외국정보기관의 인간정보(HUMINT) 활동에 대응한 산업기술 보호방안

A Research on the Industry Technology Protection Way against Foreign Secret Service's HUMINT Activity

주 일 엽*

<목 차>

<요 약>

본 연구에서는 사례연구를 통해 외국정보기관의 인간정보(HUMINT) 활동에 대응한 산업기술 보호방안을 도출하는데 그 목적이 있다.

이와 같은 목적을 달성하기 위하여 외국정보기관의 인간정보(HUMINT) 특징 및 활동사례를 구체적으로 분석하여 외국정보기관의 정보활동에 대한 국제적인 실태를 유추하고 나아가 우리나라의 산업기술 보호방안을 제시하였다. 본 연구에 사용된 사례는 ① 외국정보기관의 대미(對美) 인간정보(HUMINT) 활동, ② 외국정보기관의 대일(對日) 인간정보(HUMINT) 활동 등으로 2차 자료인 국내 및 해외 언론자료를 활용하였다.

이와 같은 연구목적과 방법을 통하여 도출한 우리나라의 산업기술 보호방안은 다음과 같다.

첫째, 외국정보기관의 인간정보(HUMINT) 활동에 대응한 인원보안의 중요성 인식이 필요하다.

둘째, 외국정보기관의 인간정보(HUMINT) 활동에 대응한 인원보안 관리수단을 확보해야 한다.

셋째, 외국정보기관의 인간정보(HUMINT) 활동에 대응한 국가 차원의 방첩능력을 제고해야 한다.

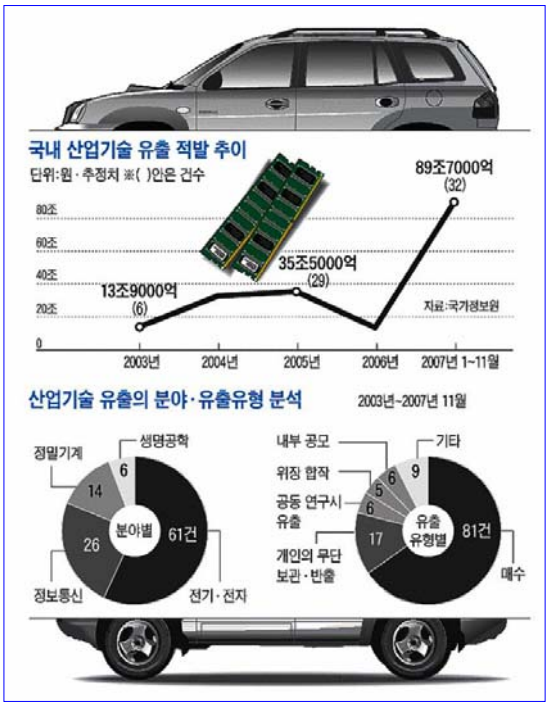
주제어 : 정보기관, 정보활동, 인간정보(HUMINT), 산업기술, 보호방안

* 대통령실 경호처 경호서기관

I. 서 론

최근 세계 각국은 자국의 생존권 확보 전략 차원에서 첨단기술 개발에 주력하고 있으며 다른 나라의 첨단기술을 입수하기 위해 수단과 방법을 가리지 않는 치열한 경제전쟁을 전개하고 있다. 우리의 첨단기술을 보호하는 문제는 국가안보의 중요한 요소로 등장하고 있는데 냉전 종식에도 불구하고 외국의 정보수집 활동은 오히려 증가하고 있다. 각국은 한국의 정치, 경제, 산업, 군사 등 전 분야를 수집대상으로 하고 있으며 기술정보뿐만 아니라 경쟁업체의 조직·운영상의 정보, 혹은 개인 신상정보도 수집대상이 되고 있다(국가정보원, 2004: 1-3).

산업기술 해외유출의 경우, 우리나라는 지난 2007년 11월 기준 산업기술 해외유출 적발사례가 32건, 예상피해액이 89조 7천억 원에 달하는 등 그 정도가 심화되고 있는데 <그림 1-1>은 2003년부터 2007년 11월까지 연도별 산업기술 해외유출 적발 현황을 나타낸 것이다.



자료 : 조선일보(2007.12.15字)

<그림 1-1> 산업기술 해외유출 적발 추이 및 분야·유형 분석

이러한 지적에도 불구하고 정보 획득의 핵심기법인 인간정보(HUMINT) 활동에 대해서는 관련연구가 거의 진행되지 못하고 있는 실정이다. 이는 정보활동의 속성상 비공개, 은밀성이 요구되고 해당국가 정보·보안기관이 국가 차원에서 대응하는 관계로 이에 대한 학문적 접근이 매우 어려운데 기인한다. 그러나 국가 간 국제경쟁이 심화되면서 인간정보(HUMINT) 활동에 대한 연구는 국가안보의 관점에서 매우 중요한 사안으로 부각되고 있다.

노호래(2008: 47)는 지금까지 정보보호에 관한 선행연구가 '산업스파이에 대한 형사사법적 대응방안에 관한 연구'(한상훈, 2001), '기업정보 유출 방지를 위한 기술'(김종원・최종욱, 2003), '국내기술 유출 및 보호 현황과 과제'(조윤애, 2004), '한국의 신종 기업범죄의 유형과 대책'(김광준, 2003), '산업기술 유출규제에 관한 법적 고찰'(조용순・홍영서, 2006), '경제범죄의 실태에 관한 연구'(옥필훈, 2006), '산업스파이 현황과 대응방안'(정덕영・정병수, 2007), '직무발명 관련 과학기술연구자의 권리보호'(정연덕, 2007), '중소기업 핵심기술 유출 실태에 관한 연구'(김문선 등, 2007) 등이 진행되었음에도 불구하고 구체적인 대안마련이 부족했다고 지적하면서 기업적 차원과 국가기관 차원의 대안을 제시하고 있어 주목된다.

그러나 이와 같은 학계의 관심에도 불구하고 외국정보기관의 인간정보(HUMINT) 활동에 대한 연구는 여전히 부진한 실정이다. 따라서 본 연구는 중국의 해외정보활동 중 미국, 일본 등 주요국가에서의 인간정보(HUMINT) 활동사례를 분석하여 대응방안을 제시하고자 한다. 이를 통해 우리나라를 대상으로 하는 외국정보기관의 인간정보(HUMINT) 활동을 통한 산업기술 획득 시도를 예방하는데 기여하고자 한다.

Ⅱ. 연구방법

정보활동의 사례는 하나의 실험된 사실적 자료이며 분석에 유익한 자료가 된다. 사례연구는 각 국가가 수행하고 있는 다양한 정보활동의 특성, 능력 및 수준을 알게 해 준다. 정보활동의 성공사례, 실패사례 등에 대한 원인과 결과에 대한 분석은 향후 정보활동에 유용한 행동지침을 알려 준다. 사례연구는 정보활동의 연구에 필수적인 분석방법이 되고 있다(김윤덕, 2001: 11). 본 연구에서는 각국의 정보기관들이 주체가 되어 수행해 온 정보활동을 이해하는데 유용한 분석방법인 사례연구를 통해 외국정보기관의 인간정보(HUMINT) 활동에 대한 연구를 진행하고자 한다. 본 연구에서 제시한 인간정보(HUMINT) 활동사례는 중국 정보기관 관련사례로서 이를 구체적으로 분석함으로써 여타 외국정보기관의 정보활동 실태를 유추하고 나아가 우리나라의 산업기술 보호방안을 제시하고자 한다.

앞서 서론에서 언급한 것과 같이 국가차원의 정보활동이 국가의 중요한 대내적・대외적

활동임에도 해당 분야에 대한 학문적 연구가 활발히 진행되지 못하였다. 이는 국가가 수행하고 있는 정보활동의 속성에 따라 많은 어려움이 있었기 때문이었다. 이 분야에 대한 연구를 어렵게 만들었던 요인들은 ① 공개자료의 부족, ② 연구대상에 대한 학문적 접근의 제약, ③ 일반적인 체계수립의 어려움 등이 있다(김윤덕, 2001: 11-13). 따라서 본 연구는 국내 및 해외 언론자료 등 2차 자료를 중심으로 외국정보기관의 인간정보(HUMINT) 활동에 대한 사례연구를 진행하였다.

Ⅲ. 이론적 배경

1. 정보이론

정보에 대한 개념적 정의는 일반적이지 않다. 정보는 용어가 쓰이는 상황에 따라 각기 다른 의미로 해석될 수 있기 때문이다(최윤호, 2000: 3-5). 제 1단계는 DATA로 단순한 사실이나 기호를 의미한다. 제 2단계는 좁은 의미로서의 정보인 INFORMATION이며 목적성을 가지고 수집한 데이터이며 아직 분석·평가 과정을 거치지 않은 것이므로 불확실성을 내포하고 있다. 제 3단계는 INTELLIGENCE라고 부르는데 특정 목적에 유용하게 쓰이도록 처리된 정보를 의미하며 특정한 상황 아래서 행동을 선택하는 판단기준이 되므로 유용성이 높다. <표 3-1>은 정보의 구분을 나타낸 것이다.

정보는 공개정보(Open Source Information), 공개소유정보(Open Proprietary Information), 비공개 비밀정보(Classified Information) 등으로 구분된다. 공개정보는 합법적이고 윤리적으로 낮은 비용으로도 획득할 수 있는 정보이다. 공개소유정보는 합법적이고 윤리적으로 얻을 수 있으나, 가치 있는 정보를 얻기 위해서는 어느 정도 비용이 요구되는 정보를 말한다. 비공개 비밀정보는 어떤 특정 조직의 안전구역 내에서만 이용이 가능한 정보로서 이러한 정보의 획득에는 스파이활동이 요구되며 높은 비용이 요구된다.

<표 3-1> 정보의 구분

구 분	DATA	INFORMATION	INTELLIGENCE
용 어	데이터	1차 정보, 첩보, 생정보	2차 정보, 분석정보, 가공정보
활 동	입력	수집	분석, 평가, 가공
활동특성	임의적	의식적	의식적
특 성	무의미	불확실성	확실성
유용성	소(小)	중(中)	대(大)

자료 : 최윤호, 2000

2. 정보기관

각국의 정보기관들은 정보활동의 특성에 따라 기능별로 분화되어 있다. 가장 두드러진 특징은 정보 수집활동을 위한 정보기관과 외국정보기관의 비밀정보활동을 차단하기 위한 방첩기관으로 나누어진다. 정보수집이 가장 광범위하게 이루어지기 때문에 정보 수집활동을 위한 정보기관들이 분화되어 있으나 국가의 규모나 역량에 따라 분화 정도가 다르다. 그러나 방첩기관들은 대부분 하나의 통합된 정보기관으로 운영되고 있다. 정보수집을 위한 정보기관들은 주로 인간정보(HUMINT), 신호정보(SIGMINT), 영상정보(IMINT) 등 수집수단에 따라 분화되어 있다. <표 3-2>는 주요국가 정보기관들의 기능별 분류를 나타낸 것이다.

<표 3-2> 주요국가 정보기관의 기능별 분류

국 가	인간정보	신호정보	영상정보	방첩활동
미 국	중앙정보국 (CIA)	국가안전국 (NSA)	국가정찰국 (NRO)	연방수사국 (FBI)
영 국	비밀정보부 (SIS)	정보통신본부 (GCHQ)		보안부 (SS)
러시아	해외정보부 (SVR)	연방통신정보국 (FAPSI)		연방보안부 (FSB)
프랑스	대외안보총국 (DGSE)			국토감시청 (DST)
독 일	연방정보부 (BND)			연방헌법보호청 (BFV)
중 국	국가안전부	기술부 (통신정보부)		국가안전부
이스라엘	모사드 (MOSSAD)			신베드 (SHINBETH)
일 본	내각조사실			

자료 : 김윤덕, 2001

3. 정보활동

국가기관의 정보활동은 크게 수색공작, 통신정보(COMINT), 위장획득공작, 인간정보(HUMINT) 등으로 구분할 수 있다(김윤덕, 2001: 237-240; 강기욱, 1997: 116).

첫째, 수색공작은 목표가 되는 외국인에게 비밀리에 접근하여 수집내용과 관련하여 남긴

흔적을 수색하여 필요한 정보를 수집하는 것이다. 수색공작은 공작원이 신분을 위장하여 접근하기도 하며, 대상인물이 없는 빈 시간을 이용하여 장소에 접근한다. 공작원의 수색활동이 노출될 경우 역효과가 매우 크기 때문에 철저한 계획을 통해서 수색공작이 이루어진다.

둘째, 통신정보(COMINT)는 대화를 감청하여 필요한 정보내용을 수집하는 활동으로 가장 흔하게 이루어지고 있는 정보활동이다. 외국인에 대한 감청활동은 공산권국가뿐만 아니라 서방국가들도 활발하게 행하고 있다. 고감도의 감청장비들이 확산되고 가격도 저렴하여 국가차원 외에도 기업 및 개인차원에서도 확산되고 있다.

셋째, 위장획득공작은 위장회사를 설립하거나 혹은 제 3자의 지원을 받아 정보를 획득하는 것으로 미국 중앙정보국(CIA)에 의하면 획득공작에 활용되고 있는 회사는 300여개사가 있었으며, 네덜란드, 오스트리아, 스위스, 캐나다, 핀란드 등에 아날로그 디지털 테크놀러지사, 콘티넨탈 테크놀러지사, 콘티넨탈 인더스트리사 등의 이름으로 설립되어 있었다.

넷째, 인간정보(HUMINT)를 통한 정보활동은 일반적으로 스파이활동이라고 불리며, 비밀수집을 목적으로 이루어진다. 인간정보(HUMINT)의 수집단계는 ① 출처의 개척, ② 수집활동, ③ 첩보전달의 단계를 통해서 이루어진다.

‘출처의 개척’은 정보관이 필요한 정보에 접근성을 가지고 있는 대상국의 사람들을 파악하여 정보를 제공받을 수 있도록 하는 일련의 과정을 통해서 이루어진다. 정보관은 그들에게 접근하여 자신의 협조자를 만들기 위해 대상자를 여러 각도에서 분석한다. 우선적으로 정보의 접근가능성을 확인하고 점차적으로 정치적 신념, 경제적 형편, 성격, 개인적 도락생활, 친구 및 여자관계 등 접근가능성이 있는 부분을 파악해서 친밀감을 형성해 간다. 정보관은 대상자가 친밀감이 형성되고 협조자로서의 가능성이 있다고 판단되었을 때, 정보제공에 대한 협조를 제안한다. 협조자는 돈, 불만, 스릴, 우정, 여자 등 여러 가지 이유로 제안을 받아들일 수 있다.

‘수집활동’은 협조자나 공작원에게 임무를 부여하고 필요한 정보를 수집토록 하여 획득된 정보를 비밀리에 전달받음으로써 이루어진다.

‘첩보의 전달’은 정보관이 수집된 정보를 본국에 비밀적인 방법을 통해 보내는 것을 의미한다. 외교관으로 가장한 정보관은 정보를 암호화하여 외교통신망을 통해서 본국에 보내게 되며, 비공식 가장정보관은 인편, 우편, 전화, 팩스 등 여러 전달수단을 동원하여 정보를 본국에 전달한다. 본국의 정보기관은 수집된 정보를 평가하고, 정보관에게 후속적인 지시를 내린다. 출처의 개척, 수집활동, 첩보의 전달은 모두 비밀활동에 의해 이루어진다.

Ⅳ. 사례분석

본 연구에서 분석한 외국정보기관의 인간정보(HUMINT) 활동 사례는 중국 정보기관의 인간정보(HUMINT) 활동 사례로서 ① 중국의 정보기관, ② 중국 정보기관의 대미(對美) 인간정보(HUMINT) 활동, ③ 중국 정보기관의 대일(對日) 인간정보(HUMINT) 활동 등을 통해 외국정보기관의 인간정보(HUMINT) 활동의 특징을 살펴보고 그 문제점 및 대응방안을 도출하고자 한다.

1. 중국의 정보기관

중국의 정보공동체의 주요기관들은 국무원 국가안전부, 중국 공산당 비서국 국제연락부, 인민해방군 총참모부 군사정보부, 인민해방군 총참모부 기술부, 그리고 신화사와 정보 기능을 가지고 있거나 가질 수 있는 다수의 연구기관을 포함하여 수개의 기관들이 있다(강기택, 2003: 182-185; 박영일, 1994: 521-522, 527-528, 535; 세계일보, 2007.5.22字; 야후 백과사전, 2008).

첫째, 국가안전부(MSS)는 대외에 공표된 유일한 정보기관이다. 해외첩보와 국내정보 수집, 보안, 방첩, 수사 기능도 지니고 있다. 국가안전부는 1983년 6월 구소련 국가보안위원회(KGB), 미국 중앙정보국(CIA)을 모델로 국가안전부가 창설되어 공안부의 방첩 및 보안기능을 인수하였으며 당(黨)과 정부, 군(軍)의 공안부분의 총책으로서 간첩활동과 중국 정부 내에서부터 외국언론에 기밀이 누설되는 것을 막고 특수공작원의 활동을 저지한다.

둘째, 국제연락부(ILD)는 중국 외교정책의 한 수단이며 비밀활동 기능과 공개적인 활동 기능을 가지고 있는데 과거에는 권력에서 물러난 사람들을 포함하여 다른 나라의 공산당과 혁명 단체에 자금을 지원하고 훈련시키는 비밀 활동을 시행하는 책임을 맡고 있었다. 그러나 최근 공개적인 공작활동을 강화하고 있으며 공산주의자 및 혁명 단체들과의 관계발전은 물론 제 3세계의 다양한 정치집단 뿐만 아니라 사회주의자, 사회주의단체 및 노동단체들과의 관계발전과 이들과 관련된 국내의 대중조직을 지원하는 기능과 해외정보 수집도 수행하고 있다.

셋째, 통일전선사업부(UFWD)는 국제연락부와 마찬가지로 정보수집 기능을 가지고 있지 않은 비밀활동 기관이다. 통일전선사업부는 여러 나라에서 막강한 압력단체로 활동하는 해외에 거주하는 중국인과 관련된 비밀활동에만 책임을 지고 있다.

넷째, 군사정보부(MID)는 전투서열(OB) 정보, 외국 무기 체계에 대한 연구 및 외국군의

능력에 대한 분석을 책임지고 있다. 군사정보부의 대부분의 업무는 정치와 군사 또는 군사 전략문제 보다는 상기 분야에 있다.

다섯째, 기술부(技術部)는 신호정보기관으로서 신호정보 네트워크를 관리하는 책임을 맡고 있다. 신호정보소가 있는 곳으로 추정되는 위치는 주로 국경지역이며 미국의 협조아래 중앙정보부(CIA)의 신호정보 운영실에 의해서 건립·훈련되었고 주기적으로 협조와 조언을 받고 있다. 기술부는 해군과 함께 수상함 및 잠수함에서 수행하는 신호정보 활동을 관장하는데 중국의 우주활동을 지원하고 러시아의 우주 활동과 미사일 작전도 감시하고 있다.

여섯째, 공안부(公安部)는 국무원 소속으로 인민해방군과 함께 중국 공산정권을 지탱하는 조직원 30만 명을 넘는 2개 무장조직으로서 비정치적 경찰행정기관이라고 할 수 있다. 국가안전부가 창설되면서 방첩 및 보안 사찰 기능을 넘겼으나 조직 내의 치안관리국, 변방관리국, 형사정찰국, 출입국관리국, 외사국, 정치부 등이 건재하여 첩보기능도 수행하고 있다.

일곱째, 신화사(新華社, NCNA)는 정부의 선전기관 역할을 하며, 국내 전역의 신문사에 대해 국내 및 해외뉴스를 내보내고 있다. 정확한 사실보도로 정평이 나 있으며, 정보지 '참고소식'은 외국의 언론에 실렸던 중국 관계 기사를 정리한 것으로, 약 700~800만 부가 발행된다. 신화사의 활동은 해외 특파원과 주재국 외교관 사이의 통상적인 정보교환을 넘어서는 수준이다. 특히 국가안전부 등 중국 정보기관의 요원이 해외에 파견될 때에는 흔히 신화사 특파원 신분으로 위장하는 것으로 알려져 있다.

여덟째, 각종 연구소에서도 정보분석 업무를 맡고 있다. 중국 공산당 서기국 예하의 당(黨) 연구실이 있고 그 안에 외무를 담당하는 그룹이 있다. 외무부 안에는 2개의 기관이 있는데 외교정책연구실과 국제연구소가 그것이다. 1978년 설립된 북경의 국제정치대학은 원래 공안부의 통제 하에 있었으나 국가안전부에 인계되었고 1979년 국방부에 의해서 전략문제와 국가 안보에 대한 연구를 수행하는 북경국제전략연구소가 창설되었다. 1979년 설립된 현대국제관계연구소가 가장 규모가 크고 현재 국가위원회에 부속되어 국제연구에 책임을 지고 있으며 국가안전부와도 밀접하게 결합되어 기밀연구를 수행하고 있다.

2. 중국 정보기관의 대미(對美) 인간정보(HUMINT) 활동

중국 정보기관의 대미(對美) 인간정보(HUMINT) 활동을 ① 자국인 및 현지인 활용 정보활동, ② 미인계 이용 정보활동, ③ 기업인 이용 첩보활동, ④ 로비 활동, ⑤ 언론신분 위장, ⑥ 중국 인민해방군의 첩보활동 등으로 구분하여 국내 및 해외 언론보도를 중심으로 분석하였다(ジョシュア・アイゼンマン, 2006; 문화일보, 2008.2.12字; 조선일보, 2005.12.28字).

첫째, 자국민 및 현지인을 활용한 정보활동이다. 중국의 대미(對美) 인간정보(HUMINT) 활동의 최대 특징은 중국인뿐만 아니라 비중국인도 적극 활용하고 있다는 점인데, 비중국인이란 주로 중국계 미국인을 의미하며 중국 본토 출신자와 중국 본토 이외의 출신자들을 포괄한다. 따라서 경계해야할 대상이 매우 광범위하며, 이는 중국의 대미(對美) 첩보 능력이 냉전 당시 소련에 버금가는 강력한 힘을 가지고 있음을 의미한다.

최근 들어 대만・말레이시아 등의 화교 출신 미국인들을 이용한 첩보 활동이 계속 증가하고 있는데, 대개 엔지니어들이 간접적인 정보수집 활동을 수행하는 것이 특징이다. 영어가 유창하고 미국 문화에 익숙한 화교계 미국인들은 겉으로는 공산주의 중국과 거리를 두고 있는 것처럼 보이므로 중국 정보 당국이 스파이로 활용하기에 적절하다. 2004년 보잉사에서 근무하던 대만계 미국인이 항공기에 사용되는 특수 트랜스미션에 관한 정보를 중국에 유출시키려다 미수에 그친 사건이 있었는데, 이는 중국의 미국 내 첩보활동이 중국 본토 출신자에 국한하지 않는다는 점을 입증한 사례이다.

지난 2008.2 미국 국방부 직원이 공범인 중국계 2명과 함께 중국 정부에 핵심군사 기밀을 유출한 혐의로 연방수사국(FBI)에 체포된 사건과 관련하여 미국 법무부는 “외국 첩보기관들이 우리의 안보시스템을 뚫고 들어와 최고급 군사기술・정보시스템을 훔치려는 무차별적인 위협”이라고 평가한데 이어 CNN 등 미국 언론들도 중국 정부의 첩보 작전이 냉전시대 구소련의 행위를 방불케 할 만큼 적극적이며 공세적이라고 전하고 있다.

둘째, 미인계를 이용한 정보활동이다. 여성을 이용하여 필요한 정보를 훔쳐 내는 수법은 긴 역사를 갖는 스파이 수법으로 ‘미인계’(Honey Trap)라고 하는데 중국 정보기관은 ‘미인계’를 이용하여 효과적으로 정보를 수집하고 있다. 중국을 한번이라도 방문한 미국인은 중국인의 환대를 잊지 못하며, 이후 넉넉하고 따뜻한 대우를 뜻하는 ‘Panda Hug’라는 중국관을 갖게 된다. 그러나 외국인에 대한 중국인의 ‘Panda Hug’에는 대부분 여성이 개입되어 있다는 사실을 경계해야 한다.

2006년 5월 중국 상해 주재 일본 총영사관의 전신관이 여성을 이용한 중국 공안의 협박을 받아 자살한 사건이 발생했다. 그는 총영사 앞으로 남긴 유서에서 “중국인 남자가 ‘비열한 협박’을 해왔다. 나라를 팔지 않으면 안 되는 상황이 되었다. 나는 절대로 나라를 팔아먹을 수 없다.”고 적혀 있었다. 이에 일본 요미우리 신문은 ‘교우 관계’라고만 보도했으나 일본 주간문춘(週刊文春)은 영사관 직원들이 자주 다니는 ‘가라오케’의 ‘류(劉)’라는 이름의 호스티스와 깊은 관계가 있다고 전했다. 주간문춘(週刊文春)은 자살한 영사가 ‘류’를 만나 사귀면서 ’탕(唐)‘이라는 중국인 남자(중국 정보기관원)를 소개받았으며, 그로부터 끊임없는 외교기밀 유출을 요구받다가 고민 끝에 자실하게 됐다고 보도했다. 일본의 한 정보소식통은 “중국 기관원은 정사(情事) 장면 사진을 몰래 찍어 영사를 협박했다.”고 언급했다.

셋째, 기업인을 이용한 첩보활동이다. 중국의 경우는 합법적이며 밝은 장소에서 당당히 스파이 활동을 하는 경우가 많다. 중국 북경에 소재한 다수의 연구단체는 독립 싱크탱크처럼 보이나 실제로는 정부와 직·간접적으로 연계되어 있고, 외국의 과학자나 연구자를 초대하여 공동작업을 수행한다. 중국 인민해방군 직속의 국제문제 관련 연구단체는 공동연구라는 명목으로 미국 학자들을 빈번히 초대하는데, 이는 합법적 활동이며 결과적으로 미국 두뇌로부터 직접 첨단정보를 입수하는 것이다. 그리고 미국에 위장회사를 설립하여 공작원을 주재원으로 파견, 원하는 정보를 갖고 있는 기업과 상거래를 하는데, 합법적 비즈니스이지만 분명한 정보활동이라고 할 수 있다.

다섯째, 로비를 통한 정보활동이다. 로비 활동은 최근 중국 정부가 많은 힘을 쏟는 합법적 정보활동의 하나인데, 로비 관련 예산도 급증하고 있다. 중국 정부는 국제 법률사무소 '호건 & 하트슨'에 2003년부터 2년간 130만 달러의 보수를 지불했다. 미국 의회에 대한 로비의 결과, 2005년에 16명의 연방의회 의원들이 자비로 중국을 방문했는데, 2003~2004년 기간 중 방중(訪中) 의원이 11명에 불과했던 점과 비교하면 약 3배 이상 증가한 수치이다.

여섯째, 언론인으로의 신분위장이다. 중국은 서방권이 향유하는 언론의 자유를 '스파이 행위를 하는 자유'로 이해하고 있다. 의회에서 중국에 관련된 문제가 의제가 되면 중국인 기자가 대거 몰려드는데, 그들 모두 기자 신분증을 제시하긴 하지만 그들의 목적이 어디에 있는지는 누구라도 알 수 있다. 중국 국영 신화사 통신에 근무하는 기자가 어느 날 외교관의 자리에 앉아 있는 등 기자와 외교관 등 두 개의 신분을 갖고 활동하는 인물들이 많이 있다.

일곱째, 인민해방군의 첩보활동이다. 중국의 공식적 정보기관은 국가안전부이지만, 인민해방군의 정보조직이 예산·조직·인재 면에서 압도적인 힘을 갖고 있다. 인민해방군 총참모부 산하 정보공작부대는 국내부서와 국제부서로 분류되어 있는바, 양 부서가 유기적으로 결합되어 있다. 국내 첩보활동의 핵심은 13만 명으로 구성된 전화도청팀인데, 이들은 특정 단어에 자동적으로 반응하는 시스템을 통해 모든 통화를 효과적으로 검열하고 있다. 국제 첩보활동은 인민해방군이 직접 지휘하는바, 외국의 중국대사관에 주재하는 무관이 현지 책임자로 활동한다.

3. 중국 정보기관의 대일(對日) 인간정보(HUMINT) 활동

1972년 日·中 국교 정상화 이후 본격적으로 시작된 중국의 대일(對日) 정보활동은 다양한 수법으로 계속되고 있다. 그간 오랫동안 경험이 누적된 결과 지금은 자위대, 경찰간부, 고급관료, 국회의원 비서 등이 협력자가 되는 등 중국 정보기관은 일본의 권력 중추에 깊숙이 개입하고 있다. "표면에 드러난 사건은 빙산의 일각에 불과하며, 이미 일본의 국가기밀에 접

근할 수 있는 위치에 있는 많은 일본인들이 중국 정보기관의 협력자가 되었다."고 일본의 공안관계자는 경고하고 있는 실정이다(袁翔鳴, 2006a; 袁翔鳴, 2006b; 大野和基, 2006).

중국의 대일(對日) 인간정보(HUMINT) 활동은 앞서의 대미(對美) 인간정보(HUMINT) 활동과 유사하나 본 연구에서는 대일(對日) 인간정보(HUMINT) 활동 중 ① 재일(在日) 중국단체와 연구회를 활용한 협조자 포섭, ② 공작원 활동 및 협력자 활용, ③ 산업스파이 활동 등 특이내용을 분석하였다.

첫째, 재일(在日) 중국단체와 연구회를 활용한 협조자 포섭이다. 일례로 일본 동경 도심에 위치한 소극장 회의실에서는 매월 마지막 휴일 야간에 백 명 안팎의 중국인들이 모여 정치, 경제, 국제문제 등에 관한 연구회를 개최한다. 참석자들은 대부분 유학생과 일본 회사에 취업한 청년들로서 중국의 미래와 중・일 관계 등 다양한 사안들을 활발하게 논의한다. 중국인들이 자유롭게 토론하는 모임이 별로 없기 때문에 연구회의 인기는 매우 높다. 그러나 내막을 살펴보면 중국 정보기관의 공작원이 모임을 이용하여 협력자를 확대해 나가고 있음을 알 수 있다. 중국 최대의 정보기관인 국가안전부와 인민해방군 첩보부의 공작원이 회사원 등으로 위장하여 참석, 일본 사회에서 기밀정보에 접촉할 수 있는 사람들에게 은밀히 접근하여 이들을 협력자로 포섭한다. 물론 이 연구회에만 국한된 것은 아니며 '일본에서 실시되는 모든 회합이 유사한 구도'라고 할 수 있다.

둘째, 공작원 활동 및 협력자 활용이다. 중국 정보기관은 전문교육을 받은 프로 정보원을 '기본동지'로 부르며, 기본동지의 포섭에 의해 공작원이 되어 정기 또는 부정기적으로 돈을 지급받는 협력자를 '운용동지'로 호칭한다. 운용동지의 수는 최소한 기본동지의 배이며 많은 경우는 10배에 달한다. 정보공작의 프로인 기본동지는 중국 내에서는 국가공무원 또는 지방공무원으로 임명되어 있으며 공적이나 연공서열에 따라 신분이 상승한다. 기본동지가 활동지에서 체포되는 경우, 중국 정부는 자국인 보호법이나 스파이 교환 등의 명목으로 외국정부와 교섭하여 철저히 보호한다.

중국 정보 공작기관은 해외에서 활동할 때 현지 정보 제공자들의 활동이 매우 중요하다는 점을 잘 알고 있으므로 각국의 협조자 포섭활동에 특별히 힘을 쏟고 있다. 현지에서 공작원을 포섭하는 무기는 중국에 대한 애국심과 금전적 보상이다. 일본에서의 경우 운용동지에 지불되는 정보료는 1건에 수만 엔부터 수십만 엔까지 다양한데, 첨단기술과 자위대의 기밀문서나 주일미군에 관한 내부자료는 매우 높아 100만 엔에 달하는 경우도 있다. 이외에 신문에 발표되지 않는 대기업의 부장급이하 인사이동이나 신뢰성이 희박한 정국 정보 등에 돈을 지불하는 경우가 있는데 이는 공작원을 묶어두려는 수법으로 정보의 가치보다 장래에 유가치 고급정보를 가져오기를 바라는 기대료가 포함되어 있다. 일본에는 78,000여명의 중국인 유학생이 체류하고 있어 중국 공작요원이 운용 동지를 포섭하는데 부족함이 없는 실정이다.

이러한 중국의 공작원 양성은 일본뿐만 아니라 유럽・미국을 중심으로 하는 세계 각지에 확대되어 중국의 민주화운동 탄압에도 활용되고 있다. 미국에서는 재미유학생, 駐워싱턴 중국대사관 등 중국 외교시설, 재미 중국기업 지사 등의 사무소가 모두 중국의 스파이망에 포함되어 있을 가능성이 있다. 미국과 유럽 등지에서 지난 수년간 기업 등의 기밀을 절취한 혐의로 체포된 유학생 등은 모두 운용동지들인데, 중국정부는 이들이 체포될 경우 방임자세로 일관한다. 미국 중앙정보국(CIA)과 영국 군사정보부(MI6) 등 정보기관은 “중국 정보기관의 정보기법은 아직 발전단계에 있으나 인해전술(人海戰術)은 무섭다.”고 평가하고 있다.

셋째, 산업스파이 활동이다. 중국의 산업스파이 활동은 크게 2가지로 분류되는데 하나는 사이버 스파이라 불리는 것으로 군 시설・핵 연구소・국방부와 계약하고 있는 기업의 컴퓨터 등을 해킹하여 중요한 기술을 훔쳐내는 것이며 다른 하나는 인간정보(HUMINT), 즉 사람이 직접 행하는 스파이 활동으로 국가안전부가 직접 관할한다. 일본은 중국의 정보수집 능력을 낮게 평가하고 있으나 실제로는 미국 중앙정보부(CIA)의 능력에 버금가는데, 도청기 등도 중앙정보부(CIA)가 사용하고 있는 것과 동일한 성능이며, 중요인물의 차에는 GPS 장치를 부착하여 소재지를 파악하고 있다.

일본 내에서 활동하는 중국 스파이는 활동 목적이 법륜공과 같은 반정부인사를 감독하는데 있는 것이 아니라 일본의 기술을 입수하는데 있다. 중국이 미국에서 입수하는 것은 핵과 미사일에 관한 군사기술이나, 일본에서는 군사전용 여부를 불문한 최첨단기술 관련 정보이다.

중국의 대일(對日)・대미(對美) 인간정보(HUMINT) 공작에서 가장 많이 사용하는 형태는 현지에 위장회사를 설립하여 주재원으로 부임시키는 방법이다. 위장회사는 겉으로 보기에 보통의 기업과 다르지 않기 때문에 동 회사원들이 스파이인지 비즈니스맨인지 구별할 수 없으며, 필요시 공식적 상거래를 통해 기술을 입수한다. 이들은 투명한 직함을 갖고 있기 때문에 스파이라는 것이 발각되기 어렵다.

일본 기업에서 일하고 있는 중국인 연구원은 입사 당시는 스파이가 아니었다 해도 도중에 포섭되어 에이전트가 되는 사례가 많다. 연구원을 스파이로 사용하는 이유는 중국에 필요한 기술이 무엇인지 판단할 수 있는 능력을 갖고 있기 때문이다. 유학 또는 상사 주재원 등으로 부임하고 있는 중국인 가운데 정부 관료 자제들은 스파이 활동에 종사하고 있을 가능성이 높다. 개별적으로 수집한 정보는 대사관이나 영사관에 배치된 특정인물이 종합한다.

4. 중국 정보기관의 인간정보(HUMINT) 활동 특징

중국은 인간정보(HUMINT) 활동을 중심으로 고급정보를 입수하는 대표적인 국가라고 할 수 있으며 전형적인 인간정보(HUMINT) 활동기법을 준수하고 있다고 할 수 있다. 중국

의 인간정보(HUMINT) 활동은 소위 '인해전술'(人海戰術)과 유사한데 중국 정보기관의 인간정보(HUMINT) 활동에 대한 미국의 위기의식을 언론보도를 통해 살펴보면 다음과 같다.

중국 국가안전부의 독특한 정보원 충원과 운영방식은 냉전 시절 소련스타일에 익숙해진 미국의 정보당국을 당혹스럽게 했는데 이는 전통적인 비밀 기법을 사용하지 않기 때문이다. 전 세계에 퍼져 있는 자국 유학생과 과학자들, 기업인들이 그들의 '잠재요원'이다. 1975년부터 3년 동안 중앙정보국(CIA) 중국지부장을, 1989년부터 2년 동안 주중 대사를 지낸 제임스 릴리는 "해변의 특수한 모래를 가져오라는 지령이 떨어졌다면 러시아라면 깊은 밤 잠수함으로 정예요원들을 침투시킨 뒤 양동이에 모래를 담아 오겠지만 중국은 자국인 500명을 해변으로 소풍을 보낸 뒤 작은 캔에 모래를 담아오게 할 것이다."는 분석이다. 국제안보연구기관인 '글로벌 시큐리티'도 "미국 내 70여개 사무실에서 일하는 1,500명의 외교관들, 매년 미국으로 유학 오는 1만 5000명의 학생과 1만여 명의 각종 사절들이 모두 잠재적 정요요원에 포함될 수 있다"고 지적하고 있다(중앙SUNDAY, 2007.6.17字; ジョシュア・アイゼンマン, 2006).

이러한 중국의 인간정보(HUMINT) 활동은 ① 출처의 개척, ② 수집활동, ③ 첩보전달 등 전형적인 인간정보(HUMINT) 이론에 근거를 두고 활동하고 있음을 알 수 있다.

첫째, 중국 정보기관은 상대국 정보제공자 즉, 출처의 개척을 위하여 수단과 방법을 가리지 않는다. 정보제공자의 성격, 신념, 기호, 취향, 재정상태, 교우 및 여자관계 등 신상을 파악하고 이에 맞는 정보공작을 통해 정보제공자를 포섭하고 정보를 자발적으로 또는 강제적으로 제공하도록 조치함을 알 수 있다. 이러한 중국 정보기관의 정보제공자 포섭 방식은 해당국의 인원보안 시스템을 치밀하게 분석하여 그 공백을 적극 활용하는 방식이라고 할 수 있다. 따라서 우리나라 입장에서 볼 때 인원보안의 중요성이 대단히 중요하다고 하겠다.

둘째, 수집활동의 경우도 상대국 정보제공자 대상 인간정보(HUMINT) 활동 이외에도 공식적인 기업 활동, 언론 활동, 로비 활동, 현지 유학생 및 자국인 활용 등 다양한 방법을 지속적으로 동원한다. 그러므로 인원보안 관리수단의 확보가 절실히 요구된다고 하겠다.

셋째, 첩보전달의 경우는 유흥업소 종사자, 유학생, 교포 등을 통해 대사관 정보요원 등이 첩보를 수집, 종합하여 인편, 우편, 전화, 팩스, 인터넷 등 다양한 전달수단을 활용하여 본국으로 송부한다. 따라서 국가 차원의 방첩능력 제고가 필요하다고 하겠다.

V. 산업기술 보호방안

최근 우리나라 기술인력의 핵심기술 유출사례 등이 계속되고 있는 점을 감안할 때 인간정

보(HUMINT)를 이용한 외국정보기관의 우리나라 산업기술 획득을 위한 정보활동을 무시할 수 없는 실정이다. 따라서 외국정보기관의 인간정보(HUMINT) 활동에 대한 적극적인 대응방안 마련이 시급하다.

본 장에서는 외국정보기관의 인간정보(HUMINT) 활동 대응방안을 우리나라의 현실적인 문제점과 연계하여 산업기술 보호방안을 중심으로 제시하고자 한다. 외국정보기관의 인간정보(HUMINT) 활동에 대한 우리나라의 산업기술 보호방안은 ① 인원보안의 중요성 인식, ② 인원보안 관리수단 확보, ③ 국가 방첩능력 제고 등이 있다.

1. 인원보안의 중요성 인식

기업이나 각급 행정기관을 막론하고 인원, 시설, 문서, 통신 등 보안관리 중에서 가장 어느 것 하나 중요하지 않은 분야가 없겠으나, 그중에서도 인원보안이 가장 중요하다고 할 수 있다. 왜냐하면 보안관리도 사람이 하는 것이고 모든 보안사고도 사람에 의하여 일어나는 것이기 때문이다. 인원보안관리가 중요한 반면에 제일 어려울 수도 있는데 사람은 상황에 따라 창의적이고 능동적인 대응을 할 수 있는 장점이 있는 반면에 이기적이고 감정적이기 때문에 이해관계 또는 기분이나 감정에 따라서는 수시로 생각을 달리할 수 있을 뿐만 아니라 심지어는 자기의 기업을 배신할 수 있는 취약점도 있기 때문이다. 이렇게 시간에 따라, 이해관계에 따라 각각 다른 생각을 가지고 있는 직원들을 오직 기업의 이익을 위하여 보안관리에 최선을 다할 수 있도록 관리하는 것은 대단히 어렵고 중요한 것이다(국가정보대학원, 2006: 77-78).

<표 5-1>은 산업기술 유출의 신분별 현황을 보여주고 있다. 2003년부터 2007년까지 산업기술 유출사례 107건 중 기술유출사범의 신분이 전직직원(61%), 현직직원(25%) 등 전·현직 직원(86%)에 의해 발생했음을 보여주고 있어 인원보안의 중요성을 강조하고 있다. 따라서 관공서뿐만 아니라 일선 기업체에서는 인원보안의 중요성을 인식하고 정보보호 차원에서 보안관리를 철저히 시행해야 할 것이다.

<표 5-1> 산업기술 유출의 신분별 현황

총계	전직직원	현직직원	유치 과학자	용역업체	외국 유학생	투자업체
107(건)	65	27	3	8	2	2
100(%)	61	25	3	7	2	2

자료 : 국가정보원, 2007

2. 인원보안 관리수단 확보

인원보안 관리를 위해서는 보안에 대한 직무지식 함양이 선행되어야 하고, 보안에 대한 실천의지(정신자세)가 투철해야 하며, 주변환경이 보안관리에 유리하게 조성되어야 한다. 이와 같은 보안관리의 요소를 구비하기 위해서는 ① 신원조사, ② 동향파악, ③ 보안교육, ④ 보안서약 등의 인원보안 관리수단 확보가 요구된다.

신원조사는 당사자와 당사자 주변인물에 대한 동향, 인품, 소행 등 당사자의 보안적 적성을 판단하는데 필요한 기초적 신원정보를 수집하기 위하여 실시하는 대인(對人) 보안조사를 말한다. 동향파악은 대상자의 신원은 조사시점에서 완벽한 조사가 되었다 할지라도 주위환경의 변화에 의해 신상의 변화를 일으킬 수 있는데 동향파악은 바로 신상동향의 변화를 주시하여 보안상 위험성의 유무를 검토하는 것이며, 감독자에 의한 예방적 신원조사를 말한다. 보안교육을 통해 인원의 보안지식을 함양함으로써 보안의식을 제고하고 보안사고를 줄일 수 있다. 보안서약은 보안대상자에게 심리적인 제약을 가하는 데 의미가 있으며 법적으로도 의미를 가지게 된다(김윤덕, 2001: 197-198).

인원보안 관리방법으로는 ① 임용시의 관리, ② 재직중 관리, ③ 퇴직시 관리 등이 있다. 임용 시에는 가능한 방법을 동원하여 다른 사람들에게 악용 당할 수 있는 취약점을 확인하고 이러한 취약점이 비교적 적은 사람을 임용하거나 보직하고 경쟁기업의 위장침투에도 유의하여야 할 것이다. 재직 중인 임직원 관리에도 보안상 중요보직을 중심으로 동향파악, 보안교육, 보안조치 등의 수단을 적절히 활용하고 취약점이 발견될 경우에는 신속한 대응책을 강구하여야 한다. 퇴직 시에는 퇴직자가 자의 또는 타의를 막론하고 기업에 대하여 나쁜 감정을 갖기 쉬우므로 보안관리 측면에서 보안협조, 보안조치 및 퇴직 후의 동향파악 등의 관리가 필요하다(국가정보대학원, 2006: 81-95).

<표 5-2>에서 나타난바와 같이 산업기술 유출의 목적이 개인영리(42%), 금전유혹(30%), 처우불만(13%), 인사불만(6%) 등으로 나타난 것은 핵심인원에 대한 보상체제의 중요성을 보여주고 있다. 따라서 핵심인원에 대한 보상체제 보완도 병행되어야 한다. 정보수집자와 정보제공자 간에는 수요와 공급의 관계가 있다. 정보수집자는 정보제공자의 신분 불안, 낮은 보상 등을 약점으로 이들에게 접근하고 있다. 정보제공자들에게 애국심과 국가관에 호소하기 보다는 이들에 대한 정당한 처우를 통해 정보수집자와 정보제공자의 접촉이 원천적으로 배제되어야 할 것이다.

<표 5-2> 산업기술 유출의 목적

총계	개인영리	금전유혹	처우불만	인사불만	비리연루	기 타
107(건)	45	32	14	7	4	5
100(%)	42	30	13	6	4	5

자료 : 국가정보원, 2007

3. 국가 방첩능력 제고

방첩(防諜)은 적대적인 정보기관의 공작에 대항하여 국가 및 자국의 정보관련 행위를 보호하기 위한 정보의 수집, 분석 및 수행된 공작활동을 의미한다. 통상적으로 방첩은 ① 자국을 겨냥한 적국의 정보수집능력에 대한 정보를 파악하는 '수집', ② 적대적 정보기관이 자국의 정보기관에 침투하는 것을 차단하는 '방어', ③ 자국의 보안체제 대응한 적의 노력을 확인하고 적의 공격을 조작하거나 허위정보를 본국에 전달하는 '공격' 등 3가지로 구분되는데 인간정보(HUMINT)를 통한 외국의 정보활동에 대처하기 위해서는 '방어'가 무엇보다도 중요하다.

방어는 적성국 정보기관의 정보활동에 대한 감시활동을 통해서 이루어진다. 적성국 정보기관의 활동을 알아보는 명확한 방법은 그들에 대한 지속적인 감시장치를 통한 감시이다. 감시활동을 통해 파악된 내용들은 혐의가 있는 인물에 대해 중요한 단서를 확보하는 방법이다. 효과적인 감시활동을 통해 적대적 정보기관이 자국의 정부・주요기관・정보기관에 침투하는 것을 차단한다. 감시활동 외에도 직접적인 조치를 통해 정보수집을 제거하고 무력화시킨다. 적성국 정보기관에 의해 고용된 공작원이 체포될 수 있으며, 외교관으로 가장한 외국정보관이 추방될 수도 있다(김윤덕, 2001: 201-203).

이러한 국가 방첩능력 제고를 위해서는 국가정보원, 경찰청, 기무사령부 등 우리나라의 정보・보안기관의 역할이 무엇보다도 중요하다. 이들 국가기관은 민주화 진전으로 관련업무 절차가 법적・제도적으로 투명해 짐에 따라 기관 고유의 정보・보안 업무가 상당부분 위축되는 등 부작용이 일부 있었다. 그러나 최근 들어 국가정보원을 중심으로 외국정보기관의 정보활동, 외국기업의 산업스파이 활동 등에 대해 관심을 가지고 적극 대처하고 있는 점은 국가간 기술경쟁이 심화되고 있는 시점에서 매우 고무적인 일이다. 이들 정보・보안기관들의 활동이 체계적으로 진행될 수 있도록 국가정보원법 등 해당기관 설치 근거법, 형법, 산업기술의 유출방지 및 보호에 관한 법률 등에 대한 보완 및 강화가 요구된다.

Ⅵ. 결론 및 제언

본 연구는 외국정보기관의 인간정보(HUMINT) 활동과 관련하여 중국 국가안전부 등 중국 정보기관들의 미국, 일본 등 주요국가 내에서 진행한 정보활동에 대한 사례연구를 진행하였다. 사례연구를 통한 외국정보기관의 인간정보(HUMINT) 활동은 ① 자국인 및 현지인 활용 정보활동, ② 미인계 이용 정보활동, ③ 기업인 이용 첩보활동, ④ 로비를 통한 정보활동, ⑤ ⑥ 언론신분 위장, ⑦ 중국단체와 연구회를 활용한 협조자 포섭, ⑧ 공작원 활동 및 협력자 활용, ⑨ 산업스파이 활동 등으로 요약된다.

외국 정보기관의 인간정보(HUMINT) 활동에 대응한 산업기술 보호방안은 다음과 같다.

첫째, 인원보안의 중요성을 인식하고 정보보호 차원에서 보안관리를 철저히 시행하여야 한다. 둘째, 보안관련 직무지식 함양, 보안 실천의지 제고, 주변 보안환경 조성 등 인원보안 관리수단을 확보하여야 한다. 셋째, 국가 정보・보안기관의 역할 강화, 정보・보안 관련법규 보강 등 국가 방첩능력을 제고하여야 한다.

이와 함께 본 연구에서는 외국정보기관의 인간정보(HUMINT) 활동과 관련하여 다음과 같이 제언하고자 한다.

우리나라는 지난 2007년 기준 1인당 국민총소득(GNI)이 20,045달러로서 사상 처음으로 2만 달러를 돌파하였는데 이는 1995년 1만 달러를 돌파한 이후(실제로는 11,471달러) 12년 만에 2만 달러 고지를 달성한 것이다. 우리나라가 국내・외의 어려운 경제여건 속에서도 2만 달러 고지를 돌파한 계기는 반도체, 조선, 휴대폰, 자동차 등 첨단 산업기술 등 관련 정보의 국제적 우위에 따른 결과라고 해도 과언이 아니다.

이러한 가시적인 성과에도 불구하고 우리는 선진국과 후진국 사이, 또는 '일본'과 '중국' 사이에 위치한 소위 '샌드위치 국가'라고 자조(自嘲)하는 경향이 있다. 우리나라가 선진국으로 도약하느냐, 후진국으로 도태되느냐는 우리 스스로가 산업기술 등 관련정보의 국가적 경쟁력을 갖추는 것에 달려 있다. 우리는 후발국가들이 우리의 첨단 산업기술 등 관련정보를 계획적으로 입수하기 위한 제반 정보활동을 전개하는데 대해 적극적인 보안활동을 통하여 차단하는 한편, 나아가 고도의 산업기술 등 관련정보를 개발하는데 중점을 두고 국가전략을 추진해야 할 것이다.

또한, 외국정보기관의 우리나라 내 정보활동도 미국, 일본 등 선진국의 사례와 대동소이할 것으로 추정되므로 우리나라 정보・보안기관에서도 국익을 해치지 않는 범위에서 관련 사건 및 자료를 공유하여 국내 국가기관 및 일반기업의 경각심을 제고하여야 한다. 최근 국가정보

원이 첨단산업기술보호동향, 정보보호백서 등을 정기・비정기적으로 발간하여 일반에게 공개함으로써 사회의 관심을 유도하는 것은 시의적절한 조치라고 할 수 있다. 학계에서도 정보・보안 관련연구를 충실히 진행하여 그 연구결과가 정부, 기업, 학계 등 관련요소에 선순환하여 보안대책 마련 및 국가 발전에 기여할 수 있도록 해야 할 것이다.

참 고 문 헌

1. 국내문헌

강기욱(1997).『정보아카데미』. 한국생산성본부.

강기택(2003).『경찰정보론』. 경찰대학.

노호래(2008), "산업기술 유출범죄에 대한 정책적 대응방안".『한국공안행정학회』 제17권 제1호: 45-77.

국가정보대학원(2006).『산업보안실무』.

국가정보원(2004).『산업스파이 식별요령』.

_____(2007).『산업기술유출방지법 要解』.

김윤덕(2001).『국가정보학』. 박영사.

문화일보(2008). "美, 中 스파이와의 전쟁"(2.12)

박영일(1994).『강대국의 정보기구』. 현대문예사.

야후 백과사전(2008).『신화사』. http://www.yahoo.co.kr.

조선일보(2007). "산업기술 잇단 유출 막으려면……. '사람 유출'을 막아라"(12.15).

중앙SUNDAY(2007). "세계의 정보기관"(6.17).

최윤호(2001).『효과적인 경쟁정보 수집활동 기법에 관한 연구』. 연세대학교 산업대학원 석사학위논문.

2. 외국문헌

ジョシュア · アイゼンマン(2006). "アメリカも頭を抱える中國スパイ網が仕掛ける罠". SAPIO (2006.4.12), 東京: 小學館.

大野和基(2006), "日本の最先端技術を盜む中國國家安全部産業スパイ · 工作員の全手口", SAPIO (2006.3.22), 東京: 小學館.

袁翔鳴(2006a), "傳說の大物工作員が5年で築き上げた對日スパイ網, SAPIO(2006.8.23), 東京: 小學館.

_____(2006b), "蠢く！中國對日特務工作白書退官陸自一佐を協力者に仕立て上げた周到工作の一部始終", SAPIO(2006.9.27), 東京: 小學館.

ABSTRACT

A Research on the Industry Technology Protection Way against Foreign Secret Service's HUMINT Activity

Joo, Il-Yeob

The purpose of this study is to progress foreign secret service's human intelligence(HUMINT) activity through case study. This study presents confrontation way of our country analyzing characteristic of foreign secret service's human intelligence(HUMINT) activity and examples concretely. The examples that is used this study is foreign secret service's human intelligence(HUMINT) in USA and Japan.

The following was the result of the study.

First, we need importance awareness of persons security that correspond in foreign secret service's human intelligence activity.

Second, we must secure administrative means for persons security means to correspond in foreign secret service's human intelligence (HUMINT) activity.

Third, we must raise anti-espionage ability that correspond in foreign secret service's human intelligence(HUMINT) activity.

Key Words : Secret Service, Intelligence Activities, Human Intelligence(HUMINT), Industry Technology, Protection Way