Jeju Peace Institute 제주평화연구원

JPI PeaceNet

평창올림픽 사이버 공격: 어떻게 이해하고, 어떻게 대응할 것인가?

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.

* 이 글에 포함된 의견은 저자 개인의 견해로 제주평화연구원의 공식입장과는 무관합니다.

평창올림픽 조직위원회 오상진 정보통신국장은 지난 5월 2일 과학기술정보통신부가 개최한 정보보호 세미나에 참석하여, 평창 동계올림픽 개막일에 조직위원회 내부 시스템의 대부분이 사이버 공격을 받았으며, 52종의 서비스가 중단되었었다는 사실을 공개하였다. 조직위원회 정보통신국장의 발표를 통해서, 그동안 외신이나 전문가들 사이에서 회자되어온 평창올림픽 중 사이버 공격의 발생사실이 마침내 공식적으로 확인된 셈이다.

조직위원회의 발표가 없었더라면 이번 공격은 "잊혀진 공격"이 되었을 가능성이 크다. 공격자들은 피해자에게 더 큰 피해를 가할 수 있는 능력과 기회가 충분히 있었지만, 서비스 장애만을 유발시켜서 올림픽의 운영에는 큰 차질이 없게 하였다. 공격에 의해 중단된 서비스는 신속히 복구되었기 때문에 일반인들은 평창올림픽 개막일 즈음에 사이버 공격이 있었다는 사실을 눈치 채기 어려웠기 때문이다. 더욱이 피해자는 사이버 공격을 당하고도 거의 3달이 지나서야 사이버 공격을 받은 사실을 공개하였으며, 그 배후가 누구인지 밝히지 않았다. 이번 사건에서 공격자가 보여준 고도의 절제(self-restraint)나 피해자의 조용한(low-profile) 대응은 공격자의 신원이나 의도, 그리고 피해자의 대응전략에 대한 궁금증을 가중시킨다.

올림픽을 전후해서 사이버 공격이 발생한 경우는 이번이 처음이 아니다. 2016년 브라질 리우데자네이루 하계올림픽 때에도 해커들이 세계도핑방지기구 (WADA: World Anti-Doping Agency)의 데이터베이스에 접근하여 유명 운동선수의 의료정보를 포함한 기밀정보를 탈취하여 인터넷에 유출한 경우가 있었다. 러시아가 국가 차원에서 올림픽 선수들에 대한 금지약물투여를 지속적으로 해왔다는 사실이 내부고발자의 폭로로 밝혀져서 러시아 선수들이 리우올림픽에 대거 출전 금지되는 사태가 발생하였었다. 따라서 리우올림픽 때 해킹은 러시아 선수들의 올림픽 참가가 금지된 데에 대한

러시아의 불만표시로 추정되었다.

평창올림픽에서도 상황은 비슷하였다. 러시아의 도핑 때문에 러시아 선수들은 러시아 국가대표의 자격으로 출전하지 못하고 "러시아 출신 올림픽 선수들 (OAR: Olympic Athlete from Russia)" 의 자격으로 출전하는 것만이 허락되었다. 따라서 평창올림픽 중 발생한 사이버 공격도 리우올림픽 중 발생한 해킹처럼 러시아의 올림픽 참가가 제한되었기 때문에 발생한 것으로 보는 견해가 서구 언론이나 전문가들 사이에서는 지배적이다. 올림픽과는 관련이 없지만, 러시아 정부가 미국의 선거에 개입하고 영국에서는 독가스를 사용한 암살을 시도한 것으로 추정되는 등 러시아 정부에 대한 의혹이 최근 서구 국가들을 중심으로 증가하고 있다.

하지만 사이버 공격의 배후를 규명하는 것은 쉽지 않다. 특히 발각되었을 때 파장이 큰 해킹은 러시아 정부가 직접 나서기 보다는 국가권력과 가까운 민간인을 앞세울 가능성이 크다. 따라서 평창올림픽 중 사이버 공격이 '러시아' 라는 국가가 일으킨 것이라고 명확하게 결론 내리기에는 어려움이 있다.

어떻게 대응할 것인가?

공격자가 상당한 '자제' 를 발휘하여 피해가 심각하지 않았고, 공격자의 신원이 정확하게 파악될 수 없기 때문에, 올림픽이 끝난 이 시점에서 이번 공격에 대해 강력하게 응징해야 할 필요성이나 가능성은 상대적으로 크지 않다고 보인다. 특히 이번 공격에서 조직위원회의 컴퓨터가 공격을 받았지만, 우리나라를 타깃으로 하였다고 보기 힘들다. 러시아의 국가 출전을 금지하거나 도핑을 조사하는 주체는 한국이 아니라 IOC와 WADA이고, 러시아에 대한 비판적 여론을 주도하고 있는 것은 주로 미국과 유럽의 국가들이기 때문이다. 따라서 IOC와 WADA와 타깃으로 한 공격에 우리나라가 2차적 피해 (collateral damage)를 입었다고 보는 것이 정확할 것이다.

한편, 공격을 당한 후 아무런 응징을 하지 않는다면 향후 유사한 사건이 반복되는 것을 방지하기 어렵다는 데 우리의 고민이 있다. 사이버 공간은 국경이 없지만, 피해를 입은 컴퓨터들은 엄연히 우리나라의 영토 안에 있었기 때문에 주권수호의 차원에서 보면 '무대응' 은 바람직하지 않다.

하지만 공격자가 누구인지 확정할 수 없기 때문에 특정 국가를 지목하여 책임을 물을 수는 없다. 만약 여러 가지 정황을 근거로 러시아 정부한테 책임을 묻기로 결정한다면 공개적으로 책임을 묻는 것보다는 조용하게 우리의 우려를 전달하고 그들의 사과와 향후 반복이 없을 거라는 약속을 받아내는 데에 노력하여야 할 것이다.

만약 러시아에게 공개적으로 책임을 묻기로 한다면, 우리가 앞장을 서는 것보다는 IOC, WADA가 일선에 서고, 우리는 미국 및 유럽 등과 연대하여 참여하는 것이 바람직하다. 우리는 2차적 타깃이었으며, 단독으로 대응을 할 경우 발생하는 부담이 크기 때문이다. 만약 공개적으로 대응하는 방향

으로 결정을 한다면 구체적으로 아래와 같은 방안을 생각해 볼 수 있다.

- **국제공조:** 영국 내에서 전직 러시아 스파이가 독살되는 사건에 대한 책임을 물어 영국뿐만 아니라 20여 개국이 러시아의 외교관을 추방한 사례에서 볼 수 있듯이, 공격자에 대해 불이익을 주는 조치는 우리 단독으로 하지 않고 국제적으로 공조하여 실행하는 것이 바람직하고 효과적.

- **Name and Shame:** 만약 공격자를 확정할 수 있다면 공격자, 그리고 공격자가 소속되어 있는 기관이나 국가를 공개적으로 거명하여 국제여론의 심판을 받게 하는 것이 바람직. (Name and Shame 전략은 기후변화 방지를 위한 국제적 노력에서 의외로 효과적인 것으로 판명되었음.)

- **"Name and No Game"**: 만약 공격자를 확정할 수 있다면 공격자, 그리고 공격자가 소속되어 있는 기관이나 국가에 대해 경기출전이나 경기개최를 제한하는 정책을 실시하고 나아가 규정으로 명문화. 만약 IOC뿐만 아니라 FIFA 등 다른 국제스포츠기구들도 연대하여 참가할 수 있으면 이상적. 특히 러시아는 2018년 월드컵의 개최국이기 때문에 경기개최 제한조치에 대해 매우 취약.

사이버 시대가 도래함에 따라서 공격자의 신원을 확인할 수 없고 물리적 또는 법적 대응도 용이하지 않은 사이버 공격이 증가하고 있다. 빈발하는 저강도 사이버 공격에 대한 효과적인 방어전략과 억지전략을 개발하는 것이 정부와 민간의 커다란 과제가 될 것이다. 하지만 방어도 억지도 실패하는 경우가 발생하기 때문에 이에 대한 대응전략을 준비하는 것이 필요하다. 그런 면에서 이번 평창올림픽 사이버 공격과 그에 대한 대응은 우리에게 중요한 학습기회가 될 것이다.

마지막으로, 이번 사건에 대해 우월한 탐지능력을 가진 우호적인 국가들이 우리와 정보공유 등을 통하여 협조한 것으로 알려졌다. 이들의 탐지능력이 우리에게 도움이 되는 것은 사실이나 국익이 상충되는 경우가 발생할 경우 우리에게 불리하게 작용할 수 있기 때문에 우리 자체의 역량을 강화하는 것이 필요하다.

2018.5.28. 게재

저작권자 © 제주평화연구원, 무단 전재 및 재배포 금지