

**Panel:** 사이버 전쟁

**Date/Time:** 2015 년 4 월 28 일 (화요일) / 15:30-16:45

**Session Sketch by:** 김종우, 아산정책연구원 연구위원

**Moderator:** 데이비드 생어, 뉴욕타임즈 외교안보 전문 기자

**Speakers:** 벤 잭슨, 미국 신안보센터 연구원

박노형, 고려대학교 교수

런 닌, 중국사회과학원 연구원

마이클 라스카, 싱가포르 난양기술대학교 교수

'사이버 전쟁' 세션은 뉴욕 타임즈의 데이비드 생어 외교안보 전문기자의 사회로 진행됐다. 첫 번째 발제자인 벤 잭슨 미국 신안보센터 연구원은 "강력한 동기가 존재하기 때문에 소니 해킹이 북한의 소행임을 확신한다"고 말했다. 생어 기자가 "미국의 신속한 대응이 북한을 억제할 수 있었느냐"고 질문하자 잭슨 연구원은 "북한의 근본적인 행동 변화가 있을 것으로는 기대할 수 없다"며 "사이버 공격은 어떤 레벨에서 결정하는지, 작전은 누가 맡는지, 공격에 정치적 의도가 있었다면 누가 결정을 하는지 같은 요소를 파악하기 어렵다"고 하였다. 그는 "그럼에도 사이버 공격에 과잉 대응하는 것은 경계해야 한다"고 덧붙였다.

고려대학교 박노형 교수는 "'사이버 전쟁'이라는 용어가 과도 사용돼 잘못된 인식을 줄 수 있다"고 우려하면서 "오바마 대통령이 이제까지 미국에 대한 사이버 공격 가운데 가장 파괴적이었던 소니사 해킹에 대한 대응을 사이버 전쟁이 아닌 사이버 반달리즘으로 규정하며 신중히 대응한 점을 주목해야

\* The views expressed herein do not necessarily reflect the views of the Asan Institute for Policy Studies.

한다"고 말했다. '사이버 전쟁'이라는 용어의 사용을 자제해야 하며 올바른 접근 방식이 필요하다는 것이다.

생어 기자가 "2 년전 북한이 한국의 은행과 방송사를 해킹 공격 했을 때 한국은 어떤 대응을 했느냐"고 질문한 데 대해 박 교수는 "한국은 미국과 달리 무반응으로 일관하였다"고 답했다.

북한의 소니사 해킹에 대해 4 월 초 미국 재무성은 북한에 대해 금융제재를 하고 국무부는 비자 관련 불이익을 주는 등의 조치를 취했다. 박 교수는 "대부분 선진 국가는 사이버 안보 전략을 공식 발표하는데 한국 정부는 조만간 국가 사이버 전략을 발표할 예정"이라고 말했다. 그는 또 "사이버 공격은 군사적 측면뿐만 아니라 교역, 디지털 거래, 인권 등 비군사적 측면으로도 활용 가능하다"고 언급하였다.

싱가포르 난양기술대학교 마이클 라스카 교수는 "사이버 공격에 대한 인식과 사이버 안보에 대해 개념이 국가별로 다르고 하나의 일관된 개념이 없으며 지역별로 다른 용어, 다른 개념, 다른 접근 방식을 택하고 있다"고 하였다. 러시아의 하이브리드 전쟁을 모방하는 중국은 사이버 전쟁을 여타 군사 역량을 보완하는 개념으로 활용하고 있다. 그러나 미국은 사이버 전쟁을 육군, 해군, 공군, 우주군과 대등한 개별 분야로 보고 다섯번 째 공격력으로 삼고 있다. 라스카 교수는 "사이버가 물리적인 것과 구분 불가능하다는 점에서 중국의 사이버 전쟁 개념이 더 적합하다"며 "이밖에 소니 사건을 통해 북한이 WMD 와 더불어 사이버 전쟁의 효과(WME)를 입증하였다"고 하였다. 핵무기 파괴력은 제한적인 범위에서만 사용 가능한 반면, 사이버 전쟁은 분쟁 지역만을 대상으로 강력한 무기화가 가능해 상호 보완적이라는 것이다. 그는 "한국의 IT 의존성이

\* The views expressed herein do not necessarily reflect the views of the Asan Institute for Policy Studies.

매우 높아 취약하며 북한은 지속적으로 전략적 약점을 찾으려고 노력할 것"이라고 지적했다.

라스카 교수는 또 "미국-북한, 미국-이란 사이에 사이버 전쟁으로 갈등이 고조될 가능성이 높으며 사이버 공격을 통한 전초전이 실제 분쟁에 앞서 발생할 수 있다"고 하였다.

그는 "북한은 정보 유입에 대해 굉장히 민감하므로 사이버 공격을 할 경우 보복하는 방법 중 하나는 라디오를 이용해 정보를 유입시키는 방법이 있을 것"이라고 말했다.

중국 사회과학원 런 닌 연구원은 "사이버 보안에 관한 개념이 확실하지 않다. 현상뿐 아니라 그 이면까지 봐야 한다"며 "핵무기의 강력한 파괴력은 세력 균형을 유지시키지만 사이버 공격이 그런 억제력을 갖는지는 의문"이라고 말했다. 그는 "국가 사이에 사이버 공격 정보를 공유할 수 있는지, 국가간 약속이 준수되는지 파악하기 어렵고, 분쟁이 심화되면서 불균형과 불안정성이 초래될 것"이라고 지적했다.

아산정책연구원 천영우 고문은 "북한이 사이버 공격을 하는 이유는 사이버 산업이 미사일, 원자력과 더불어 주력 육성 분야인데 사이버 인력을 군사적으로밖에 활용할 수밖에 없는 한계가 있기 때문이다"라고 말했다.

\* The views expressed herein do not necessarily reflect the views of the Asan Institute for Policy Studies.