사이버 범죄의 국제적 규제:
사이버범죄협약과 추가의정서

오선영
(숭실대학교)

사이버범죄의 다양화와 가속화

- 디지털 성범죄·해킹 범죄 증가에 국제 수사 공조 요청도 급증: 아동 성 착취물을 공유하는 일명 'n번방' 사건 이후 협약 가입 필요성에 대한 목소리가 커짐. 디지털 성범죄는 상당수가 해외법인이 개발한 SNS에서 발생해서 국제 공조가 범죄 수사에 필수적 (2020년 사이버 성폭력 수사를 위해 범죄 정보 제공을 요청한 건수는 767건이지만 2021년에는 1166건, 지난해는 1468건으로 3년 사이 2배 가량 증가)
- 가상자산 거래소 해킹 사건이 늘어나면서 사이버 테러 분야에 대한 공조 요청 건수 (2020년 이후 8배 증가)
- 아마존(Amazon), 마이크로소프트(Microsoft), 구글(Google) 등에 대한 클라우드 인프라 공격이 증가
- 러시아-우크라이나 분쟁이 시작된 지 1년이 지난 시점에서 몇몇 국가들은 첩보 활동과 교란 작전을 위해 공격적인 사이버 능력을 전략적으로 활용하고 있다는 보고서 출간
- 北 등 사이버범죄(北 불법취득 코인 1억달러 미사일 프로그램 사용 막아) 대응, 美법무부 국가안보국(NSD) 산하에 전담팀 신설: (2023년 6월 23일)

사이버범죄협약 vs UN협약

- 유럽평의회, 미국, 일본 등 서구 국가 vs. 러시아,중국, 북한, 이라크 등
- 외국과의 수사공조 필수, 국가통제 강화에 반대 vs 주권침해

사이버범죄 국제규제: 유럽평의회를 중심으로

명칭	발효일	당사국	대상
사이버범죄협약 (부다페스트 협약)	2004년 7월	68개국	사이버범죄의 신속한 공조
제1차 추가의정서	2006년 3월	35개국	인종주의/ 외국인 증오 범죄 확산 방지
제2차 추가의정서	2022년 12월부터 서명 시작	현재 41개국이 서명한 상태	디지털 증거 확보 공조

사이버범죄협약 (1)

- The Budapest Convention on Cybercrime (ETS No. 185)
- 사이버범죄에 대한 최초의 국제 조약으로 비유럽 국가들에게도 개방 (미국, 캐나다, 일본, 호주 등도 당사국임)
- 민간 영역에서 발생하는 사이버범죄를 규제하는데서 출발하였으나, 국경을 넘는 공공기관 해킹, 텔 등이 증가하면서 사이버안보와 직결

사이버범죄협약 (2)

- 실체법, 절차법, 국제공조 절차 등 총 4개의 장, 48개의 조문으로 구성

장	주요 내용
1장	정의 규정
2장	불법접속, 불법감청, 데이터 침해, 시스템 방해, 장치 남용, 컴퓨터 관련 위조, 컴퓨터 관련 사기, 아동 음란물 관련 범죄, 저작권 관련 범죄 등 실체법과 저장된 데이터의 신속한 보전, 제출명령, 데이터의 수색과 압수, 감청 등 절차법 및 관할에 대해 규정
3장	전통적/컴퓨터 범죄와 관련된 공조 및 범죄인 인도 규정
4장	표준조항과 유보조항

사이버범죄협약 (3)

- 사이버 범죄에 대한 최초의 다자조약
- 실체법적: 국가가 반드시 범죄화 해야 하는 범위: 가령 컴퓨터 시스템에 대한 권한없는 접속이나 아동포르노 유포 등
- 절차법적: 국가들 사이에 원활한 형사사법공조를 이루기 위한 필요한 절차들을 규정: 데이터의 신속한 보전, 정보제공명령, 상시적인 연락 거점 등

이를 통해 서로 다른 법체계를 가진 국가들 사이에 효율적인 사이버범죄 수사 협력을 위한 기반을 만드는 것

사이버범죄협약 (4)

- 러시아 반대: 국가 주권 침해 이유 등
- 제32조 b항: “데이터를 제공할 법적 권한을 가진 사람의 합법적이고 자발적인 동의가 있는 경우, 자국 내에 있는 컴퓨터 시스템을 통하여 다른 당사국에 있는 저장된 컴퓨터 데이터에 접근하거나 이를 수신할 수 있다”

  → 타국 정부의 동의 없이도, 해당 데이터에 접근 가능 (단, 데이터 접근의 권한을 가진 자의 자발적 동의 후)

  → 피의자가 스스로 자신의 이메일 등을 제출하는 것

  → 서비스 제공자에 대한 직접 요청이 아님: 이에 제2차 추가의정서 필요성이 대두

제1차 추가의정서 (1)

- Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189)
- 사이버범죄협약의 적용대상 범위를 확장
- 사이버를 통한 인종주의적이고 외국인 증오적 자료의 유포, 그리고 그러한 동기에 기반한 협박과 모욕을 범죄화하도록 규정

제1차 추가의정서 (2)

- 모든 규정들은 필수 규정으로 국내법으로 다음을 범죄화 하여야 함
- 컴퓨터 시스템을 통한 인종 차별 및 외국인 증오 자료 유포, 인종 차별적 및 외국인 증오 동기에 기반한 위협, 인종 차별 및 외국인 증오적 동기에 기반한 모욕, 그리고 집단 학살 또는 인류 범죄를 부인하거나 심각하게 간소화하거나 승인하거나 정당화 하는 것

제2차 추가의정서 (1)

- Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224)
- 사이버범죄의 다양화, 전자증거확보의 어려움, 기존 형사사법절차의 한계
- 정보를 보관하고 있는자(서비스 제공자)를 상대로 타국 정부를 거치지 아니하고 직접 공조 요청 가능하도록
- 긴급상황에서의 공조절차를 신속히
- 화상 조사를 증거로 채택할 수 있도록 절차법에 근거 규정 마련
- 수사 공조 남용방지, 개인정보 보호

제2차 추가의정서 (2)

- 타국에 위치한 인터넷 서비스 제공자를 상대로 "직접" 요청

정보 유형	내용	조문
Domain Name 등록정보	- 권한이 부여된 기관이 서비스 제공자에게 직접 요청 가능	제6조
Subscriber Info	- 직접 요청 가능 - 트래픽/내용 data는 직접 요청 불가	제7조
공조 요청 국가의 가입자 정보 및 트래픽 데이터 제공 명령에 대한 강제력 부여	- 서비스제공자에게 가입자 정보/트래픽 데이터 제공하려는 명령(order)을 공조 요청과 함께 타국 정부로 송부 시, 타국에서 이에 대한 강제력을 인정 - 내용 data는 해당범위 아님	제8조
긴급상황에서의 컴터 데이터 신속 공개	- 내용 data까지 포함	제9조

제2차 추가의정서 (3): 도메인 네임 등록 정보

- 서비스 제공자가 보유한 도메인 네임 등록정보(등록인 이름, 주소, 전화번호, 이멜주소 등)
- 권한이 부여된 권한 있는 기관은 도메인 네임 제공자에게 필요한 정보를 요청함에 있어, 해당 제공자가 위치한 국가의 정부에게 요청을 할 필요가 없이, “직접” 정보를 요청 가능하고, 이를 위한 필요한 법적 조치 마련해야
- 서비스 제공자는 반드시 정보를 제공해야 하는 의무가 있는 것은 아님

제2차 추가의정서 (4): 가입자 정보

- 권한 있는 기관이 다른 당사국 영역의 인터넷 서비스 제공자가 소유하거나 통제하는 가입자 정보의 공개를 직접 요청할 수 있도록 필요한 법적 및 기타 조치를 채택해야
- 요청되는 가입자 정보가 당사자의 특정한 형사수사 또는 소송에 필요한 경우에 한함
- 남용 방지 장치: 가입자 정보 제공 요청은 검사 또는 다른 사법 당국(judicial authority)에 의해 발급되거나 감독을 받아야 하며, 그렇지 않은 경우에는 독립적인 감독(independent supervision) 하에 발급되어야 한다고 선언(declaration)할 수 있도록 규정, 제공 요청이 이루어지는 경우 요청과 동시에 서비스 제공자가 위치한 국가에도 요청이 이루어진 사실, 보충적인 정보 및 수사와 관련된 사실관계의 개요를 통보하여야 한다는 제약 부과 가능, 유보조항 활용
- 서비스 제공자가, 정보제공을 거부하거나 가입자 정보 요청을 받은 후 30일 또는 요청기관이 요청서에 지정한 기간 중 더 긴 시간을 기준으로, 정보를 제공하지 아니할 경우에는 요청기관은 다른 형사사법공조절차를 통하여 정보 제공을 요청할 수 있음
- 요청서 기입 필수 사항: a. 요청 기관 및 요청일; b. 해당 명령이 본 의정서에 따라 발급되었음을 명시하는 성명서; c. 서비스 제공자의 이름과 주소(들); d. 수사 또는 소송의 대상이 되는 범죄(들); e. 특정 가입자 정보를 필요로 하는 당국이 정보 제출 명령을 한 기관이 아닌 경우 해당 기관의 신분 정보; 그리고 f. 요청되는 특정 가입자 정보에 대한 상세한 설명

제2차 추가 의정서 (5): 신속한 제출 명령 강제 수단

- 저장된 컴퓨터 데이터의 공개를 위한 당국 간 국제 협력을 강화하는 절차
- 요청기관이 타국에 위치한 서비스 제공자에게 가입자 정보 또는 트래픽 데이터를 제공하라는 명령을 공조 요청과 함께 타국 정부로 송부할 경우, 타국 정부는 이러한 명령이 자국에서도 강제력을 가짐을 인정하고 이를 서비스 제공자를 상대로 집행하도록 해야
- 현재의 형사사법공조절차보다 간소화된 형태로 설계
- 요청을 받은 당사국은 요청기관의 명령을 국내 명령과 동등하게 받아들여 국내 명령과 동일한 효과를 부여하거나, 명령을 보증하여 국내 명령과 동일한 효과를 부여하거나, 자체적인 제출 명령을 발령함으로써 요청기관의 명령을 이행할 수 있음
- 가입자 정보와 트래픽 데이터만을 대상

제2차 추가 의정서 (6): 긴급 상황

- 긴급한 상황에서는 각 당사국은 형사사법공조절차를 거칠 필요없이, 사이버범죄 협약 제35조에 따라 각 당사국에 설치된 연락기관(contact point)을 통하여 타국 내에 위치한 서비스 제공자로부터 신속한 필요한 정보를 제공받을 수 있도록 필요한 법적 그리고 기타 조치를 채택하여야
- 긴급상황: 자연인의 생명 또는 안전에 대한 중대하고도 임박한 위험이 있는 상황
- 긴급상황이므로 내용 데이터 포함
- 가입자 정보는 제외: 제7조를 통해 직접 요청이 가능하므로

제2차 추가 의정서 (7): 개인정보 보호

- 제14조 (총 15개항)
- 수집된 개인정보는 반드시 목적에 맞는 범위내에서만 사용되어져야
- 인종, 정치적 견해, 종교적 신념, 유전자, 건강 또는 성생활과 관련된 정보와 같이 매우 민감한 데이터(sensitive data)는 이로 인해 정보의 대상자가 부당하게 불이익을 입지 않도록 필요한 조치를 하여야
- 수집된 개인정보는 필요한 기간 내에만 보유해야 하는데, 이러한 의무를 이행하기 위해 국내법에서 데이터의 특정 보유 기간 또는 추가적인 보유 필요성에 대한 주기적 검토를 제공해야
- 개인 정보가 수집된 대상자에게 정보가 수집된 사실, 근거, 보유 기간, 정보를 수령한 기관 등에 대하여 통보가 이루어져야
- 정보를 제공받은 국가에서 제14조에 규정된 조항에 대한 체계적이거나 실질적인 위반에 대한 중대한 증거(substantial evidence)가 있거나 실질적 위반(material breach)이 임박한 경우에는 다른 국가로의 개인정보 이전을 중단할 수 있음

사이버 범죄 국제적 규제: 한국에의 시사점

- 2022년 10월 11일 사이버범죄협약 가입을 위해 유럽평의회에 협약 가입의향서를 제출. 유럽평의회는 한국에 가입 초청서를 보낸 상태.
- 신속한 수사를 위한 공조를 위해 추가의정서 가입 필요성 대두: 사이버범죄협약 당사자이어야
- 협약이나 추가의정서의 신속한 공조 절차를 통한 성공/실패 사례 연구의 필요성 대두
- 국내법 정비: 형사소송법, 통신비밀보호법, 전기통신사업법, 정보통신망 이용촉진 및 정보보호 등에 관한 법 등 → 부처간의 이견 조율의 어려움 → 각 부처와 전문가들로 구성된 협의회 활용, 사이버 범죄 관련 신속한 공조를 촉구하기 위한 특별법 마련 필요