5

민 · 군 겸용 정보보호기술의 발전전략

한국정보보호산업협회 ▌**백 의 선**

신정부 출범 이후 민간 IT 기술정책은 서비스사업의 생산력 제고와 새로운 비즈니스 모델의 창출을 위해 IT 산업과 타 산업분야간 융복합화에 중점이 두어지고 있으며, 국방분야에서는 「국방개혁 2020」에 따른 정보전 대응과 정보과학정예군 양성을 역점적으로 추진되고 있다. 따라서 2010년대를 향한 우리나라 민 · 군 양분야의 당면 현안은 IT의 중심적 활용이며, 보이지 않는 성장엔진으로서 소프트웨어 및 정보보호기술의 효과적인 획득방안을 들 수 있다.

1. 서 론

민간 IT 부문에서는 방송 · 통신 서비스의 융합과 RFID/USN 등과 새로운 무선기술이 실용화되면서 기업의 업무처리 환경이나 국민들의 생활양식(Life- style)이 단순 정보사용에서 지식기반형으로 빠르게 전환되고 있다.[1] 또한 우리가 일상적으로 사용하는 많은 IT 서비스들은 전력, 교통, 금융 등 국가 중요정보통신시설(CII; Critical Information Infrastructure)과 연동되어 운용되고 있다. 그러므로 국가 기반시설이 사이버 테러나 정보전 등 외부로부터 불법적인 공격을 당해 운용이 중단되는 긴급 상황이 발생한다면, 국가의 모든 생산 및 소비활동이 마비되어 국민경제에 엄청난 손실과 혼란이 초래될 것이다.

국방분야에서도 첨단 IT 기술의 도입이 가속화되고 있다. 센서기술을 활용한 유도 무기의 정확도 향상, 군수 정보화에 의한 보급 효율 향상, 시뮬레이션을 통한 군사 교육훈련의 효율화 등 IT 기술을 활용한 군사혁신(이하 RMA; Revolution in Military Affairs)[2] 성과가 광범위하게 나타나고 있다. 즉 RMA의 진전은 21세기의 세계 전쟁 패러다임을 과거 산업사회의 대량파괴전 양상에서 첨단 과학기술을 활용한 정밀 타격, 정보전 양상으로 혁신적인 변화를 초래하고 있다.

미국은 1990년 걸프전 이래 정보 · 지휘 통신망의 광대역화, 초고속화를 실현하여 각급 부대 지휘관의 상황파악 능력을 향상시키고, 종래 개별 운용되던 무기체계를 통합 네트워크을 통해 운용함으로써 정보전 수행 능력을 획기적으로 향상시켜 나가고 있다. 한국합동참모본부(1999)도 "정보우위를 달성하기 위해 자국의 정보 및 정보체계를 보호하며, 적의 정보체계를 교란 및 파괴시키기 위하여 실시하는 광범위한 제반 활동"으로 정의한 바 있으며[3], 국방부는 2005년 9월 정보전 수행능력 향상을 위한 「국방개혁 2020」을 발표하고 이를 추진 중에 있다.

John Arquilla & David Ronfeldt(1997)는 민 · 군 양분야에 대한 사이버 공격 혹은 사이버 위협을 망라하여 대상이 되는 정보통신 기반시설의 종류에 따라 사이버전(Cyber war)과 네트워크 중심전(NCW; Network centered war)으로 구분한다. 사이버전은 지휘 및 통제체제와 같은 군사용 정보통신망이 목표이며, 네트워크 중심전은 전력망, 송유망, 교통 · 통신망 등과 같은 민간 정보통신망이 군사적 공격목표가 된다.[4] 김기정 등(2003)도 정보전을 "정보우위를 달성하기 위해 자국의 군사부문 및 민간부문의 정보체계를 보호하며, 적의 군사부문 및 이를 지원하는 민간부문의 산업 인프라, 국가 정보통신 기반구조를 무력화시키기 위한 광범위한 제반 활동"으로 정의하고 있다.[5]

---

1) IT 기술은 자유로운 정보 유통을 실현하여 전통적 경계의 붕괴(Blurred traditional boundaries), 저렴한 생산 또는 전쟁비용(Low entry cost), 정보사용에 의한 통제능력 확대(Expanded role for perception management), 타자(他者)와의 협력관계 형성 및 유지의 어려움(Difficulty with building and sustaining coalitions) 등 기존 관념을 변화시켰다.

2) RMA란 군사력의 목표달성 효율을 획기적으로 향상시키기 위해 IT기술 중심의 핵심기술을 군사분야에 활용함으로써 발생하는 무기체계, 조직, 전술, 훈련 등을 포함하는 군사상의 혁신을 말한다.

3) 윤석준, 미래전에서의 해군 정보작전과 발전방향, 공군교리발전 세미나 자료 p. 23, 1999. 9.

4) John Arquilla & David Ronfeldt, In Athena's camp: Preparing for conflict in the information age, RAND pp. 44-45, 1997.

5) 김기정, 원영대, 정보화시대의 국가 안보, 연세대학교 pp. 6-44, 2003.

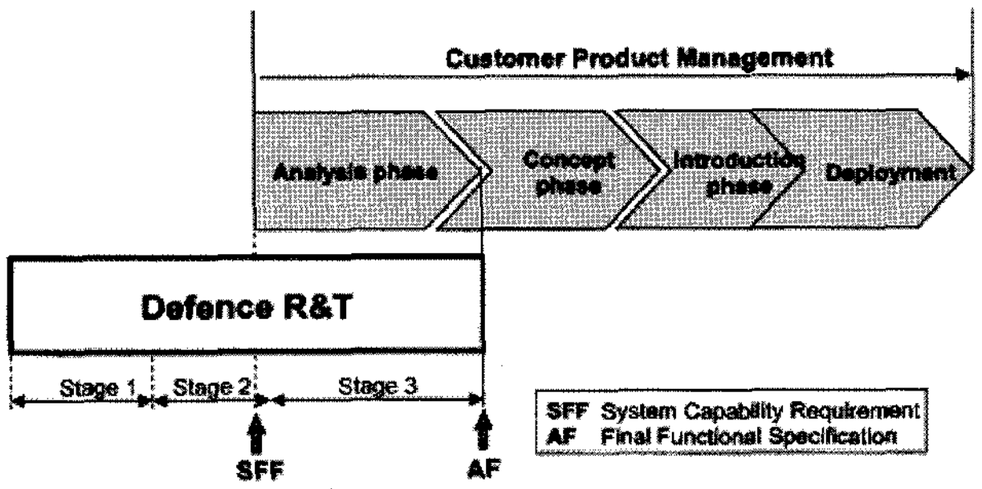
이처럼 민과 군의 모든 IT 기반 시설이나 시스템은 적국이나 반정부단체, 심지어는 사회에 적의를 품은 개인까지도 네트워크를 통해서 목표 정보체계를 공격하거나 마비시킬 수 있으므로 정보전은 사이버 테러, 사이버 공격, 사이버 범죄와 용어 정의상 구별하기가 매우 어려운 상황이다. 따라서 주요국들은 IT 시스템의 안정 운용에 필요한 정보보호기술과 IT 시스템의 고도화에 필요한 핵심 S/W 기술개발 능력의 확보를 산업경제 발전과 안전보장 환경 유지에 필수적인 민·군 겸용기술로 인식하고 이를 확보하기 위한 R&D 기능 강화와 더불어 정보보호 획득체계 수립에 박차를 가하고 있다.[6)]

우리나라는 지난 20여년간 정보화 정책을 꾸준히 추진하여 인터넷의 초고속화, 3세대 휴대전화의 보급, 통신·방송망의 융합 등 IT 강국으로서의 차세대 기술 노하우를 축적하였다. 그러나 국내 IT 산업은 H/W나 시스템 기술은 선진국 수준에 도달하였으나, 핵심 부가가치를 창출하는 S/W 기술이나 정보보호기술은 85% 수준의 기술격차를 보여주고 있다. 또 정보보호 분야의 경우에는 국방, 정부 및 공공, 민간이 각기 다른 정보화 및 정보보호 목표를 추진하는 관계로 상호간 기술협력이나 정보교류가 미흡한 실정이다.

따라서 본고에서는 S/W기술 특히 정보보호기술을 국가경제 신성장 동력인 동시에 국가안보시스템의 고도화에 필수적인 Spin-on형 민·군 겸용기술으로 인식하고, 이를 효과적으로 획득하기 위한 국가 차원의 기술개발 전략을 살펴보기로 한다.

2. 정보보호기술의 민·군 겸용적 특징

민과 군에서 필요로 하는 과학기술을 논할 경우, 대부분의 경우 하나의 기술지식(Technological Knowledge)에 공통적 기반을 두고 있기 때문에 기본적으로 민·군 겸용의 기술적 특성을 지닌다. 그러나 실용화 단계에서는 민과 군의 기술의 사용목적이 뚜렷하여 기술기획 단계부터 상호간의 원할한 연구협력이나 기술교류가 이루어지지 않고 있는 실정이다. Branscomb, L.M.(1993) 등은[7)] 국방 과학기술과 민수 과학기술이 설



출처: 이춘근 외, 민군 기술협력 촉진방안, 과학기술정책연구원, 2006. 10.

그림 1 민수기술과 국방기술의 연구개발 과정상 차이

계유인의 시장성, 개발주기의 장·단기성, 기술공유의 전유성(全有性) 등에서 각기 다른 기술 특성을 갖는다고 본다. 또한 연구개발단계에서 민수분야는 「기초연구, 응용연구, 개발, 상용화」라는 R&D(Research & Development) 단계로 추진되지만, 국방기술 분야는 그림 1과 같이 「기초 및 응용연구」와 제품생산 단계인 「체계개발」이라는 R&T(Research & Technology)단계로 추진된다. 즉, 연구개발 전 과정에 있어서 민·군의 연구개발 방법은 다르지 않으나, 국방기술은 생산단계에서 민·군간 제품 규격의 차이 등으로 실용화 범위가 극히 제한된다는 것이 크게 다르다.[8)]

그럼에도 불구하고 민·군 겸용 기술정책은 투자된 예산의 기술개발 성과를 민·군 양분야에서 극대화할 수 있다는 장점으로 인하여 기술개발과제 선정에서는 다소의 어려움이 있었지만, 민과 군 어느 한 분야의 기술적 우위를 활용하여 기술개발 기간을 단축하거나 연구개발 투자의 효율을 제고한다는 기본 목적은 시대와 상황 변화에 관계없이 일관성이 유지되고 있다.

본고에서 다루는 정보보호기술은 기술기획단계부터 민과 군이 동시에 사용할 수 있는 기술의 겸용성(Duality) 혹은 다용성(Multi-use)을 갖고 있고, 기술활용단계에서는 국가정보원으로부터 CC인증이나 보안적합성을 검증을 받아왔다는 점에서 전형적인 민·군 겸용기술이라 할 수 있다.

3. 국내 정보보호기술개발 동향

정보보호기술은 기본적으로 정보통신망이나 정보시스템상에서 처리되는 정보의 기밀성(정보유출방지), 무결성(데이터 위·변조 방지)을 유지하고 시스템의 가

6) 미국은 9.11 테러 이후 본토안보부(DHS)를 중심으로 생체정보를 활용한 개인식별 기술 등 차세대 정보보호기술을 개발 중이며, 일본은 2005년 4월 내각관방에 정보보호센터(NISC)를 설치하고, 2006년에는 민관의 정보보호체계 구축을 위해 133개 시책으로 구성된 「Secure Japan 2006」을 추진하고 있다. EU도 정보보호 구심점 역할을 담당할 ENISA(European Network and Information Security Agency)를 설립하고 네트워크와 정보보호 관련 문제를 연구하고 있다.

7) Branscomb은 설계유인, 혁신형태, R&D강도, 제품주기, 기술우선순위, 생산률, 생산과 R&D와의 관계, 기술공유의 9개 항목별로 민과 군 기술간의 특성 차이를 조사했다.

8) 국가과학기술자문회의, 민군겸용기술 개발 활성화 방안 p. 1, 1997. 5.

용성을 보장하는 기술이다.[9] 더욱이 최근에는 통신과 방송 네트워크가 하나의 통합 아키텍처로 융합되는 융복합 진화, 금융부문 네트워크 등 국가기간망에 대한 상호 연결성과 접근성 증가, IT 네트워크의 글로벌화와 제3국을 통한 우회 공격 증가 등으로 인하여 정보보호 기술개발 투자 확대의 시급성도 그만큼 높아지고 있다.

현재, 해커들은 각종 IT 시스템에 대한 우회 공격이나 S/W 취약점을 이용한 제로데이 공격 등 불법적 행위를 가하고 있다. 따라서 이에 대한 방어기술 및 방법론 개발이 정보보호기술 개발의 주류를 이루고 있는 한편에서, 새로운 IT 기술의 안전·신뢰성을 보완하기 위한 혁신적 기술개발이 이루어지고 있다. 현재 우리나라 정보보호기술과 선진국 기술간의 격차는 약 1.5년 낙후되어 약 85% 수준에 도달한 것으로 평가되는데, 주요 기술개발 동향을 정리하면 다음과 같다.

첫째, 정보보호 환경의 최대 변화요인으로는 방송, 인터넷, 통신 등 서비스망별 운영체계가 All-IP망으로 통합되는 광대역통합망(BcN)의 등장을 들 수 있다. 이를 위해 새로운 사이버 공격에 대비한 BcN 환경의 이상 징후 수집 및 분석, 침해사고 진단 및 예측, 실시간 침해사고 대응을 위한 「BcN 환경을 고려한 침해사고 조기 예·경보 시스템」을 개발하고, 사이버 공격이 발생하기 이전에 발생 가능한 주요 위협들을 식별하고 잠재적 위험을 예보하는 사이버기상예보(Cyber Weather Forecasting) 기술 연구와 BcN 일부 서비스의 장애나 침해사고시 피해가 전체 망으로 확산되는 것을 방지하기 위한 침해사고 격리 메카니즘의 개발이 요구된다.

둘째, RFID 이용 보급과 직결되어 있는 USN 보안기술은 TinyOS, Zigbee 등 소형 센서의 보안 OS 및 프로토콜 관련 보안기술 등이 활발히 진행 중이나, 보안관리 및 보안미들웨어 등 서비스 기술 표준화 측면에서 아직 초기 단계에 수준에 머물고 있다. 미국은 CENS의 환경 감시, NIST의 지진 관측, ZigBee의 주택 및 공장 제어 등과 함께, USC, UCLA, MIT, 버클리 등의 대학을 중심으로 텔레매틱스와 연관된 USN 서비스를 추진하고 있다. 우리나라도 이에 대한 기술개발의 추진이 시급하다.

셋째, 공개형(Open) 및 임베디드 S/W 정보보호 품질보증체계를 구축하기 위하여 주요 소프트웨어의 안전성을 설계 단계에서부터 확보할 수 있도록 신뢰 소프트웨어(Trusted Software) 안전기준 마련 및 검증체계가 구축되어야 한다. 최근 NIST 중심으로 Software Security Testing 및 Software Assurance Testing Tool에 대한 연구가 매우 활발하게 진행되고 있으며, 특히 Software Functional Testing 부문은 자동화되어 가고 있는 추세이다.

넷째, 디지털 증거를 쉽게 접근할 수 있는 단말기의 디지털 포렌직 기술이 개발되고, RFID, 센서뿐 아니라 각종 Embeded System 형태의 디지털 기능이 부가된 백색가전 기기에서의 디지털 증거 수집 및 분석 기술이 개발되고 있다. 미국은 포렌식 도구의 신뢰성 검증, 증거물(데이터)의 고속 검색을 지원하는 DB 구축을 정부지원하에 추진 중이며, 디지털 증거 분석 지원 기관 설립 등의 인프라를 구축하고 있다.

다섯째, 정보보호기술 국제 표준화 동향이 활발하게 진행되고 있다. 현재 ETRI, KISA 등이 국내 전자서명, 바이오인식 및 암호, RFID 보안, 다자간의 통신보안을 중심으로 ISD/IEC, IETF, ITU등에 국제 표준(안)을 제안하고 있다. 또한 관련 국제표준의 개발이 신규서비스 시장창출과 연결되도록 하는 노력이 이루어지고 있다.

4. 미·일의 정보보호 기술정책 동향

단순 해킹수준을 훨씬 넘어선 현시점에서 사이버 공격이나 테러에 대한 대응 정책은 9.11 테러를 경험한 미국에 의해 선도되고 있다. 미국의 사이버 보안 연구개발 연방정부 세부계획은 향후 우리가 중점을 두어야 할 정보보호 정책방향을 제시해 주고 있다. 이 계획은 2007 회계년도 미 행정부 연구개발 예산 우선순위에 대한 각서와 2005년 대통령 정보기술자문위원회(President's Information Technology Advisory Committee: PITAC) 의 보고서, 2002년에 제정된 사이버 보안연구개발법(the Cyber Security Research and Development Act 2002) 에서 제시한 내용들을 일정 부분 포괄하고 있다. 이 계획에서는 다음과 같은 10개의 권고안을 제시하고 있는데, 주요 내용은 다음과 같다.

1) 사이버 보안 전략 및 정부기관의 수요에 따른 연방정부 R&D 투자와 장기적 관점에서 민간부문에서의 보완 프로젝트 추진

2) IT 시스템의 전반적 보호 및 정보보증 수준을 높이기 위한 혁신적 접근방법 연구와 위기 대응능력 배양을 위한 R&D 추진

3) 사이버 보안 및 정부기관 간 연구개발을 개별 연방정부 및 정부기관 간 예산 우선순위에 두고, 임무 관련 R&D 필요요건을 충족시킬 수 있는 가이드라인

9) 정보화촉진기본법 제2조에 의하면 정보보호란 정보의 수집·가공·저장·검색·송신·수신 중에 정보의 훼손·변조·유출 등을 방지하기 위한 관리적·기술적 수단을 말한다.

개발

4) 사이버 보안 부문 R&D의 정부기관 간 조정 및 협력 유지 지원

5) 시스템 구축 초기부터 보안사항을 고려하여 불안정한 현재 인프라를 대체할 수 있는 안전한 차세대 기술지원 연구개발 추진

6) 광컴퓨팅(optical computing), 양자 컴퓨팅(quantum computing), 임베디드 컴퓨팅(embedded computing)과 같은 신기술의 보안수준 평가

7) 이 계획의 기술적 우선순위 및 투자 분석을 민간부문과 협력하여 사이버 보안 및 정부기관 간 R&D 우선순위에 대한 로드맵 개발에 활용하며, 기술 및 투자수준의 차이를 해소하기 위한 기관간 활동 조정

8) IT 요소, 네트워크 시스템 보안 등을 측정하기 위한 새로운 방법과 기술의 개발 및 적용

9) 연방정부와 민간부문 주요 인프라 운영자 간 커뮤니케이션 향상 및 조정 등을 통해 더욱 효율적인 협력체계 구축

10) 보다 안전한 차세대 인터넷 개발 및 테스트, 구축 등을 위해 정부, IT 산업, 연구자 및 민간부문 이용자, 국제 협력 파트너들 간 폭넓은 협력체계 구축

이 연방계획에는 비록 투자 수준이나 예산에 대한 세부적인 내용은 포함되지 않았지만, 미국의 IT 기반을 보다 효율적으로 보호하기 위한 정부기관간 협의 기반을 마련했다는 점에서 의의가 있다고 할 수 있다. 아울러 일반 인터넷 망뿐만 아니라 첨단 과학 기술과 비상 커뮤니케이션 시스템을 통제하고 조정하는 IT 인프라 보호를 위해 연구개발 투자 효과를 극대화할 수 있는 정부차원의 구체적 청사진을 제공하고 있는 것으로 평가된다.

한편, 일본 정부도 정부의 웹 사이트에 대한 웹서버 공격, 컴퓨터 바이러스 등을 이용한 정보탈취, 중요 IT 인프라의 장애에 의한 업무 일시 마비, 스파이웨어 등 IT 이용에 따른 불안감 해소 등을 목표로 2006년 「Secure Japan」을 발표하였다. 이 계획은 크게 민·관 각 IT 주체의 정보보호 인식제고, 첨단 정보보호기술의 개발, 정부·공공기관의 사이버 테러 대응기능 강화, 민·관 정보보호 협력체계 강화 등 4대 기본방향을 제시하였으며, IT 이용주체별 실천목표를 다음과 같이 제시하고 있다.

1) 정부는 중요 IT 인프라 안전기준 정비, 분야별 모의 사이버 훈련 강화, 공공기관의 정보보호 대책 개선, 중장기 정보보호 대책 수립, 사이버테러에 대한 정부기관의 긴급대응 능력 강화, 정부기관의 정보보호 전문가 육성을 중점 추진한다.

2) 지방자치단체는 지자체 정보보호가이드라인의 보급, 정보보호 감사 시행, 「가칭 지방자치단체 정보공유분석센터」 설립, 정보보호 전문가 육성을 중점 추진한다.

3) 기업은 기업 정보보호가이드라인의 보급, 성능이 우수한 정보보호 제품 및 서비스 보급, 기업 정보보호 전문가 육성, 취약성 정보의 조기 제공체제 구축 등을 중점 추진한다.

4) 개인은 정보보호 교육 강화, 정보보호 홍보 및 정보제공 환경 조성, 개인이 저렴하게 구입할 수 있는 정보보호 서비스 및 제품의 공급을 목표로 한다.

이상에서 보는 바와 같이 우리나라의 u-정보보호 기본전략을 포함하여 미국과 일본이 제시하고 있는 2010년까지의 정보보호 분야의 공통적인 주요 정책과제로는 IPv6, RFID, 광컴퓨팅과 같은 IT 기술 패러다임의 변화에 대한 기술적 대응과 외부로부터의 불법적 공격에 대비한 IT 주체간 정보공유 및 협력 체계 구축, 그리고 다원화된 IT 사용주체별 정보보호전문가 체계적 육성을 들 수 있다.

5. 결 론

글로벌 경제환경과 국내 군사환경의 인터넷 의존도가 날로 증대되고 있는 가운데, 민·군 정보환경의 고도화를 더욱 촉진시키고, 독자적인 정보보호체계를 운용하기 위해서는 먼저 산·학·연을 비롯한 민간과 정부, 군(軍)간의 기술협력 및 정보교류가 필수적이다. 군의 입장에서도 필요한 정보보호기술을 조기에 확보하기 위해서는 민간의 정보보호 기술력을 활용하는 것이 추가적 자원의 투입없이 목표를 달성할 수 있는 효과적 전략이라 할 수 있다. 반면, 민간기업의 입장에서는 국방 정보보호사업에 적극 참여할 경우, 새로운 시장의 확보와 더불어 정보보호 원천기술에 대한 기술 노하우를 축적할 수 있다는 장점을 활용함으로써 장기적으로 글로벌 경쟁력을 확보할 수 있는 기폭제 역할을 할 수 있을 것으로 기대된다.

이를 위해서는 먼저, 국방 및 민수 양 분야에서 활용 가능한 정보보호 기술 및 임베디드 S/W 기술의 개발을 전담할 연구조직이 필요하다. 현재 한국전자통신연구원(ETRI)과 한국정보보호진흥원(KISA) 일부에서 정보보호기술 개발을 담당하고 있으나, 대부분이 상용화를 전제로 한 기술이거나 전자서명, 침입차단 등 정책기술에 한정되어 있어 민·군간 기술교류가 매우 제한적이다. 따라서 1~2년 이내의 단기 수요는 국방관련 연구기관이 담당하는데 비하여, 정보보호 및 임베디드 S/W 기술 전담 연구조직은 3~5년의 중

장기 연구개발을 담당토록 하여 기능상 중복을 방지해야 한다. 또한, 이 연구조직을 중심으로 범 부처적인 기술기획위원회를 운영하여 민·군 겸용 S/W 기술 로드맵을 확정하고, 매년 핵심 기술수요를 예보하여 민간 기업이 로드맵상의 핵심기술을 확보하여(자체개발 또는 특화연구센터에서 기술이전) 군 사업에 직접 참여하거나 핵심기술별로 특화된 민간 수요를 창출하는 역할을 담당하도록 할 필요가 있다.

현재까지 제기되고 있는 민·군 겸용의 주요 정보보호기술 분야로는 선진 정보기관의 정보탈취에 효과적으로 대처하기 위해 암호기술 등 우리 고유의 핵심기술을 확보하고, 해킹, 바이러스 유포 등 사이버테러에 대한 대응기술, 유사시 공격자의 정보시스템을 무력화시킬 수 있는 공격기술을 들 수 있다. 세부 연구과제로서는 사이버공격 위협 예측에 필요한 이종 데이터 융합(Heterogeneous Data Fusion)기술, 전력, 가스, 급수, 댐 및 대규모 플랜트의 자동제어를 위한 안전한 자동제어(SCADA) 시스템의 보안기술, 트래픽 수집, 분류 및 분석을 통한 침입탐지 기술 개발, 공격자 역추적 기술 개발 등을 들 수 있다. 이 밖에 Lightweight 침입탐지 센서 개발, secure 클러스터 기술 개발, 침입감내(Intrusion Tolerant) 네트워크 기술 개발, 사이버전 모의 훈련 프로그램 개발 등 정보전 관련 기술을 선도할 수 있는 전략기술 개발도 시급한 과제로 지적되고 있다. 이밖에도 민·군 통합 S/W 기술인프라 연구주체의 중요 기능으로서는 리눅스 채택의 활성화 및 관련 정보보호기술의 개발, 정보보호 가이드라인의 개발 및 보급, 국제표준화 주도 등을 들고 있다.

끝으로 미래 정보전 수행에 필요한 IT기술 분야로 광역 통합전장 운영 및 관리전(지휘통제력), 장사정 초정밀 미사일전(정밀타격력), 초고속 입체 기동전(기존 주전력), 정보 수집 분석처리 및 방해 방호전(정보력) 등 4개 분야를 들 수 있다. 이를 위한 핵심 S/W 기술로는 COE, MND-AF와 같은 소프트웨어 상호 운용성 보장 기술 외에 무기체계 및 정보시스템 구축에 필수적인 내장형 실시간 소프트웨어에 관한 기술, 신뢰적인 정보전송을 가능하게 하는 기술, 그리고 정보 보안을 유지할 수 있는 기술 등이 거론되고 있지만, 이에 대해서는 좀 더 구체적인 작업이 이루어져야 할 것이다[10].

10) 현재 방위사업청에서는 대학중심의 국방 S/W설계 연구특화센터를 지정하고 2015년까지 9년간 이 분야의 R&D 활동을 지원할 계획임.

참고문헌

[1] 사이버테러정보전학회, 국가사이버전 대응방안, 2007. 2.

[2] 일본 노무라연구소, 「2010년의 IT 로드맵」, 백의선 역, 2007. 1.

[3] 일본 정보시큐리티센터, 「일본의 정보시큐리티 정책현황」, 2007. 2.

[4] ETRI 정보보호연구단, 정보보호 기술 및 제품 경쟁력 분석, 2006. 8

[5] 일본 정보시큐리티정책회의, 「Secure Japan 2006」, 2006. 6.

[6] 정보통신부·정보보호진흥원, 「u-정보보호 기본전략」, 2006. 11.

[7] 이춘근외, 민군 기술협력 촉진방안, 과학기술정책연구원, 2006. 10.

[8] 김기정, 원영대, 정보화시대의 국가 안보, 연세대학교 세미나 자료, 2003.

[9] 김의순, "C4I 체계의 의사결정지원체계 개념 및 추진과제", 국방정책 연구, 2004 봄호, 2004. 3.

[10] 방위사업청, "국방과학기술 정책의 현황과 전망", STEPI 세미나 자료, 2006. 9.

[11] 최인수 외, "국방 정보보호체계 획득업무 개선, 국방정책연구", 2004 봄호, 2004. 3.

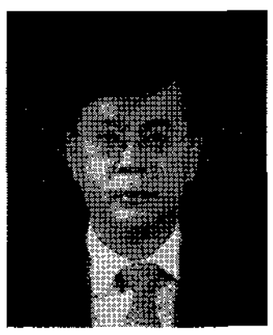
[12] 일본 방위청, 「정보 RMA에 관하여」, 2000. 9.

[13] President's Information Technlogy Advisiory Committe, Cyber Security; A Crisis of Prioritization, 2005. 2.

[14] H. Matsumoto, "미국의 군민양용 기술프로젝트 분석", 일본국제경제학회, 2005.

[15] Todor Galev, "Questioning Dual-Use Concept", IAS-STS Work in Progress Workshop, 2003. 3.

[16] John Arquilla & David Ronfeldt, "In Athena's camp: Preparing for conflict in the information age", RAND, 1997.



백 의 선

일본 요코하마국립대 경영학석사
한국과학기술원(KAIST) 경영공학박사
ETRI 연구기획실장, 지식경영연구부장
KISA 정책기획단장, 경영혁신단장
국방대학교 '07 안보과정 졸업
(現) 한국정보보호산업협회 상근부회장
관심분야 : 기술경영, R&D관리, 산업정책
E-mail : espaik@kisia.or.kr