Jeju Peace Institute 제주평화연구원

JPI PeaceNet

국제 사이버 전쟁: 한계와 가능성

Andy YEE
Google

저자 現 Google 정책분석가. 영국 School of Oriental and African Studies (SOAS)와 Cambridge University에서 수학하였으며, 베이징 소재 주중 EU대표단에서 근무함. Global Voices Online 과 China Geeks 블로거임.

블룸버그는 최근 보도에서 중국을 근거지로 하여 수백여 개의 미국회사가 해킹된 것을 '사이버 냉전'이라고 선언했다.

일본의 미쓰비시 중공업이 중국발 사이버 공격을 받은 후인 2010년 10월에 파이낸셜 타임지의 한 평론가는 사이버 위협으로 인해 미일간의 전통적 군사안보동맹을 다시 활성화시킬 새로운 공동기반이 마련될 수 있을 것이라고 평했다. 그로부터 두 달 뒤에 일본 중의원이 중국발로 알려진 사이버 공격의 피해를 입게 되자, 이는 매우 합당한 평가로 보였다.

이러한 냉전적 사고방식이 서서히 각국 정부들로 하여금 '사이버 전쟁'과 '사이버 주권'에 초점을 맞추도록 유도하고 있다. 예컨대, 2010년 5월에는 미국 사이버 사령부가 발족되었다. 2011년 5월에는 백악관이 사이버공간에 대한 국제전략을 처음으로 발표하였고, 그 뒤를 이어 미국 국방부는 '사이버공간 작전전략'을 발표하였다. 미 국방장관 레온 파네타는 특히 전면적 사이버 공격이 초래할 잠재적 결과를 '제2의 진주만'에 비유하였다. 한편, 2011년 5월에 중국은 인민해방군 내에 사이버에 중점을 둔 '청군'이 존재함을 처음으로 시인하였다. 보다 최근에는 중국의 군사전략가들이 민간, 산업 및 군사 네트워크를 포함하는 사이버 전쟁 동원에 대한 '全 사회적' 접근방법을 요구하기도 했다.

이러한 관심은 정당한 것인가? 사이버 공간을 전쟁터로 취급하는 것은 증상을 원인과 혼동하는 것이며, 사이버 공격의 근원이 다른 곳에 있다고 하는 더욱 중요한 사실을 간과하는 것이다. 일례로, 온라인 범죄와 간첩행위에는 종종 경제적인 동기가 있다. 예컨대, 중국의 사이버 간첩행위는 외국기술에 대한 의존도를 줄이고 '중국에서 제조된' 것으로부터 '중국에서 혁신된' 것으로 나아가려는 더 큰 노력의 일환이다. 이러한 맥락에서, 미국의 대응은 중국으로 하여금 외국의 비밀

을 훔친다면 중국기업들이 자신의 혁신적 역량을 개발하려는 능력과 열망을 줄이게 될 뿐이라는 것을 납득하도록 하게 하여야 한다. 기술을 중시하는 기업가정신 문화를 촉진하는 혁신전략이 더 유망한 전략이다.

사이버 공격에는 정치적인 동기가 있을 수도 있다. 예컨대 2008년에 러시아는 조지아 정부의 웹사이트에 대한 사이버 공격을 시작했는데, 이는 남 오세티아의 분리지역에 대한 군사작전과 동시에 수행되었다. 2008년에 CNN이 중국의 티베트 억압에 대하여 방송을 하자, 중국의 '애국적 해커'들이 CNN에 대해 공격을 가하였다. 2011년 6월 남중국해에서의 베트남과 중국의 대립은 사이버 공간에서도 똑같이 벌어졌는데, 양국의 해커들은 상대 정부 웹사이트의 콘텐츠를 자신들 국가의 상징물로 바꿔버렸다.

하지만 사이버 공간을 새로운 전쟁지역으로 규정하는 것은 역사적 분규나 지정학적 경쟁으로 인한 국가간 불신과 같은 보다 근본적인 이슈를 간과하는 것이다. 사이버 전쟁에 대한 과도한 관심은 그러지 않았으면 존재하지 않았을 새로운 갈등을 만들어 낼 공산이 큰데, 이는 기존의 불신을 악화시킬 뿐이다. 사이버 안보는 경제, 사회 및 외교적 이슈와 결합된 복잡한 문제이며, 군사적 접근방법만을 통해서는 해결될 수 없다.

보다 중요한 것은 이러한 군사위주의 접근방법은 개방적이고 지구적이며 경계가 없는 인터넷의 특성과 부합하지 않는다는 것인데, 이들 특성들이 지난 십 년간 인터넷의 급속한 발전과 성공에 공헌해왔다. 미군의 몇몇 전략가들은 심지어 '사이버 웨스트팔리아 시대'를 주창하기도 하는데, 소위 사이버 웨스트팔리아 시대에서는 국가들이 그들이 과거 국제 시스템을 지배하게 된 과정과 유사하게 가상의 국경을 획정하고 이를 방어하게 된다.

하지만 2011년 1월 OECD 보고서에 의하면 사이버 전쟁의 위협은 매우 과장되었다고 한다. 국가적 또는 지구적 충격을 일으킬만한 파멸적이고 대규모인 사이버 공격은 분명 심각한 결과를 초래할 수 있지만, 아직은 전적으로 이론적인 수준에 머물러 있다. 사이버 공간은 온갖 종류의 위협으로 가득 차 있으며, 각국의 정부들이 이들 위험을 견뎌낼 준비를 해야 할 필요가 확실히 있다는 점은 맞다. 하지만 사이버 공간이 특정한 이해관계와 능력을 갖춘 행위자들의 복잡한 환경임을 고려한다면, 올바른 법적인 틀과 유인을 만들고, 각기 다른 그룹간 대화를 유지하는 것만이 이러한 준비를 가능케 할 것이다.

올바른 유인체계가 마련된다면, 엔지니어와 기업 및 인터넷 서비스 제공자들은 시스템을 보다 강화하고 불법 행위들을 더욱 잘 관리하도록 동기부여가 될 수 있다. 물론, 전 지구적 차원의 공통된 이해가 생기지 않는다면 올바른 유인체계만으로는 부족할 것이다. 필요한 전 지구적 공통의 이해란 위협의 인식보다는 취약점의 공유에 근거한 것으로서, 각 국가들이 자국 내부로부터 비롯된 공격에 대해 더 많은 책임을 지게 될 것이다.

사이버 공간에서는 필연적으로 友敵이 확실하게 구분되지 않기 때문에 이러한 합의가 가능하다. 인터넷은 양극적인 전략적 지평을 수용하지 않는다. 모든 국가들이 온라인 공격에 시달리기 때문이

다. 보다 안전한 사이버 공간을 갖기 위해 최선의 접근방식은 적을 상상하고 방어벽을 세우는 것보다 보다 나은 국제 거버넌스와 국제협력을 증진하는 것이다.

** 이 글의 원본 ("International Cyber War: Limits and Possibilities")은 East Asia Forum에 게재되었던 것으로, East Asia Forum과 제주평화연구원의 협약 하에 국문으로 번역하여 배포한다. 이 글에 포함된 의견은 저자 개인의 의견으로 제주평화연구원의 공식입장과는 무관하다.*

2012.5.1