Jeju Peace Institute 제주평화연구원

JPI PeaceNet

사이버 안보 국제협력과 국가전략

김소정

ETRI 부설연구소

저자 現 ETRI 부설연구소 선임연구원. 고려대학교 정보보호대학원에서 공공영역에서 프라이버시 영향평가에 관한 연구로 박사학위를 취득.

지난 3월 20일 사이버테러 공격에 이어 6월 25일 한국이 또 다시 사이버 공격을 받았고, 이는 공격 주체가 국가인 사이버 안보 위기 발생 시 국제적으로 해결할 수 있는 체계가 없음을 재확인하는 계기가 되었다. 우리 정부는 지난 공격의 배후를 지목했으나, 공격행위에 대한 처벌이나 제재에 대해 논할 수 있는 국제적 논의의 장은 없었다. 또한 특정 국가가 공격을 주도했음을 입증하는 증거를 갖고 있더라도 규탄, 제재, 처벌 등이 불가능했기에 에스토니아 사태 이후 지속적으로 유사한 악의적 행위들이 반복되고 있다.

국제사회는 국가가 주도한 사이버 공격 행위를 어떻게 규제 및 저지할 것인지에 대한 국제적 규범을 자국에 유리한 방향으로 정립하고자 치열히 경쟁하고 있다. 그간 미국과 영국으로 대표되는 서방측과 중국과 러시아로 대표되는 非서방측은 인터넷 공간을 규율하는 규범 및 원칙 설립에 큰 이견을 보여 왔었다. 우선 서방측의 주장을 살펴보면 다음과 같다.

첫째, 사이버 공간과 인터넷 표현의 자유, 개방, 신뢰 등 기본 원칙이 존중되어야 한다. 둘째, 사이버 공간을 사용하고 있는 개인, 산업계, 시민사회 및 정부기관 등 다양한 구성원들의 의견이 수렴된 국제적 규범을 제정해야 한다. 셋째, 기존의 국제법이 인터넷 및 사이버 공간에도 그대로 적용되어야 하므로 유엔헌장 등이 사이버 공간을 규율하는 국제규범의 모태가 되어야 한다. 넷째, 상호간 사이버 공간상의 위협 요소 감축 및 신뢰 증진을 위한 사이버 공간에 적용 가능한 신뢰구축조치(CBMs: Confidence Building Measures)의 이행이 필요하다.

이러한 논의의 이면에는 중국 및 러시아 등이 언론의 자유 통제 등에 인터넷을 이용하는 등 국내 정치의 안전성 확보에 사이버 공간을 악용하지 못하도록 하겠다는 숨겨진 의도가 있다.

이에 대립하는 중국 및 러시아 등 非서방국가들의 주장은 다음과 같다.

첫째, 사이버 공간에서도 국가주권은 인정되며 필요시 정보통제가 가능한 공간이다. 둘째, 기존의 인터넷 체계를 구성하고 주도해 온 서방측의 의도대로 인터넷과 사이버 공간을 규율하는 체제를 수용할 수 없다. 셋째, 신뢰구축조치 발굴이나 이행보다는 국가의 인터넷 통제 강화 등을 내용으로 한 국제정보보안 행동수칙에 대한 합의가 시급하다. 즉, 사이버 공간에 대한 기존 서방측의 기득권을 어느 정도 제한하는 동시에 비서방국가들의 의도가 반영될 수 있는 사이버 공간상의 새로운 세계질서 구축을 원하고 있다.

하지만 최근에는 양측의 견해 차이에도 불구하고 안전하고 신뢰가능한 사이버 공간 질서확립이 더욱 중요하다는 기본원칙을 염두에 두고 상호간의 이견 차이를 좁히기 위한 적극적인 노력을 경주해왔다. 이에 주요국들은 사이버 안보 확립을 위한 협력을 양자 간 협력, 지역 안보기구를 통한 협력, 다자간 협력 등 3분야로 나누어 적극적으로 추진하고 있다.

첫째, 양자 간 협력체계 구축의 일환으로 미국은 러시아와 사이버 안보 확립을 위한 사이버 핫라인 개설 등을 협의한 사이버 안보 상호협정을 체결했으며, 일본과는 지난 5월 “미-일 사이버 안보 대화” 를 하고 “미-일 사이버 안보 대화에 따른 공동성명” 을 발표했다. 중국과는 시진핑 국가주석과 오바마 대통령간 정상회담 주요 주제로 사이버 안보가 다루어졌으며 최근 불거진 스노든 사태에도 불구하고 상호 지속적인 협력을 계속할 것으로 전해졌다. 이 외에도 미국은 영국, EU, 호주 등 주요 우방국들과도 양자 간 사이버 안보 협력체계를 구축했으며 영국도 일본과 사이버 안보 협력 체계 구축에 나서고 있다.

우방국들 간 양자 간 협력체계 구축으로 전세계 차원의 협력에 대비해 공통의 가치를 추구하는 국가의 수를 늘렸다. 또한 IT수준이 상대적으로 우수한 국가들인 주요 서방선진국들간 협력이 구체화됨으로써 IT인프라에 기반한 과학기술정책 추진 및 안보정책 추진에 있어 같은 목소리를 낼 수 있게 되었다.

이렇게 선진국들간 협력체계 우선 구축은 정보통신기술 의존도가 높은 저개발국가 및 개발도상국가들에게 큰 의미를 부여한다. 서방선진국들 대부분은 IT인프라 구축 및 인터넷 활용에 있어서 우수한 국가들이며 동시에 관련 기술, 제품 및 서비스 면에서도 최첨단의 국가들이다. 결국 이들 간 협력과 결속이 강화되면 향후 도래할 미래인터넷 서비스와 관련된 기술 및 정책이 이들에 의해 결정될 것이고 저개발국가 및 개발도상국가들의 발전은 IT 선진국들의 과학기술정책 및 전략에 구속적으로 의존할 수밖에 없게 된다.

특히 최근 G20 등 주요 국제회의마다 역량강화(CB: Capacity Building)를 모토로 저개발국가 및 개발도상국 IT수준 향상과 보안을 고려한 IT인프라 구축을 유도하고 있다는 점에서 그 의미가 더 커진다. 일각에서는 역량강화 노력이 겉으로는 저개발국가와 개발도상국을 지원하는 듯 보이나 결국 IT 강국들의 제품과 서비스, 정책과 법제도 등을 모두 일괄적으로 수출하기 위한 시장 확보의 일환이 아니냐는 부정적 시각도 있다.

두번째 형태의 협력은 지역안보기구를 통한 협력체계 구축이다. 유럽안보협력기구(OSCE: Organization for Security and Cooperation in Europe)와 아세안지역포럼(ARF: ASEAN Regional Forum)의 활동이 여기에 해당된다. OSCE는 사이버 안보 확립을 위한 신뢰구축조치 확보를 위해서 적극적으로 노력하고 있다. 물론 군축과 사이버 안보는 본질적인 측면에서 다르기 때문에 일방적인 군축 개념을 사이버 안보분야에 적용시키기 어렵다는 회의적인 시각도 존재한다. 특히 핵무기 등 전통적 안보개념에서는 억지력 확보 및 신뢰구축조치 향상으로 인한 예측성 강화가 결정적인 요소였으나 인터넷과 사이버 분야의 특성상 억지력 확보와 예측성 강화가 불가능할 것이라는 시각이다.

하지만 결국 사이버 안보 확보를 위해서도 국제적 수준의 안보차원에서 사이버를 활용한 안보위협에 대처하기 위해 일정 수준까지의 예측성 강화가 필요하며 이를 위한 신뢰구축조치 확보 및 투명성 확보가 필수적이라는 견해가 지배적이다. 이에 따라 최근 OSCE는 사이버 안보분야 CBMs 확보를 위한 작업반을 구축하여 연내 혹은 내년까지 구체적인 방안을 도출하고자 한다. OSCE가 유럽 중심의 활동이라면 ARF는 아태지역 중심으로 CBMs 확보를 위한 세미나를 개최하는 등의 활동을 펼쳐왔다.

세번째 형태의 협력은 정부 간 국제기구를 통한 협력체계 구축이다. 국제연합(UN) 군축 및 국제안보위원회(Disarmament and International Security Committee)의 활동이 여기에 해당한다. 동 위원회는 UN 총회의 6대 위원회 중 하나로 핵확산 방지 문제, 대량살상무기 문제, 우주공간 군축(disarmament of outer space) 문제 등을 다루면서 국제안보 및 평화 증진에 기여해 왔다.

군축 및 국제안보 위원회에서 사이버 안보가 본격적으로 다루어진 것은 1998년 러시아가 "Developments in the field of information and telecommunications in the context of international security" 라는 결의안을 UN에 제출하고 이를 총회에서 채택한 후이다. 동 결의안에 대해 미국은 처음부터 동조하지 않았고, 이후로도 소극적으로 사이버 안보 관련 국제협력에 대응해 왔다. 이후 동 위원회는 국제안보 차원에서의 사이버 안보 문제를 논의하기 위해 2004년부터 "국제안보 맥락에서의 IT 분야 개발에 관한 UN 정부전문가그룹(Group of Government Experts on Developments in the Field of Information and Telecommunications In the Context of International Security)" 회의를 지속해왔고 현재 3차 전문가그룹회의까지 진행되었다.

우리나라는 2004년 이후 지속적으로 GGE 활동에 참여해 왔다. 기존 회의에서는 인터넷의 국가통제를 강조하는 중국과 이에 반대하는 미국 간에 극명히 대립했었으나 지난 6월 개최된 회의에서는 러시아를 포함한 전체 참여국들이 온라인상에서도 기존의 국제법이 적용될 수 있다는 점에 합의하고 이러한 규범이 국가의 행위와 국가주도의 정보통신기술 사용에 어떻게 적용될 것인지에 대해서는 지속적으로 연구하기로 하였다. 또한 회원국들은 정보통신기술을 이용한 범죄 행위 및 테러행위를 근절하고 프록시를 이용한 악의적 행위에 자국 정보통신기술이 이용되지 않도록 주의를 기울이기로 했다. 동시에 민간영역과 시민사회도 정보통신기술의 적절한 사용과 보안 향상을 위해 적절할 역할을 수행해야 함을 인식하고 신뢰구축조치 확보 및 역량 강화를 위한 각국의 노력도 촉구했다.

상호간의 의견차이를 극복하고 기존의 국제법이 인터넷과 온라인에도 적용될 수 있는 근거를 마련한 최근 UN GGE 결과는 향후 구성될 인터넷의 미래와 사이버 안보 정책에 큰 영향력을 미칠 것으로 보인다.

올 10월 17~18일 한국에서 서울 사이버스페이스 총회(Seoul Conference on Cyberspace 2013)가 개최된다. 사이버스페이스 총회는 1차 런던(2011), 2차 부다페스트(2012)에 이은 제3차 회의로 사이버 공간상의 신뢰구축을 기반으로 글로벌 인터넷 경제의 지속적인 성장과 번영을 위하여 사이버 안보에 대한 국제적 협력을 논의하는 자리이다. 서울 총회에서는 △ 경제성장 및 복지, △ 사회문화적 혜택, △ 사이버 보안, △ 국제안보, △ 사이버 범죄, △ 역량개발 등 6개 분야에 대한 토론과 그 결과를 담은 결과문서가 발표될 것으로 알려져 있다.

6개 소의제 중 사이버 안보 관련 국외 동향 및 이에 대처하는 각국의 입장은 국제안보 분야에서 다루어질 것으로 기대된다. 국제안보분야 논의를 통해 각국은 UN GGE 회의결과를 반영한 새로운 사이버 공간 규범을 재구성하고 자국의 국가전략에 알맞은 형태의 사이버 공간을 구성하고자 최선을 다할 것이다.

이러한 국제안보 환경에 대해 우리나라는 사이버 안보 문제를 어떤 입장에서 이를 다루어야 할지에 대해 명확히 입장을 정리하지 못했다. 기존에 수립되었던 국가사이버 안보마스터플랜 및 테러 발생 시 수립된 종합대책은 국가차원의 사이버 안보전략으로 보기에는 어렵다. 향후 우리나라가 사이버 안보 확립을 통해 얻고자 하는 목표와 이를 어떻게 얻어갈 것인지, 국내 체계와 국제 협력 방향은 어떻게 될 것인지, 이를 위해 정부, 산업계, 국민은 어떤 역할을 해야 할 것인지 등에 대해 협의하고 방향을 제시할 수 있어야 할 것이다.

우리나라는 정보통신기술과 인터넷 경제의 발전 측면에서 선도국의 위상을 인정받고 있으며 IT 문제에 있어 상당한 경험과 노하우를 보유한 나라이다. 긍정적 영향력과 부정적 피해를 모두 크게 경험했기에 전세계 사이버 공간에 기반한 미래 구상에 핵심적 역할을 할 수 있을 것이다. 서울 사이버스페이스 총회를 계기로 우리의 위치를 확고히 자리매김하고 실질적 결과를 도출하고 해결이 가능한 방법론을 모색할 수 있기를 기대한다.

2013.7.24