2013-15 책임연구보고서

한국의 산업기술 해외 불법유출 실태와 대책

치안정책연구소
POLICE SCIENCE INSTITUTE

2013-15 책임연구보고서

한국의 산업기술 해외 불법유출 실태와 대책

치안정책연구소 범죄수사연구실
연구관 정 웅

목 차

Ⅰ. 서 론

우리나라는 1980년대 외환자유화와 1990년대 OECD 가입(1995) 등을 거치면서 국제적 자유무역의 확대 조류 속에 산업발전과 경제성장을 도모하여 왔다. 비록 국내적으로는 1997년 IMF 외환위기라는 단기 외환유동성 위기와 경제난을 맞기도 하였으나 2000년대 이후에도 지속적인 기술혁신을 통하여 세계경제의 무대 위에 전기전자와 조선, 자동차, 정보기술 등을 경제의 주력산업으로 발전시켜왔다. 또한 2008년에 시작된 글로벌 금융위기(Global Financial Crisis)와 뒤이은 유로존 재정위기(2011)의 상황에 직면하여서도 우리 정부는 녹색환경과 융합기술을 비롯한 첨단·신기술의 연구개발에 지속적인 정책지원을 추진하여 왔으며, 최근에는 창조산업(creative industry)에 기반한 경제구조의 고도화를 기하고 있다.

우리나라는 과거 저개발, 산업화 시기에 소위 선진 산업기술의 불법 침해 국가로 의심을 받기도 하였던 처지와 달리, 오히려 이제는 세계적 경쟁 산업국가와 경쟁기업들로부터 불법유출의 주요 대상이 될 수도 있는 입장이 되었으며, 실제로 전기전자와 정보통신, 정밀화학, 정밀기계 등 고부가 첨단기술 분야에서 국내 주요 기업들의 산업기술이 해외로 불법유출 되는 사례가 발생하고 있다. 이러한 첨단기술의 불법유출은 개인이나 개별 기업 차원의 손실을 넘어 장기적으로 해당 산업 전체의 경쟁력과 국가경제 자체의 존립 기반에 큰 위해 요인이 될 수 있다.

첨단기술 해외 불법유출이 갖는 이러한 중층적 위험성 때문에 우리나라는 기존 영업비밀보호법의 대폭적인 개정(2004) 외에도 산업기술의 보호에 관한 법률의 제정(2006)을 통해 미국의 경제스파이법(Economic

Espionage Act of 1996)이나 일본의 개정 부정경쟁방지법(1990), 또는 독일의 부정경쟁방지법(UWG, 1909년 제정) 등에도 뒤지지 않는 法制的인 불법유출 대응장치를 마련하여 왔다. 또한 첨단기술 불법유출 대응 조직으로서 국가정보원과 경찰 등 유관 부서에서는 산업기술 유출 예방 및 수사 활동 강화를 통하여 경제적 가치가 높은 첨단 산업기술에 대한 불법유출을 차단하는 노력을 지속적으로 기울여 왔다.

이러한 제도적 정비와 대응활동에도 불구하고 우리나라 첨단 산업기술의 해외 불법유출을 보면 그 추세가 꺾이지 않아 최근 2011년도까지 국가정보원에 의한 적발건수는 46건으로 사상 최대치를 기록했으며, 경찰청에 의한 검거건수 역시 2011년 24건, 2012년 27건에 달함으로써 역대 최고치를 경신하고 있다.

본 연구는 이처럼 탈냉전 이후 국제경제환경 변화와 국내 산업발전으로부터 야기되는 산업기술 해외 불법유출 방지책에 대한 필요성 문제를 제기하면서, 최근 미국의 산업보안 정책에 대한 분석을 바탕으로 이들이 우리의 산업기술 해외 불법유출 대응에 주는 함의를 도출하는데 그 목적을 두고자 한다.

본 연구는 Ⅱ장에서 국제경제환경 변화 속에 산업보안이 갖는 공공성의 의미와 산업보안의 효율성 추구를 위한 성과모형을 고찰하고 Ⅲ장에서는 우리나라의 최근 산업기술 해외 유출 실태를 살펴본 후, Ⅳ장에서 미국의 산업보안 정책을 통해 이것이 우리의 불법유출 대응에 주는 함의를 도출해 보는 순으로 진행하고자 한다.

Ⅱ. 산업보안의 公共性과 성과모형

1. 산업보안의 의의와 公共性

현재 세계경제는 글로벌 금융위기와 유럽 국가들의 재정위기의 여파로 일부 국가들의 보호무역주의적인 정책이 산견되고는 있으나 여전히 다자주의(Multilateralism)에 기초한 WTO 체제와 지역주의(regionalism) 성격이 함축된 FTA가 그 주류를 이룸으로써, 자유무역의 경제질서가 그 근간을 이루고 있다. 이것은 결국 넓어진 국제시장의 치열한 경쟁 속에 한 기업이 보유한 산업기술이 기업 자신뿐만 아니라 국가의 경쟁력을 확보하는 중요한 요소로서 자리매김하고 있다는 것을 뜻한다. 이런 의미에서 기업의 공정한 영업활동 여건 조성, 나아가 산업경쟁력 및 국가이익 확보를 위한 산업기술의 보호 또는 산업보안의 필요성이 발견된다.

산업보안이라는 용어는 첨단기술 유출방지 목적 하에 국가행정 실무에서 사용되기 시작하고, 관련 법규에도 부분적으로 사용되고는 있으나[1] 그 개념 정의는 아직까지 학문적 또는 법적으로 정립되어 있지는 않다.

다만 산업보안의 주요 대상인 산업기술에 대해서 산업기술의 유출방지 및 보호에 관한 법률(이하 산업기술보호법)에서는 “제품 또는 용역의 개발·생산·보급 및 사용에 필요한 제반 방법 내지 기술상의 정보 중에서 관계중앙행정기관의 장이 소관 분야의 산업경쟁력 제고 등을 위하여 법률 또는 해당 법률에서 위임한 명령에 따라 지정·고시·공고·인증하는 다

1) 산업기술의 유출방지 및 보호에 관한 법률[법률 제11690호, 2013.3.23., 타법개정] 제18조(국제협력), 제20조(산업보안기술의 개발지원 등)에서 ‘산업보안기술’이라는 용어의 일부로 사용된다.

음 각 목의 어느 하나에 해당하는 기술을 말한다"라고 규정하고(제2조 1호), 특히 국가핵심기술에 대해서는 "국내외 시장에서 차지하는 기술적·경제적 가치가 높거나 관련 산업의 성장잠재력이 높아 해외로 유출될 경우에 국가의 안전보장 및 국민경제의 발전에 중대한 악영향을 줄 우려가 있는 기술로서 제9조의 규정에 따라 지정된 산업기술"로 정의하고 있다(제2조 2호).

산업기술의 의미 범주에는 산업기술보호법상의 산업기술 외에 부정경쟁방지 및 영업비밀보호에 관한 법률(이하 영업비밀보호법)상의 "영업활동에 유용한 기술상 또는 경영상의 정보"를 포함할 수 있다.[2)]

이상의 법제도적 논의를 기초로 산업보안을 정의하면 산업보안이란 "국가와 기업을 중심으로 산업활동에 유용한 기술과 정보를 외부에 불법유출되지 않도록 보호하는 활동"이라고 할 수 있다.

국정원의 국가정보대학원이 편찬한 '산업보안실무'에서도 산업보안을 "산업활동에 유용한 기술상, 경영상의 모든 정보나 인원, 문서, 시설, 자재 등을 산업스파이나 경쟁관계에 있는 기업은 물론이고 특정한 관계가 없는 자에게 누설 또는 침해당하지 않도록 보호. 관리하기 위한 대책이나 활동"을 의미하는 것으로 정의하여 위에서의 정의와 유사하다. 국정원은 2002년 '산업보안업무편람'에서도 산업보안을 "산업체·기업체에서 보유하고 있는 기술·경영상 정보 및 이와 관련된 인원·문서·시설·통신 등을 경쟁국가 또는 업체의 산업스파이나 전·현직 임직원, 외국인 유치과학자 등 각종 위해요소로부터 침해되지 않도록 보호하는 활동"으로 큰 차이 없이 정의하고 있다[3)]

---

2) 영업비밀보호법[법률 제11112호, 2011.12.2., 일부개정] 제2조 제2호. "영업비밀"이란 공공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로서, 상당한 노력에 의하여 비밀로 유지된 생산방법, 판매방법, 그 밖에 영업활동에 유용한 기술상 또는 경영상의 정보를 말한다.

3) 국가정보원, 산업보안실무, 1999, p. 1; 국가정보원, 산업보안업무편람, 2002, p. 3(이상 한국산업보안연구학회, 산업보안학, 2012, p. 6-7 재인용)

현재 고부가가치 산업기술의 불법유출 특히 전세계적 규모에서 전개되고 있는 해외 불법유출 행위에 대한 기업과 국가의 대응활동은 기술유출 피해 손실(loss)로부터 기업의 사적 이익을 보호한다는 측면뿐만 아니라 산업전체의 경쟁력보호, 나아가 국민경제발전 및 국가안보라는 공익적 요구를 지향한 공공성을 함께 갖고 있는 바, 그런 면에서 산업보안은 국가적 대응 측면만을 담고 있는 소위 '국가'경제방첩의 개념과 구분되며[4], 순수한 기업이윤추구 관점에서의 기업보안과도 구별된다.

즉 기업 단위 관점에서 기업이 주체가 된 '기업보안'활동은 그 보호대상에 있어서 기업의 존립이나 영업, 영리와 관련 있는 것은 모두 기업보안의 대상이 되지만, 산업보안은 기업차원의 기술보호와 함께 산업 전반의 기술유출 취약요소의 점검 및 산업 내 주요 첨단기술 보호에도 중점이 두어진다. 따라서 개별 기업 내의 임직원에 의한 금전 비리나 회사 시설관리상의 물리적 취약요소 등은 기업보안의 대상은 될 수 있지만 산업보안의 대상은 되지 않는다.

산업보안 활동이 단순히 기업 차원에 머무르지 않고, 공공성을 띠는 국가적(national) 차원의 보안활동으로 발전할 수밖에 없는 또 하나의 이유는 바로 보안을 위해 소요되는 보안 비용(security cost) 증가 문제이다.

기업이 스스로 자신의 기술보호를 위한 비용을 부담해야 하는 보안활동을 전개한다는 것은 사실 기업성장에 우선적으로 써야할 상당한 부분의 기술개발 재원이 어쩔 수 없이 산업기술 불법유출 대응활동을 위해

4) 경제방첩의 범주에는 산업보안(industrial security) 외에도, 금융보안(financial security), 물류보안(supply chain security) 등이 포괄될 수 있으나, 중요한 것은 국가경제방첩의 경우 기업이 아닌 국가가 주체가 되는 '국가적'차원에서의 대응이라는 것이다. 경제방첩의 개념과 범주, 국가경제방첩체제에 관한 논의는 다음을 참조. 정웅, "해외 주요 국가들의 경제방첩 정책과 우리의 정책과제", 국가정보연구, 제5권 2호, 2012, pp. 159-161.

희생된다는 것을 의미한다.[5)]

이는 보안 비용이 기업의 성장과정에서 확보된 첨단기술의 보호를 위해 불가피하게 지불해야하는 파생적 수요(derived demand), 또는 파생적 비용(derived cost)임과 동시에, 지속적 성장을 기대하고 있는 기업에게는 하나의 큰 도전(challenge)이 아닐 수 없다.

이처럼 기업성장과 함께 산업 내 어느 기업에게나 공통적으로 직면하는 보안 비용의 증가 문제는 국가가 공공산업 뿐만 아니라 민간산업 부문의 보안을 위해 공공재(public goods)적 성격을 가지고 개입하는 논거가 된다.

그러나 이보다 더 중요한 논거 내지 현실적인 위협은 경쟁기업이 속한 국가와 행정부의 지원을 받는 산업기술 불법유출 기도 또는 타국 정부기관 자체에 의해 자행되는 직접적인 불법유출 활동이다. 첨단기술을 보유한 기업들은 대부분 생산 및 상거래 과정에서, 기업 차원뿐만 아니라 국가적 차원의 지원을 받는 기술유출 위해요소에 노출되어 있다.

따라서 이 같은 ① 산업기술의 공익성, ② 기업의 불가피한 보안비용 부담 문제, ③ 국가적 차원에서 전개되는 불법유출 위협의 존재 등은 산업보안이 공공성을 띨 수밖에 없게 되는 여건을 조성하고 있다.

2. 산업보안의 성과모형

국가와 기업이 참여하는 산업보안의 정책 구상에서 가장 우선적인 정책지표로는 산업기술의 해외 불법유출로 인한 손실(loss) 수준을 들 수 있다. 한편 불법유출로 야기되는 피해의 예방과 기업자산의 보호를 위한

5) ONCIX, “ECONOMIC ESPIONAGE”, http://www.ncix.gov/issues/economic/index.php (2013. 12. 1 검색).

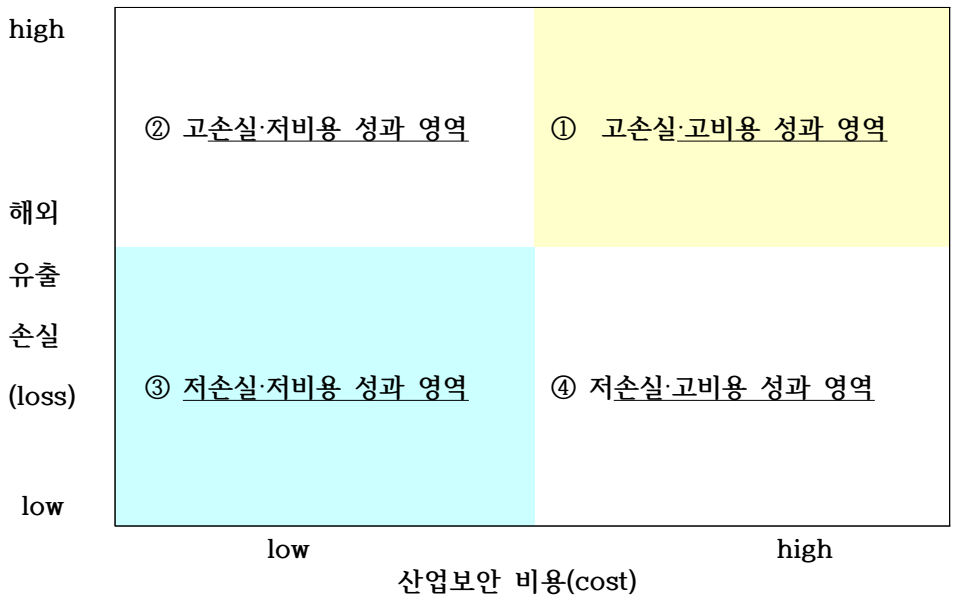
산업보안 활동에는 불가피하게 국가예산과 기업의 지출이 수반되는 바, 그에 따른 또 하나의 주요 정책지표로서 보안비용(cost)의 지출을 설정할 수 있다.

산업보안 정책의 선택과 추진 결과들은 <그림 1>과 같은 불법유출 손실과 보안비용을 각각의 行列로 하는 산업보안 정책의 손실-비용 매트릭스(matrix of loss and cost) 형태의 성과모형을 구축할 수 있다.[6)]

그에 따른 산업보안의 정책성과는 기술유출 피해로 인한 손실과 소요된 비용에 따라 다음의 4가지 성과 조합으로 분류해 볼 수 있다. 즉 ① 고손실·고비용 성과 조합 영역 ② 고손실·저비용 성과 조합 영역 ③ 저손실·저비용 성과 조합 영역 ④ 저손실·고비용 성과 조합 영역으로 나타난다.

6) 산업보안보다 넓은 범주에서의 접근된 경제방첩 모형에서는 안보위험과 방첩비용을 행렬로 하는 위험-비용 매트릭스(matrix of risk and cost)가 제시된 바 있다(정웅, 앞의 글, p. 136.). 본 연구의 손실-비용 매트릭스와 성과방정식은 위 선행연구의 모형이 변형, 발전된 것이다.

<그림 1> 산업보안 정책의 손실-비용 매트릭스(Matrix of loss and cost)



이러한 여러 가지 가능한 정책성과 조합 가운데서도 불법유출 손실의 최소화와 보안비용의 최소화라는 성과를 달성할 수 있는 ③ 분면의 저손실·저비용 성과 조합 영역이 가장 바람직한 정책목표로서 추구되어야 할 것이다. 다시 말해 산업보안 정책의 우선적 목표로서 추구되는 낮은 수준의 불법유출과 그 손실의 최소화는 불법유출 대응과정에서 상대적으로 적은 보안비용이 지출될 때 그 성과가 보다 큰 의미를 갖게 된다.

이와 같은 산업보안의 정책목표 즉 저손실·저비용 성과 조합을 달성하기 위한 정책은 투입되는 보안예산의 규모, 人·物的 보안요소에 대한 자원배분 성향, 조직의 확대와 개편 수준 등 정책수단의 가용 여건과 예상되는 정책지표의 수준에 따라 다양한 정책대안들로 제시될 수 있다.

예컨대 많은 예산을 확보하여 우선 인력 증원에 배분하고 유관부서 신

설과 조직 확대 등을 통한 정책 옵션을 선택할 때 이는 위에서 말한 소위 저손실·고비용의 정책성과 조합을 기대할 수 있다. 반면 적은 예산 투입을 염두하면서 보안 부서의 단순 재편과 인력 재배치, 다기관 협력이나 민간부문의 자발적인 참여에 의한 정책 옵션을 선택할 때 이는 소위 고손실·저비용의 정책성과 조합을 기대할 수 있다.

그러나 이것은 어디까지나 시행 전에 기대되는 각 정책대안들의 성과들이며, 실제의 결과들은 정책의 집행과 세부 운영과정에서 달라질 수 있고 따라서 손실-비용 매트릭스의 어느 분면 위에도 위치 가능하다.

특히 단일 정책대안만이 선택되는 것이 아니라 여러 정책들이 함께 집행되기 때문에 그 선택과 운용과정에서 여러 대안들의 성공적인 정책조합(policy mix), 피해손실에 대한 효율적인 위험관리(risk management)가 이루어질 경우 가장 바람직한 결과인 ③ 분면의 저손실·저비용 성과 조합 영역에 도달할 수도 있다.

그러나 이러한 손실-비용 매트릭스를 통한 성과모형은 사실 정책의 개략적인 성과 분류와 사후 비교 평가, 향후 정책 방향 선택 등에 대한 윤곽만을 제시할 뿐 정책의 실제적인 성과 측정과 조작적 운용에는 극히 미흡하다. 따라서 아래와 같은 손실-비용 방정식을 통해 성과모형의 수리적 접근, 나아가 향후 실증적 접근을 시도해 볼 수 있다.

산업보안 정책의 성과 지표는 우선 기술유출로 인한 업계의 피해 손실 수준인바, 그것은 다음과 같이 나타낼 수 있다.

$$L_t = l_{1t} + l_{2t} + l_{3t} + l_{4t} + l_{5t} + l_{6t} + l_{7t} + \cdots + l_{nt} = \sum_{i=1,\, y=t}^{n} l_{iy} \quad ,$$

또는 $\sum l_{it}$ ---------- (1)

즉, 한 국가의 산업유출 피해로 인한 t기의 전체 손실(L_t)은 국내 개별

산업(i)의 t기 유출 손실(l_{it})의 합($\sum_{i=1, y=t}^{n} l_{iy}$)으로서 산업보안의 정책목표는 이를 최소화하는 것이다.

한편 산업보안에 투입되는 보안비용(C_t)은 t기 각 정책대안(p_{it})의 집행에 소요된 비용의 합, 또는 산업보안에 투입되는 정부의 예산(G_{bt})과 민간기업의 보안지출(F_{et})의 합으로 나타낼 수 있다.

$$C_t = p_t + p_{2t} + p_{3t} + p_{4t} + p_{5t} + p_{6t} + p_{7t} + \cdots + p_{nt} = \sum_{i=1, y=t}^{n} p_{iy} \quad ,$$

$$= \sum p_{it} \qquad \text{---------- (2)}$$

또는 정부와 민간 각 부분의 지출 측면에서

$$C_t = G_{bt} + F_{et} \qquad \text{---------- (3)}$$

산업보안 정책의 성과 지표인 L_t 와 C_t에서 함수

L_t = f(C_t)를 가정하고, 보안비용 C_t의 증가에 따라 유출 손실이 감소한다고 보면, 산업보안 정책의 성과모형 함수식은

$$L_t = \mathrm{f}(C_t), \text{ 단 } \frac{dL}{dC} < 0 \qquad \text{---------- (4)}$$

산업보안의 정책성과 모형에서 제시한 성과지표로 기술유출 손실은 위 성과모형 방정식체계 중 식 (1)에서 추정할 수 있으며, 보안비용은 식 (2) 또는 (3)에서 얻을 수 있다. 손실-비용 매트릭스에서 표현되는 소위 성과 조합의 실측적 위치와 평가는 L_t와 C_t 각각에 대한 산출, 나아가

성과 총량($L_t + C_t$) 및 그 구성에 대한 시간적 또는 지역적 비교분석에 의해 찾아질 수 있다. 아울러 이 수리 성과모형에서는 L_t 값에 의해 정책의 효과성(effectiveness)을 분석해 볼 수 있을 뿐만 아니라, 투입된 C_t과 산출된 L_t간의 비율($\frac{L_t}{C_t}=E_t$)을 통해 일정 시기에서의 산업보안 효율성(efficiency)을 추정해 볼 수도 있다.

Ⅲ. 한국 산업기술의 해외 불법유출 실태

1. 산업기술 해외 불법유출 개관

우리나라 고부가가치 산업기술이 해외로 불법 유출되고 있는 실태는 우선 유관 기관인 국가정보원과 경찰의 사건 정보·수사활동 자료를 통해서 접근해 볼 수 있다. 우선 국가정보원의 산업기밀보호센터 발표에 의할 때, 국내의 첨단기술을 해외로 불법유출하려다 국가정보원 당국에 의해 적발된 건수를 보면 2004년부터 2012년까지 9년간 총 320건으로 연평균 약 36건이 적발된 것으로 나타나고 있다.

국가정보원에 적발되었던 해외 불법 유출 320건의 추이를 연도별로 살펴보면, 2004년 26건에서 시작하여 2005년에 29건, 2006년 31건, 2007년 32건, 2008년 42건, 2009년 43건, 2010년에는 41건으로 일시 감소하였다가, 2011년에는 46건으로 지속적인 증가 추세를 나타냈다. 다만 지난 2012년에 적발 건수가 30건으로 감소하는 모습을 보였다.

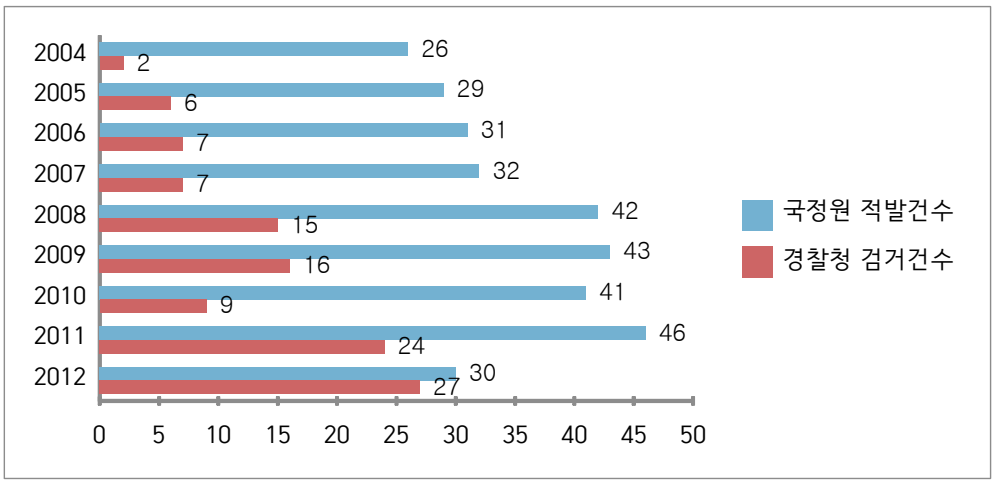
한편 경찰청에 의한 해외 불법유출사범 검거 실적 역시 국가정보원의 불법유출 적발 추이와 유사하게 2004년에 2건, 2005년 6건, 2006년과 2007년 각 7건에서 2008년과 2009년에 각각 15건, 16건으로 증가하고, 2010년에는 9건으로 감소하였으나, 2011년에는 다시 24건으로 증가하였다. 경찰청의 검거 건수는 2012년에는 사상 최고치인 27건에 달하였다(<표 1>).

<표 1> 연도별 산업기술 해외 불법유출 건수(2004-2012)

단위: 건

	2004	2005	2006	2007	2008	2009	2010	2011	2012	총계
국정원 적발	26	29	31	32	42	43	41	46	30	320
경찰청 검거	2	6	7	7	15	16	9	24	27	124

<그림 2> 연도별 산업기술 해외 불법유출 건수(2004-2012)



자료: 국정원 산업기밀보호센터, "기술유출 통계", http://service4.nis.go.kr (2013. 12. 1 검색); 경찰청, "산업기술 유출사범 단속 현황(내부자료)", 2013.

국가정보원의 산업기술 해외 불법유출 대응 활동은 유출 관련 정보의 폭넓은 수집과 사건 발생 후 적발 단계에서 중점을 둔 것으로 위법사실

확인과 형사 처벌 여부에 대한 수사를 위해서는 불법적 사건들은 관련 수사기관에 다시 통보된다. 경찰청의 검거사건수는 법집행에 중점을 둔 사건처리와 통계로 나타난 것이기 때문에 국가정보원의 적발 사건수에 비해 상대적으로 적은 실적으로 나타나고 있다.

중요한 것은 지난 2010년 일시 안정을 보이던 산업기술 해외 불법유출이 2011년 이후 다시 증가세로 돌아섰다는 점이다. 즉 2010년 다소 감소했던 국가정보원 적발건수(41건)은 2011년 46건으로 사상 최대치를 기록했으며, 경찰청에 의한 검거건수 역시 2011년 24건, 2012년 27건에 달함으로써 역대 최고 검거건수를 연속하여 넘어섰다.

국가정보원 2012년 적발건수(30건)의 경우 비록 전년 대비 감소한 양상을 보이고는 있으나 이는 유출범죄 자체의 감소라고 보이지 않는다. 오히려 첨단 대용량 정보저장장비, 차세대 통신매체, 사이버네트워크 활용에 의한 기술침해와 정보이동 등으로 불법유출이 용이한 환경이 조성되고 그에 따라 불법유출이 적발되지 못하였을 뿐, 불법유출이 이루어지고도 수사기관에 미신고되거나 인지되지 못한 사건은 더욱 늘어났을 가능성도 있다.

2. 불법유출의 유형별 분석

1) 유출 분야

국가정보원에 의해 지난 5년간(2008-2012) 적발된 총 202건의 산업기술 유출 사건을 유형별로 살펴보면, 우선 유출 분야에서는 전기전자 분야가 가장 많아 전체 불법유출의 34%를 차지한 것으로 나타났다. 다음으로 기계분야가 31%, 정보통신이 15%로서 이 상위 세 분야를 합한

비중이 80%를 점하여 전체 불법유출의 대종을 차지한 것으로 나타났다. 이밖에도 화학분야가 9%, 생명공학 3%, 기타 8%의 순으로 나타나고 있다.

<그림 3> 산업기술 해외 불법유출 분야별 유형(2008-2012)

자료: 국정원 산업기밀보호센터, "기술유출 통계"(2012).

과거 2000년대까지만 해도 불법유출의 분야별 품목들은, 전기전자 분야가 압도적이었다. 예컨대 <표 1>에서 보는 바와 같이 2004-2009년간 국가정보원에 적발된 총 203건의 불법 유출 사건 가운데에서도 특히 반도체, 휴대폰 등 전기전자 품목이 43.8%(98건), 그리고 정보통신 품목이 14.8%(30건)로서 이 두 분야 유출품목의 대종을 차지하고 그밖에 기계 14.3%(29건), 화학 5.4%(11건), 생명공학 3.9(8건)% 등으로 분포되어 있었으나 최근에는 5년간(2008-2012)은 위에서 본 바와 같이 자동차, 조선을 포함한 기계 분야 유출 비중(31%)이 크게 높아졌고, 화학 분야 유출 비중(9%)도 늘어나는 등 거의 전 분야로 불법유출이 폭넓게 확대되고 있는 추세를 보이고 있다.

국제적 시장 지배력이 높은 우리나라 첨단기술 품목의 해외 불법유출

위험은 경찰청의 검거 사례에서도 잘 나타나고 있다. 예컨대 산업기술 불법유출 급증으로 해외 유출 피해가 약 15조원(경찰청 검거사건 기준)으로 추산되던 2008년 당시 해외 유출 사건(15건)은 전체 국내외 총 검거건수(72건)의 약 1/5에 불과하였지만, 피해추산 1조원 이상의 사건이 빈발하여 시장 가치가 높은 첨단기술들이 해외유출을 겨냥한 범죄자들의 집중적인 유출목표가 되어 왔음을 보여주고 있다. 즉 고부가가치 첨단기술의 해외 유출 위험이 높다는 것은 2008년 검거되었던 고화질 HD영상 수신기 제조 핵심기술 중국유출 미수사건(피해예방액, 1조 6천억원), Dental Implagraphy(첨단 의료기기) 설계도의 미국계 회사 유출사건(피해추산, 2조 2천억원), PTMEG(첨단섬유 원료) 생산기술 중국유출 미수사건(피해예방액, 1조 2천억원) 등의 검거 사례에서 뚜렷이 나타나고 있다.[7)]

2) 유출 주체

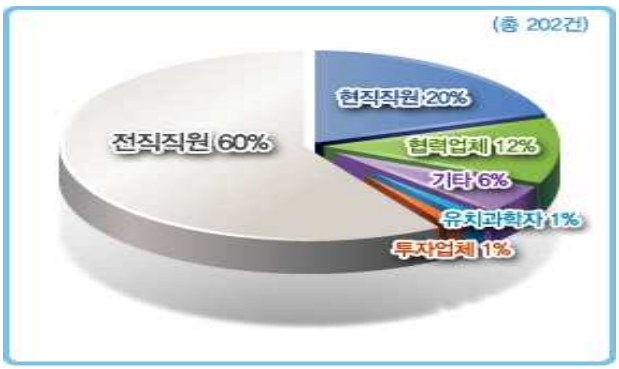
유출 유형을 유출 주체별로 살펴보면 <그림 4>에서 보는 바와 같이, 전직 직원 60%, 현직 직원 15%, 협력업체 12%, 유치과학자 1%, 투자업체 1%, 기타 6%의 순으로 나타나고 있다. 유출 주체 면에서 볼 때, 주로 전·현직 직원(75%)에 의한 기술유출, 특히 전직 직원에 의한 유출이 가장 많은 부분을 차지하고 있다는 특징을 보인다.

과거 2004-2009년간 국가정보원에 적발된 불법유출 사건(총 203건)을 보면 전직 직원 56.2%(114건)과 현직 직원 24.6%(50건)로 전·현직 직원에 의한 비중이 80.8%로 최근보다도 더욱 높았으며, 특히 당시에는 최근에 비해 전직 직원 보다 현직 직원에 의한 불법유출 비중이 높았던 것으로 나타났다.

---

7) 치안정책연구소, 치안전망, 2013, p. 108.

<그림 4> 산업기술 해외 불법유출 주체별 유형(2008-2012)



자료: 국정원 산업기밀보호센터, "기술유출 통계"(2012).

이는 최근까지도 전·현직 직원 등 내부자에 의한 기술유출이 여전히 압도적인 비중을 차지하고 있음은 분명하나, 과거에 비해 상대적으로 현직 직원에 의한 내부 통제는 개선되고 있음을 보여준다.

이밖에도 기술유출의 주체로는 협력업체와 과학자, 투자업체 등 이해관계자들에 의한 기술유출 사례도 여전히 상존하고 있음을 주목할 필요가 있다.

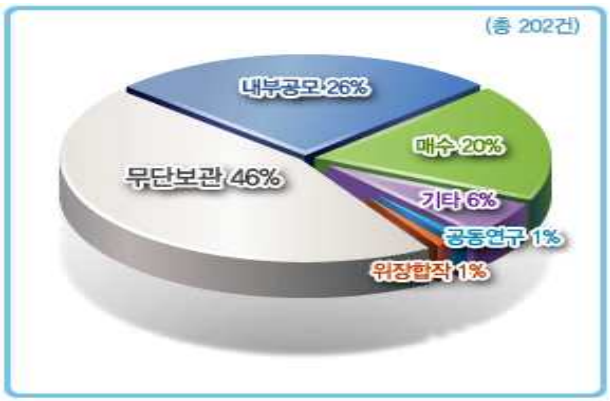
3) 유출 수법

유출유형을 수법별로 살펴보면, 무단보관 46%, 내부공모 26%, 매수 20%, 공동연구 1%, 위장합작 1%, 기타 6% 등의 순으로 나타나고 있다.

이에 비해 과거 2004-2009년간 국가정보원에 적발된 불법유출 사건(총 203건)의 수법은 무단보관 22.7%(46건), 내부공모 12.8%(26건), 매

수 52.2%(105건), 공동연구 4.4%(9건), 위장합작 3.0%(6건), 기타 5.4%(11건) 등의 순이었다.

<그림 5> 산업기술 해외 불법유출 수법별 유형(2008-2012)



자료: 국정원 산업기밀보호센터, "기술유출 통계"(2012).

따라서 과거에는 연구원 등 개인을 대상으로 금전적 유혹을 유발시키는 매수 형태가 일반적이었으나, 최근에는 무단보관 형태에 의한 것이 가장 많고, 내부공모에 의한 수법도 늘어나고 있는 특징을 보이고 있다.

.

4) 유출 동기

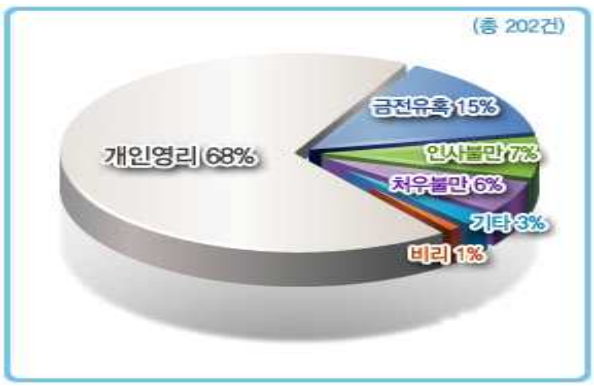
유출 동기별로 살펴보면, 개인영리 68%, 금전유혹 15%, 인사불만 7%, 처우불만 6%, 비리 1%, 기타 3% 등의 순으로 나타나고 있다. 유출 동기에서는 무엇보다도 개인영리와 금전유혹 등 경제적 동기에 의한 유출이 가장 많은 83%를 차지하고 있다.

과거 2004-2009년간의 불법유출 사건(총 203건)의 유출 동기를 보면

개인영리 47.8%(97건), 금전유혹 31.0%(63건), 인사불만 5.9%(12건), 처우불만 8.4%(17건), 비리 2.0%(4건), 기타 4.9%(10건) 등의 순이었다. 이 당시에도 개인영리와 금전유혹 등 경제적 동기에 의한 유출이 가장 많은 78%를 차지한 것으로 나타났다.

그러나 최근에는 단순한 금전유혹에 의한 유출 동기는 절반이상 감소(31.0% -> 15%)한 반면, 개인영리를 목적으로 한 유출 동기가 과거 비해 더욱 높아짐으로서(47.8% -> 68%), 이해관계자 특히 내부 직원에 대한 경제적 보상뿐만 아니라, 첨단기술 자체의 기술가치 보호 및 인적 보안에 더욱 관심을 기울여야 함을 보여주고 있다.

<그림 6> 산업기술 해외 불법유출 동기별 유형(2008-2012)



자료: 국정원 산업기밀보호센터, “기술유출 통계”(2012).

5) 유출 피해기업

피해기업 규모별로 기술유출 사례를 보면, 중소기업이 71%, 대기업이 24%, 기타 5%로 나타나 중소기업이 산업기술 해외 유출피해에 상대적으로 취약한 상태에 있음을 알 수 있다.

<그림 6> 해외 불법유출 피해기업의 규모별 유형(2008-2012)

자료: 국정원 산업기밀보호센터, “기술유출 통계”(2012).

6) 유출 상대국

국가정보원의 지난 5년간(2008-2012) 적발 자료에는 불법유출된 기술의 상대국에 대한 통계가 없으며, 또한 국가정보원은 이와 별도로 해외로 불법유출된 기술의 지역별 국가별 분포 등에 대한 정보자료를 공개하고 있지도 않다. 따라서 해외 불법유출 상대국에 대한 통계는 경찰청의 2011년 검거자료를 이용하기로 한다.

경찰청의 2011년도 해외 불법유출 검거 사건 수는 <표 1>에서 보는 바와 같이 총 24건이었다. 경찰청의 공개 자료에 따르면 2011년 해외유출 검거건수 24건 가운데 중국이 14건으로 가장 많았고, 그 외 대만, 일본, 미국, 독일, 스페인, 영국 등 다양하게 나타나고 있다.[8)]

이러한 대상국 수의 확대에 비추어 보면 국내 경제발전과 산업기술의 발달로 인해 불법유출이 과거처럼 단순히 일본, 대만, 태국 등 아시아권

8) 경찰청, “보도자료: 국제범죄수사대, 산업기술유출수사의 첨병으로 거듭나”, 2012. 2. 16.

국가뿐만 아니라 서구 선진국 등으로 다양화 되고 있는 추세에 있음은 분명하다. 그러나 중요한 것은 불법유출이 중국에 집중되는 양상(58.3%)이 여전히 계속되고 있다는 점이다.

국내 보도에서도, 국가정보원의 기술유출 적발사건의 50% 이상은 중국으로의 기술유출인 것으로 알려지고 있다. 즉 국가정보원 산업기밀보호센터에 따르면 지난 2005년부터 2011년까지 국내 첨단 기술을 해외로 불법유출했거나 유출을 시도하다가 적발된 사건은 총 264건이었으며, 그 중 130건 이상은 중국으로의 유출이었다고 한다.[9)]

중국으로의 기술유출은 2012년 능동형유기발광다이오드(AMOLED) 기술 유출, 2011년 특수선박기술 유출, 2010년 3차원(3D)기술 유출 사례 등에서 보듯이, 반도체, 조선, 디스플레이 등 첨단 산업분야가 모두 포함돼 있어 한국 경제의 산업경쟁력에 치명적인 피해를 주고 있다.

이 같은 국내로부터의 해외로의 유출뿐만이 아니라 중국에 진출한 기업이 중국 현지 자체에서 기술유출 위험에 노출되어 있는 것도 큰 도전과제이다. 특히 보안이 취약한 중소기업인 경우에는 매우 큰 문제이다.

최근 2012년 조사에서도 중국에 진출한 중소기업 중 약 절반에 가까운 중소기업들이 유출피해를 경험한 것으로 드러났다. 즉 중소기업청의 '중소기업 기술보호 역량 및 수준조사 결과 보고서'에 따르면 중국에 진출한 중소·벤처기업 138개사 중 44.2%에 해당하는 61개사가 산업기술 유출로 인한 피해를 입은 것으로 나타났다.[10)]

---

9) 『파이낸셜뉴스』, "한중 동반성장의 그늘 '기술 유출'", 2012. 8. 23; <표 1>의 국정원 공식발표자료에서도 2005-2011년간 총 적발사건은 264건으로 나타나고 있으므로, 위 중국 관련 통계수치는 국정원의 직접 발표치는 아니지만 보도내용의 신뢰성이 있다.

10) 『한국경제』, "中 진출 중기 '산업 스파이 심각'", 2012. 7. 18.

Ⅳ. 불법유출 대책: 미국의 산업보안 정책과 함의

1. 미국의 산업보안 정책 동향

1) 국가방첩전략과 산업보안 정책

미국은 부시(G. W. Bush) 대통령 당시 2002년 제정된 이른바 방첩강화법(The Counterintelligence Enforcement Act of 2002, 50 USC 401)에 의거하여, 2005년부터 국가방첩관실(ONCIX, Office of the National Counterintelligence Executive)를 통해 국가방첩전략(National Counterintelligence Strategy)을 입안하고 이를 시행해 오고 있다.[11]

국가방첩전략은 미국 국가안보전략에 맞추어 입안되었던 바, 그 의의는 국가의 방첩전략이 어떠한 방향으로 가야하는가에 대한 비전을 제시했으며, 방첩활동에 대한 국가의 임무를 처음으로 천명했고, 나아가 방첩의 기능이 미국 국가안보전략을 지원하는 것임을 확인함으로써 미국 방첩활동의 전환점이 되었다는 것에서 찾아 볼 수 있다.[12]

국가방첩전략은 그 실효적 집행을 위한 국가방첩체계의 구축(national counterintelligence system building)을 강조하고 있다. 이는 과거 미국

11) 미국 국가방첩전략 부분은 다음의 선행연구를 주로 이용하였다. 정웅. “해외 주요 국가들의 경제방첩 정책과 우리의 정책과제”. 국가정보연구, 제5권 2호, 2012, pp. 143-147.
12) 김왕식, “정보환경의 변화와 방첩제도의 개선방향”, 국가정보연구, 제5권 1호, 2012, p. 52.

의 방첩역량이 분절된 방첩제도에 맞추어 진화되어 왔고 또한 최근까지 방첩활동이 통일된 리더십을 갖추지 못한 수준에 머무름으로써, 결국 방첩공동체 조직은 파편화되어 그 활동 방향이 너무나 "전술적으로(tactically)" 경도되었다는 자성에서 출발한다. 따라서 국가방첩전략이 보다 효과적으로 되기 위해서는, 정부라는 보다 큰 구조 틀(government structures) 속에서 비용분석에 입각한 사업적 모델(business models) 방향으로 변모되어야 한다고 지적한다.

국가방첩전략의 목표와 임무 내용, 이를 달성하기 위한 국가방첩체계 등을 볼 때, 미국이 추구하는 전략적 방첩의 핵심은 한마디로 국익 확보를 위한 적극적 견지에서의 효과성 및 효율성에 대한 강조라고 요약할 수 있다. 즉 외부 위협에 대한 공세적 방첩활동의 기조, 국가안보전략을 지원하고 국가안보 및 국가이익을 달성하는 효과적 수단으로서의 방첩, 그리고 비용을 감안한 효율적 국가방첩체계 구축 등에서 그 성격이 잘 드러나고 있다.[13]

산업기술의 해외 불법유출에 대응하는 산업보안 분야도 이러한 전략적 방첩 목표의 하나로 제시되고 있다. 즉 국가방첩전략의 목표 중에는 미국의 핵심 국가기밀, 자산, 기술에 대한 보호 등 산업보안이 명백히 포함되어 있다. 또 국가방첩전략에는 광범위한 방첩수단들이 "전략적으로(strategically)"동원·배치되어야 한다고 보고 있는바, 산업보안 역시 국가안보와 국가이익을 겨냥한 국가방첩전략의 틀 속에서, 사전적인(proactive) 방첩전략으로의 전환, 민감 기술(sensitive technologies)의 보호와 공정경쟁 환경 확보(a level economic playing field), 국가안보 리더그룹을 위한 산업보안 정보의 제공 등의 활동이 이루어질 것으로 보

13) 2005년 국가방첩전략은 2007년에 전자적 침투(electronic penetration)의 위협과 사이버 대응역량 강화 등의 내용이 보완되었고, 2009년에 NIS(National Intelligence Strategy) 내 최초로 방첩의 임무목표가 포함되었음을 밝히는 내용 등이 추가되었으나, 전략적 방첩의 기본 틀에는 큰 변화가 없다. ONCIX, *The National Counterintelligence Strategy of the United States of America* (2007-2009).

인다.

또 산업보안에서의 효율성 추구는 국가방첩체계가 구축하고자 하는 안보피해손실에 대한 평가 절차, 방첩에 소요되는 자원 및 방첩성과에 대한 측정 등을 통해 이미 잘 드러나 있다.

이러한 전략적 성격의 산업보안은 2005년의 국가방첩전략에서 뿐만 아니라, 2007년에 보완된 국가방첩전략에서도 뚜렷이 나타나고 있다. 특히 2007년 국가방첩전략은 '미국의 경제적 우위, 영업비밀, 산업지식 보호(Protect US economic advantage, trade secret and knowhow)'의 제하로 산업보안을 위한 전략을 제시하면서 향후 미국의 핵심 국가자산에 대한 공격이 지적재산에 대한 절취, 금융·물류 혼란(financial or logistical chaos)을 겨냥한 정보의 조작 등으로 나타날 가능성이 있음을 지적하고, 누가 이러한 공격을 계획·수행하며 누가 그 공격을 와해시키고 나아가 미국에 유리하게 활용할 능력이 있는지를 파악하는 데 산업보안이 중요한 역할을 갖는다고 강조한다.[14] 이러한 전략적 산업보안에 대한 자세는 최근 2008년과 2009년까지 발표한 국가방첩전략에서도 변함없이 견지되고 있다.[15]

2) 오바마 행정부의 산업보안 정책

(1) 해외 불법유출 방지전략의 개요

미국 오바마 행정부(Obama Administration)는 미국 주요 기업들 상대

14) ONCIX, "PROTECT US ECONOMIC ADVANTAGE, TRADE SECRETS AND KNOW HOW", *The National Counterintelligence Strategy of the United States of America*(March, 2007). pp. 4-5.

15) ONCIX, *The National Counterintelligence Strategy of the United States of Americ*(2008), p. 5; ONCIX, *The National Counterintelligence Strategy of the United States of America*(2009), p. 5.

로 하여 지속적으로 전개되고 있는 산업기술 불법유출 행위에 대한 범정부적 대책으로 2013년 2월 20일 이른바 '영업비밀 침해 방지를 위한 행정부 전략(ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS)'제하의 산업기술 침해 방지전략을 발표하였다.

이 전략안은 미 상무부와 국방부뿐만 아니라 국토안보부, 법무부, 국무부, 재무부, ODNC, 무역대표부(the Departments of Commerce, Defense, Homeland Security, Justice, State, Treasury, the Office of the Director of National Intelligence and the Office of the United States Trade Representative)까지 입안에 참여한 산업기술 불법유출 대책안이다.

미 상무부를 비롯하여 무려 8개 국가기관이 참여한 범정부적 산업기술 침해 방지대책에는 그 전략적 행동항목(Strategy Action Items)으로 모두 5가지의 과제를 제시하고 있다. 즉 그 전략적 행동항목으로서

첫째, 기밀 절취에 대한 압력과 통상 규제 등 외교적 노력(Diplomatic Efforts to Protect Trade Secrets),

둘째, 기업의 자발적 산업기밀 보호 활동에 대한 지원(Voluntary Best Practices by Private Industry),

셋째, 법무부와 FBI의 법집행활동 강화(Domestic Law Enforcement Operations),

넷째, 기밀 절취 행위에 대한 형량 강화 등 입법론적 개선(Domestic Legislation),

다섯째, 기밀 절취 위험과 방지에 대한 교육·홍보 및 이해당사자들의 참여(Public Awareness and Stakeholder Outreach) 등의 실행 과제를 세부적으로 명시하고 있다.[16)]

에릭 홀더(E. Holder) 미 법무장관은 이 전략안 발표에서 “신기술의 발달로 글로벌 거래에서의 전통적 보호벽이 뚫리고 범죄자들이 세계 어느 곳으로부터도 산업기밀을 손쉽게 훔칠 수 있게 되었다”고 언급하고, 미국 경제와 국가안보에 심각한 위협을 주고 있는 산업기술 침해에 대한 방지가 오바마 행정부의 최우선 정책과제(top priority for President Obama, for the entire Administration) 임을 천명하면서, 미 산업기술의 해외 불법유출 방지 정책에 대한 정부의 강한 실천 의지를 보여주었다.[17]

(2) 최근 산업기술 불법유출 사건과 오바마 정부의 인식

2013년 2월에 발표한 오바마 행정부의 산업기술 침해방지 전략안에는 2009년 1월부터 2013년 1월까지 최근 3년간 미 법무부가 처리한 주요 경제스파이 및 영업비밀 절취사건이 공표되어 있다.[18] 여기서 공표된 20건의 사건들을 최근 일자 순으로 개관해 보면 다음과 같다.

(1) 2012년 11월 기소된, General Motors 중국인 엔지니어의 자동차 하이브리드기술 불법유출 사건

■ ***Trade Secrets to China*** – On Nov. 30, 2012, a former General Motors engineer and her husband were convicted by a federal jury today in Detroit for conspiring to steal hybrid technology trade secrets from GM with the intent to

16) Executive Office of the President of the United States, *ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS,* 2013, p. 3-12.

17) U.S. Department of Justice, “Attorney General Eric Holder Speaks at the Administration Trade Secret Strategy Rollout”, http://www.justice.gov/iso/opa/ag/speeches/2013/ag-speech-1302201.html(2013. 12. 1 검색).

18) Executive Office of the President of the United States, “Annex B: Summary of Department of Justice Trade Secret Theft Cases”. *ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS,* 2013.

use them in a joint venture with an automotive competitor in China. Shanshan Du and her husband, Yu Qin were convicted of unlawful possession of trade secrets.

(2) 2012년 10월 기소된, 한국 코오롱 인더스트리의 DuPont社 아라미드 섬유 관련 영업비밀침해 사건

■ *Trade Secrets to South Korea* – On Oct. 18, 2012, South Korea-based Kolon Industries Inc. and several of its executives and employees were indicted in the Eastern District of Virginia for allegedly engaging in a multi-year campaign to steal trade secrets related to DuPont's Kevlar para-aramid fiber and Teijin Limited's Twaron para-aramid fiber.

(3) 2012년 9월 기소된, 중국인 전기엔지니어의 군사기술 및 영업비밀 중국 불법유출 사건

■ *Military Technical Data and Trade Secrets to China* – On Sept. 26, 2012, Sixing Liu, aka "Steve Liu,"a native of China with a PhD in electrical engineering who worked as a senior staff engineer for Space & Navigation, a New Jersey-based division of L-3 Communications, was convicted in the District of New Jersey of exporting sensitive U.S. military technology to China, stealing trade secrets and lying to federal agents.

(4) 2012년 9월 기소된, CME Group 전직 중국인 소프트웨어 엔지니어의 영업비밀 중국 불법유출 사건

■ *Theft of Trade Secrets for Potential Use in China* – On Sept. 19, 2012, Chunlai Yang, a former senior software engineer for Chicago-based CME Group, Inc., pleaded guilty in the Northern District of Illinois to two counts of theft of trade secrets for stealing source code and other proprietary information while at the same time pursuing plans to improve an electronic trading exchange in China.

(5) 2012년 9월 절취영업비밀 구매 혐의로 조사 중인 Pittsburgh Corning社 영업비밀 불법유출 사건

■ ***Trade Secrets to China*** – On Sept. 4, 2012, Chinese citizens Ji Li Huang and Xiao Guang Qi were charged in a criminal complaint in the Western District of Missouri with attempting to purchase stolen trade secrets stolen from Pittsburgh Corning for the purpose of opening a plant in China to compete with Pittsburgh Corning.

(6) 2012년 9월 유죄 선고(징역 4년)된, Motorola社 iDEN 통신기술의 중국 불법유출 사건

■ ***Motorola Trade Secrets to China*** – On Aug. 29, 2012, Hanjuan Jin, a former software engineer for Motorola, was sentenced in the Northern District of Illinois to four years in prison for stealing trade secrets from Motorola, specifically Motorola's proprietary iDEN telecommunications technology, for herself and for Sun Kaisens, a company that developed products for the Chinese military.

(7) 2012년 5월 기소된, Orbit Irrigation Products社 영업비밀 중국 불법유출 사건

■ ***Trade Secrets to Competitors in China*** – On May 7, 2012, an indictment returned in the District of Utah in April 2012 was unsealed charging two people and two companies with theft of trade secrets, wire fraud, and conspiracy to commit wire fraud in connection with the alleged theft of trade secrets from Orbit Irrigation Products, an irrigation company headquartered in Utah.

(8) 2012년 4월 기소된, 중국인 전기엔지니어의 군사기술 및 영업비밀 중국 불법유출 사건

■ *Military Technical Data and Trade Secrets to China* – On April 5, 2012, a second superseding indictment was returned in the District of New Jersey against Sixing Liu, aka "Steve Liu," a native of China with a PhD in electrical engineering who worked as a senior staff engineer for Space & Navigation, a New Jersey-based division of L-3 Communications, from March 2009 through Nov. 2010.

(9) 2012년 3월 기소된, DuPont社 전직 중국인 과학자의 titanium dioxide 제조기술 중국 불법유출 사건

■ *DuPont Trade Secrets to China* – On March 2, 2012, former DuPont scientist Tze Chao pleaded guilty in the Northern District of California to conspiracy to commit economic espionage, admitting that he provided trade secrets concerning DuPont's proprietary titanium dioxide manufacturing process to companies he knew were controlled by the government of the People's Republic of China (PRC).

(10) 2012년 1월 기소된, Sanofi-Aventis社 전직 중국인 화학자의 (미국내) 중국 자회사 영업비밀 불법유출 사건

■ *Trade Secrets to U.S. Subsidiary of Chinese Company* – On Jan. 17, 2012, Yuan Li, a former research chemist with the global pharmaceutical company Sanofi-Aventis, pleaded guilty in the District of New Jersey to stealing Sanofi's trade secrets and making them available for sale through Abby Pharmatech, Inc., the U.S. subsidiary of a Chinese chemicals company.

(11) 2012년 1월 유죄 선고(징역 60월, 벌금 2,5000달러)된, Dow Chemical社 전직 중국인 연구원의 탄성 중합체 chlorinated polyethylene (CPE) 관련 영업비밀침해 사건

■ *Dow Trade Secrets to China* – On Jan. 12, 2012, Wen Chyu Liu, aka David W. Liou, a former research scientist at Dow Chemical Company in Louisiana, was sentenced in the Middle District of Louisiana to 60 months in prison, two years supervised release, a $25,000 fine and was ordered to forfeit $600,000.

(12) 2011년 12월 유죄 선고(징역 87월)된, 중국인의 Dow and Cargill社 영업비밀 불법유출 사건

■ *Dow and Cargill Trade Secrets to China* – On Dec. 21, 2011, Kexue Huang, a Chinese national and former resident of Indiana, was sentenced to 87 months in and three years supervised release on charges of economic espionage to benefit a foreign university tied to the People's Republic of China (PRC) and theft of trade secrets.

(13) 2011년 11월 체포되어 조사 중인, 인도인의 영업비밀 절도 사건

■ *Trade Secrets to India* – On Nov. 14, 2011, Prabhu Mohapatra was arrested on a criminal complaint in the District of Utah (filed on Nov. 10, 2011) charging him with stealing proprietary information from his employer, a Utah scientific company, and providing it to a relative in India who was starting up a competing company.

(14) 2011년 8월 유죄 선고된, 외국정부(이스라엘)로의 영업비밀 불법유출 사건

■ *Trade Secrets to Foreign Government* – On Aug. 30, 2011, Elliot Doxer, of Brookline, Mass., pleaded guilty in the District of Massachusetts to one count of foreign economic espionage for providing trade secrets over an 18-month period to an undercover FBI agent posing as an Israeli intelligence officer.

(15) 2011년 4월 기소된, 중국인의 영업비밀 절도 및 통신사기 사건

■ *Wire Fraud in Trade Secrets Case Involving China* – On April 6, 2011, Yan Zhu, a Chinese citizen in the U.S. on a work visa, was convicted in the District of New Jersey on seven counts of wire fraud in connection with his scheme to steal confidential and proprietary business information relating to computer systems and software with environmental applications from his New Jersey employer.

(16) 2010년 12월 유죄 선고(징역 15월), Valspar社 전직 중국인 화학자의 영업비밀 절도 사건

■ *Valspar Trade Secrets to China* – On Dec. 8, 2010, David Yen Lee, a former chemist for Valspar Corporation, a Chicago paint manufacturing company, was sentenced in the Northern District of Illinois to 15 months in prison for stealing trade secrets involving numerous formulas and other proprietary information valued up to $20 million as he prepared to go to work for a competitor in China.

(17) 2010년 11월 유죄 선고된, Ford社 자동차 디자인 등 영업비밀의 중국 불법유출 사건

■ *Ford Motor Company Trade Secrets to China* – On Nov. 17, 2010, Yu Xiang Dong, aka Mike Yu, a product engineer with Ford Motor Company pleaded guilty in the Eastern District of Michigan to two counts of theft of trade secrets. According to the plea agreement, Yu was a Product Engineer for Ford from 1997 to 2007 and had access to Ford trade secrets, including Ford design documents.

(18) 2010년 10월 유죄 선고(14월)된, DuPont社 영업비밀의 중국 불법유출 사건

■ *DuPont Trade Secrets to China* – On Oct. 26, 2010, Hong Meng, a former research chemist for DuPont, was sentenced in the District of Delaware to 14 months in prison and $58,621 in restitution for theft of trade secrets.

(19) 2010년 7월 기소된,GM社 하이브리드 차량 기술의 중국 불법유출 사건

■ *GM Trade Secrets to China* – On July 22, 2010, an indictment returned in the Eastern District of Michigan charging Yu Qin and his wife Shanshan Du, both of Troy, Michigan, was unsealed. The indictment charged the defendants with conspiracy to possess trade secrets without authorization, unauthorized possession of trade secrets and wire fraud.

(20) 2010년 2월 유죄 선고(징역 188월)된, 중국 스파이의 Boeing社 우주선 및 로켓기술 불법유출 사건

■ *Economic Espionage / Theft of Space Shuttle and Rocket Secrets for China* – On Feb. 11, 2010 former Rockwell and Boeing engineer Dongfan "Greg" Chung was sentenced to 188 months imprisonment and three years supervised release after his July 16, 2009 conviction in the Central District of California.

위에서 나타난 미국 내 산업기술의 해외 불법유출 사건들을 정리해 보면, 아래 <표 2>에서 보는 바와 같이 주요 피해기업은 제너럴 모터스(GM), 포드(Ford), 듀폰(DuPont), 다우 케미컬(Dow Chemical), 모토롤라(Motorola), 보잉(Boeing) 등 미국의 첨단기술 보유기업으로 나타나고 있다.

특히 주목할 것은 공표된 사건 중 유출 국가에 이스라엘, 인도, 한국 등도 포함되어 있기는 하나, 총 20건의 85% 달하는 17건의 사건이 중국기업과 중국인에 의한 산업기술과 영업비밀 절취사건이었다는 점이다.

<표 2> 최근 미국의 산업기술 해외 불법유출 사건(2009. 1 ~ 2013. 1)

	사건처리 시기	유출 국가	유출 기술	피해기업
1	2012.11월 기소	중국	자동차 하이브리드기술	General Motors社
2	2012. 10월 기소	한국	아라미드 섬유	DuPont社
3	2012.9월 기소	중국	미사일, 무인항공기 등 군사기술	L-3 Communications社
4	2012.9월 기소	중국	전자거래 소프트웨어	CME Group社
5	2012.9월 조사중	중국	발포유리단열재(cellular glass insulation) 영업비밀	Pittsburgh Corning社
6	2012. 9월 유죄 선고	중국	iDEN 통신기술	Motorola社
7	2012.5월 기소	중국	灌溉 회사의 판매&가격 영업비밀	Orbit Irrigation Products社
8	2012.4월 기소	중국	수출통제 군사기술 & 데이터	L-3 Communications社
9	2012.3월	중국	titanium dioxide 제조기술	DuPont社
10	2012.1월 기소	중국	의약품 정보	Sanofi-Aventis社
11	2012.1월 유죄 선고	중국	탄성 중합체 chlorinated polyethylene 영업비밀	Dow Chemical社
12	2011.12월 유죄 선고	중국	신제품(식품)제조기술 등 영업비밀	Dow and Cargill社
13	2011.11월 조사 중	인도	신약 & 태양전지 用 다이파이로메테인(dipyrromethane) 정보	Frontier Scientific社
14	2011.4월 기소	이스라엘	회사 고객 & 직원 정보	Akamai Technologies社
15	2011.4월 기소	중국	환경 관련 소프트웨어 등 영업 정보	New Jersey employer(미상)
16	2010.12월 유죄 선고	중국	페인트 & 코팅 기술	Valspar社
17	2010.11월 유죄 선고	중국	자동차 디자인 등 영업비밀	Ford社
18	2010.10월 유죄 선고	중국	Organic Light Emitting Diodes (OLED) 기술	DuPont社
19	2010.7월 기소	중국	하이브리드 차량 기술	GM社
20	2010.2월 유죄 선고	중국	우주선 및 로켓기술	Boeing社

자료: Executive Office of the President of the United States, “Annex B: Summary of Department of Justice Trade Secret Theft Cases”. ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS, 2013.

산업기술 침해방지 전략안에서 미국은 중국을 소위 산업스파이·해킹 국가로 특정하지는 않았지만 전략안 발표 직전인 2월 18일 미국의 컴퓨터 보안 회사 맨디언트(Mandiant)가 중국 인민해방군(PLA, People's Liberation Army) 61398 부대 등을 최근 미국에서 발생한 해킹사건의 배후로 지목한 발표가 있었다. 또 전략안 발표에 즈음해서 CIA 마이클 헤이든(M. Hayden) 국장이 “우리는 국가가 사기업을 상대로 해킹하는 초유의 상황에 있다”는 언급이 있었다.[19] 따라서 이 전략안은 애플 등 미국 내 기업에 대한 중국의 해킹 징후, 그리고 해킹의 근원지로서 PLA 61398부대를 지적하는 맨디언트의 발표를 접한 미국 오바마 행정부의 강한 對中國 위기감과 대응의식을 잘 드러낸 것으로 보인다.

이는 현 단계에서 미국이 단순히 개인과 기업 수준이 아니라 국가적 차원으로부터의 위협을 받는 상황에 있다고 평가하고 있으며, 특히 중국을 미국의 경제와 안보를 위협하는 중대한 산업기술 불법유출·해킹 국가로 주목하고 있다는 것을 여실히 보여준다.

2. 미국 산업보안 정책의 함의

미국은 자국의 핵심 국가기밀, 자산, 산업기술의 보호를 위해 이른바 국가방첩전략의 큰 틀 아래서 전략적 산업보안 정책을 추진하고 있으며, 이러한 정책 기조는 최근 오바마 행정부에서 소위 산업기술 침해방지 전략(2013)으로 더욱 강화되고 있다.

한편 Ⅱ장에서 제기했던 바, 公共性을 갖는 산업보안의 주요 정책 목표는 산업기술 불법유출 위험의 최소화와 이를 구현해내기 위한 보안 비

19) 『뉴스1』, “美백악관, 해킹·산업스파이 대책 발표”, 2013. 2. 21.

용의 최소화를 달성하는 것이라고 할 수 있으며, 이러한 산업보안의 정책목표는 미국의 전략적 산업보안이라는 정책에서도 찾아 볼 수 있다.

따라서 미 행정부의 정책 사례를 원용하여 그로부터의 함의를 모색해 본다면 첫째로 우리의 산업보안 역시 소위 “전략적 산업보안”이라는 정책 구상으로 보다 구체화되어야 한다는 것이다.

즉 전략적 산업보안이란 산업기술 해외 불법유출 위험의 최소화가 국내 기업뿐만 아니라 국가경제적 이익을 효과적으로 달성하는 수단임을 명백히 선언하는 한편, 더 나아가서 보안비용 투입-보안성과 산출 분석 등 산업보안의 비용-성과를 감안한 범기관적, 범사회적 차원의 효율적 산업보안체계를 구축하는 것이다.

위와 같은 전략적 산업보안을 산업기술 해외 불법유출 위험의 최소화와 산업보안 비용의 최소화라는 정책목표 관점에서 다시 정리해 보면, 전략적 산업보안이란 공정한 시장경쟁질서 및 국가이익을 겨냥하면서, 광범위한 국내 산업보안자원을 산업보안체계((industrial security system) 내에 전략적으로 배치하고, 그 운용을 위험관리와 비용분석에 기초하여 효율적으로 전개하는 것이다.

미국 산업보안 정책이 우리의 산업기술 불법유출 대책에 주는 또 하나의 함의는, 전세계적 규모로 전개되는 자국 기술의 해외 유출 특히 중국의 산업기술 침해 활동에 대한 진지한 인식과 침해 문제 해결을 위한 적극적이며 실천적인 대응이다.

현재 미국은 산업기술 침해 활동이 단순히 사적 개인과 기업 수준이 아니라 국가적 차원으로부터 위협(중국 정부의 직접적인 침해 또는 정부 지원에 의한 간접적 침해)을 받는 상황에 있다고 평가하고 있다. 미국은 특히 중국을 미국 경제와 안보를 위협하는 중대한 산업기술 침해 국가로서 지목하고 이에 적극적으로 대응하고 있다.

우리나라의 경우 경찰청의 해외 불법유출 검거사건에 대한 지역별 분포를 보면 중국, 미국, 독일, 스페인, 영국, 대만, 일본 등으로 나타나(2011년 24건 기준), 과거 유출 상대국이 중국과 대만, 태국, 일본 등 아시아권 특정 국가에 한정되었던 것과 달리 미국과 유럽 등 서구권으로도 다양해지는 추세를 보이고 있다.

한국은 현재 국내총생산에 대비한 무역의존도(수출입총액/GDP 기준)가 90%를 훨씬 상회하는 시장개방 국가로서[20] 교역규모에서 세계 10대 교역국의 하나이다. 향후에도 FTA 추진 등 경제개방을 통해 세계 각국과의 경제관계를 넓히고 교역이 더욱 활발해질 것으로 보인다.[21] 따라서 경제관계 확대와 교역량 증가에 수반하여 아시아 지역뿐만 아니라 전세계적 차원에서 해외 불법유출이 확산될 위험이 커질 것으로 전망된다.

이러한 해외 불법유출 상대국의 확산 속에 우리나라도 중국의 산업기술 침해 활동을 주시해야 할 것으로 보인다. 예컨대 상기 경찰청의 2011년 해외 불법유출 검거건수(24건)의 사례를 보면 중국이 14건으로 가장 많은 비중으로 나타나고 있는 것이다.[22] 즉 국내 기업의 고부가가치 기술 개발로 인해 아시아권 국가뿐만 아니라 서구 선진국 등으로 불법유출 국가가 다양화 되고 있는 추세에 있음은 분명하지만, 유출 지역이 중국에 집중되고 있는 양상(58.3%)도 여전히 계속되고 있다.

앞선 Ⅲ장에서 살펴 본 국가정보원 적발 해외 불법유출 실태에서도 적발 사건의 50% 이상은 중국으로의 기술유출인 것으로 나타나고 있다. 즉 국정원에 따르면 2005-2011년까지 국내 첨단 기술을 해외로 불법유

20) 우리나라의 GPP 대비 무역의존도는 2011년에 약 97%, 2012년에 95% 수준에 달하고 있다. 통계청, “국가통계포털”, http://kosis.kr (2013. 12. 1 검색)

21) 우리 정부는 2000년대를 통해 전세계 지역을 대상으로 동시다발적인 FTA 확대 전략을 추진하여 2013년 12월 현재 한-칠레 FTA(2014), 한-싱가포르 FTA(2006), 한-EFTA FTA(2006), 한-ASEAN FTA(2009), 한-인도 CEPA(2010), 한-EU FTA (2011), 한-페루 FTA(2011), 한-미 FTA (2012), 한-터키 FTA (2013) 등 9개 자유무역협정이 발효된 상태이다. 산업통상자원부, “FTA 종합지원포털”, http://www.ftahub.go.kr (2013. 12. 1 검색)

22) 경찰청, “보도자료: 국제범죄수사대, 산업기술유출수사의 첨병으로 거듭나”, 2012. 2. 16.

출했거나 유출을 시도하다가 적발된 사건은 총 264건이며, 그 중 130건 이상은 중국으로의 유출이었다.[23]

중국으로의 기술유출은 2012년 능동형 유기발광다이오드(AMOLED) 기술 유출 등에서 보듯이[24] 우리나라의 첨단 산업분야가 대부분 포함돼 있어 한국 경제의 산업경쟁력에 막대한 피해를 주고 있다. 더욱이 이러한 국내 기업의 산업기술 해외 유출위험 방지와 피해 회복 등은 중국 현지에 진출한 중소기업의 경우에 매우 심각한 문제이다.

앞서 보았듯이 2012년 조사에서도 중국에 진출한 중소기업 중 약 절반에 이르는 중소기업들이 유출피해를 경험하였다. 따라서 미국 정부의 對 중국 산업보안 정책에 비추어 우리 역시 대 중국 산업보안 특히 중국 진출 중소기업에 대한 산업보안에 적극적으로 역량을 모아야 할 것이다.

미국 산업보안 정책이 우리의 해외 불법유출 대책에 주는 함의 즉 전략적 산업보안과 對 중국 산업보안은 결국 중국에 대한 산업보안 자원의 전략적 배치와 운용을 통해 저손실·저비용의 바람직한 정책성과 영역 또는 정책목표에 도달해야 함을 시사하고 있다.

산업유출 피해로 인한 손실(L_t) 규모의 감소는 무엇보다 유출 위험이 가장 높은 對 중국 산업보안에 자원을 집중적으로 동원, 배분함으로써 얻어질 수 있다. 또한 대기업에 비해 중소기업의 보안이 취약하고 특히 중국진출 중소기업의 보안역량이 취약하므로[25] 이 부문에 산업기술 침해방지 역량 및 활동을 집중하는 것이 바람직하다.

---

23) 『파이낸셜뉴스』, "한중 동반성장의 그늘 '기술 유출'", 2012. 8. 23.

24) 서울중앙지방검찰청, "보도자료: 국가핵심기술인 삼성 및 LG의 아몰레드 핵심기술을 해외유출한 외국 협력기업 수사 결과-90조원 가치의 국가핵심기술 아몰레드 기술 해외 유출 사범 7명 기소(3명 구속)", 2012. 6. 28.

25) 한국지식재산연구원에 따르면 기술유출 방지를 위한 국내 중소·벤처기업의 역량 점수는 5점 만점에 평균 2.47점으로 대기업의 평균 3.79점에 비해 현저히 낮은 수준인 것으로 파악됐다. 『머니투데이』, "중소·벤처기업 기술유출 방지대책 시급", 2013. 7. 29.

이와 관련 경찰청은 2012년에 중소기업청과 합동으로 중소기업 보안 인력 양성교육(10. 25 - 26) 및 중국 진출기업 기술보호 실태조사(9. 17 - 18)를 통해 기술유출 사례 및 대응기법 예방교육을 실시하여 기술보호 활동의 중요성을 강조하고[26], 2013년에는 기술유출로 피해를 입은 중소기업이 신속하게 피해상담 및 수사지원을 받을 수 있도록 「중소기업 기술유출 피해상담·수사 One-Stop 지원시스템」을 운영한 바 있다.[27]

향후 산업기술 유출 피해로 인한 손실을 감소시켜나가기 위해서는 현재의 예방 교육 및 지원시스템 구축에서 한 단계 발전하여, 수사인력 증원배치와 예산 확대지원을 통해 유출방지 人·物的 인프라를 확충하고 특히 국내 뿐 아니라 중국 등 현지 중소기업의 산업기술보호 네트워크와 수사지원역량을 강화해나가는 것이 긴요하다.

또 한편으로 산업보안에 투입되는 이러한 보안비용(C_t)의 절약, 나아가 산출된 L_t에 대비한 이른바 산업보안의 효율성($\frac{L_t}{C_t}=E_t$)을 확보하기 위해서는 기술품목별, 유출업종별, 유출시기별, 유출지역별로 나타나는 피해손실 고위험군(high-risk group)에 대한 효율적인 위험관리(risk management)와 보안정책조합(policy mix)이 요구되지만, 무엇보다도 업계와의 産·警 협력 네트워크의 구축이 중요하다.

즉 산업기술의 내용과 진정한 현재가치, 해당 산업기술로부터 예상되는 미래수익 흐름, 보안상의 취약점을 가장 정확히 알 수 있는 주체는 기업 당사자이므로, 국가기관은 기업과의 협력 관계 구축을 통해 보안비용을 분담하고 적기적소에 국가 및 민간의 보안자원을 배분함으로써 산

26) 경찰청, 경찰백서, 2013, p. 293.
27) 경찰청, "보도자료: '경찰청-중소기업중앙회' 중소기업 기술보호「One-Stop 지원시스템」운영", 2013. 5.

업계 전반의 보안 효율성을 기할 수 있게 될 것이다.

V. 결 론

본 연구는 탈냉전 이후 국제경제환경 변화와 국내 산업발전으로부터 야기되는 산업기술 해외 불법유출 방지책에 대한 필요성 문제를 제기하면서, 최근 미국의 산업보안 정책에 대한 분석을 바탕으로 이들이 우리의 산업기술 해외 불법유출 대응에 주는 함의를 도출하고자 하였다.

우리의 최근 산업기술 해외 불법유출 실태에서 주목할 점은 2010년 일시 안정을 보이던 산업기술 해외 불법유출이 2011년 들어 다시 증가세로 돌아섰다는 것이다. 즉 2010년 다소 감소했던 국가정보원 적발건수(41건)은 2011년 46건으로 사상 최대치를 기록했으며, 경찰청에 의한 검거건수 역시 2011년 24건, 2012년 27건에 달함으로써 역대 최고 검거건수를 연속하여 넘어섰다.

불법유출 상대국을 보면 아시아권 국가뿐만 아니라 서구 선진국 등으로 다양화 되고는 있으나, 중국에 집중되는 양상(58.3%)이 여전히 계속되고 있는 것으로 나타났다(경찰청 2011년 검거사건 기준). 국가정보원의 기술유출 적발사건(2005-2011)도 50% 이상은 중국으로의 기술유출이었다.

미국의 최근 산업보안 정책 동향을 보면 자국의 생존과 번영에 핵심이 되는 국가기밀, 자산, 산업기술의 보호를 위해 이른바 국가방첩전략의 큰 틀 아래서 전략적 산업보안 정책을 추진하고 있으며, 이러한 정책 기조는 최근 오바마 행정부에서 들어서 '산업기술 침해방지 전략'(ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS)'제하의 산업기술 침해방지 전략(2013)으로

더욱 강화되고 있다.

미국은 자국의 핵심 국가기밀, 자산, 산업기술의 보호를 위해 이른바 국가방첩전략의 큰 틀 아래서 전략적 산업보안 정책을 추진하고 있으며, 이러한 정책 기조는 최근 오바마 행정부에서 소위 산업기술 침해방지 전략(2013)으로 더욱 강화되고 있다.

公共性을 갖는 산업보안의 주요 정책 목표는 산업기술 불법유출 위험의 최소화와 이를 구현해내기 위한 보안 비용의 최소화를 달성하는 것이라고 할 수 있다. 이러한 산업보안의 정책목표는 미국의 전략적 산업보안이라는 정책에서도 찾아 볼 수 있으며, 이를 바탕으로 우리의 산업보안 역시 소위 “전략적 산업보안”이라는 정책 구상으로 보다 구체화하였다. 즉 전략적 산업보안이란 산업기술 해외 불법유출 위험의 최소화가 국내 기업뿐만 아니라 국가경제적 이익을 효과적으로 달성하는 수단임을 명백히 선언하는 한편, 더 나아가 산업보안의 비용-성과를 감안한 범기관적, 범사회적 차원의 효율적 산업보안체계를 구축하는 것이다.

미국 산업보안 정책이 우리의 산업기술 불법유출 대책에 주는 또 하나의 함의는, 전세계적 규모로 전개되는 자국 기술의 해외 유출 특히 중국의 산업기술 침해 활동에 대한 진지한 인식과 침해방지를 위한 적극적이며 실천적인 대응이다

우리나라의 경우도 해외 불법유출 상대국의 확산 속에 중국의 산업기술 침해 활동을 주시해야 할 것으로 보인다. 특히 중소기업인 경우에는 보안이 취약하여, 중국 진출 중소기업 중 약 절반에 가까운 중소기업들이 유출피해를 경험한 것으로 드러났다. 따라서 미국 정부의 對 중국 산업보안 정책에 비추어 우리 역시 대 중국 산업보안 특히 중국진출 중소기업에 대한 산업보안에 적극적으로 역량을 모아야 할 것이다.

미국 산업보안 정책이 우리의 해외 불법유출 대책에 주는 함의 즉 전

략적 산업보안과 對 중국 산업보안은 결국 중국에 대한 산업보안 자원의 전략적 배치와 운용을 통해 저손실·저비용의 바람직한 정책성과 영역 또는 정책목표에 도달해야 함을 시사하고 있다.

산업유출 피해로 인한 손실(L_t) 규모의 감소는 무엇보다 유출 위험이 가장 높은 對 중국 산업보안에 자원을 집중적으로 동원, 배분함으로써 얻어질 수 있다. 향후 불법유출 피해손실을 감소시켜나가기 위해서는 현재 경찰청이 진행하고 있는 예방 교육 및 지원시스템 구축에서 한 단계 더 발전하여, 수사인력 증원배치와 예산 확대지원을 통해 人·物的 보안 인프라를 확충하고 특히 국내 뿐 아니라 중국 등 현지 중소기업의 산업기술보호 네트워크와 수사지원역량을 강화해나가는 것이 긴요하다.

산업보안에 투입되는 보안비용(C_t)의 절약과 산업보안의 효율성($\frac{L_t}{C_t}=E_t$)을 확보하기 위해서는 품목별, 업종별, 시기별, 지역별 피해손실 고위험군에 대한 효율적인 위험관리와 정책조합이 요구되지만, 무엇보다도 업계와의 産·警 협력 네트워크의 구축이 중요하다. 산업기술의 내용과 진정한 현재가치, 산업기술로부터 예상되는 미래수익 흐름, 보안상 취약점을 가장 정확히 아는 주체는 기업 당사자인 바, 기업과의 협력 관계 구축을 통해 보안비용을 분담하고, 적기적소에 보안자원을 배분함으로써 산업계 전반의 보안 효율성을 기할 수 있게 될 것이다.

참고문헌

1. 국문문헌

경찰청. 경찰백서, 2013.

경찰청. “보도자료: 국제범죄수사대, 산업기술유출수사의 첨병으로 거듭나”, 2012. 2. 16.

경찰청, “보도자료: ‘경찰청-중소기업중앙회’ 중소기업 기술보호 「One-Stop 지원시스템」운영”, 2013. 5.

경찰청. “산업기술유출사범 검거현황(내부자료)”, 2013.

김왕식. “정보환경의 변화와 방첩제도의 개선방향”, 국가정보연구, 제5권 1호, 2012.

서울중앙지방검찰청. “보도자료: 국가핵심기술인 삼성 및 LG의 아몰레드 핵심기술을 해외유출한 외국 협력기업 수사 결과-90조원 가치의 국가핵심기술 아몰레드 기술 해외 유출 사범 7명 기소(3명 구속)”, 2012. 6. 28.

한국산업보안연구학회, 산업보안학, 2012.

정웅. “산업보안범죄의 최근 동향과 대응전략”. 한국행정학회 2010 추계국제학술대회 발표논문집, 2010.

정웅. “해외 주요 국가들의 경제방첩 정책과 우리의 정책과제”. 국가정보연구, 제5권 2호, 2012.

치안정책연구소. 치안전망, 2013.

2. 외국 문헌

Executive Office of the President of the United States. *ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS,* February, 2013.

ONCIX. *The National Counterintelligence Strategy of the United States of America,* 2007-2009 각년도.
ONCIX. *The National Counterintelligence Strategy of the United States,* March, 2005.

3. 인터넷 자료 및 신문류

산업기밀보호센터. “주요국 법령정보”, “해외동향”, http://service4.nis.go.kr (2013. 12. 1 검색).
산업통상자원부, “FTA 종합지원포털”, http://www.ftahub.go.kr (2013. 12. 1 검색).
통계청, “국가통계포털”, http://kosis.kr (2013. 12. 1 검색)

ONCIX. “ECONOMIC ESPIONAGE”, http://www.ncix.gov/issues/economic/index.php (2013. 12. 1 검색).
ONCIX. “ONCIX Reports to Congress”. http://www.ncix.gov/publications/reports/fecie_all/index.php (2013. 12. 1 검색).
U.S. Department of Justice. “Attorney General Eric Holder Speaks at the Administration Trade Secret Strategy Rollout”. http://www.justice.gov/iso/opa/ag/speeches/2013/ag-speech-1302201.tml(2013. 12. 1 검색).

『뉴스1』. “美백악관, 해킹·산업스파이 대책 발표”, 2013. 2. 21.
『머니투데이』. “중소·벤처기업 기술유출 방지대책 시급”, 2013. 7. 29.
『파이낸셜뉴스』. “한중 동반성장의 그늘 ‘기술 유출’”, 2012. 8. 23.
『한국경제』. “中 진출 중기 ‘산업 스파이 심각’”, 2012. 7. 18.

책임연구보고서 2013-15

한국의 산업기술 해외 불법유출 실태와 대책

2013년 12월 31일 발행

발행인 : 치안정책연구소장

발행처 : **치안정책연구소**
경기도 용인시 기흥구 언남로 74

홈페이지 : www.psi.go.kr

POLICE SCIENCE INSTITUTE