2006 IMACS

Multiconference on Computational Engineering in Systems Applications

(CESA' 2006)

Fuchun Sun and Huaping Liu (Eds)

Beijing, P. R. China

Oct. 4-6, 2006

IMACS

Volume I

Tsinghua University Press

2006 IMACS

Multiconference on Computational Engineering in Systems Applications

(CESA' 2006)

Fuchun Sun and Huaping Liu (Eds)

江苏工业学院图书馆
藏书章

Beijing, P. R. China

Oct. 4-6, 2006

IMACS

Volume I

Tsinghua University Press
Beijing

IEEE Catalog Number: 06EX1583

图书在版编目(CIP)数据

系统应用中的计算工程2006年国际会议文集/孙富春,刘华平编.—北京:清华大学出版社,2006.10
ISBN 7-302-13922-9

Ⅰ.系… Ⅱ.①孙… ②刘… Ⅲ.电子计算机—算法理论—国际学术会议—文集 Ⅳ.TP301.6-53

中国版本图书馆CIP数据核字(2006)第115204号

出版者:清华大学出版社
http://www.tup.com.cn
社总机:010-62770175
地址:北京清华大学学研大厦
邮编:100084
客户服务:010-62776969
责任编辑:陈国新
印刷者:北京市清华园胶印厂
装订者:三河市新茂装订有限公司
发行者:新华书店总店北京发行所
开本:203×280 **印张**:71.25
版次:2006年10月第1版 2006年10月第1次印刷
书号:ISBN 7-302-13922-9/TP·8369
印数:1～500
定价:220.00元(含Ⅰ,Ⅱ册)

2006 IMACS Multiconference on Computational Engineering in Systems Applications

October 4-6, 2006

Beijing, P.R.China

Sponsored by

IMACS

Co-Sponsored by

IEEE SMC Society

Tsinghua University, Beijing, P.R.China

Ecole Centrale de Lille, France

Ecole Nationale Supérieure des Arts et Industries Textiles, France

National Science Foundation of China

Message from the General Co-Chair

The Multiconference on "Computational Engineering in Systems Applications" (CESA2006), co-sponsored by IMACS (the International Association for Mathematics and Computers in Simulation) and IEEE/SMC Society, will be held in Beijing on 4-6 October 2006. Its aim is to bring together scholars and practitioners from academia and industries to exchange the latest development in theories, and applications of computational techniques.

Over the last decades, it has become a strong need for exchange on common computational and algorithmic tools between researchers working in different application backgrounds. Under this situation, the first CESA conference (CESA96) was successfully held in Lille, France in July 1996. 657 papers from 40 countries were presented in this conference. The following two conferences CESA98 and CESA2003 were held in Nabeul-Hammamet, Tunisia in April 1998 and in Lille in July 2003 respectively. CESA98 collected 583 papers from 37 countries and while CESA2003 gathered 452 papers from 33 countries.

As the main organizer of CESA conferences, Ecole Centrale de Lille initiated and conducted most of scientific and social organization activities. However, we always have a strong wish to share our experience in CESA organization with research partners in the other parts of the world. In fact, more and more foreign partners, including Tunisian and Chinese researchers, have been involved in the organization of CESA conferences.

I should point out that many well-known scientists who play important roles in IEEE Society or IMACS have been actively involved in the CESA conferences. Special thanks go to Prof.L. Hall (USA), the current chairman of IEEE/SMC Society, J.Tien (USA), T.Fukuda (Japan), R.Saeks (USA) and M.Smith (Canada). In the previous CESA conferences, they gave many valuable suggestions. They are also involved in the activities of CESA2006 as steering committee members or symposium chairs or plenary speakers.

Since twenty years ago, as what happened in economic and social fields, great progress has also been made in China in scientific research and Chinese researchers have been more and more engaged in international research cooperation activities. It is the main reason for that the steering committee of CESA2006 decided to organize CESA2006 in Beijing with Tsinghua University. As initiator of CESA conferences, I would like to thank Tsinghua University to have accepted to co-organize this conference with the other two French research institutions. Special thanks go to Prof. Bo Zhang, Prof. Shiqiang Yang and Prof.

此为试读，需要完整PDF请访问：www.ertongbook.com

Fuchun Sun for their efforts and excellent organization work for the success of this conference. I also thank my French colleagues in Ecole Centrale de Lille and ENSAIT for their contribution in scientific organization and coordination work.

I am pleased to see that there is a strong participation of Chinese authors and also a great number of overseas authors attend this conference. I wish all of them enjoy the activities of CESA2006, make friends and have fruitful communications and exchanges between them.

Pierre Borne
General Co-Chair
Ecole Centrale de Lille – France

Message from the General Co-Chair

Welcome to the 2006 IMACS Multiconference on Computational Engineering in Systems Applications and welcome to Beijing, the capital of China.

The conference is a symposium series that had traditionally been held only in Europe over the years. We are especially proud of and excited about this year's conference. Not only is the conference being held outside of Europe for the first time in its history but it is also being hosted jointly with the first International Workshop on Intelligent Systems and Intelligent Computing. The two conferences provide an international forum for a distinguished group of experts to discuss and share their new ideas, research results, practical development and the challenges facing them. With an emphasis on systems and applications, the presentations and discussions cover various theoretical and practical aspects of computational engineering involved in system theory and its applications.

Most importantly, we would like to extend our utmost thanks to many superb individuals and various organizations. In particular, we would like to acknowledge NSFC, IEEE/SMC Society, Tsinghua University, Ecole Centrale de Lille and Ecole Nationale Superieure des Arts et Industries Textiles for their support. We are also very grateful to all authors and conference attendees for their contribution and participation.

Lastly, we hope you enjoy the conferences and your experience in Beijing!

Bo Zhang
General Co-Chair
Professor
Tsinghua University-China

Message from CESA2006 Organizers

As international program chairs and organizing committee chairs, we are pleased to welcome all the participants of the IMACS Multiconference on "Computational Engineering in Systems Applications" (CESA2006). It is the first time that a CESA conference is held in China after the success of CESA96 and CESA2003 in Lille (France) and CESA98 in Nabeul-Hammamet (Tunisia). CESA2006 is jointly sponsored by Tsinghua University, Ecole Centrale de Lille and Ecole Nationale Supérieure des Arts et Industries Textiles, in cooperation with IEEE/SMC Society.

The aim of this important meeting is to make the state of the art of the various theoretical and practical aspects of computational engineering involved in system theory and its applications. 388 papers will be presented in this multiconfénce, which include five symposiums and one workshop as follows.

1) Symposium on Mathematical Modelling, Identification and Simulation (87 papers)
2) Symposium on Cybernetics and Computational Intelligence (29 papers)
3) Symposium on Aeronautics and Astronautics Automation (44 papers)
4) Symposium on Industrial Engineering and Complex Systems (121 papers)
5) Symposium on Communication and Electronic Systems (26 papers)
6) Workshop on Intelligent Systems and Intelligent Computing (IWISIC) (81 papers)

These papers will be presented in 75 technical sessions, including 35 invited sessions and 40 regular sessions. About 10%-15% of papers presented at CESA2006 will be selected and further extended for publication in a number of international journals with SCI citation.

As the previous CESA conferences, CESA2006 is particularly oriented to industrial applications in which the following problems have been studied: logistics, production management and supply chain, industrial modeling, simulation and control, industrial design, industrial security, coding and transmission, industrial fault diagnosis and inspection, robotics, and so on. The related industrial fields include manufacturing, transportation, aeronautics, electronics, textile, medicine, economics, instrumentation, energy, automobile, chemistry, and so on. These industrial problems have been solved using the following computing techniques: signal processing, intelligent techniques, data fusion and data analysis, image processing and pattern recognition, decision making, Petri net, hybrid systems, and so on. Apart from these application-oriented papers, CESA2006 also collects a number of presentations on different theoretical aspects such as advanced control theory, system stability, discrete event systems.

As organizers of CESA2006, we would like to express our special thanks to Tsinghua University, Ecole Centrale de Lille and Ecole Nationale Supérieure des Arts et Industries Textiles for their sponsorship to this multiconference. We highly appreciate the five plenary speakers for delivering plenary talks at this conference. We are greatly thankful to all the

authors for their excellent contributions, to all the invited session organizers for their effort and enthusiasm, and to all the international program committee members and referees for their time and expertise in the paper review process. Also, special thanks go to Huaping Liu, Fengge Wu, Nathalie Dangoumau, Hervé Camus for their time and outstanding work in the organization of CESA2006.

We wish all CESA2006 participants enjoy attending conference sessions and activities, meeting research partners, setting up new research collaborations and having pleasant stays in Beijing.

Xianyi Zeng (International Program Committee Co-Chair)
Shiqing Yang (International Program Committee Co-Chair)
Fuchun Sun (Local Program Chair and Organizing Committee Co-Chair)
Emmanuel Parisis (Organizing Committee Co-Chair)

Committees

General Co-Chairs:

Pierre Borne, Ecole Centrale de Lille - France
Bo Zhang, Tsinghua University - China

International Program Committee Co-Chairs:

Xianyi Zeng, Ensait - France
Shiqiang Yang, Tsinghua University - China

Local Program Chair:

Fuchun Sun, Tsinghua University - China

Organizing Committee Co-Chairs:

Emmanuel Parisis, Ecole Centrale de Lille - France
Fuchun Sun, Tsinghua University - China

Symposiums & Workshop Chairs:

1. Mathematical Modeling, Identification and Simulation

   Co-Chairs: Mohamed Benrejeb (Tunisia), Zongji Chen (China)

2. Cybernetics and Computational Intelligence

   Co-Chairs: Michael Smith (Canada), Zengqi Sun (China)

3. Aeronautics and Astronautics

   Co-Chairs: Richard Saeks (USA), Hongxin Wu (China)

4. Computer Science and Industrial Engineering

   Co-Chairs: Isam Shahrour (France), Huimin Lin (China)

5. Communication and Electronic Systems

   Co-Chairs: Toshio Fukuda(Japan), Baozong Yuan (China)

6. Workshop on Intelligent Systems and Intelligent Computing

   Co-Chairs: Jacek M. Zurada (USA), Hongxing Li (China)

International Program Committee:

A. Appriou (France), S. Banerjee (India), N. Benhadj Braiek (Tunisia), M. Benrejeb (Tunisia), P. Borne (France), B. Bouchon-Meunier (France), J.P. Bourrieres (France), A. Bourjault (France), A. Bratsos (Greece), G.Q. Chen (China), J. Chen (China), C.B. Chu (France), G.Z. Dai (China), G. Dauphin-Tanguy (France), X.T. Deng (China), S.G. Deshmukh (India), G.Y. Ding (China), A. El Kamel (France), F. El Hawary (Canada), N. Ellouze (Tunisia), L. Fang (Canada), F. Filip (Romania), T. Fukuda (Japan), S.Z. Ge (Singapore), W. Gruver (Canada), L. Gruyitch (France), C. Guo (China), L. Hall (USA), K. Hipel (Canada), M. Jamshidi (USA), C. Kahraman (Turkey), O. Kaynak (Turkey), E. Kerre (Belgium), V. Kholodnyi (USA), L. Koehl (France), J. Korbicz (Poland), C. Kulikowski (USA), N.A. Kuznetsov (Russia), F. Lamnabhi-Lagarrigue (France), T.T. Lee (Taiwan, China), B.H. Li (China), H.X. Li (China), Y. Li (China), X.X. Liao (China), H.M. Lin (China), Z.Q. Liu (China), J. Lu (Australia), R.Q. Lu (China), N. Magnenat-Thalmann (Switzerland), J.Q. Mao (China), V. Marik (Czech Republic), L. Martinez (Spain), V. Matrosov (Russia), A. Martynyuk (Ukraine), J. Nedoma (Czech Republic), M. Neher (Germany), Z.S. Niu (China), D. Popescu (Romania), M. Ramdani (Morocco), J. Renaud (France), J.P. Richard (France), D. Ruan (Belgium), R. Saeks (USA), I. Shahrour (France), Y. Shimizu (Japan), M. Smith (Canada), R.M. Spitaleri (Italy), P. Steblyanko (Ukraine), G. Stylios (UK), F.C. Sun (China), Z.Q. Sun (China), A.Sydow (Germany), H. Takagi (Japan), W. Thissen (The Netherlands), J. Tien (USA), C. Vasseur (France), S. Vassilyev (Russia), C.H. Wang (China), J. Wang (China), P.Wang (USA), X.Z. Wang (China), H.X. Wu (China), Y. Xu (China), G. Yablonski (USA), S.Q. Yang (China), S. Yang (Singapore), W. Yang (China), B. Yannou (France), D.T. Yu (China), B.Z. Yuan (China), J. Zaytoon (France), X. Zeng (France), B. Zhang (China), J.Y. Zhao (France), N.N. Zheng (China), Y.X. Zhong (China), C.J. Zhou (Singapore), M.C. Zhou (USA), A. Zyzniewski (Canada)

此为试读，需要完整PDF请访问：www.ertongbook.com

A Computational Systems Approach To Urban Disruptions

James M. Tien
Rensselaer Polytechnic Institute
Troy, New York, USA
Phone: 518-276-6486, Fax: 518-276-8227, E-mail: tienj@rpi.edu

Abstract - Urban infrastructures are the focus of terrorist acts because, quite simply, they produce the most visible impact, if not casualties. While terrorist acts are the most insidious and onerous of all disruptions, it is obvious that there are many similarities to the way one should deal with these willful acts and those caused by natural and accidental incidents that have also resulted in adverse and severe consequences. However, there is one major and critical difference between terrorist acts and the other types of disruptions: the terrorist acts are willful – and therefore also adaptive. One must counter these acts with the same, if not more sophisticated, willful, adaptive and informed approach. Real-time, information-based decision making or decision informatics is the approach advanced herein to help make the right decisions at the various stages of a disruption. It is focused on decisions and based on multiple data sources, data fusion and analysis methods, timely information, stochastic decision models and a systems engineering outlook; moreover, it is multidisciplinary, evolutionary and systemic in practice. The approach provides a consistent way to address real-time emergency issues, including those concerned with the preparation for a major disruption, the prediction of such a disruption, the prevention or mitigation of the disruption, the detection of the disruption, the response to the disruption, and the recovery steps that are necessary to adequately, if not fully, recuperate from the disruption. The efforts of the U. S. Department of Homeland Security and its academically-based Homeland Security Centers of Excellence are considered within the proposed types, stages and decisions framework.

Keywords: Urban Disruptions, Terrorism, Homeland Security, Decision Informatics, Systems Engineering

I. INTRODUCTION

Urban infrastructures are the focus of terrorist acts because, quite simply, they produce the most visible impact, if not casualties. From the September 11, 2001 (i.e., "9/11") attack on New York City's World Trade Center to the more recent March 11, 2004, attack on Madrid's commuter trains, it is obvious that urban centers are indeed vulnerable to such hideous acts. While terrorist acts are the most insidious and onerous of all disruptions, it is obvious that there are many similarities to the way one should deal with these willful acts – which would also include a malicious prankster releasing an electronic virus on the Internet – and those caused by natural and accidental incidents that have also resulted in adverse and severe consequences. However, there is one major and critical difference between terrorist acts and the other man-made but accidental disruptions: the terrorist acts are willful – and therefore also adaptive. Since terrorist – and other willful (e.g., electronic viruses, hacker attacks, and email spam) – acts are based on the most up-to-date intelligence or information, one must also counter these acts with the same, if not more sophisticated, willful, adaptive and informed approach.

More specifically, the approach of real-time, information-based decision making – which Tien [TIE, 03] has called the decision informatics paradigm – is focused on decisions and based on multiple data sources, data fusion and analysis methods, timely information, stochastic decision models and a systems engineering outlook. It should be emphatically stated that while the terms employed in describing the methodologies that underpin decision informatics are those belonging to decision analysis (i.e., emergency management, statistics, risk analysis, etc.), decision informatics is clearly multidisciplinary in nature and, depending on the problem being considered, could include experts from science (i.e., information, cognition, sociology, etc.), engineering (i.e., telecommunications, biomedical, chemical, etc.) and other disciplines (i.e., religion, terrorism, culture). It provides a systematic and consistent way to address real-time emergency issues, including those concerned with the preparation for a major disruption, the prediction of such a disruption, the prevention or mitigation of the disruption, the detection of the disruption, the response to the disruption, and the recovery steps that are necessary to adequately, if not fully, recuperate from the disruption. More importantly, one must approach an urban emergency management problem in a systemic or holistic manner, especially given the interdependencies of the underlying infrastructure systems.

Although the focus of this paper – which draws from an earlier paper [TIE, 05] – is primarily on terrorist disruptions, it is obvious that the decision informatics approach is likewise applicable to the preparation, prediction, prevention, detection, response and recovery steps associated with the emergency management of any major urban disruption. The remaining sections of the paper deals with the types of disruption, the stages of or life cycle in a disruption, the decision informatics paradigm, and the combination of types, stages and decisions in regard to the efforts of the U. S. Department of Homeland Security and its academically-based Homeland Security Centers of Excellence, followed by some concluding remarks.

II. TYPES OF DISRUPTIONS

Modern society relies on the reliable operation of a set of human-built systems – each being a combination of people, processes, goods, services, physical structures and institutions – to sustain people themselves, infrastructures and commerce. In the U. S., the constructed systems – most of which are privately owned and operated – are so essential that they have been called the nation's "lifelines" and are included in the broader set of critical infrastructures defined by the President's Council on Critical Infrastructure Protection (PCCIP) [USP, 01] to be those physical and cyber-based systems essential to the minimum operations of both the economy and the government.

Historically, the nation's critical infrastructures have been physically and logically separate systems that had little interdependence. However, as a result of advances in information technology and the necessity for improved efficiency and effectiveness, these infrastructures have become increasingly automated and interlinked. In fact, because the information technology revolution has changed the way business is transacted, government is operated, and national defense is conducted, the U. S. President [USP, 01] singled it out as the most critical infrastructure to protect following 9/11. Thus, while the U. S. is considered a superpower because of its military strength and economic prowess, non-traditional attacks on its interdependent and cyber-supported infrastructures could significantly harm both the nation's military power and economy. Clearly, infrastructures, especially the information infrastructure, are among the nation's weakest links; they are vulnerable to willful acts of sabotage. The U. S. National Academies' Committee on The Role of Information Technology in Responding to Terrorism [NAT, 05] has made a number of recommendations to reduce vulnerabilities associated with the information infrastructure, including undertaking more research in authentication, detection, containment and recovery.

The infrastructure interdependencies are most obvious when a disruption occurs. For example, interruptions in power and communications following the 9/11 attack, in turn, forced the closing of the New York Stock Exchange, which is a critical part of the nation's banking and finance infrastructure. As another example, the August 2003 electrical power outage on the east coast caused the failure of wireless communications and affected the City of Cleveland's water system. Clearly, there are innumerable interdependencies among the various infrastructure networks or systems that provide for a continual flow of goods and services essential to the defense and economic security of a nation. Indeed, for this reason, it is inappropriate to only categorize some infrastructure systems as being critical; they are all critical to the proper functioning of a nation or urban center – otherwise, the non-critical ones might well become the weakest links and thus vulnerable to attack and destruction. More importantly, the infrastructure interdependence problems should not be minimized, especially from a security and reliability perspective; in fact, contingency plans or backup systems should be developed and employed to mitigate these problems.

Sadly, the same advances that have enhanced interconnectedness have created new vulnerabilities, especially related to equipment failure, human error, weather and other natural causes, and physical and cyber attacks. Thus, electronic viruses, biological agents and other toxic materials can turn a nation's "lifelines" into "deathliness", in that they can be used to facilitate the spread of these materials – whether by accident or by willful act. Even the Internet – with almost a billion users – has become a terrorist tool; jihad websites are recruiting members, soliciting funds, and promoting violence (e.g., by showing the beheading of hostages). Also, as evidenced by the 9/11 attack, components of an infrastructure system can be used as weapons of destruction. As identified earlier, there are, in essence, three types of disruptions: those natural incidents due to nature and/or natural forces; those accidental incidents due to human errors and/or structural failures; and those willful incidents due to human acts and/or destructive weapons. The who, what, when and where of a number of well known disruptions occurring in the latter half of the 20th century are considered in Table 1. The question remains: Are there differences between natural, accidental and willful disruptions? The answer is an emphatic yes; indeed, these differences point to the earlier stated need for a more adaptive, informed and decision-oriented approach to dealing with willful acts than to reacting to natural and accidental disasters. More specifically, Table 2 considers the different types of disruptions from four perspectives: cause, onset, target, and impact.

III. STAGES IN A DISRUPTION

The mission and overriding objective of the U. S. Federal Emergency Management Agency (FEMA), which is now a part of the 2002 established Department of Homeland Security (DHS) [Public Law 107-296, 2002], is to help the nation be ready to respond to disasters and disruptions of all kinds through a comprehensive, risk-based emergency preparedness program. Traditionally, FEMA's comprehensive emergency management system is composed of four stages: preparedness, mitigation, emergency response and recovery. From a decision perspective, it is helpful to consider an expanded, six-stage process: preparation (corresponding to preparedness), prediction, prevention (corresponding to mitigation), detection, response (corresponding to emergency response), and recovery (corresponding to recovery). The additional prediction stage is necessary because it is beyond general preparation and helps focus prevention tactics; it requires a set of methodologies and/or technologies that is statistical in nature and risk-based in approach. The additional detection stage is also necessary; it follows prediction and precedes response and is very much dependent on data obtained from multiple data sources or sensors and the careful fusion and analysis of that data. Table 3 identifies the six stages of a disruption's life cycle in terms of related decisions that must be considered at each stage.

IV. DECISION INFORMATICS

In critically reviewing the disruption characteristics and related decisions identified in Tables 2 and 3, respectively, it is obvious that real-time, information-based decision making is needed for addressing major disruptions, especially in regard to terrorist acts that are quite adaptive in reality. Alternately, what is needed is, as depicted in Figure 1, a decision informatics paradigm. That is, the nature of the required real-time decision (in connection with each of the six stages of a disruption) determines, where appropriate and from a systems engineering perspective, the data to be collected (possibly, from multiple, non-homogeneous sources) and the real-time fusion and analysis to be undertaken to obtain the needed information for input to the modeling effort which, in turn, provides the knowledge to support the required decision in a timely manner. The feedback loops in Figure 1 are within the context of systems engineering; they serve to refine the analysis and modeling steps. Thus, decision informatics concerns three related issues (i.e., decisions, data and information) and is underpinned by three multidisciplines (i.e., data fusion and analysis, decision modeling, and systems engineering). In abbreviated form, there are six steps in the decision informatics process: decisions, data, analysis, information, models, and systems. These six steps are summarized in Table 4.

Finally, it should be noted that decision informatics is, as a framework, generic and applicable to most, if not all, decision problems. Further, since any data analysis or modeling effort should only be undertaken for some purpose or decision, all analyses and modeling activities should be able to be viewed within the decision informatics framework. In short, decision informatics represents a decision-driven, information-based, adaptive, real-time, human-centered, integrated and computationally-intensive approach to intelligent decision making by humans or software agents. Consequently, it can be very appropriately employed to address decisions at the preparation, prediction, prevention, detection, response, and recovery stages of an urban disruption.

V. HOMELAND SECURITY

Following the 9/11 attack on the U. S. homeland in 2001, the U. S. Homeland Security Act of 2002 – Public Law 107-296, 2002 – was promptly passed; it established the Department of Homeland Security (DHS) with a mission to "a) prevent terrorist attacks within the United States; b) reduce the vulnerability of the United States to terrorism; and c) minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States." Additionally, a number of high level reports have been published on how to make the homeland more secure from future acts of terrorism. The U. S. National Academies formed a Committee on Science and Technology for Countering Terrorism; it strongly urged, among several other important recommendations, a risk or decision based approach to measuring and countering terrorism, and it also helped to define the Directorate of Science and Technology that is now a part of DHS. More recently, the National Commission on Terrorist Attacks Upon the United States [NAT, 04] is recommending the establishment of a National Counterterrorism Center – with a National Intelligence Director – to unify all counterterrorism intelligence and operations across the foreign-domestic divide in one organization; this and other Commission recommendations are currently being addressed in Congress. As stated in two related Presidential directives [USP, 03(a,b)], the National Response Plan [DHS, 04] establishes a comprehensive all-hazards approach to enhance the ability of the nation to manage domestic incidents. The National Response Plan (NRP) incorporates best practices and procedures from incident management disciplines—homeland security, emergency management, law enforcement, firefighting, public works, public health, responder and recovery worker health and safety, emergency medical services, and the private sector—and integrates them into a unified structure. It forms the basis of how the federal government coordinates with state, local, and tribal governments and the private sector during incidents. Further, to enhance the ability of the nation to manage domestic incidents, a single, comprehensive National Incident Management System (NIMS) is being established. The NRP is predicated on the NIMS; together, the NRP and the NIMS provide a nationwide template for working together to prevent or respond to threats and incidents regardless of cause, size, or complexity.

The Department of Homeland Security (DHS) is organized into four major directorates: Border and Transportation Security (including sensors, signals, passenger profiling, and prevention tactics), Emergency Preparedness and Response (including preparation, prediction, prevention, detection, response, and recovery), Information Analysis and Infrastructure Protection (including data fusion and analysis, disruption modeling, performance versus cost analysis, vulnerability/risk assessment tools and systems considerations), and Science and Technology (including biometric systems, weapons detection systems, and satellite image systems). DHS actually out sources many of its activities through contracts and grants – to federal laboratories, government agencies, and private organizations. In April 2004, the $130M, 4.5-year Homeland Security Institute was established at Analytic Services, Inc. or ANSER, a systems engineering "think tank" modeled after the RAND Corporation. Additionally, through the Office of University Programs within the Science and Technology Directorate, DHS is engaging the academic community to create learning and research environments in areas critical to homeland security. Labeled Homeland Security Centers of Excellence, it is helpful to consider them within the three dimensional – types, stages and decisions – framework discussed in the previous sections of this paper. Thus, with 3 types (i.e., natural, accidental, and willful), 6 stages (i.e., preparation, prediction, prevention, detection, response, and recovery), and 6 decision steps (i.e., decisions, data, analysis, information, models, and systems), we have 108 possible foci for study consideration. To date, five university-based Homeland Security Centers of Excellence have been established; they are summarized in Table 5.

VI. CONCLUDING REMARKS

Securing the homeland from damaging willful acts is a matter of tradeoffs. It is a tradeoff between security and people; in particular, people's privacy, civil liberties and quality of life. It is a tradeoff between security and infrastructures; in particular, infrastructures that are highly interdependent. It is a tradeoff between security and commerce; in particular, commerce that is dependent on highly efficient and non-redundant processes. In short, it is a tradeoff between security and a free society. Interestingly, the tools or technologies that underpin a modern society are likewise the weapons that can be used to undermine, if not destroy, society. Biological, chemical and nuclear breakthroughs can also be considered to be weapons of mass destruction; the highly effective Internet provides a medium for cyber viruses, hackers and spammers; and airplanes are employed as missiles against people, infrastructures and commerce.

The decision informatics approach to urban disruptions that is detailed herein can clearly address a number of vulnerabilities, including natural disasters, accidental tragedies and willful acts. Several comments should be made in regard to this approach. First, it is multidisciplinary in nature; obviously, depending on the problem being considered, it requires experts from many disciplines. Second, it is evolutionary in practice; as a problem becomes better understood, the approach could be better refined and made more expeditious. Third, it is systemic in scope; it seeks to consider a problem from different perspectives, in terms of, as examples, efficiency and reliability, public and private goals, and domestic and international concerns.

The purpose of this paper, then, is to augur for the development of decision technologies that can be employed to prepare for a major disruption, if not predict and possibly prevent the disruption. Such technologies should also detect the disruption, identify the responses required to deal with the resultant situation, and then, following the disruption, specify the recovery steps that are necessary to satisfactorily recuperate from the disruption.

REFERENCES

[COM, 03] Committee on Science and Technology for Countering Terrorism (Co-Chairs: L. M. Branscomb and R. D. Klausner), *Making The Nation Safer: The Role of Science and Technology in Countering Terrorism*, Washington, DC: The National Academies Press, National Research Council, 2003.

[COM, 05] Committee on The Role of Information Technology in Responding To Terrorism (Co-Editors: J. L. Hennessy, D.A. Patterson, and H. S. Lin), *Information Technology for Counterterrorism*, Washington, DC: The National Academies Press, National Research Council, 2005.

[DHS, 04] Department of Homeland Security (DHS), *National Response Plan*. Washington, DC: DHS, December 2004.

[NAT, 04] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, Washington, DC: U. S. Government Printing Office, 2004.

[PUB, 02] Public Law 107-296, As Amended, *Homeland Security Act of 2002*, Washington, DC: U. S. Congress, H. R. 5005-8, January 2002.

[TIE, 03] Tien, J. M., "Towards A Decision Informatics Paradigm: A Real-Time, Information-Based Approach to Decision Making," *IEEE Transactions on Systems, Man, and Cybernetics, Special Issue*, Part C, Vol. 33, No. 1, 2003, pp. 102-113.

[TIE, 05] Tien, J. M., "Viewing Urban Disruptions from a Decision Informatics Perspective", *Journal of Systems Science and Systems Engineering*, Vol. 14, No. 3, September 2005, pp. 257-288.

[USP, 01] U. S. President, *Executive Order on Critical Infrastructure Protection*, Washington, DC: White House, October 2001.

[USP, 03(a)] U. S. President, *Homeland Security Presidential Directive (HSPD) 5*, Washington, DC: White House, February 2003(a).

[USP, 03 (b)] U. S. President, *Homeland Security Presidential Directive (HSPD) 8*, Washington, DC: White House, December 2003(b).

TABLE 1. EXAMPLE DISRUPTIONS

Description	Nature of Disruption			
	Who?	**When?**	**What?**	**Where?**
Natural • 1969 Hurricane Camille • 2002 SARS (Severe Acute Respiratory Syndrome) epidemic • 2004 South Asia Tsunami	• Category 5 (out of a possible 5) hurricane. • Employing DNA sequencing information, SARS was identified in 24 hours as a coronavirus strain from wild animals, including poultry. • Magnitude 9.0 Indian Ocean earthquake causing tsunami tidal waves of up to 50 feet high.	• 2 AM, August 17, 1969. • November, 2002 —July, 2003. • 8 AM, December 26, 2004.	• Regional: 255 killed; thousands evacuated; $4.2B damage. • Worldwide: 774 killed; 7,322 injured. • Regional: over 160K killed; thousands injured; millions displaced.	• Makes landfall along Mississippi coastline. • Began in South China, then Canada and Southeast Asia plus a few cases in Europe and U.S. • Affecting Indonesia, Sri Lanka, India and Thailand.
Accidental • 1984 Bhopal Gas Tragedy • 1986 Chernobyl Nuclear Disaster • 1989 United 232 Explosion	• Toxic methylisocyanate chemical vapor escaped from Union Carbide plant due to safety valve malfunction. • While testing Reactor 4 and ignoring safety procedures, a chain reaction caused explosion and release of highly radioactive material. • Failure of all 3 hydraulic flight control systems of Northwest's DC-10.	• 11 PM, December 2, 1984. • 1 AM, April 26, 1986. • 3 PM, July 19, 1989.	• Regional: Over 10K killed; over 0.5 million injured. • Regional: 31 immediately killed; thousands injured and suffering disease; millions affected by remaining radiation. • Local: 186 (out of 300) crew and passengers killed; many injured.	• Small town of Bhopal, India. • Chernobyl nuclear power plant consisting of 4 reactors located in the Ukraine. • Plane crash lands on runway in Sioux City, Iowa.
Willful • 1993 Oklahoma City Bombing • 1995 Tokyo Subway Sarin Attack • 2001 9/11 Tragedy	• Timothy McVeigh and others built bomb that was placed in a rented Ryder truck. • Members of terrorist group attacked 5 subway lines leading to center city with toxic sarin nerve gas. • 19 terrorists took over 4 airliners, each loaded with thousands of gallons of jet fuel, and crashed them into highly visible U.S. targets.	• 9 AM, April 19, 1993. • 8 AM, March 20, 1995. • 8:47 AM—10:06 AM, September 11, 2001.	• Local: 168 killed, hundreds injured; building destroyed. • Local: 12 killed, thousands injured. • Local: 3000 killed; billions of dollars of infrastructure and commercial damage.	• Oklahoma City Alfred P. Murrah Federal Building. • Subway cars in Tokyo, Japan. • American 11 crashes into World Trade Center (WTC) north tower; United 175 crashes into WTC south tower; American 77 crashes into Pentagon; United 93 crashes in field near Shanksville, PA.

TABLE 2. DISRUPTION CHARACTERISTICS

Characteristics	Types of Disruption		
	Natural	**Accidental**	**Willful**

Cause:			
• Primary	• Nature	• Human Errors	• Human Acts
• Secondary	• Natural Forces	• Structural Failures	• Destructive Weapons
Onset:			
• Period	• Hours/Days	• Hours	• Minutes
• Predictability	• High	• Medium	• Low
• Adaptability	• Low	• Low	• High
Target:			
• Primary	• Infrastructures	• Infrastructures	• People
• Secondary	• Commerce/People	• Commerce/People	• Infrastructures/Commerce
• Vulnerability	• Indiscriminate	• Indiscriminate	• Weakest Link
Impact:			
• Spatial	• Regional/Worldwide	• Local/Regional	• Local
• Temporal	• Years	• Months/Years	• Month/Years
• Damage	• Medium/Large	• Medium/Large	• Medium/Large

此为试读，需要完整PDF请访问：www.ertongbook.com