EU-한국 사이버 협의

사이버공간에서의 회복력과 신뢰

개요

사이버 보안은 COVID-19 대유행으로 인한 경제적, 정치적, 사회적 파장을 성공적으로 관리하는 핵심요소가 되었다. 유럽연합(EU)과 한국은 사이버보안 회복력을 높이고 국제공조를 강화함으로써 즉각적이고 중장기적인 사이버 안보 문제를 해결해야 할 필요성을 인식하였다. 기존의 제도적 환경에서 사이버공간의 회복력과 신뢰도를 높이기 위한 목표를 달성하기 위해 EU 사이버 다이렉트(Cyber Direct) 프로젝트와 국가보안기술연구소(NSR)는 2020년 10월 6일부터 7일까지 1.5트랙으로 구성된 "EU-한국 사이버 협의: 사이버공간에서의 회복력과 신뢰(EU-ROK Cyber Consultations: Resilience and Trust in Cyberspace)" 회의를 개최하게 되었다.

이번 협의는 EU와 EU 회원국 기관, 한국 정부와 관계기관의 고위관료를 포함한 유럽과 한국의 비정부기관 전문가들이 참여함으로써 다양한 이해당사자 간 가교 역할 뿐 아니라 정부 주도의 사이버 규범 구축 절차에 비정부기관의 입장을 반영하는데 도움이 되었다. 본 협의에서는 1) 사이버 회복력과 주요기반시설의 보호, 2) 사이버 분쟁 예방 및 신뢰구축 방안(CBM), 3) 5G의 지정학, 4) 사이버 범죄와 관련된 문제에 대해 의견을 교환하고 공통의 이해를 공유하기 위한 사항들을 비공개적으로 논의하였다.

1. 사이버 회복력

- 참석자들은 EU와 한국의 주요 기반시설(CI) 보호에 관한 모범 사례를 교환하였다. 한국은 2014년 원자력 발전소를 대상으로 한 사이버 공격을 기점으로 회복력 보다는 복구에 초점을 둔 사이버보안 정책을 추진 중이었으며, 회복력의 개념을

포함할 수 있는 사이버보안 정책을 개발·이행하기 위해 노력 중이다. EU에서는 현재의 네트워크 및 정보 보안(NIS) 지침과 사이버 보안 전략을 모두 검토하여 CI 보호를 위한 새로운 우선순위를 반영하였다. 참석자들은 양측이 기본권을 포함한 회복력의 이익과 비용을 신중하게 측정할 수 있는 위험관리, 전략적 파트너십 및 글로벌 공통 재화의 제공을 균형 있게 혼합하여 개발할 필요가 있다고 제안하였다.

- 금융분야에서의 위험과 취약성은 특히 높은 것으로 평가되었으며, 이를 통해 EU와 한국 양측은 해당분야에서의 회복력 강화 대책의 우선순위가 높게 지목되었다. 또한 참석자들은 글로벌 헬스 부문의 회복력 강화를 위한 긴급성과 병행적 노력이 필요하다는 점에 주목하였다.

- 양측은 CI 보호에 관한 보다 글로벌한 접근방식의 필요성을 인식하고 리스크 관리와 관련된 정보공유의 확대(예: 측정기준의 표준화), 합동 비상대응훈련(TTX) 및 시나리오 기획, 공동 연구 프로젝트에 대한 투자 등 EU-한국 간 협력 증대를 위한 다양한 논의가 이루어졌다.

- 또한 CI에 대한 협력은 유사 입장국가에만 국한되어서는 안 되며, EU 회원국들이 9월 말 UN 안전보장이사회에서 '주요 기반시설에 대한 사이버 공격'에 관한 아리아-포뮬라(Arria Formula) 회의를 개최했다는 점에 대해 언급하였다.

- EU와 한국은 COVID-19의 확산 속에서, 사이버 회복력에 대한 글로벌 협력이 필요하다는 상위 관점의 정치적 인식을 활용하여 CI를 보호하기 위한 노력을 두 배 가까이 줄일 수 있을 것이다.

2. 사이버 갈등 예방

- 사이버 분쟁 예방과 관련하여 국제법의 적용가능성, 책임 있는 국가의 행동규범 및 CBM의 이행에 중점을 두어야 한다는 필요성에 대해 양측 간 의견수렴이 이루어졌다. 참가자들은 사이버 위기상황에 필요한 직접 통신수단인 2020년 “빨간 전화(red telephone)”의 필요성을 논의하였다.

- EU가 지난 7월 처음으로 사이버 제재를 가한 반면, 동북아시아 환경에서는 한국과 북한, 중국 간의 지속적이고 비대칭적 경쟁 등으로 사이버 제재와 공개적인 귀속 수준이 "고위험"으로 인식되고 있었다. 한국 측 연사는 "특정 대상 지목 및 비난(naming and shaming)"이 가져오는 잠재적인 역효과에 대해 경고하고, CBM을 포함한 제약 없는 외교적 도구를 더욱 발전시킬 것을 제안하였다.

- 참석자들은 CBM의 효과적인 이행을 위한 전제조건으로 사이버 역량 구축의 필요성을 강조하였는데, 이는 국가 우선순위와 체계에 대한 정보 공유를 위한 국가 사이버보안 입법 및 전략의 개발; 국제 파트너와의 대화를 촉진하기 위한 국가 차원의 공통된 사이버보안 전문용어의 홍보, 공공-민간 및 다수이해당사자간 파트너십의 필요성 등을 포함하고 있다.

- 향후 EU-한국 간 협력은 OEWG(Open-Ended Working Group)를 통해 보다 밀접하게 이루어질 수 있으며, ARF, OSCE 등 지역 협의체를 통한 일관성 있는 CBM 개발 및 구현 노력을 수행하고, 기존의 협력 기반인 EU와 한국의 GCCD(Global Cybersecurity Center for Development), CAMP(Cybersecurity Alliance for Mutual Progress)를 통해 분쟁 확대 방지를 목표로 하는 사이버 역량 구축 협력을 강화할 수 있다는 의견이 제시되었다.

3. 5G의 지정학

- EU와 한국은 모두 국가의 전략적 자율성을 수립하면서 무역과 위험관리의 원칙을 조화시키려고 한다. 브뤼셀은 2019년 3월 발표된 연합 EU 접근법에 대한 권고안을 이행하고 있으며, 그 프로세스의 첫 단계로 5G 네트워크의 사이버보안에 대한 위험평가 조정안과 위험 완화를 위한 툴박스를 공표한 가운데, 한국은 새로운 5G 시스템에 사용될 기술에 대한 결정을 네트워크 사업자에게 위임하였다. 이와 관련하여 참석자들은 특히 한국의 경제가 중국의 경제 보복에 취약할 것이라는 점을 강조하였다.

- 2020년 1월 EU가 5G 위험 완화 조치를 위한 툴박스를 채택한 것은 회원국 간

조정이 이루어진 독특한 사례였지만, 2020년 7월 발표된 EU 집행위원회 보고서는 EU가 이와 관련한 노력을 두 배로 줄일 필요가 있음을 명시하였다.

- 참석자들은 ICT 제품 인증제도에 관한 정보 공유가 확대되어야 한다고 강조하였다.
- 양측은 상호간의 기술 협력이 강화되어야함을 강조하면서, 관련 문제를 논의할 수 있는 기술 및 정치 전문가가 참여하는 다원적 플랫폼을 제안하였다. 한국은 AI와 6G 네트워크 등 신흥 기술분야의 선도국가로서 해당 분야에서 EU와의 협력을 지속적으로 강화해나갈 것이다.

4. 사이버 범죄

- 한국이 2019년에 부다페스트 협약에 가입하기로 한 가운데, 관련된 구체적인 요구사항들을 국내법에 적용하는데 있어 우려사항들은 여전히 존재하고 있다. 참석자들은 증거의 보관, 암호화된 통신 접근, 증거 요청에 대한 대응능력 등 협약에 참여하기 위한 전제조건들을 충족하기 위해 한국에서 진행 중인 다각적인 노력들을 간략하게 설명하였으며, 이는 독일, 프랑스, 스페인 등 EU 회원국의 입법 사례와 추가적인 비교 분석을 실시함으로써 보다 효과적인 진행이 가능할 것이라고 논의하였다.
- 초국경적 데이터 접근 이슈는 양측 모두 의견교환이 이루어져야 할 우선순위이자 더 많은 투자가 이루어져야할 사항이다.
- “No More Ransom”, “Safer Internet Day”, 한-유럽 평의회 대화와 같은 기존의 이니셔티브를 바탕으로 향후 협력이 이루어질 수 있다는 의견이 제시되었다. 미래의 협력은 유엔 총회 제3위원회에서 진행 중인 인권과 시민자유 보호에 관한 협상에서 강력한 입장을 견지하기 위한 유사 입장 국가들 간의 외교관 및 법 집행기관들을 한데 모으는데 초점을 맞출 수 있을 것이며; UN 협상 및 UN 마약범죄사무소(UNODC)를 통한 사이버범죄 역량 구축을 위한 공통된 접근방법의 개발; (유로폴과의) 공동 프로젝트와 수사팀 등 운영 협력 등을 통해 이루어질 수 있다.

- 참석자들은 코로나19 팬데믹이 사이버범죄 협력에 있어 데이터 보호와 프라이버시 관련 논의가 배제될 수 없음을 강조하게 되었다고 언급하였다. 한국이 팬데믹을 완화하기 위한 감시 기술을 사용하는 것과 관련하여 그 적절성에 대한 논의는 이러한 사안을 더욱 복잡하게 만들 수 있으며, 유럽 사회는 국내문제에 치중하게 될 가능성이 높다. 자유롭고 개방적이면서 안전한 사이버공간을 구축하려면 유럽과 한국의 다양한 사이버 정책 환경에서 다양한 이해당사자들의 지속적인 참여를 필요로 한다.

결론

EU-한국 사이버 협의에서는 사이버 회복력, 사이버 갈등 예방, 5G, 사이버 범죄 분야에서 EU와 한국 간 협력 강화의 필요성이 거듭 제기되었다. EU는 한국이 증가하는 중-미 긴장관계 속에서 "중립적" 역할을 추구하고 있음을 인지하였다. 사이버공간에서의 제한적 조치의 적용과 같은 문제에 있어 양측이 서로 다른 견해를 표명하기도 하였지만, 참가자들은 국제법, 책임 있는 국가의 행동규범 이행, CBM과 같은 분야에서 높은 수준의 합의점을 도출해내기도 하였다. 또한 EU와 한국의 참가자들은 사이버공간에서의 회복력과 신뢰구축을 위한 양자, 지역 및 다자간 노력을 위한 비정부 전문가의 참여와 그에 대한 가치를 한결같이 강조하였다. 2020년 11월 말로 예정되어있는 금번 EU-한국 사이버 협의에서는 이러한 이와 관련한 권고안의 추가적인 검토를 제안하였다.

EU 사이버 다이렉트(Cyber Direct)와 파트너에 관하여

EU 사이버 다이렉트는 한국을 포함한 전략적 파트너들과 사이버 회복력, 규범, CBM에 관한 EU의 대화를 넓히기 위해 노력하고 있다. 이 프로젝트는 유럽 및 협력국 워크숍을 구성하여 자유롭고 개방적이며 안전한 사이버공간을 공동으로 구축하기 위한 효과적인 방법을 비공식적으로 논의함으로써 정부 및 민간 사이버 전문가 간의 대화를 촉진하고 관련 연구를 수행한다. 또한 EU의 사이버 보안 및 인터넷 거버넌스 정책에 대한 지식을 보급하고 지역과 부문에 걸친 가교역할도 수행한다. 이 프로젝트는 유럽위원회가 주관하는 파트너쉽 기구 활동(Partnership Instrument Action)에 해당되는 *국제 디지털 협력 – 사이버공간에서의 신뢰와 보안(International Digital Cooperation – Trust and Security in Cyberspace)*로부터 자금을 후원받고 있으며, GMF, EUISS, SNV가 공동으로 시행하고 있다.

국가보안기술연구소(NSR)는 2000년 국방과학연구소(ADD)와 한국전자통신연구원(ETRI)의 정보보안 및 암호 연구 부서를 통합하여 설립한 대표적인 정부출연 사이버보안 연구기관으로, 공공 및 국방 부문, 주요기반시설을 위한 국가 사이버보안 정책 및 전략, 암호, 암호화 장치, 사이버보안 제품 및 기술 등의 개발을 담당한다. 국가보안기술연구소는 이러한 업무를 수행하는 총 5개 연구 부서와 사이버안전훈련센터(CSTEC), IT보안인증사무국(ITSCC)으로 구성되어있다.