Jeju Peace Institute 제주평화연구원

JPI PeaceNet

사이버 시대의 국가 안보

한인택

제주평화연구원

저자 現 제주평화연구원 연구위원. 연구 분야는 국제정치경제, 핵전략, 공공외교. 서울대학교에서 경제학 학사 및 정치학 석사를 취득하고, UC 버클리에서 정치학 박사학위를 받음.

사이버 시대에 맞는 안보인식의 필요성

북한의 ICBM급 장거리 미사일 발사 성공과 곧 있을 것으로 보이는 3차 핵실험을 앞두고 안보분야를 총괄조정하는 관제탑 (control tower)으로써 국가안보실 설치에 관심이 쏠리고 있다.

국가안보실 설치를 지지하는 견해는, 안보관련 제도와 조직의 편제구조가 정부의 안보정책능력을 좌우한다는 전제 아래, 위기관리 능력의 향상, 그리고 나아가 중장기적인 안보전략의 준비를 위해서 안보관련 제도와 조직을 개편할 필요가 있다고 주장한다. 이러한 전제와 주장은 충분히 설득력이 있다. 어느 분야가 되든 정부의 제도와 조직의 편제구조는 그 분야에서의 정부 정책능력에 영향을 미치기 때문이다. 따라서 국가안보실을 신설하는 형태가 되든지 기존의 외교안보수석의 기능을 강화하는 방식이 되든지 간에 어떤 식으로라도 정부의 정책능력을 최대화하는 방향으로 제도와 조직을 개편하는 것이 바람직하다.

그런데 제도와 조직의 개편 못지 않게 인식과 사고의 발전도 정부의 안보정책능력의 향상을 위해서 필요하다. 아무리 잘 짜인 제도와 조직이라도 인식하지 못하는 위협과 경험해 보지 않은 위기에는 효과적으로 대응할 수 없기 때문이다.

제도와 조직 개편의 논의 과정에서 인식과 사고의 발전을 언급하는 이유는, 현재의 논의가 주로 기존에 확인된 위협을 최소화하고, 과거 경험한 위기의 반복을 막으려는 강한 동기에서 진행되기 때문이다. 물론 북한의 핵무기, 장거리 미사일, 서울을 사정거리에 둔 장사정포는 당연히 안보에 위협이 된다. 또 천안함 침몰이나 연평도 포격은 명백히 중대한 안보위기를 낳았다. 하지만 이렇게 알려진 위협과 경험해 본 위기에 잘 대응하도록 개편되는 제도와 조직이 반드시 새로운 위협과 위

기에 잘 대응할 수 있는 것은 아니다. 기술관리를 비유로 들자면, 기존의 아날로그 기술을 잘 다루는 조직이 반드시 새로 등장하는 디지털 기술을 잘 다루는 것은 아니다.

새로운 안보적 위협을 신속하게 인식하고 선제적으로 대응하기 위해서는 조직과 제도의 개편은 물론 기존의 안보개념으로부터 전향적으로 진화할 필요가 있다. 기존의 안보 개념은 '단선적'이고 '물리적'이다. 국경선, 휴전선, NLL 등의 경계선을 기준으로 '안'과 '밖'을 구분하고, 그 경계선을 강화하거나 물리적으로 침범되지 않게 하는 데에 주력하였다. 최근의 변화들은, 특히 국제화와 정보화의 진전은 경계선의 의미를 많이 퇴색시켰고, 사이버 공격이 물리적 타격 못지 않게 국가안보를 위협할 수 있음을 보여주었다. 새로운 안보 개념은 이러한 경계의 약화나 비물리적 위협의 등장을 반영하여야 한다.

최근의 사이버 공격사례**

새로운 안보적 위협을 이해하기 위해서는 최근 발생하고 있는 사이버 공격을 살펴보는 것이 유용할 수 있다. 아래는 최근 들어 사이버 '피공격의 대상지'로서 그리고 사이버 '공격의 진원지'로서 급부상하고 있는 중동지역에서 발생한 사이버 공격의 주요사례들이다.

- Stuxnet 공격: 2010년 상반기에 처음으로 확인된 이란 Natanz 소재 우라늄 농축시설에 대한 악성코드 공격. 이 공격으로 이란이 갖고 있는 원심분리기 5,000 개중 약 1,000 개 정도가 파괴되었고, 이란의 우라늄 농축 프로그램이 약 18개월에서 2년 정도 지연된 것으로 평가되고 있음. Stuxnet 공격은 미국과 이스라엘의 합동작전으로, 이로 인해 사이버 무기 사용에 대한 국제적 '금기'가 깨지게 되었다는 인식이 다수.

- Flame 공격: 2012년 5월 발견된 Flame 은, 소리, 화면, 키보드 동작, 네트워크 활동, 나아가 블루투스 설치되어 있는 컴퓨터의 경우 그 주변에 있는 블루투스 기기의 활동과 데이터까지도 탐지하는 종합적인 첩보 프로그램으로, 이 프로그램의 개발과 투입은 이란에 대한 미국과 이스라엘의 합동작전으로 알려져 있음.

- Shamoon 공격: 2012년 8월에는 사우디 아라비아의 국영석유회사 Aramco와 카타르의 RasGas에 대한 바이러스 공격이 발생하여 수만 대 컴퓨터의 데이터가 파기됨. 이란이나 이란의 비호를 받는 세력이 공격한 것으로 추정됨.

- 아울러 최근 들어서는 미국의 금융기관과 언론사, Google에 대한 중동발 사이버 공격도 증가하고 있음.

이제 사이버 공격은 통상적인 군사공격이나 테러공격과 함께 안정과 평화를 위협하는 새로운 변수로 부상하고 있다. 뿐만 아니라 사이버 무기는 그 특성상 사용이 특정 지역에 제한되지 않고, 대상에 있어서도 전후방의 구분이 없으며 군과 민간도 잘 구분하지 않는다. 더욱이 사이버 무기는

은밀하게 이전도 진행될 수 있기 때문에 다른 지역으로 확산될 가능성이 존재한다.

정책적 시사점

새로운 기술의 등장은 새로운 안보적 위협과 문제, 그리고 기회를 낳고 국제관계의 성격도 변화시킬 수 있다. 그러한 기술의 예로서, 핵미사일이나 인공위성, 최근에 들어서는 무인비행기 드론과 사이버 무기를 들 수 있다. 사이버 시대의 안보 위협에 대응하기 위해서는 효과적이고 안정적인 사이버 안보전략을 미리 수립해 놓을 필요가 있다. 그렇지만 새로운 기술이 주는 안보적 위협과 기회를 예측하기란 쉽지 않다는 데에 안보당국의 고민이 있다. 이러한 면에서 앞에서 살펴본 최근 사이버 공격의 사례들은 우리의 사이버 안보전략을 수립하는데 중요한 준거점이 될 것이다.

우리나라의 경우는 다른 나라보다도 정보통신기술에 대한 사회적, 경제적 의존도가 높아서 사이버 공격에 특별히 취약하다. 만약 일부의 견해처럼 북한과 이란 간에 군사협력이 존재한다고 한다면, 중동에서 발생한 사이버 공격이 한반도에서도 재연될 가능성을 배제할 수 없다. 따라서 사이버 안보전략의 수립이 그 어느 나라보다도 시급하다. 그렇기 때문에 앞으로 추진될 안보 제도와 조직의 편제 개편은 전통적 안보뿐만 아니라 사이버 안보도 증진하는 방향으로 이루어져야 할 것이다. 새로이 등장하는 안보 위협을 신속히 인식하고 선제적으로 대응하기 위해서는 안보를 담당하는 기구는 무엇보다도 “학습하는 조직(learning organization)“ 일 필요가 있다.

사이버 시대의 안보 위협과 기회에 대처해야 하는 것은 단지 우리나라의 과제만은 아니다. 대개의 나라들이 최근에야 사이버 안보에 관심을 기울이기 시작했으며, 국제적으로도 사이버 공간의 평화적 사용이나 사이버 분쟁의 평화적 해결 등에 관한 규범이 아직 발달하지 못한 상태이다. 우리나라는 2013년 제3차 사이버 스페이스 총회의 개최국으로서 사이버 공간에 관련된 국제적 규범을 창출하는 데 중요한 역할을 할 것으로 기대된다. 서울 사이버 스페이스 총회에서 참가국들이 사이버 공간에서 허용되는 정당방위는 무엇이고, 사이버 무기의 군축을 위한 원칙과 절차는 어떻게 되어야 하는지에 대해 견해를 교환하고 의견을 수렴할 수 있다면 우리의 안보증진뿐만 아니라 국제적 위상도 높아질 것이다.

** 보다 자세한 내용은 한인택, “최근 중동지역 사이버 공격의 사례와 함의,“ 주요국제문제분석 (2012-42), 국립외교원을 참고

2013.3.21