Jeju Peace Institute 제주평화연구원

JPI PeaceNet

랜섬웨어와 북한의 사이버위협

장노순

한라대학교 교수

저자 現 한라대학교 교수. 미국 플로리다주립대학교에서 정치학 박사학위를 취득하였음. 최근 저술로는『국제관계와 신뢰외교』(공저), “한반도에서 중층적 안보구조와 고비용 신호“, “사이버안보와 선도국 우위의 전략적 선택“ 등이 있음.

<목차>

1. 랜섬웨어의 등장

사이버 공격은 나날이 진화하여 정교해지고 심각성은 더욱 위협적이다. 이메일 첨부파일에 숨겨 둔 악성코드를 이용한 자료 훼손에서부터 시설을 파괴하는 정밀한 사이버무기까지 다양한 목적의 사이버위협이 지리적 공간의 한계를 넘어서 이루어지고 있다. 개인과 해커집단이 사이버 공격의 중심에 서 있지만, 국가가 직접 나서거나 배후에서 조종하는 은밀한 활동이 복잡하게 얽혀 나타난다. 정부가 직접 관리하는 사이버전사와 정부와 연계되어 활동하는 해커집단은 경계가 모호하고, 사이버 공격의 책임도 구분하기 어렵다.

금년 5월 중순 전 세계에 공포와 혼란을 불러일으킨 랜섬웨어 공격은 다시 한 번 사이버위협의

심각성을 일깨워줬다. 아주 단기간에 피해가 광범위하게 발생했고, 주요 강대국들이 예외 없이 공격을 받았다는 점에서도 우려가 컸다. 150여개 국가에서 30만대 이상의 컴퓨터가 감염됐고, 최초 공격 대상이었던 영국의 국가보건의료서비스(NHS) 산하 병원에서는 환자의 수술일정을 재조정하거나 응급실 혼란으로 퇴원조치를 취하는 등 심각한 부작용이 있었다. 프랑스 르노자동차는 직원들의 컴퓨터 사용을 막기 위해 임시 휴무를 결정했고, 그에 따른 비용을 감수해야 했다. 한국은 랜섬웨어 공격이 발생하고 주말로 이어지는 바람에 사전 대비책을 마련하면서 피해를 최소화할 수 있었다.

2. 북한 배후설의 확증

이번 랜섬웨어는 시스템이나 자료를 암호화하여 소유자가 접근하려면 비용을 지불하도록 요구했다. 몸값을 지불해야 풀려난다는 점에서 '컴퓨터 인질'인 셈이다. 한국을 비롯한 영국, 미국, 중국, 러시아 등을 포함한 주요 선진국들은 워너크라이(WannaCry)라고 불리는 랜섬웨어 웜 공격을 받았다. 미국의 국가안보국(NSA)이나 영국 정보기관인 정보통신부(GCHQ) 등 주요 국가와 민간 보안업체들이 찾아낸 근거들은 워너크라이가 북한이 배후로 깊이 연계된 해커그룹의 소행으로 점차 확증하고 있다. 국가가 직접 관여한 랜섬웨어의 공식적인 첫 사례라는 지적도 있다.

북한과의 연계가 분명한 라자러스(Lazarus) 해킹그룹은 2014년 말 소니영화사 해킹, 2016년 방글라데시 중앙은행 해킹, 금년 초 폴란드 은행들에 대한 해킹을 시도했다. 이들이 사용한 코드, 통제서버, 자료삭제 방식 등 유사성이 매우 높은 것으로 판명됐다. 이쯤 되면 북한 정권이 직접 관여하여 랜섬웨어 공격을 주도했다고 보더라도 큰 무리가 없을 듯싶다. 라자러스는 암호 해제의 조건으로 가상화폐 비트코인을 지불하도록 했지만, 전 세계가 겪은 혼란과 놀라움에 비하면 금전적 수익은 크지 않았다. 이는 국제사회가 북한 정권의 위험을 다시 확인하는 사건이었지만, 국제안보적 시각에서는 간과할 수 없는 숙제를 남겼다.

3. 워너크라이 랜섬웨어의 국제안보적 의미

북한의 성공 여부와 관계없이 이번 랜섬웨어는 사이버안보의 전략적 의미를 새롭게 부여하는 계기가 됐다. 지금까지 어떤 국가나 집단도 경험하지 못한 랜섬웨어 공격의 특징은 각국 정부의 고민을 한층 깊게 만들게 분명하다. 우선, 국가는 사이버시스템의 취약점을 비밀리에 활용하면서 국제사회의 공익 보호는 뒷전에 밀려있다는 점을 확인해 줬다. 워너크라이 웜의 공격은 마이크로소프트 윈도우의 운영체제에 있던 취약점을 이용했다. 윈도우의 취약점은 미국 국가안보국이 최소 2년 전에 파악하여 사이버무기로 해킹 툴을 만들어 활용되어왔다. 아직 확실하지 않지만 어떤 연유로 유출되어 공개됐다. 워너크라이는 이 취약점을 활용했다. 미국은 사이버 첩보활동을 위해 수백만 달

러의 비용을 들여 사이버무기를 만들어 이용했지만, 무기고 관리가 소홀하여 도난을 맞은 것이다.

브래드 스미스 마이크로소프트 사장은 미군이 토마호크 미사일을 분실했고 범죄 집단이 미사일을 획득하여 위협하는 꼴이라고 지적했다. 사이버공간에 대한 미국의 태도는 분명했다. 자국의 이익이 최우선 고려됐다는 점에서 사이버공간의 관리가 결코 공공재가 될 수 없음을 보여준 것이다. 다만 영국의 핵잠수함도 랜섬웨어 공격이 가능했던 윈도우 운용체제를 이용하고 있었으니, 도난당한 사이버무기의 위협은 금전적 손실로는 비교가 안 되는 심각성이 있었던 것이다.

둘째, 국제사회는 워너크라이 랜섬웨어 공격을 사이버 범죄 혹은 사이버 재난으로 여기면서 안보 위협이 아니라 인식이 강하다. 자료 접근의 비밀을 해제해 주는 대가로 돈을 요구했다는 점에서 범죄의 영역에 있다. 보안을 향상시키는 업데이트 서비스 대상에서 제외된 윈도우 운영체제는 범죄의 대상이었고 이런 유사한 사례는 얼마든지 일어날 수 있다. 금전적 목적이라 하더라도 배후 세력으로 확실시 되는 북한의 연루 가능성은 의미가 다르다. 사이버공격이 시설을 파괴하거나 엄청난 사회적 혼란을 목적으로 이루어진다면, 국가안보 위협의 범주에 있고 그에 따른 대응의 정당성도 한층 강화된다. 정치적 목적으로 행해진 사이버 공격은 전쟁 행위로 간주하는 국제법의 기준에 더욱 근접한다. 하지만 범죄는 대응 방식과 절차가 개인이나 집단을 대상으로 이루어진다.

북한은 절묘한 전략을 선택했다. 핵과 미사일개발로 국제사회의 경제제재가 강화되면서 북한은 외화벌이가 크게 위축되는 압박을 받는 상태다. 무기개발이나 통치자금의 부족은 북한정권의 심각한 위기이기도 하다. 경제제재를 우회하는 수단이 절박했던 북한의 입장에서 사이버 전략은 효율적인 대안이다. 방글라데시 중앙은행이나 폴란드 은행해킹 혹은 동남지역에서 사이버도박 등은 북한의 새로운 외화획득 방식으로 부상했다. 북한은 이번 랜섬웨어 방식이 아니더라도 사이버수단을 통해 전략적 목적을 달성하고자 할 것이다. 특히 북한정권이 국제사회가 논의하고 있는 규범적 제재의 대상이 되지 않는 안보와 치안이 혼재된 회색지대에서 활동할 가능성이 높다.

4. 국제사회의 대응과 한국의 처지

워너크라이 공격은 미국과 서유럽 국가들이 특정한 사이버 공격에 대해 실질적인 응징과 제재를 공동으로 추진하는 첫 사례가 될 수 있다. 국가가 연계된 사이버 공격이 불특정 다수의 국가(혹은 조직)를 직접 겨냥한 적이 없다. 이란의 핵시설을 공격했던 스턱스넷처럼 사이버 공격의 부작용이 여러 국가에 피해를 입힌 적이 있지만, 워너크라이는 단종된 윈도우 운영체제를 사용한 기관을 국적에 관계없이 표적으로 삼았다. 인명 피해가 없었고 엄청난 경제적 손실이 발생하지 않았지만, 미국과 서유럽 국가들은 북한의 소행으로 공식 확인한다면 이에 따른 제재 논의는 불가피할 것으로 보인다. 러시아의 사이버 공격에 대해 나토 회원국들이 공동 대응을 다짐했지만, 여타의 사이버 공격 사례에서 구체화된 적이 없다는 점에서 향후 국제사회의 태도는 안보와 외교적 의미가 크다. 사이버위협을 통제하려는 국제규범이 구체화하는데도 상당한 영향을 미칠 것으로 예상된다.

북한은 사이버 공격으로 미국의 제재를 받은 경험이 있다. 오바마 대통령은 소니영화사 해킹의 책임을 물어 대북 경제제재를 취했고, 사이버 반격으로 북한의 서버를 마비시켰다는 주장도 있다. 하지만 한국 정부와 은행, 언론기관을 상대로 북한의 사이버 공격이 있었지만, 이에 상응한 한국의 대응조치는 공식적으로 확인된 적이 없다. 미국이나 한국은 북한의 사이버위협을 억제하려는 추가적인 시도를 추진했었다고 하더라도 효과를 거두었다고 보기 힘들다. 북한은 거의 통제되지 않은 상태에서 사이버공간을 안보 목적의 새로운 전선으로 활용하고 있다. 이런 점에서 이번 랜섬웨어 공격에 대한 국제사회의 대응이 주목된다. 미국과 서유럽 국가들이 공동 대응의 출발점으로 부다페스트협약을 기반으로 삼고 이를 계기로 비회원 국가를 포섭하려는 확장의 기회로 삼는다면, 한국 정부는 회원 가입을 압박받는 숙제를 떠안게 될 것이다.

한국은 북한의 사이버 공격에 여러 차례 심각하게 노출됐고, 앞으로도 안심해도 될 만큼 사이버안보를 확보하는 일이 쉽지 않다. 그렇다고 국제사회와의 사이버 협력으로 자국의 사이버안보를 강화하기에는 여전히 가야할 길이 멀다. 국제사회는 지난 십여 년 이상 사이버위협의 확산을 통제하려는 노력을 경주했다. 유엔의 논의는 어려운 난제들이 합의되며 발전했음에도 불구하고 사이버위협의 속도를 충분히 따라지 잡지 못했다. 트럼프 행정부가 들어서면서 유엔의 다자간 협상에 대한 미국의 피로감이 표출될 수 있다. 북한의 사이버 공격이 이런 흐름에 촉매제로 작용한다면, 한국 정부는 전통적인 한미 안보동맹의 작동 원리를 넘어서는 더 깊은 전략적 사고를 해야 한다. 북한의 사이버위협에 대한 미국의 사이버 안보전략과 역량은 한국의 사이버안보를 보호해 줄 수 없다. 적어도 북한의 사이버위협에 맞서는 한국과 미국 간 사이버 안보협력은 군사동맹보다는 균형을 이룬 상태에서 추진될 수 있다.

2017.8.29 게재