정보·사이버전 유형과 정보기술 측면의 보안전략 발전방향

안 정 철*　권 혁 진*

◈ 목 차 ◈

1. 서　론

사이버 공간은 이미 10 여년전 부터 제 4의 전장으로 강조 및 인식되고 있으며 침해 및 공격기술은 IT 기술과 함께 급속히 발전하고 있다. 이와 더불어 해킹을 통한 국가/군사자료 유출, 은행/전산망 마비 등의 외부적인 위협과 발전소 무력화 시도인 스턱스 넷과 같이 다방면적이고 불특정다수 및 특정 시스템을 공략하는 광범위한 공격들이 증가 하고 있다. 본 논문에서는 이러한 정보·사이버전의 유형과 정보기술 측면의 보안전략을 검토하여 대응전략에 대하여 고찰하고자 한다.

2. 정보·사이버 개념 및 목적

오늘날의 정보·사이버전은 기존의 단순한 서버 해킹/침해 등을 벗어나 사이버 첩보전, 테러전, 심리전, 물리적 연계전등의 전방위적인 개념을 포괄하고 있다. 전쟁으로의 사이버전은 기존의 물리적 전쟁과는 다르게 가상의 공간을 이용하여 정보절취, 위/변조, 체계마비 등의 정보우세와 물리적, 심리적 공격의 위협을 포괄하고 있다.

본고에서는 사이버스파이[2]Cyber Espionage) + 사이버전쟁[3]Cyber Warfare) + 사이버테러[4]Cyber Terror)를 합쳐서 정보·사이버전으로 정의한다.

정보·사이버전은 비대칭전력으로 분류되며, 공격자 식별과 피해대상을 구분하기가 어렵다는 특징을 가지고 있다. (표 1)과 같이 기존의 재래식(물리적) 무기와는 다른 피해 양상을 보인다. 주로 정보의 절취에서부터 국가 시스템마비, 위성해킹을 통한 위성 소유권 탈취와 같은 물리적 공격 등 다양한 용도로 활용되고 있다.

(표 1) 사이버전의특징 및 용도

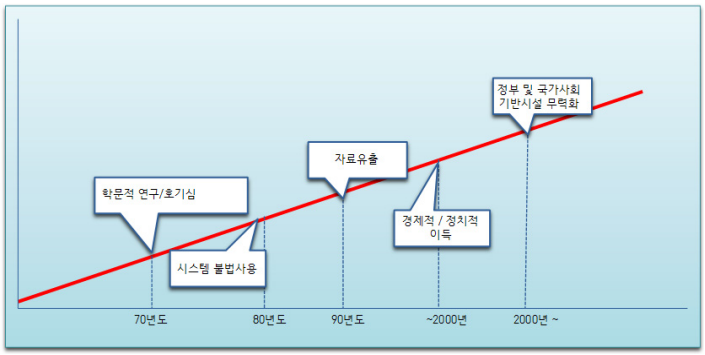
사이버전 특징	비대칭전력 물리적 무기와는 다른 피해 양상 피해대상 구분이 모호 공격자 식별 및 유무확인의 어려움
사이버전 용도	정보 절취 정보의 위/변조 기반체계 무력화 국가마비 물리적 피해강요

* 한국국방연구원

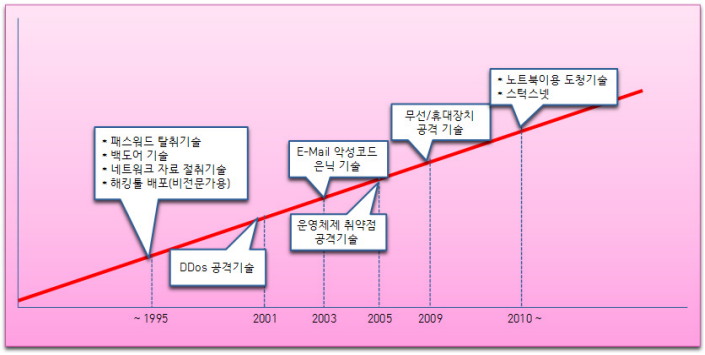
1) Cyber Espionage : 인터넷 등의 사이버 공간에서 회사의 정보를 빼내 다른 회사로 팔아 넘기는 활동을 하는 컴퓨터 산업 스파이

2) Cyber Warfare : 인터넷 등의 사이버 공간에서 다양한 공격수단을 활용하여 적의 정보체계를 교란/거부/통제/파괴하는 등의 공격과 이를 방어하는 활동

3) Cyber Terrorism : 인터넷 등의 사이버공간상의 정부/민간기관의 정보시스템에 침입하여 장애 또는 파괴 등의 피해를 야기시키는 해킹/바이러스유포/DDOS등의 가상공간상의 범죄 행위



(그림 1) 공격목적의 변화



(그림 2) 공격기술의 변화

3. 사이버 공격 패턴의 변화

가. 공격목적의 변화

사이버 공격은 (그림 1)과 같이 70년도 학문적인 연구와 호기심으로부터 시작되어 시스템과 SW에 불법적으로 사용되고 있었다. 최근 10년 전 부터 국가기반 네트워크 공격을 통한 사회 혼란이나 기반체계 중지 등의 목적으로 개인적인 호기심으로 부터 국가기반을 흔드는 목적으로 패턴이 변화되고 있다.

나. 주요 공격기술의 변화

사이버 공격 목적의 변화의 흐름에 맞추어 공격기술도 (그림 2)와 같이 변화하게 되었는데, 사용자 몰래 정보를 절취하는 기술로부터 스턱스넷 등과 같은 기반시설 공격기술까지 변화하고 있다.

4. 정보·사이버 공격 유형 및 사례

정보·사이버전의 공격유형을 살펴보면 초창기의 공격유형인 정보절취(옥션, Nate 등의 개인정보 유출) 패턴에서 부터 2차 이라크전 당시의 EMP탄 공격 및 최근의 이란 브세르 핵발전소 스턱스넷과 같은 시설물에 대한 공격과 같은 물리적 공격까지 유형별로 크게 5가지로 분류할 수 있다.

가. 정보의 절취

- 개인정보 수집(Auction, Nate 등)
- 미군 시스템 개발 중이던 미 군수업체 컴퓨터 해킹으로 2만 여개의 파일 유출(2011년)

나. 정보의 위/변조

- 이스라엘-하마스 분쟁 : 아랍권 해커집단 '팀 이블'이 이스라엘 일간지 와이네트 등 400개이상의 사이트를 해킹·변조했으며, 이스라엘의 가자 침략 부도덕성을 선전하는 정치적 도구로 이용(2008년)
- 시리아 내전(2012) : DDoS/분산서비스공격 및 정보 변조(허위기사 송출 등)

다. 기반체계 무력화

- 1차 이라크전(1991년) 미 국가안보국 컴퓨터 바이러스 침투에 의한 이라크 방공망 교란과 미군에 의한 이라크 정보망 교란 및 사이버심리전
- 코소보전(1993년) 세르비아 해커들이 미군 네트워크 상대로 컴퓨터 해킹 및 바이러스 유포

라. 국가 시스템 마비

- 러시아-에스토니아 사이버전(2007년 4월): 러시아의 사이버 공격으로 에스토니아는 3주간 대통령궁, 의회, 정부기관, 은행, 이동통신 네트워크 등 국가 시스템 전체가 마비

마. 물리공격과 병행

- 2차 이라크전(2003년 3월) : 컴퓨터 해킹, 전자전 장비와 [4]EMP탄을 이용한 이라크 방송, 지휘통신망 및 정보체계 무력화
- 이스라엘-시리아 분쟁(2007년 9월) : 이스라엘 공군기가 시리아 방공망을 뚫고 시리아 영토에 미사일 투하전 정보전 무기를 이용하여 시리아 레이더망 무력화 시도로 추정
- 러시아-그루지아 사이버전(2008년 8월) : 러시아와 그루지아의 영토 분쟁에 앞서 러시아는 2008년 6월 28일부터 사흘 간 그루지아의 정부 홈페이지, 언론사, 포털 사이트 등이 대규모 분산서비스거부(DDoS) 공격을 수행
- 이란 브세르 핵발전소 원격공격(2010년 6월) : 발견된 스턱스넷은 이란 브세르 핵발전소 원격감시제어시스템을 타깃으로 제작되었으며, 당시 외신들은 미국 또는 이스라엘의 등의 국가적인 지원하에 스턱스넷이 개발되었을 것으로 추측함.

5. 정보·사이버침해 현황 및 대응전략

앞 단락에서 구분한 공격유형별 대표적인 공격사례들을 분석하고 이에 대한 예방방법을 제시하고자 한다.

5.1 공격유형별 대표사례

다음과 같이 대표적인 몇 가지 기술로 취합이 된다.

가. 정보절취

1) 사례
   - 북한의 농협 해킹
   - 뉴질랜드-호주 정보망 해킹(2007년 9월)
   - 미국 국방부 해킹(2008년 11월)
   - 중국 정부 컴퓨터 해킹(2009년 4월)
   - 영국RBS 월드페이 해킹(2008)
   - 다국적 석유회사 해킹(2009~2012)
   - 미국 국립오크리지연구소 해킹(2011년 4월)
   - 현대캐피탈 해킹사건(2011년 4월)
   - 네이버/싸이월드 개인정보 유출(2011년 7월)
2) 대표 기술
   - 취약점 공격
   - 악성코드 침투
   - [6]APT 공격

나. 정보위변조

1) 사례 : 일본 반크 홈페이지 해킹(2008년 12월)
2) 대표기술 : 취약점 공격

다. 기반체계 무력화

1) 사례
   - 이스라엘-아랍 사이버전(2009년 1월)
   - 미국 연방항공국 네트워크 해킹(2009년 2월)

4) EMP탄 : 직접적인 파괴 효과보다는 형광등, TV, Computer 등과 같은 전자기기를 무력화 시키는 공격무기

5) APT(Advanced Persistent Threat) 공격 :특정 기업 또는 조직 네트워크에 침투후 활동거점을 확보한 다음 정보를 외부로 유출하는 공격을 총칭

2) 대표기술
- 취약점 공격
- 악성코드 침투

라. 국가시스템 마비

1) 사례
- 북한의 7.7 DDos 공격
- 미국 전력망 해킹(2009년 4월)
- 중국-티벳 사이버전(2009년 3월)

2) 대표기술
- DDoS 공격
- 비인가 장비(취약점) 접속/공격

마. 물리공격과 병행

1) 사례
- 이스라엘-시리아 분쟁(2007년 9월)
- 이란 브세르 핵발전소 원격공격(2010년 6월)

2) 대표기술
- DDoS 공격
- 스턱스넷 기술 적용

5.2 공격기술에 대한 방어와 예방방법

식별된 대표적이 공격기술에 대한 방어와 예방방법은 다음과 같다.

가. DDos(Distributed Denial of Service)/서비스 분산공격 공격 : 공격자가 컴퓨터를 조정할 수 있는 바이러스와 스파이웨어를 유포하여 원하는 시간에 타켓 서버 또는 시스템 등의 공격목표에 방대한 패킷을 보내서 시스템을 마비시키는 공격방법
- 방화벽을 통한 공격 트래픽량 제거
- DDoS 방어존 구축
- iptables명령어 등을 이용한 필터링
- 사용자들의 정기적인 악성코드/바이러스 제거 작업
- [7]NIDS(Nwtwork Intrusion Detection System) 를 이용한 네트워크 트래픽 상시 감시

나. 비인가 장비접속: 기업/기관 내부 네트워크에 인가 받지 않은 노트북, 스마트폰, 스마트패드, 핸드폰 등을 접속을 하여 자료 절치, 파괴, 변조 등의 침해 활동을 하는 공격방법
- 출입자 신원확인 및 이동경로 관리
- 조직 직위 또는 외부 인원의 물리적 접근범위 제한
- LAN/WIFI 보안강화(ip/mac address 강제 적용 및 네트워크 사용권한 제어 프로그램 등의 보안툴 활용)
- 사용자 / 조직별 시스템 접근권한 통제강화
- 자료 유출 방지를 위한 DRM, File 저장통제 등의 툴 사용

다. 컴퓨터 침입 : 바이러스/스파이웨어/에드웨어 등을 이용하여 버퍼 오퍼플로우, IIS(Internet information server) 공격 등을 통한 원격 접속방법
- PC 접근포트 차단(필수 port를 제외한 기타 port 사용제거)
- PC 설치 프로그램 관리 / 비인가 프로그램 설치 제안정책 수립/시행
- 정기적인 시스템 감사 및 취약점 점검
- 정기적인 보안패치
- [8]HIDS(Host-based Intrusion Detection System)을 이용한 시스템 내부 감시/분석

라. 정보의 절취 : 주로 신용카드, 고객정보, 비밀자료 절취 등의 목적으로 사용되는 방법으로 키보드 후킹, 네트워크 패킷복제, Evi Twin (합법적인 네트워크로 위장한 무선네트워크)등을 이용한 정보절취 방법
- 중요자료 전송간 패킷 암호화 전송 (Server -

6) NIDS(Nwtwork Intrusion Detection System) : 네트워크 트래픽을 감시하여 서비스 거부공격(Dos), 포트스캔, 컴퓨터 크랙시도등가 같은 동작을 탐지하는 시스템

7) HIDS(Host-based Intrusion Detection System) : 컴퓨터 시스템의 내부를 감시하고 분석하는데 중점을 둔 호스트기반 침입탐지 시스템의 종류

사용자)
- 키보드 후킹 방지툴 활용
- Wi-fi 무선 적용시 패킷 암호화/별도 사용자 서버간 인증툴 적용

마. 시스템 취약점 공격 : 컴퓨터의 소프트웨어나 하드웨어 및 컴퓨터 관련 전자제품의 버그, 보안 취약점등 설계상 결함을 이용해 공격자의 의도된 동작을 수행하도록 프로그램, 스트립트 등을 이용한 공격행위
- 사전 취약점 점검을 통한 취약점 보완(구축단계에서부터 시스템, 응용체계 전 분야에 걸쳐 취약점 점검)
- 취약점에 대한 보안패치(시스템/상용SW/OS등의 패치)
- 최신 버전의 백신으로 점검
- 침입차단/탐지 시스템 운영
- NIDS를 이용한 포트스캔 등의 패턴 감시

6. 각국의 사이버 대응체계

오늘날의 사이버전은 특정 부서와 기관에서만 준비하고 대응한다고 문제가 해결되는 범위를 초과하고 있다. 따라서 범 국가적인으로 사이버전을 대응하기 위한 조직, 훈련, 규정들을 수립하여 운영하는 국가들이 늘어나고 있다.

미국은 9.11테러이후 사이버 공격의 위력을 핵무기와 동일시하면서 사이버 안보담당 특별보좌관이 신설되는 등 대폭적으로 사이버보안이 강화되었다. 2003년 9월 국토안보부 산하기관으로 미국 전역의 사이버 테러 방지, 경고, 대응을 통합 지휘하도록 국가 사이버 보안부로 창설 하여, 매년 사이버전쟁 모의 훈련을 실시하고 있다.

EU는 정보보안에 대한 유럽 각국의 초국가적 협력을 위해 20004년 유럽 네트워크 정보보안청(ENISA)을 설립해 유럽 각구의 CERT 구축지원 및 우수사례 전파 등의 사이버 테러 대응을 위한 공동 대응체계를 갖추고 있다. 유럽지역의 사이버 테러방지를 위해 NATO(북대서양조약기구) 주도하에 2008년 5월 독일, 이탈리아, 라트비아, 리투아니아, 슬로바키아, 스페인 등 7개국이 참여하여 '사이버테러 방어센터'(The Cooperative Cyber Defence Centreof Excellence)를 설립하는 협정을 맺었다.

영국은 2007년 2월 창설된 국가기반보호센터(CPNI:Centre for the Protection of National Infrastructure)의 정보통신보안단(CESG) 초동 대응팀(Incident Response Team (GovCertUK))에서 보안관제와 유사한 업무를 수행하고 있다.

초동 대응팀은 영국 정부의 컴퓨터 비상대응팀(The UK Govenrnment's Computer Emergency Response Team)을 말하며, CESG의 임무중의 하나인 정부시스템에 대한 전자적 공격의 위험과 후속 여파를 최소화 시키는 기능을 수행한다.

중국은 1985년 국방과학기술정보센터를 설립해 정보전을 연구해 왔으며, 1997년 중앙군사위원회 직속의 컴퓨터바이러스 부대가 설립되었다. 2000년에는 사이버 공격 및 정보교란 모의 훈련 전담부서가, 2003년에는 전자전 부대가 창설되어 운영중에 있다. 2000여명의 유학생들을 기반으로 일명 홍커라 불리우는 민산 해커들을 이용하여 해킹기술 개발 및 외국 정보기관의 자료를 빼내는 임무를 수행중에 있다.

러시아는 연방보안부(FSB) 소속 정보통신정보국(FAPSI)에서 국가기관의 인터넷망에 대해 24시간 모니터링을 실시하고 있다. 사이버 위협징후를 탐지, 분석한 후 같은 소속기관인 정보보안센터(ISC)에 통보, 피해 PC에 대한 사고조사, 취약점 개선 등 대응활동과 공격자 색출활동을 수행하고 있다. FAPSI는 ISP업체를 통해 인터넷망에 [8]'SORM'이란 하드웨어 디바이스를 설치하여 인터넷트래픽에 대해 필터링과 원격제어를 하고 있다.

일본은 2000년 10월 육/해/항공 자위대 통합으로 사이버테러 대응조직을 창설했다. 이듬해에 사이버 테러를 방어하기 위한 장비확보 및 기술 개발비를 방위예산에 특별 편성하여 운영중에 있다. 2001년에는 사이버 전투부대를 창설하는 등 사이버 보안능력을 강

8) SORM : 수사보장체계의 약어로 러시아의 모든 인터넷 서비스 공급업체들이 자체 컴퓨터 안에 블랙박스를 설치해 모든 인터넷 통신을 실시간으로 감시할 수 있도록 만든 시스템

화하고 있다. 그리고「정보시큐리티센터의 설치에 관한 규칙(내각총리대신결정)」에 의거 설립한 '내각관방 정보보호센터(NISC, National Information Security Center)'에서 2009년 1월부터 중앙 성청(省廳)에 대해 24시간 해킹·웜 바이러스 등 사이버위협징후에 대한 모니터링을 실시하고 있다. 탐지된 위협에 대해서는 공격자정보, 공격시간, 공격방법 등을 분석하여 해당 성청(省廳)에 지원하는 업무를 수행중이다.

북한은 1993년 이후로 인민군 총참모부 산하에 관련부대를 창설하였다. 전국적으로 컴퓨터영재의 발굴, 특수교육실시, 중국으로부터 핵심기술 전수, 북한내 인터넷훈련망의 부설, 실전상황의 사이버공격훈련, 중국과 일본 유럽 등지에서 사이버공격 과정들을 매우 치밀하고 전개하면서 사이버테러의 실전능력들을 갖추어 가고 있다. 사회에서 배출된 젊은 인력과 미림대학의 출신들로 조직된 전문사이버전 부대들이 조직개편을 통해 각종 상황에 대비하여 운영되고 있다.

7. 미래 주요사이버공격 예측

첫 번째, 사이버 공격중 가장 적은 지식으로 효과적인 공격이 가능한 DDos공격이다. DDos 공격은 특정 서비스에서 DNS 서버등으로 기반체계 공격으로 확전될 우려가 존재한다. 타 서비스 보다 취약하다고 알려진 DNS 서비스들이 동시다발적으로 공격당할 경우, 정보화시스템이 익숙해져 있는 대다수의 사용자들이 느끼는 혼란은 2009년 7.7DDos 공격을 몇십배로 상회하는 혼란 및 피해를 받을 것으로 추정된다. 이러한 DDos 공격으로부터 서비스를 지키기 위해서는 DDos방어 솔루션 및 DDos 대피소등을 구축하고 활용해야 하겠다.

두 번째는 Stuxnet이다. 이란 브세르 핵발전소 원격공격"처럼 폐쇄망이나 무중단 시스템등의 주요 시설물을 공격대상으로 공격을 수행한다. 사전 탐지 및 차단의 어려움으로 인하여 비인가 장치, 프로그램 설치 통제 및 주기적 보안교육, 모니터링 등의 사전예방업무와 관리 시스템과 시설장비에 사용되는 통신규칙을 지속적으로 파악/차단하는 솔루션 도입 등이 필요하다.

개인소유단말기(BYOD: Bring Your Own Device)공격은 스마트폰의 급속한 보급과 장비의 소형화로 단말기도청/정보절취/접근인증 등의 공격 형태로 증가할 것이다. 예방방법으로 통합관리 솔루션을 이용한 중앙집중형 관리체계구축, 비인가 APP 설치 통제 기술, 기기 성능통제 솔루션 등의 도입이 필요하다.

특정 기업/조직 네트워크에 침투해 활동거점을 마련한 뒤 정보를 외부로 빼돌리는 APT(Advanced Persistent Theat) 공격은 다양한 기술(악성코드, 스파이웨어, 피싱,SQL 인젠션 등)을 이용하고 탐지회피를 위한 Zero-Day 취약점등의 회피기술을 적용하여 사고가 발생 한후에 식별되는 경우가 많기 때문에 지휘부에서 최 말단까지의 보안의식의 고취, CERT 전담팀 구축/운영, 보안관리체계 구축, 자산접근통제, 보안/최신 패치 상시업데이트, 필요시 망분리등의 기술/정책 도입과 더불어 민·관·군 전반의 서비스(신규/기존 서비스)에 신속한 시큐어 코딩(2012.12.1.일부터 행정·공공기관 시스템 개발시 적용) 적용이 필요하다.

목표체계 또는 전방위적인 단말장비에 침투하여 공격자에게 유리한 정보를 위/변조하는 공격방법은 정보화 의존도가 높아질수록 파급효과도 기하급수적으로 늘어 날 수 있다. 예를 들어, 전쟁에서의 정보변조 공격은 군의 C4I체계에 침투된 악성코드가 정보를 왜곡하거나, 국민들이 보는 뉴스, 신문, 스마트폰 등에 위/변조된 정보을 배포하여 전쟁과 관련한 오판을 유도하는 방법으로 사용이 될 수 있다. 이러한 정보의 위/변조 공격은 특성 서비스/체계의 BYOD / APT의 대응전략뿐만이 아니라 국가적인 대응체계가 필요하다.

8. 맺음말

사이버공격 기술의 큰 흐름은 목표체계에 몰래 접근하여 원하는 정보를 절취하는 것에서 무력화 또는 파괴를 하는 흐름으로 변화 하고 있으며, 무력화/파괴의 흐름에 더불어 정보 위변조의 공격패턴이 더욱더 발전될 것으로 보인다. 최근 첨단화된 전쟁은 정보의 중요성을 아무리 강조해도 지나치지 않다. 적대국이 정보를 차단하거나 위/변조를 임의로 처리할 수 있다면 전쟁에서 승리하기가 어려워진다.

정보 사이버전에 대한 대비는 관·군만이 준비를 해

서는 대응이 불가능한 상황에 이르렀다. 사이버전은 국가 총력전이다. 민·관·군이 상호 보완적으로 협력했을 시에만 사이버전에서 유리한 고지 점령이 가능할 수 있으며, 또한 정부는 정보 사이버전 무기 및 방어 체계 개발에 더 많은 투자를 해야 할 것이다.

참 고 문 헌

[1] 남길현, "군의 사이버전 대응체계 현재와 미래", 정보과학회지, 2005.7

[2] 국가사이버안전센터, "사이버 시큐리티", 2008.1

[3] 김승권외 2명, "미래 사이버전 및 대비방안", 정보과학회지, 2008.11

[4] 김영진외 3인, "국가 전산망 보안관제업무의 효율적 수행방안에 관한 연구", 정보보호학회 논문지, 2009.2

[5] 전자신문 미래기술연구센터, "사이버 테러와 IT코리아의 현주소", 2009년 7월

[6] 국방부, "국방정보보호훈련 보호규정", 2009.8.7

[7] 전자신문, "사이버 테러와 IT코리아 현주소", 2009.8

[8] 이상호, "군사전략차원에서 정보·사이버전의 효용성", 세종정책연구, 2010년 6권

[9] 한국형사정책연구원, "사이버안전체계 구축에 관한 연구", 2010-12

[10] 윤규식, "북한의 사이버전 능력과 위협 전망", 군사논단, 제68호, pp.64-95, 2011.

[11] 국방부, "국방정보화업무훈령", 2011.2

[12] 조현숙, "사이버 냉전시대(현현황과 미래과제)", 한국과총 2011-03

[13] 인터넷진흥원, "2010 해킹· 바이러스 현황 및 대응", KISA-RP-2010-0051

[14] 디지털타임즈, "세계 각국의 사이버전", 2011.6.13

[15] 합동참모본부, "정보작전방호태세규정", 2011.8.1.

[16] 임강규, "세계 각국의 사이버 안보 전략과 우리의 정책 방향-미국을 중심으로", KIDA 국방주간논단 2011.9.1

[17] 최광복, "사이버전 대응을 위한 국방 정보보호환경 분석과 보안관리모델 연구방향 고찰", 정보보호학회지, 2011.10

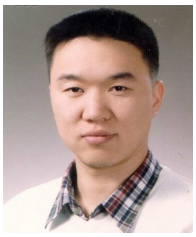
[18] KUSCO, "미국 과학기술분야 동향 보고서", KUSCO 정책동향보고서 2011.8

[19] 국가정보원, "2012국가정보보호백서", 2012

[20] 엄정호, "사이버공간에서 정보우세를 위한 사이버 방위전략", 보안공학연구논문지 2012.10

[21] 국방부, "http://www.mnd.go.kr"

◐ 저 자 소 개 ◑



안 정 철

1998년 밀양대학교 컴퓨터공학과(공학사)
2004년 세종대학교 정보통신대학원(공학석사)
1998년~2003년 해병대 전산실장/개발팀장
2003년~현재 한국국방연구원 IT컨설팅그룹 선임전문연구원
관심분야 : 정보보호정책, 유비쿼터스 구축전략, IT전략컨설팅
E-mail : kkillban@daum.net

권 혁 진

1982년 성균관대학교 산업공학과(공학사)
1989년 성균관대학교 산업공학과(공학석사)
2000년 성균관대학교 산업공학과(공학박사)
1991년~현재 한국국방연구원 획득연구센터 연구위원
관심분야: 정보화수준평가, 청보체계사업평가, IT전략컨설팅
E-mail: khjsjy2001@daum.net