국가 사이버 안보 역량 강화를 위한 '사이버 방위산업' 육성 방안†

박준정*, 김광조*
*카이스트 정보보호대학원

Promoting Cyber Defense Industries for Strengthening the National Capabilities of Cyber Security

Joon-Jeong Park*, Kwangjo Kim*
*Graduate School of Information Security, KAIST.

요 약

국내 정보보안 산업 규모는 증가하고 있지만, 그 성장률이 둔화되는 등 관련 산업이 침체 우려에 있다. 정부 차원의 지원 없이 업계 자체 역량만으로 해외 수출을 확대하기도 곤란한 상황에서 새로운 성장 동력을 개척해야만 하는 현실에 처해 있다. 한편, 지속적으로 사이버 전쟁을 수행하고 있는 우리나라는 적보다 우세한 사이버 안보 역량을 구비해야 하지만, 군 자체적으로는 나날이 발전하는 기술에 대응할 수 없는 실정이다. 따라서 민·관·군 공동으로 사이버 안보 역량을 제고할 수 있도록 정보보안 산업을 방위산업의 범주에 포함시켜 적정한 이윤 보장 및 수출 지원, 인력 양성 지원 등 다양한 혜택을 제공하는 한편, 사이버전 대응 간 업계의 첨단 기술과 전문인력을 군에서 활용할 수 있는 방안을 제안하고자 한다. 이를 통해, 사이버 안보 강국 구축 및 정보보안 산업 생태계 강화 효과를 동시에 달성할 수 있다.

I. 서론

국내 정보보안 산업은 지속 발전하고 있으나 그 성장률은 매년 낮아지는 추세로, 관련 업계에서는 정보보안 산업 발전을 위한 범정부 차원의 대책 마련을 요구하는 등 문제점이 제기되고 있다. 한계 상황에 봉착한 정보보안 산업을 발전시키기 위해 정부에서는 다방면으로 노력하고 있으나, 기존에 제기된 문제점들을 종합하는 수준의 해결책을 제시하고 있어 그 실효성을 예측해 보기 어려운 상황이다.

우리나라와 대치하고 있는 북한은 비대칭전을 능숙하게 구사하고 있으며, 그 중에서도 세계 최고 수준의 사이버전 인력을 보유하고 있는 등 사이버전 강국으로 널리 알려져 있다. 이에 대비하여 군에서는 사이버사령부를 창설하였으나, 인력 양성 및 기술 발전 등 제반 분야에서 아직 미흡한 실정이다. 국방 분야에서 뿐만 아니라, 민간에서도 사이버 안보 유관 산업을 발전시켜야 할 필요성이 대두되는 이유이다.

이에, 본 고에서는 국가 차원에서 사이버 안보를 강화하고 국내 정보보안 산업을 발전시킬 수 있는 두 가지 목적을 동시에 달성하고 민·관·군이 상호 win-win할 수 있는 방안을 마련하고자 한다. 정보보안 산업을 방위산업의 범주에 포함하여 적의 사이버 공격으로부터 아군 정보체계를 보호하기 위한 '사이버 방위산업'을 전략적으로 육성하는 정책에 대해 고찰해 보고자 한다.

이를 위해, 제 2장에서는 국내·외 정보보안 산업 및 우리나라 사이버전 관련 실태 등을 진단하고, 제 3장에서는 상기 분야에 대한 선행연구에 대해 분석한 후, 제 4장에서는 양 분야를 동시에 발전시킬 수 있는 방안을 제시한다. 제 5장에서는 제안한 정책에 대한 기대효과를 논의한 후, 마지막 제 6장에서는 향후 연구를 제시하면서 결론을 맺는다.

II. 관련 현황 및 내용

2.1 국내 정보보안 산업

국내 정보보안 산업은 매년 발전하고 있지만, 그 성장세가 둔화되고 있음을 통계자료를 통해 확인할 수 있다. 정부에서는 2012년을 기준으로 향후 5년 간 연 평균 성장률을 12.48%로 예상[1]하였으나, 2014년에는 향후 5년 간 연 평균 성장률이 9.6%로 줄어들 것으로 판단[2]하고 있다.

또한, 2013년 말 기준 전국 컴퓨터 보유 사업체(약 260만 개) 중 86.5%가 정보보안 제품을 이미 사용[3]하고 있는 등 국내 시장은 어느

† 본 연구는 KAIST 미래전략대학원이 지원한 '국가재난안전 통신망의 장기간 보안성을 보장하는 산업 발전 전략' 연구결과[N01150155]로 수행되었습니다.

정도 한계 상황에 봉착했다고 판단할 수 있다.

내수 시장의 한계를 극복하기 위해서는 해외 시장 개척을 통해 수출을 확대해야 하나, 현재로서는 정부 차원의 지원 등 특별한 대책이 없는 실정이다. '사이버 안심 국가 실현을 위한 정보보호 대토론회'에서 심종헌 정보보호산업협회 회장은 "지금은 산업이 선 순환할 수 있는 연결고리가 없다."며 애로사항을 표출[4]하였다.

이에, 미래창조과학부는 2019년까지 시장 규모를 100% 확대하고 수출액을 3배 증대키는 한편, 전문인력을 적극 양성한다는 청사진을 제시[5]하였으나, 목표 달성 가능 여부를 낙담할 수 없는 상황이다.

2.2 시장 확대를 위한 정부지원 필요사항

국내 정보보안 산업체(256개)를 대상으로 설문조사한 결과, 시장 확대를 위해 정부에 요청하는 사항[2]은 [표 1]과 같다. 업계에서는 새로운 시장수요 창출 및 세제 지원, 관련 법규 정비 등을 주요 과업으로 판단하고 있다.

[표 1] 정보보안 시장 확대를 위한 정부지원 필요사항

순위	지원 필요사항	요구 수준 (5점 만점)
1	정부 공공부문의 시장수요 창출	4.16
2	각종 자금 및 세제 혜택	4.10
3	기술개발 연구 지원	3.92
4	정보보안 산업을 위한 법 제·개정	3.91
5	소비촉진 및 투자 활성화	3.82
6	해외지원 사업 확대	3.61
7	자격증 제도의 활성화 및 전문인력 양성	3.51
8	기술이전 활성화 및 M&A 지원	3.28

2.3 해외 정보보안 산업

2011년 ~ 2016년 간 전 세계 정보보안 시장은 연 평균 7.6% 성장할 것으로 전망[6]된다.

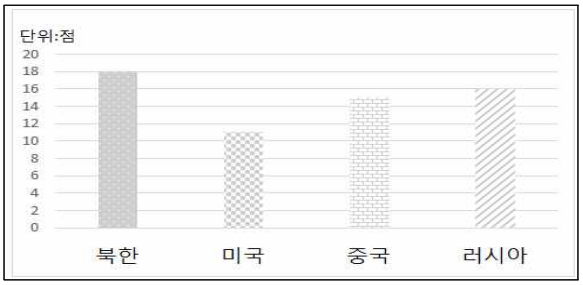
미국은 전 세계 정보보안 시장의 약 40%를 차지하는 가장 큰 시장으로 연 평균 10%대의 성장세를 보이고 있으며, 2013년 시장 규모는 375억 달러에 육박할 것으로 예측[7]되었다.

또한, 미국 정부는 2015년 4월 사이버 공격자를 강력히 제재할 수 있는 행정명령을 발령하였으며, 2016 회계연도에 전년 대비 12% 증가한 140억 달러의 사이버보안 예산을 책정하여 사이버 위협과 공격에 대해 국가적 차원의 고강도 대응 방안을 추진 중[8]이다.

영국 정보보안 시장은 2013년 27억 9,500만 파운드 규모를 형성하고 있으며, 연평균 5.7% 성장할 것으로 전망된다. 이 중 방위 및 정보기관 시장은 규모는 크지 않지만, 가장 높은 수준의 보안 기술을 요구[9]하고 있다.

2.4 사이버전

북한은 6,000여 명의 사이버전 인력을 운영하고 있으며, 남한 내부의 심리적·물리적 마비를 위해 군사작전에 차질을 유발하고 주요 국가기반 체계를 공격하는 등 사이버전을 수행[10]하고 있다. 또한, [그림 1]과 같이 북한의 사이버전 능력은 총 18점으로 세계 최고 수준[11]이다.



[그림 1] 국가별 사이버전 능력

우리나라 사이버전 전문인력 현황은 공식적으로 발표된 자료가 없어 정확한 수치는 알 수 없다. 다만, 언론 등 인터넷에 공개된 자료에는 600명 수준[12]으로 알려져 있다.

단순히 인력으로만 비교하더라도 북한의 1/10에 불과한 열세에 처해 있어, 사이버전 규모 및 역량 향상을 위한 대책 마련이 긴요한 실정이다.

2.5 국내 방위산업체

우리나라는 군수물자의 안정적인 조달원 확보를 위해 방산물자 및 업체를 지정하여 다양한 혜택을 부여하고 있다. 2013년 말 기준 국내 방산업체는 총 97개로, 통신전자 분야는 16개 업체[13]가 지정되어 있다.

이 중에는 암호장비 개발업체가 일부 포함되어는 있지만 대부분이 지휘통신체계 개발업체이며, 관련 법률의 미비로 인해 다수의 정보보안 업체는 방위산업으로 진출이 제한되는 실정이다.

2.6 시사점

미국은 사이버 위협을 국가 안보에 직접적으로 영향을 미치는 중대한 사안으로 판단하여 선제적으로 대응하고 있으며, 정부 차원에서 관련 산업 규모를 확장시키기 위해 적극적으로 노력하고 있다. 영국은 방위·정보기관 시장을 별도의 시장으로 분류하고 있으며, 전문 지식 등이 필요한 방산 전문 업체들이 주로 납품[9]하고 있다.

국내 정보보안 산업체 요구사항 및 미국·영국 등 선진국의 사례를 종합해 보면, 정부의 적극적인 지원을 통해 안정적인 수요를

창출하여 산업 규모 자체를 확장시키는 것이 무엇보다 중요하다. 또한, 자금 및 연구개발 지원, 관련 제도 정비도 시급한 과제이다.

또한, 민・군 경계가 없는 사이버 전문인력을 양성하고 국내 정보보안 산업 시장을 확대함과 동시에 사이버전 수행 역량 발전을 위해 필요한 기술을 안정적으로 확보할 수 있는 방안을 마련해야 한다.

III. 관련 연구

3.1 정보보안 산업 관련 분야

정보보호 투자성과를 측정하기 위한 방법론 연구[14, 15]를 필두로, 정보보호 관련 산업의 경제적 파급효과 분석[16], 사이버 공격에 대한 피해액 추정 방법론[17, 18, 19] 등이 활발히 연구되었다.

또한, 한국과 미국의 정보보호 산업의 경쟁력을 분야별로 비교한 연구[20]와 유망한 정보보안 제품・서비스를 제시하고 정책 방향을 제안한 연구[21]도 진행되었다.

3.2 사이버전 분야

선행연구로는 사이버전에 대비하기 위한 보안기술 현황과 전망[22], 사이버전의 형태에 따른 정보보호 기술에 대한 연구[23] 등이 있다. 사이버전에 효과적으로 대응하기 위해 기술・인력 분야 / 시스템・장비 분야 / 법・제도 분야 대책을 도출한 연구[24]도 수행되었다.

3.3 한계점

정보보안 산업 분야와 사이버전 분야 모두 활발한 연구가 진행되고 다양한 연구 논문이 발표되었다. 하지만 정보보안 산업 분야는 대부분 경제학적 접근을 통해 계량화된 수치를 제시하는 위주의 연구가 주로 진행되었을 뿐, 거시적 관점에서 새로운 산업 시장을 개척할 수 있는 구체적 대안과 관련 법규 정비 방안까지 제안한 연구는 진행되지 않았다. 사이버전 분야는 산업 분야와 연계시켜 국가 차원에서 사이버 안보를 강화하고 관련 산업을 발전시킬 수 있는 측면에서 접근하지 못했다.

IV. 발전 방안

과거에는 전시에 Off-line에서 일어나던 전쟁이 현재는 평시에도 On-line에서 끊임없이 진행되는 양상으로 변화하고 있다. 따라서 적의 사이버 공격으로부터 아군을 보호하기 위한 정보보안 산업은 단순히 1개 산업 영역이 아니라 국가안보 차원의 전략 산업으로 집중 육성해야 한다.

미국은 '수출관리규정'을 통해 국가안보에 영향을 미칠 수 있는 암호장비 등의 수출을 엄격히 금지하고 있다. 우리나라도 국가 총력적 차원에서 사이버 안보 역량을 향상시키기 위해 전향적인 자세로 정보보안 산업을 방위산업 관점으로 접근해야 한다.

이를 위해, [표 2]에서 제안하는 바와 같이 '방위사업법[25]'을 개정하여 중요 방산물자의 범주에 정보보안장비를 포함해야 한다.

[표 2] 방위사업법 제 35조 2항(주요 방산물자) 개정案

	현 재	개 정
내용	1. 총포류 및 화력장비 2. 유도무기 ~ 10. 화생방장비 11. 지휘 및 통제장비	1. ~ 11. (좌동) **12. 정보보안장비 (추가)**

V. 기대 효과

- 국내 정보보안 업계 보호

  단기적으로는 정보보안 업체의 적정 이윤을 보장하고 정부 우선 구매를 통해 안정적인 공공시장 수요를 확대할 수 있다. 필요시 방위산업 육성자금 융자 제도 등을 통해 업계를 지원할 수도 있고, 장기적으로는 국내 정보보안 시장 규모 자체가 확대되는 효과도 달성 가능하다.

- 품질보증 및 수출경쟁력 향상

  우수 정보보안 제품에 대해 국방기술품질원에서 수여하는 '국방품질마크(Defense Quality) 인증'을 통해 정부가 품질을 보증할 수 있으며, 이를 통해 해당 업체의 수출 경쟁력 향상까지 도모할 수 있다.

- 민・관・군 상호 기술 교류 활성화

  민간 분야에서 발전된 기술을 관・군에 최단시간 내 보급(spin-on)하고, 관・군에서 개발한 기술을 민간 분야로 이전(spin-off) 할 수 있다. 또한, 민・관・군 범용 기술은 공동으로 개발・활용(spin-up)하기 용이하다.

- 전문인력 양성 등 국가 사이버 안보 역량 제고

  양질의 정보보안 제품(기술)이 군 및 정부기관에서 활용될 경우, 우리나라 사이버 안보 역량이 한층 제고될 것이다. 또한, 평소 정보보안 산업 종사자에게 정부 차원의 교육 기회를 제공하는 한편, 사이버전 대응 간 필요시 관련 업체 인력을 지원받을 수 있도록 제도화하여 '사이버 예비군[26]' 개념으로 활용한다면, 정보보안 업계와 정부가 상호 win-win할 수 있는 선순환 프로세스를 구축할 수 있다.

VI. 결론 및 향후 연구

본 고에서는 한계에 봉착한 국내 정보보안 산업의 발전 대책을 마련함과 동시에 적의 사이버 위협으로부터 국가 안보를 공고히 할 수 있도록 정보보안 산업을 방위산업의 범주에 포함시켜 '사이버 방위산업'을 육성하는 정책을 제시하였다.

이를 통해, 정보보안 업계를 보호하고 수출경쟁력을 향상시키며 전문인력을 육성·활용하여 사이버 안보 역량이 제고될 것으로 기대된다.

앞으로는 미래 전쟁양상을 고려하여 국가 사이버 역량 강화를 위한 정책·제도·법률 정비 방안에 대해 추가적인 연구가 요구된다.

[참고문헌]

[1] Korea Internet & Security Agency, "Survey for Knowledge Information Security Industry in Korea: Year 2012," Nov. 2012.

[2] Korea Information Security Industry Association, "Survey for Knowledge Information Security Industry in Korea: Year 2014," Dec. 2014.

[3] Ministry of Science, ICT and Future Planning and Korea Inetnet & Security Agency, "2014 Yearbook of Information Society Statistics," Dec. 2014.

[4] ZDNet Korea, "http://www.zdnet.co.kr/news/news_view.asp?artice_id=20150204144703&type=det&re=," Feb. 2015.

[5] Ministry of Science, ICT and Future Planning, "K-ICT Security Development Strategy," Apr. 2015.

[6] Korea Information Security Industry Association, "Survey for Global Information Security Industry in Americas: Year 2013," 2013. [International Data Center(2012) 자료를 재인용]

[7] IDC & RNCOS, "Global IT Security Market Forecast to 2013," 2013.

[8] Korea Information Security Industry Association, "ICT Issues Weekly," Apr. 2015.

[9] Korea Information Security Industry Association, "Survey for Global Information Security Industry in Europe and Middle East: Year 2013," 2013.

[10] Ministry of Nation Defense, "2014 Defense White Book," Dec. 2014.

[11] Richard Clarke, "Cyber War," 2010.

[12] Kookminilbo, "http://news.kmib.co.kr/article/view.asp?arcid=0008890015&code=61111911&cp=nv," Nov. 2014.

[13] e-나라지표, "http://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx_cd=1702," July 2014.

[14] Jong-sun Lee and Hee-Jo Lee, "Evaluation Information Security Investment using TCO-based Security ROI,", Proceeding of The 2007 Spring Conference of The Korea Information Processing Society, Apr. 2007.

[15] Sun-ok Ahn and Hee-Jo Lee, "Analyzing nformation Investment using AHP-based Security ROI," *Journal of Korea Multimedia Society*, vol. 12, no. 5, pp. 575-578. May 2009.

[16] Woo-Soo Jeong *et al.*, "Analysis of Economic Efforts for Information Security Industry in Korea," *Journal of The Korea Institute of Information Security and Cryptology*, vol. 24, no. 2, Apr. 2014.

[17] Jin Shin, "Economic Analysis on Effects of Cyber Information Security in Korea: Focused on Estimation on National Loss," *Journal of The Korea Institute of Information Security and Cryptology*, vol. 23, no. 1, Feb. 2013.

[18] Il-Seok Oh and Seok-Yun Lee, "A Study on cost damage of Cyber Attacks and their Impact on Stock Market," *Journal of The Korea Information Processing Society*, vol.13, no. 1, pp. 63-68. Feb. 2006.

[19] Youngyung Shin *et al.*, "Economic Damages Assessment for National Cyber Security Measures: Analysis of the March 20 Cyber Attack," *Journal of The Korea Association of National Intelligence Studies*, vol. 6, no. 1, pp. 129-173, June 2013.

[20] 원종성, "한·미 정보보호산업의 국제경쟁력 분석: 포터의 다이아몬드 모델을 중심으로," 고려대학교 석사학위 논문, 2012.

[21] 손경호, "정보보안 산업 현황 및 전망," *Journal of The Korea Information Processing Society*, vol. 17, no. 6, pp. 67-75, Nov. 2010.

[22] 서동일, 조현숙, "사이버전을 위한 보안기술 현황과 전망," *Journal of The Korea Institute of Information Security and Cryptology*, vol. 21, no. 6, pp. 42-48, Oct. 2011.

[23] 박호균, "Types and Information Security Technology on Cyber Warfare," *Journal of Korea Contents Association*, vol. 11, no. 4, pp. 41-44. Dec. 2013.

[24] 박대우, "대한민국 국군의 사이버전 대응," 한국군사학회 군사논단, vol. 75, pp. 37-72, 2013.

[25] 방위사업법, 법률 제 12,559호, 2014. 5. 9.

[26] Congress, "https://www.congress.gov/bill/113th-congress/senate-bill/658," Mar. 2013.