

사회과학적 위기관리이론을 활용한 국가사이버안보 평가체계 구축 가능성 고찰

이 상 호

경기대학교 정보보호학과

요 약

2003.1.25 인터넷대란 이후 정부는 국가위기관리차원에서 사이버안전확보에 심혈을 기울이고 있으나 현실은 국가안보위기 및 이와 관련된 정보·사이버위협에 대한 조기경보 및 위기평가체계가 미비하여 사이버위기·위협 발생 이후 수동적으로만 대응하고 있는 형편이다. 따라서 이런 한계를 극복하기 위해서는 보다 자동화되고 포괄적인 범국가차원의 사이버위기 평가체계 구축이 필요한 것으로 판단된다. 이에 본 논문 특히 이벤트데이터 관련 최근 기술발전 동향을 추적하였으며, 특히 동 기술을 사회과학분야의 위기관리이론 및 모델들과 결합시켜 사용할 경우 국가사이버안보 평가목적 종합 정보화시스템 개발이 가능할 것으로 판단했다. 비록 사이버위협 같이 그 속성상 매우 신속·광범위하게 발생하는 사건에 대한 정확한 예측은 어려울 수 있으나 이들 패턴을 체계적으로 유형화하고 각각에 대한 대응책을 시나리오형태로 제시하는 일은 가능할 것으로 보여 궁극적으로 국가사이버안보 및 위기관리 노력에 크게 기여할 수 있을 것으로 예상된다.

A Study on the Feasibility of Developing a Nationwide Cyber Risk Management System utilizing Social-Science Analytic Theories

Sangho Lee*

ABSTRACT

Since the 2003.1.25 Internet Crisis, the government has been looking at a number of options to strengthen national cyber-security/crisis management capability to guard against ever increasing threat of cyber-war and terror. Thus, the focus of this study was to explore new ways of developing a comprehensive cyber-security/crisis management system, in particular by combining modern social-science analytic theories. As a result, although there has to be more in-depth researches into incorporating advanced techniques to generate more detailed and object-specific indexes and protocols, the use of "event data system," which has been widely utilized in many recent social science researches to assess a wide-range of socio-political risks and crises, could be adopted as a basis for a comprehensive nationwide cyber-risk management system.

1. 서 론

2003.1.25 인터넷대란 이후 정부는 국가위기관리차원에서 사이버안전확보에 심혈을 기울이고 있으며, 이를 국가가 당면할 수 있는 다양한 위기, 재난·재해와 함께 국가차원에서 포괄적으로 관리하기 위하여 국가안보회의(NSC)사무처의 기능을 강화하고 산하에 “위기관리센터”를 운영하고 있다. 그러나 현실은 국가안보위기 및 이와 관련된 정보·사이버위협에 대한 조기경보 및 위기평가체계가 미비하여 사이버위기·위협발생 이후 수동적으로만 대응하고 있는 형편이다. 따라서 이런 현실적 한계를 극복하기 위해서는 보다 포괄적인 범국가차원의 사이버위기 평가체계 구축이 필요한 것으로 판단되며, 이에 본 논문은 인공지능, 이벤트데이터 등의 최근 정보 분석 및 처리기술 발전 동향을 추적하고 이들 기술을 사회과학분야의 최신 위기관리이론 및 모델들과 결합시켜 국가사이버안보 평가 목적 종합정보화 시스템 개발 가능성을 타진하려고 한다.

2. 위기평가·관리관련 최신평가모델들

사회과학분야서는 위기발생시 극도의 불확실성과 그에 따른 엄청난 스트레스를 특징으로 하는 위기상황 동안에 정책결정자들에게 빠르고 정확한 정책대안 선별능력을 제공하기 위한 노력을 기울여왔다. 특히 1990년대 들어 각광을 받기 시작한 Philip Schrodt의 KEDS(Kansas Event Data System)/PANDA 프로그램, 뒤이은 Doug Bond의 FRED, Bloomfield와 Moulton의 CASCON 프로그램, 기존의 기대효용 모델을 더욱 발전시킨 Bueno de Mesquita의 POLICON/FACTION 프로그램 등이 대표적인 사례들이다.[1] 이들 프로그램들의 특징은 고도의 시뮬레이션 모델링, 또는 인공지능기법을 활용한다는 점이다. 인공지능기반 모델의 특징은 축적된 데

이터를 기반으로 유사사례 또는 전례를 추적하는 방식을 채용하고 있다는 점이며 이는 사람들이 복잡한 상황에 직면하였을 경우 가장 손쉽게 그리고 가장 많이 사용하는 인식기제가 유사사례 추적이라는 판단과 함께 정책결정자들은 위기에 직면할 경우 그 위기를 해결하기 위한 주요방책으로 과거의 교훈을 거울로 삼는 경우가 많다는 현실적 인식에 기반을 둔 것이다. 특히 위기와 같이 상황이 복합적이고 위험이 많이 따르는 경우, 사람들은 연역적인 추론에 의한 결정보다는 실제로 있었던 역사적 사례에 의존하는 경향 많다는 판단에 기인한 것이다.[2]

이와 같은 인공지능적 위기평가기법에 대한 연구는 기술적인 문제 때문에 그 동안 기대만큼 실효를 거두지는 못하였다. 특히 선례분석에 근거를 둔 분석모델은 관련되는 역사적 선례와 이에 대한 정보가 데이터베이스에 충분하게 저장하여야 하고, 현재의 상황을 이미 입력된 과거의 사례들과 구체적이고도 명확하게 비교 해 줄 수 있는 능력이 있어야 한다. 이후, 이와 같은 기제는 피드백을 통하여 잘못된 유추를 바로 잡고 올바른 유추를 위한 새로운 정보를 제공할 수 있는 기능이 있어야 한다. 그러나 최근의 컴퓨터 기술의 비약적인 발전, 특히 인공지능 및 통계분석 분야의 획기적인 발전과 모델링기법의 고도화는 과거의 한계를 극복하면서 새로운 미래 가능성을 제시하고 있다.[3]

그중 특히 이벤트데이터시스템(Events Data System)을 주목할 필요가 있다. 상기 인공지능적 판단에 필요한 지능형 데이터를 제공해 주기 때문이다. 이를 보다 자세히 설명하면 컴퓨터가 기계적 코딩 및 자연어처리기법을 사용하여 다양한 사건을 구성하는 핵심 내용, 즉, “누가, 누구에게, 무엇을 했는가?”에 대한 정보를 자동으로 추출하여 데이터베이스화 하는 방법이다. 과거 컴퓨터 기능의 한계로 판독 불가능했던 범세계적으로 발생하는 다양한 사건 및 이와 관련된 행위·반행위에 대한 정보를 최신의 컴퓨팅 기

술을 이용하여 대량의 데이터를 자동적으로 추출, 보관함으로써 비용 및 효율성 면에서 급속한 개선이 이루어졌다. 특히 이러한 자동 코딩방식은 전체 이벤트데이터 매트릭스를 포괄하는 동적지표를 만들어낼 수 있는 능력을 지니고 있으며, 따라서 원하는 형태로 이벤트데이터를 가공해낼 수 있는 맞춤형데이터(data-on-demand)를 생산해낼 수 있어 좀 더 그 기능을 발전시킨다면 사이버위기 평가를 포함한 다양한 위기·위협상황을 분석하는 평가체계를 구축할 수 있다 는 점이다.

3.이벤트데이터의 내용 및 활용

3-1. 이벤트데이터의 수집과 처리를 위한 시스템 사례

사이버위기·위협을 포함한 다양한 위기상황을 조기에 판단하고 평가하기 위한 체제 개발에 있어 가장 시급한 과제는 기본적인 데이터를 확보하는 일인데, 현재 이벤트데이터 기반의 과학적 분석을 위한 체계적인 포맷과 자동화된 처리방식이 가용단계에 있다. 데이터는 기본적으로 “누가, 누구에게, 무엇을 했는가?”의 형태로 포맷되며, 수많은 사례들을 집적하여 이를 체계적으로 분석하기 위해서는 표준화된 방식이 절실하다. 특히 대량의 데이터 처리를 인력에 의존하기 보다는 컴퓨터로 자동화함으로써 비용 및 효율성 면에서 급속한 개선을 이룰 수가 있는데 유사작업이 가능한 현존체계로는 VRA의 Knowledge Manager System을 들 수 있다.[4]

3-2. VRA KM System 개황

VRA KM은 과거 FRED라는 명칭으로 알려져왔다. FRED란 Find·Read·Evaluate and Display의 앞머리 글자로 만들어진 약어 조합명칭으로서 미 하버드대학 출신 학자들이 설립한 VRA사가 개발한 이벤트데이터 기반 포괄적 위기·위협 조기경보·평가시스템이다. FRED의

뿌리는 이미 언급한 Schrodt의 KEDS로서 동 시스템은 사회과학분야 최초로 중동지역 정치·군사 문제 관련 대량의 사건·사고 이벤트 D/B를 구축하였고, 동 D/B에서 위기관련 신뢰성 있는 정보만을 추출, 이를 기반으로 다양한 위기사태에 대한 사전파악이 가능하다는 사실을 밝혀내게 된다. 이후 KEDS는 UN의 지원을 받는 PANDA 프로젝트로 확대되는데, 이는 기존 체계를 대폭개선하고 분석범위를 확장하여 현실 상황에서 사용이 가능한 포괄적 위기조기경보시스템으로 승화시키려는 시도였다. 따라서 후속 모델인 FRED는 PANDA에 기반을 두고는 있지만 훨씬 성능과 기능이 앞서는 시스템이다. 특히 FRED는 1998년도부터 상용화되었고, display체제의 기능을 대폭 개선하여 현재의 VRA KM System으로 진화하였다.

간단하게 정리하면 FRED 시스템은 전세계 뉴스, 수집정보 등 각종 정보자료를 이벤트데이터로 변환, 컴퓨터 D/B에 실시간 저장하여 내장되어 있는 각종 분석모델을 활용, 범세계적 그리고 세계 각국의 정치·사회·경제적 위기수준 및 안정도 등을 자동으로 파악, 이해하기 쉬운 그래픽 display를 통해 사용자에게 관련 정보를 제공해 주는 종합정보시스템이다. 특히 국가안정도 추적과도 같은 거시적인 상황평가시스템으로 주로 운영하지만, 테러, 화재방사고 등의 세부 상황추적도 가능하여 향후 필요시 국가 사이버안전 및 위기·위협평가체계로서 진화 가능성이 매우 높은 포괄적 정보시스템이다.

특히 동 시스템은 상황에 따라 소수의 PC가 정보 D/B에 연결된 형태의 소규모의 네트워크로의 구성도 가능하고, 필요시 이를 기반으로 수십·수백 대의 컴퓨터, 정보터미널, 지휘·통제체제를 갖춘 대규모 상황실·통제센터의 구축도 가능하다. 무엇보다 여러 형태의 위기발생 징후가 포착되었을 경우 언제·어디서·어떻게·왜 발생할 것인지를 파악하면서 기축적 자료와의 통합분석을 통해 동 위기의 발생 시기 및 전개

과정을 예측하는 기능이 있다.[5]

따라서 FRED의 정보처리 능력, 내장 분석모델을 개선해 사용할 경우, 작계는 국내의 사이버안보 위기발생 상황뿐 아니라 국내의 제반 위기 상황에 대한 위기징후 조기탐지와 한반도 주변 국제 상황변화에 대한 각종 정보를 자동 추적하고 예측·분석이 가능한 지능화된 정보수집·분석기반을 확충한다는 의미가 있으며, 크게는 정부 차원의 포괄적인 위기경보센터, 종합상황 지휘·통제본부의 구축이 가능하게 된다.

3-3. VRA KM System 시스템 구성 및 운영 개념

VRA KM System은 Find, Read 등 다양한 모듈로 구성된 복합시스템으로 각각의 단위가 독립기능을 가지고 simultaneous하게 작동된다. 우선 이런 동작이 가능하려면 초기에 자료를 원소스로부터 공급받아 보관을 하고, 지속적으로 축적해 나갈 수 있는 대용량 D/B가 필요하다. D/B에 축적된 자료를 정리하고 가치를 판단하여 가공정보로 추출하기 위해서는 Find 및 Read 작업을 거치게 된다. 이 과정에서 두 가지 핵심 S/W가 활용이 되는데, 첫 번째는 자료의 내용을 인식하고, 컴퓨터가 이해할 수 있는 형태의 정보로 처리해 주기위한 정보 「판독기(parser)」이다. 두 번째는 인식된 자료를 각주제별, 행위별, 사건별 정보로 재분류, 정리해주는 「사건규약집(protocol)」이다. 특히 사건규약집은 내장 언어 사전을 통해 원 소스로부터 인물, 사건, 사건 발생일시 등을 고유명사, 동사 등으로 구분해 정리하게 도와줘 의미 있는 이벤트데이터로 변환시켜주는 역할을 한다.

이후 다음 단계인 Evaluate 과정에서는 기본적으로 「통계학적 회귀분석」 방식의 「시계열」 및 「빈도분석」 모델을 사용하여 사건의 발생 빈도를 내용과 분류별로 축적해서 종합적인 위기 상황 발생가능성 여부를 판단하게 된다. 그러나 각 사건의 의미나 영향력이 틀릴 수 있기 때문에 특정 행위의 중요성에 대해 가중치를 부여하

는 등 제한적 가중치분석 기능이 추가되어 단순 통계학적 모델의 한계를 보완하려고 했다. 또한 그밖에 다양한 고급 분석도구를 독자 개발·사용함으로써 시스템의 신뢰도 향상에 주력했다. 따라서 제공되는 기본정보의 질과 「판독기(parser)」 및 「사건규약집(protocol)」의 정교함과 성능에 따라 VRA KM System의 전반적인 기능 및 예측정확도가 결정이 된다고 봐야한다.

3-4. VRA KM System 사용국가 및 기관

동 시스템 개발 초기에는 미태평양사령부가 아·태지역 조기경보체제 구축을 위해 활용했고, UN의 경우는 르완다 지역 난민발생 사태에 관련 사전경보체제로 사용했다. 이후 UNICEF 등 국제기구, 미국 정부기관, 미육군과 해군 등의 기관에서 필요에 따라 동시스템을 부분별, 또는 포괄적으로 사용해왔다. 미 CIA 역시 이에 관심을 가지고 지속적으로 VRA사와 접촉을 해 온 것으로 알려져 있으며, 여타 정보기관도 많은 관심을 표명하고 있다. 특히 이들 기관의 주요관심사는 VRA KM의 정보추출, 판독, 지식 D/B로 재구축해주는 기능, 즉 이벤트데이터 구축능력에 대해 매우 관심이 많은데, 이는 동 기관들이 VRA KM의 이벤트 D/B를 활용해 자체 분석기술과 도구를 적용한 분석을 원한다는 사실을 증명해 주는 것이기도 하다.

현재의 VRA KM은 그밖에도 다국적기업, 증권회사, 보험회사 등을 포함 다수의 민간기업에서도 활용 중이며, 특히 UNICEF 등의 국제기구, 미 학술재단, 하버드 및 오하이오대학 등의 학술계 및 스위스평화재단(Swiss Peace Foundation), World Vision International 등 NGO에서의 활용 등 다양한 분야에서의 활약이 돋보인다. 특히 최근에는 경제정보 및 생화학무기, 테러 및 재난구호 관련 정보도 분석할 수 있게 업그レード되고 있어 많은 기대를 모으고 있다.

3-5. VRA KM System의 이벤트데이터 추출 방식의 특징

부분적으로 언급했듯이 VRA KM은 데이터를

자동으로 읽어 들어 표준화된 포맷으로 바꾸어 주는 Automated Parser, 수집된 데이터를 분석하는 Field Reporter(Reader의 개선형), 그리고 데이터를 시각적으로 정리하여 보여주는 Display Modules 등 3가지의 모듈로 이루어져 있다. VRA KM은 특히 Reuters Business Briefing(RBB) 뉴스원을 바탕으로 하여 시범적으로 지난 10여 년간의 이벤트데이터를 수집해 왔는데, 그 효율성이나 신뢰성에 있어서 인력에 의존하는 수집방식에 비해 훨씬 앞서고 있다는 평가를 받고 있다. 따라서 앞으로 이러한 데이터 추출 및 분석도구들을 적극 활용할 것이 기대되고 있다.

한편 기존의 이벤트데이터 세트들이 다양한 포맷으로 이루어져 그 호환성이나 신뢰성에 다소의 의문을 야기 시켜왔다는 점을 감안하여 이들을 포함하는 새로운 형태의 광범위 표준화를 이루자는 움직임이 있어왔는데, 그 결과로 등장한 것이 IDEA(Integrated Data for Events Analysis)이다. VRA KM 역시 IDEA와 호환되게 설계되었다. IDEA 프로토콜은 다음과 같은 특징을 지니고 있다. 특히 인력에 의존하여 수집되어온 기존의 이벤트데이터들과는 달리 컴퓨터에 의한 자동입력방식을 지원함으로써 그 효율성 면에서 획기적인 전기를 이루고 있다. 이러한 자동 코딩방식은 기존의 KEDS 프로그램의 포맷을 따르고 있지만, Summary Index 등 전체 이벤트데이터 매트릭스를 포괄하는 동적 지표를 만들어낼 수 있는 능력을 지니고 있다. 따라서 원하는 형태로 이벤트데이터를 가공해낼 수 있는 맞춤형 데이터(data-on-demand)를 생산해낼 수 있다. 또한 WEIS 등 기존의 이벤트데이터들이 대부분 정치적인 이벤트에만 주안점을 두어 왔으나, IDEA에서는 국내사회적인 요인들도 지표화함으로써 보다 적실성 있는 분석이 가능하게 되었다. 이러한 접근방식은 국가를 하나의 획일화된 단위체로만 보던 좁은 시각에서 벗어나 타국의 국내사회적인 변수들까지도 종합적으로

고려하는 광범위한 사회과학적 분위기를 반영하고 있다고 보여진다. 특히 “양면게임(Two-Level Games)” 등 국가 간 관계의 분석에 있어서 최근 활발하게 이용되고 있는 분석도구들과 동일한 이론적 프레임워크를 따르고 있어서 학술적, 정책적 활용가치가 배가되었다고 할 수 있다. 이 부분은 특히 사이버안전, 위기·위협평가용 이벤트데이터를 구축하는데 합의를 갖고 있다.

3-6. 이벤트데이터를 이용한 사이버안보 평가 체계의 개발

현 실상으로는 고전적인 형태의 이벤트데이터 프로토콜을 사이버안보 분야에 적용하기 위해서는 별도의 추가적인 코딩표준이 요구되며, 이러한 분야에서는 한국이 상당히 앞서나가고 있는 상황이므로 기존의 이벤트 데이터와 호환 및 보완성을 갖춘 형태의 기준을 마련할 필요가 있다. 본 연구에서는 이러한 문제의식 하에 이벤트 데이터 분석기법에 기반하는 사이버위기 경보의 지표 개발에 주안점을 두고 있다.

사이버안보는 그 특성상 매우 빠른 속도와 광범위한 대상영역을 포함하고 있으므로 다양한 전문가들을 포함하는 공동의 표준화작업이 요구된다. 전통적으로 국가 간에 일어나는 정치, 외교, 군사, 경제 등 상호작용들은 대부분 국가쌍(dyads)의 이벤트데이터 수집과 계량화를 통해 분석이 가능했지만, 사이버 상호작용의 경우에는 일대일보다는 일대다 또는 다대다의 속성에 더하여 빠른 속도와 불확실성, 광범위한 영향력의 범위 등이 혼합되어 적실성 있는 대응을 어렵게 만드는 측면이 있다. 따라서 사이버안보에서의 위기에 대처하기 위해서는 다음의 몇 가지 점에 주목할 필요가 있다.

사이버안보는 기본적으로 전통적인 국가 간 관계의 프레임워크로서는 다룰 수 없는 다양한 행위자들을 포함한다. 특히 뛰어난 실력을 갖춘 컴퓨터 해커라든가 테러범, 조지 소로스(George Soros)와 같은 펀드관리자 등 개인뿐만 아니라 다양한 NGO, 국제기구, 다국적 기업(MNC) 등

비국가기구들의 비중이 높아졌다는 점을 간과할 수 없다. 일반적으로 이러한 현상은 전통적인 국가기구의 영향력 약화를 가져옴으로써 앞으로의 국제정치 패턴에 큰 변화를 유도할 것으로 보인다. 이러한 변인은 기존의 위기관리지표 작업에 이미 반영되고 있으므로 이를 적극적으로 활용할 필요가 있다 하겠다.

사이버안보는 기존의 여러 분야를 모두 포괄하는 다면적, 통합적 접근방식을 요구한다. 즉 기존의 국제관계들이 분야별 구분을 대체로 선명하게 나타낸 반면, 사이버안보 분야는 이들 모두에 걸쳐 일어날 수 있다는 특징을 가진다. 사이버안보 상의 문제들은 기존의 영역들에 중첩되어 나타날 수도 있으며, 또 기존의 영역으로 분류할 수 없는 새로운 영역을 창출해내기도 한다. 따라서 전통적인 유형화작업을 넘어서는 새로운 메타(meta) 접근법을 필요로 한다. 위기관리의 지표화작업에 이러한 요소를 고려해 넣는 것 역시 중요한 과제라고 할 수 있다.

사이버안보는 전 세계적으로 나타나는 네트워크화 현상을 기반으로 한다. 이는 우리가 기존에 익숙해져 있던 국가 간 상호의존 현상보다도 훨씬 더 복잡한 것으로서, 국제문제를 바라보는 우리의 시각에 새로운 변화를 가져다주고 있다. 국내 및 국제관계의 네트워크화는 효율성과 예측 불가능성이라는 양면적 속성을 지니고 있어서 다양한 전략적 고려가 더욱 절실하게 요구된다. 예를 들어 네트워크화가 진행될수록 시장선점을 통한 수확체증(increasing returns)의 법칙이나 잠금효과(lock-in), 양(陽)의 되먹임 효과(positive feedback) 효과 등 전통적인 사고방식으로는 이해하기 힘든 현상들이 나타난다. 사이버안보 분야에서 일어나는 사건들이 우리를 당황케 하는 이유도 바로 이러한 비합리성에 기인하기 때문에 이러한 속성에 대한 철저한 이해를 필요로 한다.

4. 결 론

현 수준에서 이벤트데이터를 활용한 정책결정은 어디까지나 정확한 예측을 지향하는 것이라기보다는 대략적인 패턴의 분석을 통하여 유용한 정보를 이끌어내는데 기본 목적이 있다고 할 수 있다. 특히 사이버안보와 같이 그 속성상 매우 빠르고 광범위하게 일어나는 이벤트에 대해서는 정확한 예측이 거의 불가능하다고 할 수 있다. 하지만 기존의 현상에 대한 경험적 분석과 이론적 작업을 통하여 이들의 “패턴(pattern)”을 체계적으로 유형화하고 이들 각각에 대한 대응책을 시나리오형태로 제시하는 일은 가능할 뿐더러 매우 시급한 일이라고 할 수 있다. 어떤 종류의 행위자가 어떤 자원을 활용하여 어떤 종류의 안보위협을 제기할 수 있는가에 대한 패턴분석은 앞에서 언급한 이벤트데이터의 프로토콜 개량 및 그에 따른 데이터 수집 및 분석을 통하여 상당한 정도로 이루어질 수 있다.

따라서 향후 연구되어야 할 분야로는 이벤트데이터의 수집을 바탕으로 하여 사이버안보 분야에 적합한 형태의 위기경보 지표(index)를 개발하는 것이다. 정책결정의 보조수단으로서 이루어지는 이러한 지표개발은 확장된 프로토콜에 의거하여 수집된 이벤트들이 거시적인 맥락에서 세계질서의 추세를 어떻게 나타내는가를 개괄적으로 보여줄 수 있도록 해준다. 특히 세부적인 상황에만 집착할 경우 헤아리기 힘든 전반적 패턴을 가려낼 수 있는 인덱스를 만드는데 주안점을 두고 있으므로, 이를 통하여 빠른 속도로 전개되는 사이버 공간 상에서의 이벤트에 대해서도 적절한 대응과 사전 경보가 가능할 수 있는 시스템을 구축할 수 있도록 해야 할 것이다. 이 경우 현재 그 성능과 신뢰도에 있어 강력한 도구로 부상한 VRA KM의 시스템 구성과 운영에 착안한 독자 모델을 개발해 볼 경우 안정된 운영이 가능할 것으로 판단된다.

결과적으로 이러한 다양한 기능의 첨단 소프트웨어들의 순기능과 장점을 극대화시키고 역기능과 단점을 최소화할 경우 새로운 지능형 사이

버위기 평가시스템의 개발이 가능할 것으로 판단되는 바, 그 동안 정제되었던 국가사이버위기 관리 체제의 효율성을 강화하는데 크게 기여할 수 있을 것으로 판단된다.

참고문헌

[1] Bloomfield, Lincoln and Allen Moulton, *Managing International Conflict: From Theory to Policy, A Teaching Tool Using CASCON*, New York: St.Martin's Press, 1997; Doug Bond, S. Lee and K. Rothkin, "PANDAs Early Warnings on Conflict," a paper presented at the International Studies Association Annual Meeting in Chicago, 1995; Bruce Bueno de Mesquita, "An Expected Utility Theory of International Conflict" and "A Decision Making Model: Its Structure and Form," *International Interactions*, Vol.23.,No.4. pp. 235-266.; Stanley Feder, "Factions and Policon: New Ways to Analyze Politics," *Studies in Intelligence*, Vol. 31, No. 1, (Spring 1987); Philip Schrodt and Gerner Deborah, "Cluster-Based Early Warning Indicators for Political Change in the Contemporary Levant," *American Political Science Review*, Vol. 94, No. 4, (December 2000) 등의 문헌을 참조.

[2] John Davis and Ted Gurr, *Preventive Measures: Building Risk Assessment and Crisis Early Warning*, Lanham, MD: Rowman & Littlefield, 1998; Valer, Hudson, ed., *Artificial Intelligence and International Politics*, Boulder: Westview Press, 1991; Ian Witten and Frank Eibe, *Data Mining: Practical Machine Learning Tools and Technologies*, San Diego: Morgan Kaufman Publisher, 2000 Ray

Wyatt, *Computer-Aided Policy Making: Lessons from Strategic Planning Software*, London: E & FN Spon, 1999 등의 문헌은 인공지능을 포함한 다양한 첨단 분석기법 적용을 소개.

[3] David Garson, *Social Dimensions of Information Technology*, Hershey, PA: Idea Group Publishing, 2000; S. M Weiss and N. Indurkya, *Predictive Data Mining: A Practical Guide*, San Fransico: Morgan Kaufmann, 1998; Robert Jacobson, *Information Design*, Cambridge: MIT Press, 1999; Susanne Schmeidl and Adelman Howard, *Early Warning and Early Response*, New York: Columbia University Press, 1998등의 문헌은 위기경보에서의 컴퓨터역할을 소개.

[4] 상세소개는 <http://www.vranet.com>참조

[5] Doug Bond, C. Jenkins, K. Schock, "Mapping Political Conflict and Civil Society," *Journal of Conflict Resolution*, Vol. 41., No. 4, (1997)

※ 본 논문 집필에 많은 도움을 주신 선문대 허태희 교수님 및 서울산업대 민병원 교수님께 감사드립니다.

이 상 호

1988년 미 세인트존스대학교 국제학과 (문학사)
 1991년 연세대학교 정치학과 (정치학석사)
 1994년 영 런던대학교 킹스칼리지 전략학과 (전략학박사)
 현재 경기대학교 정보보호학과 연구교수
 <관심분야> 국가안보·정보, 군사전략·작전술
 무기체계, 정보·사이버전