국가전략연구위원회 이슈브리핑 26호 (발간일: 2024.5.5.)

정보기관의 디지털정보 수집 권한[1)]

김창섭 (고려대학교)

1. 머리말

인터넷 확산과 인권 강화로 인해 정보기관의 정보수집 환경(패러다임)이 크게 변화하고 있다. 정보기관은 인터넷의 보편적 확산으로 직접 이동 없이도 全세계를 대상으로 정보수집이 가능해지고 AI와 빅데이터 기술의 발전으로 대량의 디지털 데이터에서 필요한 정보만을 선별하여 활용할 수 있는 기회를 갖게 된 반면에, 고비도 암호기술의 대중화로 인해 감청 등의 전통적인 정보수집 방법이 무력화되는 위기를 맞게 된다. 또한, 기본권의 강화로 인해 국민들은 신뢰할 수 있는 정보기관의 활동에 대한 합리적인 법제도 마련을 요구하고 있다.

본 발표에서는 이러한 정보수집 환경의 글로벌화, 암호화 및 법제도화 추세에 따른 주요국 해외정보기관의 변화된 디지털정보 수집 권한을 중심으로 기술하기로 한다.

이미 많은 나라에서 암호통신, 역외통신 및 사이버 침투 등과 같은 새로운 정보수집 권한을 정보기관에 법적으로 부여함으로써 정보역량을 더욱 강화하고 있다. 또한, 이와 같은 디지털 정보수집 권한의 부여와 함께 오남용 통제장치도 지속적으로 강화하고 있다.

1993년 통신비밀보호법 제정 이래 시대 변화를 반영하지 못한 채 아날로그 수준에 머무르고 있는 우리나라의 정보수집 현실을 감안할 때, 최근에 정보법률(intelligence laws)을 활발히 제·개정한 주요국들의 디지털 정보수집 권한을 고찰해 봄은 우리에게 상당히 유익한 시사점을 줄 것이다.

---

1) 이 글은 2024년 5월 2일 제9차 사이버 국가전략 포럼에서 발표된 발표문을 수정보완한 것이다.

Ⅱ. 정보수집 패러다임의 변화

1. 정보수집 기술의 발전

국가안보의 개념은 군사안보뿐만아니라 경제안보, 과학안보, 환경안보 및 인간안보 등을 포함하는 포괄적인 안보로 확대되고, 이를 뒷받침하는 해외정보(foreign intelligence)는 국외정보, 국내 안보정보 및 우주·사이버 정보까지 포함하고 있어 국가의 해외정보 수집 역량은 더욱 중요해지고 있다.

인간을 통한 물리적인 방법으로 시작한 정보수집 활동은 과학기술의 발달에 따라 기술적인 진보를 거듭해오고 있다. 특히, 인터넷 기술의 발달로 인해 사이버공간을 통한 원격 정보수집이 가능해지면서 과거와 달리 타국 영토에 들어가지 않고서도 정보활동이 가능해져 정보활동의 패러다임 변화를 촉진시키고 있다. 과학기술을 통한 정보수집 활동은 저위험, 고효율의 대량 정보수집을 가능하게 하여 정보활동의 대상과 범위를 확대시키고 있다.

현재 수집되고 있는 정보의 대부분은 디지털 정보 형태이다. "디지털 정보"란 전자적 방식으로 처리되는 음성, 문자, 부호, 음향, 영상 등으로 표현된 디지털자료로서, 실시간 송수신 중인 통신데이터나 정보저장매체에 저장된 데이터를 모두 포함한다. 우리나라에서 디지털 정보수집을 규율하는 법은 통신비밀보호법이다.

이와 같은 디지털정보는 끊임없이 발전하는 정보통신기술로 인해 강력한 암호화와 익명화의 기술적 속성을 갖게 되며, 정보수사기관의 입장에서는 정보수집이 곤란해지는 위기를 맞게 된다. 2017년 호주 연방경찰은 감청으로 수집한 데이터의 90% 이상이 암호화된 디지털 통신이어서 해독할 수 없어 사실상 수집에 실패하였음을 언급한 바 있다.[2)]

이러한 디지털정보의 암호화 및 익명화 특성으로 인해 全세계 정보기관들은 정보를 수집하고도 해독할 수 있는 기술 능력을 확보하지 못하는 수집의 "암흑화(going dark)" 상황에 처해 있고 이는 법집행의 공백 상태로 이어진다.

2. 정보활동의 제도화 추세

정보수집 활동은 전통적으로 비밀리에 이루어진다. 비밀을 속성으로 하는 국가의 정보활동은 기본적으로 명문화된 제도화를 거부해 왔다. 그러나 오늘날 국가의 정보활동은 빠르게 제도화되고 있는 경향을 보이고 있다. 가장 뚜렷하게 나타나고 있는 제도화의 형태는 국내 입법이다. 정보활동에 관한 조직, 임무, 목표 등을 국내법으로 규정하여 법률적으로 제도

2) The Parliament of The Commonwealth of Australia, Telecommunications and Other Legislation Amendment(Assistance and Access) Bill 2018 Explanatory Memorandum, 2018, p.2

화하고 있다. 이는 국가들이 정보활동의 법적 정당성을 확보하기 위한 것으로 오늘날 대부분의 국가에 의해 일관되게 나타나는 현상이다.[3] 더불어, 국가의 정보활동은 국제협력을 통해서도 제도화되고 있다.

이러한 정보활동의 제도화를 촉진시킨 요인으로는 정보활동의 체계적 관리를 위한 국가의 의지, 불법 정보활동에 대한 감시·감독 및 국제협력 필요성 등의 다양한 환경들이 작용한다고 볼 수 있다.[4] 특히, 유럽인권협약(European Convention on Human Rights) 등의 국제 인권표준은 정보기관의 권한이 법적 체계내에서 명확하게 규정되기를 강하게 요구하고 있다. 이제 개인정보보호와 데이터 보호 등의 기본권 강화 추세로 정보기관의 활동에 대한 명확한 법적 근거와 감독체계가 마련되어야 하며, 정보활동에 대한 투명성과 책임성을 지속적으로 제고하는 것이 정보기관의 중요한 과제가 되고 있다.

Ⅲ. 주요국 해외정보기관의 디지털정보 수집 권한

인터넷 확산에 의한 정보수집 기회의 포착, 첨단 정보통신 암호화에 따른 위기 봉착 및 국제적인 기본권 강화의 움직임 등 정보수집 환경의 패러다임 변화에 대응하기 위해 대부분의 서구 국가는 디지털정보를 수집하기 위한 정보법률(intelligence laws)을 최근에 개혁 수준으로 제·개정하고 있다.

각국은 다양한 형태로 해외정보기관을 운영하고 있으며, 또한 각 해외정보기관은 다양한 형태로 법적 체계와 통제장치를 가지고 있다. 국가별로 해외정보기관의 권한, 수집 방법 및 통제장치 등을 종합해 보면 다음과 같다.

미국은 해외정보감시법(Foreign Intelligence Surveillance Act, FISA)과 대통령 행정명령 12333호(Executive Order 12333, EO 12333)에 의해 해외정보 수집을 규율한다. 내국인 수집 대상자는 FISA에 근거하며, 해외정보법원(Foreign Intelligence Surveillance Court, FISC)에서 승인한다. 해외정보 수집의 대부분은 국가안보국(NSA)에서 수행한다. 해외(역외) 소재 외국인 수집 대상자는 EO 12333에 근거하며, 대통령의 위임받은 법무장관이 승인한다. 각 법률의 적용은 수집정보의 형태, 대상자 국적, 대상자 소재지 및 수집위치 등에 따라서 달라지며 세부적으로 규정되어 있다. 해킹 활용한 능동적인 수집은 EO 12333 등에서 주로 허용된다.

영국은 해외정보 수집을 GCHQ와 MI-6에서 수행하며, 통신발전과 테러위협 등에 대응하기 위해 정보수사기관의 수집 권한을 확대한 2016년 수사권한법(Investigatory Powers Act, IPA)에 근거하여 디지털정보 수집을 규율한다. IPA는 정보수사기관에게 정보통신 내용을 확보하도록 모든 권한을 부여하며, 이는 표적감청, 대량감청 및 능동적 수집(equipment

3) Countering State-Sponsored Cyber Economic Espionage under International Law Lotrionte, Catherine, pp.487-488
4) 최성규,『국가의 비밀 정보활동과 국제법』(삼우사, 2023), p.48

interference) 등의 형태로 규정된다. 정보수사기관의 수집요청에 따라 독립 기구인 수사권한위원회(Investigatory Powers Commissioner's Office, IPCO)내 사법위원(Judicial Commissioners, JC)이 최종 승인한다.

독일의 경우, 해외정보 수집은 연방정보부(BND)에서 수행하며, 기본법 제10조법(G-10법)에 의해 안보목적의 감청을 규율하고 정보수사기관의 신청에 따라 독립감독기관인 G-10 위원회에서 수집을 승인한다. 암호통신을 포함하여 전송 중인 또는 저장자료에 대한 능동적인 수집이 가능하다.

프랑스는 대외정보총국(DGSE)이 해외정보 수집을 담당하며, 2015년 테러발생 이후에 정보법률[5]에 근거한 국가안보법[6]에서 정보기관의 수집을 규율한다. 국가안보법은 국가위협과 중대범죄에 대응할 수 있는 법적 근거를 마련하고 정보수사기관이 합법적이고 일관된 정보수집 활동을 할 수 있도록 보장한다. 안보목적의 정보수집인 행정감청은 국가안보법에서 허용하며, 독립기관인 국가정보기술통제위원회(CNCTR)[7]의 감독을 받는다. 행정감청의 7개 대상 中에서 국가안보, 과학·경제 보호, 범죄행위 및 조직범죄 예방 등이 포함된다.

2015년 국가안보법에서는 실시간 위치추적, 실시간 네트워크 모니터링, 소프트웨어(알고리즘), 메타데이터 활용 및 사이버 침투기술 적용 등과 같은 새로운 정보수집 기술을 추가하여 명시하였다. 국가안보법에서는 안보목적으로 정보기관이 다양한 새로운 수집기술을 합법적으로 활용할 수 있다는 특징이 있다.

호주는 호주신호국(Australian Signals Directorate, ASD)에서 해외정보 수집을 주로 담당하며, 암호통신과 컴퓨터 접근을 강화하기 위해 2018년 제정된 TAA법(TIA, SDA 등 개정)[8]을 근거로 안보목적의 정보수집을 규율한다. 법무장관이 감청영장을 발부한다. TIA법에서는 실시간통신, 저장통신 및 능동(해킹) 수집 가능하며, SDA에서도 랩탑, 휴대폰, 라우터 등의 디지털 장비에 대한 수집을 위한 능동 수집이 허용된다, 수집장비는 수집하는데 사용할 수 있는 모든 장치 또는 프로그램으로 정의된다.

캐나다는 통신안보청(Communications Security Establishment, CSE)법과 안보정보원(Canadian Security Intelligence Service, CSIS)법에서 해외정보 수집을 규율하고 있다.[9] Five Eyes 동맹의 참여기관인 CSE는 신호정보와 사이버안보를 담당하는 조직이다. CSE는 2019년 CSE법에 의해 CSE의 권한, 활동 및 운영의 합법성을 명확히 규정하는 한편, 향후 수십년동안 수행할 수 있는 CSE 활동의 범위를 확대하였다. 기존의 3개 권한(해외정보, 사이버안보 및 기술지원)에서 방어적 사이버 작전(defensive cyber operations)과 적극적 사이버 작전(active cyber operations)을 추가하여 총 5개 권한(임무)으로 확대하였다. 안보위협에 대처하

5) loi relative au renseignement 2015 : 정보활동에 관한 법
6) Code de la sécurité intérieure
7) Commission nationale de contrôle des techniques de renseignement
8) Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018
9) 본 소논문에서는 포괄적 안보 개념의 확장 추세를 고려하여 정보기관 명칭에 포함된 "Security" 용어는 "안보"로 국역하기로 한다.

기 위해선 새로운 사이버 역량과 도구가 필요하며, 이를 반영하여 CSE법은 신호정보·사이버 작전(적극·방어)·대규모 사이버안보 권한(임무)을 구체적으로 규정하고 있으며, 해킹 등의 능동적 수집 방법을 승인하는 법적 근거를 제시한다. 해외정보 수집과정은 장관 승인 → 정보커미셔너 최종승인이나, 사이버작전의 경우에는 정보 커미셔너없이 장관의 승인으로 진행된다.

네덜란드에서 안보목적의 정보수집은 종합정보안보부(Algemene Inlichtingen-en Veiligheidsdienst, AIVD)와 국방안보부(Militaire Inlichtingen-en Veiligheidsdienst, MIVD)에서 담당하며, Wiv 2017법[10]에 의해 업무 권한을 갖는다. 정보기관을 규율하는 Wiv 2017법에서는 통신의 장소와 상관없이 모든 형태의 대화, 통신 및 데이터에 대해 수집, 저장 및 복호화할 수 있는 법적 근거를 제공하며, 휴대폰, 컴퓨터나 주변장치와 같은 컴퓨터 장치나 시스템에 접근할 수 있는 "특수권한"이라 불리는 해킹 권한을 부여한다. 직접 대상자 해킹 곤란한 경우에는 제3자 장치에 대한 해킹도 허용되며, 제3자가 암호화 지식이나 복호화 키를 보유하고 있는 경우에는 이를 정보기관에 제공해야 한다. 수집 요청에 대해서 독립기관인 권한심사위원회(TIB)가 사전 승인한다. 또한, 독립기관인 정보안보감독위원회(CTIVD)가 사후 감독한다.[11]

스웨덴의 해외정보 수집은 국방통신정보부(Försvarsmaktens rättsliga enhet, FRA)에서 담당한다. FRA는 신호정보, 사이버, 컴퓨터보안 등의 임무를 수행하며 FRA법에 근거하여 활동한다. FRA법에 따라 안보위협, 국익위협, 공공인프라에 대한 외부위협 등의 8개의 명시적 정보수집 목표에 대해 유무선 및 이메일 감청과 정보수집을 수행한다. 수집은 표적감청, 대량감청, 능동적 수집이 가능하며, 대량감청의 경우에는 검색어를 통해서 수집되어야 한다. FRA법은 디지털정보 수집도구 및 수집방법에는 제한이 없다. 모든 수집활동은 정보법원이 최종 승인하게 된다.

노르웨이의 경우, 해외의 외부 위협과 국익 정보를 수집하는 유일한 해외정보기관은 노르웨이 정보원(Norwegian Intelligence Service, NIS)이다. 2020년 개정된 정보원법(Intelligence Service Act, ISA)에서는 NIS의 권한, 수집 방법 및 통제장치 등을 구체적으로 명시하고 있다. 권한(임무)에는 안보, 국익, 테러, 대량살상무기 뿐만아니라 "외국 사보타주 및 영향력 작전" 등 총 9개 분야가 정의된다.

ISA법의 수집 방법 규정에 있어선, 오픈소스, 관찰 및 기술적인 수집 등이 가능하며, 전송중인 통신수집을 위한 중간단(mid-point) 수집, 컴퓨터시스템에서 정보수집하는 종단(end-point) 수집 등을 구체적으로 정의하고 있다. 또한, 수집방법 집행에 있어 소프트웨어를 규정함에 따라 해킹 등의 능동적인 수집기술 활용이 가능하다. 아울러, 수집장비의 교육 및 시험을 위한 국내에서의 수집도 규정하고 있다. NIS長의 수집 요청에 대해 오슬로 지방법원에서 영장 승인하며, EOS 위원회(EOS Committee)가 사후 감독한다.

10) Wet informatielevering ter veiliging van de informatiemaatschappij 2017
11) TIB(Toetsingscommissie IT-beveiliging), CTIVD(College voor de Toezicht op de Inlichtingen- en Veiligheidsdiensten)

앞서 살펴본 각 해외정보기관 관련한 법률들의 공통점을 살펴보면 첫째, 인권수준과 기술발전 등의 시대상을 고려하여 정보법률을 지속적으로 제·개정하며, 둘째, 정보기관의 권한, 수집 방법 및 통제장치 등을 정보법률內에 세부적으로 명시하는 추세이며, 셋째, 인터넷, 암호 및 해킹 등의 미래 신기술을 포함할 수 있는 유연한 법제를 설계하여 능동적인 수집과 사이버 작전(cyber operations)까지도 가능하도록 합법적인 근거를 마련하고 있다는 점이다.

Ⅳ. 맺음말

2022년 미국은 적국의 컴퓨터에 접근하여 정보를 수집하거나 기능을 무력화시키는 공세적인 사이버 대응(offensive cyber operation)을 수행하고 있음을 언급한 바 있다.[12] 또한, 영국은 공세적인 사이버 대응에 있어 국내법과 국제법을 준수하고 있으며, 장관들과 사법위원들(JC)의 승인하에 수행하고 있음을 공개적으로 밝히고 있다.[13]

이처럼 새로운 위협에 대한 실효적인 대응과 적법 근거 마련을 위해 2015년 이후부터 영국, 독일, 프랑스, 호주, 네덜란드 등 대부분의 해외정보기관은 관련된 정보법률을 크게 개정하면서 디지털 정보수집 역량을 강화하고 있다.

구체적으로 살펴보면 첫째, 기술 발전과 인권 수준 등 시대 변화를 고려하여 정보기관의 수집 권한, 방법 및 통제장치 등을 법률로써 세부적으로 명시하고, 둘째, 인터넷, 암호 및 해킹 등의 신기술을 활용하는 적극적인 수집 방법을 법률로 규정해 기술 발전에 유연하게 대응하며, 셋째, 외부의 독립 감독기관을 마련해 정보기관의 오남용 통제장치를 강화하고 있다. 이와 함께, 국제 인권 원칙과 규범이 정보기관의 정보수집 권한, 방법 및 통제장치를 강화하고 예측 가능한 법체계를 갖추도록 요구하고 있다.

이제 정보기관의 활동을 규율하는 명확한 법체계와 독립적인 감독체계가 시대적 흐름으로 자리하고 있다. 이를 수용해야 정보기관은 정보수집 역량을 확충할 수 있고 국민의 신뢰를 얻을 수 있으며 국가안보와 국익의 강화를 도모할 수 있다.

한편, 우리나라는 그동안 정보기관의 비밀주의 관행, 부처 간 이해관계 충돌 등으로 인해 정보기관의 권한 및 방법 등을 명확히 규율하지 못하고 있다. 정보통신 발전과 기본권 강화 등의 현실변화에도 뒤처지고 있다. 현행 정보수집 법률인 통신비밀보호법은 불명확하고 한정된 수집 권한, 재래식 수집 방법, 실질적 감독기관 부재 등의 문제점을 갖고 있다. 또 다른 법률인 국가정보원법 또한 동일한 문제를 내포하고 있어 아직까지 디지털 정보수집을 뒷받침할 수 있는 국내 법제도는 미흡한 상황이다.

---

12) "UKRAINE SYMPOSIUM – U.S. OFFENSIVE CYBER OPERATIONS IN SUPPORT OF UKRAINE", Michael N. Schmitt, LIEBER INSTITUTE, 2022.6.6., https://lieber.westpoint.edu/us-offensive-cyber-operations-support-ukraine/

13) The head of GCHQ says Vladimir Putin is losing the information war in Ukraine, Sir Jeremy Fleming, The Economist, 2022.8.18

한참 늦었지만, 이제라도 정보기관의 디지털정보 수집활동에 대한 권한과 방법 등을 법률에 명확하게 규정하고, 잠재적인 오남용 방지를 위한 감독체계도 개선해야 한다. 이를 위해 최근 정보법률을 활발하게 개정한 캐나다, 네덜란드, 노르웨이 등의 해외사례를 벤치마킹하여 우리나라도 정보기관 조직법인 국가정보원법에 디지털정보 수집의 권한과 절차를 규정하고 전문적·독립적인 감독기관을 신설 규정하는 방안을 고려할 수 있다. 통신비밀보호법 또한 디지털정보 환경을 반영해 최신기술을 활용한 수집 방법을 감청 수단으로 수용하는 등의 개선이 요구된다.

이제 국가의 정보역량 강화를 위해 시대 변화를 유연하게 반영할 수 있는 실효적인 디지털정보 수집 권한을 정보기관에 부여하되 이를 감독하는 법적 체계를 조속히 마련해야 한다.

<참고자료>

※ 이슈브리핑에 수록된 내용은 필자 개인의 의견이며, 한국사이버안보학회의 공식적인 입장이 아님을 알려드립니다.