2013 국가 사이버안보 심포지움

미국 사이버안보 대응체제 및 이슈

2013.08.28. (수)

KIDA 한국국방연구원
Korea Institute for Defense Analyses

순 서

- 국내동향
- 미국 사이버안보 대응체제
- 미국 사이버안보 주요이슈
- 한국군 주요이슈
- Q & A

국내동향 (1/4)

- 군 내부체계(국방C4I체계 등) 및 국가급 SCADA에 대한 적의 사이버 공격 시, 군사작전 운용 능력의 심각한 장애로 국가안보 위기가 예상됨
  - 다양한 사이버전 공격 수단/방법 고려 시, 국방정보체계에 대한 사이버공격 가능성이 상존함
    - 주요 국방정보체계는 인터넷과 분리된 내부망 환경에서 운용, 직접적인 원격 사이버공격이 제한
    - 그러나 근간에 웜바이러스(스턱스넷 등)를 활용하여 내부망에 사전 침투한 후 작전시간에 파괴 가능한 수법 등장
    - 2011 '농협'사태와 같이 치밀한 '사이버전 공작'을 통해 국방정보체계에 대한 공격도 가능할 것으로 판단
  - 국가 중요기반시설에 적의 사이버 공격으로 인한 위험성이 증대되고 있음
    - 주요 전력/원자력/산업시설의 SCADA시스템
    - 공공 방송시설/망, 주요 정보통신시설/망 등

국내동향 (2/4)

KIDA

□ 북한은 사이버공격을 평시 활용 가능한 효과적인 '비대칭전력'의 수단으로 사용, 확대 예상됨

◆ 앞으로도 북한 및 주변 위협국의 사이버 공격 대상 및 공격 능력의 시험장이 될 것으로 전망

- ➢ 사이버 공간은 익명성, 실시간 공격자 역추적 제한 등의 특수성 때문에 물리적 공간과 달리 즉시적 반격 제한
- ➢ 또한, 북의 열악한 정보통신 환경은 동등한 수준과 동등한 방법의 반격 및 응징 제한

◆ 북은 다양한 정치적 · 군사적 목적을 달성하고자 다각적인 사이버공격을 수행할 것으로 전망

- ➢ 국가 사이버안보 능력의 신뢰성을 손상시켜 국민의 정부 불신을 유도
- ➢ 금융, 전력 등 국민이 체감하는 국가 기간산업/서비스의 마비 및 장애를 일으켜 사회 혼란 및 경제적 피해 유발
- ➢ 사이버공간을 통한 여론 조작, 정부 불신 조성, 사회갈등 조장
- ➢ 국가 기밀정보 수집 및 전시·유사시 대비 잠재 취약점 분석 등

국내동향 (3/4)

- 특히, 금번 3.20 사이버테러도 북한의 소행으로 중간조사 결과 발표됨에 따라, 軍의 선제적 대응에 문제점이 노출됨
  - 국방부는 당일 사전에 통보받지 못했고, 언론 통해 최초로 인지함 (문화일보('13.3.22))
  - KBS, 신한은행 등 언론/금융 분야 6개 기관 48,000 여대 컴퓨터 파괴, 3.29 복구 완료됨

- 이어진 6.25 사이버공격으로 국민 여론과 국가 기능이 일부 제한됨
  - 청와대, 국무조정실, 한국언론진흥재단 등 서버 다운되며 접속이 이루어지지 않으며, 청와대 홈페이지에 북한찬양 메시지가 붉은 글씨로 도배됨

- 더불어, 북한은 대남 사이버 심리전의 강도를 강화할 전망임
  - 김정은, 작년 '조국통일을 위한 싸움에서 적 와해 사업의 의의와 중요성을 인식하고 적공(심리전) 부문 싸움준비를 철저히 갖출 것'을 지시함 (세계일보('13.3.6))

국내동향: 2013 국방부 업무보고 (4/4)

□ 우리 군의 사이버전 능력 강화 추진

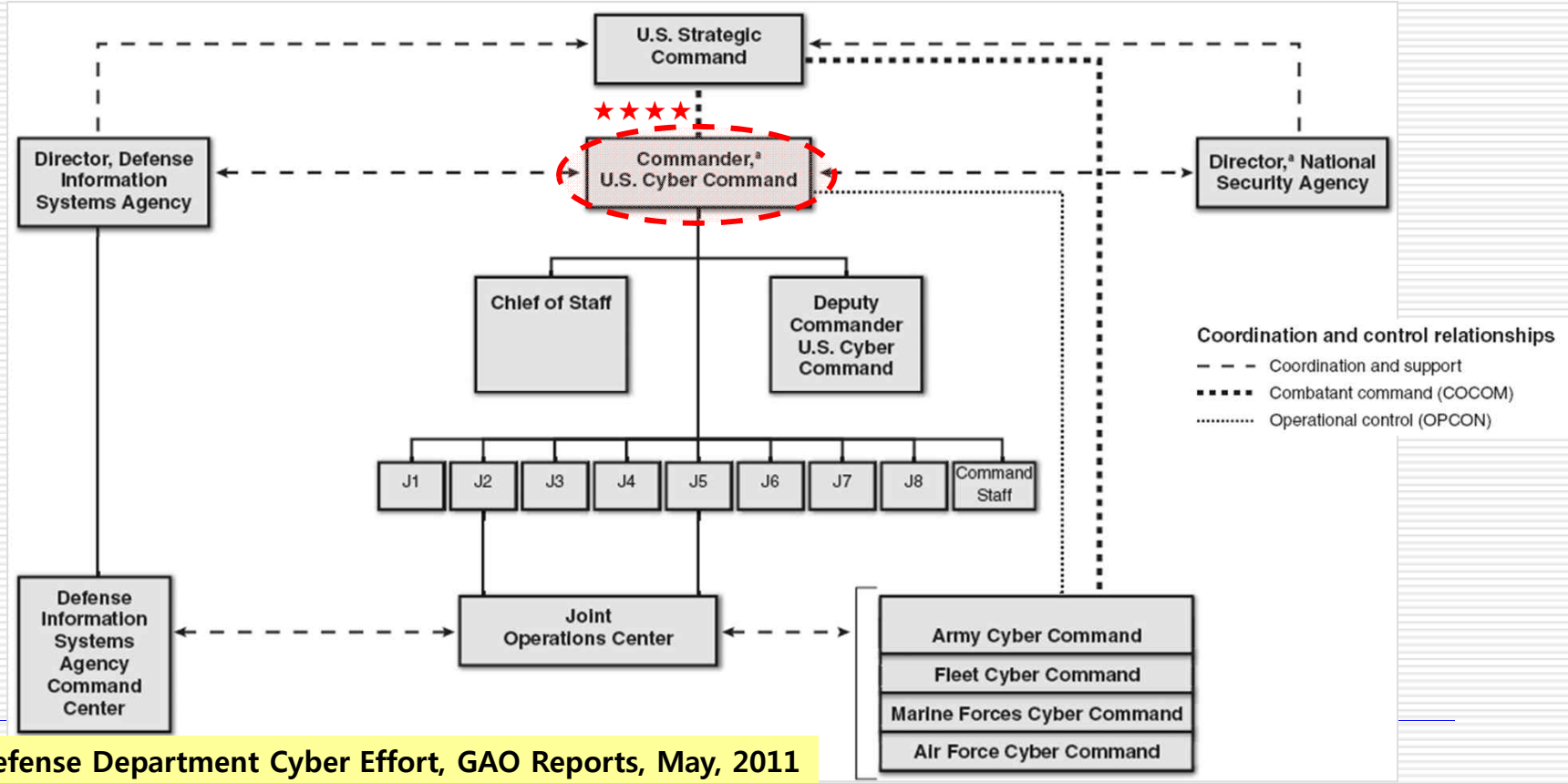
- ◆ 국방 사이버정책 총괄 조직을 보강함
- ◆ 사이버 공격양상에 따른 군사적 대응 시나리오 개발함
- ◆ 사이버전 수행인력 대폭 증원함

美사이버안보 대응체제 (1/3)

□ 미 사이버사령부('09.10 창설)

◆ 사이버전 관련 군사 활동 총괄 조정 • 통제 • 동기화

- ➢ 사이버전 방어(CND) : 군 부대/기관과의 협조 하에 주도
- ➢ 사이버전 공격(CNA/CNE) : 사령부 조정 및 통제



※ 출처: Defense Department Cyber Effort, GAO Reports, May, 2011

美사이버안보 대응체제 (2/3)

□ 제반 사이버전 수행 능력의 균형적인 발전 추진

◆ 방어 : 표면적으로는 사이버전 방어 중심의 정책/제도 발전 지속

구분	주요 정책/제도
전략/정책	• DoD The National Military Strategy for Cyberspace Operation('06) • DoD, Operational Concept for Cyberspace('08) • DoD Cyber, Identity & Information Assurance Strategy Plan('09) • US army's Cyberspace Operation Concept Capability Plan '16-'28('10) • US AirForce Cyberspace Operation(Doctrine Document 3-12)('10) • DoD, Strategy for Operating in Cyberspace('11) 등
국방부/합참 규정 (훈령/지침 등)	• DoDD O-8530.1, Computer Network Defense(CND) • DoDI O-8530.2, Support to Computer Network Defense(CND) • DoD O-850.1-M, CND Service Provider Certification and Accreditation Program • CJCSI 6510.01, IA and CND 등
업무/절차	• SD 527-01, DoD INFOCON System Procedure • CJCSM 6510.01, IA and CND Vol.1(Incident Handling Program) 등

◆ 공격 : 수행체계는 비공개이나, 능력을 지속 발전시키는 것으로 추정

- ➢ '02년 : 부시 대통령은 사이버 공격에 관한 국가 차원의 지침 마련 지시
- ➢ '90년대 중반 이후 : 군사적 수단으로 공격에 대한 법/제도적 연구 지속

美사이버안보 대응체제 (3/3)

- 미국 : 오바마 대통령, 2011년
  - 미국 사이버 공격받을 시 물리적 타격 국제법 검토 지시
- ‘플랜 X’ (사이버전 대비 디지털 전장지도 제작) 프로젝트 착수
  - 미 국방부가 사이버전의 초점을 ‘방어’ -> ‘공격’ 전환하는 프로젝트
  - 향후 약 5년간 1억1,000만 달러 투입 예정
  - 기존의 외부 침입으로부터 국방부 시스템을 지키는 것으로부터, 앞으로는 적의 시스템을 교란·파괴하는 것이 된다는 의미

    => 소극적인 방어에만 치중할 수 없다는 판단에 따른 것
  - 전 세계 사이버공간에 포진해 있는 수백억개의 컴퓨터 도메인과 서버를 총망라해 표시하고 이들의 커넥션을 보여주는 것

    => 이를 통해, 사이버전 전장을 완벽하게 장악하겠다는 계획임

    =>이 지도는 끊임없이 스스로 업데이트함
  - 용도 : ① 타켓을 공격하기 위한 루트

    ② 공격을 받을 때 반격루트를 효과적으로 파악하는데 활용

    => ‘자동 공격시스템’ 도 도입할 계획임

    (조작 없이도 필요할 때 미리 짜인 시나리오에 따라 자동으로 사이버 공격을 가할 수 있는 시스템, 즉 미리 짜인 시나리오에 따라 ‘빛의 속도’로 대응하는 개념)

* 조선일보 (2012.06.01.(금) A16면 국제) 기사

美주요이슈: 사이버사 임무

□ 사이버전장에서의 기회와 도전과제

기 회	직면한 도전과제
세계 인터넷 사용자 • 2000년: 3억 6천 • 2011년: 23억(세계인구의 38%) • 2015년: 한 사람 당 2개 장치 현재 • E-mail = 사용자 32억명 • Facebook 10억 가입자(작년9월 기준) • 80만개의 애플리케이션	• 공격 44% 증가 • 악성코드 60% 증가 • 6만8천개의 해커 이용가능 도구 • Mcafee(美보안업체) 7천5백만 악성코드 관리 • 봇넷에의한 일일 895억개 해킹메일 발송 • 80%의 웹사이트 해킹피해 • 국방부 매월 5만개의 해킹메일 대응

□ 사이버사 임무

국방정보네트워크의 방호와 제 작전들을
지도하기 위하여 행동을 계획·조정·
통합·동기화하고 수행하며,
지시에 의거,
전 영역에서 행동을 가능하게 하고
사이버공간에서의 미국과 동맹국의
행동의 자유를 보장하고 적대세력의
행동을 거부하기 위하여 전 영역 군사
사이버공간작전의 수행을 준비한다.

美주요이슈: 사이버사 과제

- 사이버전장에서 작전을 위한 구상
  - 새로운 교리, 전술, 기술 및 절차를 만들어 내는 작업 추진
- 사이버안보 책임 강화
  - 국가 지도자들에게 신속하게 정보공유, 정부 vs. 민간 정보공유 필요
  - 美 사이버사가 수행할 교전규칙과 기준수립을 정부와 긴밀히 협의
- 잘 준비되고 훈련된 군대 사이버조직 건설
  - 실제의 적에 대해 현실감 및 강력한 모의 사이버 전투 수행
- 사이버방어 가능한 구조 설계
  - 국가 현존은 보호기반 구조로 구성, 네트워크수를 조정 보안성 향상
- 행위 가능환 국제적 사이버안보 시각 능력 확보
  - 언제, 어떻게, 안과 밖에서 위협받고 대응하는지를 항상 알아야 함

美주요이슈: 사이버안보 관련법령 (1/7)

- **Cybersecurity Act of 2012 (CSA)**
  - 사이버안보 전반을 다루고 있음
    - 주요기반시설 보호
    - 정부망 보호
    - 현행기관의 역할 및 권한 강화, 명료화
    - 인력 강화, 연구개발 강화
    - 연방 획득위험관리 전략
    - 정보공유
    - 현황보고 및 인식제고
    - 국제 협력 등
  - 상원의원 공동발의, 2012.02.14
  - 상원에서 통과 시, 하원에서 재표결

美주요이슈: 사이버안보 관련법령 (2/7)

- **Cyber Intelligence Sharing and Protection Act (CISPA)**
  - 민간기업과 정부기관 간 사이버 정보공유 강화가 주된 내용
  - 형식 상 기존 국가안보법(National Security Act of 1947)의 개정
    - 국가안보법에 '사이버위협 정보 및 첨보 공유(Cyber Threat Intelligence and Information Sharing)' 라는 장을 추가하여 정보공유 강화에 관한 내용을 정하도록 함
  - 하원의원 공동발의, 2011.11.30
  - 현재 상원에서 계류 중
  - 상원에서 통과 시, 백악관으로 이송하여 공포, 시행 여부 결정

美주요이슈: 사이버안보 관련법령 (3/7)

- **Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012 (SECURE IT Act)**
  - 민주당 주도의 ‘Cybersecurity Act of 2012’에 대응하는 법안
    - 反규제적 입장에 기반한 사이버안보 추구
    - 민간기업과 정부 사이버위협 관련 정보공유 촉진과 사이버범죄 처벌 강화에 중점을 둠
  - 상원과 하원에서 각각 발의, 2012.03
  - 상원에서 수정 발의, 현재 상원 계류 중

美주요이슈: 사이버안보 관련법령 (4/7)

National Defense Authorization Act of 2012 (NDA)

- 2012 회계연도의 새로운 국방사업 승인과 유관기관에의 권한부여
  - 국방사업의 추진내용 및 예산액 확정, 일부 법률의 개정
- 사이버안보에 대한 내용 일부분으로서 포함됨
- 하원 국방위 의원 공동발의, 2011.04.14
- 하원, 상원 통과, 대통령 서명 공포, 2011.12.31

美주요이슈: 사이버안보 관련법령 (5/7)

- **Advancing America's Networking and Information Technology Research and Development Act of 2012**
  - 형식 상 '고성능 컴퓨팅법(High-Performance Computing Act of 1991)' 의 개정임
    - 국가 고성능 컴퓨팅 프로그램을 네트워킹 및 정보기술 연구개발 프로그램으로 변경
  - 하원의원 공동발의, 2012.01.27
  - 하원 본회의 통과, 상원에서 계류 중
  - 상원에서 통과 시, 백악관으로 이송하여 공포, 시행 여부 결정

美주요이슈: 사이버안보 관련법령 (6/7)

- **Federal Information Security Amendment Act of 2012**
  - 미 관리예산처(OMB)의 감독권한 재설정 내용 포함
  - 형식 상 '연방정보보안관리법(Federal Information Security Management Act of 2002)' 의 개정임
  - 하원의원 공동발의, 2012.03.26
  - 하원 본회의 통과, 상원에서 계류 중
  - 상원에서 통과 시, 백악관으로 이송하여 공포, 시행 여부 결정

美주요이슈: 사이버안보 관련법령 (7/7)

Cybersecurity Enhancement Act of 2012

- 제111대 의회 하원에서 발의되어 하원에서는 통과되었으나, 상원에서 처리되지 못하고 임기만료로 폐기된 Cybersecurity Enhancement Act of 2010과 유사한 내용임
  - 사이버보안 연구개발 강화를 위한 관련 프로그램 개선 및 추진체계 정비가 주된 내용임
  - 형식 상 '사이버보안연구개발법(Cyber Security Research and Development Act)' 의 개정임
- 하원의원 공동발의, 2011.06.02
- 하원 본회의 통과, 상원에서 계류 중
- 상원에서 통과 시, 백악관으로 이송하여 공포, 시행 여부 결정

美주요이슈: 국방부 사이버전 교전규칙 작성

- 미국이 대응하고 있는 사이버위협에 대응하는 지침서
- 대통령정책지침 20호 (Presidential Policy Directive-20)
  - * "PPD on US Cyber Operation Policy"
- 사이버작전 범주와 성격 정의함
  - 방어적 사이버효과작전(DCEO)
  - 공격적 사이버효과작전(OCEO)
  - 비침입방어대응(NDCM)
  - 긴급사이버행동(ECA) 등
- 사이버첩보 통한 해외 사이버 공격대상 리스트 작성 규정함
- 사이버안보 관련한 美정부기관 사이버작전 수행 역할과 책임 규정함

☞ 사이버안보 강화와 사이버전장에서 우위 선점 위한 높은 수준의 정책 마련, 공격적 사이버작전 규정, 세계 국가의 잠재적 사이버공격 대상 파악 등 구체적인 노력 규정함

美주요이슈: 행정부 단기실행계획(Near-Term Action Plan)

- 국가의 사이버안보 정책추진 총괄지휘하는 사이버안보정책관 임명
- 정보통신 인프라를 안전하게 보호하기 위한 새로운 국가전략 마련
- 대통령의 국정 우선순위로 사이버안보 책정하고, 성과평가 지표 설정
- NSC 사이버안보국에 프라이버시 및 시민자유권담당관 임명
- 사이버안보 관계부처회의 및 연방정부의 사이버안보 통합지침 마련
- 사이버안보 촉진 위한 범국가차원의 인식제고 및 교육 캠페인 착수
- 국제 사이버안보 정책 위한 직위신설 및 국제 파트너쉽 관련 역할강화
- 사이버 침해사고 대응계획 수립, 민관 파트너쉽 향상 위한 대화 촉진
- 연구개발 전략 프레임워크 구축 및 연구촉진 위한 침해사고 정보제공
- 시민자유 및 사생활 보호를 위해 ID 관리 비전 및 전략 수립

美주요이슈: 중기실행계획(Mid-Term Action Plan) (1/2)

- 법률 해석, 정책실행 등에 대한 기관간 불일치를 해결하기 위해 프로세스 개선
- 부처 및 기관들이 사이버안보 목표 달성 위해 기획예산처(OMB) 평가 체계 적극 활용
- 국가 경쟁력 유지 위해 교육 및 연구개발 프로그램 지원 확대
- 연방정부, 사이버안보전문가 확보 및 유지 가능한 인력양성전략 개발
- 예경보 제공, 상황전파, 사고대응 위한 효과적/효율적 메커니즘 결정
- 리스크 관리 결정, 복구 계획, R&D 우선순위 설정 등에 활용 가능한 위협 시나리오 및 메커니즘 개발
- 사이버사고 예방/탐지/대응 위해 정부와 민간부분 협력프로세스 개발

美주요이슈: 중기실행계획(Mid-Term Action Plan) (2/2)

- 프라이버시 및 지적재산권에 대한 우려 해소, 상호효과적 작용 가능한 사이버안보 정보공유 메커니즘 개발
- 네트워크 중립성과 병행, 국가재난/위기/갈등 대비 비상통신 대책 마련
- 상호다자간 협력 강화 위해 네트워크 사고 및 취약성 정보공유 확대
- 연구개발 및 혁신기술 신속히 보급 위해 학계 및 산업체 협업 촉진
- 국가 및 국제표준 조직 위한 목표 정의 위해 인프라 목표 및 연구개발 프레임워크 활용
- 온라인 거래 신뢰 확보, 프라이버시 향상 위해 상호운용 가능한 ID 관리 시스템 구축
- 정부 조달 정책 재정립, 안전하고 복구가능한 하드웨어, 소프트웨어 제품 및 서비스 개발 유도 가능한 시장 인센티브 향상

한국군 주요이슈: 관련법령 論據 (1/3)

□ 경우(CASE) 비교

물리전\사이버	low	mid	high
평시		CASE#2	
위기시	CASE#3		
전시		CASE#1	

- CASE#1: 軍주도(콘트롤타워) 물리전과 병행, 사이버전 수행
- CASE#2: 國家주도(콘트롤타워), 물리전은 없음, 사이버위협 대응
- CASE#3: 特定組織주도, 사이버 관련 모든 영역 독자 대응

한국군 주요이슈: 관련법령 論據 (2/3)

KIDA

□ CASE#1 분석

- ◆ 목적: 군 주도 물리적 군사작전에 사이버전 병행 수행을 보장함
- ◆ 시점: DEFCON III , 충무3종 발령시
- ◆ 현실태: 기 존재하는 법령에 사이버전 포함 법령 없음
- ◆ 대책: 기존 관련법령에 사이버전 기능 추가 (국방부 주도로 개정안 제시)

1) 계엄법 (법률 제8852호)
2) 통합방위법 (법률 제11635호)
3) 비상대비자원관리법 (법률 제11690호)
4) 징발법 (법률 제10100호)
5) 병역법
6) 국방정보화법 (법률 제9995호)
7) 국가전쟁지도지침 (대통령령 제284호)
8) 국가위기관리기본지침 (대통령령 제229호)
9) 정보작전방호태세규정(INFOCON) (합참규정343-01)
10) 한미연합작전계획(OPLAN)
11) 충무계획(행정안전부)

한국군 주요이슈: 관련법령 論據 (3/3)

□ CASE#2 분석

- ◆ 목적: 국가 주도 사이버위협에 군이 지원, 공조, 협조하는 기능 명시함
- ◆ 시점: 국가 사이버 위협(Low~High) 발생시 (물리전과 무관한 상태에서)
- ◆ 현실태: 기 존재하는 법령에 국방부장관 기능 포함 법령 없음

  * 장관의 국가 사이버위기 대응 평시에 모니터링 하는 기능 필요

- ◆ 대책: 기존 관련법령에 국방부 기능 추가 (국가에 협력내용 개정안 제시)

  1) 국가 사이버테러 방지 법률 (의원발의안)

  2) 국가 사이버 안보법률 (의원발의안)

  3) 국가사이버안전관리규정(국가정보원)

  4) 사이버안전분야 위기관리 표준메뉴얼(국가정보원)

참고문헌

- 해외 사이버전 저널, 국군사이버사령부, 2012.11~2013.07.
- 각국 사이버안전체계 보고서, 국가보안기술연구소, 2013.
- 美사이버안보 법령제도 분석, 국가보안기술연구소 R&D전략실, 2012.
- 사이버전 수행체계 발전방안 연구, 한국국방연구원, 2012.
- 보도자료(2013-0041호), 국방부 대변인실, 2013.04.01.
- 국방 사이버안보 관련법령 발전방안 연구, 한국국방연구원, 2013.
- 美군사청문회 사이버사령관 답변 보고서, 2013.03.20.
- 美육군사이버사령부 공무국외출장 결과보고서, 육군본부, 2013.
- 임종인, 美대통령정책지침(PPD-20) 관련 기고문, 국방일보, 2013.07.18.
- 기타 인터넷 및 관련 언론보도 자료, 다 수, 2012~2013.

Q & A