Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.6, Dec. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.6.1571

국방 사이버전 분야에 적용 가능한 유망 민간 정보보호 기술 선정 방법론에 대한 고찰*

이 호 균,[1†] 임 종 인,[2] 이 경 호[2‡]
[1]국방기술품질원, [2]고려대학교 정보보호대학원

Study on Selection Methodology of Applicable Prospective Civil Information Security Technologies in Defense Cyberwarfare Sector*

Ho-gyun Lee,[1†] Jong-in Lim,[2] Kyung-ho Lee[2‡]
[1]Defense Agency for Technology and Quality,
[2]Graduate School of Information Security, Korea University

요 약

본 논문은 민간 정보보호 분야의 기술 분류와 국방 사이버전 분야의 기술 분류를 연계하는 방법론을 제안하고 이를 기반으로 다원속성효용이론을 이용하여 국방 분야에서 추후 도입, 발전시킬 민간 유망기술을 선정한다. 선정된 유망기술의 연구추진 방안에 대한 설문조사 결과 다음과 같은 사실을 발견하였다. 첫째, 사회적 파급효과가 클수록 그 기술에 대한 정부 주도 연구개발 필요성은 커지는 것으로 나타났다. 둘째, 파급효과 중 사회, 경제, 기술 순으로 정부 주도 연구개발 필요성과 상관관계가 높은 것으로 나타났다. 셋째, 국방 적용성과 기술의 중요성은 투자주체나 개발주체 선정에 영향을 미치지 않는 것으로 분석되었다. 이것은 사회적 파급효과 큰 기술에 대해서 정부가 선도적으로 연구개발 투자를 추진해야 하나, 그 연구개발의 추진에 있어 국방 적용성, 기술의 중요성에 따라 단순히 투자/개발 주체가 결정될 수 없음을 시사하고 있다.

ABSTRACT

This paper suggests a methodology for linking technology classification of nongovernmental information security field and technology classification of cyber-warfare in national defense field. Based on this methodology, Multi-Attribute Utility Theory(MAUT) is applied for the purpose of selecting promising nongovernmental technology that is worthy of later introduction or development. After studying the result of the survey regarding the research progression plan of the selected promising technology, the following three facts are discovered: Firstly, the greater the social spillover effect, the greater the need for the government lead R&D. Secondly, among the spillover effects, the social aspect has the highest correlation with respect to the need for the government lead R&D, while the economical aspect and the technological aspect come in the second and the third place, respectively. Finally, according to the correlation analysis, the defense application and the technological importance do not affect the subject of investment or the subject of development. This indicates that even though the R&D for technology with high social spillover effect should be lead by the government, the subject of the investment or the development cannot be determined solely by factors such as military application and technological importance.

Keywords: Cyberwarfare, Information Security, Multi-Attribute Utility Theory, Technological Planning

Received(08. 04. 2015), Modified(11. 05. 2015), Accepted(11. 09. 2015)

* 본 연구는 국방부의 2015 국방 정보기술(IT) 조사 용역의 연구결과로 수행되었습니다.(제2014MCD0056호)

† 주저자, hglee@dtaq.re.kr
‡ 교신저자, kevinlee@korea.ac.kr(Corresponding author)

I. 서 론

사이버전의 중요성이 강조되면서 세계 각 국에서 사이버전 전문기관 설립 및 연구개발 추진이 활발해지고 있다[1-3]. 우리나라에서도 사이버사령부 창설과 함께 사이버전 무기체계의 운영개념 수립 및 핵심기술 연구개발/무기체계 획득을 위한 중장기계획 수립을 연구 중에 있다. 국방 분야의 사이버전 연구개발 이전에 민간 정보보호 분야에서도 1990년대 중반부터 ETRI, KISA, 국보연 등을 중심으로 정보보호 분야를 발전시켜 오고 있다. 기존에 연구된 민간의 우수 연구개발 실적이 국방 분야에 바로 적용될 수 있다면 국가 예산절감이나 연구실적의 활용분야를 확대하는 효과를 기대할 수 있을 것이나, 국방 정보에 대한 접근의 어려움과 산재된 민간 연구개발 실적을 국방 분야와 연계하는 어려움 때문에 민간 정보보호 기술의 국방 사이버전 적용 방법론이 아직 수립되지 못한 실정이다. 한국 정부 차원의 민간 정보보호 연구개발은 침입탐지시스템, 영상감시기술 등의 연구개발 실적이 있다. 사이버전 개념 수립 초기부터 민간 정보보호와 국방 사이버전의 차이점과 공유점을 잘 정립할 수 있다면 사이버전 분야의 최선진국 기술수준을 빠르게 따라잡고 민간 산업경쟁력 강화에도 기여할 수 있을 것이다. 국방기술과 민간기술의 연계를 통해 민간분야에서 기 개발한 우수 정보보호기술을 국방에 적용하는 Spin On사업과 국방에서 기 확보한 핵심기술을 민간에 적용하는 Spin Off 사업을 활성화시키고, 이를 통해 전체 국가 R&D 예산을 효율적으로 집행할 수 있기 때문이다.

민군기술협력사업 또는 민군겸용기술 활성화 사업은 국가안보와 산업경쟁력 강화를 동시에 향상시킬 수 있는 정책으로 국내에서는 1990년대 중반부터 중요성을 인식하고 추진 중에 있다[4]. 그러나 기존 협력사업은 8대 무기체계 분류에 기반한 접근 방식이 주였기 때문에 무기체계로 분류되지 못했던 사이버전 분야는 민군협력 수행사례나 방법론 수립이 아직 미진한 상황이다.

본 논문에서는 민간 정보보호 기술분류와 국방 사이버전 기술분류를 연계하고, 이를 기반으로 국방 사이버전 분야에 적용이 가능한 유망 민간 정보보호 기술을 선정하는 방법론을 제안한다. 또한 선정된 유망기술에 대하여 투자/개발 주체에 대한 설문조사를 실시하여 유망기술 선정 요소와 투자/개발 주체간의 상관관계를 분석하였다. 논문의 구성은 다음과 같다. 2장에서는 기존 관련연구의 조사결과를 기술한다. 3장에서는 본 논문에서 적용한 연구방법론을 설명하고 4장은 연구방법론에 따른 조사분석 결과를 항목별로 제시한다. 마지막으로 5장에서는 결론을 기술한다.

II. 기존 연구

2.1 민군기술 융합 및 유망기술 선정 방법론 연구

김철환은 민군겸용기술사업의 효율성 부족과 추진실적 저조를 개선하기 위한 활성화 방안을 연구하면서 기술수준조사를 기반으로 핵심기술을 선정하고 이를 선 개발해야 함을 주장하였다[4]. 안영수는 국내 민군기술융합의 발전과정과 주요과제를 정리하고, 민군기술융합 촉진을 위한 정책방안을 제안하면서 정부 핵심사업의 민군기술융합 사전 검토 기능을 강화해야 함을 정책 제안하였다[5]. 권경용은 국방 IT 기술조사 활동의 일환으로 민간 IT 기술의 국방 적용을 위한 실태를 분석하고 민간 유망기술별 기술수준을 조사하였다[6]. 박경진은 국방과학기술을 분류하고 기술 분류별 수준을 조사하였으며, 이를 기반으로 핵심기술을 도출하고 연구개발 로드맵을 제시하였다[7][8]. 국방부에서는 정보화 신기술의 국방 적용을 촉진하고 정보 기술 연구개발사업 소요의 기준 문서로 활용할 수 있도록 주요 정보화 신기술에 대한 기술 개발 현황, 발전추세, 적용방향 등을 제시하는 국방 IT 조사서를 3년 단위로 발간하고 있다[9][10].

세계 각 국은 미래의 경쟁에서 살아남기 위해 핵심기술과제를 선정해 연구 개발에 박차를 가하고 있다. 미국의 랜드 연구소는 1998년에 27개 세부영역, 103개 기술목록을 발표하였고, 일본 문부과학성은 과학기술예측조사를 거쳐 10대 기간기술을 선정하였으며, EU는 NEST 프로그램을 추진하고 있다[11].

국내 각 부처의 기술기획 전문기관에서도 전략기술 목록과 유망기술 선정을 주기적으로 수행하고 있다. 한국과학기술기획평가원에서는 국가과학기술표준분류체계를 관리하면서 NTIS등에서 과학기술 성과관리의 표준기술분류로 활용하고 있으며, 산업자원부의 한국산업기술진흥원은 산업기술로드맵을 발표하고 있다[12]. 또한 민간기관인 한국정보통신기술협회에서도 ICT 표준화전략맵을 발표해서 표준 대상 기술을 관리하고 있다[13]. 원유재는 국내 정보보호 기술의 세계 시장 점유율 향상을 위해 세계일류 10대 제품을 선정하고 기술개발 로드맵을 제안하였다[14]. 장

태우는 철도 IT 융합기술 연구개발 기획연구를 하면서 전문가 설문조사와 다원속성효용이론 방법론을 이용해서 핵심 연구과제를 선정하였다[15].

본 논문에서는 김철환과 안영수의 주장에 따라 민간 정보보호 분야에서 정량적으로 유망기술을 선정하고 선정된 유망기술들의 군 적용성 등을 사전에 검토할 수 있는 방법론을 고안한다. 민간 IT 기술의 국방 적용방안 연구는 기존에 권경용의 연구에서 이미 다룬 바가 있으나 본 논문에서는 민간 연구기관들의 기술분류와 국방 기술분류를 연계하는 민군통합기술목록을 수립하고 이를 기반으로 다원속성효용이론에 기반을 둔 유망기술 선정절차를 새롭게 제안하고 있다. 또한 유망기술 선정 속성과 국가주도 연구개발 사업추진 필요성 간의 상관관계에 대해서 분석한다.

2.2 사회적 파급효과와 국가주도 연구개발 사업추진 필요성 간 관계

성지은은 연구개발사업의 사회적 파급효과 분석 가능성을 연구하면서 연구개발사업 평가에서 사회적 파급효과가 중요한 가치로 등장하고 있다고 하였다. 주요 선진국에서는 연구개발사업 평가 항목에 사회적 파급효과를 정성적 지표로 포함하여 오래 전부터 강조하고 있고, 연구개발 성과의 사회적 활용·확산이 강조되고 있으며, 특히 사회문제 해결을 위한 연구개발사업이 등장하면서 사회적 파급효과가 연구개발사업의 중요한 가치 목표로 논의되고 있다고 한다[16]. 본 연구에서는 정보보호(사이버전) 기술의 국가 주도 연구개발 사업 추진 필요성에 대하여 사회적 파급효과가 영향을 미치는지 검증하기 위해서 다음과 같은 가설을 설정하였다.

가설 1. 정보보호(사이버전) 연구개발 사업의 투자 주체 선정에 있어 사회적 파급효과는 국가 주도 연구개발 필요성과 양(+)의 관계를 가질 것이다.

2.3 전략적 중요도와 국방 적용성의 국가주도 연구개발 사업추진 필요성 간 관계

이형진은 국제기술협력 결정요인을 연구한 결과, 국방기술의 중요도와 상대적 기술수준은 국제기술협력 필요성과 양의 관계에 있고, 국방기술의 기술성숙도와 국제기술협력의 필요성은 음의 관계에 있는 것으로 분석하였다[17]. 국제기술협력의 추진도 일종의 국가주도 연구개발 사업이라는 관점에서 정보보호 기술의 전략적 중요도는 국가주도 연구개발 추진 필요성과 양의 관계를 보일 것으로 기대할 수 있다. 본 연구에서는 정보보호 기술의 국가 주도 연구개발 사업 추진 필요성에 대하여 전략적 중요성과 국방 적용성이 영향을 미치는지 검증하기 위해서 다음과 같은 가설을 설정하였다.

가설 2. 정보보호(사이버전) 연구개발 사업의 투자 주체 선정에 있어 전략적 중요도와 국방 적용성은 국가 주도 연구개발 필요성과 양(+)의 관계를 가질 것이다.

III. 연구방법

3.1 민군 기술분류 연계 및 유망기술 선정

3.1.1 민간과 국방 기술분류 연계

국방 IT 유망기술 선정을 위한 기존 연구[6]는 전문가 인터뷰 방식을 통해 유망기술을 선정한 반면 본 조사에서는 최신 민간 정보보호 기술 목록과 국방 사이버전 기술 목록을 연계하는 민군통합기술목록을 수립하고 이를 유망기술 도출에 활용하였다. 이때 유사기술을 통합하여 기술 중복을 제거하고, 국방 적용성이 전혀 없는 기술을 배제하였다. Table 1은 기존 KIAT, TTA, 국방기술품질원에서 발표한 기술분류 중 중분류 기술을 KISTEP의 국가과학기술표준 분류체계로 매핑한 결과를 보이고 있다. Table 2는 매핑 결과를 바탕으로 중복기술 제거과정을 거쳐 민군 통합 정보보호 기술목록을 도출한 결과를 보이고 있다. 민간의 기술분류는 KISTEP의 분류체계에 근거하여 대분류 수준에서 공통보안, 산업/융합보안, 시스템/네트워크 보안, 서비스/응용보안, 기타 5개 분류로 크게 나뉘고, 국방기술 분류는 공통보안, 시스템/네트워크 보안, 공격 기술 3개 분류로 나뉜다.

민군통합기술목록은 대분류 단계에서 민간/국방 분야에서 공통으로 갖고 있는 공통보안과 시스템/네트워크 보안은 그대로 연계하고, 민간에만 있던 산업/융합보안은 기술적 고유성이 약한 융합부분은 제외하고 명칭을 물리 보안으로 변경하여 대분류로 편제하였다. 서비스/응용 분야는 국방 적용성 검토시에 적

Table 1. KIAT-TTA-DTaQ technology mapping results based on National Science and Technology Standard Classification System

KIAT		TTA		DTaQ	
{1}	Network intrusion prevention solution	(1)	Password and Its use	〔1〕	Malware collection / analysis / detection technology
{2}	Host intrusion prevention solution	(2)	Device authentication	〔2〕	OS security technology
{3}	Password safety verification solutions	(3)	Integrated authentication scheme	〔3〕	DBMS security technology
{4}	Malware corresponding solutions	(4)	OTP-based authentication	〔4〕	Data(Contents) security technology
{5}	Authentication and Access control solutions	(5)	Anonymous authentication	〔5〕	Wireless network security technology
{6}	Security dedicated chipset	(6)	Identity management	〔6〕	Intrusion detection / reasoning technology
{7}	Wired and wireless access security solutions	(7)	Privacy protection solutions	〔7〕	Intrusion prevention / response technology
{8}	RFID / USN security solutions	(8)	Objectionable information prevention	〔8〕	Encryption technology
{9}	IT security management solutions	(9)	Smartphone Security	〔9〕	Password application technology (Key management technology)
{10}	Privacy protection solutions	(10)	Cloud security	〔10〕	Security protocol technology
{11}	Knowledge content security solutions	(11)	Cyber attack response	〔11〕	HW security technology (Security-chip technology)
{12}	Security control services	(12)	Malware corresponding solutions	〔12〕	Quantum cryptography technology
{13}	Application service security solution	(13)	Smart network	〔13〕	Rights management (access control) technology
{14}	Video security	(14)	Future internet security	〔14〕	Integrated security management technology
{15}	Facility security	(15)	IoT / M2M security	〔15〕	Security assessment(CC)
{16}	Biometrics	(16)	Knowledge content security solutions	〔16〕	Digital forensic technology
{17}	Car security	(17)	Financial security	〔17〕	Cyber command and control / training skills
{18}	Aviation / maritime security	(18)	Smart grid security	〔18〕	Vulnerability collection / analysis technology
{19}	Robot security	(19)	Cloud applications	〔19〕	Secure encryption technology using a quantum computer
				〔20〕	Malware design and manufacturing technology
{20}	Health security	(20)	Big Data security	〔21〕	Cryptanalysis / response technology
{21}	Construction security	(21)	Web services security		
{22}	Defense security	(22)	Biometrics		
{23}	Smart Grid security	(23)	Security assessment(CC)		
{24}	Industrial Infrastructure security	(24)	Security management(ISMS)		

National Science and Technology Standard Classification System (KISTEP)
Common Security Technology
Network Systems Security Technology
Service / application security technology
Industry / convergence of security technologies
Etc. information security technology

Table 2. Civil-military integrated information security technology list

Category			Element Technology	KIAT	TTA	DTaQ
Main	Mid					
Common ground security technology	Encryption technology	1	Encryption technology			[8]
		2	Password and Its use	{3}	(1)	
		3	Secure encryption technology using a quantum computer			[19]
	Password Application Technology	4	Authentication and Access control solutions	{5}		[13]
	Security protocol technology	5	Security protocol technology			[10]
	Security HW Technology	6	IoT / M2M security		(15)	
		7	Robot security	{19}		
		8	Security dedicated chipset	{6}		
		9	HW security technology (Security Platform technology)			[11]
	Quantum cryptography technology	10	Quantum cryptography technology			[12]
	Rights management technology	11	Identity management		(6)	
		12	OTP-based authentication		(4)	
	Integrated security management technology	13	IT security management solutions	{9}		[14]
		14	Security control services	{12}		
	Security assessment(CC) technology	15	Device authentication		(2)	
		16	Security assessment(CC)		(23)(24)	[15]
		17	Cyber-Electronic warfare security SW technology			[15]
	Digital forensic technology	18	Digital forensic technology			[16]
	Cyber command and control / training technology	19	Cyber command and control / training skills			[17]
	Privacy protection technology	20	Privacy protection solutions	{10}	(7)	
	Vulnerability collection / analysis technology	21	Vulnerability collection / analysis technology			[18]
System/Network security	Malware collection and analysis techniques	22	Malware corresponding solutions	{4}	(12)	[1]
	Security OS technology	23	Security OS technology			[2]
	DBMS security technology	24	DBMS security technology			[3]
	Data(Contents) security technology	25	Web services security		(21)	
		26	Application service security solution	{13}		
		27	Health security	{20}		
		28	Knowledge content security solutions	{11}	(16)	[4]
	Wireless network security technology	29	RFID / USN security solutions	{8}		
		30	Smart network		(13)	
		31	Smartphone Security		(9)	
	Intrusion detection / reasoning technology	32	Intrusion detection / reasoning technology			[6]
	Intrusion prevention/correspondence technologies	33	Network intrusion prevention solution	{1}		
		34	Intrusion prevention technology			[7]
		35	Intrusion response technology			[7]
		36	Cyber attack response		(11)	
		37	Wired and wireless access security solutions	{7}		[5]
		38	Host intrusion prevention solution	{2}		
	Big data/Cloud security technology	39	Big Data security		(20)	
		40	Cloud security		(10)	
Physical security	Monitoring Technology	41	Construction security	{21}		
		42	Video security	{14}		
		43	Car security	{17}		
	Facility security	44	Facility security	{15}		
	Recognition Technology	45	Biometrics	{16}	(22)	

용성이 거의 없는 것으로 조사되어 대분류에서 제외하고 하위기술 중 적용성이 있는 일부 기술은 시스템/네트워크 보안기술 등으로 편제하였다. 결과적으로 기존 KISTEP 5개 대분류에서 민군통합기술 목록은 3개 대분류로 조정되었고, 이를 기반으로 중분류, 요소기술 순으로 기술명과 명세를 검토하여 동일 기술끼리 연계/통합 작업을 거쳐 통합목록을 수립하였다.

Table 3은 민간기술 조사대상이 된 한국과학기술기획평가원(KISTEP), 한국산업기술진흥원(KIAT), 한국정보통신기술협회(TTA) 기술분류의 특성을 정리하고 있다[12][13].

Table 3. Civil IT technology Classification Characteristics

구분	KISTEP	KIAT	TTA
Source	National Science and Technology standard classification system	2012 Industry Technology Roadmap	2013 ICT Standardization strategy map
Competent ministries	Ministry of Science, ICT and Future Planning	Ministry of Commerce, Industry and Energy	Civil
Merit	Standardized formal classification scheme	More specifically identified technologies	Integrated with the latest classification
Disadvantages	The latest classification not reflected	Redundancy among technology	Limited to the required technical standards

3.1.2 국방 사이버전 분야 유망기술 선정

민군통합기술목록을 기반으로 국방 분야에 적용 가능한 유망기술을 선정하는 방법론을 고안하였다. 유망기술 선정 절차는 아래와 같다.

1) 민군통합기술목록의 기술을 대상으로 세 가지 속성(국방 적용성, 전략적 중요성, 파급효과)에 대한 전문가 설문조사를 수행한다. 유망기술 선정 설문조사는 국내 산학연 전문가 12명이 참석하였으며 Table 4는 유망기술 선정 시에 참여한 전문가의 소속을 나타내고 있다. 참여 전문가들은 민군통합기술목록의 45개 요소기술에 대해서 세 가지 속성값을 설문조사로 답변 후, 전문가토론회를 통해서 설문 조사결과를 상호 조율하였다.

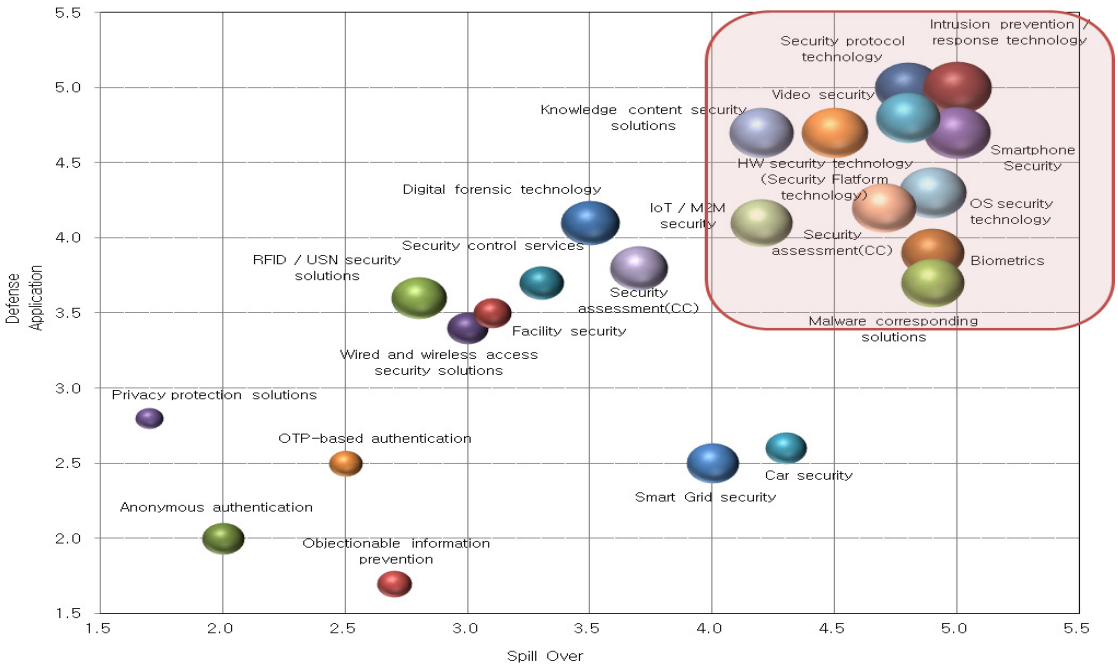
Table 4. Survey Participants Statistics for Promising Technologies Selecting

Industry	Academia	ADD	Military	Research Institute
1	2	2	1	6

Table 5. Defense Information Security Promising Technology Derived Results

Mid Category	Promising Technology	MAUT Result
Security protocol technology	Security protocol technology(VPN) (5)	8.5
Security HW Technology	IoT / M2M security (6)	7.4
	HW security technology (Security Flatform technology) (7,8,9)	8.1
Security assessment(CC) technology	Security assessment(CC) (16)	7.9
Vulnerability collection / analysis technology	Vulnerability collection / analysis technology (21,22)	7.7
Monitoring Technology	Video security (43)	8.3
Recognition Technology	Biometrics (46)	7.5
Security OS technology	Security OS technology (23)	8.2
Data(Contents) security technology	Knowledge content security solutions (28)	7.9
Wireless network security technology	Smartphone Security (31)	8.4
Intrusion prevention/correspondence technologies	Intrusion response technology solution (32,33,34,35,36,38)	8.7

2) 다원속성효용이론(Multi-Attribute Utility Theory, MAUT) 산식을 적용하여 기술간 비교우위를 평가한다. 적용산식은 아래와 같다. 이때, 파급효과 e는 기술/경제/사회적 파급효과를 각각 조사한 다음 이를 산술평균해서 도출하였다.



Legend : x-axis (Spill Over), y-axis (Defense Application), Size of Circle (Strategic Importance)

Fig. 1. Defense Information Security (Cyberwarfare) Promising Technology Derived Results

Table 6. Survey Results of Investment Entity / Development Actors for the Defense Information Security Promising Technology

	Defense Application	Strategic Importance	Spill over Effect (Tech.)	Spill over Effect (Econo.)	Spill over Effect (Social)	Investment Subject (Gov.)	Investment Subject (Private)	Development Subject (Industrial)	Development Subject (Research)
Intrusion response technology solution	5	5	5	5	5	80	20	20	40
Security protocol technology(VPN)	5	4.9	4.9	4.7	4.9	80	20	10	70
IoT / M2M security	4.1	4.5	5	5	5	70	30	20	60
Video security	4.8	4.7	4.7	5	4.8	70	30	20	70
Vulnerability collection / analysis technology	3.7	4.6	4.9	4.8	4.9	70	30	20	60
Security assessment(CC)	4.2	4.7	4.7	4.6	4.8	50	50	20	60
Smartphone Security	4.7	4.8	5	5	5	40	60	50	40
Security OS technology	4.3	4.9	4.9	4.9	4.9	30	70	50	40
Biometrics	3.9	4.6	4.5	4.5	4.6	30	70	50	40
HW security technology (Security Flatform technology)	4.7	4.8	4.7	4.4	4.5	30	70	60	30
Knowledge content security solutions	4.7	4.7	4.2	4.1	4.3	20	80	40	50

$$\text{총점}(P) = \sqrt{m^2 + t^2 + e^2}$$

m : 국방 적용성 (5점 척도)
t : 전략적 중요성 (5점 척도)
e : 기술적/경제적/사회적 파급효과 (5점 척도)

다원속성효용이론(MAUT) 방법론은 다수의 평가 대상에 대해서 우선순위를 부여하기에 적합하고 평가가 단순하여 평가자의 평가 거부감을 줄일 수 있다. MAUT는 Von Neumann과 Morgenstern의 효용이론을 기반으로 Keeney와 Raiffa에 의하여 구체적인 기법과 적용 절차 등이 정립되었다. MAUT는 정성적인 요인들도 종합적으로 고려할 수 있다는 점과 요인들 간의 상대적 중요도를 구할 수 있다는 점에서 그 유용성이 높다. 또한 연구 과제의 우선순위 선정 시에 비교적 단순하고, 직관적이며, 편리하게 가중치를 할당할 수 있다는 장점이 있다. 이때 우선순위 계산식으로 가장 많이 쓰이는 방식이 선형 가중 합(weighted linear average)이다. 다원속성효용이론은 기존 유망기술 선정 연구에서 많이 쓰인 방식으로 본 연구에서도 다원속성이론을 적용하여 유망기술을 도출한다[15]. 유망기술 선정 연구간 차이점은 다원속성이론 적용 시에 속성값들을 어떻게 선정하고 속성값 간의 가중치를 어떻게 조정해서 유망기술을 적절히 선정하느냐에 있다. 본 연구에서는 국방분야와 민간분야 기존 연구에서 공통적으로 조사한 기술의 중요성과 기술의 기술적/경제적/사회적 파급효과에 국방 적용성을 추가하여 속성값을 선정하였다. 이때 각 속성값의 가중치는 1로 동일하게 설정하였다. 본 연구는 3년마다 수행되는 국방 IT 조사활동의 일환으로 이번에 선정된 유망기술에 대해서는 3년 뒤에 국방정보화 기획업무 관련자들에게 만족도 평가를 실시할 예정이다. 이를 통해 유망기술 선정 적절성을 평가하고 그 결과를 다시 속성값과 가중치 설정에 반영하도록 할 예정이다.

3) 다원속성효용이론 산식을 적용한 평가결과를 도식화 하고 상위 N개 기술을 유망기술로 선정한다.

민군통합기술목록에서 요소기술 45개를 대상으로 다원속성효용이론산식을 적용하여 유망기술 11개를 도출하였다. Table 5와 Fig.1은 각 유망기술별 MAUT 계산결과를 표와 그림으로 나타낸다. 유망기술 도출결과 사이버전에서 C4I 체계 방어를 위한 필수기술로 인식되는 침입대응솔루션 기술이 가장 높은 점수로 선정되었다. 이외 디지털 포렌식 기술 등 중장기적으로 유망기술로 인식되는 기술들은 유망기술 선정 구분선 근처에서 선정되지 못하였다.

3.2 투자/개발 주체결정에 영향을 미치는 요인 분석

3.2.1 데이터

유망기술 선정의 세 가지 요소 중 투자/개발 주체 선정에 영향을 미치는 요소가 무엇인지 파악하기 위해 "국방 적용성/전략적 중요성/파급효과"와 "투자주체/개발주체"의 관계에 대해 분석하였다. 분석 데이터는 국방기술품질원에서 2014년 4월부터 2014년 9월까지 국방 IT 유망기술 선정을 위해 조사한 사이버전 분야 11개의 유망기술 데이터를 기반으로 하였다.

3.2.2 변수

독립변수는 국방 적용성, 전략적 중요성, 파급효과로 설정하였다. 국방 적용성은 유망기술이 추후 국방무기체계(전력지원체계) 개발에 얼마나 적용될 수 있는지를 나타내고, 전략적 중요성은 해당 유망기술 확보의 전략적 중요성을 나타내고, 파급효과는 유망기술의 기술적/사회적/경제적 파급효과의 평균을 나타낸다.

종속변수는 선정된 유망기술이 정부 주도의 투자가 필요한지를 나타내는 정부투자필요성, 정부 주도의 개발이 필요한지를 나타내는 정부개발필요성 두 가지로 설정하였다. 정부투자필요성은 연구개발 재원을 100% 정부 예산으로 투자하는 경우를 말하고, 정부개발필요성은 정부출연연구기관(국방과학연구소)에서 연구개발을 주관해야할 필요성을 말한다.

3.2.3 측정방법

독립변수는 유망기술 선정에 활용된 세 가지 속성값을 활용하였고, 종속변수는 11개의 유망기술에 대하여 11명의 국내 전문가를 선정하여 정부투자필요성, 정부개발필요성 정도를 100점 단위로 설문조사하였다. 독립변수와 종속변수의 설문조사 결과는 Table 6과 같다. 본 연구에서는 종속변수와 독립변수와의 가설을 검증하기 위해 상관관계 분석을 실시

하였다.

IV. 실증분석 결과

4.1 유사도 분석 결과

유망기술 선정요소(국방 적용성, 전략적 중요성, 파급효과)와 투자/개발 주체와의 정량적 비교분석을 통해 연관성을 추정할 수 있었으며 표본은 민군통합 기술목록에서 도출된 45개 기술에 대한 산학연 전문가 12명의 유망기술 선정 설문조사 결과와 유망기술 전문가 11명에 대한 투자/개발 주체결정 설문조사를 활용하였다. Table 7은 독립변수와 종속변수 간의 상관계수 계산결과를 보이고 있다.

일반적으로 $0.0 \leqq |r| < 0.2$는 상관관계가 없으며, $0.2 \leqq |r| < 0.4$는 약한 상관관계, $0.4 \leqq r < 7.0$은 상당한 상관관계, $0.7 \leqq r < 1.0$은 매우 강한 상관관계로 해석한다[18]. 본 연구에서는 일반적인 판단 기준에 따라 피어슨계수 0.4 이상부터 유의미한 상관관계가 있는 것으로 판단하였다.

상관계수 계산결과, 세 가지 파급효과와 투자주체(정부) 간에는 양의 관계에 있다고 판단이 가능하다. 특히 사회적 파급효과는 0.6922로 거의 0.7에 근사하게 조사되어 매우 강한 상관관계에 있다고 판단된다. 또한 파급효과 중 사회, 경제, 기술 순으로 상관계수가 높게 조사되어, 정부 주도의 연구개발 필요성은 사회적, 경제적, 기술적 파급효과 순으로 중요하게 인식되고 있음을 알 수 있다.

Table 7. The correlation coefficient between independent variables and the dependent variable

Correlation Properties		Correlation Coefficient
Economical Spillover Effect	Governmental Investment	0.6368
Social Spillover Effect	Governmental Investment	0.6922
Technical Spillover Effect	Governmental Investment	0.6273
Defense Application	Governmental Investment	0.1652
Strategic Importance	Governmental Investment	0.0902
Economical Spillover Effect	Governmental R&D	0.2113
Social Spillover Effect	Governmental R&D	0.2557
Technical Spillover Effect	Governmental R&D	0.0662
Defense Application	Governmental R&D	-0.0267
Strategic Importance	Governmental R&D	-0.3113

4.2 사회적 파급효과와 정부투자 필요성과의 상관관계

상관계수가 가장 높게 조사된 사회적 파급효과와 정부투자 필요성 간에 상관관계 분석을 실시하였다. 사회적 파급효과와 정부투자 필요성은 피어슨 상관계수가 0.6922이고, 양방검정 유의도는 0.018, 공분산은 3.618로 분석되었다. 두 변수는 0.05 레벨에서 상관관계가 있다고 할 수 있다. 따라서 가설 1은 지지되었다. 전문가들은 정부투자 연구개발 과제 선정에 있어 사회적 파급효과를 중요한 요소로 판단하고 있음을 확인할 수 있었다.

Descriptive Statistics

	Mean	Std. Deviation	N
Social_Spillover_Effect	4.791	.2300	11
Governmental_Investment	51.82	22.724	11

Correlations

		Social_Spillover_Effect	Governmental_Investment
Social_Spillover_Effect	Pearson Correlation	1	.692*
	Sig. (2-tailed)		.018
	Sum of Squares and Cross-products	.529	36.182
	Covariance	.053	3.618
	N	11	11
Governmental_Investment	Pearson Correlation	.692*	1
	Sig. (2-tailed)	.018	
	Sum of Squares and Cross-products	36.182	5163.636
	Covariance	3.618	516.364
	N	11	11

*. Correlation is significant at the 0.05 level (2-tailed).

Fig. 2. Correlation Analysis Result of Social impact and the need for government investment

4.3 국방 적용성과 정부투자 필요성과의 상관관계

국방 적용성과 정부투자 필요성은 피어슨 상관계수가 0.1652이고, 양방검정 유의도는 0.627, 공분산은 1.673로 분석되었다. 두 변수는 0.05 레벨에서 상관관계가 없다고 할 수 있다. 따라서 가설 2 중 국방적용성과 정부투자 필요성의 상관관계 가설은 기각되었다.

Descriptive Statistics

	Mean	Std. Deviation	N
Defense_Application	4.464	.4456	11
Governmental_Investment	51.82	22.724	11

Correlations

		Defense_Application	Governmental_Investment
Defense_Application	Pearson Correlation	1	.165
	Sig. (2-tailed)		.627
	Sum of Squares and Cross-products	1.985	16.727
	Covariance	.199	1.673
	N	11	11
Governmental_Investment	Pearson Correlation	.165	1
	Sig. (2-tailed)	.627	
	Sum of Squares and Cross-products	16.727	5163.636
	Covariance	1.673	516.364
	N	11	11

Fig. 3. Correlation Analysis Result of Defense applicability and need for government investment

국방 적용성이 높다는 이유만으로는 정부 주도 연구개발과제로 채택될 수 없다고 전문가들이 판단하고 있음을 알 수 있다. 국방 적용성이 높은 경우에도 민간의 기술력이 높고 민수시장 기회가 많다면 민간 주도의 연구개발로 기술을 확보할 수 있을 것이다.

4.4 전략적 중요성과 정부투자 필요성과의 상관관계

전략적 중요성과 정부투자 필요성은 피어슨 상관계수가 0.09이고, 양방검정 유의도는 0.792, 공분산은 0.309로 분석되었다. 두 변수는 0.05 레벨에서 상관관계가 없다고 할 수 있다. 따라서 가설 2 중 전략적 중요성과 정부투자 필요성의 상관관계 가설은 기각되었다.

Descriptive Statistics

	Mean	Std. Deviation	N
Technology_Importance	4.745	.1508	11
Governmental_Investment	51.82	22.724	11

Correlations

		Technology_Importance	Governmental_Investment
Technology_Importance	Pearson Correlation	1	.090
	Sig. (2-tailed)		.792
	Sum of Squares and Cross-products	.227	3.091
	Covariance	.023	.309
	N	11	11
Governmental_Investment	Pearson Correlation	.090	1
	Sig. (2-tailed)	.792	
	Sum of Squares and Cross-products	3.091	5163.636
	Covariance	.309	516.364
	N	11	11

Fig. 4. Correlation Analysis Result of Strategic Importance and need for government investment

전략적 중요성이 높다는 이유만으로는 정부 주도 연구개발과제로 채택될 수 없다고 전문가들이 판단하고 있음을 알 수 있다. 전략적 중요성이 높은 경우에도 민간의 기술력이 높고 민수시장 기회가 많다면 민간 주도의 연구개발로 기술을 확보할 수 있을 것이다.

V. 결 론

본고에서는 국방 사이버전 분야에 적용 가능한 우수 민간 정보보호 기술을 선정할 수 있는 새로운 조사방법론을 제시하고 이를 기반으로 조사결과를 분석하였다. 새로운 조사방법론은 민간 정보보호 기술과 국방 사이버기술을 연계하기 위한 민군통합기술목록을 제안하였고, 여기에 다원속성효용이론을 적용하여 유망기술을 도출하였다. 기존 국방 IT 조사활동에서는 민간 IT 기술 분류와의 연계가 연구된 적이 없었기 때문에 본 연구결과는 추후 국방 IT 조사활동에 많은 기여가 있을 것으로 기대된다.

도출된 유망기술에 대해서 투자주체와 연구개발 주체에 대한 전문가 설문조사를 실시한 결과 사회적 파급효과와 정부주도 연구개발은 양의 관계에 있음을 확인할 수 있었다. 이 분석결과를 기반으로 추후 국방 핵심기술 R&D 투자방향 설정 시에 경제적/기술적 요구로 인해서 민간에서 자연적인 투자가 예상되는 기술들 보다는 공세적 대응기술 등과 같이 민간의 수요는 없으나 사회적 파급효과가 큰 기술들 위주로 개발을 추진해야 할 것으로 판단된다.

국방 적용성과 전략적 중요성이 투자/개발 주체와 상관관계가 낮은 것으로 조사된 것은 국방 적용성이 높거나 전략적 중요성이 크다고 무조건 정부 주도로 투자/개발될 것이 아니라 민간 주도로 투자/개발된 후 국방 분야로 Spin-On(역 도입)될 수 있음을 시사한다. 즉 국방 적용성이 높은 기술이라 하더라도 민간의 기존 보유 기술수준이 높고 시장성도 높은 기술이라면 민/군간 공동 기술개발 로드맵 수립 후에 민간 정출연/산업체에서 기술을 개발하고 국방에 적용하는 방안도 고려할 수 있을 것이다.

References

[1] Paul Cornish, D. L., Dave Clemente and Claire Yorke, On Cyber Warfare, A Chatham House Report, 2010.

[2] Schreier, F., On Cyberwarfare, DCAF, 2012.

[3] Service, E. P. R., Preparing for Cyber Warfare?, European Parliamentary Research Service, 2014.

[4] Kim, ChulWhan, et al., "A Study on the Activation of Dual Use Technology Program," Journal of the Military Operations Research Society of Korea 32(1): pp. 13-35, 2006.

[5] Ann, Youngsoo, et al., Enhancing Civil-Military Technology Integration through Institutional Improvement, KIET Research Report 2013-689, 2013.

[6] Kwon Kyeong-Yong, et al., "A Study on the Technology Level Survey and Analysis of Problems for improving the Defense IT Survey," Journal of The Korea Society of Computer and Information 18(1): pp. 111-121, 2013.

[7] KyungJin Park, et al., Defense Science and Technology Survey 2013, DTaQ research report, 2013.

[8] Hongseock Go, et al. Understanding and Practice of the Level Research of Defense Technology, Hyeongseol Publisher, 2010.

[9] Kwon Kyeong-Yong, et al. 2012 Defense IT Technology Survey. Ministry of National Defense, DTaQ, 2012.

[10] KyungJin Park, et al. 2015 Defense IT Technology Survey. Ministry of National Defense, DTaQ, 2014.

[11] Kim, MyungKwan, et al., R & D planning for the research planning assessment practitioners, The Korea Industrial Technology Association, 2007.

[12] Lee, GieNyung, "R & D key strategic industrial technology roadmap for future industries upbringing," ie magazine 19(3): pp. 29-33, 2012.

[13] Jeon, DeockJoong, et al., "ICT Standardization strategy map Ver. 2013 Study on the standardization target item and the international standardization strategic direction of information security," Korea Communications Society General Conference (Summer) 2013: pp. 523-524, 2013.

[14] Won, Yoojae, et al., "Issues and R&D Promoting Direction of Information Security," Information & Communications Magazine 31(1): pp. 48-51, 2013.

[15] Chang, Tai-Woo, et al., "A Study on the R&D Planning of Railway IT Convergence Technology," Journal of Society for e-Business Studies 18(4): pp. 67-82, 2013.

[16] Seong, Jieun, et al., "Possibilities and Challenges of Social-impact Analysis for R&D," Journal of Science and Technology Studies 14(2): pp. 49-84, 2014.

[17] Lee, Hyungjin, et al., "What Drives International Technology Cooperation?: Joint R&D Cooperation in Defense Core Technology," Technology Innovation 21(2): pp. 355-373, 2013.

[18] Nam, Chunhyun, et al., Contemporary Statistics, Shinyoung-Sa, pp. 313, 2005.

〈저자소개〉

이 호 균 (Ho-Gyun Lee) 정회원
1998년 2월: 경북대학교 컴퓨터공학과 학사
2000년 2월: 경북대학교 컴퓨터공학과 석사
2011년 3월~현재: 고려대학교 정보보호대학원 박사과정
2000년 2월~2002년 11월: LG정보통신 생산기술연구소
2002년 12월~2007년 6월: 한국전자통신연구원 정보보호연구단
2007년 7월~현재: 국방기술품질원 기술기획부 기술조사팀 선임연구원
〈관심분야〉 사이버전, 정보보호, 국방과학기술기획, 기술수준조사

이 경 호 (Kyung-Ho Lee) 종신회원
1989년 8월: 서강대학교 수학과 학사
1997년 8월: 서강대학교 정보통신대학원 석사
2009년 8월: 고려대학교 정보경영대학원 박사
1994년 2월~현재: 삼성그룹, nhn, 시큐베이스 등 근무
2011년 9월~현재: 고려대학교 정보보호대학원 부교수
〈관심분야〉 위험관리, 정보보호컨설팅, 정보보호 및 개인정보보호정책

임 종 인 (Jong In Lim) 종신회원
1980년 2월: 고려대학교 수학과 졸업
1982년 2월: 고려대학교 수학과 석사
1986년 2월: 고려대학교 수학과 박사
현재: 청와대 안보특별보좌관, 고려대학교 정보보호대학원 교수, 개인정보보호위원회 위원, 한국인터넷진흥원 비상임이사, 방송통신위원회 기술자문위원, 대검찰청 디지털수사자문위원장, 경찰청 사이버테러대응센터 자문위원, 국가정보원 국가보안협의회 위원
〈관심분야〉 사이버 국방, 정보법학, 디지털포렌식, 개인정보보호, 융합기술보안