TRUST ENGINEERING AND RISK MANAGEMENT FOR SAFETY OF METROPOLIS AND MEGALOPOLIS CITIZENS

Brian Bailey
●
Digital Security International
2703 Arlington Blvd., Suite 101
Arlington, VA, USA
bbailey@dciencryption.com

Igor Safonov
●
International Unity Science Institute
1011 Arlington Blvd., Suite 403
Arlington, VA, USA
isafonov@aol.com

ABSTRACT. The article describes the problems and solutions in the field of safety enhancement in emergency situations of the complex urban agglomerations and analyses of the most actual problem for all metropolises and megalopolises – terrorism, proposing the rational models and techniques of counterterrorism strategy, based on knowledge and experience.

Keywords: metropolis, megalopolis, emergency, terrorism, trust engineering, risk management, safety, models, evolutionary games, tools.

INTRODUCTION

Terrorism threats and terrorist activities became the most important factors of people troubles and government care ahead of traditional risk factors of nature, economic and technological characters. We are in need of tools and resources for engineering and management of safety in emergency situations for big cities in the most economically attractive way. The conceptions of Trust and Risk are at the focus of our attention.

"Terrorism threatens us deeply because it puts into question our ordinary lives and the trust we need to conduct them. … Sociologists sometimes say that trust is the glue that holds society together. … You could say that terrorism poisons the social glue, inspiring fear that it just won't stick any longer. When you stop to think about it, terrorists could operate nearly anywhere. A taxi? Didn't one of those hijackers work for a while as a taxi driver? Your cup of tea? Who had access to the water used to make it? That polite young man at the Xerox machine? He might be making false documents to support somebody who wants to launch another attack." [14]

In the first part of the article we describe the problems and decisions in the field of safety enhancement in emergency situations for one of the complex urban agglomerations – Washington, the capital of the United States of America, the country located between two choppy oceans, achieved technological peaks, abused human possibilities, and attracted attention of terrorists. The second part of article analyzes the most actual for all metropolises [22] and megalopolises problem – terrorism, proposes the most rational models and techniques of counterterrorism strategy, based on experience and common sense.

There are known three kinds of Trust [13]: 1) Strategic Trust – trust that the organization is doing the right things (goal and strategies), 2) Organizational Trust – trust in the way things are being done (processes and decision making), 3) Personal Trust – trust in the people leading the organization (trust in you, trust in them). Analysis of these three kinds of trust shows us that we have a Goal, Behavior (strategies, processes, and decision making), and a Structure (you and them), but that we have not yet a Resource model. This means we cannot formulate and decide problems of Trust Engineering not only optimally, or even rationally. In a similar manner, we have the same incompleteness in Risk Management.

Big cities – big troubles. Not only for regular people, but also for businesses. On November 26, 2002, President Bush signed into law The Terrorism Risk Insurance Act of 2002 (TRIA). The primary objective of the TRIA is to mainly ensure the availability of commercial property and casualty insurance

coverage for losses resulting from acts of terrorism. The TRIA will also allow for a transitional period for the private markets to regain stability, resume pricing and build capability to absorb damages in the future. But companies at risk of a terrorist attack are rejecting the expensive premiums sought by insurers for required coverage, sending a signal that TRIA could fail to meet its targets. Several high-risk groups have recently rejected the TRIA policies because the quotes were either too expensive or they felt they would be able to negotiate with rival insurers.

We propose the original decision of the problem using Anti-Terrorism Engineering and Management Approach (ATEMA), which is the part of Trust Engineering and Risk Management (TERM) approach and framework. The ATEMA problems, in contrast to more regular and traditional TERM problems, are characterized by the lack of understanding a terrorist processes, imperfect investigation of terrorist events, and not sufficiently developed models of decision making for loss prevention. Furthermore, the factor priorities are cardinally different. In this case, the immigration policies and technologies have become the subjects of care and study.

There are three major areas in which changes in immigration policies and technologies may be able to counter future terrorist threats: visa issuance and entry inspections, border controls, and interior enforcement. Of course, in considering the problems highlighted by the terrorist attacks, and the options to head off future attack, it is important to reach a trade off between enhanced security and reliability of safety procedures and privacy and liberty in Open Society.

The objects of our research and development are safety problems and procedures of megalopolis and metropolis citizens, partly based on one author experience in terrorism investigation and the Loss Prevention Program creation for Washington, DC Government, and on second author experience in cyber crime prevention technologies for governmental and corporate customers.

In the procedural direction, we can investigate the real world problems of criminal activities, which can help terrorists and threat citizens of megalopolises and metropolises, on base of mournful experience of New York City, District of Columbia, Tokyo, London, Moscow, and other big cities of the World. We must concentrate our attention on fact and document falsification as one of the major factor of terrorism oriented frauds, provide the most typical case studies (personal and corporate identity thefts, criminal placement in banks and businesses), and propose recommendations and procedures of fraud prevention and detection based on optimal or rational use the available resources and restricted time. In the technological direction, we can analyze, compare and recommend devices, systems and technologies of document control and fraud detection for government and businesses, propose methodology of multicriteria selection of appropriate equipment, services and its vendors, and direct the way to improvements in the techniques and technologies. In a general way, we must propose models and tools of resources trade off between procedures and technologies of Safety Enhancement and Loss Prevention for citizens, businesses and governments of metropolises and megalopolises.

A Loss Prevention Program (LPP) have been developed for prevention and elimination of human suffering, life and resource loss of the District of Columbia government, officers and employees in process of disaster events and emergency situations. Our problems were close, but no similar to problems of the District Response Plan (DRP) [10]: “The DRP provides a new framework for District Government entities to respond to public emergencies in the metropolitan Washington area. The DRP provides a unified structure for District emergency response operations to ensure a coordinated and effective operation. The plan describes how District agencies will work collaboratively within the District and with our regional and federal partners. The ultimate goal is to protect the public and respond efficiently and effectively to significant incidents that threaten life, property, public safety, and the environment in the District of Columbia.”

If the DPR has orientation toward the external goals and behavior of DC Government, the LPP was directed toward the internal goals of DC Government, in particular to protect own officers and employees, structure and behavior in emergency situations. Therefore, the first steps of the LPP development were concentrated in the next areas:

1. Reasons why the LPC is needed and what must be developed – employee motivation to participate in the LPC development and collaborate with the LPC developers.

2. Efficient goal decomposition on personal and team objectives for effective loss prevention and limitation directed to create a safe working environment ready for disaster events and emergency situations.

3. Complete (all functions and all employees) emergency responsibility distribution between all levels of job executors with rational redundancy for the LPP reliability.

4. Communication with and between top managers for information and knowledge feedback oriented on the LPP correction and adaptation with accordance with DC Government goals, it employee responsibilities, real circumstances and accessible resources.

MOTIVATION. DC Government managers, officers and other employees are motivated, like all others members of the human species, by species-wide needs for food, etc.; needs for safety, protection, and care; needs for gregariousness and for affection-and-love relations; needs for respect, standing, and status, with consequent self-respect; and by need for self-actualization or self-fulfillment of the idiosyncratic and species-wide potentialities of the individual person [18]. In emergency situations everything looks less important than safety and everybody may be characterized as living almost for safety alone.

SAFETY RULES & PROCEDURES. The common safety rules and procedures in emergency situations are inherited from normal situations, but must be reengineered for emergency because obvious restrictions in accessible resources and limited time for making decisions. These rules and procedures will be analyzed in context of forecasting (modeling) emergency events and situations and modified for real emergency conditions. Following DRP definition, during the normal situations (Normal Operations) DC agencies, divisions, managers, officers and employees "should be engaging in preparedness, training, and exercise activities to ensure continual readiness." [10]

EMERGENCY RULES & PROCEDURES. The special safety rules and procedures in emergency situations must be created and developed on the base of world experience and DC peculiarity as a capitol of the USA. In this case, we need to take into account the next three operation levels of emergency proposed by the DPR: Operation Level 1 – a monitoring phase triggered by the potential threats for life, property, or the environment; Operation Level 2 – a partial activation of the CMT triggered by highly probable hazardous conditions and a strong potential for property damage and loss of life; Operation Level 3 – a full activation of the CMT triggered by extremely hazardous conditions that are imminent or occurring.

MONITORING & INSPECTIONS. Following to the Federal Response Plan (FRP) [12], the DC has identified 15 Emergency Support Functions (ESF) as the priorities of emergency preparedness and loss prevention. These functions are our guiding lines for internal monitoring and for external inspections. Of course, the priorities must be established with taking into attention the DC peculiarity as a capitol of US and operation level of emergency. Also, we reserve the right to extend or (and) modify the ESF list:

1. Transportation
2. Communications
3. Public Works and Engineering
4. Firefighting
5. Information and Planning
6. Mass Care
7. Resource Support
8. Health and Medical Services
9. Urban Search and Rescue
10. Hazardous Materials
11. Food
12. Energy
13. Law Enforcement
14. Media Relations and Community Outreach
15. Donations and Volunteer Management

According to a vulnerability assessment of the District, there are five major categories of hazards that may pose a threat to the District: 1) Natural Hazard – sever weather, hurricanes, tornadoes, flooding, or earthquakes; 2) Infrastructure Disruptions – utility and power failures, water supply failures, critical resource shortages, or exploding manhole covers; 3) Human-caused Events and Hazards – urban fires, special events, civil disorder, or transportation accidents; 4) Technological Hazards – hazardous materials, radiological, biological, or computer-related incidents; and 5) Terrorist Incidents – bomb threads, sabotage, hijacking, or armed insurrection, which threaten life or property. Terrorist attacks can also be conduits through which biological, chemical, and radiological agents can be employed.

REPORTING, INVESTIGATION, ANALYSIS & CORRECTION. All accidents and injuries must be reported immediately. Very important part of this activity is the performance management in conditions of emergency. The traditional performance management [1] is the systematic process of: planning work and

setting expectations, continually monitoring performance, developing the capacity to perform, periodically rating performance, and rewarding good performance. This systematic process is never happened in real life and even in a no-emergency case is subject to mistakes, malfunctions, and failures. The performance management becomes especially difficult in emergency cases, but composition of Trust Engineering and Risk Management means does the problem solvable.

TRAINING & CONSULTING. Training and consulting are important components of the loss prevention and control process. Their importance cannot be overestimated. The training course must cover the basics of emergency management, the role of your department and your personal possibilities and responsibilities in case of emergency events and in process of emergency situation. Therefore, as you study our course and participate in training, think about adapting the information and knowledge to your particular job and to your personal safety. The format of our course is design to help DC managers, officers and employees learn and apply to team and person safety the principles, rules and procedures involve in emergency management and self-protection. First of all you will study the concept of Comprehensive Emergency Management (CEM) [34], which consist of three interrelated components: 1) All types of hazards, 2) An emergency management partnership, and 3) An emergency lifecycle. But before the detail explanation of these components, allow us to acquaint you with principal notions of the CEM.

Emergency is defined as any event or (and) situation, which threatens (threaten) to, or actually does, inflict damage to property or people. Large disasters can range from hurricanes and floods, to explosions and toxic chemical releases. Management has a traditional definition as the coordination of an organized effort to attain specific goals or objectives. In our case, emergency management means an organized effort to mitigate against, prepare for, respond to, and recover from an emergency. Comprehensive clarifies "emergency" by including all forms of natural, technological, human-caused and infrastructure hazards which threaten or adversely affect lives and properties; by bringing together the proper mix of resources from the federal, state, and local governments, from business and industry, and from the public; by adding phases of disaster lifecycles. The four phases of CEM are: 1) Mitigation, 2) Preparedness, 3) Response, and 4) Recovery.

Mitigation: Any activities that actually eliminate or reduce the occurrence of a disaster. It also includes long-term activities that reduce the effects of unavoidable disasters.

Preparedness: The activities are necessary to the extent that mitigation measures have not, or cannot, prevent disasters. In the phase, government, organizations, and individuals develop plans to save lives and minimize disaster damage. Preparedness measures also seek to enhance disaster response operations.

Response: The activities follow an emergency of disaster. Generally, they are designed to provide emergency assistance for casualties. They also seek to reduce the probability of secondary damage and to speed recovery operations.

Recovery: The activities continue until all systems return to normal or better state. Short-term recovery returns vital life support systems to minimum operating standards. Long-term recovery may continue for a numbers of years after a disaster. Their purpose is to return life to normal, or improved levels.

In our course, we recommended the DC government employees to recognize and share the basic philosophy of promoting safe and secure urban planning [20]:

1. To assume their respective roles, help each other, and liaise with each other in order to promote the realization of safe families, teams, and themselves.
2. To foster a wide range of department, team and community emergency activities and good relations with other employees for ensuring the safety and security.
3. The lessons, experience, and knowledge gained from living through disaster, crime, and accident will be put to good effect if everyday life and duty in order that we may be prepared for emergencies, and in order that we may hand our wisdom down to future generations.

HARDWARE AND SOFTWARE. The consulting services in case of emergency are oriented on future support by the Integrated Transportation and Public Safety Wireless Information Network (CapWIN) – the common project of DC and the States of Maryland and Virginia [4]. In the Washington Metropolitan Region – MD, VA, and DC, more than one hundred various fire, transportation, police and emergency medical services agencies are available to respond to emergency and life threatening incidents that impact public safety. These emergency services agencies utilize individual, proprietary communications systems that limit the user's ability to quickly share vital information with other responding agencies.

The CapWIN project will integrate transportation (ESF # 1) and public safety data and voice communication (ESF # 2) systems in two states and the DC and will be the first multi-state transportation and public safety integrated wireless network in the US.

Potential benefits of CapWIN for emergency events' and situations' consulting are: 1) "Real time" information to improve decision making and resource allocation; 2) Improve response to natural, technological and man-made disasters; 3) Increased accuracy and reliability of reports, investigations and analysis; 4) Direct communications between mobile units of departments and agencies; 5) Enhanced safety for government employees and their families.

PERSONNEL SELECTION & PLACEMENT FOR EMERGENCY ACTIVITY. Traditionally, this is to insure, that the best-qualified person is hired and placed based on job qualification standards, but in our case we need to orient all managers, officers and employees on very special conditions of emergency. Good personnel are the most valuable assets of an operation. Poorly performing workers can severely constrain and hamper a program. So it follows that personnel evaluation is a critical function of disaster managers.

The selection of the right person for a specific job is crucial in both normal and emergency situations. In pre-disaster situations, such as disaster mitigation and preparedness programs, the staff size is constant and usually small. A manager must be able to evaluate each person and assign him or her to the right task. In post-disaster environments, a program staff expands quickly for the emergency, and then contracts as rehabilitation and reconstruction phases occur. For this reason, the manager must constantly assess the staff to ensure that each project is being properly executed. When the size of the organization is reduced, the manager must carefully evaluate the staff to determine whom to let go. In disaster management, there are two purposes for personnel evaluation: to provide the basis for making staffing decisions during the transition between phases of a disaster and to help improve the performance of the operation by determining what aspects of an individual person's work need improvement. Thus, personnel evaluation is an important control technique.

The task of fairly, thoroughly and regularly evaluating the performance of others is a difficult one, but is indispensable to smooth operations. Subordinates need to know how they are doing; managers need to know how their subordinates are performing; and organizations need to know if personnel are being used effectively. Personnel evaluations must be approached carefully. If conducted poorly or with disregard of people's emotions, the evaluation will be disruptive, and it will serve little, if any, purpose. A manager's task is to develop a systematic evaluation process that is meaningful, fair and comprehensive. In modern management, the term "performance appraisal" is often used instead of "personnel evaluation," as it is considered to be less threatening.

WHAT & HOW. Information Technologies (IT) not only had absorbed a lot of scientific and empirical results from different fields of human activity, but also received a lot of own results, which can be feasibly implemented into other technologies. We hope to actively use the IT (primary, methodological) results for loss prevention (engineering) and control (management) programs. One of our approaches based on concern separation and aspect engineering. The approach is grounded on principal difference between External and Internal Behavior of any object what help us to separate goal functions and their aspects for more convenient implementation of system engineering and management.

The functions of external behavior are regular, but the functions of internal behavior are casual. Yet, if the functions of external behavior are goal (objective) determined, the functions of internal behavior are common for different goals (objectives). Absolute different departments or employees have a lot of common internal functions (for safety, performance, reliability, security, quality, etc.). Separation of concerns (particularly, in software engineering) has always been a very natural means to handle complexity of (software) development. However, modularizing concerns can be a very tricky task for the developer and raise some issues such as performance, crosscutting, or redesigning when the software is used in a context that is quite different from the overseen one. By handling crosscutting within the language or system, the recent approach of Aspect-Oriented Programming (AOP) seems to be a very promising way for helping developers to handle separation of concerns and to overcome the drawbacks of traditional design approaches.

However, if AOP introduces a new programming paradigm that complements existing ones, it is clear that it brings a new bunch of difficult but solvable problems, which can not be practically solved in Object-Oriented Programming. The main of them is an optimization. We developed a lot of different models and techniques algorithm and program optimization, which can be used in Trust Engineering for Emergency

Availability Support and in Risk Management for Emergency Loss Prevention. In order to define problems and generate novel courses of action, we need to draw on our experience to make judgment about [17]: reasonable goals and their attributes; the appearance of the anomaly; the urgency of solving a problem (whether to take anomalies seriously or treat them as transient that will go away); what constitutes an opportunity worth pursuing? Which analogues best fit the situation, and how to apply them? The solvability of a problem. It seems, as there are two primary sources of power for individuals in emergency situation problem solving:

Pattern matching (the power of intuition) provides us with a sense of reasonable goals and their attributes. It gives a basis for detecting anomalies and treating them with appropriate seriousness. It helps us to notice opportunities and leverage points, discover relevant analogies, and get a sense of how solvable a problem is. The judgment of solvability is also responsible for letting us recognize when we are unlikely to make more progress and that it is time to stop.

Mental simulation (the power of imagination) is the engine for diagnosing the causes of the problem, along with their trends. It plays a role in coalescing fragmentary actions to find a way to put them together. And it is the basis for evaluating courses of action. The themes covered thus far in reviewing problem solving and decision-making are the core components for a perspective on naturalistic decision making.

The next question is: Can we research the terrorist activity in the same way as we study the majority of surrounding us processes? In other words, can we exploit the scientific methods? The article with intriguing name "Modeling for Terrorism" [33] makes one of the first attempts to answer on this question in the affirmative agrees. Tom Stamer analyses three model approaches and corresponding techniques, proposed by Risk Management Solution, EQECAT, and Worldwide Corporation.

GAME THEORY APPROACH. The approach based on the Game Theory supposes that targets and techniques of possible terrorist attacks can be modeled by behavioral structures and parameters of terrorist organizations. The Risk Management Solution (RMS) developed an application called U.S. Terrorism Risk. The main goal of the U.S. Terrorism Risk is quantification of catastrophic terrorist attack risk. The model uses information from terrorism experts, estimates the probabilities and costs of property damages, business interruptions, casualties and injuries, taking into account 16 modes of attack. The modes are based on 4 types of terrorist weapons – biological, chemical, nuclear and radiological. High-resolution of simulation tool allows to model a lot of loss and damage agents, from blast pressure to airborne and ground-based contaminants. The simulated events cover close to 1,500 potential terrorist targets in the United States of America – business centers of megalopolises, government districts of metropolises, facilities, landmarks, etc. The model is focused on the most probable attacks and uses reflection approach to understand the corresponding models of an enemy.

PROBABILITY THEORY APPROACH. The approach based on the theory of probability, was developed by EQECAT Inc. It strikes by its dimensionality: the model takes into consideration hundreds of thousands terrorist targets and millions of events. President of EQECAT (Oakland, California) Richard Clinton says: "We believe our model is the only one currently available that is fully probabilistic and covers all relevant risk sources, including bomb blast, aircraft impact, and CBNR (chemical, biological, nuclear and radiological) weapons for all 50 states and the District of Columbia". The National Council on Compensation Insurance (NCCI) selected the Terrorism Model of EQECAT for terrorism loss evaluation in every state of the USA. Here is the NCCI opinion about the model: "By definition, events that cause catastrophic losses occur infrequently but have the potential to create massive claims costs. … For example, predicting the annual number of hurricanes or major earthquakes with any precision is impossible, in spite of more than a century of experience and extensive meteorological and geological/seismic research. In the case of terrorism events, we are fortunate to have few historical data points for the U.S., but this means that forecasts for the likely number of future terrorist events can be little more than conjecture.

The catastrophe-modeling firm EQECAT, at NCCI's request and with its support, developed a terrorism model that clearly details the devastating potential consequences of likely terrorist events. Using NCCI's terrorism model to analyze a range of specific events (e.g., truck bombs, sarin gas, chlorine, anthrax) confirms that the workers compensation losses alone from a single event could have a devastating financial impact on a significant portion of the country's property and casualty industry. This would create major hardships for the families of workers killed or injured in the attack, and extensive financial and administrative burdens for insurance regulators, policyholders, and the U.S. economy. NCCI's analysis also

confirms that this is a problem for all regions of the country—not just major metropolitan areas." The EQECAT model is supported by ABS Consulting's MIDAS software, which has been used for counterterrorism planning and response. It also helps insurers to optimize their risk portfolio, -- says Clinton. Because attacking the heartland of any country might be easy for terrorists, but could have a psychological impact on the country, Clinton recommends using the model and software for evaluation of probability and loss of midsize and small cities and towns.

DELPHI METHOD APPROACH. Developed by RAND Corporation the Delphi Method uses special procedure for processing of expert opinions and allows forecasting a place, time, means and impact of terrorist attacks. AIR Worldwide Corporation (Boston, Massachusetts) applies the method for estimation of numbers and sites of attacks. The AIR model is supported by the database of potential terrorist targets – buildings, bridges, tourist attractions and national infrastructure. The model was chosen for the terrorism preparedness exercise Silent Vector, where the roles of government leaders were played by former Virginia Governor James Gilmore, former Senator Sam Nunn, former FBI Director William Sessions, and former CIA Director James Woolsey. "The lessons learned from Silent Vector will help the government prepare for, and possibly deter, future attacks in the United States," says Jack Seaquist, product manager from the AIR.

GENERALIZED DYNAMIC SYSTEMS. All of these approaches are known for dozens of years and have been applied for forecasting and analysis of very complex processes with big degree of vagueness. The most powerful models and tools were created by Viktor Glushkov's team [2, 16, 23-28, 30,31] in the Kiev Institute of Cybernetics, named now the V.M.Glushkov Institute of Cybernetics. The experience of application Event- and Process-Forecasting systems, based on the Theory of Generalized Dynamic Systems, for Politic, Economic, Social, Science, and Engineering forecasting and analysis situations approved not only their wide possibility, but also demonstrated a lot of restrictions. Ignoring of these restrictions in the interest of special groups (lobbyists) is open to many hazards. For example, it may be in interests of the nuclear military industry. A shorthand text of the illustrated statement is cited below [29].
"Foresee and foreworn! Looking through an article "Don't be afraid of the nuclear winter" published in "Rossiyskaja Gazeta" May 16, 1992, we consider our professional duty to express discrepancy with stated in the article of the Associated Press information about necessity of reconsideration of climate consequence forecasts of the large-scale nuclear war – so called "nuclear winter". The article informs that scientists from a number of the US scientific centers consider that relatively weak and local changes of air temperature near earth in result of the Kuwait oilfield fires confirm that climate consequences of nuclear war may be small and the maiden earlier nuclear war forecasts must be revised. This assertion is mistaken. The analysis of climate consequences of Kuwait fires does not invalidate by any means the correctness of nuclear winter calculations. A nuclear winter is caused by nuclear bombing and followed by gigantic fires in big cities, when burning products elevate to a higher troposphere and stratosphere (to 10 km) and there they firstly extend toward the Northern Hemisphere followed by the Southern. Conflagrations in cities and oilfields differ essentially by composition of their combustibles, fire characters and consequences. The burning products from oilfield fires did not elevate to big height. That is why the temperature of air close to ground surface was comparatively less changed. By this means it is beyond reason to reconsider forecasts of nuclear winter because of information about conflagrations in Kuwait."

ASYMMETRIC INFORMATION AND EVOLUTIONARY GAMES. The Nobel prizes of last years (John C. Hasanyi, John F. Nash, and Reinhard Selten – 1994, James A. Mirrlees and William Vickrey – 1996, George A. Ackerlof, A. Michael Spence, and Joseph E. Stiglitz – 2001) and a movie "A Beautiful Mind" about a great mathematician John Forbes Nash attract public attention to the Game Theory and Asymmetric Information for modeling of economic conflicts, contemporary wars, emergency situations and counterterrorism activity. Yet, a "hungry" market also attracted a lot of popularizers and advertisers, which inadequately evaluate orientation and availability of these mathematic tools, causing the discredit of all the scientific movement, created by such Titans as John Von Neumann and John Maynard Smith. Using concepts taken from the theory of games formulated by John von Neumann in the 1940s, Maynard Smith introduced the idea of an Evolutionary Stable Strategy (ESS) in the 1970s. Assuming that two animals are in conflict, then an ESS is one that, if adopted by the majority of the population, prevents the invasion of a mutant strategy. Stable strategies by definition thus tend to be mixed strategies. Many aspects behavioral pathology of human relations from economic fraud to terrorist activities may be investigated and prevented

with the Evolutionary Games models developed by Maynard Smith. Modeling of intra-corporation (collaboration) and inter-corporation (competition) relations demonstrated that infiltration of criminals can be detected and their influence can be restricted using local- or wide-area networks (Intranet, Internet, etc.) and corresponding software [6-9]. Our experience in development and application the Theory of Evolutionary Games, Asymmetric Information and Knowledge, Conflict Resolution and Disaster Prevention [6-9] did not destroyed our pragmatic optimism, but has taught us to be careful. Money and Knowledge are the main resources of Contemporaneity, Law and Ethics – Bottom line Frameworks of Progress. "As we struggle to come to terms with vulnerability and fear, pointing to a need for moral reflection and logical evaluation that tend to be rare in times of crisis." [14] Following [32], we try to orange institutionalization of individual and collecting knowledge about terrorism and counterterrorism and transfer the knowledge between individuals, groups and organizations. We do it using the common principles of Trust Engineering and Risk Management and separating functions/aspects in context of bipolar dimensions of Internal/External, Actual/Future, Explicit/Implicit and Experimental/Theoretical Knowledge. Steven R. Newcomb made a huge job by rapprochement and attachment of net models and technologies of data, information and expert knowledge processing, particularly for terrorism patterns recognition and terrorism activities forecasting [19]. Gordon Woo is making first steps from the mathematics of natural catastrophes to modeling of artificial ones in attempt to quantify terrorism risks and justify terrorism insurance [36]. By the time of this article completion, The Associated Press correspondent Gene Johnson reported [15] about five day large-scale counterterrorism exercises in Seattle (an imaginary "dirty bomb") and Chicago (fake threat of a biological agent). The exercises involve more than 8,500 people from 100 federal, state and local agencies, and it cost was estimated $16 million dollars. Hundreds of evaluators are watching the exercises.

ILLEGAL MIGRATION AND IDENTIFICATION FRAUD. "Those who enter Japan illegally cannot take up regular employment, and often get associated with Japan criminal organizations to become criminal elements." [11] USA Census Bureau estimates (March 2002) the population of foreign-born residents in country 32.5 million or 11.5 percent of the 282.1 million common population. Illegal alien population in the USA, by estimation of Census Bureau (2002), is shortly close to 9 million. The General Accounting Office (GAO) concluded that immigration fraud is rampant and the Immigration and Naturalization Service (INS) has no idea how to get it under control. The agency's lax bureaucratic practices have even helped open the door for terrorism. In a report released 15.02.02, GAO came to a conclusion that immigration benefit fraud is "pervasive and significant and will increase as smugglers and other criminal enterprises use fraud as another means of bringing illegal aliens, including criminal aliens, into the country." INS fraud falls into two categories: using fake document, and lying on an application for a green card or U.S. citizenship. When perpetrators of fraud are caught, little is done to them. The usual penalty for immigration fraud is a denial of benefits, not criminal prosecution." [5]

CONCLUSION.

"In the short term, a military approach to terrorism may protect us, but in the long term, we need to find solutions by pursuing education, development, dialog, negotiation, and law. In such contexts, we can only be assisted by an appreciation of values and value differences, and the limitation of violence as a means of conflict resolution." [14] We agree to this. Our future research and development oriented to combine mathematical and engineering tools for conflict resolution and disaster prevention, for safety of citizens.

REFERENCES

1. A Handbook for Measuring Employee Performance. – Workforce Compensation and Performance Service. Washington, DC: U.S. Government Printing Office, 2001. – http://www.opm.gov/perform/articles/1999/pdf10.asp
2. Balmin, Lev, and Igor Safonov. Optimal Scheduling of Complex R&D Programs. – Vladivostok: Far-East Polytechnic University, 1985.
3. Brinkhoff, Th. The Principal Agglomerations of the World. – http://www.citypopulation.de -- 12.11.2002

4. Capital Wireless Integrated Network. Strategic Plan 2001. May 9, 2001. – HTTP://www.capwinproject.com
5. D'Agostino, Joseph. GAO: INS Bungling Facilitates Fraud, Terrorism. February 22, 2002. – http://www.humaneventsonline.com/articles/02-25-02/dagostino.htm
6. Degtiar, Vladimir, and Igor Safonov. Evolutionary Mechanism of Conflict Resolution. – New York, NY: Plenum Publishing Corporation, No. 2401-0114, 1988.
7. Degtiar, Vladimir, and Igor Safonov. Behavioristic and Ethical Aspects for Computerized Collective Decision Support Systems. – Moscow: 1989.
8. Degtiar, Vladimir, and Igor Safonov. An Evolution-Stable Conflict-Reducing Mechanism with Side Payments. – New York, NY: Plenum Publishing Corporation, No. 2602-0297, 1990.
9. Degtiar, Vladimir, and Igor Safonov. Distributed System for Decision Ethics Support. – Proceedings of the Fifth All-Union Seminar "Synthesis Technique and Development Planning for Large-Scale System Structures". – Moscow: NKAU USSR, 1990.
10. District of Columbia. District Response Plan. April 4, 2002. – http://dcema.dc.gov/info/pdf/basic.pdf
11. Ensuring urban security. – http://www.chijihonbu.metro.tokyo.jp
12. FEMA. The Federal Response Plan. April 1999. – http://www.app1.fema.gov/fema/fed1.htm
13. Galford, Robert, and Anne Seibold Drapeau. The Trusted Leader. – New York, NY: The Free Press, 2002.
14. Govier, Trudy. A Delicate Balance. – Boulder, CO: Westview Press, 2002.
15. Johnson, Gene. Terror Drills in Seattle, Chicago. – The Associated Press. – 12.05.2003.
16. Karas, Viacheslav, and Igor Safonov. Organization of Research and Development for Concurrent Projects. - Proceedings of the Ninth All-Union Symposium "Logical Control in the Industry". – Tashkent: MISIS, 1986.
17. Klein, Gary. Sources of Power. How People Make Decisions. – Cambridge, MA: The MIT Press, 1998.
18. Maslow, A. Motivation and Personality. – New York, NY: Harper & Brothers, 1954.
19. Newcomb, Steven. Forecasting Terrorism: Meeting the Scaling Requirements. – Extreme Markup Languages 2002, Montreal, August 2002. – http://www.coolheads.com/SRNPUBS/extreme2002/forecasting-terrorism.hml
20. Outline of the Ordinance. – http://www.gity.kobe.jp/cityoffice/15/092/Jorei/Outline.htm
21. Principles of Management. Lesson 11: Personnel Evaluation. – University of Wisconsin Disaster Management Center, 2002. – http://dmc.engr.wisc.edu/courses/principles/AA04-11.html
22. Ruble, Blair. Second Metropolis. Pragmatic Pluralism in Gilded Age Chicago, Silver Age Moscow, and Meiji Osaka. – Cambridge, UK: Woodrow Wilson Center and Cambridge University Press, 2001.
23. Safonov, Igor. Methods and Systems of Forecasting Using Expert Appraisals. – Kiev: Znanie, 1973.
24. Safonov, Igor. Optimization of the Structured-Algorithmic Systems. – Kiev: Znanie, 1978.
25. Safonov, Igor. SELENA - the Expert-Modeling System Presenting Symbiosis of DSS and CAD. - Proceedings of the Regional Conference "Mathematical and Programming Techniques for MIS and CAM Design". – Penza: Polytechnic University, 1986.
26. Safonov, Igor. Information Security and Information Terrorism. - Capital and Vicinity, (6), 1996.
27. Safonov, Igor. Trust Engineering and Risk Management of Complex Systems. – Proceedings of the International Scientific School "Modeling and Analysis of Safety, Risk and Quality in Complex Systems." – Saint-Petersburg, Russia: Russian Academy of Sciences, 2001.
28. Safonov, Igor, Sergey Poroshin, and Nikolay Yukhin. Expert-Modeling System for Economic Analysis and Development Optimization of Production. – Proceedings of the All-Union Conference "Problems and Techniques of Science-Technical Progress Acceleration Using MIS", Part 1. – Moscow: VNIIPOU, 1985.
29. Safonov, Igor, and Alexander Tarko. Foresee and foreworn! – Business World, May 29, 1992.
30. Safonov, Igor, and Anna Tolmacheva. Optimization and Interaction in CAD of MIS. - IFAC Workshop "Computer-Aided Control Systems Design". – Moscow: Institute of Control Science, 1980.
31. Safonov, Igor, and Igor Tsikunov. Automation of the Situation Analysis. – Proceedings of the Conference "Analysis and Synthesis of Finite Automata." – Saratov: State University, 1973.

32. Schuppel, Jurgen, Gunter Muller, and Peter Gomes. The Knowledge Spiral. – Knowing in Firms. – London: SAGE Publications, 1998.
33. Starner, Tom. Modeling for Terrorism. – Risk & Insurance, April 1, 2003.
34. The Emergency Program Manager. – Emergency Management Institute. Federal Emergency Management Agency. – 2001.
35. What NCCI's Terrorism Modeling Demonstrates. December 10, 2002. – http://www.ncci.com/nccisearch/news/ceocorr/terrorism_model.htm
36. Woo, Gordon. Quantitative Terrorism Risk Assessment. – Risk Management Solutions Ltd. – www.rms.com/NewsPress/ Quantitative_Terrorism_Risk_Assessment.pdf