 예상보다 강력했기 때문에 실제 공격을 시행했음에도 불구하고 효과를 보지 못했다는 의견이다. 이는 실제 공격에는 성공했지만, 우크라이나가 러시아에 다른 기밀절취 등 사이버공격을 되돌림으로써 약점이 잡혔기 때문에 쉽게 다음 행위로 넘어가지 못했다는 주장이 힘을 실어주고 있다. 네 번째 가설은, 러시아가 예전에 에스토니아, 그루지아, 크림반도를 대상으로 시행했던 사이버공격 이후 NATO가입국들이 포함된 국가들로부터 보복 공격을 받았고, 그 보복공격으로 인한 러시아의 피해가 컸기 때문에 또다시 그러한 공격을 감행할 수 없었다는 의견이 있다. 현재로써는 어떤 것이 정확한 이유인지는 알 수 없다.

하지만 여기에서 중요한 사실은 핵심기반시설에 대한 공격이 국제적으로 지탄받는 행위가 될 수 있는 환경이 이미 조성되었다는 점이다. 실제 2010년대 중반 이후부터 핵심기반시설에 대한 공격이나 복구 방해 행위에 대해 국제적 제재를 가하자는 의견이 종종 제기되어 왔었고, 2016년 방글라데시 금융공격 이후 IMF와 G7 국가들은 국제금융시스템 안전성과 신뢰성에 위해를 가하는 악의

적 행위에 대해 국제적으로 금지하고자 하는 국제전략을 발표하기도 했다. 주요핵심기반시설에 대한 중대한 사이버공격 발생 시 국제적인 대응 필요성에 대한 국제사회의 합의가 이번 우크라이나 전쟁에서 러시아의 변화를 야기했을 가능성이 있다. 핵심기반시설에 대한 보호는 국제적십자사 활동이나 전쟁시 의료진의 활동에 준하는 중요성을 갖고 대응해야 한다는 의견도 있었다는 점은 앞으로 평화적인 사이버공간을 규율하는 기준이 될 수 있을 것으로 판단된다. 우리나라에서 발생했던 피해측면에서 중간이상의 심각도를 가진 공격들이 대부분 기반시설에 대한 공격임을 생각하면, 앞으로 우리나라도 기반시설에 중대한 공격을 받게 되는 경우 국제적인 기준에 따라 대외적인 대응 수준과 방안을 정할 수 있기에 이러한 규율기준을 참고해야 할 것이다.

또 한 가지 살펴보아야 하는 점은 이번 우크라이나 사태 전개 과정에서 인터넷 통제권 보호를 위해 보여준 “민간전문가” 들의 기술적 접근과 “민간기업” 의 역할이다. 러시아가 전쟁 중, 우크라이나의 인터넷서비스를 마비시켰을 때, 우크라이나는 바로 서방국가들에게 기술적 지원을 요청했고, 서방국가들로부터 즉각적인 반응과 지원을 얻어냈다. 일론 머스크는 위성을 통한 인터넷접속을 지원했으며, 마이크로소프트도 유사한 역할을 했다. 뿐만 아니라 도메인네임 만기에 이른 러시아 사이트들의 인증서 갱신을 거부함으로써 러시아 국민들의 인터넷 접속 제한, 사업체들의 영업 방해 등 러시아를 인터넷으로부터 차단시키는 현상도 일어나고 있다. 또한 각국의 사이버보안 전문가들이 일종의 “민병대” 로 우크라이나의 사이버공격을 자발적으로 지원하고 도움을 주고 있기도 하다. 이 과정에서 주목해야 할 점은 이 모든 행위들의 주체가 국가가 아닌 “민간기업”, “민간 전문가” 들이라는 점이다. 물론 큰 틀에서 관할국가의 정치적 방향과 일치하기에 묵인되고 가능한 일이기는 하지만, 국가가 주체가 되어 판단하고 집행하는 정책이 아니라, 실제 정보통신 인프라를 설치ㆍ운영하고 활용하는 민간기업과 민간전문가들의 영향력이 크게 작용하고 있다는 점은 국제관계적 측면에서는 새로운 양상으로 보여진다.

인터넷 연결로 인한 초국경성, 사이버공간 생성으로 인한 초연결성은 그 인프라를 제공하는 기업과 기술전문가들에 대한 의존도를 상당히 높였고, 이들이 실제 인터넷과 사이버공간의 미래 모습과 방향을 결정해 왔다는 점은 주지의 사실이다. 하지만 이제는 이를 넘어서서 이들 민간기업과 민간전문가들이 사이버공간에서 발생한 부적절한 행위(irresponsible behaviour in cyberspace)에 대해서 사이버공간에서 책임있는 행위(responsible behaviour in cyberspace)에 대한 국제규범 형성 노력과 별개로, 기술적으로 이에 대한 접근과 활용을 제한하는 것을 결정하고 시행할 수 있게 된 것이다. 이는 한편으로는 초기 인터넷 개발자들 이후 기술전문가들이 지속적으로 주장해 온 “기술적 진보와 코드가 결국 미래를 결정한다” 라는 주장의 현실화이면서, 동시에 정책입안자들이 두려워 한 “이해하지 못하는 방식으로, 기술이 정책 의지를 반영하지 않은 채 앞서서 발전할 수도 있다” 는 가능성이 현실화 된 것이다.

사이버 공간 국제규범 논의에의 함의

여기까지가 지금까지 실제 일어난 현상이라고 한다면, 앞으로의 전망과 평화로운 사이버공간의 국제규범 논의를 위한 국가 정책 수립 방향은 어떠해야 하는가의 문제가 제기된다. 이에 대해서는 다음 네 가지에 대해 정부가 진지하게 고민해야 할 것이다.

첫째, 국가들은 인터넷을 구성하는 정보통신기술과 사이버공간을 "제대로" 이해해야 좋은, 제대로 된 정책 방향을 설정할 수 있음을 인식해야 한다. 아직까지는 스마트폰을 어느 정도 사용하는 사람들이 정보통신과 인터넷, 사이버공간의 미래의 방향을 기획하고 설계할 수 있었을지 몰라도, 앞으로는 상당한 수준의 전문성과 이해도가 없으면, 기술이 만들어내는 세상을 알 수 없는 시대가 되고 있음을 인지해야 한다.

둘째, 국가별 ICT 기술수준과 격차, 인프라 구축과 운영의 성숙도의 차이는 기존 국방력과 과학기술력의 차이와 마찬가지로 국력의 주요 요소가 될 것이다. 정보통신기술에 대한 국가적 차원의 지원은 해당 국가의 경제력과 국력에 선순환적으로 영향을 받지만, 그 비중이 기존의 전략무기나 방산물자에 대한 의존도와 유사하거나 그 이상으로 해당기술의 전문성과 성숙도가 차이가 발생할 수 있다. 우리나라가 국제전기통신연합(ITU)의 Cyber Index나 국제연합(UN)의 전자정부수준 평가에서 높은 순위를 기록하고 있는 것은 사실이나, 사이버공간의 방어·공격 측면 역량을 우리나라의 기준으로 평가·분석하기 위한 방법을 구비해야 한다. 현재 국가보안기술연구소에서 개발하여 방법론을 일부 공개하고 있는 국가사이버역량평가(K-GCCA) 결과와 IPA 방법론을 적용한 강약점 분석결과는 이러한 목적에 크게 활용될 수 있을 것이다. 특정 국가의 정보통신기술, 사이버기술의 성숙도에 대한 정확한 평가, 해당 국가의 강약점에 대한 명확한 이해에 기반해 신기술 개발과 활용을 위한 인력과 예산의 집중과 선택이 뒤따라야 한다.

셋째, ICT 기술인프라 수준의 차이는 원천기술을 얼마나 자국이 확보하고 있는가, 그 기술을 구현하고 배치할 수 있는 역량을 갖춘 민간 글로벌기업이 자국에 얼마나 있는가에 따라 해당국가의 역량을 판가름 나게 한다. 다행히 우리나라는 삼성, 네이버, 카카오 등 굴지의 IT 기업들을 보유하고 이들이 내놓는 훌륭한 서비스와 제품을 잘 구축된 인프라망을 통해 선도적으로 사용하고 있다. 하지만, 사용자가 인지하지 못하는 한 단계 아래의 원천기술 혹은 기반기술은 타국에 의존하는 경우가 많아 유효한 통제권이 있다고 보기는 어렵다. 이를 ICT 공급망 문제로 확대하면 우리가 최근 겪었던 화웨이 사태와 같은 일들이 지속될 수 있다는 것이고, 이 과정에서도 전략적 자율성 확보에는 한계가 발생할 수 있음을 인지해야 한다. 즉, 국가적 차원에서 전략적 원천기술과 사업 추진이 가능한 민간기업 확보 중요성이 더욱 커지고 있다.

넷째, 민간전문가와 민간기업이 주도하는 국제적 규범형성을 대비해야 한다. 여기에서 어려운 점은 국가가 주체가 아닌 규범형성 과정에 국가는 개입하기가 어렵다는 점이다. 국제적 규범을 형성하는 과정에서 국가가 뒤로 빠져있으면서 민간에서 알아서 만들어놓는 규범은 기술과 시장에 의존한 결정일 확률이 높아지는데, 과연 국가들이 이를 수용할 수 있는가, 이는 국가가 나아가고자

하는 방향과 합치하는가 등의 문제가 발생한다. 어떤 국가는 국제규범 형성과정에서 필요한 민간의 의견을 사전에 내부적으로 민간전문가들과 기업의 의견을 수렴·반영한 최종적인 국가의 입장을 제시하고 있으니 지속적으로 국가가 주도하는 플랫폼에서 해당 내용을 다루어야 한다고 주장할 수도 있다. 예를 들어 중국은 사이버공간 국제규범 형성을 위한 UN 정보안보 전문가그룹(GGE)에서 이와 같이 주장해왔다, 다른 한편으로는 다양한 이해관계자가 직접 참여하고 의사결정에 영향을 미칠 수 있는 플랫폼이 확장될 수도 있다. 미국 등 서방국가들은 UN GGE 회의 이외의 논의 플랫폼에 시만텍, MS, 아마존 등 민간기업을 적극적으로 참여시켰으며, 이들은 자발적으로 그들이 생각하는 안전한 사이버공간에 대한 원칙을 제시하거나, 공격근원지 추적시 국가를 적극적으로 지원하기로 협의하는 등의 활동을 꾸준히 지속해오고 있다. 우리나라의 삼성과 같은 일부 기업들도 사이버상에서의 신뢰와 보안 제고를 위한 Paris Call 이니셔티브에 참여한 바 있다.

그리고 마지막으로 이러한 상황에서 우리 정부는 어떤 외교적 입장을 견지할 것인지 구체적으로 고민해야 한다. 대내적으로는 이와 관련한 협의, 판단 및 결정을 정부가 주도적으로 이끌어갈 수 있는지, 가능하다면 누가 리더십을 가지고 추진할 것인지, 현재 과기계와 외교계가 나누어져 대표성을 나누어 가진 것은 문제가 없는지에 대해 다시 생각해 보아야 한다. 동시에, 대외적으로는 우리가 국제규범 형성과정에 참여하여 기여할 수 있는 여지가 있는지에 대한 냉정한 판단이 필요하다. 우리나라가 지금까지 어쩔 수 없이 보여왔던 전략적 모호성은 동맹국들에게 충분한 설득력을 갖고 있었는지, 신규로 출범한 다양한 협의체에서 제외되거나 정보공유 대상이 되고 있지 못한 것은 아닌지, 사이버공간의 국제규범 형성과정에서 우리 의견이 소극적으로 반영될 환경인 것은 아닌지 판단하고 앞으로의 대응방향과 노력의 정도를 결정하고 지속해야 할 것이다.

저자 사항

김소정은 現 국가안보전략연구원 책임연구위원으로서 공공영역에서 프라이버시 영향평가에 관한 연구로 고려대학교 정보보호대학원에서 박사학위를 취득하고, 국가보안기술연구소 정책연구실장을 맡았다.

2022년 4월