연구보고서

한국의 국가정보협의체 형성과 국회 정보위원회의 역할

연구기관명 : 사단법인 국가정보포럼
책임연구원 : 석재왕 건국대교수
공동연구원 : 김은혜 건국대연구원

2021. 8.

▷ 이 책자는 2021년도 정책연구개발(의정활동지원현안과제연구 또는 해당 부서예산내역) 용역과제에 의하여 (사)국가정보포럼으로부터 제출받은 보고서로서 의정활동연구에 활용되도록 발간한 것입니다.

제 출 문

국회정보위원장 귀하

본 보고서 “한국의 국가정보협의체 형성과 국회 정보위원회의 역할”을 2021년 정보위원회의 정책연구개발 용역과제 최종보고서로 제출합니다.

2021. 8.

(사)국가정보포럼

목 차

표 목차

그림 목차

한국의 국가정보협의체 형성과 국회 정보위원회의 역할

Ⅰ. 서론

1. 연구 배경 및 필요성

오늘날 정보통신의 발달과 민주주의의 진전 그리고 전쟁 양상의 변화는 현대 정보기관의 조직운영과 활동 방식에 지대한 영향을 미치고 있다. 정보통신의 발달은 정보소비자의 생산자화, 비밀공작 추진 여건 악화, 수집과 분석의 연계 및 공개정보의 중요성 등을 야기시켰다. 이와 함께 민주주의의 진전은 정보활동의 투명성 강조, 정보통제의 강화 그리고 시민적 자유 보호의 중요성을 각인시켰다. 그리고 사이버 전쟁이 일상화된 안보 환경의 변화로 인해 정보기관은 보이지 않는 적과 싸워야 하는 새로운 위협에 직면해 있다.

정보기관을 둘러싼 환경의 변화는 한국 정보기관의 효과성과 효율성에 대한 평가와 이에 기초한 혁신을 요구한다. 한국의 정보기관의 기본 틀은 냉전기 이후 변화에도 불구하고 큰 변화 없이 유지되고 있다. 국정원의 경우 현 정부 들어 방첩을 제외한 국내 정보조직을 폐지하고 2023년 수사 기능의 이관을 법제화하였지만 국내외 정보통합형을 유지하고 정보기획 조정 및 조사 활동을 수행하는 권한도 보유하고 있다. 군 정보기관의 경우에도 정보사령부나 합참정보본부, 기무사 등 군정보 및 보안방첩기관의 조직과 활동 방식 역시 근본적으로 변화한 것은 없다. 통일부·외교부·경찰청 등 안보부처와 법집행기관에서 수행하는 정보활동 방식이나 조직 또한 크게 변화한 내용은 찾아볼 수 없다.

그렇다면 이 같은 환경의 변화에 직면한 정보기관과 안보부처들이 개혁 없이 국가안보라는 본연의 목적을 제대로 수행할 수 있을 것인가? 한국의 정보기관은 냉전기 권위주의 시대 창설된 이래 개별 정보기관을 중심으로 운영되어 왔기 때문에 융합과 통합이 강조되는 오늘날 환경변화에서는 효과적으로 작동할 수 없다.

미국 등 선진국에서 운영하고 있는 국가정보조정협의체, 국가정보생산 시스템, 경쟁적 분석체계와 같은 통합기제나 독립된 감사관과 같은 통제시스템이 없다.

새로운 위협에 대한 대응은 정보기관과 행정부처의 기능을 단순히 재조정하는 차원에서 해결될 수 있는 사안이 아니다. 신안보(emerging security)시대 불확실성과 복합성을 특징으로 하는 위협 유형들에 대응하기 위해서는 민간 정보기관, 군 정보기관 및 안보부처의 거버넌스를 통한 문제해결을 추구해나가야 한다.

본 연구는 한국의 실정에 부합한 정보공동체의 형성 필요성을 제시하고 국회의 바람직한 역할에 대해 살펴볼 것이다. 개별 정보기관 차원의 미시적인 변화나 개

혁을 주창하는 것이 아니라 국가 차원의 정보시스템을 구축할 것을 제안한다. 국회의 정보통제 강화 방안으로 의원들의 전문성의 강화, 당파성의 극복, 정보에 대한 접근 강화, 청와대 정보 감사 필요성, 감사원과 차별화된 통제 등을 제시한다. 본 연구는 총 6장으로 구성되어 있다. 제1장에서는 연구 배경과 필요성, 연구 방법을, 제2장에서는 정보협의체 구성요건과 선진국 정보기관의 특징, 제3장에서는 선진국 국가정보협의체와 의회 통제 방안을 살펴본다. 그리고 제4장에서는 한국의 정보체계와 국회의 정보통제, 제5장에서는 한국형 정보협의체 형성방안과 국회 역할, 제6장에서는 요약과 함께 전망이 제시될 것이다.

2. 연구범위와 방법

본 연구는 한국의 정보협의체 형성방안을 모색하고 국회 정보위원회의 역할을 살펴보는 데 목적이 있다. 선진국과 달리 한국은 국가 차원의 정보조정·생산할 수 있는 국가 차원의 협의체가 존재하지 않는다. 따라서 선진국 정보체계를 살펴볼 필요가 있는 만큼, 미국, 영국, 독일, 호주, 프랑스, 이스라엘 6개국에서 운영하는 국가정보협의체를 연구대상으로 선정하였다. 이들 국가 정보기관들의 조직 및 활동 방식, 정보협의체 유형 등을 살펴볼 것이다. 또한 이들 정보협의체가 제대로 작동하기 위한 의회의 통제 권한과 방식, 조직 등에 대해서도 연구한다. 연구의 과학화와 정책적 함의를 도출하기 위해 연구 방법론으로는 이들 국가정보협의체과 국회 역할의 유사점과 상이점을 비교하는 비교정보연구방법론을 적용할 것이다. 공개자료와 문헌 등을 통한 질적 연구를 통해 진행할 것이다.

Ⅱ. 이론적 배경 : 정보협의체 구성 요건과 선진국 정보기관의 특징

1. 정보공동체 개념과 구성 요건

1) 기원과 개념

오늘날 상당수의 선진국의 정보기관들은 정보공동체(intelligence community) 형식을 통해 운영되고 있다. 정보공동체는 정보기관, 행정부처 정보기관 및 군 정보기관 등으로 구성되는 관계로 공통점보다는 상이한 요소가 많다. 그럼에도 미국에서 정보공동체라는 용어를 사용하게 된 데는 이유가 있다.
원래 community라는 용어는 아리스토텔레스 이후 사랑과 애정으로 결합된 인간집단을 의미하였다. 그러나 실제 미국의 정부 기관들은 조직·개인간 갈등과 불신, 그리고 경쟁으로 얼룩져있었다. 따라서 이를 최소화하기 위해 하나됨(oneness), 전체성(wholeness) 그리고 통일성(togetherness)을 강조하기 위해 붙인 명칭이다.[1]정보공동체는 1981년 레이건 대통령 행정 명령 12333호에 의해 공식적인 용어로 사용되기 시작하였다.
정보공동체는 “정보업무를 수행하는 정부부처 연합체”,[2], “중앙정보장(DNI)의 지휘를 받으며, 정보업무를 수행하는 기관 및 조직들의 연합체”등으로 정의된다.[3]

2) 유용성과 한계

1950년대 냉전기 정보공동체가 운영되기 시작한 이래 현재까지 유지되고 있는 사실 자체가 이 제도의 유용성을 말해주고 있다. 선진국가들이 정보공동체 형태를 운영하는 배경에는 역사적·현실적 요인들이 작용하고 있다. 미국 IC의 경우 다른 국가들에 비해 특징들이 보다 두드러게 나타난다. 1947년도에 CIA발족되기 이전인 18세기말 이후 미국의 비밀공작활동은 국무성에서 수행해왔으며 1909년 FBI가 창설되면서 FBI가 해외 방첩활동을 담당해왔다. 행정부처 정보기관들의 기득권 유지와 중앙정보기관 설립에 대한 반발로 인한 파편화를 방지하기 위해 국가차원의 통합된 정보생산의 기능을 갖추기 위해 정보공동체를 설립하였다.

---

1) Lock K. Johnson and James J. Wirtz,『Strategic Intelligence』(Los Angels: Roxbury Publishing Company, 2004), p.26.
2)Jeffrey T. Richelson, 『The U.S. Intelligence Community』(New York: Routledge, 2016).
3) https://www.dni.gov.검색일 : 2021.7.19.)

정보공동체의 유용성을 정리해보면 다음과 같다. 첫째, 범정부차원에서의 정보역량을 극대화할 수 있다. 정도의 차이는 있지만 대부분의 행정부처는 정보를 수집, 분석하는 역량을 갖추고 있다. 행정부처는 정책을 입안, 집행하는 과정에서 정보기관이 얻기 어려운 양질의 정보를 수집, 분석할 수 있는 강점을 가지고 있다.

둘째, 정보기관들의 정보독점과 경쟁에서 비롯된 정보왜곡과 남용을 방지할 수 있다. 미국의 국가테러정보센터(NTCT)나 영국의 합동정보위원회(JIC), 호주의 정보평가실(ONI)은 국가정보(National Intelligence)를 생산하는 과정에서 5~6개 정보기관이 공동으로 정보를 생산하고 있어 정보의 정치화나 오류 가능성을 최소화하고 있다

셋째, 포괄안보 시대 산업보안 유출, 원자력 안전, 해양 안보 등 다양한 영역에서 범정부차원에서 안보위협을 효과적으로 대응할 수 있다.

넷째, 한국의 경우 2020.12 국정원 개혁에 따른 정보의 역량 약화 등 부작용을 최소화할 수 있다.[4] 외교안보 및 행정부처, 법집행기관들이 국정원이 수집·생산할 수 없는 정보들을 제공하는 한편, 정책과 정보 간 긴밀한 협업체제를 구축할 수 있다. 다섯째, 정보 소비자 위주의 정보활동이 가능하고 정보활동을 효과적으로 감독하고 시민적 자유를 보호함으로써 국민에 대한 신뢰성 제고할 수 있다. 한편, 정보공동체는 기관 간 명령, 수직 관계라기보다는 수평적, 횡적 관계를 통해 업무를 수행하기 때문에 부처 간 불화와 갈등이 발생하기도 한다. 예를 들어, 미국의 9/11테러에 대한 첩보를 사전에 입수한 후에도 CIA와 FBI 간의 협력의 부재로 정보실패로 이어진 것이 대표적인 사례이다.

3) 구성 요건

가. 규칙 : 법률, 대통령령(행정명령), 지침, 가이드

정보공동체가 원활하게 작동하기 위해서는 정보기관들을 통제하고 작동하게 하는 규정들이 필요하다. 미국의 예를 들어보면 대표적인 것으로는 법률, 행정명령(executive order) 및 국가상임위원회(NSC) 및 국가정보장(DNI) 지침서 등이 있다.[5]규정들은 정보기관이 합법적이고도 효과적인 활동을 가능하게 하는 기능을 수행한다. 먼저, 법률형식을 띤 것으로는 미국 안

4) 예를 들면, 수사권 이양에 따른 법집행정보의 약화, 국내 정책정보 기능 폐지에 따른 국내 정보역량 약화를 들 수 있다.

5) Charles D. Ameringer, 『U.S. Foreign Intelligence: The Secret Side of American History』 (New York: Lexington Books, 1990), pp.186-87.

보틀을 형성한 1947년 국가안보법(NSA), 정보통제를 법제화한 휴즈-라이언법(Huges-Rian,1974), 해외정보감시법(FISA, 1978), 정보감독법(IOA, 1980), 감사관법(IGA, 1989), 미국 애국법(USA PA, 2001), 정보개혁 및 테러방지법(IRTPA, 2004)등이 있다. 의회의 승인을 받았다는 점에서 정보기관에 미치는 구속력이 가장 강력하다.

그리고 대통령의 행정명령(executive order)을 통해 정보공동체 구성 요소들의 일반적인 기능과 책임을 규정한다. 법률이나 행정명령이 다소 일반적인 성격을 띤 데 비해 NSC 지침서는 보다 구체적 내용을 하달할 때 사용된다. NSC지침은 NSC회의에서 하달되는 만큼 정책과 정보가 소통하는 매개역할을 수행하며 안보부처 장관과 대통령 국가안보보좌관 등이 참석하는 만큼, IC전반에 걸쳐 영향력을 행사한다.

한편, 실무적이고 보다 구체적인 내용을 전달하는 경우에는 과거 정보기관 CIA국장(DCIA)지침서가 있었으며 비공식적인 경우에는 대통령정보 체크리스트(presidential checklist)와 같은 형식으로 발표되기도 하였다.[6] 2004년 설립된 DNI지침서는 보다 구체적인 형태를 띠고 있다. DNI는 지휘 지침, 정책 및 계획, 지시 이행 등의 내용을 전달하기 위해 정보공동체 지침(ICDs), 정보공동체 각서(ICPMs), 정보공동체 지침(ICPGs) 등을 내릴 수 있는 권한을 보유하고 있다. 구체적으로 설명하면 다음과 같다.[7]

각서(Memorandum)는 지침으로 포함되기 이전 정책방향을 제시하고 지침(Guidance)은 IC지침에 보조적인 역할을 하면서 구체적인 내용을 제시하는 기능을 수행한다. 일반적으로 국가정보장은 예산통제와 정보분석 지침, 정보활동 방향, 인사, 예산전용, 대의회 및 시민적 자유를 보장하기 위한 방향을 제시한다.

나. 정보기관 : 정보기관 및 행정부처

정보공동체 구성 요소로서 독립된 정보기관, 행정부처 산하 정보기관 및 군 정보기관은 견제와 협력 하에 중요한 역할을 수행한다. 미국을 비롯하여 영국, 호주, 독일, 프랑스 등 선진국의 정보기관은 아래 <표2.1>에서 보듯이 구성 요소에 있어서 유사한 패턴을 보여주고 있다.

---

6) Ameringer(1990), p. 187.

7) https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links /intelligence-community-directives(검색일 : 2021.7.21.)

<표2.1> 정보공동체 구성 체계

유형	국가	기관
독립 기관	미국	국가정보실(ODNI, 2004), 중앙정보국(CIA,1947)
군	미국	국가안보국(NSA), 국가정찰국(NRO), 국가지형정보국(NGA), 국방정보국(DIA), 육군정보국(G-2), 해군정보국(ONI),제16공군(16thAF), 해병대정보부(MCID)
	영국	국방부 국방정보부(DI)
	프랑스	국방부 해외안전총국(DGSE), 군사정보부(DRM), 국방보안국(DPSD)
행정부처	미국	국토안보부 정보분석국(I&A), 국토안보부 해안경비대정보국(CGI), 법무부 마약단속청 국가안보정보실(DEA ONSI), 국무부 정보조사국(INR),재무부 정보분석실(OIA), FBI정보실(FBI-IB), 에너지부 정보방첩실(OICI)
	영국	내무부 보안부(SS), 외교부 비밀정보부(SIS), 외교부 정보통신본부(GCHQ)
	프랑스	내무부 국내보안총국(DGSE)

2. 선진국 정보체계 주요 특징

1) 국가차원의 정보협의체 운영

선진국의 경우 민간, 군 정보기관 및 행정부처 정보기관이 참여하여 공동으로 정보 보고서를 생산하는 공동체(intelligence community)를 운영하고 있다. 특정 기관의 정보 독점이나 왜곡을 방지하여 정보에 대한 신뢰성과 객관성을 제고하고 다양한 안보위협에 대해 범 정부차원에서 대응하고 있다.이 과정에서 최고 정보소비자인 수상과 대통령이 정보기관협의체에 직접 관여하고 있는 것이 주요 특징이다.

<표2.2> 주요 국가별 국가정보 협업시스템 구축 현황

국가	기관명	구성 및 주요 기능
미국	합동정보공동체위원회(JICC), 국가테러정보센터(NTCT)국가정보장실(ODNI), 국가정찰국(NRO), 국가안보국(NSA) 등	o **구성** : 수상 또는 대통령 비서실장(관방부장관), 정보기관장, 군 및 경찰수장, 안보부처 및 경제부처 장관 o **기능** : 안보위협 공유, 기관간 갈등 조정, 정보목표 우선순위 조정,국가정보 판단 보고서 생산 및 배포
영국	합동정보위원회(JIC),정부합동대테러센터(JTAC)	
일본	내각정보회의, 합동정보회의	
호주	국가정보평가실(ONI)	
이스라엘	정보기관장 협의체(CDIS)	

이들 기관들은 불법 자금세탁, 사이버 범죄, 산업보안 및 대규모 전염병 등 분야에 대한 행정부처의 법적 권한과 전문성을 활용하면서 정보기관과 협업을 진행하고 있다. 새로운 안보영역에 대해 정보기관은 법적 근거나 전문성이 부족한 경우가 있기 때문에 정보협의체는 문제해결에 매우 유용한 수단이 될 수 있다.

2) 행정부처 산하에 정보기관 설치·운영

독립된 정보기관뿐 아니라 행정부처 산하에 정보기관을 운영하고 있다. 행정부처에서 필요한 정보를 자체 충당할 수 있고 정보기관에 대한 통제를 효율화할 수 있는 장점이 있다. 이 밖에 정책과 정보기관 간 협력을 강화할 수 있어 정보의 효과성을 제고할 수 있다. 주요 국가들의 실태를 살펴보면 다음과 같다.

- 미국 : 국무성(INR 정보조사국), 에너지부(OICI정보방첩실), 재무부(OIA정보분석실), 법무부(FBI, DEA정보처), 국토안보부(I&A정보분석국), 국방부(NSA 국가보안국 등 8개)
- 영국 : 국무성(SIS 비밀정보부, GCHQ정부합동통신본부), 내무부(SS, 보안부) 등
- 프랑스 : 국방부(DGSE 해외정보총국), 내무부(국내보안총국 DGSI)
- 호주 : 내무부(ASIO호주 보안부), 외교부(ASIS 호주비밀정보부) 등

다. 국가정보활동과 법 집행(경찰)활동을 분리, 운영

수사와 국가정보활동은 아래 <표2.3>에서 보는 바와 같이 목적과 활동방식이 상이하여 선진국에서는 분리, 운영하고 있다. 국가정보와 수사정보는 아래와 같이 구분되기 때문에 범죄수사에 필요한 법집행정보(law enforcement intelligence)는 수사기관이 직접 수집, 분석하고 있다.

<표2.3> 수사활동과 국가정보활동의 차이점 비교

구분	수사(법집행)정보 (law enforcement intelligence)	국가정보(national intelligence)
목적	범인 기소	합리적 국가안보 정책(대북, 외교 등) 결정에 투입요소
비밀성	공개적인 압수수색, 판결시 정보공개로 비밀성이 약함	매우 강함
합법성	엄격한 법적용, 불법시 무효	경우에 따라 해외에서의 불법 정보활동도 용인(예, 비밀공작)
내용	내사, 증인 신문 등	비밀공작, 수집, 분석, 방첩

Ⅲ. 선진국 국가정보협의체와 의회 통제

1. 미국의 정보협의체와 정보 통제

1) 정보공동체 현황과 특징

미국의 정보협의체는 정보공동체 형식을 통해 구성되고 운영되고 있다. 미국은 세계 어떤 국가의 정보기관들보다 차별화된 정보기관을 운영하고 있다. 첫째, 18개 정보기관으로 구성된 정보공동체(Intelligence Community)방식을 통해 국가안보와 국가이익을 추구하고 있다. 국가정보장(DNI)이 조정·감독하는 정보공동체는 독립된 정보기관인 CIA, 국방부 산하 군 정보기관 그리고 행정부처 산하 정보기관으로 구성된다.[8]정보공동체는 획일적인 명령체계가 아닌 느슨한 정부 부처 연합체와 같은 것으로 권력 분립을 반영한 연방제적 성격과 부처 간 견제와 균형을 중시하는 미국적 가치를 반영하고 있다.

둘째, 해외정보와 국내정보를 분리·운영하고 있다.[9] 분리형 정보시스템을 채택한 가장 큰 이유는 국내외 정보통합 운영에서 야기될 수 있는 시민적 자유나 인권침해를 차단하기 위해서이다. 외부 감독이 어려운 비밀정보기관은 자칫 게슈타포로 변질되어 국가안보 본연의 임무 보다는 정치개입과 국민 사생활 침해와 같은 불법활동을 자행하기 쉽다. 이러한 우려를 불식하기 위해 미국은 냉전기나 9/11직후 정보기관 개혁을 추진하는 과정에서 국내정보기관 설립에 대한 논의가 있었으나 용인하지 않았다.[10]

셋째, 다양한 정보기관의 활동을 통합하기 위한 조직체를 운영하고 있다. CIA산하 국가비밀공작국(SNB), DNI, DNI 산하 국가대테러센터(NTCT) 및 국가정보위원회(NIC), 국방부산하 국가정보수집기관인 국가정찰국(NRO), 국가안보국(NSA), 국가지형국(NGA) 등이 대표적인 사례에 해당된다. 이들 기관은 단일 행정부처 내에 소속되어 있으나 분야별로 국가 전체 차원에서 정보활동을 수행하고 있다. 또한 2004년 합동정보위원회(JICC)를 설치하여 정보요구 우선순위 확정, 예산, 정보활동 평가 등 관련 DNI에 자문하는 역할을 수행하는 것도 동일한 맥락에서 이해될 수 있다.

---

8) Richelson(2012).

9) 유럽의 정보기관들이 국내외 정보기관과 별도로 법집행기관을 운영하고 있는 것과 달리 미국은 법집행기관인 FBI에서 방첩 및 국내보안정보활동을 수행하고 있는 데 이는 법무부장관의 감독 하에 정보활동을 감독하고 인권침해 가능성을 최소화하려는 목적이 있다.

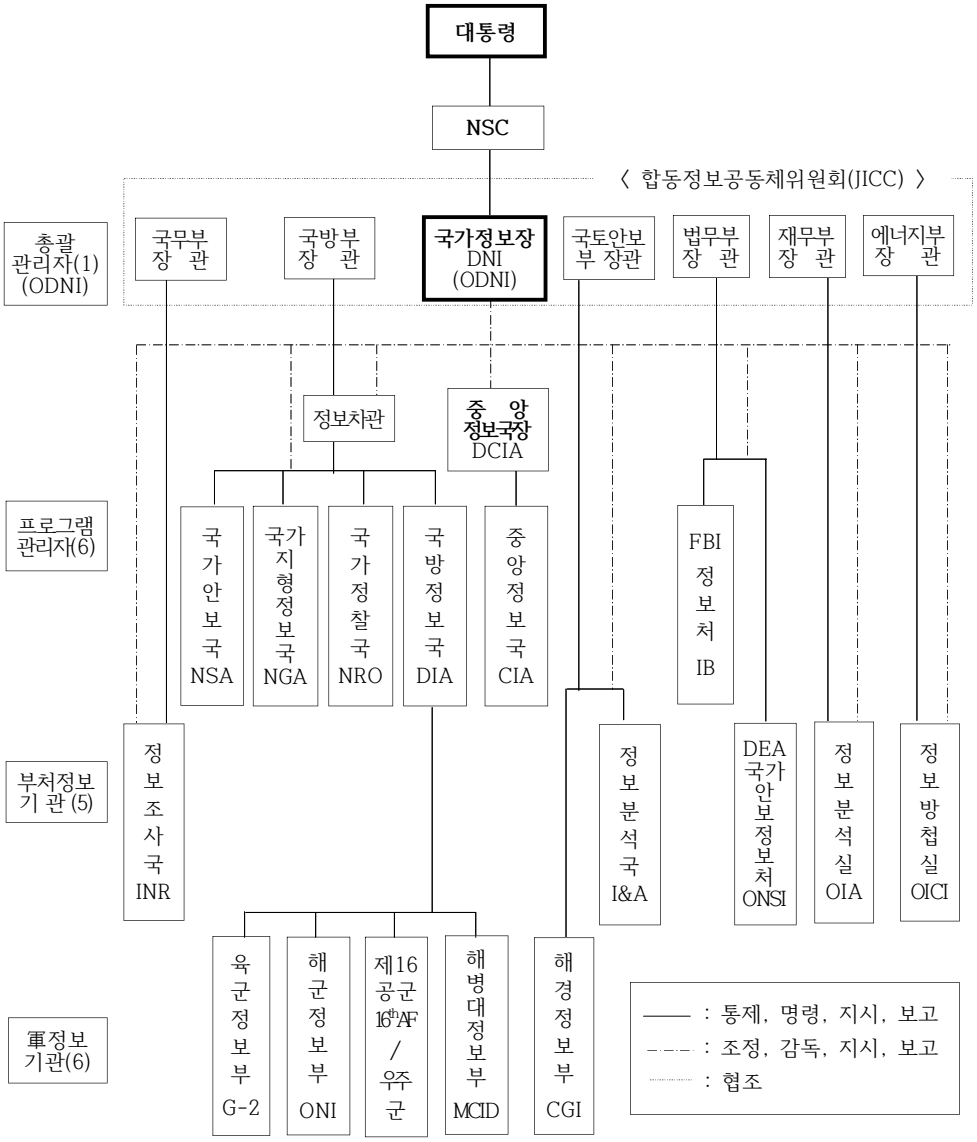
10)미국의 국내보안정보활동은 법집행기관인 FBI에 의해 수행되고 있다는 점에서 영국의 MI5, 호주의 ASIO, 독일의 BND 등 순수한 국내 정보기관과는 다르다.Peter. Gill, 『Policing Politics: Security Intelligence and the Liberal Democratic State』(New York:Routledge,1994).

넷째, 기존 국실과 같은 계선조직 이외 융합 센터(fusion center), 미션 매니저(mission manager) 등 다양한 조직형태를 운영하고 있다. 계층제에 의한 정보왜곡과 관료적 이기주의에 따른 차단벽을 제거하고 신속한 정보보고를 위한 노력의 일환이다. CIA 조직의 경우 전통적인 구분 방식인 지역과 기능으로 구분하면서 이를 계선조직과 센터로 양분하여 운영하고 있다.[11)]

다섯째, 다른 선진국들에 비해 방대한 규모의 정보시스템을 운영하고 있다. 따라서 미국의 정보개혁의 일관된 특징은 통합성을 강화하는데 있다. 특히, 수집을 담당하고 있는 국방정보 분야에서도 통합된 조직체를 운영하고 있는데, 미국의 경우 1962년에 창설된 국방정보실(DIA)이 대표적인 사례이다. 2021년 현재 미국의 정보공동체는 총 18개 기관으로 구성되어 있으며 2020년도 기준 정보공동체 전체 예산 규모가 858억불 규모로 영국의 45억여불과 비교했을 때 큰 차이를 보여주고 있다.[12)]

11) https://www.cia.gov/index.html(검색일 : 2021.7.14.)
12)https://www.dni.gov/index.php/what-we-do/ic-budget(검색일 : 2021.10.6.).

<그림3.1. 미국 정보공동체 체계도>



2) 정보공동체의 통합성 추진 방향

20세기 이래 정보활동의 통합과 조정문제는 정보기관과 대통령이 해결해야할 주요 과제가 되어왔다. 일반적으로 그 필요성은 전쟁 수행 과정에서 제기되었고 전후 구체적인 방안들이 논의되었는데 대체로 조정 기능을 갖춘 '단일기관' 형태와 상대적으로 느슨한 '협의체나 포럼' 과 같은 2가지 방식으로 논의되어 왔다. 1차 대전직후 미국은 대통령이 임명하고 대통령에게 책임지는 정보국(Bureau of Intelligence) 창설을 고려하였으나 관련 기관들의 반대에 부딪쳐 실현되지는 못했다. 다양한 정보기관들의 정보활동을

조정하려는 노력이 시작된 것은 2차 세계대전 중에 진행되었다. “부처간 정보조정위원회”(Interdepartmental Intelligence Coordinating Committee)가 창설되었지만, 상설 직위가 없었고 참여 기관들이 정보공유를 기피하여 효과는 제한적이었다.[13] 루즈벨트 대통령의 친구인 도노반(W. Donovan)의 “중앙집권적인 민간정보기관의 창설”주장에 의거 하여 1941.7 첩보 조정관(COI, Coordinator of Information)이 신설되었다. COI는 대통령과 안보 고위관계자들에게 국가안보와 관련된 첩보를 수집, 분석하는 업무를 담당하였다.

영국 정보기관 모델을 모방하여 학계 인사들과 정보기관 요원들은 협력하여 통합된 정보분석 활동을 하였는데, ‘중앙집권화된 분석’이라는 개념이 형성되기 시작하였다. 한편, FBI는 미국 내 간첩조사, 대간첩, 사보타지, 중립법 위반 등을 조사하는 기능을 수행하면서 여타 정보기관의 활동을 경계하며 상당히 비협조적인 태도를 보였다. 미국이 2차 대전에 개입하기 전 정보기관은 군(해외 군사 수집 정보), 국무성(외교 정보 및 공작활동), FBI(국내 및 해외 방첩 활동)가 협력과 통합적 차원보다는 경쟁적인 분위기 가운데 정보활동을 진행하고 있었다.

통합성이 결여된 정보시스템과 문화는 1941년 일본의 진주만 기습을 허용하면서 미국의 국가안보에 치명적인 정보실패를 유발하는 요인이 되었다. 미국은 통합적이고 시스템적인 첩보수집과 분석, 그리고 이행 권한이 책임자에게 배포되어야 한다는 교훈을 얻게 되었다.[14]미국 정보기관의 통합을 의한 노력은 아래 <표3.1>에서 보는 바와 같이 제도화 수준이 점차 높은 방향으로 진행될 필요가 있었다.

<표3.1> 정보통합 제도화 수준

구분	낮은 수준의 제도화	높은 수준의 제도화
목적 및 주된 기능	특정 개인 또는 특정 집단의 목적 실현	구성원들의 가치, 비전 등 공유
존속 기간	단명, 리더와 공동운명	지속, 특정 개인과 분리
자생력	부족, 외부 지원에 의존	자기 충족 가능
권한 행사 방식	사적 이용 빈발	권한 위임, 사용 절차의 제도화
조직 내 감시 수단	개인에 의존, 엄격한 규칙	윤리,

13)Johnson and Wirtz(2004), p.7.
14)Ameringer(1990), p.140.

3) 정보협의체

가. 9/11테러와 국가정보장실(ODNI)신설

미국 정보공동체는 9/11사태를 계기로 정보기관 조직, 문화, 운영방식 전반에 걸쳐 광범위한 개혁이 추진되었다. 2012년 상하정보위원회는 9/11테러 공격에 대한 합동조사 보고서와 2014년 9/11위원회 보고서를 발표하였다. 의회는 정보공동체 리더십 확립, 분석 능력 향상, 정보기관 간 정보공유, 시민적 자유, 기타 교육훈련 필요성을 지적하면서 행정부에 개혁을 권고하였다.

의회는 9/11테러 방지 실패 원인이 정보공유와 통합의 결여에 있다고 평가하고 정보공동체에 대한 근본적 개혁을 착수했다. 정보공동체의 개혁은 2005년 신설된 국가정보장실(Office of the Director of National Intelligence, ODNI) 창설로 나타났다. ODNI 창설을 통해 미국 정보체계의 전반에 걸친 시스템과 문화를 개혁하기 시작했다. 즉, 미국은 ODNI설립을 통해 정보기관들의 이기주의나 편협성을 극복하고자 노력했다. 국가안보법에 따라 CIA가 불완전한 IC 수장 역할을 수행한 지 67년이 지나서야 DNI가 기능할 수 있는 법률적·제도적 토대가 형성되었다. 이전에는 1981년 대통령 행정명령 12333에서 중앙정보장(DCI)이 수집·분석·생산 및 배포와 관련하여 IC의 방향설정 권한을 보유한다는 정도의 조정통제 권한을 부여하고 있었다. 이에 반해, 정보개혁 및 대테러 방지법(IRTPA, 2004.12)와 'EO 13470'(2008.7)은 "DNI가 IC 정보업무 관리 및 지휘한다"고 명기하여 DNI의 지휘권을 보다 명확히 하였다. 국가정보장실의 통합권한을 ODNI 지침서를 기준으로 살펴보면 다음과 같다.[15)]

① 미션 매니저 운영 방향 및 역할 : 미션 매니저는 기본적으로 정보공동체 주요 관료들로서 각자 담당하고 있는 지역과 관련된 국가 정보를 총괄하는 임무를 수행한다. 이들은 지역 내 책임이 중첩될 경우 정보공동체 역량 통합 및 효율적인 대응을 위해 협력하도록 하며, 미션 매니저들은 DNI에게 보고하고 국가정보장은 미션 매니저들의 활동을 지시, 감독한다. 미션 매니저들은 정책 입안자들이 필요로 하는 각종 정보를 제공하며 정보 공동체의 활동이 이를 뒷받침할 수 있도록 역할을 수행한다.

미션 매니저들은 대테러, 비확산, 방첩, 이란, 북한, 쿠바, 베네수엘라 지

15)국가정보장실은 최고 책임자인 국가정보장을 비롯하여, 국가정보수석차장, 임무통합 차장, 정책과 역량 차장 등 3명의 차장 직제를 두고 운영되고 있다. https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives(검색일 2021.7.21.)

역을 담당한다. 이들은 수집된 정보의 문제점을 확인하고 극복하기 위해 노력하며 실제 극복하였는지 여부를 평가한다. 또한 분석 상태를 평가하면서 할당된 임무와 관련된 주제에 대한 경쟁력과 대안을 갖춘 분석이 이루어질 수 있도록 한다.
또한, 미션 매니저들은 정보공동체의 수집, 분석, 배포, 정보공유, 대외관계 활동이 효율적으로 진행되는지 여부를 평가하여 연례적으로 국가정보장에게 보고한다.
미션 매니저들은 모든 정보공동체 구성원이 참여하는 화상 원격회의 등을 포함한 정기 모임을 소집, 주재해야 하며 회의를 통해 관련된 모든 정보 소비자들이 만족할 수 있도록 조율하는 기능을 수행한다.
이들 미션 매니저들은 국가 우선정보체계표(NIPF)에 근거하여 분석 및 수집 우선순위를 수립한다. 모든 미션 매니저들은 업무수행을 위해 충분하고 완전한 자료에 접근이 가능해야 한다. 미션 매니저들과 기관 간 정보 접근과 관련하여 이견이 있을 경우 국가정보장은 접근 허용 여부와 접근 정도를 결정해야 한다.

② 인적자원 관리 : 이 지침은 DNI 직속의 센터 및 정보공동체 구성기관 간의 직원 임명 및 임시 파견임무를 원활히 수행하기 위한 인사 정책을 이행하는데 목적이 있다. DNI는 순환보직을 임명할 수 있는데 다른 정보기관에 공석이 있다는 사실을 최소 15일간 공지하고, 공지시에는 직위와 자격요건, 근무 소재지, 파견 임무 기간, 보안 요건 등과 같은 적절한 정보를 알려야 한다. 순환보직에서 복귀하는 직원에 대해서는 이전에 근무했던 보직이나 동등한 직책에 배치해야 한다.

③ 정규직 임명 : 국가정보장실에 근무 예정인 정규직원은 정보공동체 내에서 자격을 구비한 모든 후보들 중에서 공개경쟁을 통해 선발해야 한다. 공개경쟁이 요구될 때 다른 모든 정보기관에 공석 사실을 알리고 모든 기관들은 자격을 갖춘 직원들이 최대한 인지할 수 있는 방식으로 공지한다. 다만, DNI 산하 센터에서 근무할 직원들을 충원할 경우 DNI는 본 지침의 시행일로부터 6개월 동안 정원의 최고 25%를 정규직으로 충원할 수 있으며 반드시 공개경쟁을 통해 선발하지 않아도 된다. 국가정보장실 내 순환보직의 임무 기간은 최소 12개월에서 최대 36개월로 한다.

④ 정보취급 인가와 정보 접근 : 정보 인력의 순환 근무를 촉진하기 위해 모든 정보공동체 소속 기관들은 다른 기관에 의한 정보 취급인가와 정보 접근권 결정을 인정해야 한다. 또 어떠한 기관도 동등한 수준의 보안조사가 이

미 존재할 경우 동일한 조사를 반복할 수 없다.

⑤ 분석 관리·통합 및 감독 : 이 지침은 분석업무의 기본적인 틀을 제공하기 위한 것으로 DNI 분석차장의 권한과 책임을 명확히 하는데 있다. 정보공동체 분석업무는 다음과 같은 방향으로 운영되어야 한다. 정보분석은 정치적 고려를 배제해야 하며, 정보공동체는 정보 사용자 요구 충족을 위해 소속 기관에 상관없이 전문가들을 활용하도록 지원해야 한다. 또한, 정보기관 간 정보협력은 예외 없이 정해진 표준안에 의해 이뤄져야 하며, 분석관 및 수집관간 업무 협조시 기술, 정책, 문화적 장애요소를 최소화해야 한다. 분석관과 수집관간 업무 협조는 필수적이며 분석관은 수집관으로 부터 제공받은 정보에 대한 활용 가치 등 관련 피드백을 반드시 제공해야 한다. 그리고 정보기관들은 모든 분야에 대한 전문가를 채용하는 것보다 외부 전문가 집단과의 교류를 통해 최신 기술과 정책을 받아들여야 한다.
DNI 분석차장은 국가정보 분석보고서의 생산, 배포와 공개여부에 관한 업무를 총괄한다. 정보공동체의 모든 정보 분석에 대한 우선순위를 적시 결정, 지시하는 한편 정보 분석에 필요한 수집, 분석, 처리, 배포와 일반 공개 여부 등을 관장한다.
정보공동체 내 분석 관련 인식의 차이를 확인하고 간극을 감소하는 한편 분석보고서의 생산·배포에 대한 지시와 관리업무를 총괄한다.
분석 능력을 극대화하기 위해 정보수집 능력이 무엇보다 중요한데 수집역량과 이에 관련된 공작활동에 예산이 적절히 편성되었는지에 대해 검토한다. 그리고 대통령 일일보고(PDB) 작성기법, 생산, 배포 보존 및 폐기를 관장하며, 관련 직원들의 관리업무도 병행한다.

⑥ 분석기준 : DNI는 분석업무 역량 강화를 위해 분석관과 관리자들에게 가이드 라인과 목표를 제시는 데 분석 기준을 살펴보면 다음과 같다.

- 객관성 : 분석관과 관리자가 편견에 치우치지 않고 객관적인 관점에서 분석 기능을 수행할 것을 요구한다.

- 정치적 고려로부터 독립 : 분석관과 관리자들은 특정 정책, 정치적 관점, 정치적 선호와 요구에 기초한 분석이 아니라 객관적 평가를 제시해야 한다.

- 적시성 : 분석관은 소비자들이 즉시 분석 결과물들을 활용할 수 있도록 생산물을 적시에 전달하기 위해 노력해야 하며 분석부서는 사용자의 스케줄과 요구사항을 인지해야 할 의무가 있다.

- 활용 가능한 모든 정보출처에 의존 : 분석부서는 적절한 수집, 보급, 접근 전략을 개발하기 위해 수집관과 함께 노력해야 한다.

⑦ 정보수집과 비밀공작의 통합 관리 : DNI는 정보 사용자들에게 시의 적절하고 유용한 국가정보를 제공하기 위해 정보 공동체의 수집능력과 활용을 통합하고 극대화하는데 필요한 정책을 수립해야한다. 또한, 민감한 수집출처를 보호하고 운영상의 위험과 불필요한 활동의 중복 및 정보기관 간 갈등과 혼란을 최소화하며, 모든 수집활동이 국가 정보사용자들의 우선순위에 부응해야 한다. 한편, DNI수집 차장은 미국인들의 기본적인 인권을 보호하기 위해 노력해야 한다. 또한 국가정보 수집과 비밀공작에 관련된 DNI로부터 위임받은 임무를 총괄하며, 정보공동체의 활동이 미국 정보 우선순위에 따라 최대한 효과를 얻을 수 있도록 협력 시스템을 유지해야한다.
그리고 국가정보가 통합적으로 적기에 수집될 수 있도록 지시하고 정보기관들로 하여금 수집업무를 관리토록 지침을 하달한다. 이와 함께 국가정보프로그램(NIP)에 속하지 않는 부문정보기관 구성원들에게 국가정보 수집 임무에 대해 조언한다.

⑧ 정보프로그램 예산 : DNI는 대통령에게 연례 통합 국가정보프로그램 예산안 제출과 관련하여 전반적인 정책방향을 수립해야한다. DNI관리차장은 정보 역량 수준을 확인하고 유지에 필요한 예산이 대통령과 의회에 명확히 전달될 수 있도록 DNI에 보고하고 자문하는 역할을 수행한다.
정보공동체 구성 기관들에 대한 예산안은 DNI 국가정보 전략에 따라 평가되며, DNI는 예산안이 전략목표 달성과 소비자들의 수요 요구를 어느 정도 충족할 수 있는지를 고려하여 승인한다. DNI는 정보공동체 연도별 실행계획을 제출하고 목표 수준과 국가정보 우선순위를 고려하여 예산을 각 기관에 통보한다.
DNI는 예산관리국장의 승인을 거친 예산을 각 부서와 CIA에 배분한다. 그리고 DNI 관리차장은 정기적으로 국가정보프로그램과 군사정보 프로그램의 예산 집행 과정을 검토하며 정보 자원에 대한 적절하고 효율적인 지출이 이루어졌는지를 확인하기 위해 관련 기관들과 협의한다. 정보기관들은 국가정보 예산 관련 자료들을 백악관 예산관리국, 의화와 언론에 배포하기 전에 국가정보장실에 제출, 검토와 허가를 얻어야 한다.

나. 통합을 위한 조직

① 조정 직제의 신설: DNI자문기구로 합동정보공동체위원회(JICC, Joint Intelligence Community Council)를 신설함으로써 DNI의 위상과 권한이 강화되었다. DNI가 JICC 의장이 되고, 국방·국무·법무·재무장관 등 IC의 관련 장관들이 구성원이 되었기 때문이다. 또한, ODNI에 6개 센터[16]가 설치됨으로써 테러리즘을 포함 국가안보 중요사안과 관련하여 정보공동체 구성 기관들에 대해 통합하여 운영할 수 있는 구조가 만들어졌다. 국가정보 관리자(National Intelligence Manager)도 지역별, 요소별로 운영됨으로써 정보통합이 한층 강화되었다.

또한 DNI는 IRTPA 이행을 위해 각종 지침(ICD, ICPG 등)을 정보기관들에게 하달할 수 있는 시스템도 갖추게 되었다. 이러한 조직구조와 시스템들은 DNI가 방대한 IC 조직을 일사분란하게 지휘할 수 있는 운영체제가 갖추게 되었음을 의미한다.

② 국내 정보조정 권한 강화 : 9/11 조사위원회는 과거 국내 정보기관과 해외 정보기관들이 분리 운영된 결과, 정보기관들의 협조가 어려워, 9/11 테러를 사전에 방지할 수 없다는 진단을 내린 바 있다.
IRTPA에서는 정보를 기존 해외정보 이외에 국내정보도 포함하는 국가정보 개념으로 정립하여 DNI가 국내외 정보를 동시에 관장할 수 있는 권한을 부여하였다. 이로써 ODNI 산하 기관들은 물론 정보공동체를 구성하는 정보기관, 법집행 기관들이 국내외 정보를 통합하여 수집·분석할 수 있는 시스템이 구비되었다.

③ 예산 재조정 : DNI는 IRTPA에 근거하여 국가정보프로그램 예산의 책정·집행 및 재조정 권한을 보유하게 되었다. 세부 사업내용에 대해 DNI의 접근이 어렵고 예산 재조정 규모가 미미한 관계로 조정 기능에는 한계가 있다.[17] 그러나, 과거 중앙정보장(DCIA)에 비해 NIP 예산에 대한 DNI의 총괄적인 조정 권한이 강화된 것은 긍정적인 변화로 볼 수 있다. 또한, 초대 DNI 존 네그로폰테 이후 군 출신으로 DNI[18]로 임명된 것은 국방부의 국가정보프로그램에 대한 이해도가 증진된 사실을 의미하는 만큼, 통합 차원에서

16) 국가대테러센터(NCTC), 국가비확산센터(NCPC), 국가방첩및안보센터(NCSC), 사이버위협정보통합센터(CTIIC), 국가정보위원회(NIC), 정보선진화개발프로젝트(IARPA)이다.
17) DNI가 NIP 전체 예산 가운데 1억5천만불(기관별로는 NIP예산의 5%) 이내에서 변경이 가능하다.
18) Mike McConnell(Vice Adm., 07.2~09.1), Dennis Blair(Adm., 09.1~10.5), James Clapper(공군 Lt.Gen., 10.8~17.1).

볼 때 긍정적인 측면으로 이해된다.[19] 국방부 산하 국가정보기관인 NSA, NGA, NRO를 포함하여 군 정보분야 사업내용과 예산편성의 메커니즘을 보다 상세히 이해하게 되었다. 따라서 DNI가 보다 충실하게 정보기관들을 관리·감독할 수 있게 되었다. 군 출신 클래퍼(J. Clapper)DNI가 첩보위성 구입사업을 상업위성 활용으로 재조정하여 NIP 내실을 기함으로써 예산을 절감했던 사례가 대표적이다.[20]

다. 합동정보공동체위원회(JICC)

합동정보공동체위원회(JICC)는 2004년 IRTPA(§1031)에 의해 설립되었다 IRTPA·ICD1에 따르면 JICC는 DNI의 정보 요구사항 수립, 예산 개발, 재정관리, IC 성과 모니터링·평가 등에 대해 조언함으로써 통합적인 국가정보활동을 개발하고 이행하는 기능을 수행한다. 그리고 DNI가 수립한 프로그램·정책·지시를 적시에 이행할 수 있도록 협력, 지원한다. DNI가 위원장인 JICC는 DNI를 위원장으로 하여, 국무·국방·국토안보·법무·에너지·재무부장관과 대통령 지명인사로 구성된다.

JICC는 6개월 마다 정기회의를 개최하기로 되어있었으나 국방수권법2020(§6311)에서 DNI가 적절하다고 판단한 시점에 개최 가능한 것으로 개정[21]하였다. JICC 위원장과 위원의 지위나 성격 그리고 과거 의회의 JICC폐지안 제출사실 등을 고려해 볼 때 JICC의 실효성이 크지 않은 것으로 보인다. DNI가 JICC업무에 전념할 수 있는 시간이 없는데다 정책 결정 및 집행권한을 보유하고 있는 부처 장관[22]들을 정기적으로 소집, 회의를 개최하기란 용이하지 않다가. 뿐 만 아니라 장관들이 정보관련 전문지식이 별로 없고 관심도 높지 않기 때문에 JICC에 대한 호응도도 높지 않는 한계를 보이고 있다.

---

19) Richard A. Best Jr., *Leadership of the U.S. Intelligence Community: From DCI to DNI*, (International Journal of Intelligence and CounterIntgelligence, Summer 2014), p.314.

20)앞의 책. p.314.

21) JICC는 2018년 115대 의회에서 하원이 정보수권법2019(§2304)를 통해 폐지를 추진했으나 상원의 동의를 얻지 못해 무산되었다(https://www.congress.gov/bill/115th-congress/house-bill/6237/text(검색일 : 2021.7.17.). 그러나 하원이 2019년 116대 의회에서 개정안을 재제출하여 국방수권법2020의 일부로 채택되었다.

22) 국방부장관은 1947년 이전부터 행정부에서 행정부 서열이 최고위급에 해당되며 국방부내 정보기관을 총괄하는 기능을 수행하고 있다.

라. 국가정보위원회(NIB)

국가정보위원회(NIB)는 국가정보 생산·검토·조정, 기관 간 국가 정보 첩보 교환 등에 대하여 DNI에 조언하는 기능을 수행 한다. 2004년 IRTPA 제정 당시에 NIB의 사실상 전신이었던 국가해외정보위원회(NFIB)에 대한 조항이 없었다. 2006년 NIB가 신설될 때까지 NFIB는 필요 없는 조직으로 간주되었다. 그러나 IC가 최고수준의 기관 간 조정·자문기구 없이 관리는 불가능하며 미국 정보공동체의 특징을 볼 때 기관 간 위원회가 협력관계가 유지된다 하더라도 통합 위원회 없이 IC를 관리할 수 없다. 이러한 이유로 NFIB의 부재는 오래가지 않았고 2007.1 NIB는 이라크 관련 국가정보판단보고서(NIE)[23]를 생산하게 되었다. NIB는 의장인 DNI와 정보기관장으로 구성되며, 국가정보판단 보고서(NIEs)를 검토하며 NIB의 승인후 대통령과 고위정책결정자에게 보고된다. NIB는 NFIB보다 구성원은 확대되었지만 담당 권한과 임무는 축소되었다. 네그로폰테 DNI는 국가정보위원회(NIC)에 NIB의 행정사무국이라는 새로운 조직을 신설하고 조정 권한은 국가정보차장·차장보급 관리자에게로 이관하였다.

마. IC 집행위원회(IC EXCOM)

2007.3 맥코넬 DNI은 ODNI 조직개편을 발표하면서 IC 집행위원회(EXCOM)를 설립했다.[24]집행위원회는 IC 정책·목표·우선순위 관련 IC역량 확보 등 IC의 리더십·조정·관리를 강화하기 위해 DNI에 조언하고 지원한다. IC EXCOM[25]은 산하기구로 차장급 집행위원회(Deputy Executive Committee : DEXCOM)를 설립하고 EXCOM의 의제를 다루었다.

바. 첩보공유 관련 위원회(ISC, ISPCC, ISCC)

첩보시스템위원회(Information Systems Council : ISC)는 2004년 대통령 행정명령 13356에 의거 설립된 위원회로서 정보기관 간 테러첩보의 공유를 강화하기 위한 기구이다. ISC 임무는 기관간의 테러 첩보의 자동 공유를 촉진하기 위해 상호운용 가능한 테러첩보 공유 환경 구축에 관한 조언과 정보를 제공하고 IRTPA §1016(g)에 명시된 책무[26]를 수행한다. ISC 구성원은 행정명령

23) https://fas.org/irp/dni/iraq(검색일 : 2021.7.14).
24) https://www.dni.gov/files/documents/Newsroom/Press(검색일 : 2021.7.14.).
25) EXCOM은 DNI가 IC의 일상적인 관리와 거버넌스를 위해 의장을 맡고 16개 IC기관 수장, 국방부 정보차관, 합참 정보부장(J-2), PDDNI이 위원으로 되어 있다.
26) 주요 임무를 살펴보면 다음과 같다. 정보공유환경(ISE)의 수립·시행·유지에 필요한 정책·절차·지침·역할·표준 등 개발에 대해 대통령·프로그램 관리자에게 조언하고, ISE의 구축·구현·

13388에 의거 당초 구성단체들이[27]이 변경되어 IRTPA §1016(g)에 의한 프로그램관리자가 위원장을 맡고 국무·재무·국방·상국무부·에너지·국토안보·법무부장관, DNI, DCIA, OMB·FBI국장, 국가대테러센터장 등으로 구성된다. 2005년 부시 대통령은 첩보공유정책조정위원회(Information Sharing Policy Coordination Committee : ISPCC)를 설립하였다. ISPCC는 부처간 첩보공유정책 조정을 위한 주요 일일 포럼으로서 국토안보회의(Homeland Security Council : HSC)·국가안보회의(NSC)에 분석과 권고사항을 제공하고 대응토록 하는 기능을 수행한다. NSC와 HSC가 공동 의장의 역할을 담당한다.

2007년 맥코넬 DNI는 IC 첩보공유 운영위원회(Information Sharing Steering Committee : ISSC)설립했다.[28]. 이는 IC가 첩보를 ' 공유할 필요 '에서 ' 제공할 책임 '으로 전환하기 위한 것으로 ISSC는 IC내에서 첩보공유를 위한 조정 방안을 개발하며 첩보공유 환경(ISE) 구축을 위해 IC 외부 조직과의 첩보 공유를 이행한다. 또한 ISSC 참여자는 정책·예산·프로세스·기술을 포함한 첩보공유 문제에 대해 협업·협력하고, 직접 조치를 취하게 된다.

사. 국가정보조정센터(NIC-C)

맥코넬 DNI은 2007년 국방부 및 행정부처와 협력하여 행정부 전체 정보활동을 조정하는 메커니즘을 제공하기 위해 국가정보조정센터(NIC-C)를 설립했다. NIC-C는 DNI가 미국의 전략적 정보 우선순위에 대응하여 국가 전체의 정보수집 역량을 효율적으로 협업·조정·통합하기 위해 설립되었다. 특히 Humint와 관련해서는 IC수집 역량을 NIC-C로 통합하여 정보·국방·외국·국내 영역 전반에 걸친 전략적 관리를 도모한다. 또한 CIA국장은 국가 휴민트조정관으로서 국가 Humint 수집 역량을 NIC-C로 통합하는 책무를 수행한다.[29]

4) 의회 통제

의회는 기본적으로 정보기관과 그들의 정보활동이 합법적, 효율적으로 수행되는지 여부를 감독하는 역할을 수행한다. 그러한 역할을 수행하는 수단

유지관리에 있어 ISE참여 부처·기관간을 조정한다. 또한 연방 부처·기관이 첩보공유를 위해 사용하는 프로그램·시스템·프로세스의 통합 및 제거를 확인하고, 필요시 기존 자원의 재설정을 권고하는 등이다(IRTPA §1016(g)).

27) 최초 구성원은 관리예산국(OMB)장이 지명한 인물이 위원장이고 국무·재무·국방·상무·에너지·국토안보·법무부장관, DCI, FBI국장, 국가대테러센터장 등이 지정한 자와 기타 OMB국장이 지명하는 자로 구성되었다(행정명령13356).

28) ISSC. https://www.dni.gov/files/documents/Newsroom/Press(검색일 2021.7.14).

29) ICD304 §D.

으로서 의회는 입법권, 예산심의권, 청문회, 임명동의, 정보자료 요구, 조사와 보고 등의 권한을 가진다. 미국 의회의 정보기관 통제에 대한 헌법상의 근거조항은 의회에 입법권을 부여한 헌법 제1조 제8절 제8항 제18호[30]와 의회에 예산권을 부여한 헌법 제1조 제9항 제7호이다. 미국 의회는 입법권과 예산권에 근거하여 청문회와 조사활동을 비롯한 각종 통제수단을 확보하고 통제와 감독기능을 수행한다.[31]

가. 입법권

미국에서도 의회가 모든 입법적 통제권을 보유하는 것이 정당한지에 대한 논란이 없었던 것은 아니다. 그러나, 미국 법원은 “의회가 입법할 수 있는 어떠한 주제에 대해서도 집행부의 보고를 요구할 수 있는 권한을 가진다”고 판시하였다.[32]1972년 워터게이트 사건 재판 등을 통해 CIA가 불법적이고 비윤리적인 비밀공작을 통해 칠레 아옌데 대통령을 살해하는데 개입했다는 사실이 밝혀졌다. 1974.8 닉슨대통령이 사임하는 상황이 발생하면서 정보통제 필요성에 대한 여론이 확산되었다. 이에 미국 의회에서는 1974년 휴즈-라이언 법안을 제정하여 정보기관이 비밀공작을 수행하기 전에 대통령의 승인을 거치도록 했고 ‘적절한 시기’에 의회의 관련 위원회들에 보고하도록 규정하였다.[33]

휴즈-라이언 법안은 불이행시 처벌 조항이 구체적으로 규정되지 않는 등 정보기관에 대한 통제력을 행사하는 데 필요한 내용을 완전하게 구비하지는 않았다. 그러나 최초로 정보기관에 대한 의회의 감독 및 통제 기능을 법률적으로 공식화하였다는 점에서 의의를 가진다.[34]이후에도 미국 의회는 정보기관 통제를 지속 강화하는 조치를 취해 나갔다. 1978년 감청 등 기타 감시활동에 대해 영장심사를 의무화함으로써 부적절한 국내 정보활동을 금지하는 ‘외정보감시법(Foreign Intelligence Surveillance Act, FISA)을 통과시켰다. 이어서 1980년에는 휴즈-라이언 법률안을 수정한 정보감독법(Intelligence Oversight Act)을 제정하여 정보기관에 대한 감독 권한을 보다 강화시켰다. 이 법률에 따라 비밀공작을 포함하여 정보기관의 정보활동 전반을 소위 8인방(Gang of Eight)[35]이라고 불리는 의회의 주요 인사들에게

30) 미국 헌법 제1조 제8항 18호에서 “의회는 앞에 열거된 권한과 이 헌법에 따라 미국 정부와 그 부처와 관료에게 부여된 기타 모든 권한을 실행하는데 필요하고도 적절한 모든 법률 제정권을 가진다.”고 규정하고 있다.
31) 한희원, 국회 정보위원회의 운영과 입법방향에 대한 고찰, 법학연구 제54집, 2014. P.89
32) Lowenthal(2006), p.275.
33)문정인(2002), pp.286-320.
34)문정인(2002). pp.286-310.

보고하도록 규정했다.

이어 1989년 미국 의회는 CIA 감사관법(CIA Inspector General Act)을 제정하여 감사의 권한을 강화한 독립 감사관(Inspector General)제도를 도입하였다. CIA 독립 감사관은 CAI 정보활동을 감사하고 감사결과를 정례적으로 의회에 보고하도록 의무화하였다.[36]1991년 정보수권법(Intelligence Authorization Act)은 그동안 모호하게 규정되어 있던 비밀공작의 개념을 보다 구체적으로 명료하게 규정하고, 비밀공작 추진 시 의회에 사전 보고하는 것을 의무화 하였다. 이로써 정보기관이 비밀공작을 은밀히 추진하고도 이에 대해 의회에 보고하는 것을 의도적으로 회피하려는 기도를 차단하였다.

한편, 2001년 9/11 테러사건 이후 미국 애국법(USA Patriort Act)은 의회의 정보기관 통제활동을 다소 완화시키려는 취지에서 제정되었다. 그동안 의회의 지나친 정보기관 감독과 통제가 국내 전복세력에 대한 감청 등 정상적인 정보활동조차 못했다. 9/11 테러 용의자를 사전에 색출하는 데 실패했다는 지적에 따라 감청 등 기타 감시활동에 대한 FISA[37] 재판부의 영장심사 의무를 한시적으로 완화하는 내용을 포함하고 있다.[38]

나. 예산안 심의권

행정부의 예산안에 대한 의회 심의권은 입법부가 행정부를 견제할 수 있는 강력한 수단이다. 의회는 예산안 심의를 통해 정보기관의 활동을 감시하고 효율성을 향상시키는 역할을 한다. 미국 헌법 제1조 제9절 제7항에는 “법에 의해 정해진 의회의 세출승인 없이는 어떠한 자금도 인출할 수 없으며 모든 공공자금에 대한 정기적 수입·지출 상황과 회계는 수시로 출판되어야 한다.”고 명시되어 있다. 예산 절차는 크게 2가지 절차를 통해 이루어지는데 허가(authorization)와 세출승인(appropriation)이다. 허가는 특정 프로그램 자금 지원을 제시하는 것을 의미한다. 하원과 상원 정보위원회가 정보활동 예산의 주요 허가자이다. 하원과 상원 군사위원회는 일부 국방 관련 정보활동 프로그램을 허가한다. 세출 승인은 허가된 프로그램에서 구체적인 금액을 배당하는 것으로 이루어진다. 하원 및 상원 세출위원회의 국방

35) ‘8인방’은 상·하원 정보위원회 위원장(2명)과 상·하원 정보위원회 소속 의원 중에서 소수당 출신 간사(각 2명), 하원 의장 및 하원의 소수당 대표(2명), 상원의 다수당 대표 및 소수당 대표(2명)을 의미한다(전웅, 2015), p.585.

36) 전웅(2015), p.586.

37) FISA : Foreign Intelligence Serveillance Act(‘해외정보감시법’ 또는 ‘외국정보감시법’), 정식 명칭은 An Act to Authorize Electronic Surveillance to Obtain Foreign Intelligence Information이다.

38) 전웅(2015), p.586.

소위원회가 정보활동에 대해 이 기능을 수행한다. 의회는 처음에 허가하지 않았던 프로그램에 대한 자금을 승인하지 않는다. 의회 회기가 끝나기 전에 허가 입법이 통과되지 못하면 세출승인 법안은 허가 법안이 통과될 때까지 그 법안으로 기능할 수 없다.[39]의회는 예산 심의, 편성 기능을 통해 정보활동에 대한 통제 권한을 가진다. 예를 들면, 1980년대에 의회는 레이건 행정부의 니카라과 정책을 제한하기 위해 정보활동 예산을 이용했다. 의회는 하원 정보위원회 의장인 볼란드(Edward P. Boland) 후원을 받아 니카라과 반정부 세력인 콘트라에 대해 자금 지원을 거부하는 일련의 개정안을 통과시켰다.

다. 조사와 보고

대부분 민주주의 국가에서 의회는 행정부의 정책이나 활동에 대해 조사하고 결과를 보고받을 권한을 가진다. 의회의 정보기관 통제와 관련하여 의회는 각종 위원회를 구성하여 정보활동의 효율성과 합법성, 그리고 인권 남용 여부를 조사한다.[40]예를 들어, 한국의 국회도 정보기관이 정치에 개입하거나 대북 정보실패가 발생할 경우 국정원에 자료를 요구하거나 관련 사실들을 조사한다. 2001년 발생한 9/11 테러 사건 이후 미국 의회에서는 공화당과 민주당 양당 동수로 추천한 전문위원 10명으로 9/11 진상조사위원회[41]를 구성하였다. 조사위원회는 1년 8개월 동안 조사활동을 전개하여 마침내 9/11 Report를 발간했다. 2004년 부시 대통령이 이라크 WMD(대량살상무기) 정보오류를 포함한 미국의 정보능력을 조사할 특별조사위원회(The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction)를 구성했다. 위원회는 베트남 참전군인인 찰스 롭(Charles S. Rob, 민주당) 전 버지니아 상원의원 겸 주지사와 닉슨·포드 대통령 시절 법무장관을 역임한 로렌스 실버먼(Laurence H. Silberman, 공화당)이 공동위원장에 임명되었고, 나머지 초당적 인사 7명을 포함하여 9명으로 구성되었다.[42] 위원회는 2005.3 총 692쪽에 달하는 최종 보고서를 발간했는데, 여기서 미 정보공동체의 이라크에 대한 WMD 정보판단은 '치명적인 실패'로 규정했다.[43]의회의 정보역량 강화를 위한 방안으로

39) Lowethal(2012), p.277.
40)전웅(2015), p.592.
41)National Commission on Terrorist Attacks upon the United States, 일명 9/11 Commission.
42)서울경제 2004.2.9.자
43)The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, Report to the President of the United States*March 31, 2005), http://whitehouse.gov/wmd : 전웅(2015), p.593.

정보위원위원들의 임기가 제한하는 방안이 논의되었다. 감독기관인 정보위원회와 대상기관인 정보기관 간에 유착관계를 방지할 수 있고 다양한 의원들이 정보위원회 활동 경험을 가질 수 있다는 장점이 있다. 반면에 대부분의 의원들은 정보에 대해 문외한 이거나 경험이 없어 정보 통제에 대한 전문성이 미약할 수 밖에 없다. 더욱이 비밀성을 중시하는 정보통제는 공개성과 투명성을 강조하는 의정활동과는 양립하기 어려운 측면이 있다.

라. 기타 권한

미국 의회 정보통제 과정에서 하원이 중요한 역할을 수행하고 있는데 18개 정보기관의 정보 및 정보 관련 활동에 대한 통제 업무를 수행하고 있다.[44]하원 정보위원회 소관사항은 첫째, 중앙정보국(CIA) 및 중앙정보국장, 국가보안법 제3조 제6항에 규정된 국가해외정보계획(NFIP)에 대한 감시와 통제업무를 수행하고 있다. 둘째, 연방정부와 산하 기관의 정보 및 정보관련 활동(예를 들어 국방부의 전술정보 및 정보관련 활동 포함[45])에 대한 정보통제를 실시한다. 셋째, 연방정부의 정보 및 정보 관련 활동과 관련한 조직 구성 및 개편에 관한 사항, 그리고 연방정부의 정보 관련 활동에 대한 직·간접적 지출승인에 대한 권한을 보유하고 있다.[46]

정보위원회는 연방정부 기관의 정보 및 정보 관련 활동에 관한 정기 보고서를 하원에 제출할 책임을 지며, 정기보고서 작성에 있어서 정보위원회는 국가기밀유지 의무를 준수해야 한다. 또한 정보위원회는 중앙정보국장,국방부장관, 국무부장관, 연방수사국장으로부터 보고를 받는다. 위원회 보고서에는 관계기관의 정보 및 정보관련 활동과 미국과 정보협력 관계에 있거나 관심의 대상이 되는 외국의 정보기관 및 정보 활동에 관한 검토 사항이 포함되어야한다.

---

44)https://intelligence.house.gov/(검색일 : 2021.10.1.).

45)정보 및 정보관련 활동은 ① 외국이나 외국의 특정 정부·정치집단·정당·군대·운동단체 및 여타 단체에 관한 정보로서 미국의 국방정책·외교정책·국가안보와 관련한 정보의 수집·분석·제공·배포·이용 및 이러한 활동을 지원하는 기타의 활동, ② 미국을 겨냥한 유사한 활동에 대응하기 위한 활동, ③ 미국과 외국의 특정 정부·정치집단·정당·군대·운동단체 및 여타 단체와의 관계에 영향을 미치는 비밀활동, ④ 미합중국본토·준주·속령에 거주하는 자 또는 해외거주 미합중국국민으로서 그들의 정치활동이나 정치관련 활동이 미합중국의 국내안보에 위협이 되는 것으로 연방정부부처, 각 기관 및 공무원들이 판단하는 자들의 활동에 관한 정보의 수집·분석·제공·배포·이용, ⑤ (E)D목에 규정된 자들에 대응한 비밀활동 등을 의미한다.(「하원의사규칙」제10장제11조(j)(1))

46) 하원의사규칙 제10장 제11조 (b)(1)

마. 정보위원회 운영실태

정보위원회는 다양한 수단들을 활용하여 정보기관의 권력남용 또는 불법적이고 비윤리적인 정보활동을 감시하며, 나아가 정보활동의 효율성을 제고하도록 유도하는 등의 역할을 수행한다. 정보기관의 정보활동은 대부분 국가의 안보와 관련된 사안이다. 그런데 정보위원회가 당파성을 극복하지 못하고 여야 간 각기 상반된 견해를 제시하면서 충돌하는 경우가 빈번하게 발생한다. 대체로 상원이 초당적으로 정보위원회를 운영하는데 반해 하원은 당파성이 강한 것으로 알려졌다.[47)]

정보공동체에 관한 정보는 정보위원에만 배포되고 엄격히 통제된다. 정보위원회는 행정부로부터 엄청난 양의 정보를 제공받고 있다. 그런데, 엄격한 보안이 요구되는 정보는 정보위원회 소속 의원들에게조차도 배포되지 않는다. 대통령은 비밀공작을 시행하기 전에 의회에 사전에 통보하도록 법률에 규정되어 있지만 배포범위는 의회 정보위원회 위원장, 상·하원 양원의 다수당 및 소수당 대표 등을 포함한 8명으로 제한된다.[48)]정보위원회 회의는 대체로 비공개를 원칙으로 하며 위원들은 위원회에서 보고 또는 논의된 내용에 대해서 비밀을 엄수해야 한다. 위원회에서 보고 또는 논의된 내용을 대외적으로 발표하고자 할 경우 위원회 결의를 거친 후 해당 정보기관의 동의를 얻어 위원장이 발표하게 된다.

47) Lowenthal(2006) p.212.
48) 전웅(2015), p.596.

2. 영국의 정보협의체와 정보통제

1) 정보체계

영국 정보기관의 기원은 엘리자베스 1세 당시인 1573년 월싱햄 경(F. Walsingham)이 설립한 비밀조직에서 찾아 볼 수 있다. 월싱햄은 비밀조직을 활용하여 스페인의 무적함대를 격파하고 영국은 해양강국으로 성장하게 되었다. 비밀정보조직은 1584년에 스코틀랜드의 메리 여왕이 엘리자베스 1세의 암살모의에 연루되었다는 사실을 조사하는 등 왕실 보호에 주력하는 역할을 수행하기도 했다. 이후 영국의 위상은 세계를 지배하는 국가로서 인식되었으며 국가정보기관의 중요성이 한층 강조되기 시작하였다.
이후 20세기 유럽대륙은 두 차례의 세계대전을 거치면서 영국의 정보기구는 급속히 발전하게 되었다. 1차 대전 중 영국의 비밀정보업무는 군사정보(Military Intelligence: MI)[49]기관을 위주로 이루어졌으며 이후 민간정보기구로 전환되었다. 전쟁종료후 MI5와 MI6은 각각 국내와 해외정보를 담당하였으며 정부통신본부(GCHQ)는 MI1(암호해독), MI8(군사감청), MI13(정찰)업무를 흡수하여 신호정보기구로 창설되었다. 현재 영국의 정보공동체는 합동테러분석센타(Joint Terrorism Analysis Center: JTAC)를 비롯하여 비밀정보부(MI6), 보안부(MI5), 국방정보참모부(DIS)로 구성되어있으며 법집행기관에 대한 지원과 상호협력이 강조되고 있다.

가. 비밀정보부(Secret Intelligence Service, MI6)

비밀정보부는 외무·연영방부 소속 해외정보기관으로 1909년 창설되었으며 1·2차세계대전중에는 대독일 정보활동에 치중해오다가 전후에는 미국과 정보협력을 통해 소련 등 공산주의국가들의 팽창과 공작활동에 대응하는 정보활동을 전개했다. 냉전종식후 러시아에 대한 정보활동보다는 지역 불안정, 테러, WMD확산 등에 대한 정보활동을 전개하였으나 이라크의 WMD에 대한 정보실패로 조직 개혁을 단행한 것으로 알려져 있다. 현재 비밀정보부의 활동방향[50]을 살펴보면 국가안보에 위협이 되는 대테러활동, 대량살상무기확산 방지, 세계지역의 불안정과 갈등문제, 사이버안보에 집중하고 있다. 비밀정보부의 존재는 2006년 정보요원 인터뷰 등을 통해 일부 공개되고 있지만, MI5와는 달리

49) 대표적으로 MI5:국내, MI6:해외, MI2: 러시아, MI3: 동유럽, MI14, MI15: 독일제국 전담, MI7: 항공정찰, MI10:무기분석, MI19: 전쟁포로 심문 등이 있다. 한희원, 『국가정보체계혁신론』(서울: 법률출판사, 2009), p.81.
50) https://www.sis.gov.uk/our-mission.html(검색일: 2021.7.15)

여전히 베일에 쌓여있다고 볼 수 있다. 1994년 정보서비스법(Intelligence Service Act)이 의회에서 제정됨으로써 법적 근거를 확보하게 되었다. 동법 제1조에 따르면 비밀정보부의 역할은 영국의 영토 밖에 있는 인물들의 행동과 의도에 대한 정보를 수집·제공하며, 국방 및 외교정책과 관련된 국가안보 이익, 영국의 경제적 이익 중대 범죄의 예방과 적발을 위한 업무를 수행하는 데 있다.[51]

비밀정보부의 조직[52]을 살펴보면 정보수장 아래 4개의 부처 즉 ①인사/행정처(Personnel and Administration) ② 특수지원처(Support Service) ③ 방첩 및 보안처(Security and Counter-Intelligence) ④ 정보요구 및 생산처(Requirement and Production)가 있다. 특이한 점은 정보요구 및 생산처 산하에 해외공작을 감독하는 지역별 7명의 감사관(영국, 유럽, 러시아, 아프리카, 중동, 극동, 서반구)이 있다는 사실이다. 이후 2004.8 스칼렛 부장취임을 계기로 버틀러 위원회에서 제기한 이라크 정보실패를 계기로 대테러·공작역량 강화를 위한 조직개편이 이루어진 바 있다.[53]기존 4개처 이외에 공작지원처와 정보감사관실 직위를 신설하고 인력재배치를 단행한 것으로 알려졌다. 아울러 지역별 부서가 국제 테러, WMD 및 국제 범죄와 같은 글로벌 이슈가 새로운 정보 현안으로 부상함에 따라 각 지역부서별 활동은 축소되고 기능별 활동이 부각되는 방향으로 조직이 개편되었다.

나. 보안부(Security Service, MI5)

보안부는 내무장관 직속으로 대간첩, 대테러활동 등 국내보안업무를 수행하는 기관으로 1909년에 군내에 설립된 비밀정보국이 해군과(해외첩보)와 육군과(국내방첩)로 분리된 이후 육군과가 보안부로 발전하였다.

설립 초기 보안부는 경찰과 합동으로 외국 간첩을 색출하는 역할을 수행하였으며 2차 대전 이전까지 활동영역을 급속히 확대되었다. 공산주의자나 파시스트들에 의한 내부전복 위협 뿐 아니라 소련과 나찌 독일의 간첩활동에 대응하면서도 평화주의자나 노동조합의 활동에 대한 분야까지 담당해왔다. 영연방 전역에 걸쳐 보안 정보활동을 확대했으나 의회에 의한 정보통제는 제대로 이루어지지 않았다. 이후 수상직속에서 내무장관으로 소속이 변경되고 소련의 부상, 북아일랜드 독립, 국제테러에 대한 새로운 도전에 직면하게 되었다. 1989년에 보안서비스법(Security Service Act 1989)이 제정되고 1994년에 정보서비스법

51)한희원(2009), pp.330-338.
52)김왕식, “영국 보안부와 비밀정보부의 조직과 양상,” 『국가정보연구』 제4권 제1호(2011), p121.
53)제성호, “영국의테러방지법과 테러대응기구,” 『저스티스』, 제114권 제1호(2009), p.283.

(Intelligence Service Act)이 제정되면서 법적 기반[54]을 갖추게 되었다.
냉전이후에는 대테러활동범위가 확대되었다. 북아일랜드 테러증가로 2007년 북아일랜드에서 정보활동을 수행할 수 있는 권한을 보유하게 되었으며 9/11테러 이후 이슬람테러주의자에 대한 감시를 비롯해 다양한 형태의 대테러 정보활동을 전개하고 있다. 한편. 2000년 조사권한규제법(Regulation of Investigatory Powers Act)제정으로 법적 준수를 강하게 요구되고 있는 실정이다. 보안부[55]는 해외정보기관인 SIS와는 달리 국장의 신원까지 밝히는 등 상대적으로 투명한 활동을 전개하고 있으며 테러리즘, 스파이, 사이버위협과 대량살상무기 확산을 영국의 주요 위협요인으로 평가하고 있다. 한편, 합동테러위원회는(JTAC)은 블레어총리의 행정명령에 의해 SS, SIS, 경찰, 외교부 등 16개 정부부처 기관들로 2003.6에 설립된 테러 전문 정보협의체이다.
주요 임무로는 국내외 테러리즘에 대한 종합분석 및 평가를 들 수 있다. 협의체는 보안부장에게 책임을 지지만 기구상으로는 독립적인 지위에 있으며 경찰청과 밀접한 협조관계를 유지하고 있다. 또한 2007.2 국가 기반보호센타(CPNI)를 설립하였는데 여기서는 국가 핵심시설에 대한 보호와 보안에 대한 정책적 조언을 제공하고 취약점을 분석한다.

한편, 각 부서에는 관리위원회(Management Board)가 있으며 이들은 정기적으로 회의를 통해 정책과 전략이슈들을 논의하는데 보안부 활동의 우선순위와 제반 위협의 변화를 반영하여 조직의 변화, 적응의 방법을 결정한다. 현재 인원은 약 4,000여명으로 이중 40%가 여성이며 직원 과반수이상이 40세 이하이며 흑인과 소수인종이 8%, 장애인 3%로 구성된 점도 특이하다. 주요 업무 우선 순위를 보면, 대테러, 방첩 및 반확산, 북아일랜드 관련 테러대비 업무인 것으로 알려져 있다.

다. 정부통신본부(Government Communication Headquaters: GCHQ)

정부통신본부(GCHQ)는 비밀정보부(SIS)와 함께 외무·연방부 산하 정보기구로 1919년 창설된 정부암호학교(Government Code and Cipher School)가 전신이다. 2차 세계대전 중 독일의 암호체계인 에니그마를 해독하는 성과를 보였으며 전쟁 종료 후 1946년 정부통신본부로 확대 개편되었다.
정보통신본부는 내각과 군지휘관들에게 국방과 외교 그리고 경제정책과 관련

54) 보안서비스법 1조에서는 SS임무를 국가안보수호, 간첩 및 테러와 태업으로부터 위협, 해외세력으로 부터의 위협, 정부를 전복하거나 의회민주주의를 손상시키는 행위로부터 보호, 해외세력으로부터 대영제국의 경제적 복지의 수호로 규정하고 있다, 정보서비스법은 SS를 비롯하여 SIS, GCHQ의 감독과 감독 에 대한 조문을 제정하였다.한희원(2009), pp.324-338.
55) https://www.mi5.gov.uk (검색일:2021.7.14.).

정보를 제공한다.[56]또한, 보안부 산하 국가기반보호센타(CPNI)에 기술적 조언을 제공하는 한편, 국내외에 기지국을 건설하여 신호정보를 수집하고 있으며 미국과 함께 감청 기구인 에셸론(ECHELON)을 운용하고 있다.
정보통신본부는 두개의 주요 부서로 구성되어 있는데, 정보수집을 담당하는 CSO(Composite Signals Organization)와 통신보안을 담당하는 CESG(Communications-Electronics Security Group)이다. 한편, GTLS(Joint Technical Language Service)이라는 소규모 부서도 있는데, 주로 정부 기관에 대해 전문 용어의 번역 및 해석 지원을 담당하는 범정부적 조직이다

라. 합동정보위원회(Joint Intelligence Committee)

영국의 정보시스템은 보안부(SS), 비밀정보부(SIS), 정부정보통신본부(GCHQ), 정보참모부(DIS)를 중심으로 이루어져 있다. 보안부와 비밀정보부가는 설립이후 외무장관과 내무장관에게만 각각 보고해왔으나 9/11테러이후에는 합동정보위원회(JIC, Joint Intelligence Council)와 총리에게도 보고하는 체제로 전환하였다. 또한 2003년에는 정보기관, 경찰, 행정부처 등 16개 기관이 참여하는 정부합동테러분석센터(JTAC, Joint Terrorism Analysis Center)를 설치하여 정보통합성을 강화하였다.
합동정보위원회(JIC)는 1936년에 창설되어 정보조정기구(Intelligence Coordinator)로서의 기능을 수행해왔다. 정보공동체의 수장과 평가 참모단, 외교부, 내무부, 재무부, 국방부, 국제개발부, 내각사무처 등에서 파견된 고위관리들로 구성되며 매주 정기회의를 개최하고 있다. 내각사무처의 조직에 의해 지원을 받고 있으며 그 역할을 살펴보면 아래와 같다.[57]

- 비밀정보, 외교보고, 공개정보 등을 통해 외부 사건, 국방, 테러, 국제범죄활동, 과학적, 기술적 그리고 국제 경제문제와 초국가적 이슈와 관련된 사건이나 상황에 대한 평가
- 국제사회와 영국의 이익 및 정책과 관련한 직·간접적인 위협과 기회에 대한 감독 및 조기경보
- 국내·외 안보위협 점검 및 이에 연관되는 안보 이슈를 검토

56) 한희원(2009), pp.334-335.
57) https://www.gov.uk/government/groups/joint-intelligence-committee#contents (검색일 : 2021.7.15)

- 정보기관들이 정보수집과 활동을 위한 요구와 우선순위에 대한 지시를 이해하고 수행하도록 권고
- 정보분석가들을 통해 정보공동체의 분석능력에 대한 감독을 유지하거나 영국 및 외국 정보기관과 연락체계를 유지

JIC의 기능은 총리와 장관들에게 국가 안보목표를 위해 정보수집과 분석의 우선순위 조언하고, 정기적으로 정보기관에 부여된 수집요구와 관련하여 기관들의 성과를 조사하는 한편, 정보분석가들에 대해 분석 기준을 제시하는 것으 정리될 수 있다.[58)]

보증 이처럼 JIC는 정보기구들에 대해 업무와 전략에 대한 지시와 통제업무를 담당하며 총리와 내각, 고위공무원들에게 평가한 국가정보를 제공하면서 정보기관간 업무내용을 조정하여 중복업무를 방지하고 있다. 한편, 깁슨(S.D Gibson)은 영국정보시스템의 미래역할에 대해 다음과 같은 주장을 하고 있다. 영국 정보기관의 3가지 주요 역할로 전통적 방식에 의한 전략평가, 테러와 국제범죄조직을 감시하는 세계경찰 역할, 대테러를 위한 타국가 지원능력 지원을 제시한 바 있다.[59)]

2) 의회 통제 : 정보보안위원회(Intelligence and Security Committee)

정보기관에 의한 통제는 내각에 의한 통제와 의회의 정보보안위원회에 의한 통제로 대별된다. 또한, 정보기관 법률인 보안서비스법(1989)과 정보서비스법(1994)에 의해 정보기관에 대한 통제를 실시하고 있다. 뿐 만 아니라 2000년 제정된 조사권한규제법(Regulation of Investigatory Power Act 2000, RIPA)에 의해 특별법원을 설치하여 하여 정보활동을 통제하는 등 정보기관의 불법, 일탈 활동을 최소화하는데 주력하고 있다. .

의회통제가 중요한 만큼 정보보안위원회(Intelligence and Security Committee:ISC)를 중심으로 살펴본다.[60)]1994년 정보서비스법에 의해 설립되어 정보기관의 예산지출, 행정 및 정보활동을 감사하여 활동결과를 매년 총리에게 보고한다. 위원회는 상하원 9명의 위원으로 구성되며 이들은 야당당수와 협의하여 총리가 임명하고 정기 및 수시 보고서를 작성하여 총리에게 보고하고 총리는 보고서를 의회에 제출한다. 2013년 사법보안법(The Justice and Security Act)

58) https://en.wikipedia.org/wiki/Joint_Intelligence_Committee(검색일 2020.5.11)
59) Gibson, S.D, 「Future role of the UK intelligence system」, 『Review of International Studies』,vol.35 No 4, 2009
60) http://isc.independent.gov.uk/(검색일:2021. 9.30)

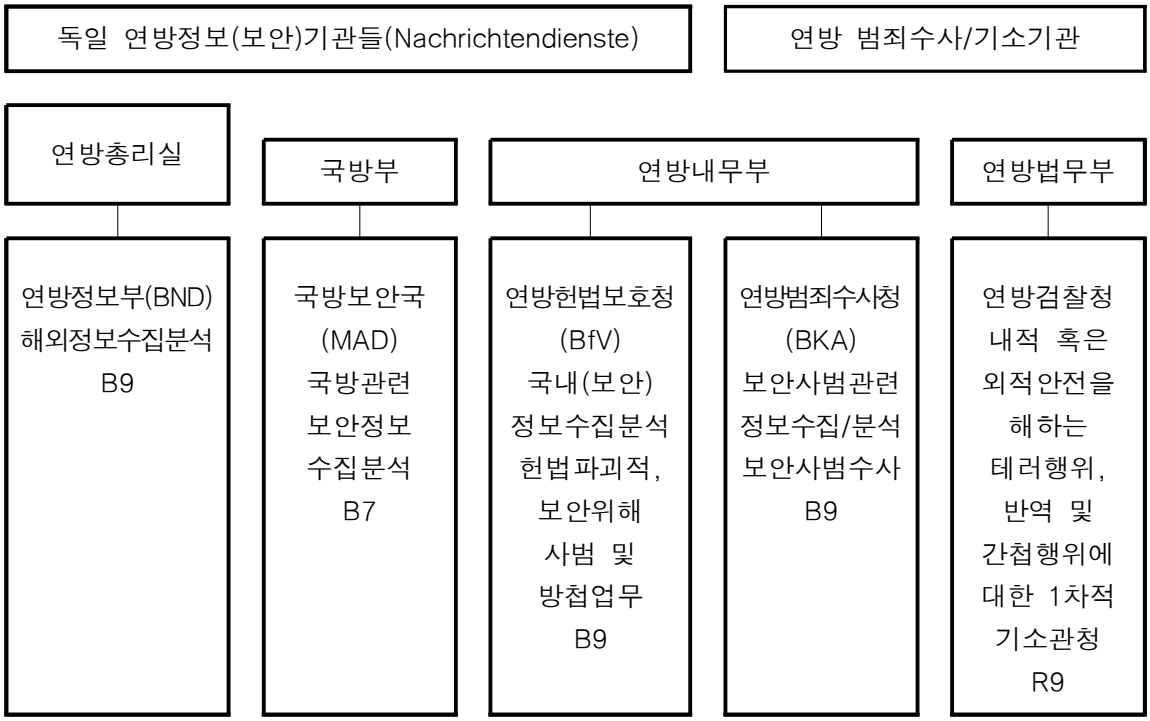
울 제정하여 정보기관과 정부의 정보 및 보안활동에 대한 감독권한을 포함하여 업무범위를 확장하였는데, 정보기관 이외 JIC, 평가요원, 국가안보국장들을 포함한 광범위한 감독권한을 행사하고 있다. 위원회는 의회에 직접 보고하고 민감한 사안에 대해서는 총리에게 보고하고 내용 일부를 삭제하여 다른 의원들도 열람토록 의회에 비치한다.

3. 독일 정보공동체와 정보통제

1. 정보체계[61]

2차 대전 이후 독일의 정보기관들은 견제와 균형을 유지하고 적절한 역할 분담을 하고 있어 정보활동과 조직운영에 있어 모범이 되고 있다. 독일의 정보기관은 연방총리실(Kanzleramt) 소속의 연방정보부(BND), 연방내무부 소속 외청인 연방헌법보호청(BfV), 국방부 소속의 국방보안국(MAD) 등이 있다. 정보보안기관들은 연방하원 정보감독 위원회(PKG)의 감독을 받고 있으며 이들 정보기관들은 강제 수단이나 법집행권한이 없다. 이는 과거 나찌 독재정권시절 정보기관에 권력이 과도하게 집중되었던 것과 같은 폐해를 방지하기 위해 2차 대전이후 정보기관에 수사권과 집행권한을 부여하지 않았다.

<그림3.2> 독일 연방정보 및 수사 체계



61) 임준태, “독일 정보기관의 직무영역과 법적 토대에 관한 연구”,「한독사회과학논총」 제20권 제1호, (2010)

가. 연방정보부(Bundesnachrichtendienst, BND)

독일 연방정보부은 수상 직속기구로서 연방차원의 정보수집·분석 및 공작을 담당하는 정보기관으로 산하 12개의 국으로 구성되어 있다.[62]해외정보기관이지만 해외 뿐 아니라 국내에도 지부를 운영하고 있다. BND는 민간 분야 첩보는 물론 군사 분야의 첩보들도 수집하고 있다. 구체적으로 연방정부의 해외 특수임무 수행(인질구출 등), 대간첩 업무, 산업정보수집, 국제 테러리즘, WMD 확산, 첨단기술의 불법 유출, 조직범죄, 불법무기 및 마약 거래, 자금세탁, 불법 이민, 정보전 등의 업무를 담당하고 있다. 특히, 독일 통일 이후에는 구 동독 정보기관인 슈타지(Stasi)청산 업무도 수행한 바 있다.

히틀러 집권 당시 나치 치하에서 게슈타포의 통제와 박해를 경험했 때문에 대부분의 서독 국민들은 스파이활동에 대해서 부정적인 인식을 갖고 있었다. 이에 따라 초기 BND의 정보활동은 주로 소련과 폴란드, 체코슬로바키아, 헝가리, 유고슬라비아 등 동유럽 국가들을 주요 목표로 제한하여 임무를 수행하였다. BND는 독일군의 협조를 얻어 동유럽 지역 내 소련과 동구 공산국가들에 관한 신뢰성 있는 정보를 수집하였다. BND정보는 NATO에 대한 소련군의 군사작전에 대한 대응하기 위한 경보체계(warning system)를 수립하는데 중요한 역할을 담당했다. 한편 BND는 정보역량 제고를 위해 엄격한 간부 임명 기준과 정치적 중립성 확보 방안을 제시하고 있는데 주요 내용을 살펴보면 다음과 같다.

- 정보부서의 책임자는 해당분야 유경험 인사(법률가, 경찰, 연방정보부, 헌법보호청, 내무부, 외교분야 등)가운데 임명.
- 임기는 법률상 규정된 것은 없으나 관례상 5년간 근무.
- 정권이 교체되어도 과거 집권정당에 의해 임명된 부서책임자를 곧바로 교체하지 않음. 1998년 전후 기독민주당 정부에서는 야당출신 인사를 정보책임자로 임명.

---

62) 12개국은 총괄지원국(Gesamtlage/FIZ und Unterstützende Fachdienste: GU), 작전지원 및 연락국(Operative Unterstützung und Liason: OL), 기술지원국(Technische Aufklärung: TA), A지역국(Länder Region A: LA), B지역국(Länder Region B: LB), 테러담당국(Terrorismus: TE), 확산 ABC- 무기국(Proliferation ABC-Waffen: TW), 보안·간첩방첩(Eigensicherung: SI), 정보기술국(Informationsthechnik: IT), 총무국(Zentralabteilung: ZY), 인사국(Innerer Dienst: ID), 조직이전·건축국(Umzug)이 있다. [출처 : 김현우, “독일 정보기관의 대테러정책에 대한 의회의 통제방안 연구”, 「한국테러학회보」 제11권 제4호(2018. 12), p.187.

- 야당출신의 정보부장 임명은 초당적 차원에서 협력한 좋은 사례이며, 이러한 관행을 통하여 정보기관 수장의 전문성과 직무 연속성을 확보.

연방정보부가 임무를 수행하는 과정에서 특별한 경우 정보기관으로의 역할을 넘어서서 경찰권을 행사할 수 있는지의 여부가 문제가 된다. 이에 대하여 연방정보부법 제2조 제3항은 “연방정보부에는 경찰의 권한 또는 지시권이 인정되지 아니한다. 연방정보부는 경찰에 대하여 업무협력의 방식으로 원래 연방정보부가 처리할 권한이 없는 처분을 요청해서도 안 된다”고 명시하고 있다. 따라서 연방정보부는 순수한 정보기관이며 연방의회로부터 감독을 받고 있으며 규정에 따른 의무를 충실히 이행해야한다.

나. 헌법보호청(Bundesamt für Verfassungsschutz, BfV)

독일 헌법보호청은 국내 정보를 수집·평가하는 정보기관으로 연방헌법보호청과 주헌법보호청이 있으며, 8개 국으로 구성되어 있다.[63]연방헌법보호청의 주요 기능을 보면 다음과 같이 정리될 수 있다. 첫째, 자유와 민주주의 기본질서 또는 연방정부의 존립에 위협을 가하는 행위와 연방헌법보호청의 기능을 불법적으로 약화시키는 행위, 둘째, 독일의 안보를 위태롭게 하는 행동 및 스파이활동 등 이적행위, 셋째, 독일의 국제적 이해와 국익을 위태롭게 할 수 있는 폭력행위, 넷째, 국가 안전을 침해하는 활동에 관한 정보로서 물적·인적 정보, 비밀정보 및 문건 등에 대한 정보를 수집·평가하는 것이다.[64]

헌법보호청은 간첩행위, 반국가활동 등 자유민주주의적 질서를 파괴하는 세력들에 대한 감시를 통해 국가안보 위해요인을 조기에 탐지·예방하고 헌법질서를 수호하는 임무를 수행하고 있다. 역사적으로 1972년 뮌헨 올림픽 테러사건을 계기로 헌보청법을 확대 개정하여, 외국인 과격단체에 대한 동향파악 과 감독임무를 수행하게 되었다. 냉전시대 동안 헌보청의 주요 임무는 서독 내에서 암약하던 동독 스파이들을 추적하고 색출하는데 역점을 두었다.

---

63) 8개국의 주요 담당 업무는 제1국의 총괄(Grundsatz) 업무를 비롯하여, 제2국인 극우주의·극우테러(Rechtsextremismus/-terrorismus), 제3국인 중앙전문지원(Zentrale Fachunterstützung), 제4국인 간첩방첩, 비밀보호·사보타지보호(Spionageabwehr, Geheim- und Sabotageschutz), 제5국인 외국인 혐오 및 극좌주의(Ausländer- und Linksextremismus), 제6국인 이슬람주의·이슬람테러(Islamismusund islamistischer Terrorismus), Z국인 중앙총무(Zentrale Dienste), IT국인 정보기술 및 특수기술(Informations- und Sondertechnik) 업무를 담당하고 있다. [출처 : 김현우, “독일 정보기관의 대테러정책에 대한 의회의 통제방안 연구”, 「한국테러학회보」 제11권 제4호(2018. 12), p.189.]

64) 전웅(2015), pp. 451-453.

그러나 동독과 구소련이 해체되면서 헌보청의 정보활동은 독일 내 극좌 또는 극우 급진주의자들을 대상으로 확대되었다. 이에 따라 헌법보호청은 극좌 공산주의자, 신나치주의 극우파, 이슬람 극단주의자들, 테러단체, 조직범죄 등의 동향을 파악하고 그들의 헌법질서 파괴 행동에 대응하는데 많은 노력을 기울이고 있다. 또한, 헌보청은 관련 정보를 조사할 수 있으나 연방헌법보호법에서 규정한 사생활이나 인권침해 금지와 같은 특별 규정을 위반하지 않아야 한다. 헌법보호청은 다양한 정보 수집수단을 활용할 수 있다. 예를 들면, 정보원의 투입, 관찰, 사진촬영, 녹음녹화, 위장신분증, 위장문건 등과 같은 비밀리에 정보를 수집하기 위한 방법, 물건 및 도구를 사용할 수 있다. 그러나 개인의 권리에 대한 침해는 특별한 권한의 기준에 따른 경우에만 가능하다.

그러나 연방헌법보호청 뿐만 아니라 주헌법보호청도 경찰의 권한이나 수사권을 보유하지 않고 있으며, 경찰에 대하여 처리할 권한이 없는 처분을 요청해서도 안 된다.

다. 군사방첩국(Militärischer Abschirmdienst, MAD)

군방첩기관으로 독일 국방부산하의 군 관련 정보를 수집, 분석하는 정보기관이다. 연방 국방부와 육·해·공군 등 각 군 정보기관의 협력을 통해 군사 부문 정보활동을 수행한다.[65]MAD는 연합군과 독일 정부 간 연락사무소에 기원을 두고 1956년에 창설되었다. 1986년까지는 연방군 보안국(ASBw)으로 알려졌는데, 1990년 군사보안국(MAD)으로 개칭하고 활동 영역도 확장되었다. MAD는 외국 스파이 및 국내 안보 위해 극단주의(주로 좌익) 세력의 연방군에 대한 침투 공격을 차단하고, 군사분야 활동 요원들에 대한 보안감사 및 감찰활동 등을 주요 임무로 수행하고 있다.

라. 연방총리실 정보업무조정국(Abteilung VI)

독일의 정보활동 통합을 위한 기구는 연방총리실 장관 산하 정보업무조정국(제6국:Abteilung VI)이 있다. 조직은 2개 부와 5개과로 구성되어 있으며 연방정보부를 비롯한 정보기관들의 업무를 조정·감독한다. 이들 기관들은 연방정보부의 예산과 하원정보감독 위원회에 대한 업무를 담당하고 있다.

---

65) 4개국 업무는 제1국인 총괄, 법, 정보수집수단(Grundsatz, Recht, nachrichtendienstliche Mittel), 제2국인 극우주의, 테러리즘, 간첩, 사보타지(Extremismus-, Terrorismus-, Spionage- und Sabotageabwehr), 제3국인 외국에서의 정보수집(Einsatzabschirmung), 제4국인 인적/물적 비밀·사보타지의 방지업무를 담당하고 있다. 김현우, “독일 정보기관의 대테러정책에 대한 의회의 통제방안 연구”, 『한국테러학회보』 제11권 제4호(2018. 12), p.191.

한편, 최근 독일은 핵심안보 이익 위협 대응하여 법률이 정하는 범위 내에서의 광범위한 활동을 용인하는 경향을 보여주고 있다. 대테러·사이버 등 초국적 위협이 확산되면서 냉전기 국가로부터 위협과 다른 유형에 대응하기 위해 정보기관의 활동을 폭넓게 보장하고 있다.
법률적 차원에서도 이를 반영하고 있는데, 헌보청의 미성년자 급진주의자 단속과 개인정보 수집연령을 16세에서 14세로 낮춘 것이 대표적 사례에 해당된다. 또한, 전자통신법 개정을 통해 통신회사가 개인과 계약하기 전에 필요한 정보를 수집할 의무를 부여하고 정보기관이 관련 정보를 필요로 할 경우 제공토록 규정하고 있다. 이로 볼 때 독일의 정보기관들은 연방정보국 통신정보 수집법에 근거하여 개인 사생활 침해 우려가 있는 부분을 제외하고 국민안전을 위한 통신정보 수집 권한을 광범위하게 해석하고 있다. 그러나 정보기관의 정보활동 영역 확대는 엄격한 정보통제와 법적 근거에 기반하여 이루어지고 있다는 사실이다.

2) 정보 통제[66]

독일 의회의 정보통제는 1978년 의회통제위원회(PKK)법[67]제정됨으로써 제도화되었다. 정보기관의 정치개입과 권력남용 방지, 미국 의회의 정보기관 통제제도 도입, 기욤간첩 사건[68] 등이 의회통제 위원회를 설치하게 된 요인이 되었다. 의회정보위원회는 하원 의회통제위원회, 특별예산위원회, 기본법10조위원회 등 3개 위원회로 구성되고 있다. 의회통제위원회는 여당 5명, 야당 3명 등 총 8명으로 구성되며 내무 및 법사위원회 소속 중진의원 가운데서 선임되며, 임기는 4년으로 연임제한 규정이 없다. 위원장은 6개월마다 여·야당이 교대로 담당하고 있다.
특별예산위원회는 하원 예산결산위원회의 소위원회 형태로 운영되며 여당 3명, 야당 2명 등 5명으로 구성되어 있으며, 정보기관의 통신 감청만을 통제하는 기본법10조위원회는 여당 3명, 야당 2명 등 5명으로 구성되어 있다.

66) 염돈재, “의회의 정보기관 통제제도와 운영실태에 관한 비교연구”, 「행정논총」 제41권 제1호(2003).
67) 독일의 의회통제위원회는 1978년 설치 당시에는 PKK로 명명되었으나, 1978년 결성된 쿠르드족 테러단체인 쿠르드 노동당이 PKK라는 약칭을 사용하자 이와 구별하기 위해 1999년 PKG로 변경하였다.
68) 1974년 빌리 브란트 수상비서였던 귄터 기욤이 17년간 암약해온 동독 현역장교 신분 간첩이었다는 사실이 드러나면서 브란트 수상은 사임하게 되었다.

4. 이스라엘 정보공동체 및 정보통제

1) 정보체계[69)]

이스라엘 정보기관은 1948년 건국 이전부터 영국이 팔레스타인 지역을 위임통치하던 시기 독립전쟁을 위한 유대인들의 지하조직 활동에 그 기원을 두고 있다. 1920년 아랍측의 팔레스타인 지역 내 유대인 공동체에 대한 공격으로부터 보호하기 위해 정보기관을 운영하기 시작하였다. 유대인들은 하가나(Haganah)를 결성하였고 첩보부대 샤이 (Shai)를 운용하였는데 유대 독립국 건설 및 시온주의 선전을 위한 정치정보 수집 팔레스타인 등 주변국을 대상으로 공작활동을 전개하였다.
또한, 하가나 장교들이 주축이 된 모사드 알리야 베스(Mossad Aliyah Beth)는 유대인들을 팔레스타인에 밀입국시키는 역할을 담당하면서 무장 투쟁을 주도하였다. 이 조직은 훗날 모사드(ISIS)의 전신이 되었다.
1948년 건국을 맞아 이스라엘은 새로운 정보체계를 갖추게 되는데 군정보기관인 아만(Aman), 해외정보기관 모사드(ISIS), 그리고 국내 정보기관 ·신베트(ISA)으로 재편되고 여타 일부 정보기능은 경찰·외교부 등 행정기관에서 수행하게 되었다. .

가. 비밀정보부(ISIS : Israel Secret Intelligence Service) : Mossad

1948년 독립이후 군과 외교부 등 여러 기관에 의해 해외정보활동이 수행되면서 비효율적이라는 평가에 따라 새로운 정보기관의 설립 필요성이 제기되었다.[70)].[71)]이에 총리 소속하에 중앙보안정보부(Central Agency for Problems of Security and Intelligence)의 설립이 추진되면서 모사드가 탄생한 것이다. 이 기관의 태동은 외교부와 보안정보부(GSS), 그리고 이스라엘방위군(IDF)와 같은 기관들의 해외 정보수집 권한을 박탈하는 것이기 때문에 이스라엘 정보체계의 커다란 변화를 초래하였다.[72)] 초기에 모사드 요

---

69) 석재왕,『안보문화와 정보실패』(성균관대학교 박사논문, 2005).
70) Ian Black & Benny Morris,『Israel's Secret Wars: A History of Israel's Intelligence Services』(New York : Grove Press;1991), p.75.
71) 정보기관의 통합의지는 처음 발족당시 '통합기구 '(HaMossad LeTeum, Institute for Coordination)라는 이름이 붙여진 데서도 확인된다.
72) 다른 국가와 마찬가지로 이스라엘에서도 모사드의 설립은 다른 정보기관의 격렬한 저항을 초래하였다. 정치국(Political Division)해외 거점 간부대부분은 집단사표를 제출함으로써 이른바 '스파이 반란(the spies' revolt)이 발생하였다. 이들은 ' 정치국 간부들이 해외정보활동을 계속 수행하지 않으면 이스라엘의 정보업무는 어려움에 직면할 것이라 '고 경고하였다. 그러나 실로아는 정치국 요원들이 회합과 국제전화를 이용한 통화도 금지하였으며 심지어 일부 요원들의 여권을

원들은 정보활동 경험이 있던 정치국, 모사드 리알리야 벧, 그리고 샤이의 요원들로부터 충원되었으며 보안정보부(GSS)와 방위군(IDF)의 정보 요원들도 새로운 정보기관에 합류하였다. 모사드는 각 정보기관의 고유업무를 자연스럽게 계승하면서 정보기관으로서의 위상을 정립해나갈 수 있었다. 현재 모사드의 기능과 임무를 살펴보면 군사정보를 제외한 모든 해외 정보 수집·분석 및 공작하는 기능을 독점하고 있다.

모사드는 인간정보를 중심으로 활동하고 있으나 기술적인 문제는 군정보기관이 담당하고 있다. 모사드는 텔아비브에 본부를 두고 WMD차단·방지, 해외 대테러활동(이스라엘 해외관광객, 시설 등 보호) 등을 포함한 해외정보 활동을 수행하고 있다. 특히 200여개 국가 350개 기관과의 정보협력 관계를 바탕으로 한 정보수집 기능이 강력한 것으로 알려져 있고 이 외에도 총리의 지시에 따른 특수임무·공작 수행 역량은 전 세계 정보기관들의 모범이 된다는 평가를 받고 있다.

모사드는 부장산하에 조직운영과 공작을 담당하는 2개 차장 체제로 운영하는 것으로 알려져 있는데 구체적인 내용은 부인하고 있고 비교적 소규모 조직과 인원(2500여명 추정)에도 불구, 세계 최강의 공작전문 정보기관으로 자리매김하고 있다.

세계 각국 유대인들이 모여 세운 국가인 만큼 각국 사정과 언어에 정통한 전문 인력을 상당수 보유하고 있어 다양한 분야의 우수요원 선발·양성이 가능하다. 전 세계에 흩어져 있는 1,300만명의 유대인 협조망을 공작 및 정보수집 자산으로 활용하고 있는데 냉전시대 모사드가 구소련 및 동구권 관련 정보에서 CIA를 능가한다는 평가를 획득할 수 있었던 것도 당시 200만명의 유대인 활용이 주원인이라 할 수 있다. 특히, 소수 인원으로 인한 한계를 극복하기 위해 철저한 '선택과 집중' 원칙하에 자국에 대한 안보위협이 높은 분야에 공작역량을 집중하고 있다. 모사드의 정확한 실체와 공작능력에 대한 정보는 여전히 베일에 가려져 있다.

모사드는 이스라엘의 특수한 안보상황에 따라 사실상 준군사 조직·대중동 테러조직으로 운영되고 있는데 정부 및 국민들은 모사드가 이스라엘의 국가안보를 위해 필요한 조직이라는 확고한 인식아래 모사드 활동을 전폭 지지하고 있다. 공작실패로 인한 외교문제 발생시에 정부차원에서 적극적으로 보호하고 언론도 보도하지 않는 것이 관행이다.

한편 직원과 원활한 소통 및 업무 효율성 제고를 위해 부장 직속으로 '옴부즈만' 제도를 운영 중인데 옴부즈만은 정보의 객관성을 제고하기 위해 은퇴

몰수하는 가하면 해고도 서슴지 않았다. Ian Black & Benny Morris(2001),p.75.

직전 직원이 임명되어 사업·예산·인사 등 모든 분야에 대해 감독 보고서를 작성, 부장에게 직보하는 체계이다. 직원들도 옴부즈만에게 각종 고충·승진불만 등을 자유롭게 상담하며, 통상 옴부즈만을 통해 직원 불만사항의 30%정도 해결하는 것으로 알려져 있다.
부장은 국가 비밀서열 13번째에 해당될 정도로 중요인물로 간주되고 있다. 모사드의 주요 부서는 일반적으로 전체 8개 부서로 이루어져있는 것으로 알려져 있다. 수집국(Collection Department), 작전기획조정국(Operational Planning and Coordination Department), 정치활동연락국(Political Action and Liason Department), 인력·재정·병참·보안국(Manpower, Finance, Logistics, and Security Department), 훈련국(Training Department), 분석국(Research Department) 등으로 구성되어 있다.[73] 한편, 모사드 부장은 법률상 임기제한 규정이 없으며 통상 부장 취임이후에는 정권교체와 무관하게 5~6년 정도 재직하는 것으로 나타난다.

나. 보안정보부(ISA : Israel Security Agency) : 일명 'Shin Bet'

1948년 6월 국내 쉐이로 불리면서 태동된 신베스는 국내 보안방첩과 보안활동을 담당하고 있다. 이 기구의 기원은 1920년대 발족된 유태인 자체 방위조직인 하가나가 독립이후 IDF로 개편되는 과정에서 보안정보부(GSS)로 발족하면서 태동되었다.[74] 2002.2월 근거법인 ISA법이 제정되었으며 주요 임무 기능은 ①국내 보안·방첩·대정부전복 차단 ②테러 정보수집 및 테러기도 차단 ③VIP 경호정보 수집 및 경호 담당 ④국가안보 위해 우려 인물 암살을 포함한 특수·비밀공작 수행 ⑤보안업무(비밀보호, 중요시설·공항만 보호, 신원조사 등) 감독 및 기획·조정 등이다.
여타 정보기관보다 휴민트에 의존하는 비중이 높고, 지역 주민 등으로부터 하마스 및 이슬람 지하드 등 반 이스라엘 세력에 대한 정보를 수집하고 있다. 테러·국가전복·간첩행위 등 중대한 국가안보 위협 사안의 경우 48시간까지 법원 영장 없이 총리 재가만으로 감청을 실시할 수 있으며 특히 정치인도 반국가 행위·테러 연계 혐의시 감청을 통해 불순동향을 포착, 총리에게

---

73) 이스라엘의 정보기관의 조직체계도는 베일에 싸여 있어 접근하기가 어려우며 정보활동 역시 몇 가지 실패와 성공사례 이외에는 거의 알려져 있지 않다. 또한 수시로 직제개편을 통해 조직의 구성체계가 변화하기 때문에 체계적인 조직표를 입수하기란 매우 어렵다. 모사드 요원의 수도 1,200여명이라는 주장도 있으며 편제 또한 10-11개부서로 평가하는 자료도 있다. 본 논문에서는 다음 논문과 자료를 재정리하였다. 문정인 편저, 국가정보론(서울: 박영사, 2002). pp. 420-427; Walter Laquerur(1992), pp. 220-224; Fedeation of American Scientists(FAS),Mossad, http://www.fas.org /irp/world/israel/index.html(검색일 : 2021.7.21.).
74) 신베스의 기원과 발전과정에 대해서는 다음 글을 참조할 것. Black & Morris(2001),pp.134-46.

보고하고 있다.

국내정치와 관련된 일체의 활동을 금지하고 있는 ISA법에 의거해 강력한 조사권을 보유하고 있으며 필요시 대법원의 허가를 받아 혐의자에 대한 신체적·정신적 압박을 가할 권한도 보유하고 있다. 이스라엘 관리들과 공관시설의 안전을 보장하며 국내외 사보타주 및 테러를 포함한 내부 또는 외부의 적에 대한 일체의 정부전복 획책에 대한 대응활동을 수행하고 있다. 최근 사이버테러 급증으로 철도·전력회사 등 국가기간 시설은 물론 금융기관 컴퓨터에 대한 감독·감독을 강화하는 등 업무영역을 확장중이다.

한편, 신베트 부장의 경우 ISA법에 따라 임기가 5년으로 보장되어 있으나 정부결정으로 임기가 단축될 수 있으며 반대로 임기만료 이후에도 특별한 사정이 있을 경우 최대 1년까지 1회에 한해 연장 가능하다. 신베트 부장의 임명절차는 모사드 부장과 동일한 데 의회의 인사 청문을 받지 않고 총리 지명 외부위원회 자격심사, 내각 찬반투표로 결정되나 실제로는 총리의 독자적 판단 및 책임 하에 선임하는 방식으로 이루어진다.

다. 군정보국(DMI : Directorate of Military Intelligence) : 별칭 'Aman'

아만(Aman)은 국방부 산하기관으로 국방부장관의 지휘·감독 하에 군사정보를 처리·작성·배포한다. 통신감청을 통해 인근 국가들의 동향을 면밀히 파악하고, 국가정보판단보고서를 생산하여 총리와 내각에 제공하며, 일일정보보고서·전쟁위험평가보고서 등의 보고서도 생산한다. 아만 산하에는 외국 군 정보기관과 정보협력, 해외 주재 이스라엘 무관들의 활동 조정 등 임무를 담당하는 대외관계국(Foreign Relations Department), 이스라엘 정보공동체내 신호정보(SIGINT) 수집을 담당하는 정보단 등이 있으며, 각 군마다 정보기관을 별도로 두고 있으나 이들의 독립성은 어느 정도 보장된다. 최첨단 기술정보 수집수단을 활용하여 아랍국의 군사동향과 전투력 등에 대한 정보를 효과적으로 수집·분석하여 전쟁 위험성을 사전에 알리는 역할을 한다. 1973년 10월 욤 키푸르 전에서의 정보 실패를 겪은 후 아만 내에서는 큰 변화가 일어났다. 직속상관이 자신의 견해를 수용하지 않는 경우, 비록 하위직 정보관일지라도 그의 상관보다 더 높은 직위의 상관에게 자신의 판단과 관점을 호소할 수 있도록 제도적으로 보장되었다. 또한 기관 내 통제단(Control Unit)이 새로 편성되어 악마의 옹호(devil's advocate)의 역할을 수행하게 하였는데, 이들은 부장에게 언제든 직접 보고하는 것이 허용되었다.

아만은 군 관련 정보를 다루지만 활동영역은 다른 국가의 군 정보기관보다 업무영역이 넓고 비군사적인 국가안보와 관련된 정보활동도 수행하고 있다. 이는 이스라엘 건국 초기 정보활동 기능을 수행할 수 있는 조직이 '아만' 밖에 없었던 역사적 배경이 있고 총리 및 내각에 일일동향정보, 전쟁예측, 아랍국가 상황, 통신감청 등에 대한 보고서를 작성하며 국경근처 정탐활동을 수행하고 있다.

라. 라캄(LAKAM)

1957년 핵개발을 목적으로 설립된 이 조직은 군사 부문의 과학기술정보를 수집하는 역할을 담당했다. 미국과 유럽의 대사관에 과학담당관을 두고 정보수집활동을 전개하기도 하였으나 1986년에 미국 내 이스라엘 간첩사건인 '폴라드 사건'으로 해체되었다.

마. 정치연구소(the Center for Political Research)

이스라엘 외교부 산하의 정치연구소는 미 국무부 정보조사국(INR)과 유사한 기능을 수행하고 있다. 중동국가 지도자들의 정치적 성향, 정당 등 주요 정치집단들의 활동상황, 국민여론 동향 등에 관한 첩보를 수집하고 분석하는 임무를 수행한다. 이스라엘 외교부 자체가 국가안보 문제 결정과정에서 큰 역할을 하지 못하고 있다. 외교장관 자체도 전문성을 가진 인사를 임명하기 보다는 이스라엘의 연립정부 구성원칙에 따른 각료 배분의 결과인 경우가 많아 역할이 미미하다. 이로 인해 이따끔 외교장관이 안보관계 장관회의에서 보통 배제되는 현상이 발생하고 있다.[75]

2) 정보통제

의회(Knesset)의 외교국방위원회 산하 정보소위원회가 모사드·신베트·아만 등 3개 정보기관에 대한 통제를 관장하고 있다. 외교국방위 산하에 주요 소위원회는 6개이며 임시·합동(다른 상임위와 공동 구성) 소위원회까지 포함하며 10개로 운영하고 있고, 정보소위 외에 정보기관을 관할하는 여타 위원회는 부재한 실정이다.
정보소위는 정보기관에 대한 신뢰를 바탕으로 정보기관을 감독하면서도 공작

75) Freilich, Charles D, "National Security Decision-Making in Israel: Improving the Process," Middle East Journal, Vol. 67, No. 2 Spring(2013).

등 정보활동을 침해하지 않도록 유의하고 있다.

가. 정보소위원회(Subcommittee for Intelligence and Secret Services)

① 기능 및 구성

이스라엘 의회는 외교국방위에서 민감한 외교현안이나 병력동원과 같은 국가안보에 직결되는 현안을 처리하였다. 그러나 비밀누설 사례가 잇따라 발생하면서 보안유지하에 정보기관의 비밀 활동 관련 논의가 가능토록 소규모 인원으로 구성된 소위원회 구성 필요성이 대두되었다. 이에 2002년 ISA법이 제정되면서 정보소위에 법적인 권한을 명시적으로 부여하게 되었다. 정보소위는 외교국방위원회 산하 6개 소위중 하나로서 긴밀한 논의, 신뢰구축 및 비밀유지를 위해 5명을 위원으로 구성되며 외교국방위원장이 정보소위 위원장을 겸임한다.

외교국방위 위원 17명의 투표로 정보소위 위원을 선출하되, 총선 이후 각 정당간 연정구성 협상 결과에 따라 위원직을 정당별로 배분하며 각 정당이 자기당 인사의 임명을 위해 치열하게 경쟁하는 등 핵심 위원회로 인식하는 경향이 있다.

정보소위 위원으로 선발되기 위하여 법률·규정으로 명시된 자격조건은 없으나 중요한 국가안보 사안을 다루는 소위인 만큼, 대개 각 정당의 중진급이 포진되고 있다. 대체로 안보분야 전문지식을 구비한 인사로 구성하는데 군사 분야 경력이 필수적인 것은 아니나 안보관련 경험 보유시 위원 피선에 유리한 것으로 알려져 있다 정보소위 위원들은 타 위원회 및 외교국방위 내 타 소위 위원을 겸임이 가능하다.

민감한 안보현안을 다룬다는 이유로 아랍계 배경을 가진 의원(전체 의원의 20% 수준)들은 임명 대상에서 비공식적으로 배제하고 있고 정보소위 위원의 명단은 외교국방위 위원 17명에게만 공개되며 이들 위원은 직무상 동 명단을 알고 있더라도 외부공개가 절대 불가할 정도로 보안유지에 각별한 실정이다. 의원들의 임기는 4년으로 동일하나 최소 임기는 3개월로 규정하고 있다.

한편, 정보소위 회의 운영과 관련하여 정보소위는 총리와 최소 년 1회, 정보기관장과는 2회 정도 회의를 개최하고, 3개월마다 각 기관들이 업무에 대해 브리핑을 실시하며 전문위원(1명)은 정보소위 회의에 참석 가능하나 의원보좌관·정당 간부들은 제외하고 있다. 민감한 공작사항은 정보기관장이 우선 정보소위 위원장에게 보고하며 추후 여타 위원들과 공유한다. 정보기관은 정보소위에 과거 발생 사안에 대한 자료를 제공하고 진행 중 또는 미래사항에 대

해서는 관련 정보를 제공하지 않지만 국가안보에 중대한 사안일 경우 일반적 수준에서 지원이 가능한 것으로 알려져 있다.
이스라엘 정보기관들은 정보소위에 적극 협력하고 있지만 활동과 역할이 정보소위에 의해 크게 제약을 받지 않기 때문에 수월하게 본연의 임무를 수행하고 있다. 한편, 자료요구 범위는 총리와 소위 위원장의 협의에 따라 결정하는데 위원장 명의로 간사를 통해 정보기관에 요청하며 개별요구는 금지되고, 정보소위 회의실내에서만 비밀문건 열람이 가능하며 정보기관장은 필요시 정보소위의 자료제출 요구에 대해 사유를 붙여 거부 가능하다.

② 예산 편성

정보기관의 예산은 국방예산에 분산 계상되며 모사드 등은 총리와 협의를 거쳐 예산안을 외교국방위 및 예산부에 제출하는데 예산안 제출시 세부내역은 보고하지 않으며 공작비, 인건비 및 유지비 등을 총액으로만 보고한다. 국방예산은 5명의 재정위 소속 위원들과 5명의 외교국방위 소속 위원들로 구성된 공동위원장(위원장 : 외교국방위원장)이 결정한다. 이중 모사드, 신베트 및 군 정보기관 예산은 2명의 재정위 소속 위원과 3명의 정보소위 위원으로 구성된 공동소위에서 통상 1회 심의로 확정한다. 특히, 정보기관의 경우 회계연도 종료전이라도 예산이 부족하면 정보소위와 협의를 거쳐 추가예산 요구가 가능하다.

③ 비밀누설 방지제도

이스라엘 의회는 2006년 별도 건물을 신축하였으며, 외교국방위 산하 위원회에서 주관하는 모든 회의를 이 건물 안에서 개최토록 하고 있는데, 특히 정보소위는 여타 위원회와 상당히 떨어진 별도의 회의실에서 개최하고 있다.[76]정보소위와 관련하여 회의 일시, 개최여부 및 위원들의 명단 등 모든 내용은 비밀사항으로, 2006년 이전에는 정보기관장도 의회 내 중앙 복도를 통해 이동하였다. 그러나 이후에는 외부인들이 정보소위 개최 사실을 인지하는 경우가 발생한다는 이유로 비밀유지를 위해 정보소위 참석차 의회를 방문하는 정보기관간부들은 외부에 노출되지 않도록 별도의 출입문을 통해 소위원회에 출석토록 하고 있다.
정보소위 위원은 위원회에서 지득한 내용을 공개하지 않겠다는 비밀준수 서

76) 이스라엘 정보기관 창설 배경이 1979.1월 이란의 미 대사관 점거 당시 CIA 작성문서가 공개되면서 외부에 알려지게 되었다는 사실은 이스라엘 정보기관이 보안을 얼마나 철저하게 유지하고 있는지를 잘 말해준다

약을 실시한 후 회의에 참석하고 있으며 정보기관은 정보소위가 대외유출을 하지 않을 것이라는 전제로 공작사항 등을 보고하기 때문에 정보위원들도 회의 참석 중에 휴대폰 배터리를 분리·소지하고 있다. 또한 정보소위 개최시 배포된 문서의 경우 회의장 밖으로 유출되지 않도록 법으로 단속하고 있으며 회의내용을 메모하여 회의장 밖으로 반출하는 행위도 절대 불가하다.

정보소위에 대한 보고는 회의실 내에서만 이뤄지고 정보소위의 회의록은 비공개하며 정보소위 위원들이 비밀을 누설할 경우 형법에 의거 3년 이하 징역을 받을 수 있으나 아직까지 위원들이 보고한 내용이 공개된 사례는 전무한 실정이다.

비밀자료는 위원장으로부터 별도의 허가가 없는 한 소위 회의실에서만 정보소위 위원에 한해 열람이 가능하고 외부유출 및 복사가 금지되어 있으며 위원들이 자료를 열람할 경우 예외없이 관리대장에 서명하여야 하며 회의종료 후에는 반드시 비밀문서 캐비넷에 보관해야 한다. 보안시설은 소위 사무실, 회의실, 비밀문서 보관소, 컴퓨터실 등이 해당되는데 의회경비가 매일 아침 정보소위 회의실 등에 대한 보안점검을 실시하고 일과 후에는 알람 시스템을 작동하고 있으며 신베트는 매년 위원회 회의실에 대한 대도청 점검을 실시한다. 출입문에는 암호화된 시건장치가 되어 있어 위원 및 직원들만 출입이 가능토록 감독 하고 있으며 정보소위 위원은 물로 속기사 등 모든 관계자가 보안검색을 받고 있는 실정인데다 비밀문서 작업 시에는 지정된 컴퓨터실을 이용하고 일반 업무를 수행하는 사무실에 컴퓨터, 가구, 냉난방 장치 등을 설치할 시에도 보안절차 완료 후에나 가능하다.

의회 인터넷 시스템에 연결된 컴퓨터에 비밀문서를 저장·인쇄하는 행위는 절대 불가하고 위원회 회의실내 비밀문서 방치도 엄격히 금지되어 있다. 따라서 비밀문서 복사는 지정된 복사기에서만 가능하며 파기해야 할 비밀문서는 반드시 파쇄기로 처리하고 일반우편을 통한 비밀문서 배포행위가 금지되어 있어 반드시 비밀취급 허가자를 통하거나 비화팩스로만 배포할 수 있다. 이스라엘과 한국의 의회 비밀누설 방지대책을 도표로 정리하면 다음과 같다.

<표3.2> 이스라엘과 한국 의회의 보안체계 비교

구분	의회 감독 기관	비밀누설 방지대책
이스라엘	o 국방외교위원회산하 정보소위원회 - 재산에 유리한 핵심 위원회로 인식(5명, 임기4년) - 타위원회와 겸임 가능,	o 정보소위원 명단은 외교국방위위원(17명)에게만 공개, 외부 공개 절대 불가 o 의원, 개별 자료 제출요구 불가 o 정보소위위원회 사무실에서만 자료열람 가능, 외부 유출 및 자료 복사 불가

		비밀 케비넷에 보관, 인터넷에 연결된 컴퓨터 내 저장된 민저 인쇄 금지 o 정보기관장, 필요시 자료제출 거부 (사유 첨부) o 예산 편성 : 국방예산에 분산 계상, 총액보고, 공동소위에서 1회 심사 o 정보소위, 여타 위원회외 이격된 장소에서 진행 o 정보소위 회의시 휴대폰 배터리 분리, 배포된 자료 반출 절대 불가 o 비밀누설시 3년 징역 가능 * 정보 누설 사례 거의 없음
한국	o 정보위원회(12명) - 의석 비례에 의거 선출 - 임기 2년, 여타 위원회와 겸임가능 o 총액 예산제도, 비공개 회의 등	o 정보위원 전체 대상 정보보고 o 비밀정보 보안유지 관련 세부 규정 별무 * 정보누설 사례 수시로 발생

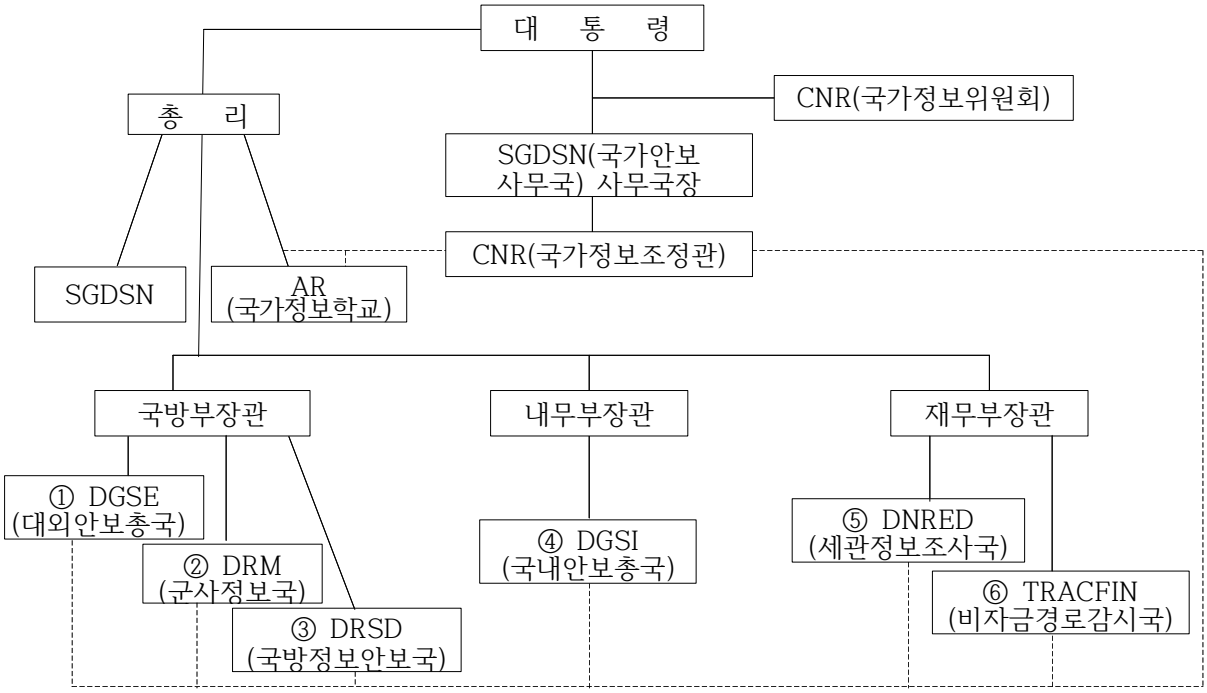
5.프랑스 정보공동체와 정보 통제

1) 정보 체계

프랑스 정보공동체는 DGSE(해외안보총국), DGSI(국내안보총국), DRM(군사정보국), DRSD(국방정보안보국), DNRED(세관정보조사국), TRACFIN(비자금경로감시국)6개 정보기관으로 구성되어 있다. 해외정보기관은 직제상 국방부 소속이며 DRM·DRSD는 군정보기구이다. DGSI는 내무부 소속으로 DCRI(국내중앙정보국)·DST(국토감시국)[77]·RG(일반정보국)[78]가 통합되어 2014년 설립되었고, DNRED·TRACFIN은 재무부 소속이다.

6개 정보기관장은 CNR(국가정보위원회)에 참여하며 대통령이 CNR위원장이다. 그리고 총리 산하에 AR(국가정보학교)가 설치되어 효율적 정보공동체 유지 및 활성화를 위한 정보요원 교육 훈련을 하고 있다.

<그림3.3> 프랑스 정보체계[79]



77)1982년 12월 설립되었으며 프랑스 안전을 위협하는 활동의 조사·예방·진압을 담당하고 있으며 본부에는 관리부서이외 방첩부, 방호·보안부, 테러대책부, 전기통신경찰부 등이 설립되어 있고 지방조직도 운영하고 있으며 인원은 1,500여명으로 추정된다.

78) 1941년 4월 설치되었으며 정치·경제·사회질서(테러리스트 및 직접행동주의자와 그 단체에 관한 정보 등) 관련 정보의 수집(공작 포함)·종합 임무를 맡고 본부는 관리부서 이외 분석·종합과, 조사과(테러대책·공작담당), 경마·도박과(카지노·경마 감독)로 구성어 있다. 지방조직은 8개 관구·22개 지역권·103개 현에 설치되어 있다. RG의 중점 대상은 프랑스 공산당(1950년대),알제리 민족해방전선(60년대),극좌세력(70년대),테러리즘(80년대) 이었으나 90년대 이후에는 목표가 점차 모호해지고 있다. 손재락(2021)

79) http://www.academie-renseignement.gouv.fr/communaute.html(검색일: 2021.7.17).

가. DGSE(해외안보총국)

해외정보를 담당하는 DGSE는 1982년 4월에 재편·신설되었으며 전신은 SDECE(국외정보관리·방첩부였다. 행정적으로 국방부에 속해 있지만, 실제 프랑스 대통령과 총리의 지휘를 받고 정보를 보고하고 있다. 베를린 장벽 붕괴 후 정보기관 강화 정책에 영향을 받아 인원과 업무가 확대되었다.
DSGE는 전략부(중장기 전략수립), 정보부(정보의 수집·분석), 작전부(특수부대 지휘), 기술부(작전 신호정보 개발·관리) 등으로 구성되어 있다. 임무는 휴민트·시긴트 등 모든 수단을 통한 정보수집 권한을 보유하고 있으며 정보 종합분석 기능과 해외에서의 비밀공작 활동을 수행한다. 특히, 해외에서 프랑스의 국익에 반하는 활동을 자행하는 인사들에 대한 강도 높은 공작활동도 수행하는 것으로 알려져 있다.

나. DRM(군사정보국)

1992.6 DRM을 신설하였는데 3군의 참모본부 제2과(정보담당), 군사정보분석센터(CERM), 전자자기정보센터(CIREM), 엘리오스(Helios) 화상분석센터, 3군 정보어학학교를 통합한 결과였다. DRM창설은 걸프전 당시 첨단기술을 활용한 정보 수집 역량이 부족한 나머지 대부분 미국정보 자산에 의존한 반성에서 출발하였다. 이에 따라 국방부 내 전술정보 조직의 재편이 진행되었는데, 이는 국방부장관·COS(특수전군)·여타 유관 기관들의 필요에 부응하기 위한 것이었다. DRM은 직제상 COS에 보고하게 되어 있지만 국방부 산하 기관으로 국방부장관에게 직접 보고한다.[80]

DRM의 임무는 첫째, 군사개입 전 단계에서 프랑스 안보에 잠재적 위협이 되는 대상·지역에 대한 일반적 정보를 수집하여 이를 토대로 개입 계획을 수립하며 둘째, 분쟁·위기 발생시 어떠한 지역에서 어떠한 위협이 존재하는지에 대한 정보를 적시성 있게 의사결정 기관에 제공하는 역할을 담당한다. 셋째, 군사개입 상황시 관련 정보를 정책결정자에 지원하고 사후 정세를 분석하는 역할을 담당하고 있다. DRM은 관리지원과, 분석과, 조사과, 기술과, 군비관리과, 3군 정보어학 학교 등으로 구성되며 육군정보부대, 제13긴급 공정부대, 전파위성사진 수신센터도 예하에 두고 있다.

80) 전웅(2015), p.445.

다. DRSD(국방정보안보국)[81]

군사 방첩활동과 군의 정치적 신뢰성 확보를 목적으로 군에 대한 정치적 감시를 담당하는 기능을 수행하고 있다. 이는 프랑스 혁명으로부터 기원하는데 당시 특명 파견대표들은 정치위원으로서 프랑스 사령관들을 감시하는 역할을 맡고 있었다. 군이 프랑스 정치과정에 개입하거나 간섭할 수도 있다는 가능성과 위협을 전제한 것이다.
국방부 소속 인원, 정보, 장비, 민감시설, 방위관련 산업 인프라 등을 보호하는 임무를 띠고 있으며 예방적 접근을 통해 국방관련 기관의 이익에 반하는 잠재적 위협과 관련된 정보를 수집・분석・배포한다.[82]

라. DGSI(보안정보부)

DGSI는 2014년 5월 내무부 소속의 국내 정보기관으로 신설되었다. 이는 舊 국내 정보기관이었던 경찰청 소속 DCRI(국내중앙정보국)가 2010년 사르코지 대통령에 대한 악성 루머를 공식 조사한 것이 사생활 침해・정치적 문제 등으로 비화되면서 재편된 것이다. DGSI는 DCRI 업무를 승계하여 주로 방첩, 대테러, 사이버 범죄 대응, WMD 확산방지, 경제주권 수호, 프랑스 영토에 대한 각종 잠재적 위협 감시 등 업무를 수행한다.[83] 또한 2013년 5월 정보기관 관련 국회보고서는 2013년 2월 메라 테러에 대해 정보기관의 실수와 DCRI를 비판했으며 이에 따라 DGSI로 재편되면서 내무부 장관이 감독아래 있게 되었다.[84]영국과 다르게 DGSI 관리는 사법권을 보유하고 있으며 특히 테러나 방첩사건에 있어 그들의 능력을 증대되고 있다. 2017년 노틀담 테러 사건에 대한 수사를 국가 대테러 센터와 합동으로 수행했다. 그리고 직원은 대부분 경찰서장이나 국립경찰 출신이다.

마. 재무부 정보기관(DNRED, TRACFIN)

DNRED(세관정보조사국)는 세관에 소속되어 정보・감독・사기행위 단속

81) 2016년 10월 법령에 따라 DPSD가 DRSD로 대체되었는데 이는 기관을 현대화하고 정체성을 명확히 하는 등 조직을 강화해야 할 필요성에서 추진되었다.http://www.academie- renseignement.gouv.fr/drsd.html(검색일: 2021.7.18.). 동 기구는 SSM(1946년, 군사안보부), SSFA(1948년, 군안보부), SSDNFA (1953년, 국방군사안보부), DSM(1961년, 군사안보국), DPSD(1981년, 국방보호안보국)으로 변화해 왔다. 손재락(2021)
82) Philippe Hayez and Hedwige Regnault de Maulmin, “Guide to the study of intelligence, French Intelligence” *The Intelligencer* Volume 21(Summer 2015), pp.49-50.
83) 문경환, “주요국가의 국내정보활동 및 조직체계 연구 : 영국, 미국, 프랑스, 우리나라의 국내정보기구를 중심으로”. 한국경호경비학회지 제41호(2014.12), pp.153-183.
84) 문경환(2014), p.170.

관련 정책을 시행하고 있으며 정보활동이 경제분야에 유용성이 입증된 대표적인 사례에 해당된다. TRACFIN(비자금경로감시국)은 미국의 FinCEN(금융범죄단속반)과 유사한 기능을 수행하고 있다. 불법 금융네트워크, 돈세탁, 테러 금융 등 관련 업무를 수행하며 법적 보고의무가 있는 기관들의 수상한 거래에 대한 정보를 수집·분석한다. 다수의 유가치한 정보를 직접 수집할 역량이 부족한 관계로 관련 기관들의 협력을 필요로 한다.

바.CNR(국가정보위원회), CNR(국가정보조정관), AR(국가정보학교)

2008년 국방안보백서에 따라 2008.7. 정보기관에 대한 거버넌스 강화를 위해 국가정보위원회(CNR; Conceil national du renseignement)와 국가정보조정관(CNR; Coor- donnateur national du renseignement)이 설치되었는바, 이는 해외 테러위협에 대응하는데 목적이 있다.
CNR은 프랑스 정보기관의 운영위원회로 활동하고 있으며 부처간 정보위원회(CIR)[85]의 임무를 인수하였다. CIR에 대한 책임은 총리에 있었던 반면, CNR은 대통령이 책임을 지고 있어 대통령에게 정보를 보다 직접 통제할 수 있는 수단을 제공하였다. CNR은 미국의 NSC 역할을 하며 주요 참석 인사는 총리, 관계 장관, 정보보안기구 수장, 국가정보관 등이다. 3년마다 국가정보추진계획(PNOR)을 통해 국가정보의 전략적 방향과 우선순위를 제공하는 역할을 수행한다.

CNR 설립 후 임명된 정보조정관은 CNR에 보고하며 CNR이 제대로 작동하도록 보장한다. 정보분야 대통령 자문, 대통령 지시 전파, 대통령 일일 정보보고 준비, CNR 결정사항 이행여부 감독 등 임무를 수행한다. 그리고 정보 PNOR를 통해 행정부의 정책 및 그 우선순위를 정하는 데 참여하며 주요 역량 간 상호 협력을 감독하고 정보기관 수장들과의 정기적 회의를 통해 기관들 사이에 교류를 촉진시킨다. 조정관은 관계부처 전문 요원들로 구성된 팀에 의해 지원을 받거나 각 정보기관으로부터 직접 지원을 받는다.[86]

85) CIR은 1959년에 설치되어 정보기관의 활동방침을 시달하고 협력을 증진하기 위하여 국가정보계획을 수립하는 것이 임무였으나 거의 기능을 하지 않고 있었다. 1988년 로카르 총리 재임당시 정보기관 개혁조치 일환으로 CIR을 활성화시킨 바 있다. CIR은 의장인 총리가 소집하며 국방, 내무, 외무, 재무, 예산, 산업, 조사연구, 통신, 우주개발, 해외 縣·영토 담당 장관들이 참석하고 필요시 관련 각료도 참석한다. CIR 산하에 실무회의도 개최되는데 DGSE국장이 의장이 되고 대통령실 관방장, 총리실 외교고문·군사고문, 내무부 국립경찰청장, 국방사무국장 등이 참석한다. 손재락(2021).

86) Hayez and Maulmin(2015), p.50.

이와 함께 2008년 AR(국가정보학교)가 총리 산하에 설립되었는데 이익·목표·친화·신념·문화 등을 공유한 정보공동체를 육성하고 정보문화를 발전시키기 위한 것이었다. 각기 다른 기관의 훈련을 상호 대체하기 위한 것이 아니라 상호 이해를 증진하고 기관 간 협업을 증진하려는 것이다.[87]

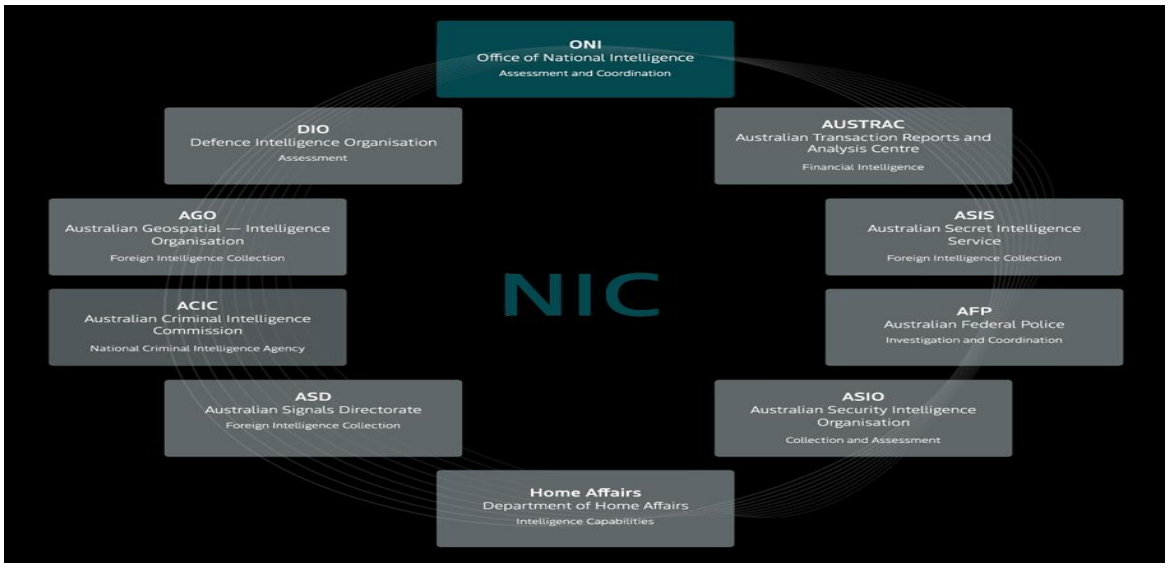
87) Hayez and Maulmin(2015), p.51.

6. 호주 정보공동체와 정보통제

1) 정보체계

호주 정보기관은 2차 세계대전 중 태평양에서 미국과 호주 군대를 지원하기 위한 정보활동에서부터 출발하였다. 1947년 국방신호국(Australian Signals Directorate)이 정보기관 중 가장 먼저 공식적으로 설립되었다. 소련 통신첩보 수집업무를 중심으로 운영되다가 1949년 국내정보기관 보안정보국(ASIO)을 설립하였는데 호주 내 러시아 스파이 색출이 주된 목적이었다. 1952년에는 영국의 MI6를 모델로 해외 정보기관 비밀정보국(ASIS)을 국방부 내 설립하였다. 이 기관은 1954년에 외무부로 소관 사무가 변경되었고 1977년이 되어서야 존재가 공개적으로 인정되었다. 2차 세계 대전 당시부터 국방부 내 정보평가 팀을 운영하였고 냉전기 1970년에는 합동정보국(JIO)이 설립되었으며, 현재 국방정보부(DIO)로 발전하였다. 정보 통합을 위해 1978년 왕립위원회의 권유에 따라 국가평가실(ONA)이 설립되었다. 지리정보기능은 1964 년 이후에도 있었지만 1998년까지는 DIO에 통합된 부분이었다. 2001년에 ISA(Intelligence Service Act) 법이 제정되면서 오늘날 호주 정보공동체의 모습을 갖추게 되었다. 호주 정보공동체(AIC)는 6개 기관으로 구성되어 있으며 책임과 기능 명확히 구분된다. ① 국가정보평가실(ONI) ② 호주보안부(ASIO) ③ 호주비밀정보부(ASIS) ④ 신호정보국(ASD) ⑤ 국방정보국(DIO) ⑥ 영상지리정보국 (AGO) 등이다.

<그림3.4> 호주 국가정보체계도[88)]



88) https://www.oni.gov.au/national-intelligence-community(검색일 : 2021.10.17.)

가. 국가정보평가실(ONI)

ONI(Office of National Intelligence)는 2018년 전신인 ONA(Office of National Assessments)로부터 개칭된 것으로 국가 차원에서 분석된 정보를 통합, 평가하는 수상직속 정보기관이다. ONI는 2018년 제정된 ONI 법에 의거하여 정보활동을 수행하고 있다. 정부부처의 정보 및 기타 보고 및 공개된 정보를 활용하여 국제 정치, 전략 및 경제 발전에 대한 평가를 수행하는 기능을 담당한다.[89]사무총장은 독립된 기관장이며 독립성을 보장하기 위해, 호주 독립 감사관(IGIS)[90]이 ONA의 활동에 대해 정기적인감사를 실시하고 있다. ONA 관련 정보는 정보공개 대상에서 면제되지만 기록보관소 법 (Archives Act, 1983)에 의거하여 일정한 기간이 경과되면 일반 공개 대상으로 분류된다. ONA의 주요 기능을 살펴보면 다음과 같다.[91]

- 국가안보위원회 (National Security Committee of Cabinet)의 소속 장관들에게 국제 정치, 전략 및 경제 발전에 관한 내용을 제공
- 공개정보 센터, 전자매체 및 웹사이트와 같은 출처로 부터 지리, 인물정보, 문화 등과 관련된 다양한 공개정보를 수집, 분석
- 행정부처를 대상으로 국가안보 이슈에 대한 분석 결과물들을 제공, 합리적인 정책결정에 기여

나. 보안정보부(ASIO)[92]

호주 보안부(Australian Security Intelligence Organization)는 1979년 ASIO 법에 따라 내무부 장관 산하에 설립된 국내정보기관이다. 1956.12 보안정보조직법(Security Intelligence Organization Act, 1956)에 의해 법적기관으로 발전하였다. 보안부는 사보타지, 외국의 간섭행위, 정치적 동기에 의한 폭력, 호주 방위체제에 대한 공격, 테러리즘으로부터 국가 및 시민을 보호하는 기능을 수행한다. ASIO는 국익 수호를 위해 광범위한 감시 기능을 갖고 있으나 수사권을 보유하고 있지는 않다. 특정 정보가 필요한 경우 연방 및 지역 경찰 협조하에 법무부장관으로 부터 체포·구속 영장을 발부를

89) https://www.ona.gov.au/about-ona/overview(검색일 : 2021.10.4).
90) IGIS(Inspector GeneralI Intelligence and Security)는 1986년 정보보안감독원법 (IGIS Act)으로 설립
91) https://www.ona.gov.au/about-ona/overview(검색일 : 2021.7.19.).
92) https://www.asio.gov.au/what-we-do.html(검색일: 2021.7.19.)

받을 수 있다. 전기통신법에 근거하여 합법적인 감청활동을 수행하고 있다. ASIO는 금융계좌 추적을 추적할 수 있는 명시적인 권한은 없으나 국내보안, 대테러분야 정보수집을 위해 금융정보를 제공받아 정보활동에 활용하고 있다.

법무장관이 승인한 영장에 의해 우편검열, 출입감시, 통신통제를 할 수 있으며 긴급상황 발생시 법무부 장관으로부터 승인을 받아 영장없이 긴급 조사권을 집행할 수 있는 권한도 보유하고 있다. 다만, 테러단체 구성원들을 조사할 경우에는 사법당국으로부터 영장을 발부받아 용의자를 강제 심문할 수 있다. ASIO는 외무부, 국방부 장관의 요청에 따라 호주 내에서 외국정보를 수집할 수 있는 권한을 보유하고 있다. 이밖에 여타 정부부처와 합동정보작전(Joint Intelligence Operations)을 수행하여 호주 주재 외국 공무원·단체들에 대한 보안정보를 광범위하게 수집할 수 있다.[93]

다. 호주비밀정보부(ASIS)[94]

ASIS (Australian Secret Intelligence Service)는 냉전기 주로 아시아태평양 지역에서 해외 정보를 수집해왔으며 2001년 정보서비스법(ISA, Intelligence Services Act)[95] 제정으로 공식적으로 설립되었다. ASIS는 해외 HUMINT 수집기관으로서 호주의 중대한 국익을 보호하고 증진하기 위해 다음과 같은 기능을 수행하고 있다.

- 호주 이익에 영향을 줄 수 있는 해외 분야에 대한 정보수집
- 핵심정책 부처 및 기관을 대상으로 정보 및 분석 결과를 배포
- 호주의 이익과 국가 주권을 보호하는 정보활동
- 호주의 국익을 위해 해외 정보기관 및 보안기관과 정보협력
- 국방, 국제관계 및 경제 문제와 관련된 정보 수집. 테러와 대량살상무기의 확산 및 밀수와 같은 초국적 이슈를 해결하기 위한 노력

한편, ASIS는 외무부 장관의 관리 책임하에 있으며 부장은 ASIS와 관련된 핵심 사안에 대해 장관에게 조언해야한다. ASIS의 재무회계는 감사원 일반법(Auditor-General Act 1997) 제19조에 따라 감사를 받고 있다. 또한 공익

93) ASIO는 캐나다(CSIS),뉴질랜드(NZSIS),영국(MI5),美연방수사국(FBI)등 국내외 정보 및 보안기관 등 120개국 311개 기관과 정보협력을 유지하고 있다.
94) https://www.asis.gov.au/About-Us/Overview.html(검색일: 2021.7.26.).
95) https://www.legislation.gov.au(검색일: 2021.7.26.).

공개법 (Public Interest Disclosure Act 2013)의 적용을 받아 정보정책 및 절차 과정에서 일탈을 방지한다.

라. 국방정보국(DIO)[96]

DIO(Defense Intelligence Organization)는 2차 세계대전 시기 군합동정보국이 발전하여 1990년도 국방정보국으로 개편되었고 국방부장관의 지휘를 받고 있다. 주요 임무는 국방 장관·정책 결정자 및 군인, 기타 정보소비자들에게 가능한 최고의 정보를 제공하는데 있다. 국방능력 및 정책과정에서 합리성을 제고하는 데 주안을 두고 이루어진다. 또한, 호주의 보안 및 전략적 환경과 관련된 외국 및 외국기관에 대한 정보평가를 실시하는데 국방기술, 무기시스템, 사이버 위협 등이 주요 내용으로 다루어진다.

마. 호주영상정보국(AGO)[97]

2000년 호주 영상기구, 군사지리전략정보국 및 방위지형국을 합병하여 2013년 정보서비스 법(ISA)에 따라 호주 지리 영상 정보기구(AGO)이 설립되었다. AGO는 국방부의 지형 공간 및 이미지 정보기관으로서 그 기능은 다음과 같다.

- 호주 국경 밖의 인력과 조직의 능력·의도 또는 활동에 대한 지형 공간 및 이미지 정보 수집
- 호주 방위군의 작전, 목표설정, 훈련 및 요구사항을 충족시키기 위해 지형 공간 및 이미지 정보를 수집
- 연방 및 주 당국을 지원할 목적으로 지형 공간 및 이미지 정보를 수집
- 국방장관이 승인 한 정보를 연방 및 주 당국에 제공
- 군사작전에 필요한 정보를 방위군에 제공하고 정보 관련 문제에 협력

96) http://www.defence.gov.au/ago/about.htm(검색일:2021.7.20.).
97) http://www.defence.gov.au/ago/about.htm(검색일:2021.7.20.).AGO(Australian Geospatial intelligence Organization)는 2015년 수정된 '2001 ISA' 법에 따라 DIGO(Defence Imagery and Geospatial Organisation)가 AGO로 변경되었다.

바. 국가신호정보국(ASD)[98]

- 신호정보는 호주 방위군 및 호주 정부에 제공하여 군사 및 전략적 의사 결정과 정책 개발에 효과성을 제고
- 호주 밖의 인원이나 조직의 능력, 의도 또는 활동에 대한 정보를 제공
- 호주 정부의 요구 사항에 따라 외국 기관에 정보를 전달
- 호주 방위군에 군사작전을 지원하기 위해 정보를 제공하고 협력
- 암호화, 컴퓨터 및 통신기술, 관련 기능의 수행에 필요한 특수기술을 연방 및 주 당국에 제공
- 영국-미국 신호정보협정에 따라 5Eyes에 가입, 활동하며 지원

사. NICC(국가정보조정위원회)[99]

국가정보조정위원회(NICC, National Intelligence Coordination Committee)는 법정부차원의 정보통합 및 조정 기제이다. NICC는 국가정보실(Office of National Intelligence)의 사무총장이 주재한다. 영국 합동정보위원회(Joint Intelligence Committee)와 미국의 국가정보장(Office of Director of National Intelligence)와 유사한 기능을 수행한다. NICC의 역할은 국무회의와 국가안전보장회의의 지시에 따라 국가정보 우선순위에 대해 자문하고 호주 정보기관들의 목표와 활동 방식 등에 대해 조정하고 통제하는 역할을 수행한다. 구성 기관들은 국가정보실장(Director-General of the Office of National Intelligence), 호주비밀정보부장, 호주보안정보부장 등으로 구성되어 있다.

2) 정보 통제[100]

가. 정보서비스법 ISA 2001[101]

호주의 정보공동체의 활동에 관한 법적 기반을 제공하여 정보기관들이 정

98) https://www.asd.gov.au(검색일: 2021.7.20.). ASD(Australian Signals Directorate)은 종전의 DSD(Defense Signals Directorate)를 개편하였다.
99) https://en.wikipedia.org/wiki/National_Intelligence_Coordination_Committee(검색일: 2021.7.20.)
100) https://www.ona.gov.au/about-ona/governance/oversight-and-regulation(검색일: 2021.7.20.)
101)https://www.legislation.gov.au/Details(검색일: 2021.7.21.). ISA(Intelligence Services Act) 2001은 2001년 10월 제정 이래, 2016년까지 25회 개정, 보완되었다.

보활동을 수행할 있도록 기능한다. 또한, 이 법에 의거하여 의원이 정보활동을 감독할 수 있으며 의회 합동위원회를 설립할 수 있다. 의회는 정보기관에 대한 불만을 조사하고, 연방 및 주 법률 준수 여부를 검토하고 정보기관의 활동을 감독할 수 있는 정보보안 감독사무소 (IGIS)역할도 규정하고 있다. ISA 법안은 다양한 수단을 통해 정보기관들의 정보활동을 규제하며 이에 기초하여 각 장관의 특별 지침을 제정하여 국민들의 사생활 보호에 관한 규칙도 마련하고 있다.

나. 정보 및 보안 감독관(IGIS)[102]

감독관은 1986년 정보보안감독원법 (IGIS Act)에 따라 설립되었으며, 정보기관장으로부터 독립적인 정기 검사 및 정보활동을 모니터링할 수 있는 권한을 보유하고 있다. IGIS는 6개의 호주 정보기관인 ONA, ASIO, ASIS, DIO, AGO, ASD를 감독하며 법률과 지침을 준수토록 함으로써 합법적 활동을 유도하고 규정 위반시 독립적으로 조사할 수 있는 권한을 보유하고 있다.

- 조사를 수행하는데 필요한 증인의 출석, 증거수집, 문서 복사 및 보관, 정보기관의 출입을 포함하는 등 광범하고 강력한 권한을 보유
- 감독관은 예비 조사를 실시하여 전체 조사를 개시할지 여부를 결정하며 조사 후 정부에 권고사항을 작성하고 연례보고서를 의회에 제공
- 감독관은 자신이 동의하거나 국무총리 및 정보기관 책임자의 요청에 따라 모든 파일을 조사하고 언제든지 정보기관의 활동에 대해 소급하여 감사할 수 있는 권한을 보유

다. 의회 통제[103]

의회정보보안합동위원회(Parliamentary Joint Committee on Intelligence and Security)는 2001 ISA법에 근거하여 설립되었으며 정보기관을 통제할 수 있는 권한을 보유하고 있다. PJCIS는 하원과 상원의원들로 구성하여 모든 정보기관에 대해 감독 기능을 수행하며 정보기관의 운영 및 지출을 통제하고 있다. 위원회는 정보정책과 정보활동에 있어서 우선순위를 검토하는 일

102) http://www.igis.gov.au(검색일:2021.7.21.).IGIS(Inspector GeneralI Intelligence and Security)는 1986년 정보보안감독원법(IGIS Act)에 따라 설치되었다.
103) https://www.aph.gov.au/committee(검색일: 2021.7.20.)

은 없으나 정보공동체 각 기관의 정책·행정 및 성과를 포함하여 재무제표 관리와 지출내역 검토한다. 이 외에도 상원 재정행정위원회는 ONA·IGIS를, 외교국방통상위원회는 AGO·DIO· ASD를, 법사위원회는 ASIO를 각각 추가로 통제하고 있다.

라. 내각 통제

내각 국가안보위원회 (National Security Committee of Cabinet, NSC)는 장관급 의사결정기구이며 안보위원회비서실은 국가안보 문제를 고려하는 최고수준 관리위원회이다. 국가안보담당 차관이 위원장을 맡는 국가정보조정위원회(NICC)는 정보기관의 역량을 광범위하고 효과적으로 통합하고 있다. 수상은 ONI를 직접 관할하고, 내무부장관은 ASIO, 외교장관은 ASIS, 국방장관은 DIO, ASD, AGO를 각각 감독한다.

Ⅵ. 한국의 정보체계와 국회의 정보통제

1. 신안보환경과 정보활동

동북아 지역은 북한의 핵개발과 중국의 부상으로 안보질서가 격변하고 군비증강을 가속화해왔다. 21세기 동북아는 핵강국과 비핵국가들이 병존하면서 질서를 구성하고 있으며 특히, 북한의 핵개발은 핵질서 파괴 및 역 내 불안정성의 심화를 야기해왔다. 남북 정상회담 긴장 완화 분위기가 일시 창출되었으나 북한의 추가 핵역량 강화 동향이 포착됨에 따라 불안정성은 또 다시 고조되고 있는 실정이다. 중국·일본 등 주변 국가들은 치열한 국가이익을 추구하고 있다. 한국은 미국과 관계에서 대체로 추종적인 성격을 띠고 국가이익을 추구해왔으며 미국의 대북정책 변화에 민감하게 반응해왔다. 주변 강대국 사이에 놓인 지정학적 위치와 북한의 대남위협은 한국의 국가안보환경을 이루면서 안보전략과 정보활동에 중요한 요인으로 작용해왔다.[104] 한국은 반도적 위치로 인해 주변국가와의 지정학적 요인이 매우 중요하게 작용해왔으며 국가이익 추구나 위협의 대상면에서 북한 또는 북한과 관련된 사안에 국한되는 경향이 강하다. 문재인 정부 출범 직전까지도 북한의 직접적이고 명시적인 위협이 지속되고 있었다는 사실을 상기해볼 필요가 있다. 북한은 지난 70여 년간 요인 암살 및 납치 등 미시적 차원의 테러의 형태로부터 핵 및 미사일 발사 실험, 연평도 포격 등 거시적 차원의 직접적 군사공격을 감행한 바 있다. 소련과 같은 주적(dominant enemy)이 사라진 미국의 경우와 달리 한국은 여전히 국가로부터의 위협을 받고 있으며 북한의 비핵화와 이를 둘러싼 안보환경은 한국의 대외정책과 행동을 제약하는 구조적 요인으로 존재한다. 이러한 차원에서 볼 때 외부 위협요인을 정확하고, 신속하게 포착하고 전달하는 정보기관의 역할은 실로 중요하다.

현대 한국의 정보기관의 역사는 1948년 해방과 더불어 육군정보국이 설립되면서부터 비롯되었으나 1961년 5월 중앙정보부가 창설되면서부터 비로소 국가차원의 통합된 정보활동이 시작되었다.[105]중앙정보부(훗날 안기부, 국정원)를 중심으로 한국의 정보기관의 형성과정에서 나타난 주요 특징들을 살펴본다.

---

104) 한용섭, “부분별 국가전략의 상호관계와 우선순위의 변화,” 백종천(편), 『한국의 국가전략』(서울: 세종연구소, 2004), p.109.

105) 미국CIA의 권유로 1959년 1월 육해공군 장교들로 구성된 ‘중앙정보부’가 설립되었으며 1961년 1월 ‘중앙정보연구회’라는 명칭하에 20여명의 요원으로 구성되었다. 그러나 이들 정보기관은 법적 근거도 없었으며 중앙정보기구로서의 위상이나 기능을 부여 받지 못했다. 전웅,『현대 국가정보학』(서울 : 박영사, 2015), pp.486-487.

첫째, 처음부터 한국의 정보기관은 대북 정보수집과 방첩활동과 같은 본연의 임무와 함께 정권적 차원의 업무를 담당하기 위해 설립되었다. 중앙정보부의 설치 목적으로 “공산세력의 간접침략과 혁명과업수행의 장애를 제거하기 국가재건최고회의에 중앙정보부를 둔다”고 한 규정에서 분명히 드러난다.[106] 정보기관의 국내정치 개입 근절 노력은 1961년 중정창설 이후 지속되어 왔으나 정치적 중립성에 대한 논란은 끊임없이 제기되었다. 문재인 정부에 이르러서야 종지부를 찍게 된 점은 그나마 다행이라고 하지 않을 수 없다. 둘째, 정보기관 창설과 운영과정에서 민간 전문가들은 배제되거나 극히 제한적으로 충원되었다. 이는 미국과 달리 군의 정치개입이 30년간 지속된 데다 상대적으로 외부 민간 정보전문가 인력풀이 부족한 데 기인한 것으로 보인다. 김영삼 정부이후에야 민간관료들이 정보업무의 핵심역할을 담당했으나 폐쇄적인 조직운영의 문화와 관성을 단기간 극복할 수는 없었다. 이로 인해 정보개혁 요구에 대한 무관심과 거부, 성찰적 태도의 결여, 경쟁력 약화로 이어지는 결과를 초래하였다. 미국의 정보기관이 설립 초기부터 고위직에 민간인들을 포진시키고 다양한 외부 인력들을 충원한 것과는 대비된다. 한편, 군정보기관의 폐쇄적 운영 행태는 민간정보기관 보다 심하다. 군 특성상 일정부분 불가피한 측면도 있으나 특정 학교 출신인맥이 지배할 경우 조직의 효과성, 국가안보 목표보다는 자칫 사적 이해관계나 집단사고에 의한 정보업무를 수행할 가능성이 높다.

셋째, 정보기관의 개혁과 발전은 합리적인 로드맵에 의해 추진된 것이 아니라 정치적 요인에 의해 이루어진 결과 정보기관은 장기적인 정상적인 발전을 기대하기 어려웠다.[107]미국이 정보개혁과 발전전략이 주로 정보기관 본연의 업무 수행의 실패에서 비롯된 정보실패의 개선책 마련이라는 차원에서 진행된 것과는 사뭇 다르다. 정권 교체기 마다 단행된 한국의 정보개혁은 일관성의 결여와 전문성의 부족으로 소기의 성과를 이루지 못했다. 미국이 1970년대 의회 처치위원회가 정보위원회를 발족하여 정보기관의 불법 정치개입을 차단하고 정보활동을 제도적으로 지원해나간 사실과 차이가 있다. 정보실패를 방지하려는 종합적이고 성찰적인 노력 대신, 정치적 곤경이나 위기를 벗어나기 위한 임시방편적인 개편으로 일관하다보니 정권교체기 마다 개혁의 대상으로 전락하고 있다.

---

106) 국가재건최고회의법 제18조(1961.6.10.). http://www.law.go.kr.(검색일 : 2018.8.8.)

107)10.26사건 이후 1980년 국가안전기획부 창설, 1992 김영삼정부 등장이후 안기부의 개혁, 1998김대중 정부 출범이후 국가정보원으로의 개칭, 댓글과 특활비 상납으로 인한 2018년 이후 일련의 국정원 개혁 등으로 정보기관의 활동이 정치로 부터로 점진적으로 단절되는 긍정적인 성과도 있었다. 그러나 정보역량 강화를 위한 경쟁적 분석, 영상정보 역량 제고, 보안과 정보접근의 균형, 관리능력 제고와 같은 개혁은 이루지 못했다.

한편, 오늘날 위협은 전통적인 군사안보위협 이외 전염병, 기후변화, 사이버공격 등 다양한 요인에 의해 비롯된다. 이 같은 위협요인들은 미중경쟁의 국제정세와 연계되어 안보이슈로 발전한다. 최근 중국에서 발생한 코로나19는 세계적 대유행으로 선언되면서 미중 경쟁을 심화시키고 국제 안보 질서의 변화를 유발하고 있다. 코로나 전염병은 다양한 영역에서 안전 문제를 야기 시키고 나아가 국가안보의 문제로 발전하는 경향을 보이고 있다. 본 연구에서는 군사력에 치중하는 전통안보나 그 연속선상에서의 비전통 안보의 협소하고 소극적인 접근을 넘어 보건·사이버 등 분야에서 초국적으로 발생하는 새로운 위협을 이해하기 위해 신안보(emerging security)라는 개념을 제시한다.[108]

오늘날 우리가 직면하고 있는 새로운 안보 즉 신안보 위협은 기존의 위협과는 몇 가지 차원에서 차별화된다. 기존의 전통안보 위협은 국가나 테러단체와 같은 보이는 적(visible enemy)으로부터 근원을 두고 있다. 안보 위협은 비교적 가시적이며 예측가능하며 의도적인 경향이 강하다. 그러나 신안보 위협은 전염병, 기후변화, 식량위기에서 보는 바와 같이 주적 개념이 부재하다. 또한 신안보 위협은 전통안보에 비해 비가시적이며 예측이 곤란하며 주어진 것(a given)이 아니라 사회적으로 구성(socially constructed)되는 특징을 지니고 있다. 안보위협의 변화는 정보활동의 양상과 내용상의 변화뿐 아니라 활동 방식 또한 정보기관을 포함한 행정부처와 협업을 불가피하기 만들기 때문에 정보체계 작동방식에 커다란 변화를 야기한다. 정보요원의 충원에서부터 정보주기의 혁신, 정보통제에 이르기까지 과거의 패러다임과 방식으로는 효과적인 대응이 어렵게 되었다. 따라서 한국의 정보체계를 선진국과의 성찰적 비교를 통해 발전 방안을 마련하는데 국회정보위의 주도적인 역할이 요구된다.

2. 선진국 정보체계와 한국 정보체계의 비교

1) 선진국 정보체계 특징

가. 국내외 정보 및 수사기관의 분리

비밀 정보활동으로 인한 불법행위나 인권침해 가능성을 사전에 차단하기 위한 최소한의 장치는 법집행기능과 국가정보기능을 분리하는 일이다. 동서

108) 석재왕•오일석, “코로나19이후 신안보 위협과 대응전략,” 『경호경비학회』, Vol.No.60. pp.117-135.(2020).

고금을 막론하고 행정부처와 달리 비밀정보기관은 정치일정에 관여하거나 행정부처의 자율성을 침해해온 것이 사실이다. 이와 같은 이유로 미국 등 선진 정보기관은 수사와 정보의 통합보다는 분리형을 선택하여 통제를 용이하게 한다. 미국의 경우 9/11사태로 국내정보기관 설립에 대한 논의가 있었으나 인권침해 가능성을 들어 무산되었다.

20세기 초 근대 정보기관이 태동된 이래 사법경찰 기능은 정보기관과 분리되어 정보기관이 아닌 법무부나 경찰청 산하에서 이루어지고 있다. <표4.1>에서 보는 바와 같이 선진국들의 경우 대부분 분리형을 선택하고 있음을 확인할 수 있다.[109)]

앞서 서술한 바와 같이 미국은 CIA를 제외한 대부분의 정보기관을 국방부, 국무부 등 행정부처 산하에 설치, 운영하고 있다. 영국의 경우도 해외정보는 외교부 산하, 국내정보기관은 내무부 산하에 설치, 운영하고 있다. 심지어, 불가리아나 루마니와 같은 체제전환 국가들도 국내외 수사 분리형 정보체계가 민주적 요구와 국가안보 수요를 잘 충족시킬 것이라는 확신에서 비롯된 것이다.

<표4.1> 국가별 정보기관 유형 비교

유형	주요 국가	비고
국내외 정보 및 수사 분리형	o 서방권 : 미국, 영연방 국가, 프랑스, 이스라엘 등 o 체제전환국가 : 불가리아, 헝가리, 루마니아 등	
국내외정보 및 수사통합형	o 중동 및 이슬람국가 : 이라크정보부(IRIS, 혁명평의회),사우디 정보총국(GIP) 등 o 아시아 : 한국 국정원	
국내정보수사통합형	o 유라시아 및 중동 : 러시아 연방보안부(FSB), 이집트 보안총국(SSIS) 등 o 아시아 : 말레이시아 국내정보부(SB) 등	
국내외정보통합형	o 동유럽 및 중동 : 불가리아 정보부(NSS), 크로티아 보안정보부(SIA), 이집트 정보부(GIS) 등 o 아시아 : 인도 내무성 정보부(IB),인도네시아 국가정보보부(BIN), 대만 국가안전부(NSB) 등	

109) 한국에서는 5.16혁명 과업 수행을 위해 창설된 중앙정보부는 국내정보, 해외정보, 수사기능 통합된 기관으로 60년 이상 유지된 결과 동일한 기관 내에서 정보와 수사 양 기능의 융합 또는 존치를 별다른 문제의식 없이 받아들이는 경향이 있다. 양 기능을 동시에 보유한 정보기관의 문제점은 중앙정보부를 창설한 김종필 전부장이 “대공수사권을 검찰에 넘기고 정보기관의 기본 임무만 수행하면 된다”고 언급한 데서 잘 드러난다(.http://blog.joins.com/media/folderlistslide.asp.검색일: 2021.7.70).

나. 정보공동체(Intelligence Community)구축

선진국들은 법적 근거와 무관하게 실제 정보기관 협의체나 공동체를 운영하고 있다. 미국의 경우 가장 일찍 1947년에 국가안보법을 제정하여 정보공동체를 운영하기 위한 기본적인 틀을 마련하였다.[110]이렇게 함으로써 개부처수준을 넘어 국가차원의 정보활동이 가능하다. 이는 분할 통치(divide and rule)의 원칙이 반영된 것으로 특정 부처가 정보를 독점할 경우 발생하는 폐단을 최소화하고 정보기관 이외 부처의 전문성을 활용하는데 매우 유용하다. 국방부산하 정보수집기관인 NRO, NSA, NGA와 DNI 산하 국가대테러센터(NTCT) 및 국가정보위원회(NIC) 등이 대표적인 사례에 해당된다. 이들 기관은 형식적으로는 개별 부처소속으로 되어 있으나 국가 차원에서 정보활동을 수행하고 있다.

융합 센터(fusion center), 미션 매니저(mission manager)와 같은 유연한 조직을 신설하여 관료제적 병폐를 최소화하고 있다. 관료적 이기주의와 계층제에서 오는 정보왜곡과 정보실패를 예방하기 위해 다양한 방식의 정보조직을 운영하고 있다. 9/11이후 미국 정보기관 특히 CIA의 경우 계선조직과 함께 통합된 정보 생산을 위한 센터 형식의 조직을 운영하고 있는 것으로 알려져 있다.[111] 한편, 군 정보기관 운영과 관련 독일, 영국 등 선진국의 경우 개별 군 정보기관의 운영을 축소하고 있는 데 비해, 미국은 1962년 국방정보를 총괄하는 DIA의 설립에도 불구하고 육·해·공군·해병대 별도의 정보부대를 운영하고 있다.[112]

다. 국가정보조정 협의체 운영

미국을 비롯한 대부분의 선진국들은 정보공동체 이외 국가차원에서의 정보통합과 조정을 위해 정보기관 및 군·행정기관 소속 정보기관들로 구성된 협의체를 <표4.2>에서와 같이 운영하고 있다. 미국의 경우 합동정보공동체위원회(Joint Intelligence Community Council, JICC)를 보면 국가정보장(DNI)이 의장으로 있으며, 국방장관, 국무부장관, 검찰총장 등이 참석한다. 이 위원회는 행정부처의 정보요구, 정보성과 평가, 예산 등을 DNI에 자문하는 임무를 맡고 있다. JICC 위원들은 DNI가 제공한 정보와 상반되는 내용을 대통령에게 보고할 수 있는 권한을 가지고 있다.

110) Lowenthal(2012), p.31.
111) https://www.cia.gov/index.html(검색일: 2021.7.25.)
112)전웅(2015), p.378.

< 표4.2> 주요 국가의 정보 협의체

국가	기관명	구성 단위
미국	국가정보장(DNI)	국무부, 법무부, 재무부, 에너지부 등 17개 기관
영국	합동정보위원회(JIC)	국내외 정보기관, 외교부, 재무부, 통상산업부 등
프랑스	국가정보위원회(CNR)	총리, 정보기관장, 국가정보조정관 등
이스라엘	정보기관장협의체(CDIS)	국내외 정보기관장

위의 <표4.2>에서 보듯이 이들 국가의 정보조정기구들은 정보 최고 소비자(대통령, 수상)직속으로 설치, 운영되고 있는 관계로 정보 통합·조정의 실효성이 보장되고 있다. 한편, 행정부처 또는 정보기관 내 정보조정협의체를 신설·운영하고 있는 경우가 있다. 이 역시 특정 정보기관의 정보 독점·남용 방지 및 행정부처와 정보기관의 융합을 통한 시너지 효과를 거양하는데 그 목적이 있다. 영국의 합동테러분석센터(JTAC), 이스라엘 정보기관장회의(CDIS)가 대표적인 사례에 해당된다.

라. 효과적인 중층 통제 시스템

미국 등 선진국들은 정보기관의 일탈과 불법활동을 방지하기 위한 다양한 통제 기제를 마련하고 있다. 통제 주체는 의회, 행정부처, 독립된 감사관, 법원 등 다양하다. 특히, 이들 상당수 정보기관들은 행정부 산하에 설치되어 있는 관계로 장관을 비롯한 행정부 통제를 받고 있는 점이 주요 특징이다.

<표4.3> 주요 국가의 정보통제 유형

주체	대상	비고
의회	미국, 영국, 호주 등 선진국 정보기관	
대통령 또는 수상	미국(대통령정보자문위원회,예산관리국), 프랑스(국가정보조정관실), 독일(정보조정관실), 일본(내조실), 호주(국가정보평가실), 아태리(정보차관)	
행정부처	법무부(미국), 내무부(영국, 독일, 캐나다, 프랑스, 호주 정보기관), 국방부(프랑스 해외정보기관), 외교부	

	(영국,호주 정보기관 등)	
(독립) 감사관(IG)	미국(CIA, FBI, NRO, NGA, NSA), 호주(ASIO)	* 호주의 경우 감사결과를 홈페이지에 공개

① 대통령 정보자문위원회(President's Intelligence Advisory Board): 자문위원들은 대통령에 의해 임명되지만 초당파성을 유지하며 보고 받은 내용에 대한 비밀은 엄격하게 유지한다. 주요 임무로는 대통령에게 정보활동 향상을 위한 권고안이나 연구결과들을 보고한다. 그리고 정보활동의 양과 질 그리고 적절성을 평가하고, 조직 및 인력의 효과성을 진단하고 정보를 수집·생산·평가하는 모든 기관들의 활동을 평가한다.
이러한 노력 덕분에 PIAB는 60년 이상 미국 정보기관의 활동과 조직에 영향력을 지속 행사해오고 있다. 안보·학계 및 민간단체인사들로 구성된 비상설 조직으로 운영되고 있으며 정치적 책임은 지지 않는다.[113]

② 정보감독위원회(Intelligence Oversight Board, IOB) : PIAB의 부설기관으로 정보기관의 감사관과 법률고문으로부터 정기적으로 보고를 받으며, 지휘·감독권한을 갖는다. 정보기관의 활동이 헌법, 행정명령 및 대통령 지시와 부합하는지 여부를 감독하고 정보활동의 합법성과 우선순위 평가와 관련하여 대통령에게 자문한다. 또한 검찰총장이나 DNI 등이 제기하지 않는 정보활동에 대해서도 자문을 한다. 정보활동 위법성 여부에 대해 조사하는 권한을 갖고 있지만, 사건을 추적하거나 인력을 소환할 있는 권한은 없다. 불법적인 정보활동을 발견하는 즉시 대통령과 검찰총장에 통지하는 임무도 맡고 있다.[114]

③ 감사관실(Office of the Inspector General, OIG) : 1989년에 설립된 감사관은 독립적인 감사 업무를 수행하고 있으며 감사관은 대통령과 상원의

113)1956년 아이젠하워 대통령은 미국의 정보활동에 관하여 진솔하게 평가하고 자문을 제공할 수 있는 인사들로 구성된 대통령 해외정보활동자문위원회(President's Board of Consultants on Foreign Intelligence Activities, PBCFIA)를 설립하였다. 이후 케네디 행정부 시기 대통령 해외정보자문위원(President's Foreign Intelligence Advisory Board, PFIAB)로 개칭하고 2008년 부시 대통령시기 대통령정보자문위원회(President's Foreign Intelligence Advisory Board, PIAB)로 명칭을 변경하였다. https://obamawhitehouse.archives.gov/administration/eop/piab/history(검색일 : 2019.7.12.)

114)전웅(2015), p.575.

인준에 의해 임명되며, 대통령에 의해 해임된다.[115] 법률 제50조 규정에 의해 감사관은 CIA부장과 의회에 대해 보고한다. 독립부서로서 회계감사, 감독, 조사, CIA프로그램(공작, 분석, 예산 등)과 정보활동에 대한 검토를 통해 CIA업무를 관리하고 경제성과 효율성, 그리고 책임성을 증진시킨다. 감사관은 정보활동과정에서 발생할 수 있는 직원들의 규정 위반, 사기, 권한 남용 등에 대해 CIA국장이 충분히 인식토록 정보를 제공한다.
독립 감사관은 감사결과를 직속 상관인 CIA부장에게 보고후 30일 이내 의회 정보위원회에도 보고해야 한다. 다만, 정보기관의 불법활동이나 심각한 권력 남용이 있다고 판단할 경우 CIA국장의 의사에 반하여 조사하고 그 결과를 CIA국장과 의회 정보위원회(7일 이내) 에 제출한다.

④ 행정부처에 의한 정보통제 : 선진국 정보기관은 기본적으로 행정부처 산하에 설치되어 있는 만큼, 행정부의 통제를 받게 되어 있다. 대부분의 정보기관장들은 차관보급이나 차관급으로 장관의 통제를 받고 있다. 물론, 모든 비밀정보를 장관에게 보고하는 것은 아니지만, 장관이 정보기관장들에 대해 정치적 책임을 지는 만큼 행정부처 통제가 이루어진다. 또한, 정보기관은 직속 장관 뿐 아니라 대통령이나 수상실에서 정보기관에 대한 통제를 실시하고 있다. 미국 백악관의 경우 예산국(OMB)와 NSC를 통해 정보공동체의 활동을 통제하고 조정하고 있다. 프랑스나 독일 등 기타 선진국가들도 예외없이 정보통제 및 조정 직제를 신설, 운영하고 있다. 이러한 조치들은 분리형 정보시스템을 채택하고 정보 사각 지대와 부처 이기주의를 최소하려는 차원에서 통합기제를 운영하고 있다.

3. 한국 정보체계의 특징

1) 정보 기구

미국 등 선진국의 복잡한 정보조직에 비해 한국의 정보조직은 비교적 단순하다. 전 세계 걸쳐 군사력을 투사하면서 이익을 추구하는 선진국의 정보기관의 조직규모와는 다를 수 밖에 없다. 한국 정보기관은 다음과 같은 조직상의 특징을 나타내고 있다. 첫째, 국정원의 경우 대통령 직속 기관으로 국내외 및 수사기능을 통합한 정보기관 형태를 유지하고 있다. 앞에서 언급한 바와 같이 국정원은 5.16군사 혁명의 과업수행 목적으로 1961년 창설된 이래 탈냉전기와 민주화 과정을 거치면서도 통합형 틀을 유지하고 있다. 문

115) https://www.cia.gov/offices-of-cia/inspector-general(검색일 : 2021.7.14.).

재인 정부가 출범하면서 안보와 무관하거나 거리가 먼 국내 정보수집이나 정보관(I/O)를 폐지하였으나 방첩 및 보안정보활동은 그대로 수행하고 있어 국내외 통합정보 유형의 틀은 유지되고 있다.
둘째, 북한 및 해외정보 분야를 중심으로 정보활동이 이루어지고 있으나 조직 구성면에서 보면 여전히 국내정보기관의 비중이 높다. 국정원의 조직체계를 정확하게 알 수는 없지만 문재인 정부에서도 국내 정보를 담당하는 지부조직가 유지되고 있다는 사실이 이를 뒷받침한다.
셋째, 각 부처별 개별 정보활동위주로 이루어지고 있으며 정보활동을 통합·운영하는 시스템이 존재하지 않는다. 그 결과 정보기관, 행정부처 및 군정보기관간 대통령에 대한 보고를 둘러싼 소모적인 경쟁이 치열하다. 청와대 국가안보회의(NSC)는 정책심의 기관이라는 점에서 정보활동만을 대상으로 조정·협의하는 영국의 JIC와 차이가 있다.
넷째, 정보조직이 전통적인 편성 원리인 지역과 기능위주로 이루어지고 있다. 한국의 정보기관에서 정보기술의 발달과 전쟁 유형의 변화 등 정보환경의 변화에 따른 융합조직이나 네트웍 중심의 조직은 매우 제한적으로 운영되고 있다. 미국에서 융합적인 업무를 수행하는 센터와 같은 조직도 기존 계선조직에서 다루기 어렵거나 애매한 업무를 처리할 목적으로 운영하고 있다.

2) 정보활동

정보활동의 범위와 성격은 한국을 둘러싼 안보환경, 특히 지정학적 요인으로부터 크게 영향을 받는다. 미국과 영국의 경우 해양으로 둘러싸인 관계로 외부로부터 위협강도가 중국이나 이스라엘 보다는 매우 낮았다. 한국 정보활동의 방향은 안보위협과 밀접한 관계가 있는 바, 북한의 핵개발 동향이나 의도가 가장 중요한 정보활동의 목표가 될 수 밖에 없다.
다만, 탈냉전이후 국제테러 단체와 같은 주요 행위자들을 대상으로 한 정보활동 확대되었고 최근에는 사이버 단체나 외국의 대규모 전염병 동향도 정보활동의 대상이 되고 있다.
정보활동의 범위와 관련하여 정보협력 또한 중요한 요인이 된다. 한국의 지정적학 위치나 국력, 그리고 국익적 차원에서 볼 때 우방국 정보기관들과 정보협력을 통한 유가치 정보의 입수는 매우 효과적인 정보수집 수단이 된다. 동맹관계에서 볼 때 강대국의 경우 기술정보를 제공하고 피후견 국가들의 경우 휴민트를 제공함으로써 상호 보완적인 관계를 유지하는 경우도 많이 있다.

정보활동 유형면에서 볼 때 문재인 정부 이전까지는 국내정보활동이 해외정보활동 보다 비중 있게 다루어지고 있었으며 정치일정에 개입하거나 대통령의 정무적 기능을 보좌하는 역할까지 담당해왔다. 국정원의 정치개입 활동은 안기부, 국정원 등으로 정보기관의 명칭 변경에도 불구하고 지속되었으며 기무사의 민간인 사찰이나 세월호사건 관련 보고서에서 보듯이 한국의 정보기관은 민간·군정보기관을 막론하고 정치화되고, 일탈이 일상화된 상태에서 정보활동을 수행했던 것으로 드러났다. 한편, 정보와 정책관계를 보면 이들 양자 간의 합리적 연계성은 그리 높지 않은 편이다. 정보사령부는 주로 군사 휴민트 및 영상 첩보 수집, 대북 공작 업무를 수행하는 등 최근 업무 영역을 확대하는 것으로 알려져 있다.[116] 한국의 정보기관들은 미국과 달리 정보공동체나 정보조정협의체가 형성되지 않은 관계로 개별 부처의 이기주의가 매우 강해 국가차원의 통합된 정보활동이 이루어지지 않고 있다.[117]

3) 정보와 정책관계

정보소비자 또는 정책과의 관계에서 한국의 정보기관, 특히 국정원은 최근까지 대통령에 대해서는 맹목적인 충성을 보인 반면 행정부처에 대해서는 우월적인 입장을 견지하는 양면적 태도를 보여 왔다. 이로 인해 남북관계와 해외 분야 정보적 성과에도 불구하고 비난과 개혁의 대상으로 전락하였다.[118]국정원은 대통령 직속기관으로 대통령의 지시를 수행하였으며 정기적인 보고는 대부분 대통령에게만 집중되었다. 대통령은 국회의 반대에도 불구, 원장을 임명할 수 있으며 대통령으로부터 지휘·감독을 받는다. 대통령은 직원의 정원, 조직의 설치, 보안업무 기획조정권한도 보유하고 있기 때문에 정보기관은 대통령으로부터 거의 모든 것을 승인을 받는다.[119]말하자면 대통령은 인사, 조직, 정보활동 모든 면에 영향력을 행사할 수 있으며 정치적 목적으로 정보기관을 이용할 경우에도 이를 견제할 수 있는 장치가 사실상 전무하다. 대통령과 정보기관의 수직적 지배관계는 다른 어떤 요인보다 막강한 영향력을 미친다.

반면, 행정부처와 정보기관의 관계는 대통령과의 관계와는 매우 상반된 형태로 진행되었다. 한국 정보기관은 서구 정보기관과 달리 행정부로부터

116) 국가정보포럼, 『국가정보학』(서울 : 박영사, 2006), p.262.
117) 한국의 정보기관의 발전방안의 일환으로 정보공동체 형성 필요성에 대해서는 다음 논문을 참조. 석재왕, “한국형 국가정보공동체 형성 방안,”2018 국회 정보개혁 세미나(2017.11.24.)
118) 김당, “한국의 국가정보기관,” 『국가정보론』, 문정인(편), (서울: 박영사, 2001), p.592.
119) 국가정보원법 제3조, 4조, 7조.

지휘와 평가를 받지 않은 것은 물론 대통령 보고, 공직자 신상 보고를 통해 일반 행정기관을 견제하고 감독해왔다. 이 같은 업무 관행으로 행정기관에 대한 정보 지원업무는 부차적이었으며 상황논리에 따라 좌우되었다. 이와 같은 형태의 정보기관은 근대화 과정에서 대통령의 정책적 의지를 관철하고 국내외 통합적 정보활동을 통해 다소 순기능을 발휘한 것은 사실이다.[120] 그러나 국내에 치중된 정보활동은 외부 위협에 대한 조기경보 시스템 구축과 예산의 활동에 무관심하거나 정보의 정치개입을 초래함으로써 부작용을 양산하였다.[121] 정보기관은 대통령의 선호나 정권의 정책과 일치하지 않는 행정업무는 감독 되거나 조정되었다. 행정부처들이 정권의 목표와 부합하지 않을 경우 충성심이 약하거나 잘못된 것으로 인식하기도 했다. 따라서 조정의 대상으로서 행정기관이 정보기관의 통제와 관련하여 영향을 미칠 수 있는 부분은 매우 미약하다.[122]

120) 김당(2001), p.591.

121) 정보의 정치화(Politicization of Intelligence)는 정보기관이 정보소비자의 선호나 요구에 영합하는 정보(intelligence to please) 생산하거나, 정보기관이 정치적 쟁점이 되거나 또는 대중들에 의해 논쟁이 대상이 되는 경우를 의미한다(. 정보기관이 직접 정치에 개입하는 경우는 서구 학자들이 말하는 정보의 정치화와는 상이한 개념이다.(Cimbala,Stephen J.(eds.)*Intelligence and Intelligence Policy in a Democratic Society* (Dobbs, NY: Transnational Publishers, 1987), pp.25-44. 정보기관의 정치개입으로 인해 정치권과 대중들사이에서 쟁점화되는 경우에는 정보의 정치화 현상으로 볼 수 있을 것이다.

122)행정부처 정보통제 가운데 감사원의 감사는 일정부분 정보기관의 자의적인 예산 남용을 방지할 수 있는 효과는 있을 것으로 보인다.

Ⅳ. 한국형 정보협의체 형성 방안과 국회 역할

한국의 정보시스템은 해방 이후 냉전기를 거쳐 성장해오면서 많은 개혁과 변화를 겪었으나 여전히 구조, 활동적 측면에서 많은 문제점을 안고 있다. 수사·정보 활동 및 정책기능의 혼재, 분명한 목표와 비전의 부족, 국가정보시스템의 결여 등이 문제점이 지속 나타나고 있기 때문이다. 이제 국가안보는 더 이상 정보기관이나 안보기관만의 전유물이 아니다. 민주주의 진전, IT의 발달, 미중 전략 경쟁의 격화, 대규모 전염병의 확산 등 환경의 변화로 인해 정보기관이나 정책기관만으로 대응하기에는 한계에 봉착했기 때문이다.

따라서 안보·정치적 상황 변화를 고려하면서 정보기관과 안보 및 여타 행정부처의 정보역량 강화를 통한 국가정보시스템을 새롭게 구축할 필요가 있다.

1. 정보협의체 형성방안

1) 청와대 직속 독립된 국가정보위원회 신설

현재 한국의 어떤 정보기관도 과거와 같이 정보를 독점하거나 각 부처를 조정하여 정보를 생산할 수 없다. 이러한 사실은 개별 부처 차원을 넘어 국가 차원의 정보 생산의 필요성을 말해주고 있다. 따라서 부처 간 정보공유 확대, 정보 왜곡 및 남용방지, 정보소비자 위주 정보생산, 정보 협력 강화, 정보예산의 심층 검토 등을 위해 정보기관과 행정부처가 참여하는 정보 협의체를 신설·운영할 필요가 있다. 이 협의체는 형식적, 일방통행식이 아닌 정보 거버넌스(Intelligence Governance) 방식으로 운영된다.

한편, 정보기관들로만 구성될 경우 이스라엘의 정보기관장 협의체(CDIS)를 모델로 하여 국정원장을 위원장으로 한 (가칭) ‘국가조정 협의체’를 신설, 운용하는 방안도 있으나 참여 기관의 거부감과 반발의 해소 여부가 관건이 될 것이다.

협의체는 부처 간 정보공유, 정보 흐름의 문제점 점검, 정보 협력 강화, 정보목표 우선순위 결정, 정보기관 평가 등 다양한 기능을 수행하게 될 것이다.

구성은 장관급 및 차관급 정보 협의체로 구성되며 정책 관련 업무는 배제된 협의체는 청와대 내 2가지 유형으로 설치하되 장관급협의체에는 NSC실장을 비롯하여 국정원장, 국방·행안·통일·외교부 등 안보부처 장관과 행안·산자부 등 신안보 분야와 밀접한 관련이 있는 부처가 참석한다. 또한, 장관급 협의체를 실무적으로 뒷받침하기 위해 차관급 협의체를 구성할 필요가

있는데, 장관급 협의체 참여 기관 차관급 인사와 경찰청, 해양경찰청 및 관세청 등 주요 차관급 기관들이 참여하여 전통안보 이외 다양한 안보위협을 대처할 수 있도록 해야 할 것이다.

2) 국가정보조정관제도 도입

국회에 의한 비밀정보기관의 통제는 사후통제인 만큼 외부통제는 한계가 있을 수밖에 없다. 따라서 행정부처를 통제하는 권한을 보유하고 있는 청와대에 의한 통제는 효과성이 높을 것으로 판단된다.
특히, 국가정보조정관은 안보실 산하에 설치된 경우 정보기관은 물론 행정부처 내 정보기관들 간 업무 조정, 정보목표에 대한 우선순위를 조정하거나 정보활동에 대한 기본적인 방향을 제시하는 일을 하게 될 것이다. 다만, 국가정보조정관 역시 행정부처 산하인 점을 고려해볼 때 통제에는 한계가 있을 수 있다. 자칫, 정보의 정치화를 유도하는 요인으로 작용할 수 있다는 점에서 도입 시 독립성을 보장하는 장치도 함께 마련해야 할 것이다. 아래 <표5.1>에서 보는 바와 같이 선진국들은 대통령이나 수상실에 정보통제기구를 설치하고 있다.

<표5.1> 주요 국가별 행정부처 정보통제 유형

구분	소속	정보 조정·감독기관	비고
미국	대통령	o 정보자문위원회(PIAB) o 정보감독위원회(IOB)	
		o 예산관리국(OMB)	
		o 국가안보회의(NSC)	
프랑스		o 국가정보조정관	
독일	총리	o연방총리실정보업무조정실(Abteil-ung VI, 제6국)	
		o 정보조정관	
호주		o 정보 및 보안 감사관(IGIS)	
		o 국가정보평가실(ONA)	
이태리		o 정보차관(정보정무장관)	
		o 보안정보부(SID)	

3) 대통령 국가정보자문위원회 신설

자문위원회가 설치될 경우 주요 임무는 정보기관의 성과와 효율성을 평가하고 정보역량을 강화할 수 있는 방안을 대통령에 조언하는 역할을 하게 된다. 최고 정보소비자인 대통령으로 하여금 정보의 중요성을 인식시키고 국가정보 운영 방향과 정보역량 강화 방안 등 광범위한 주제에 대해 자문하는 기능을 담당하게 될 것이다.
자문위원회는 대통령이 정보 기관에 대해 관심을 갖고 관리·통제하는데 크게 기여할 것으로 보인다. 정보활동의 선진화와 효과적인 조직 관리에 대한 권고를 통해 정보기관에 대한 통제 효과도 거둘 수 있다. 특히, 대통령 직속인 국정원의 경우 대통령 이외 여타 행정부처로부터 간섭이나 통제를 거의 받지 않는 상황에서 대통령자문위원회의 효용가치는 크다. 국정원장 이외 다른 채널을 통해 정기적으로 대통령에게 정보 관련 사안들이 보고되고 평가된다는 자체만으로도 정보기관으로서는 긴장할 수 있다.
위원회의 숫자는 정보·외교·군 고위인사, 중진급 학계 10여 명 정도면 무난할 것으로 보인다.

4) 내부 견제 장치의 도입

한국의 정보기관들은 냉전기 권위주의 시대에 설립된 만큼, 견제와 균형의 원리가 제대로 작동하지 않은 경우가 많다. 최근 이들 기관들의 정치개입이나 일탈행위에서 보듯이 내부 통제 장치가 사실상 전무한 점이 잘 드러난다.
정보기관장이나 청와대로부터 일정부분 독립성을 갖춘 감사관제도나 법률고문제도를 도입하여 정보기관의 내부 통제를 확립하는 방안을 고려해볼 필요가 있다. 미국 CIA, FBI 및 국방부 산하 정보기관, 그리고 호주와 뉴질랜드 정보기관들이 운영하고 있는 독립감사관 제도를 도입하여 정보의 정치화나 불법 활동을 최소화하는데 유용할 것으로 관측된다.

2. 국회 정보위원회 통제[123]실태와 문제점

1) 청와대로부터 독립성의 부족

한국의 정보위원회의 경우 설립 당시부터 행정부로부터 독립되어 의회가 독자적으로 정보위원들을 임명할 수 있었다. 미국 정보위원회 위원들은 소속 정당의 의원총회에서 선출되고 정보위원장은 다수당 의원 중에서 상원의장이 임명한다. 하원의 경우 상원과 다르게 각 당 원내총무의 추천에 의해 하원의장이 임명하며 정보위원장도 하원의장이 지명한다.
반면 영국 의회의 정보보안위원회의 임명권이 수상에게 있기 때문에 행정부로부터 독립성을 확보하지 못한 것으로 보이나 의원 내각제인데다 임명과정에서 수상이 야당과 협의하고 있는 점을 고려해보면, 독립성이 크게 훼손되는 것은 아니다. 한국의 경우는 당 대표가 소속당 정보위원을 의장에게 추천하면 의장이 부의장과 각 당 대표와의 협의를 거쳐 임명하도록 되어 있다. 국회 정보위원회 위원의 임명과 활동 방식은 국회 정보위가 독립성을 확보할 수 있는지를 결정하는 중요한 요인이다. 한국의 경우 형식적으로는 국회의 자율성이 높은 것으로 보이지만, 실제로는 대통령의 의중이 많이 반영되어 독립성이 약한 것이 현실이다.

2) 높은 당파성

국회의 정보통제는 기본적으로 여야 간 이해관계를 떠나 공정하고 객관적으로 수행되어야 한다. 그러나 현실은 의회가 당파성을 극복하지 못하고 여야가 사사건건 충돌하는 경우가 빈번하게 발생한다.[124]
미국의 경우 상원은 비교적 초당적으로 운영되고 있는데 반해 하원은 당파성이 강한 것으로 나타난다. 한국의 경우 당파성이 강하게 표출되는 경향아 빈번하여 정보공동체에 대한 효율성이 낮을 뿐 아니라 정보역량 강화를 위한 발전적인 방안을 모색하기도 어렵다.
의회 정보위원회의 비정치성과 비당파성은 또한 위원장의 선출방식과도 밀접히 연관되어 있다. 초기의 미국 정보위원회가 초당파적으로 운영될 수 있었던 것은 합리적 리더십을 갖춘 위원장들이 있었기 때문에 가능하였다.

---

123) Oversight는 일반적으로 수평적인 관계에 있는 부처에 대한 감독 또는 감독을 의미하는 데 반해 Control은 수직적인 명령계통에 있는 기관을 대상으로 한 감독을 의미한다. 그러나 한국의 정보학계에서는 양자에 대한 구분 없이 혼용하는 경향이 있는데 본 논문에서도 감독이라는 용어로 통일적으로 사용하였다.

124) 전웅(2015), p. 602.

한국의 정보위원회 위원장도 회의를 주재할 수 있는 권한을 가지고 있기 때문에 위원장의 정치적 태도에 따라 정보위원회의 회의가 개최되지 않을 수도 있다. 이처럼 의회 정보위원회의 운영과 관련하여 위원장이 막강한 권력을 행사하고 있기 때문에, 국가정보개혁을 위해서는 강력하고 초당적인 리더십을 가진 위원장을 발탁해야 한다.

3) 낮은 전문성

정보위원회의 전문성은 당연히 효과적인 정보통제에 중요한 요인이 된다. 정보에 대한 전문성은 국가안보에 영향을 미칠 수 있고 정보기관의 활동 방향과 범위, 정보개혁에도 중요한 영향을 미칠 수 있다.
정보위원회의 전문성이 여타 위원회보다 낮은 데는 몇 가지 이유로 설명될 수 있다. 첫째, 국가정보 관련 경험이나 연구를 할 수 있는 영역이 거의 없기 때문에 정보위에서 활용될 수 있는 여지가 많지 않다는 점이다. 21대 국회의원 분포를 보면 순수하게 국가정보와 관련한 경험을 갖춘 위원은 김병기 위원 정도에 불과하다.[125]
둘째, 정보위원들의 재임 임기가 2년 미만인데다 높은 교체율로 인해 전문성이 낮다. 한국 정당의 잦은 이합집산과 변화로 인해 정보위원 또한 탈당과 입장을 수시로 하면서 교체율이 높을 수밖에 없는 구조이다. 셋째, 정보위를 지원하는 전문 보좌진이나 사무처 직원들의 낮은 전문성과 무관심도 요인으로 작용한다. 한국 정보위의 경우 수석 전문위원이 1명에 불과하고 대부분의 사무처 직원들도 정보업무와는 무관한 배경을 가지고 업무를 처리하고 있다.

3. 국회 정보위원회 역량 강화 방안

1) 정보위원 및 사무처의 전문역량 제고

2020.12 국정원법 개정 이후 정보통제의 필요성은 더욱 증가된 만큼, 정보위원들의 전문성에 대한 필요성은 더욱 증대되었다.[126] 앞에서도 언급했듯이, 한국 정보위원회의 경우 정보와 관련한 경험이나 높은 전문성을 가진 의원들이 소수인데다 데다 임기 2년 위원들의 잦은 교체로 전문성을 갖추기

125) https://www.assembly.go.kr/assm(검색일: 2021.8.5.).
126) 정보위원회 재적위원 2/3찬성시 정보조직·소재지 및 정원 공개 관련 실효적 이행 방안 확보, 정보경찰 및 대공수사권 확보로 비대화된 경찰권 통제,정보통제가 별무한 군정보기관(정보사, 합참 등)에 대한 민주적 통제 강화 필요성 등이 주요 요인이 될 것이다.

어려운 실정이다. 이 같은 문제점을 개선하기 위해 다음과 같은 방안을 고려해볼 수 있을 것이다. ①정보위원장과 위원들의 임기를 2년에서 과거와 같이 4년으로 환원하고[127] ②외통위나 국방위 등 관련 상임위와의 겸임을 활성화하고 ③ 미국 하원정보위원회와 유사한 소위원회[128]를 설치하는 한편, ④전문가들로 구성된 국회정보자문원회를 설립하여 전문성을 제고하는 방안을 생각해볼 수 있다. ⑤ 비밀정보기관을 감독하는 정보위원회의 활동이 재선이나 지역구 활동에 도움이 되지 않은 경우가 많은 점을 고려하여 국회 또는 당 차원에서 정보위원에 대한 정치적 배려도 필요하다.
⑥ 의원 보좌진들에게는 승진 및 교육의 기회를 확대하는 한편, 국가정보학 전공 석박사들의 채용을 검토해볼 필요가 있다. ⑦ 이와 함께 국회의정연수원 내 정보 관련 교육과정 개설, 전문가 초빙 특강 등을 통해 직원들의 관심과 전문성을 제고할 필요가 있다. 한편, <표5.2>에서 보는 바와 같이 미국 의회조사국(CRS)과 정보위원회의 연구보고목록은 한국 국회의 전문성 향상에 시사점을 줄 수 있을 것이다.

<표5.2> 미국 의회조사국 및 정보위원회 주요 보고서 목록

주체	내용(일시)
의회 조사국	정보공동체 : 국가 및 국방정보(2020.12), IC리더십의 임명 일시 및 규정(2019.3.19.), 정보공동체 내 고발자 보호방안(2019.1.18.)
	국가방첩보안센터 개관(2018.10.18.) 의회의 정보공동체의 비밀공작 및 비밀정보활동에 대한 감독 기본방향(2018.5.15.)
	정보공동체 지출(spending): 추세와 이슈(2016.2.16-6.18)
정보위원회	정보 관련 각종 법률에 대한 DNI에 대한 질의서(2018)/ DNI대상 사이버공격 관련 정보 요구서(2018)/FBI의 클린턴 이메일 조사 관련 추가자료 요청서(2018) 등

2) 국회 정보자문위원회 신설

미국 등 선진 국가들과는 달리 우리의 경우 청와대나 국회 내 초당적으로 정보기관에 대한 연구와 자문 기능을 수행하는 기관이 전무하다. 국가안보

127) 미국 상원정보위원회는 위원들의 임기제한을 폐지하였으며 하원정보위원회는 8년으로 제한하고 있다.
128) 미국 하원상임선출위원회는 국방정보 및 전쟁지원, 방첩·대테러 및 반확산, 정보현대화 및 대응, 전략기술 및 선진 연구 위원회 등 4개 소위원회를 운영하고 있다. https://intelligence.house.gov/subcommittees/star-subcommittee.htm 검색일: 2021.8.1)

에 있어 정보의 중요성과 의회의 역할을 고려해볼 때 국회(의장) 산하에 국회정보자문위원회를 설치·운영할 필요가 있다.
민간 및 군 정보 전문가, 외교안보 전문가 등 10~15여 명으로 구성하여 국가정보 우선순위 선정, 정보개혁 방안, 정보기관의 법규 준수 여부 및 비밀정보에 대한 국회의 효과적인 관리 방안 등에 대해 자문하게 될 것이다.
이 위원회는 정보위원회의 활동을 보완하고 대국민 신뢰성을 제고하는 등의 긍정적인 효과를 거둘 수 있을 것이다.[129]

3) 정보기관과 신뢰 구축 및 협력의 제도화

국회와 정보기관 간의 신뢰 형성은 정보기관에 대한 효율적인 통제나 정보기관 발전에 중요한 요인이 된다. 정보기관에 대한 통제의 효과성을 높이기 위해서는 정보기관의 자발적인 협력이 필수적이다. 이 같은 당위성에도 불구하고 한국의 국회와 정보기관 간의 불신은 지속되고 있고 그 벽은 상당히 높다. 대부분의 의원들은 정보위가 효과적으로 작동하지 못한 데는 정보기관의 불성실한 보고에 그 원인이 있다고 주장하는 반면, 정보기관은 의원들에 의한 정보 누설로 인해 민감한 정보 보고가 불가하다는 입장을 보이고 있다.
국회와 정보기관 간 신뢰 증진을 위해서는 의원들의 정보누설 방지가 중요하다. 한국을 비롯하여 대부분 국가의 의회위원들은 정도의 차이가 있지만 정보누설을 하고 있는 것이 현실이다. 그럼에도 정보누설에 따른 처벌을 받은 의원들을 찾아보기 어렵다. 사실, 정보기관의 보고의 외부유출은 정보기관과 정보위 사이의 갈등을 유발하는 가장 큰 원인으로 간주되어 왔다.
이와 같은 한계에도 불구하고 정보누설은 국가안보 차원에서도 반드시 시정되어야 하는 만큼 다음과 같은 개선 방안을 생각해볼 수 있다.
첫째, 정보위원들을 안보, 국방 및 정보기관에 경력이 있는 인사들 위주로 구성하는 방안이다. 이는 이들 위원들의 보안의식과 정보에 대한 중요성을 인식하기 있기 때문에 비밀누설을 빈번하게 하지 않을 것이라는 믿음에 기인한다. 영국의 보안정보위원회(ISC)의 사례를 보면, 합동위원회로서 ISC회원은 정보공동체와 일한 경험을 가진 다수의 상원의원들을 포함하고 있다. 이들 중에는 과거 장관, 고위공무원, 비밀정보부 요원 등이 포함되어 있다.[130]
둘째, 국회 차원에서 불법 기밀 누설 시 처벌, 국회 자체 비밀규정 마련 및

129) 필자는 2020년 초 여야 정보위원들을 대상으로 정보위원회 내 정보자문위원회를 설치할 것을 제안했으나 의견차이로 수용되지 않았다, 대신, 각 당별로 정보연구 모임으로 대체하기로 하였으나 코로나19로 인해 연기된 상태이다.
130) https://books.openedition.org/obp(검색일 : 2021.8.5.).

준수, 정보위원의 축소 및 최소화 등을 고려해볼 수 있다. 셋째, 국정원 차원에서는 비밀누설 빈도가 높은 의원에 대한 답변 거부 또는 최소화, 민감정보 출처 삭제, 정치인 대상으로 비밀누설 방지를 지속 당부하는 등의 노력이 이루어져야 한다. 이와 같은 조치에도 소속 정당이나 자신의 정치적 의도나 홍보효과가 높다고 판단되는 경우에는 언론에 누설할 가능성을 배제할 수 없다. 비밀누설 방지는 효과적인 정보통제를 위해 해결해야 할 가장 중요한 과제중 하나이다. 정보기관이 의원들의 비밀 유지 조건 하에서 보고하되 정보기관의 정보 제공의 수준과 범위, 정보위의 언론 및 제3자에 대한 정보제공 범위 등에 대해서는 사전 합의에 의거하여 추진할 필요가 있다.

필요한 경우 (가칭) “정보위-정보기관 신뢰 구축 메모랜덤” 과 같은 협약을 체결하고 효력 유지를 위해 학계 및 NGO대표들이 참여하는 방안도 고려해볼 만하다. 한편, 이스라엘의 정보기관들이 정보소위원장에게만 보고하고 위원장의 책임하에 각 위원들에게 배포하는 방안을 도입하는 것도 대안이 될 수 있다.

<표5.3> 국회의 비밀누설 방지 방안

구분	개선 방안
공통	o 신뢰 구축 : 정보위 소속 이외 경찰, 군 및 검찰출신 의원들을 통해 비밀누설의 폐단을 설명하고 중단을 설득
국회차원	o 문서 유출 방지 및 처벌 등 관련 국회(사무처 및 정보위) 차원의 세부 규정을 마련, 관행에 의존하는 행태 시정 - 국회의장 및 관련 위원회(국방, 법사, 외통위)등과 공유 o 정보보고 대상을 정보위원장 및 여야간사 3인에게 국한, 최소화(미국, 이스라엘 모델) o 의원들의 개별 질문 금지 o 현재 12명의 정보위원 숫자를 9명으로 축소 보안누설 가능성을 최소화 : 여당5, 야당4
국정원 차원	o 당대표 및 원내대표와 접촉하여 보안누설 문제의 부작용을 설득, 재발방지 지속 당부 o 세부 정보출처 삭제 o 의원들의 개별 질문에 답변 최소화 - 특히, 의원들이 언론 답변 등 정보위 업무와 무관한 질의할 경우 거부 o 외교·국방위원회위원들의 보안누설 방지책이나 관행 등을 정보위원들에게 소개, 비밀 누설 필요성을 설득
기타	o 학계 및 시민단체 등 참여 하 국회-정보위간 비밀 누설 방지 협의서 체결

4) 보안유지 전제하 비밀자료 접근 권한 강화

정보위원들은 2년의 임기 중에도 잦은 교체율을 보여 전문성이나 보안 의식이 약화되고 이로 인해 정보위원회에 제공되는 정보자료도 매우 제한적임에 따라 상호 신뢰관계가 구축되지 않고 통제가 효과적으로 이루어지지 않고 있다. 현재 정보위원회는 비공개회의 후 여야 간사 합의 하에 언론에 브리핑을 실시하고 있는데, 공식적인 브리핑 내용 이외에도 정보위원들을 통한 비밀누설 사례가 자주 발생하고 있다. 이런 경우에는 관련 법규에 따라 관련된 위원을 국회 윤리특별위원회에 회부하여 징계 및 사법처리 여부를 결정하도록 되어 있으나 지금까지 실현된 적이 없었다.

정보기관이 수집·분석한 자료에 대한 접근은 국회의 정보통제의 효과성을 높이는 중요한 요인이 된다. 국회의 비밀정보에 대한 접근 수준은 국가별로 상이하나 민주주의 국가의 경우 일반적으로 광범위하게 인정되고 있다(붙임 참조). 특히 미국의 경우 정보기관들에게 시민의 권리를 침해하였거나, 법과 행정명령, 대통령 지시 또는 기관의 규칙과 통제를 위반했다고 간주되는 모든 국가정보활동에 대하여 위원회에 보고하도록 규정하도록 하고 있다.[131] 또한, 정보 보고 시점과 관련하여 모든 정보는 '완전하게 그리고 즉각적'으로 통보되어야 한다고 규정하고 있으며, 특히 현재 진행 중인 활동뿐만 아니라 향후 진행할 활동에 대한 사전 보고 및 승인 규정까지 마련하고 있다. 반면 한국의 경우 비밀 자료에 대한 의회의 접근권이 상당부분 제한되어 있으며, 정보기관들의 자료제출과 보고에서 상당히 비협조적인 태도를 취하고 있기 때문에 의회의 통제기능에 한계가 있다. 그러나 미국 의회의 비밀정보에 접근 허용 범위를 한국에 그대로 적용하기는 어렵다. 보고된 정보가 누설되지 않을 것이라는 신뢰가 형성되어야 하기 때문이다. 따라서 정보기관이 보고한 정보의 보안이 유지된다는 전제하에서 국회의 비밀자료 접근권한을 한층 확대할 필요가 있다.

5) 초당적 합의문화 형성과 당파성 극복

여야 간 외교안보 이슈에 대해 비교적 초당적 합의 문화가 형성된 미국 등 선진국과 달리 한국의 국회의 경우에는 이념적, 당파적 요소가 매우 큰 비중을 차지한다. 특히, 북한에 대한 인식을 둘러싸고 첨예하게 대립되는 만큼, 국회 역시 타협점을 찾기 어려울 정도로 극한 대립을 보이고 있다.

131) 허태회·박진수, "미국, 영국, 한국 의회의 국가정보 감시제도 비교 연구," 『분쟁해결연구』 (2015), pp.121-147. Vol.13 No1.

미국 상원의 경우 여당이 야당보다 1석을 많게 함으로써 여당에 권한을 주면서도 극한적인 대립을 방지하는 역할을 하는데 이러한 제도를 한국도 도입해 볼 만하다. 제도적인 개혁 이외 여야 정보위원들이 정보기관의 고유의 역할과 한계에 대한 인식이 무엇보다 필요하다.
대부분의 정보위원들은 정보기관의 조직의 개혁, 정보활동의 역량 강화에 대한 문제의식보다는 남북관계에서 정보기관의 역할이나 불법활동을 중심으로 정보통제를 인식하는 경향이 강하다. 따라서 여야 위원들이 이념적, 당파적 이해관계를 초월하여 정보기관이 수행해야 할 본연의 업무인 수집, 공작 방첩 활동에 대한 이해에 대한 합의만 도출하더라도 정보위의 당파성을 약화시키는 데 도움이 될 것이다.

6) 청와대를 포함한 감독 대상 기관 확대

현재 국회정보위원회는 1994년도 설립된 이래 민간정보 기관인 국정원 단일기관에 대한 감독에 주안을 두고 업무를 수행하고 있다. 그러나 다음과 같은 이유에서 정보위의 정보감독 범위를 확대할 필요성이 있다. 첫째, 청와대(대통령, 국가안보실 등)는 최고 정보소비자일 뿐 아니라 정보실패 상당수가 대통령을 비롯한 청와대의 지시와 요구에 의해 발생하고 있다. 둘째, 미국·영국 등 선진국 국회정보위원회는 단일 부처가 아닌 민간정보기관, 군, 행정부처 산하 정보기관 전체를 감독하거나 직간접적으로 업무에 관여하고 있다.[132] 셋째, 국정원은 세계를 상대로 정보활동을 수행하는 미국이나 영국의 정보공동체와 비교해볼 때 예산, 조직 및 활동 범위가 협소하다. 1개 정보기관을 통제하기 위해 12명의 의원들을 필요로 하는지 생각해볼 여지가 있다. 넷째, 국정원의 업무 중 많은 비중을 차지했던 국내 수집·분석활동의 상당부분이 폐지됨에 따라 정치개입이나 불법 활동 가능성이 크게 감소한 만큼, 국회의 감독 방식도 달라져야 할 필요가 있다. 다섯째, 포괄안보시대 과학기술의 발달로 정보업무가 행정, 군 업무 영역과 중복이 심화되고 있다는 점을 고려할 필요가 있다. 사이버 테러가 대표적인 사례인데, 이는 도발 주체가 불분명하고 추적도 어려운데다 공공기관과 민간인들도 피해가 발생하고 있기 때문에 효과적인 대응을 위해서는 정보기관은 물론 민간전문가들을 포함한 국가적 차원의 대응이 불가피하다
그리고 첩보수집자산 대부분을 보유하고 있는 군 정보기관과 민간 정보기관의 협력 문제뿐 아니라 수집 첩보의 배포범위도 통일부, 외교부 등 안보부처를 대상으

132) 독립적인 정보위원회가 구성되지 않은 이스라엘도 국회외교위원회 산하 정보소위원회에서 국내외 정보기관을 감독하고 있다.

로 확대함으로써 위협인식을 공동평가하고 공유할 수 있어야 한다. 이를 위해 청와대를 포함하여 군 정보 및 수사기관(정보사, 합참정보본부, 기무사), 외교부와 통일부 정보 분석, 경찰청(보안 및 대테러 등) 및 해양경찰청의 정보업무에도 직간접적으로 관여할 수 있어야 국가 차원의 정보역량이 강화될 수 있을 것이다.

<표5.4> 국회정보위원회 권한 강화 방안

구분	개선 전	개선안
정보접근		'위원 2/3이상 요구시 자료 접근 강화' 권한을 효과적으로 활용
정보위원 임기	2년	4년
정보위원회 감사 대상	국정원 위주	국정원, 합참 정보본부, 경찰청, 해경청 등 정보업무를 다루는 기관(7개)으로 확대
정보위(2년) 이후 배려	별무	당차원에서 향후 원하는 위원회 또는 당직 배려를 제도화
정보위원회 사무처	전문위원 1명(국회사무처 출신)	정보학 전공 전문위원 1명 공채
국회 국가정보 자문위원회		o 외부 전문가 7-8명으로 구성

7) 정보기관장 임명 기준을 제시

한국의 국회는 미국 의회와는 다르게 정보기관장 후보자에 대한 인준 권한이 없다. 그러나 국회는 정보기관장 후보자의 능력, 자질, 도덕성, 국가관 등을 검증하고 부자격자로 판단될 경우 지명 철회를 강력하게 요구해야 한다. 이를 위해서는 국회법 개정을 통해 인준 권한이나 거부권을 규정하는 방안이 있다. 또한, 사전에 국회 자체 기준을 마련하여 대통령에게 제시하는 방안도 고려해볼 수 있다. 정보기관장이 임명된 후에는 정보기관 특성상 감독이 어렵고 재량권을 남용할 경우에는 폐해가 실로 크기 때문이다. 정보의 경험이 전혀 없거나 정보업무와도 무관한 인사가 정보기관장으로 임명되어 정보기관이 권력의 시녀 역할을 하거나 국가안보에도 심각한 피해를 끼친 사례가 많이 있었다. 따라서 국회에서는 정보기관장이 정보기관을 사유하거나 권한 남용 방지하기 위한 구체적인 방안을 마련, 시행해야 할 필요성이 있다.

8) 감사원과 차별된 감사로 위상 제고

국정원에 대한 감사원 감사가 강화되면서 국회 감사의 상당 부분, 특히 회계 부분 감사는 행정기관에 의해 대체될 우려가 있다. 감사원의 감사는 국회의 정보통제 기능의 약화로 이어질 수 있고 감사원이 대통령이 직속 기관인 점을 감안해볼 때 국회의 행정부 견제라는 삼권분립의 의미가 퇴색될 수 있다. 감사원의 감사는 회계 감사 등 기술적 분야로 한정하고 비밀 준수가 요구되는 공작, 방첩, 분석 활동에 대한 감사는 국회에서 전담 방안이 바람직하다. 나아가 국회는 정보기관의 활동 역량이 강화될 수 있도록 대안을 제시하는 방향으로 업무 영역을 확장해나가야 할 것이다.

Ⅴ. 결론

불확실성과 복잡성이 증대되고 있는 상황에서 다양한 안보 위협을 조기에 포착하고 대응하기 위해서는 정보기관만으로는 대처할 수 없다. 이러한 이유로 분리형 선진국 정보기관들은 국가 차원의 정보를 생산하기 위한 정보협의체를 운영하고 있다. 협의체는 대부분 최고 정보소비자인 수상이나 대통령 직속 하에 설치되거나 경우에 따라 독립적으로 운영되고 있다. 이들 협의체는 정보목표 우선순위 설정, 정보예산 심의, 정보기관 업무 영역 조정, 국가 차원의 정보보고서 생산, 정보 왜곡 방지 등 다양한 기능을 수행하고 있다.

그러나 우리의 경우는 민간 및 군 정보활동을 사전에 조정하는 협의체가 부재한 관계로 복합위협을 평가하고 대응책을 제시할 수 있는 수단이 매우 제한되어 있다. 통합 기재가 없다 보니 대통령에 대한 보고를 둘러싸고 부처 간 치열한 경쟁을 벌이고 있다. 보고된 정보와 실제와의 부합여부나 정보왜곡 또는 남용에 대한 검증 없이 보고되는 경우가 다반사이다. 이와 같은 현실을 고려해볼 때 한국형 정보공동체 설립의 필요성은 충분히 설득력을 갖는다. 이를 위해 청와대 내 일정 부분 독립성을 갖춘 장관차급 정보협의체를 신설하고 이행력을 강화하기 위해 국가정보조정관을 신설하는 방안을 제시하였다.

국회의원들 스스로가 언급한 바와 같이 정보기관의 부실한 보고와 국회의 취약한 통제 권한이 문제점으로 드러났다. 민의의 대표기관인 국회 차원에서 정보기관을 통제하고 정보역량 강화를 위한 방안을 모색해야 한다. 구체적인 내용으로는 국회(의장) 산하 국회정보자문위원회 신설, 국회와 정보기관 간의 신뢰 제고, 청와대를 비롯한 정보통제 대상 부처의 확대, 보안 유지 하에 정보 접근 권한 확대, 정보위원 및 보좌관의 전문성 향상, 감사원과는 차별성 있는 감사의 실시 등이 포함될 수 있는 것이다.

이 같은 제안들이 이행되고 성과를 도출하기 위해서는 양 기관 간의 신뢰 구축이 무엇보다 중요하다. 정보기관이 국가안보에 중요한 필수불가결한 존재라는 사실과 정보기관이 국회에 보고한 비밀정보가 누설되지 않는다는 확신에 대한 공감대가 형성되어야 한다.

국회와 정보기관의 신뢰가 제고되기 위해서는 합법적인 정보활동, 효율적인 의회 감독 그리고 의원들의 비밀정보에 대한 준수가 이루어져야 한다. 제공된 정보를 누설하는 관행이 지속되는 한 양 기관 간의 신뢰 구축은 어렵게 된다. “의회와 정보기관의 정보공유는 양 기관이 보안에 대해서도 공동으로 책임진다는 사실을 의미한다”는 독일의원들의 정보보안에 대한 태

도가 우리에게도 시사하는 바가 크다. 정보기관의 불법·일탈 행위를 감시는 국회의 중요한 기능 중 하나이다. 그러나 국회가 정보기관을 단순히 통제하고 규제하기보다는 정보기관이 국가안보 본연의 목적을 충실히 이행할 수 있도록 방향을 제시하고 필요한 경우 정보역량을 강화할 수 있는 법적·제도적 기반을 제공해줄 필요가 있다.
이와 함께 정보기관의 국회에 대한 태도 또한 변화가 요구된다. 정보기관은 국민의 대표기관인 국회에 객관적인 정보를 제공하는 것이야말로 국민에 대한 의무라는 점을 인식할 필요가 있다.
정보기관에 대한 통제 역시 최고소비자인 대통령이나 정보기관의 입장에서는 불편하고 다소 고통스러운 일일지 모르나 궁극적으로는 합법성과 효과성을 제고함으로써 정보기관이 역량 강화와 신뢰성 확보에 도움이 될 것이다.

비밀 정보기관에 대한 통제는 행정부처와 달리 어려운 측면이 많이 있다. 국가정보기관의 정보활동에 대한 의회 통제는 민주주의 사회에서는 필수불가결한 요소이며 정보활동의 정당성과 효율성 강화 차원에서도 반드시 시행되어져야 할 중요한 제도이다. 민주화가 진전되고 있는 상황에서 정보기관의 권한 남용을 방지하기 위한 의회 통제의 중요성은 점점 확대되고 있다.

1970년대 정보학자 라쿠어(W.Quer)는 “이스라엘 정보기관은 정보실패로 인해 비난은 받을지언정 정치개입으로 인해 비난받은 적은 없다”고 언급한 바 있다. 우리의 정보기관들도 오직 국가안보와 국민의 안전을 보장하는 일에만 전념함으로써 국민의 신뢰를 받는 기관으로 거듭나야 한다. 이를 위해 그 어떤 기관보다 국회의 책임이 막중하다는 사실을 인식하고 여야 간 초당적 협의를 통해 실효성 있는 방안들을 수립·시행해 나가야 할 것이다.

<붙임 > 주요국 정보통제 사례 비교[133)]

1. 미국 정보통제 기관(7개)

감사기관	감사독립	자체 조사기능	결과보고	정보접근 제한	감사중단	법적근거	시정조치
Inspector General FBI	부분적	Yes	법무장관	법무장관	대통령	IG Act 1978	권고
Inspector General CIA	부분적	Yes	CIA국장	CIA국장	대통령	CIA Act 1978	권고
Inspector General NSA	부분적	Yes	NSA국장	국방장관/ DNI	대통령	IG Act 1978	권고
Inspector General NGA	부분적	Yes	NGA국장	국방장관/ DNI	NGA국장	IG Act 1978	권고
Inspector General for the Intelligence Community	Yes	Yes	DNI	DNI	대통령	National Security Act 1947	권고
Senate Select Committee on Intelligence	Yes	Yes	상원	대통령	No	상원결의 400	권고
House Committee	Yes	Yes	의회/상원	대통령	No	하원결의 658	권고

2. 영국 정보통제 기관(4개)

감사기관	감사독립	자체 조사기능	결과보고	정보접근 제한	감사중단	법적근거	시정조치
Investigatory Powers Tribunal	Yes	No	Prime Minister	No	왕실 추천의원	Regulation of Investigatory Power Act 2000	강제
Intelligence and Security Committee	Yes	Yes	Prime Minister/의회	the Head of the relevant agency-sensitive	해당사항 없음	Justice and Security Act 2013	해당사항 없음
Intelligence Services Commissioner	Yes	No	Prime Minister	No	해당사항 없음	Regulation of Investigatory Power Act 2000	해당사항 없음
Interception of Communications Commissioner	Yes	No	Prime Minister	No	해당사항 없음	Regulation of Investigatory Power Act 2000	해당사항 없음

133) Sophie Richardson & Nicholas Gilmour (2016). pp. 14-19.

3. 캐나다 정보통제 기관(2개)

감사기관	감사독립	자체 조사기능	결과보고	정보접근 제한	감사중단	법적근거	시정 조치
Communications Security Establishment Commissioner	Yes	Yes	Responsible Ministerr	nil access to Cabinet confidences	for breach of good behavior	National Defence Act 1985	권고
Security Intelligence Review Committee	Yes	부분적	Responsible Minister	nil access to Cabinet confidences	for breach of good behavior	Canadian Security Intelligence Services Act 1985	권고

4. 호주 정보통제 기관(2개)

감사기관	감사독립	자체 조사기능	결과보고	정보접근 제한	감사중단	법적근거	시정조치
Inspector-General in Intelligence and Security	Yes	Yes	Responsible Minister	matters outside Australia or matters that occurred prior to the commencement of the Act	Governor-General	Inspector General of Intelligence and Security Act 1986	권고
Parliamentary Joint Committee on Intelligence and Security	Yes	No	Prime Minister/의회	Responsible Minister-sensitive information / information that may prejudice national security	No	Intelligence Services Act 2001	해당사항 없음

5. 뉴질랜드 정보통제 기관(2개)

감사기관	감사독립	자체 조사기능	결과보고	정보접근 제한	감사중단	법적근거	시정조치
Inspector-General in Intelligence and Security	Yes	Yes	Responsible Minister	Responsible Minister-information prejudicial to security, safety or defence	Governor-General	Inspector General of Intelligence and Security Act 1996	권고
Intelligence and Security Committee	Yes	No	Prime Minister/의회	Head of the relevant agency-sensitive information	No	Intelligence and Security Committee Act 1996	해당사항 없음

6. 노르웨이 정보통제 기관(1개)

감사기관	감사독립	자체 조사기능	결과보고	정보접근 제한	감사 중단	법적근거	시정조치
EOS Parliamentary Committee	Yes	Yes	Storting (Parliament)	Protests from the Head of the relevant agency	-	Oversight of Intelligence, Surveillance and Security Services Act 1995	권고

7. 독일 정보통제 기관(2개)

감사기관	감사독립	자체 조사기능	결과보고	정보접근 제한	감사중단	법적근거	시정조치
Parliamentary Control Panel	Yes	No	Bundestag (의회)	Head of the relevant agency	No	Federal Intelligence Activity Act 2009	해당사항 없음
G10 Commission	부분적	No	해당사항 없음	No	-	Act Restricting the Privacy of Correspondence, Post and Telecommunications(Article 10 Act)	강제

8. 네덜란드 정보통제 기관(3개)

감사기관	감사독립	자체 조사기능	결과보고	정보접근 제한	감사중단	법적근거	시정조치
Intelligence and Security Review Committee (CTIVD)	Yes	Yes	Responsible Ministers/ Public	No	Royal Decree	Intelligence and Security Services Act 2000	권고
Committee on the Intelligence and Security Services	Yes	No	의회	-	No	해당사항 없음	-
Committee on the Interior	Yes	No	해당사항 없음	해당사항 없음	No	해당사항 없음	-

9. 남아프리카 정보통제 기관(2개)

감사기관	감사독립	자체 조사기능	결과보고	정보접근 제한	감사중단	법적근거	시정조치
Inspector General of Intelligence	Yes	Yes	Responsible Ministers	No	대통령	Intelligence Services Oversight Act 1994	권고
Joint Standing Committee on Intelligence	Yes	부분적	의회	Head of the SSA-sensitive information	No	Intelligence Services Oversight Act 1994	권고