Jeju Peace Institute 제주평화연구원

JPI PeaceNet

하드웨어 해킹의 위협과 국제협력의 필요성

한인택
제주평화연구원 연구위원

저자 現 제주평화연구원 연구위원(연구실장). 서울대학교 경제학과와 同 대학원 외교학과를 졸업한 후 UC, Berkeley 정치학과에서 박사학위를 취득. UC, Davis, University of Washington, 이화여자대학교, 제주대학교 등에서 강의. 핵전략, 안보협력, 공공외교가 주요 관심분야이며, "한국형 공공외교 모델의 모색: 정책네트워크를 활용한 맞춤형, 과학적 공공 외교"와 "핵폐기 사례연구: 남아프리카공화국 사례의 함의와 한계" 등의 저술이 있음.

블룸버그 통신은 지난 달 4일 애플과 아마존 등 30여개 미국 기업에 공급된 중국산 서버 컴퓨터에서 해킹을 목적으로 한 마이크로 칩이 삽입되어 있는 것을 발견했다고 보도했다. 중국이 미국 회사들로부터 정보를 빼내기 위해서 문제의 마이크로칩을 삽입한 것으로 블룸버그는 추정했다. 중국 정부는 블룸버그의 이러한 보도를 즉각 부인하였다. 애플과 아마존도 성명을 통해서 블룸버그의 보도를 부인하였고, 급기야 영국의 정보기관인 정보통신본부(GCHQ)의 국가사이버안보센터(NCSC)와 미국의 국토안보부(DHS)까지도 블룸버그 보도의 正誤를 둘러싼 논쟁에 끼어들어 애플과 아마존의 성명을 지지한다는 입장을 밝혔다. 하지만 블룸버그는 보도된 내용을 아직도 고수하고 있어서 중국산 서버 컴퓨터에 삽입된 마이크로 칩의 정체를 둘러싼 논쟁은 아직도 해결되지 않고 있다. 그러는 사이에 문제가 된 서버를 제작한 Super Micro 사의 주식은 폭락했다.

만약 애플과 아마존의 서버 컴퓨터에 스파이 칩을 몰래 심어 놓는다면 해당기업의 영업에 관련된 정보에서부터 전세계 각지에 있는 고객의 개인정보까지 막대한 양의 민감한 정보에 대해 접근이 가능하기 때문에 엄청난 문제가 발생할 수 있다. 소프트웨어 해킹과 달리 하드웨어 해킹은 물리적으로 증거가 남기 때문에 일단 발각이 되면 조사가 용이할 것으로 일반적으로 생각이 되었으나 영국과 미국의 정보기관까지 끼어들어도 논란이 종식되지 않는 것을 보면 그러한 통념이 실제로는 잘 맞지 않는 것으로 보인다. 하드웨어 해킹을 통해 심각한 정보의 유출이 발생할 수 있으나 하드웨어 해킹의 탐지나 확인은 쉽지 않은 것이다.

한 통계에 의하면 전세계 휴대전화의 75%와 전세계 컴퓨터의 90%가 중국에서 생산되고 있다고 한다. 휴대전화와 컴퓨터뿐만 아니라 중국에서 생산되는 정보통신기술 제품과 장비는 무수하다. 특히 사물인터넷(IOT: Internet of Things)이 보급되면 우리 주변은 24시간 중국산 정보통신기기에 둘러

싸여 있게 될 것이다. 만약 블룸버그가 보도한 것처럼 중국정부가 중국에서 생산되는 제품과 장비에 '악성 칩(malicious chip)'을 심는 하드웨어 해킹을 한다면 어떻게 될까? 굳이 중국을 특정하는 이유는 중국정부가 유달리 나쁜 의도를 갖고 있다고 생각하기 때문이 아니다. 미국 국가안보국(NSA) 직원이었던 에드워드 스노든의 폭로를 통해서 알려졌듯이 미국처럼 자유와 사생활의 권리를 보장하는 법치주의 민주국가에서도 미국에서 생산된 하드웨어와 소프트웨어에 백도어(back door)를 만들어 놓고 비밀리에 사찰을 하였다(스노든의 폭로 이후에도 방법은 달리하겠지만 미국의 비밀사찰은 계속되고 있을 소지가 크다). 따라서 중국정부가 중국산 제품과 장비에 악성 칩을 심는 것은 충분히 가능성이 있는 일이고, 중국이 정보통신기기의 생산에 있어서 '세계의 공장' 역할을 하기 때문에 중국의 경우를 집중적으로 살펴보는 것뿐이다.

기존의 악성 코드 방어 도구나 방법을 통해서는 하드웨어 해킹의 탐지나 무력화가 어렵기 때문에 효과적인 대응이 힘들다. 따라서 사이버 안보를 중시한다면 중국산 제품과 장비의 사용을 제한하는 것이 바람직할 것이다. 하지만 만약 중국이 하드웨어 해킹을 시도하지 않고 있는데도 중국산 제품과 장비의 사용을 제한한다면 외교적 문제가 되는 것뿐만 아니라 중국산 제품의 새로운 기술이나 저렴한 가격의 혜택을 누리지 못하는 대가도 지불해야 한다. 그렇다고 새로운 기술이나 저렴한 가격의 혜택을 우선시하다가는 사이버안보가 취약해질 가능성이 있다. 즉, 하드웨어 해킹의 탐지나 분석이 어렵기 때문에 중국산 정보통신기기의 사용은, 특히 정부나 중요 산업에서 중국산 통신기기의 사용은 심각한 '안보'와 '혜택" 간 딜레마를 발생시킨다. 특히 5세대 이동통신 시대의 도래를 앞두고 '안보'와 '혜택'의 딜레마가 세계 도처에서 발생하고 있어서 충분한 분석과 현명한 대응이 요구된다.

중국 화웨이는 미국이나 한국, 유럽의 경쟁제품보다 기술도 앞서고 가격도 저렴한 5G 통신장비를 생산하고 있다. 따라서 화웨이의 5G 통신장비를 사용하는 것이 경제적으로나 기술적으로는 합리적인 선택이 될 것이다. 하지만 중국 정부에 의한 하드웨어 해킹의 위험성이 있기 때문에 각국은 선뜻 그러한 결정을 내리지 못하고 있다. 화웨이 5G 통신장비를 둘러싸고 세계 각국에서 현재 논란이 발생하고 있는데, 하드웨어 해킹의 위협이 발생시키는 '안보'와 '혜택' 간의 딜레마에서 각국이 어떻게 대응하는지를 잘 보여주고 있다. 예를 들어서 미국, 영국, 호주, 뉴질랜드, 캐나다의 경우를 살펴보면 이들 국가들은 Anglo-Saxon 국가들로 정치적, 문화적으로 유사성을 공유하고 있고, Five Eyes (FVEY)라고 하는 상호첩보동맹를 맺은 국가들이다. 이들은 신호정보에 관한 상호 협조 조약인 UKUSA 협정의 조인국이다.

하지만 이들 국가들은 중국 화웨이의 5G 통신장비가 주는 하드웨어 해킹의 위협 가능성에 대하여 다르게 대응하고 있다. 중국의 하드웨어 해킹의 가능성에 대응하여 미국과 호주의 경우는 화웨이 제품을 금지하는 방향으로 나가고 있고, 영국과 캐나다는 화웨이 제품을 사용하는 방향으로 나가고 있다. 한편, 뉴질랜드의 정책은 미국•호주와 영국•캐나다의 중간쯤에 위치하고 있다. 미국의 경우, 연방수사국(FBI), 중앙정보국(CIA), 국가안보국(NSA)이, 화웨이 스마트폰이 중국 정부의 정보수집 통로로 이용될 수 있다는 우려 아래, 미국 국민들에게 화웨이 스마트폰을 사용하지 말라고

공개적으로 경고를 하고 있다. 소비자 제품이 아니라 통신장비의 경우에는 더욱 엄격해서 트럼프 행정부는 한때 중국의 안보위협을 이유로 미국의 5G 통신망을 국유화하는 방안까지 검토한 것으로 알려져 있다. 이와 정반대로 미국과 바로 이웃하고 있는 캐나다에서는 사이버 안보 담당기관(Canadian Center for Cyber Security)의 수장이 의회증언을 통해서 화웨이를 5G 통신장비 시장에서 금지할 필요가 없다고 밝혔다.

각국이 혼자만의 정보와 분석에 의존해서 이렇게 하드웨어 해킹의 위협에 개별적, 차별적으로 대응하는 것은 최상의 선택이 아니다. 우선, 하드웨어의 생산국과 하드웨어의 소비국 간에는 정보의 공개와 공유를 통하여 불필요한 우려를 줄이는 것이 바람직하다. 하드웨어 해킹의 탐지나 분석의 어려움으로 인해서 만약 중국이 해킹을 할 의도가 없고 실제로 하드웨어 해킹을 하지 않더라도 이를 다른 나라에서 인식하고 인정하기가 어렵다. 따라서 실재하지도 않는 하드웨어 해킹의 위협에 대응하여 중국산 장비와 제품을 제한하는 상황이 발생할 수 있는데 이러한 상황을 막기 위해서는 하드웨어 생산국과 소비국이 보다 많은 정보를 교환하고 공유하는 것이 필요하다. 제품과 장비의 디자인, 제조, 배포, 운영, 유지 등 각 단계에서 정보의 교환과 공유는 소비국이 불필요한 의심을 줄일 수 있을 뿐만 아니라 생산국이 불순한 시도를 계획하기 어렵게 만드는 이중 효과가 있다(이러한 정보 교환과 공유는 전통적인 안보용어를 사용하면 신뢰구축행위에 해당할 것이다). 생산국과 소비국 간의 협력에 있어서는 영국과 캐나다가 선례가 되고 있다. 영국과 캐나다는 화웨이에 대해서 보안검증을 요구하였고, 화웨이는 영국과 캐나다의 정부기관과 협력하여 보안검증을 받은 후 양국의 통신시장에 진출하였다.

한편, 하드웨어의 소비국들은 하드웨어의 검사나 R&;;;D에 있어서 서로 협력하는 것이 바람직하다. 그리고 만약 하드웨어 생산국이 하드웨어 해킹을 저질렀다면 단합하여 책임을 묻는 것이 필요하다. 혼자서 책임을 요구하는 것보다 하드웨어 소비국들이 단합하여 책임을 물으면 그 효과도 크고 향후 하드웨어 해킹 가능성도 감소할 소지가 크다(이러한 협력을 전통적 안보용어를 사용하여 표현하면 안보협력이나 동맹에 해당할 것이다). 만약 더 많은 국가들이 참여하여 보안검증을 실시한다면, 즉 소비국 간에 협력이 이루어진다면 그 결과는 더 정확할 수 있을 것이고, 화웨이도 더 적극적으로 보안검증의 요구에 응할 것이다.

우리나라는 세계최초 5G 상용화를 목표로 5G 통신망 구축을 서두르고 있다. 이 과정에서 우리 정부는 5G 장비선정과 보안검증은 이동통신사 책임이라고 보고 화웨이 장비의 도입여부를 기업이 판단하도록 하고 있다. 이렇게 정부가 손을 놓는 태도보다는 영국이나 캐나다처럼 정부기관이 화웨이와 협력하여 보안검증을 실시하고, 비슷한 상황에 있는 다른 국가들과 보안검증에서부터(혹시라도 화웨이에서 하드웨어 해킹을 시도하였을 경우) 화웨이에 대한 제재까지 국제적으로 협력하는 것이 바람직하다. 하드웨어 해킹에 대응하는 데 있어서도 국제적 협력은 유용하다. 우리나라라고 예외가 될 수 없다.

2018.11.16. 게재