DOI: http://dx.doi.org/10.14248/JKOSSE.2014.10.1.065
ISSN 1738-480X (Print)
ISSN 2288-3592 (Online)
Journal of the Korea Society of Systems Engineering

사회기술적 시스템의 시스템보안과 시스템엔지니어링

한명덕

에스앤에스이앤지

Systems Approach to Sociotechnical Systems - Cyber Security

Myeong Deok Han[1)]

SNSEng, Technical Adviser

Abstract : As one member of the Korea Society of Systems Engineering (KOSSE) and especially as a member of Sociotechnical Systems session of the KOSSE, I tried to contribute somehow to the activity of KOSSE to help development of better Korea systems. This report is a brief discussion of the need for KOSSE activity in the Cyber Security area especially for the protection of national critical infrastructure systems from cyber terror.

Key Words : 국가핵심기반시설, 기반시설, 해킹, 사이버보안

* corresponding author : Myeong Deok Han/SNSEng, Technical Adviser/hanmydog@chol.com

1. 검토의 배경

2014년 4월은 잔인한 4월이 되었다. 세월호 침몰 사고로 인해, 정부와 국민은 재난대응 시스템의 부실함을 알게 되었고 대통령은 모든 국가 시스템을 재검토하겠다고 약속했다. 어디서부터 손을 보아야 한단 말인가? 모두 "시스템"개혁이 필요하다고 외치고 있을 때 시스템을 전문적으로 다루는 시스템엔지니어링 공동체는 무엇을 해야 하는 것인가?

대규모 사고가 발생한 직후에는 모든 언론이 나서서 안전대책을 강조하고 투자가 필요하다 부서가 필요하다고 주장하지만, 그렇게 해서 만들어진 정부의 안전부서가 일을 잘해서, 또는 운이 좋아서 한동안 사고가 없으면 안전에 대한 투자는 불필요한 투자로 보이고, 안전 요원들은 하는 일 없는 사람들로 비추어져 다른 부차적인 일들을 시키다가 결국에는 부서가 축소되고 예산지원도 사라져버린다. 일종의 시스템 다이나믹스적 현상인가?[1]

어떻게 하면 이러한 일시적 관심과 집중 투자 그리고 곧 이어지는 무관심과 소멸이라는 악순환을 끊고, 지속가능한 안전관리 시스템을 유지할 수 있을까? 아마도 이것이 시스템엔지니어링이 고민해야 할 안전 시스템 문제라고 보여 진다. 왜냐하면 시스템엔지니어링은 모두가 "안전"을 외칠 때 보다 큰 시스템을 생각해보고, 문제를 특정 부분에 치중하지 않고 전체적인 관점에서 균형 있게 바라보며, 또한 시간적으로도 지속가능한 시스템을 설계, 구축, 운용, 개선, 폐기하는 일까지 수명주기 전반을 균형 있게 들여다보도록 훈련되었기 때문이다.

그동안 시스템엔지니어링이 취급하는 다양한 시스템들은 일반적으로는 기술적 시스템이었다. 국방에 사용되는 무기시스템, 예를 들어 전투기, 구축함, 잠수함, 유도탄 같은 무기들을 어떻게 하면 주어진 예산, 일정, 품질 요구사항을 충족하면서 실패 없이 성공적으로 개발할 것인가를 주로 관심 있게 다루어 왔다.

그러나 미국의 MIT(매사추세츠 공과대학)에서는 개별 시스템보다도 더 크고, 복잡하고, 어려운 시스템의 문제를 해결하기 위해 "엔지니어링 시스템"[2] 학과를 개설하여 운영해오고 있다.

INCOSE [3]도 미국이 9.11 테러를 당하자 시스템엔지니어링을 활용하여 테러와의 전쟁을 지원할 수 있는 방법들을 논의하기 시작하였다. 이것이 사회기술적 시스템에 관한 실제 활동의 시작으로 생각된다.

이러한 문제를 논의해본 적도 없고 그러한 분야에 깊이 연구가 있었던 적이 없는데다 섣불리 나서서 준비없이 인터뷰에 응하게 되고 신문에 보도가 된다면 그동안의 노력에 대해 부정적인 영향을 줄 수도 있겠다는 생각에 준비가 될 때까지 "국가시스템 개조"에 관한 의견개진은 자제하는 것이 필요하다고 생각하였다.

우리 한국시스템엔지니어링학회 안에도 "국가시스템 연구 동호회"를 만들어 "대상시스템으로서의 국가", "국가 재난대비시스템", "핵심기반시설 보안 문제" 등 세 가지 분야에 자료를 축적하면서 접근해 나가고 있다. 자료들은 학회 홈페이지의 국가시스템 SE 연구회 동호회 이름으로 공유하고 있다.[4]

2. 국가 핵심기반시설 보안

2.1 국내 관련 연구

한국행정연구원은 2009년 사회안전 · 안전관리 연구총서의 일부로 "자연재해 및 국가위기 발생 시 국가적 종합위기 관리방안 연구" 시리즈를 발간하였다.[5] 4권의 책자 가운데에 "재난에 강한 사회시스템 구축"이라는 제목이 있다.[6]

국가 핵심기반시설의 사이버 보안 관련 국내 자료는 2011년 정보통신정책연구원에서 "IT실용화를 통한 국가정보화 선진화 방안 연구(III)"의 일환으로 수행한 협동연구 보고서 2 건이 식별되었다. 하나는 정보통신정책연구원 연구보고서로 "정보화 선

진화를 위한 디지털위험 관리 방안 연구"[7]이고 다른 하나는 고려대학교의 협력연구보고서 "디지털 위험도 관리 및 디지털재난 대응 모델 개발 방안 연구"[8]이다. 요약하면 "국가기반시설 제어시스템의 위험은 곧 국가적 재앙이다."[9] "디지털재난 대응 모델을 개발하여 대응해야 하겠다."[10] 하는 내용이다.

국가핵심기반시설은 국가위기관리기본지침에서 정한 에너지, 식 · 용수, 의료 · 보건, 정보 · 통신, 사이버, 금융, 수송, 원자력, 주요 산업단지, 정부 중요시설 등 국가 경제 및 정부의 기본기능 유지에 중대한 영향을 미치는 인적 · 물적 기능체계 10개 분야를 말한다. "디지털재난"이란 "디지털 위험이 원인이 되어 국민의 생명과 재산에 심각한 손실과 국가의 경제적 피해 사회적 혼란을 발생시킨 상태,"[11]로 연구자들이 정의하였다. 대응 모델은 "예방-대비-대응-복구" 단계별로 디지털재난 관리의 효율성을 제고하도록 방안을 제시하였다.

유사한 논문으로는 박대우의 "국가사이버보안 정책에서 해킹에 대한 소고"[12]가 있다. 박대우는 국가사이버보안법, 동법시행령 제정, 국가사이버보안위원회, 국가사이버보안 자문회의, 국가사이버보안협력회의 등의 설치를 제안하면서 해킹 프로세스에 대비한 대응전략도 제시한 바 있다.

학술대회 보고서로는 2013년 11월 18-19일 양일간에 서울 코엑스에서 개최된 ISEC2013 정보보안 컨퍼런스[13]와 연계하여 개최된 제3회 제어시설 정보보호 세미나[14]가 있다. 이 2개 학회 및 세미나를 통하여 최근에 발생한 사이버 테러에 대한 분석보고도 있었다. 특히 국가핵심기반시설에 사용되는 제어시스템의 사이버보안에 관한 대책도 보고되고 있었다. 대책 중에서는 핵심기반시설의 제어시스템에 대한 외부 장악을 피하면서 꼭 필요한 통신기능은 보장하기 위해 "일방향 전송장치"개발하는 방안이라든가,[15] 제어시설의 사이버 보안을 위한 보안 솔루션 제품 개발의 실태에[16] 대한 보고가 있었다.

[Figure 1] recent cyber security conferences

2.1 외국의 관련 연구

9.11 테러로 인해 직접 피해를 경험하여 이 분야에 대해 실제적인 대비가 이루어지고 있는 곳은 미국이다.

미국의 핵심기반시설보호 자료로는 미 상원 도서관 연구실에서 2011년 발간한 "미국 핵심기반시설 : 배경, 정책, 실천,"이라는 자료가 있다.[17]

이 자료를 보면 1998년 클린턴 대통령의 대통령 훈령 PDD-63 (1998)에서 클린턴 대통령은 국가 핵심기반시설을 해커로부터 보호하는 것의 중요함을 인식하고 핵심기반시설과 책임기관을 지정하는 문제, 해커의 활동을 탐지하고 차단하는 문제에 대하여 훈령으로 강조하였다.

2001년 9.11 테러로 직접 물리적 공격을 경험한 부시 대통령은 기반시설방호를 사이버 보안으로부터 물리적보안으로 전환하면서 2003년 HSPD-7이라는 대통령 훈령을 통하여 국토안보부를 신설하고 기존의 재난관리업무와 사이버보안 업무를 통합하여 콘트롤타워를 단일화하는 정책을 취하게 된다.

그러나 오바마 대통령은 2013년 다시 사이버 보안을 강조하게 되는데 이는 최근 들어 확대되고 있는 사이버 공격 활동에 대비하기 위한 것으로 보인다.

국가기반시설 방호의 쟁점은 무엇을 핵심자산, 핵심기능으로 볼 것인가? 무엇이 우선 방호해야할 핵심시스템인가? 이들의 취약점과 위험은 무엇인가? 이들을 방호하기 위해 자원할당을 어떻게 해야

할 것인가? 효율적인 방호를 위해 필요한 정보의 공유를 어떻게 할 것인가? 이를 위해 관련 법률과 규정을 어떻게 보완할 것인가? 하는 문제로 요약되고 있다.

특히 오바마 대통령이 2013년 2월 훈령에 따라 미국 정부는 그 실천방안의 일환으로 "핵심기반시설 사이버보안 증진을 위한 사이버보안 프레임워크" [18]초안을 작성하였다. 이에 의하면, 핵심기반시설의 사이버보안 리스크를 관리하기 위해서는 정보기술(IT) 및 산업제어시스템(ICS) 고유의 보안 문제와 고려요소를 명확히 이해해야 하고, 이를 바탕으로 리스크 기반의 접근방법을 채택하여 대응방안을 프레임워크로 제정하여 이를 실천하여야 한다는 것이다.

여기서 프레임워크는 크게 5대 기능 – 식별, 보호, 탐지, 대응, 복구 기능을 구분하고, 이들 5대 기능을 다시 22개 주요 활동(categories), 97개 세부활동(subcategories)로 세분하여 구체적인 활동은 기 발간된 관련문헌을 적시하는 방법으로 정리하였다.

유럽연합에서도 국가기반시설의 사이버보안에 대한 정책연구 자료들이 식별되어지는데, 그 중에도 사이버보안 프레임워크 매뉴얼이 눈에 뜨인다.[19]

INCOSE에서도 최근 시스템 보안을 취급하는 워킹그룹이 결성되어 INCOSE SE 핸드북 개정판에 시스템 보안을 반영하기 위해 준비 중이다.[20] 시스템 보안이 시스템엔지니어링의 책임이라는 인식에서 출발한다. 지금까지 시스템 보안은 INCOSE SE 핸드북에 포함되지 않았고, 굳이 분류하자면 특수공학의 하나로 취급되어 왔지만, 앞으로는 시스템 개발 시 반드시 포함하여 요구하고, 설계에 반영해야하는 필수 요소로 보안을 취급하겠다는 것이다.

IT 기술의 발전에 따라 디지털 콘트롤 시스템과 디지털 데이터 시스템이 거의 모든 시스템에 존재하기 때문에 매우 취약한 특성이 모든 시스템에 존재한다는 것이다. 시스템을 다 완성한 다음에 별도로 시스템 보안을 반영하는 것은 부적절한 방법이라는 인식이다. INCOSE에서는 이러한 구상에 따라 시스템 보안 문제를 Insight 잡지 2013년 7월호에 특집으로 소개하였고,[21] 2014년 라스베가스 국제심포지엄에서 시스템 보안 분야의 논문을 다수 포함시키기로 하고 있다.

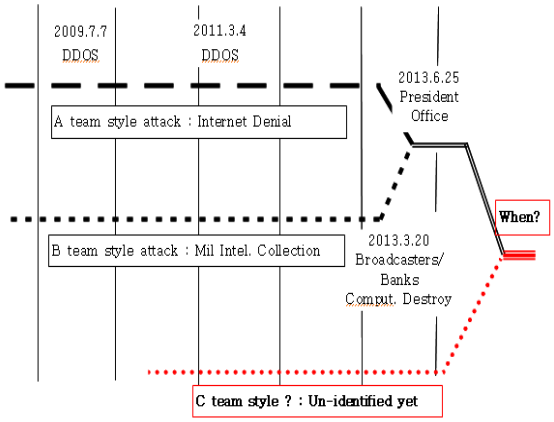
호주에서는 기반시설 제어에 사용되는 SCADA 시스템보안 과목을 대학원 시스템엔지니어링 석사과정 교과목에 포함하기 위해 특별히 노력하기도 했다. 호주에서 폐수처리장 IT시스템을 해커가 침입하여 150개 펌프장을 장악하고 1백만 리터의 미처리 폐수를 수로로 방출하는 조작을 하여 문제를 야기한 바 있었다. 체포된 범인은 전직 계약자로 직업을 잃고 나서 복수할 목적으로 폐수처리 시설을 공격한 것이었다.[22]

3. 해킹 보안 기술

3.1 최근 국내 주요 해킹 사건

2013년 우리나라는 3.20 사이버테러, 6.25 사이버테러 두 차례의 심각한 해킹 공격을 당했다. 한국인터넷진흥원 조사분석팀에서는 "국내 주요 인터넷 사고 경험을 통해 본 침해사고현황," 자료를 통해 최근 10여년간 발생한 주요 인터넷 사고를 정리하였다.[23]

2013년 11월 코엑스에서 개최된 ISEC 2013 국제 정보보안 컨퍼런스 행사에서 최상명은 최근에 발생한 사이버공격의 기술적인 특징을 분석한 결과 2개의 서로 다른 팀이 조직적으로 해킹 공격을 수행해 오다가 6.25 사이버테러에 이르러 이들 2개 팀이 협력하여 공격한 것처럼 보인다고 소개하였다.[24] 아래 그림은 최상명의 설명을 듣고 상상력을 더하여 그렇다면 다음 해킹 공격은 언제 어떤 방법으로 이루어질 것인가를 도식화해 본 것이다. 물론 아직 제 3의 해킹 방법이 무언지 알 수 없다.



[Figure 2] recent hacking skils reported

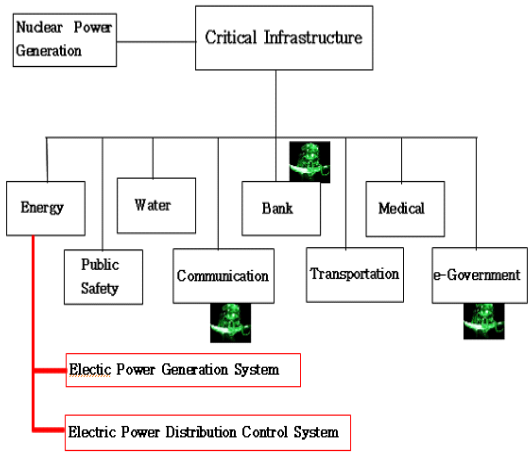
다음 대규모 해킹 공격이 언제 발생할지도 아직 알 수 없다. 그러나 다음번 공격은 또 다른 새로운 기법을 동원할 수 있을 것이고 보다 피해가 클 수 있을 것이라는 점을 감안하여 대비해야 할 것이다.

제3회 제어시설 정보보호 세미나에서 김유태는 [25] 기존의 주요 해킹 공격 대상으로 통신(방송국 포함), 은행, 전자 정부 3개 분야라고 소개하였다. 다음번 공격이 이루어진다면 가장 걱정스런 부분은 바로 전력 시스템일 것이라고 생각된다.

실제로 대정전 블랙아웃을 경험한 미국은 사이버 테러를 포함한 복합적 공격으로 전력 시스템이 마비되는 시나리오를 작성하여 이에 대응하는 연습을 두 차례 실시하였다. 2011년 GridEx I 및 2013년 GridEx II 등 전국적 규모의 전력망에 대한 연습에서 송전선과 변압기가 사이버 공격으로 파괴되고 수천만 명이 전기가 끊긴 어둠 속에 갇혔다.[26]

북미주 전기 신뢰성 회사 (North American Electric Reliability Corporation)가 작성한 시나리오 각본에 의해 거행된 워게임에서 경찰관, 소방대원, 전기기사 등 7명이 사고 현장에 출동했다가 테러분자의 공격으로 사망하고 150 명이 부상당했다. 물론 사망이나 부상은 시뮬레이션이지만 출동과 대응은 실제로 이루어 진 것이었다.

전력망을 복구하려고 출동한 전기기사들은 총격 현장을 경찰이 출입 통제하는 바람에 전력망 복구 작업 현장에 들어가지 못했다. 사이버 테러 시나리오에는 DOS 공격도 병행되었다.

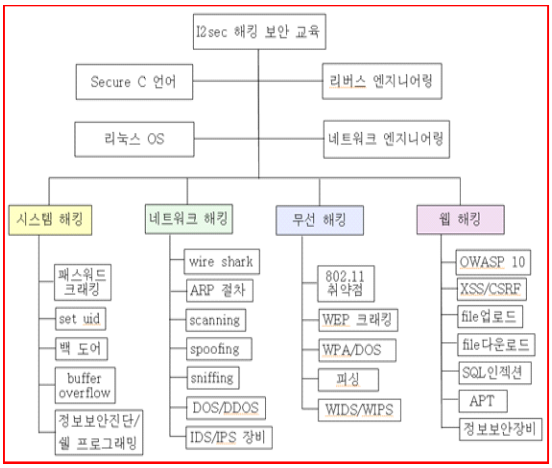


[Figure 3] probable cyber attack targets

사이버 공격은 크게 네 가지 형태를 취한다.[27] 해킹 기술을 이용하여 침투하는 방법, 누설된 직원 개인정보를 취득하여 사회공학적으로 접근하는 방법, 내부직원이나 하청업체 등 신뢰를 바탕으로 허가받은 접근권을 차후 신뢰를 배신하고 이용하는 방법, 마지막으로 지켜야할 보안 준칙을 지키지 않은 멍청한 직원의 허점을 이용하는 방법 등이다. 따라서 컴퓨터 소프트웨어나 정보통신 네트워크 기술을 이용한 전문해커의 공격만 대비하는 것으로는 충분하지 않을 것이다.

사이버보안 전문인력의 양성문제에 관해서 미국의 국토안보부는 NICE (사이버보안 교육 국가 구상)의 일환으로 내셔널 아카데미에 국가 사이버보안 인력 전문화 의사결정을 위한 판단기준을 마련하기 위해 연구용역을 의뢰하였다.[28] 연구보고서는 얼마나 많은 인력이 필요하고 또 어느 수준의 능력을 갖춘 인력이 필요한가, 사이버 보안 인력 중 어느 직종을 어느 정도나 전문화해야 하는가, 사이버 보안 인력 전문화를 국가주도로 해야 하는가 등을 검토하였다. 논의 중에는 전문화의 역할이 무엇이 되어야 하는가, 전문능력의 평가는 어떻게 해야 하는가, 자격제도가 필요한가, 면허제도가 필요한가 등이 포함되었다. 그러나 이 사이버보안 분야가 구

체적으로 어느 직종을 어느 수준으로 전문화해야 한다는 결론을 내기에는 아직도 너무나 변화가 빠른 진화단계에 있고, 자칫 자격제도나 면허제도가 인력 유입의 장애가 될 수 있다는 우려가 포함되어 뚜렷한 결론은 내리지 못하였다. 미국과 같은 곳에서도 사이버 보안, 시스템보안에 어떤 전문교육이 필요한가를 결정하지 못하고 있다면, 우리로서도 당분간은 각자 능력이 닿는 대로 서로 도와가며 전문기술을 익히는 방법이 최선일 수 있겠다. 아래 그림은 대구의 한 사설 정보보안 교육기관에서 실시하는 교육과목의 구조이다.



[Figure 4] cyber security training (example)

4. 결 론

온 나라가 시스템 개혁을 부르짖는 시점에 시스템엔지니어링을 공부하는 한 사람으로서 어떻게 하면 시스템엔지니어링을 사회 기술적 시스템의 개선에 적용할 수 있을것인가 상당한 심적 부담을 갖게 된다. 세월호 침몰 사고 같은 것은 비록 많은 인명손실이 있기는 했지만, 어떻게 보면 국가 시스템이 마비되는 위험한 사태는 아니었다고 보겠다. 보다 더 중대한 문제가 사이버 테러를 통한 국가 핵심기반 시스템의 마비 또는 붕괴 위험이라고 보았다.

해킹의 기법과 기술은 날로 새롭게 발전하고, 우리의 안보를 위협하는 적대세력은 이러한 최신의 기법을 활용하여 우리의 취약점을 노리고 사회를 혼란에 빠뜨리기 위해 기회를 노리고 있다. 시스템엔지니어링을 배우고 익힌 우리는 과연 무엇을 어떻게 하면 도움이 될 것인가? CMMI를 담당하고 있는 카네기멜론 대학교 소프트웨어공학연구소나 CMMI연구소에서도 새로 개발하는 시스템에 사이버 보안 분야를 포함하여 시스템엔지니어링 능력성숙도 평가를 하기 위해 기존 모델을 수정하기 시작했다. 우리도 이러한 국제적인 흐름에 뒤늦지 않도록 사이버보안 문제에 관심을 가지고 대처할 필요가 있다.

References

[1] Miller, “Systems Thinking for a Secure Digital World,” Cross Talk 2012. Sept-Oct. P.11
[2] MIT Engineering Systems Division
[3] INCOSE http://www.incose.org/
[4] Korea Society of Systems Engineering, http://www.kosse.or.kr/?MID=home-Club&TOP=NQ==
[5] KIPA, Social Risk and Safety management Research Collection, “Studies on Comprehensive National Crisis Management against Natural Disasters and National Crisis” , Bobmunsa, 2009.12
[6] Chung Ji-Bum, “Building Robust Social Systems against Disasters -Resilience and Social capital,” Bobmunsa, 2009.12
[7] Chung K H, et al., “A Study on Digital Risk Management for the Information Advance” KISDI, 2011.12
[8] Lim J I et al, “Digital Risk management and Digital Disaster Response Model Development,” KISDI, 2011.12
[9] Chung et al, ibid [9], p.18

[10] Chung et al,, ibid [9], p.12
[11] Chung et al, ibid [9], p.19
[12] Park Dae-Woo, "A Study on Hacking in the National Cyber Security Policy," KIISC review / v.21 no.6, 2011년, pp.24-41
[13] ISEC 2013, The 7th International Information Security Conference, COEX, Seoul, Korea, Nov. 18-19, 2013
[14] KISA, The 3rd ICS Cyber Security Seminar proceeding, 2013.11.18
[15] Ahn S J, "One Way Transmission Model," The 3rd Information Security Seminar proceeding, p.23, 2013.11.18
[16] Ahnlab, "The Threats and Solutions for Industrial Control System Security," The 3rd Information Security Seminar proceeding, p.97, 2013.11.18
[17] Moteff, J. D., "Critical Infrastructures : Background, Policy and Implementation," Congressional Research Service, July 11, 2011
[18] National Institute of Standards and Technology (NIST), "Improving Critical Infrastructure Cybersecurity Executive Order 13636, Preliminary Cybersecurity Framework".
[19] Klimburg A. ed, "National Cyber Security Framework Manual," The NATO Science for Peace and Security Program. 2012
[20] Rick Dove, "SE responsibility for System Security" INCOSE Enhancement Chapter, 2012. 9. 12
[21] INCOSE Insight, Vol 16, Issue 2, 2013. July.
[22] Slay, J. S. and E. Sitnikova, "Developing SCADA Systems Security Course within a Systems Engineering Program," Proceedings of the 12th Colloquium for Information Systems Security Education 2008.
[23] Shin J H, "Major Internet Accidents and Penetration Status, Korea," Internet & Security Focus, KISA, Sept., 2013, pp.36-53
[24] Choi Sang-Myung, ISEC 2013, "We are in the Real Cyber War," issue analysis, 2013.11.18
[25] Kim Yu-Tae, "Realization Theorem & Countermeasure for SCADA Viruse," The 3rd ICS Security Seminar, 2013.11.18
[26] Wald, M. L. "Attack Ravages Power Grid (Just a Test)," NewYork Times, 2013. 11. 14
[27] Miller, "Systems Thinking for a Secure Digital World," Cross Talk 2012. Sept-Oct. P.13, quoted from the original reference INCOSE INSIGHT 2011 July
[28] National Research Council of National Academies, "Professionalizing the Nation's Cybersecurity Workforce," Report to the US DHS, 2013