국제협력을 통한 사이버안보 강화방안 연구

김소정* · 박상돈*

요 약

3.20, 6.25 등 사이버공격을 받은 우리 정부는 지난 공격의 배후를 지목했으나, 공격행위에 대한 처벌이나 제제에 대해 논할 수 있는 국제적 논의의 장은 없었다. 이렇게 특정 국가가 공격을 주도했음을 입증하는 증거를 갖고 있더라도 규탄, 제재, 처벌 등이 불가능했기에 에스토니아 사태 이후 지속적으로 유사한 악의적 행위들이 반복되고 있다.

현재 사이버안보에 관한 국제적 논의는 크게 국제적 수준, 지역적 수준 및 양자간 협력의 3계층으로 나뉘어 진행되고 있다. 이 중 국제적 사이버안보 규범 논의 방향 정립은 주로 국제연합과 세계 사이버스페이스 총회 2개 축으로 움직이고 있다. 물론 민간 중심의 인터넷 거버넌스 논의나 UN 전문기구인 국제전기통신연합 등에서도 사이버보안 이슈가 논의되고 있으나 본 논문에서는 2013년 주요 성과가 도출된 국제연합의 정부전문가그룹(GGE) 활동 결과와 우리 정부가 주최한 제3차 세계 사이버스페이스 총회의 사이버안보 논의 흐름을 분석하여 2014년부터 시작될 제4차 UN 전문가그룹(GGE)의 활동을 예상해보고 앞으로의 사이버안보 논의 방향을 짚어보고자 한다. 또한 이러한 논의들에 대한 국내 대응전략을 도출해보고자 한다.

A Study on Cybersecurity Policy in the Context of International Security

So Jeong Kim* · Sangdon Park*

ABSTRACT

Cyberspace, based on the dramatic development of information and communications technology, has brought enormous benefits to mankind. However, concerns over cyber terrorism and cyber attack are becoming serious. It is time to expand the global dialogue on international security issues in cyberspace. It is imperative to have a common understanding that cyberspace, the infrastructure for prosperity, should not be utilized as a space to create conflicts among states, and that all states agree to build confidence and peace in cyberspace. For this purpose, there are 3 tracks of international cooperations: 1)international cooperation such as UN and Conference on Cyberspace, 2)regional cooperations such as ARF and OSCE. 3)bilateral cooperations such US-Russia Cybersecurity Agreement, US-China presidential level dialogue. This paper will analyze the 1st track of international cooperations of UN and Conference on Cyberspace. With this, Korean government can prepare the forthcoming GGE activities and make our own strategy to deal with the global norms of good behaviour in cyberspace.

Key words : Cybersecurity strategy, UN GGE, Conference on Cyberspace, International Security, Capacity Building

접수일(2013년 11월 29일), 수정일(1차: 2013년 12월 12일), 게재확정일(2013년 12월 13일)

* 한국전자통신연구원 부설연구소

1. 서 론

3.20, 6.25 등 사이버공격을 받은 우리 나라는 대내적으로는 우수한 IT 인프라를 구축하고 세계 최고 수준의 IT 서비스 환경을 갖고 있기 때문에 사이버안보에 있어 상대적으로 공격받기 쉬우며, 피해발생시 영향력이 큰 국가임을 다시 한 번 보여주었다. 동시에 대외적으로는 공격 주체가 국가인 사이버안보 위기 발생시 국제적으로 해결할 수 있는 체계가 없음을 재확인하는 계기가 되었다. 특히 북한은 세계최고수준의 실력으로 사이버공격에 국가존망을 걸고 지속적으로 공격하고 있으나[1] 우리가 취할 수 있는 대응방법은 없었다.

우리 정부는 지난 공격의 배후를 지목했으나, 공격행위에 대한 처벌이나 제제에 대해 논할 수 있는 국제적 논의의 장은 없었다. 특정 국가가 공격을 주도했음을 입증하는 증거를 갖고 있더라도 규탄, 제재, 처벌 등이 불가능했기에 에스토니아 사태 이후 지속적으로 유사한 악의적 행위들이 반복되고 있다[2].

현재 사이버안보에 관한 국제적 논의는 크게 국제적 수준, 지역적 수준 및 양자간 협력의 3계층으로 나뉘어 진행되고 있다. 3계층으로 분류한 것은 해당 국제회의 및 논의의 참여주체가 대부분 국가이나, 참여국 수가 논의의 장에 따라 다르게 구성되며, 참여국 수 및 참여국 성격이 달라짐에 따라 논의 내용의 깊이 및 범위가 달라지기에 <표 1>과 같이 분류하였다.

<표 1> 계층별 사이버안보 논의 기구, 주체 및 주요내용

	기구	내용
국제	UN, 세계사이버스페이스 총회 등	국제안보, 사이버범죄, 역량강화, 사이버보안 등
지역	ARF, OSCE 등	사이버 신뢰구축조치
양자	미-러, 미-중 등	핫라인 개설, 실무작업반 구성 등

이 중 국제적 사이버안보 규범 논의 방향 정립은 주로 국제연합과 세계 사이버스페이스 총회 2개 축으로 움직이고 있다. 지역적 수준에서는 유럽안보협력기구(OSCE : Organization for Security and Cooperation in Europe)의 사이버공간 신뢰구축조치(CBMs: Confidence Building Measures) 확보 논의를 중심으로 이루어지고 있으며[3], 이에 대응하는 아태지역 안보기구인 아세안 지역포럼(ARF: ASEAN Regional Forum)이 사이버공간 신뢰구축방안에 관한 세미나를 개최하는 등 역할을 수행하고 있다[4]. 양자간 협력은 미국과 러시아, 미국과 중국간 협력이 있으며, 이들 국가외에도 다양한 국가들이 양자간 협력관계를 구축하고 있다[5][6].

물론 민간 중심의 인터넷 거버넌스 논의나 UN 전문기구인 국제전기통신연합 등에서도 사이버보안 이슈가 논의되고 있으나, 본 논문에서는 2013년 주요 성과가 도출된 국제연합의 정부전문가그룹(GGE) 활동 결과와 우리 정부가 주최한 제3차 세계 사이버스페이스 총회의 사이버안보 논의 흐름을 분석하여 2014년부터 시작될 제4차 UN 전문가그룹(GGE)의 활동을 예상해보고 앞으로의 사이버안보 논의 방향을 짚어보고자 한다. 또한 이러한 논의들에 대한 국내 대응전략을 도출해보고자 한다.

2. 국제연합에서의 사이버안보 논의

2.1 참여주체

국제연합(UN)의 논의에는 기본적으로 정부가 회원이므로 각국 정부 대표들이 참여하고 있다. 따라서 모든 의사 결정은 각 회원국이 1표씩을 갖는 1국1표 시스템으로 국제사회에서의 의제주도력과 패권적 영향이 투표결과에 반영되지 않는 구조이다. 또한 전세계적으로 선진국보다는 저개발국이나 개발도상국이 많기에 이들 국가간 이해관계는 다를 수 밖에 없어 특정 이슈에 대한 시각차가 크게 나타나고 있다.

이에 따라 미국 중심의 국가들은 인터넷과 사이버공간에 대한 규범 정립 논의에 UN이 적합지 않다고 주장하지만, 러시아와 중국 등 상하이협력기구 중심 국가들은 국제연합 및 그 전문기구인 국제전기통신연합(ITU)에서 사이버안보 관련한 논의가 국제안보의 맥락에서 지속되어야 한다고 주장하고 있다. 이에 ITU에서 관련 이슈를 논의하는

것에 대해 국가별 갈등이 있었고, 이것이 작년 두바이에서 개최되었던 WCIT 회의에서 드러나게 되었다. 작년 두바이에서 개최되었던 ITU-WCIT 회의는 ITU가 사이버안보 정책 문제를 다룰 수 있도록 전기통신규약을 개정하는 데에 대해 각국이 1표씩 투표권을 행사한 자리로 사이버보안 문제가 업무범위에 포함되었으나[7] 이에 따른 본격적인 논의가 진행되지 않았기에 본 논문에서 자세히 다루지는 않았다.

2.2 논의 경과

국제연합의 사이버안보 관련 논의는 정부간 국제기구를 통한 협력체계 구축 논의의 핵심으로 국제연합의 제1위원회(군축 및 국제안보위원회 : Disarmament and International Security Committee)의 활동이 해당한다. 동 위원회는 UN 총회의 6대 위원회 중 하나로 핵확산 방지 문제, 대량살상무기 문제, 우주공간 군축 문제 등을 다루면서 국제 안보 및 평화 증진에 기여해 왔다[8].

군축 및 국제안보 위원회에서 사이버안보가 본격적으로 다루어진 것은 1998년 러시아 외교장관이 1998년 9월 “Developments in the field of information and telecommunications in the context of international security”라는 결의안 초안을 UN에 제출하면서부터이다. 이는 러시아가 미국의 사이버안보 정책에 대해 양국간 협의를 지속적으로 추구했음에도 불구하고 이를 이루어내지 못하자 새로운 논의의 장으로써의 UN을 주목함으로써 시작된 것이다. 동 초안은 약간의 수정 후 총회에서 결의안으로 채택되었다[9].

러시아의 제안에 대해 미국 등 서방국가들과 상하이 협력 기구 국가들간 이견이 발생했었다. 이견은 주로 주제의 범위, 위협 인지에 대한 문제, 해당 이슈에 대한 UN의 역할 및 제1위원회의 역할 문제 등이었다[10]. 이는 결국 사이버안보 관련 논의의 장을 어디로 하느냐에 따라 결과가 달라질 수 있음을 염두에 둔 각국의 외교전략이 맞부딪친 결과라고 볼 수 있다.

이후 동 위원회는 국제안보 차원에서의 사이버안보 문제를 논의하기 위해 “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)”을 구성하고 관련 논의를 지속했다[8]. GGE는 제1차(2004-2005), 제2차(2009-2010)를 거쳐 올해 마무리된 제3차(2012-2013) 활동까지 진행되었다. 우리나라는 제1, 2차 GGE 활동에 참여했었다.

2.3 사이버안보에 대한 입장

사이버안보 논의 주도를 위해 국제사회는 국가가 주도한 사이버 공격 행위를 어떻게 규제 및 저지할 것인지에 대한 국제적 규범을 자국에 유리한 방향으로 정립하고자 치열히 경쟁해 왔다.

그간 미국과 영국 중심 국가들과 중국과 러시아 등 상하이 협력 기구측 국가들은 인터넷 공간을 규율하는 규범 및 원칙 설립에 큰 이견을 보였다. 미국은 2011년 발표한 사이버공간에 대한 국제전략(International Strategy for Cyberspace : Prosperity, Security, and Openness in a Networked World)에서 강조한 역량강화, 국가의 올바른 행동에 관한 국제 규범 마련 등을 추진하고 있다[11].

우선 미국 중심 국가들의 주장을 살펴보면 다음과 같다. 첫째, 사이버 공간과 인터넷 표현의 자유, 개방, 신뢰 등 기본 원칙이 존중되어야 한다. 둘째, 사이버공간을 사용하고 있는 개인, 산업계, 시민사회 및 정부기관 등 다양한 구성원들의 의견이 수렴된 국제적 규범을 제정해야 한다. 셋째, 기존의 국제법이 인터넷 및 사이버공간에도 그대로 적용되어야 하므로 유엔헌장 등이 사이버공간을 규율하는 국제규범의 모태가 되어야 한다. 넷째, 상호간 사이버공간상의 위협 요소 감축 및 신뢰 증진을 위한 사이버공간에 적용 가능한 신뢰구축조치(CBMs : Confidence Building Measures)의 이행이 필요하다. 이러한 논의의 이면에는 중국과 러시아 등이 언론의 자유 통제 등에 인터넷을 이용하는 등 국내 정치의 안전성 확보에 사이버공간을 악용하지 못하도록 하겠다는 숨겨진 의도가 있다[12].

이에 대립하는 중국 및 러시아 등 국가들의 주장은 다음과 같다. 첫째, 사이버공간에서도 국가주권은

인정되며 필요시 정보통제가 가능한 공간이다. 둘째, 기존의 인터넷 체계를 구성하고 주도해 온 서방측의 의도대로 인터넷과 사이버공간을 규율하는 체제를 수용할 수 없다. 셋째, 신뢰구축조치 발굴이나 이행보다는 국가의 인터넷 통제 강화 등을 내용으로 한 국제 정보보안 행동수칙에 대한 합의가 시급하다. 즉, 사이버공간에 대한 기존 서방측의 기득권을 어느 정도 제한하는 동시에 비서방국가들의 의도가 반영될 수 있는 사이버 공간의 새로운 세계질서 구축을 원하고 있다[12].

2.4 제3차 GGE 결과[13]

기존 회의에서는 인터넷의 국가통제를 강조하는 국가들과 이에 반대하는 국가들 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 한 보고서 작성에 합의했다. 또한 회원국들은 IT를 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. 3차 보고서의 주요 내용을 살펴보면 다음과 같다.

- o 국제 평화, 보안, 안정에 대한 위협을 완화하기 위해서는 기존 국제법을 토대로 국가의 ICT 사용 기준을 확립하는 것이 중요하다. 이들 기준을 국가 활동과 국가의 ICT 사용에 적용하는 방법에 대해 추가 연구가 필요하다.
- o 국제 평화와 안정성을 유지하고 개방적이고 안전하며 평화적이고 접근 가능한 ICT 환경을 장려하기 위해서는 국제법, 특히 UN 헌장을 적용하는 것이 매우 중요하다.
- o 국가의 ICT 관련 활동과 ICT 인프라가 구축된 관할권에는 국가 주권 및 주권에 대한 국제 기준과 원칙을 적용해야 한다.
- o 국가는 국제적 불법 행위와 관련되어 있는 경우 국제적 의무를 충실히 이행해야 하며, 대리인을 통해 국제적 불법 행위를 주도 또는 가담해서는 안 된다. 국가는 비국가 행위자가 자국 영토에서 불법으로 ICT를 사용하지 못하도록 조치해야 한다.
- o 국제 협력 관계를 강화하기 위해 국가 전략 및 정책, 모범 사례, 의사 결정 과정, 관련 국가 조직 및 정책 등을 토대로 정보와 의견 교환. 정보 교류 범위는 정보를 제공하는 국가에서 결정할 수 있으며 양자간, 지역 그룹, 기타 국제 포럼에서 이들 정보를 공유할 수도 있다.
- o 신뢰 구축을 위해 양자간, 지역적, 다자간 협의 프레임워크 구축. 워크숍, 세미나, 실습 등을 통해 국제적 수준에서 국가의 ICT 사용으로 인한 사고를 예방하고 이들 사고를 관리하는 방법 등을 논의할 수 있다.
- o ICT 또는 ICT에 기반한 산업 제어 시스템을 사용하는 주요 인프라에 영향을 미칠 수 있는 문제 해결을 위한 협력을 증진한다. 국가는 이를 위해 비국가 행위자의 파괴 활동에 대응하는 지침과 모범 사례를 공유할 수 있다.
- o 연구 기관 및 대학의 ICT 보안 연구를 장려하고 이들 연구 기관이 유엔 회원국과 국제 사회에 기여하는 정도를 고려하여 관련 유엔 연구 및 교육 기관이 ICT 보안 강화에 중요한 역할을 수행할 수 있도록 지원해야 한다.

2.5 향후 전망

제3차 UN GGE 활동은 상기 보고서의 도출 및 총회 보고로 마무리되었고, 이는 10여년이 넘게 지속되어온 주요국간 사이버공간을 규율할 수 있는 기본 방향에 합의했다는 점에서 큰 의의가 있다. 하지만 이를 어떻게 풀어갈 것인가에 대한 세부적 논의는 제4차 GGE 활동으로 넘기고 2014년부터 지속적으로 활동할 예정이다.

이에 우리나라도 상기 활동에 외교부를 중심으로 적극적으로 참여할 예정인 것으로 알고 있다. 하지만 사이버안보 확립을 위한 국제안보 논의는 단순한 기술적 보호정책 검토나 외교적 활동이 아닌 국가안보 차원에서 다루어져야 할 사항이므로 반드시 청와대를 포함, 국가안보기관과 공동으로 의제 분석, 주력 의제분야 설정을 통한 대응방침 마련이 선행되어야 할 것이다.

또한 UN 내 사이버안보 관련 이슈가 제1위원회 뿐 아니라 다른 분야에서도 논의되고 있으므로 이들 논의 현황에 대한 적절한 정보 공유 및 의견수렴을 통해 국가 차원의 총괄적 대응 방안을 마련해야 할 것이다.

3. 세계 사이버스페이스 총회

3.1 총회 배경 및 참여주체

지난 10월 한국 정부는 서울 세계 사이버스페이스 총회(Seoul Conference on Cyberspace 2013)를 개최하였다. 동 총회는 1차 런던(2011), 2차 부다페스트(2012)에 이은 3차 회의로 사이버 공간상의 신뢰구축을 기반으로 한 사이버안보에 대한 국제적 협력 방안을 논의했다[14].

세계사이버스페이스 총회는 자유로운 인터넷의 흐름을 강조하고 인터넷은 만인을 위한 평등하고 자유로운 정신을 가져야 하므로 이를 위해 사이버 공간을 사용하고 있는 개인, 산업계, 시민사회 및 정부기관 등 다양한 구성원들의 의견이 수렴된 국제적 규범을 제정해야 한다는 측면에서 다층적 행위자가 모두 의사결정과정에 참여해야 한다는 다중 이해관계자 모델(multi-stakeholder model)을 인터넷 및 사이버 공간을 규율하는 규범 제정에 있어 바람직한 모델로 설정하고 있다. 통칭 런던 프로세스(London Process)라 불리는 총회는 사이버공간에 대한 최소한의 공감대를 형성하기 위하여 정해진 회원국이 없이, 개최국이 중심이 되어 정부기관, 국제기구, NGO, 민간기업, 학계 등 다양한 이해관계자들을 초청, 사이버 분야에 대한 공감대 형성 및 원칙에 합의해가는 과정이다. 이에 따라 금번 총회에는 87개국 정부대표 및 주요 국제기구 대표, 지역협력기구 대표, 학계/연구계/산업계 및 시민사회 등 총 1,300여 명이 참석하였다[14].

3.2 의제

서울 총회의 대의제는 'Global Prosperity through an Open and Secure Cyberspace'이며 경제성장과 복지, 사회/문화적 혜택, 사이버보안, 국제안보, 사이버범죄, 역량개발 등 6개 분야에 대해 토론하였다.

국제안보분과는 이번 서울 총회의 핵심이었다고 할 수 있다. 2장에서 분석했던 제3차 UN GGE 결과보고서 작업 논의에 총 15개국이 참여한 데에 반해 총회에서는 87개 참여국 및 기타 산업계, 연구계, 학계, 시민사회 등 모든 참가자들이 사이버안보 논의에 참여하여 사이버공간에 대한 인식과 규제를 위한 규범의 틀 정립에 의견을 제시하였다.

국제연합에서와 마찬가지로 국제안보분과 의제 설정에 있어서는 주요 강대국을 중심으로 한 국가간 이견이 커 갈등의 소지가 많았었다. 이러한 첨예한 갈등 속에 국제안보분과 논의를 실질적으로 도출해내기 위해 우리나라는 한국, 영국, 헝가리, 미국 4개국이 참여한 사이버안보대화(비공개) 개최, 국제안보분과 사전워크숍 개최[15], ICT4Peace 재단의 사이버 CBMs 워크숍 참석[16], 경제협력개발기구(OECD: Organization for Economic Cooperation and Development) 및 유럽네트워크보안청 (ENISA: European Network and Information Security Agency)과의 의제 논의, 러시아, 중국, 일본 등 주요 국가들과의 협의 과정을 진행했다. 이러한 과정을 통해 사이버안보 중요성에 대한 공감대 형성, 사이버안보 논의 현황 정리, 국가 및 그 대리자 주도의 사이버공격에 대한 국제적 제재를 위한 규범 정립 필요성 논의, 향후 협력 방안 마련 등 총회 패널토의 주제를 도출했다.

3.3 총회 결과문서

이번 총회에서는 이전 총회와는 달리 의장성명서 및 요약문 외 부속문서로 "서울 프레임워크 및 공약"과 "최적관행"을 포함한 결과문서를 발표했다. 사실 기타 문건의 마련 및 발표에는 각국 이견이 없었으나 "서울 프레임워크 및 공약"의 작업 및 배포에 대해서는 각국의 이견이 첨예하게 대립되었었다. 원래 우리 정부는 총회 결과문서를 "서울선언문"으로 발표하고자 사전작업을 진행했으나 명칭에 대한 러시아 등 반발로 "서울 프레임워크 및 공약"의 이름으로 발표하게 되었다.

6월 말 GGE 보고서가 채택되기 전까지는 이러한 결과물이 도출되는 것이 불가능해 보였었으나 GGE

보고서 작성을 통해 미국과 러시아 등 주요국이 기존 국제법이 온라인에서도 적용된다는 큰 틀에 합의함으로써 온라인에서 다루어지는 사이버안보 관련 다양한 원칙들이 지지받고 있음을 공식화할 수 있게 되었다[1].

"서울 프레임워크 및 공약"은 6개 분야별 논의시 해당 논의에 참여하는 국가들이 기본 원칙으로 생각하는 내용을 집대성하여 하나의 문서로 만든 것으로, 향후 관련 국제회의에서 언급될 것이며 이는 우리나라가 사이버안보 관련 논의에서 주도권과 영향력을 미칠 수 있게 되었음을 의미한다. 주요내용은 다음과 같다[17].

- o **경제성장과 발전** : 인터넷 경제가 글로벌 경제 성장에 지속적으로 기여해온 바, 더 많은 사람들이 광대역 인터넷 통신망에 접근할 수 있도록 보장함으로써, 모든 국가들이 인터넷을 통해 세계 경제로 통합되고, 지속 가능한 발전과 기술 경쟁력 확보, 정보 접근권 보장, 빈곤 해소 등이 가능하도록 노력한다.
- o **사회•문화적 혜택** : 인터넷의 개방성을 확보하기 위해서는 표현의 자유가 온라인에서도 보호받아야 하며, 인터넷은 다자적이고 투명하며 민주적으로 관리되어야 한다.
- o **사이버보안** : 정보통신기술의 발전 및 의존성 증대에 따라 다양한 사이버 보안문제가 제기되고 있으므로, 안전하고 신뢰 가능한 사이버공간 구축을 위해 노력한다. 각국 및 국제기구가 수립한 사이버보안 전략의 공유와 기술적·관리적 대책 마련을 위한 민-관 협력, 그리고 최적 관행의 공유 등이 필요하다.
- o **국제안보** : UN헌장을 포함한 기존 국제법은 온라인에서도 적용된다. 앞으로는 이러한 국제법이 어떻게 사이버공간에 적용될 수 있을지에 대해 각국이 더 많은 노력을 기울여야 한다. 또한 주요정보통신기반시설(CII) 보호를 위해 각국이 지속적으로 노력한다. 국가가 국제적으로 잘못된 행동을 야기할 경우 해당 국가는 이에 대한 국제적 의무를 진다. 자발적인 신뢰구축조치(CBMs)는 예측 가능성 증대와 오해소지의 감소를 통해 갈등 유발 위험을 줄이는데 기여한다.
- o **사이버범죄** : 사이버범죄 해결을 위해서는 법집행기관 및 민간부문과의 협력이 필수적이다. 개인의 자유와 사생활을 보호하면서 사이버범죄 수사 및 기소에 협조하기 위하여 국가와 관련 기관, 민간기업, 시민사회 간의 협력을 강화하고, 사이버범죄 대응 기술지원과 역량강화를 위한 파트너쉽을 제고한다.
- o **역량강화** : 사이버보안 및 디지털 격차를 극복해야 궁극적으로 안전하고 신뢰가능한 사이버공간 확보가 가능함에 비추어, 각국은 ICT의 보편적 접근과 주요정보통신기반시설 보호를 위하여 최적의 사이버보안 기법 및 교육 훈련 분야와 관련된 정보통신기술을 전파하고 역량강화를 지원한다. 역량강화에는 정부와 기업, 시민사회의 전면적인 참여가 필요하다.

또 다른 부속문서인 "최적관행"은 참여국들의 총회 주제와 관련해 실시한 정책들 중 개도국 및 저개발국 정보화와 사이버안보 정책 수립 및 시행에 필요한 모범사례를 카탈로그 식으로 정리한 것으로 IT 저개발국 등이 참고자료로 활용할 수 있다. 특히 모범사례로 채택된 정책의 경우 전세계적 확산이 가능하며 이는 향후 시장개척 및 제품수출 등 산업화에도 기여할 수 있을 것으로 기대한다[18].

4. 결 론

국제연합에서의 사이버안보 논의와 세계 사이버스페이스 총회는 국제수준의 사이버안보를 논의하는 양대 산맥이다. 향후 우리나라가 상기 두 기구에서의 사이버안보 논의에 적극적으로 나서기 위해서는 다음과 같은 사항에 대해 고려해야 한다.

첫째, 사이버안보 논의를 주도하는 국가들의 입장에 대한 세밀한 분석에 기반한 사이버안보 정책 방향 설정 및 외교전략 마련이 필요하다. IT선진국인 미국은 1국1표를 행사할 수 있는 국제연합 체제보다는 세계사이버스페이스총회 체제에 더 적극적이다. 기존 국제연합의 의사결정 과정에서도 미국측 주장이 적극적 지지를 받아오지 못했다는 점과 인터넷 정책의 미국 중심성에 대한 타국의 반발을 고려했을 때 총회에 더 비중을 두고 있다. 그럼에도 불구하고 미국은 총회를 중심으로 한 런던 프로세스에서 주도적 역할을 수행할 수는 없기에 영국을 내세우고 숨어서 회의의 맥락을 주도하고자 하고 있다. 따라서 우리나라는 남북한 정전중인 상황에서 북한으로부터

1) 저자는 금번 총회 준비기획단 일원으로 결과물 작업에 직접 관여하였다.

지속적으로 공격받고 있는 현실을 감안하여 최상의 이익을 끌어낼 수 있는 중간자적 입장의 외교전략을 구사해야 할 것이다.

둘째, 첫 번째에서 고려한 대내외적 상황을 고려한 우리나라의 사이버안보 전략을 수립하고 이에 바탕한 정책을 펼쳐야 한다. 우리나라는 총회 개최를 통해 국제안보분과 논의 의제설정에서부터 토의 맥락 설정, 연사 및 토론자 선정 등에 깊이 관여했고 특히 의장요약문과 그 부속문서들을 도출해내는 성과를 보였다. 하지만 우리나라의 사이버안보 전략이 없는 상황에서 일관되고 체계적인 대응 논리나 외교 전략이 부재했으므로 이를 보완해야 할 것이다.

셋째, 사이버안보의 중요성과 필요성을 적극적으로 어필할 수 있는 사이버안보 전문가가 국제적 논의에 적극적으로 참여할 수 있도록 해야 한다. 국가중심의 UN GGE 활동에도 전문가를 포진시켜 전문가 의견이 반영될 수 있도록 하고, 산/학/연 및 시민사회 등 모든 사이버 공간상의 행위자가 참여할 수 있는 세계 사이버스페이스 총회에는 10월 총회를 위해 구축되었던 전문가 집단을 적극적으로 활용하여 의제 설정 과정에서 적극적으로 참여하고 논의를 주도할 수 있도록 해야 한다.

넷째, 국가 중심의 논의에서는 공식적인 정부입장을 언급함으로써 대화가 경직되거나 겉돌 수 있으므로 연구기관 등을 활용한 공동연구 프로젝트 발굴 및 추진을 통해 각국의 입장과 실질적 의사결정 체계 이해도 향상, 허심탄회한 의견교환의 장을 많이 마련할 필요가 있다. 이러한 논의들이 결국 정부기관의 의견수렴과정에 반영되어 국제사회에서의 논의시 핵심이 될 수 있기 때문이다.

다섯째, 이번 총회에서 새로운 의제로 추가되었던 역량강화(Capacity Building) 및 최적관행의 의미에 대해 되새겨볼 필요가 있다. 역량강화나 최적관행은 우리 정책, 법제도, 철학, 제품, 인력, 시장 등을 총체적으로 외국에 공개할 수 있는 좋은 계기가 될 수 있으므로 이에 대해 국가가 어떤 입장을 취할 것인지를 고민해 보아야 할 것이다.

여섯째, 국제적 사이버안보 규범 논의에서 민생과 직결되는 기반시설에 대한 사이버공격은 절대로 안된다는 합의가 이루어지려 하고 있으며 주요정보통신기반시설에 대한 보호의 중요성이 점점 더해지고 있다. 이는 연초에 오바마 대통령이 발표한 대통령 행정명령에서도 드러났다[19]. 우리나라와 같은 IT 선진국은 특히 정보통신기반시설에 대한 의존도가 높기에 이는 중요한 의미를 지닌다. 이러한 흐름속에서 우리나라 기반보호 정책과 국제적 논의의 궤를 어떻게 조율할 것인지에 대한 대내외적 정책 마련이 필요할 것이다.

마지막으로 우리가 흔히 말하는 민관협력모델이 향후 사이버안보 정책 논의의 기본이 된다는 점은 국가정책 수립에 큰 중요성을 갖는다. 우리나라는 2004년부터 국가정보보안연합회(NISA)를 운영하여 정부부처간 협의회, 공기업 협의회, 산/학/연 협의회 등 분야별 주요 정책 현안 논의에 기여해 왔다. 이러한 체계를 구축한 국가는 전세계적으로 많지 않으며, 각국 전략수립 시 새로운 대내적 협력모델로써 추진하고자 하는 주요 어젠다 중의 하나이다. 우리나라는 기 구축된 협력모델을 잘 활용하여 어떻게 선도적 역할을 수행할 수 있을 것인지에 대해 고민해 볼 필요가 있다.

내년부터 시작될 제4차 GGE활동, 2014년 ITU 전권회의, 차기 세계 사이버스페이스 총회 등 사이버안보는 이제부터 본격적으로 논의될 것이다. 우리나라는 정보통신기술과 인터넷 경제의 발전 측면에서 선도국의 위상을 인정받고 있는 나라이다. 긍정적 영향력과 부정적 피해를 모두 크게 경험했기에 전세계 인터넷에 기반한 미래 구상에 핵심적 역할을 수행할 수 있을 것이다. IT기술력을 바탕으로 주도적 사이버안보 정책과 사이버공간 규범 제정에 적극적인 역할을 수행할 수 있기를 기대한다.

참고문헌

[1] Richard A. Clarke and Robert Knake, Cyber War : The Next Threat to national Security and What to Do About It, Harper Collins, 2010.

[2] 한인택, “사이버 시대의 국가 안보”, 제주평화연구원, JPI PeaceNet 2013-04, 2013. 3.

[3] OSCE Decision No. 1039, “Development of Confidence-building Measures to reduce the risks of conflict stemming from the use of information and communication technologies, PC.DEC/1039, 2012. 4. 26.

[4] ARF, “Co-Chair’s Summary Report of the ARF Seminar on Confidence Building Measures in Cyberspace”, Seoul, Republic of Korea, 11-12 September 2012

[5] Karina G. Ibrahim, “From Arms Race to Cyber -Space: U.S.-Russian Relations and the Prospects of Cyber Warfare”, 2013. 7.

[6] http://www.reuters.com/article/2013/07/10/us-china-usa-cyber-idUSBRE96904820130710

[7] www.itu.int/en/wcit-12

[8] Enneken Tikk-Ringas, “Developments in the Field of Information and Telecommunications in the context of international security: Work of the UN first Committee, 1998-2012”, ICT for Peace Foundation, 2012.

[9] United Nations General Assembly, Resolution 53/70, "Developments in the field of information and telecommunications in the context of international security," A/RES/53/70, January 4, 1999

[10] Tim Maurer, “Cyber Norm Emergence at the United Nations - An Analysis of the Activities at the UN Regarding Cyber Security”, Harvard Kennedy School Belfer Center for Science and International Affairs, 2011. 9.

[11] 김소정, “오바마 정부의 사이버안보 정책 추진현황과 정책적 함의”, 외교안보연구 제7권 제2호, 2011.12.

[12] 김소정, 제주평화연구원 JPI Peace-Net 2003-17, “사이버안보 국제협력과 국가전략”, 2013. 7. 24.

[13] UN GGE Report, A/68/98, 2013.

[14] 서울 사이버스페이스 총회 홈페이지 http://www.seoulcyber2013.kr

[15] Preparatory Secretariat for Seoul conference on Cyberspace 2013, “Workshop Report : The Pre-workshop on International Security for Seoul Conference on Cyberspace 2013”, 2013. 7.

[16] Daniel Stauffacher, Camino Kavanagh, “Confidence Building Measures and International Cyber Security”, ICT4Peace Foundation, 2013. 7.

[17] Preparatory Secretariat for Seoul conference on Cyberspace 2013, “Seoul Framework for and Commitment to an Open and Secure Cyberspace”, 2013. 10.

[18] Preparatory Secretariat for Seoul conference on Cyberspace 2013, “Best Practices”, 2013. 10.

[19] White House, Presidential Policy Directive 21, “Critical Infrastructure Security and Resilience”, 2013. 2.

[저 자 소 개]

김 소 정 (So Jeong Kim)

1998년 8월 부산대학교 사학과(학사)
2001년 2월 경희대학교
평화복지대학원 동북아학(석사)
2006년 2월 고려대학교
정보보호대학원
정보보호정책학과(박사)
2004년 ~ 현재 한국전자통신연구원
부설연구소 정책연구실
선임연구원

email : sjkim@ensec.re.kr

박 상 돈 (Sangdon Park)

2002년 성균관대학교 법학과(학사)
2004년 성균관대학교 법학과(석사)
2010년 성균관대학교 법학과
박사과정 수료
2008년~ 현재 한국전자통신연구원
부설연구소 정책연구실
연구원

email : sdpark@ensec.re.kr