[세션5] (Youth) 사이버안보 관점에서 인터넷거버넌스의 발전방향

목차

서론

인터넷의 기술 표준인 주소자원 관리체제에 대한 논의에서 출발한 인터넷 거버넌스는 인터넷이 전 세계 네트워크의 표준이 되고, 나아가 인터넷에 기반한 초연결사회 시대에 접어들면서 사이버 공간에서 일어나는 활동 전반에 대한 넓은 의미의 거버넌스로서 기능한다. 한편 인터넷 이용자가 급증하고 그에 따라 인터넷에 대한 의존도 역시 증가하면서, 사이버 공격은 개인에서 범세계적 규모에 이르기까지 중대한 위협으로 다가오고 있다. 비단 지구 안의 일이 아니라, 우주 상공을 떠도는 인공위성을 대상으로 한 사이버 공격에 대해 우려의 목소리가 높아지면서 사이버안보는 전 우주적 차원의 문제로 거듭나고 있다. 흔히들 보안 기술 자체에 주목하지만, 단순한 최신 기술 확보만으로는 분명한 한계가 있다. 2022년의 대표적인 사이버 공격 사례, 즉 러-우 전쟁에서의 러시아의 사이버공격, 랩서스 그룹의 해킹, 콘티 랜섬웨어 등의 경우를 보면, 전에 본 적 없던 새로운 공격 수법이 아닌, 널리 알려진 취약점을 악용하는 경우가 많다. 따라서 진정한 사이버 안보의 실현은 법적, 제도적 기반이 뒷받침되어야만 가능하다

국제연합(UN)의 경우 기존의 안보리 내의 논의와 더불어 '사이버안보 관련 국제규범을 마련하기 위해 유엔 정보안보 정부전문가 그룹'(GGE)과 사이버/ICT 안보 개방형 작업반(OEWG)을 통해 관련 논의를 진행해오고 있으며, UN 이외에도 다양한 국제 협의체가 사이버 안보에 관해 논의하고 협력하고 있다.

제 1장 한국 사이버안보 현황

우리나라 경우는 어떠한가? 우수한 ICT 인프라 환경을 구축한 것이 특징이다. 한국의 인터넷 이용률은 97.6%, 인터넷 접속 가구 비율 또한 99.9%로 OECD국가 중에서도 인터넷 접속성이 높은 국가이다.

또한 세계적으로 뛰어난 전자정부를 보유하고 있다. 한국은 2002년 11월 전자민원 단일 창구(G4C)를 개통하고,「전자정부법」시행과 함께 전자정부 구축을 본격적으로 추진한 결과, 유엔 전자정부 발전지수에서 3회 연속 1위를 기록하였으며, 2022년에는 온라인 참여지수 3위, 네트워크 준비지수 9위를 차지하는 등 편리하고 선진적인 전자정부 서비스를 제공하고 있다. 지난 2022년 5월에는 정부에서 모든 데이터가 연결되는 '디지털플랫폼정부'추진 계획을 발표했는데, 이는 단일 플랫폼 내 모든 데이터, 즉 공공행정 정보, 국민 개인정보 등의 통합이 본격적으로 이루어질 것을 의미한다. 한편으로, 이를 악용하여 고부가가치 데이터를 탈취하려는 해킹조직들이 한국을 주요 공격 대상으로 삼을 가능성이 높다.

한반도의 정치적 긴장 상황 역시 중요하다 . 최근 미국·중국, 러시아·우크라이나 등 국가 간 갈등과 분쟁이 심화되면서 국가 배후 해킹 조직의 활동이 증가하고 있으나, 한국의 경우 휴전 상황까지 고려해야 한다. 북한의 사이버 전력은 세계적인 수준으로, 김수키, 라자루스 등의 강력한 해킹 그룹을 보유하고 있다. 특히 휴전 대상인 한국에 집중적인 공격이 이루어지고 있는데, 2018~2022년 방위 산업 기술 연구·개발·생산과 관련된 국방과학기술연구소와 방위산업청을 대상으로 한 북한의 해킹 시도만 3만 건 이상이며, 북한은 해킹으로 첩보를 수집하고 가상 자산을 탈취하는 형식의 사이버 범죄를 자행하고 있다. 이때 빼앗은 자산은 북한의 스파이 활동 지원금이나 ICBM, 수중 핵 어뢰 등의 무기 제작 비용에 투입된다. 해킹으로 확보한 자산이 무기 제작에 사용된다는 점에서 한국의 국가 안보에 실질적인 위협이 될 수 있다.

제 2장 부다페스트 협약 및 해외 비준 사례

부다페스트 협약은 인터넷을 이용한 모든 범죄행위에 대한 상세한 규정을 두고, 이를 처벌하도록 한 최초의 국제조약이다. 2001년 헝가리 부다페스트에서 열린 사이버 범죄 회의에서 정식 발효되었다. 각국의 법집행기관들에게 사이버범죄를 수사할 수 있는 가이드라인을 제시하고 있으며, 각국의 법률과 상충되는 문제를 유연하게 표현하여 법률 개정에 있어 편리함을 보장하는 국제규범이다. 또한 국제적 수준의 효과적인 민관 협력을 촉진하는 협약으로써 위치하고 있다.

2023년 5월 기준 비준한 국가는 총 68개국이며, 비유럽 국가의 경우 미국과 일본을 비롯해 21개국에 달한다. 2001년이후 디지털화가 가속되고 새로운 IT환경에서의 사이버 보안 조약이 필요해지면서, 2003년 더 발전된 내용의 제 1 추가 의정서가 만들어졌다.

2022년에 발효된 제2 추가의정서의 가장 큰 특징은 '전자 증거의 협력 및 공개 강화'와 '가입국 간 더욱 신속한 수사 공조 체제 조성'이다. 아래의 3가지 조항이 이와 같은 특징을 잘 보여준다.

제 6조 : 도메인 이름 등록 정보를 얻기 위해 다른 관할권의 등록 기관에 직접 요청

제 7조 : 가입자 정보를 얻기 위해 다른 관할 지역의 서비스 제공업체와 직접 협력

제 8조 : 정부 간 협력을 통해 가입자 정보 및 트래픽 데이터를 보다 효과적으로 얻을 수 있는 수단

제 7조와 8조의 경우 둘 모두 타국에 위치한 전자 증거 제공에 관한 조항이라는 점에서 같지만, 제 7조는 가입자 정보만을 인터넷 서비스 제공자에게 직접 요청할 수 있고, 제 8조는 제7조와는 달리 서비스 제공자에게 직접 요청을 하는 것이 아니라 타국 정부를 상대로 요청을 하게 되며, 대신 가입자 정보와 함께 트래픽 데이터까지 요구할 수 있도록 한다.

사이버 범죄 수사와 관련하여 다음과 같은 부다페스트협약 비준의 성공 사례가 있다.

1. 일본 : 2018년 발생한 크립토재킹 범죄. 용의자들이 검거된 이후 검찰은 즉시 압수수색을 통해 압수한 컴퓨터에서 증거를 확보했다. 이렇게 압수수색이 바로 이뤄질 수 있었던 이유는 일본이 부다페스트 협약에 가입하기 위해 부다페스트 협약 제3조, 무단 컴퓨터 엑세스 행위에 대한 조항을 위해, 가입을 준비했던 당시 형법과 컴퓨터 무단접근 금지법을 개정했기 때문이다.

2. 스리랑카 부활절 폭탄테러 : 2019년 4월 21일, 스리랑카의 최대 도시 콜롬보를 비롯한 전국 8곳에서 동시 다발적으로 폭탄 테러가 발생. 이 사건은 국가 비상상황으로서, 범죄 해결을 위해 범죄자들의 연락 수단, 범죄 방법 등 증거가 필요했고, 해외에 데이터가 저장된 서비스 제공 업체로부터 전자 증거의 수집이 필요했다 이를 해결하기 위해 협약에 가입한 여러 국가로부터 즉각적인 국제 지원을 받았으며, 계정 세부 정보, 대화 내용 등을 포함한 전자 증거를 성공적으로 수집했다.

제 3장 한국 부다페스트 협약 비준의 필요성

한국은 2022년 10월 유럽평의회에 협약 가입의향서를 제출했다. 가입의향서를 제출할 경우 5년간 관찰국으로 지정되고, 5년동안 사이버 안보 관련 성과를 보이지 못한다면 협약을 비준할 수 없다. 따라서 작년에 가입의향서를 제출한 것은 협약 비준 과정의 시작 단계에 불과하다. 이런 상황 속에서 미국소비자협회(CTA)는 한국에게 보안 분야 F등급을 부여했는데, 이유는 부다페스트 협약 미가입으로 확인되었다.

우리나라가 부다페스트 협약을 가입해야 하는 이유는 다음과 같다.

1. 부다페스트 협약 가입이 되면 가입된 국가들간의 핫라인이 설치되어 공동으로 대처할 수 있다. 협약에 가입하지 않을 경우 회원국들만의 핫라인 사용을 못하는 것은 물론이고 필요한 사이버범죄 관련 정보 공유도 할 수 없어서 국제 공조의 한계에 부딪힐 수 있다. 지난 달 한국은 유엔 회원국 192개국 중 180개국의 지지를 얻어 유엔 안전보장이사회(안보리) 비상임이사국으로 선출되었다. 이렇게 국제 사회에서 안보 분야의 영향력을 키워나가고 있는 한국이 사이버범죄 협약 핫라인을 사용할 수 없는 것은 다소 모순된 상황으로 보인다.

2. 사이버 공간의 주도권을 얻기 위해 각국이 치열하게 경쟁하고 있는 상황에서, 한국이 사이버안보 강국으로 거듭나기 위해서 부다페스트 협약이 효과적인 동시에 필수적인 전략이다. 한국은 현재 유엔 안보리 비상임이사국으로 선출되었고, 아시아지역포럼(ARF)와 같은 부다페스트협약과 유사한 역할을 수행하는 국제기구를 통해 사이버 안보 협약에 참여하고 있다. 또한 작년 5월에는 아시아 국가 중 최초로 NATO 사이버방위센터에 정식 가입하는 등 국제사회에서의 사이버 안보 분야에서 입지를 키워가고 있기 때문에 부다페스트 협약 가입 필요성에 대한 회의적인 의견도 있다. 그러나 사이버범죄가 날로 진화하고 그 기술력이 발전하는 상황에서 향후의 범세계적 범위의 사이버범죄의 예방과 방지를 위해서는 현재 국제 사이버범죄에 대하여 가장 강력하게 합의된 대응책으로 평가되는 부다페스트 협약에 정식으로 가입하여 사이버안보에서의 한국의 주도적 위치를 굳건히 해야 한다.

게다가 부다페스트협약에 의거한 사이버범죄에 대한 국제 공조를 통해 한국이 이미 속해 있는 조약이나 사이버안보 조직의 긍정적 효과를 높일 수 있고, 비준 준비 과정에서 법적 개편과 사이버 수사 과정 개편이 국제 표준에 부합하는 사이버안보 체계 구축의 계기가 된다는 점에서 가입의 가치는 충분하다고 볼 수 있다.

제 4장 비준을 위한 사이버 수사 절차 개편 논의

원격 또는 역외 압수 수색은 실무상으로 필요성이 인정됨에도 불구하고, 이를 허용하는 명시적인 규정이 없어 합헌성 논란을 초래할 수 있다. 따라서 다음과 같은 대책이 필요하다.

역외 압수 수색의 경우 부다페스트 협약 가입국은 인터넷 서비스 제공자인 ISP를 통해 자

료를 확보하거나, 원격정보를 통해서 자료를 확보한다. 하지만 한국의 경우 ISP를 통한 자

료 확보가 불가능하다. 또한 영장 발부와 관련된 어려움도 있다. 일례로, 수사기관이

적법한 절차로 취득한 정보를 이용해서 영장을 발부받아 해외서버에 접속하였으나

서울고등법원은 이 사안에 대해 해외 ISP에 영장을 제시하지 않았기 때문에 해당 절차가 위

법하고 증거능력이 없다고 판시했다.

원격 및 역외 압수수색에 대해서 해외 이메일과 관련해서 대법원의 판단이 엇갈리기도 합니다. 이메일 서비스 관리자의 협조나 참여가 필요하지 않고 국제법상 관할권의 문제를 야기하는 것이 아니라서 사법 공조를 거칠 필요가 없다는 판례와, 압수수색 시 영장에 내용을 정확히 기재해야 한다는 판례가 존재하는 등 판례가 엇갈리고 있다.

도감청 관련해서도 한계가 있는 상황이다. 국내외 모두 범죄 수사나 안보를 목적으로 전기통신

사업자들에 정보를 요청하거나 영장발부에 따른 감청이 허용되고 있다. 영장 발부를 받아야 해서 신속성이 매우 떨어진다. 따라서 이와 관련한 법적인 부분의 보완이 필요하다.

제 5장 비준을 위한 국내 입법 논의

1. 부다페스트협약의 제2추가의정서의 6조에 따라 통신비밀보호법 도메인을 개정하는 내용

부다페스트협약 제2추가의정서의 6조는 도메인 이름 등록 정보를 얻기 위한 직접 요청을 규정하고 있다. 이에 따른 수사공조 효력으로, 사이버범죄를 수사할 때 다른 관할권의 등록 기관에서 도메인 정보를 제공받아 수사할 수 있다.

현재 빈번히 발생하는 사이버범죄 유형인 해킹, 랜섬웨어, 사이버 성범죄, 포르노 유포 등은 대부분 사이버국제수사의 취약점을 이용해 제3국에 서버를 두고 여러 나라를 경유하여 최초 공격지의 확인을 어렵게 한다. 현재의 수사법은 도메인 정보 외의 자료만을 요청해서 수사를 진행했으나, 각 해외 사이트의 도메인 정보를 당사국으로부터 직접 공조받아 수사를 진행한다면 도메인 등록자의 개인정보를 직접 수집해 수사 대상을 특정할 수 있고 이는 국경을 초월한 사이버범죄 수사를 원활하게 하며,현재 제한적인 수사상태를 극복할 수 있다.

부다페스트협약 제2추가의정서 6조에서 규정하고 있는 바와 현재 국내법 중 통신비밀보호법과 도메인 이름 관리준칙의 부합여부를 분석했을 때, 통신비밀보호법 제5조 범죄수사를 위한 통신제한조치의 허가요건에 관한 법률에서 검토가 필요하다. 현재 통신 허가 범위는 국가보안법, 군사기밀에 한해 제한되어 있으나, 협약에 부합하기 위해선 앞서 말한 해킹, 랜섬웨어, 포르노 유포 등 사이버범죄 수사공조에 적극적으로 활용될 수 있는 분야를 추가하여 확대할 필요가 있다. 동시에 도메인이름 관리준칙 제5장 25조에서 규정되어 있는 허용범위 또한 협약에서 규정한 범주에 포함되지 않아 이행입법이 필요하다.

1. 협약 제 19조 (저장된 컴퓨터 데이터의 수색과 압수) 제2항 원격수색의 허용 필요성

부다페스트협약 제 19조 제2항은 압수수색 대상자의 컴퓨터에서 정보통신망으로 연결되어 있는 다른 컴퓨터 시스템에 접속하는 원격수색에 대해 규정하고 있다. 이 조항의 효력으로 가입당사국들은 클라우드 서비스나 웹 하드등의 데이터에 대하여 각 국가간 원격수색이 가능하다.

하지만 국내법은 이와 관련하여 원격수색을 허용하는 현행법이 없습니다. 전통적인 압수수색에서 정립되어 있는 압수수색 장소의 특정성 뿐, 사이버 범죄에서 인터넷 시스템을 이용한 데이터에 대한 접근 권한 유무는 정립되어 있지 않다. 따라서 원격수색과 데이터 접근 권한 여부를 결

정하는 국내법의 입법을 상세히 검토하여 진행해야 한다.

도감청 수사의 경우 미국이 '감청통신지원법'을 통해 통신사업자와 협조하여 체계적인 수사를 진행하는 반면, 현재 국내는 데이터에 암호화 기술이 적용되어 실시간 감청이 불가능하며, 원격 압수수색이 규정되어 있지 않아 자료 요청에도 강제적 의무가 없기 때문에 요구에 대부분 불응하는 등, 범죄 수사에 어려움을 겪고 있다. 따라서 국내법의 데이터 원격수색 허용 범위와 행정 절차를 새로 정립하고, 더 개방적으로 부다페스트협약에 비준해야 한다.

결론

인터넷은 자유의 가치를 실현할 수 있는 공간이기도 하지만 때로는 갈등과 범죄의 온상이 되기도 한다. 인터넷이라는 공유재를 적절하게 관리하고 보호하기 위해서는 사이버안보에 대한 논의 및 발전이 필수적이다. 흔히들 '안보'라는 용어를 흔히 물리적인 안보의 의미와 사이버안보의 의미로 혼용하여 쓰곤 한다. 그러나 이 두 가지의 안보는 정치적 관점에서 그 궤를 달리한다. 물리적인, 혹은 전통적인 안보는 소수의 권력층이 결정권을 가지고 있고, 만약 그로 인한 피해가 발생할 경우 결정권이 없는 대다수가 피해를 입는 경향이 있다. 한편 사이버안보의 경우 인터넷 이용자 모두의 참여가 필수적인 동시에 안보의 성공 여부를 좌우한다. 이는 인터넷 거버넌스의 핵심 논제라고 할 수 있는 다중이해당사자주의(multistakeholderism)에 부합한다. 또한 직접 민주주의의 특성도 가지고 있다. 현재 많은 국가들이 민주주의를 표방하고 있고, 또 그들 중 대다수는 대의(**代議)** 민주주의를 채택했다. 소수가 다수를 대표한다는 점에서 대의 민주주의의 한계가 분명히 존재하지만, 오히려 인터넷이 만든 사이버 공간 상에서 이상에 가까운 민주주의가 실현될 수 있다. 사이버 세계가 오히려 현실 세계의 민주주의를 발전된 방향으로 견인할 수 있는 것이다. 한국은 민주주의 후발국이지만, 동시에 기존과는 다른 선진적인 민주주의를 실현하고 있는 나라이기도 하다. 그렇기에 한국은 인터넷 상에서의 민주주의 실현의 가능성에 누구보다 먼저 주목하고 논의해야 한다. 물론 이 모든 것들에 앞서서 제도적 규범적 기반이 중요하며, 그렇기에 한국이 사이버안보 분야에서 가장 시급히 해결해야 할 국제공조의 문제를 부다페스트 협약 비준과 관련하여 다루었다. 한국보다 앞서 부다페스트협약을 비준한 일본과 스리랑카의 경우 비준을 위한 준비에만 7년 이상의 시간이 걸렸고, 한국은 작년에 가입의향서를 제출했기 때문에 비준까지 채 5년이 남지 않았습니다. 그러나 당국이 사안의 중요성을 인식하고, 사이버 수사절차개편, 입법과 같은 제도적 개선, 그리고 이미 보유하고 있는 뛰어난 정보보안 기술을 충분히 활용한다면 부다페스트 협약 비준을 성공적으로 이끌 수 있다.