Proactive Infrastructure Security: Evolutionary Generation of Terrorism Scenarios

Stage I: Feasibility Study and Building Demonstration Systems

Proactive Security: A Co-evolutionary Approach*

Tomasz Arciszewski[1]
Kenneth DeJong[2]
Andrew Sage[3]
Mike Goode[4]
Rafal Kicinger[5]
Zbigniew Skolicki[6]

ABSTRACT

The objectives of this working paper are to propose a general concept of proactive security in the context of co-evolutionary computation and to briefly discuss the initial results of research recently began. First, the paper provides an overview of infrastructure security in the context of asymmetric threats. Next, concepts of proactive security are proposed based on co-evolution of terrorist scenarios and security plans. The paper also presents an outline of generation of terrorist scenarios in the context of conceptual design. Finally, it describes TerrorMax/Capitol Hill, a demonstration system being developed for dealing with the generation of terrorist scenarios related to the Capitol Hill in Washington DC. The paper also provides initial discussions of this recently initiated project.

KEY WORDS

Infrastructure security, proactive security, co-evolutionary system, terrorist scenario, generation of terrorist scenarios, TerrorMax/Capitol Hill.

---

[1] Principal Investigator, Professor & Chair, Civil, Environmental & Infrastructure Engineering Department, Information Technology and Engineering School, George Mason University, Fairfax, VA 22030, email: tarcisze@gmu.edu

[2] Investigator, Professor, Computer Science Department, Information Technology and Engineering School, George Mason University, Fairfax, VA 22030, email: kdejong@gmu.edu

[3] Faculty Associate, Chaired Professor, Systems Engineering & OR Department, Information Technology and Engineering School, George Mason University, Fairfax, VA 22030, email: asage@gmu.edu

[4] Consultant, Principal, Telford Consulting, Fairfax, VA 22030, email: mgoode@attglobal.net

[5] Graduate Research Assistant, Ph.D. Student, Civil, Environmental & Infrastructure Engineering Department, Information Technology and Engineering School, George Mason University, Fairfax, VA 22030, email: rkicinge@gmu.edu

[6] Graduate Research Assistant, Ph.D. Student, Computer Science Department, Information Technology and Engineering School, George Mason University, Fairfax, VA 22030, email: zskolick@gmu.edu

* *Citation:*
Arciszewski, T., De Jong, K. A., Sage, A., Goode, M., Kicinger, R., and Skolicki, Z. "Proactive infrastructure security: evolutionary generation of terrorist scenarios." *Proceedings of the Workshop on the Critical Infrastructure Protection Project, Airlie Center, Warrenton, VA, August, 2003,* A. Woodcock and K. Thomas, eds., George Mason University Press, Fairfax, VA, 378-391.

1. Introduction

Countering terrorism is a major national goal at this time (National Research Council, 2002). Providing infrastructure security is extremely difficult when dealing with an enemy employing asymmetric measures, which are approaches that are directed against a nation's vulnerabilities and weaknesses while ignoring its strengths. To counter these approaches requires a great deal of strategic thinking and restructuring of contemporary approaches to threat interdiction in order to successfully undertake fourth-generation warfare against asymmetric threats — the kind of threats generally posed by terrorist networks. Such threats will potentially allow a less technologically advanced enemy to achieve the advantage of surprise, and to cause disproportional loss of human lives and resources while they utilize only very limited material and human resources.

A proactive approach to security in the face of asymmetric threats calls for the development of an entirely new understanding of infrastructure security. It is postulated here that in the future infrastructure security professionals in charge of a specific infrastructure system (for example, a water distribution system in a given county, or a computer network) will have a computer tool, customized for their system, which will provide a holistic picture of security including possible threats and protective measures. In developing such a tool, a security situation should be considered in the context of two coevolving issues. The first issue relates to generation of terrorist scenarios while the second one is associated with the identification of appropriate security plans. This would provide an infrastructure security professional with a relatively complete picture of a security situation, and support and enable learning about both potential terrorist scenarios and appropriate interdictory security plans. Thus, these professionals will be able to make rational decisions regarding the security of a given infrastructure system such as to obtain a significant advantage over a terrorist attack planner.

The above-described vision is feasible when results of design research, particularly those related to co-evolutionary conceptual design (Arciszewski & De Jong, 2001), are utilized. During the last

20 years, significant research effort has been focused on engineering design. As one result of this research, a new engineering science has emerged, called "Design and Inventive Engineering" (D&IE). George Mason University's IT&E School is one of the pioneers of D&IE, particularly when "out of the box" thinking approaches to design are concerned. It has active research on co-evolutionary conceptual design (Shelton, 2003). It integrates results of the leading research on co-evolutionary computation (De Jong, to appear; Potter & De Jong, 1994) in our Computer Science Department and of design research in the Civil, Environmental and Infrastructure Department (Arciszewski & De Jong, 2001). The School even offers the Graduate Certificate Program, "Discovery, Design and Innovation," as well as several academic courses, directly related to D&IE. Both the National Science Foundation and NASA have provided significant funding for design research of the PI (about $1M). It has resulted in a large body of knowledge and experience that is utilized today for various projects directly related to engineering design and associated applications to infrastructure security.

The objectives of this working paper are to propose a general concept of proactive security in the context of co-evolutionary computation and to briefly discuss the initial results of research recently began. First, the paper provides an overview of infrastructure security in the context of asymmetric threats. Next, the concept of proactive security is proposed, which is based on co-evolution of terrorist scenarios and security plans. The paper also presents an outline of generation of terrorist scenarios in the context of conceptual design. Finally, it describes TerrorMax/Capitol Hill, a demonstration system being developed for dealing with the generation of terrorist scenarios related to the Capitol Hill in Washington DC. The paper provides also initial conclusions.

2. Proactive Security

The best long-term way to provide a desired level of security for infrastructure systems is to design them properly to be resistant against potential threats. However, there are two problems since this has not been accomplished, and may well not be accomplished. First, the security of all existing infrastructure systems must be improved as soon as possible. Next, improving security through

design requires changing the existing design paradigm. Thus, an evolutionary approach is needed, and will doubtlessly always be needed. At present, only traditional nature-caused threats are considered during the design process, for example, gravity, live and earthquake forces. Unfortunately, loads related to various terrorist threats (scenarios) will have to be considered in the future, for example human-caused explosions, fires, etc. Unfortunately, there is still a lot of fundamental and applied research to be done before the design for security becomes a common practice. In this situation, our present focus is on the improvements of security of existing infrastructure systems through "Proactive Security" That will assure that we are responsive to threats in an evolutionary and emergent, and therefore adaptive, fashion.

Proactive security is understood here as a class of methods, models, and tools which have to be used in a systematic way in order to maximize the security of a given infrastructure system in an evolutionary and emergent fashion. The fundamental premises of proactive security, as related to infrastructure security professionals in charge of a given system, are:

- They have a better/more complete understanding of a given situation than a terrorist attack planner.
- They have a holistic understanding of security in which they consider all elements of the situation, including the terrorist attack process planning and its results, feasible security plans, etc.
- They constantly run simulation models of the situation in which co-evolution of terrorist scenarios and security plans can be monitored and analyzed to make security decisions.

The critical element of proactive security is the co-evolution of terrorist scenarios and security plans, which can be modeled, computationally simulated, and used for various security-related purposes.

Co-evolution of terrorist scenarios and security plans is understood here as an evolutionary process in which two populations co-evolve (Angeline & Pollack, 1993) as shown in Figure 1. Both populations may have the same evolution

mechanism or two different mechanisms may be employed. These evolutionary mechanisms are based on the use of evolutionary algorithms (Fogel, Owens, & Walsh, 1966; Holland, 1975; Rechenberg, 1973). The objective of evolution of terrorist scenarios is to determine the scenario that will provide the most harmful impact of a terrorist attack (measured by human life loses, economic impact, or other measures of effectiveness or utility for terrorists). Conversely, the objective of evolution of security plans is to minimize the impact of the worst feasible terrorist attack, or of all high probability terrorist attacks, if possible.

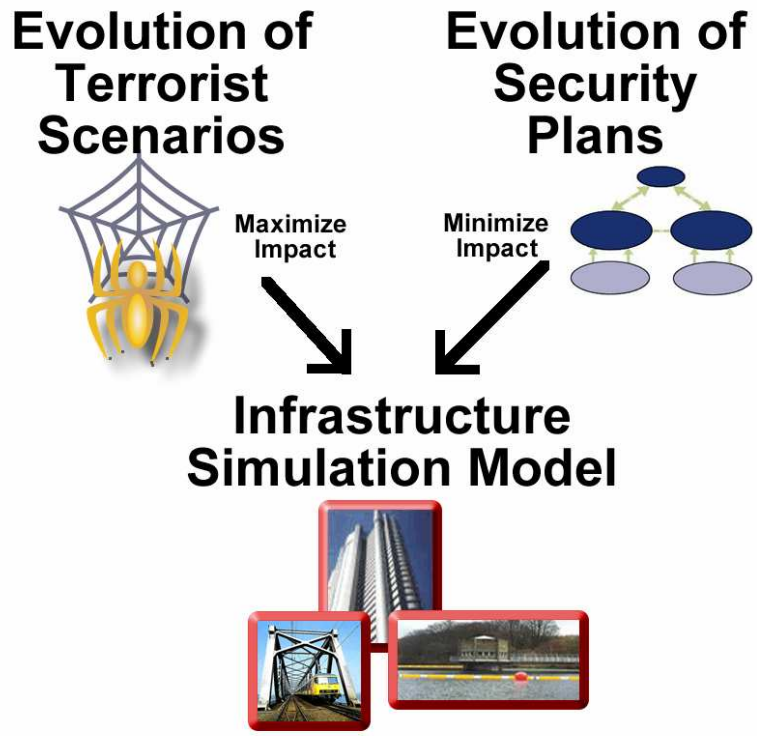

Figure 1. A model of a co-evolution of terrorist scenarios and security plans.

This co-evolution process is a multi-stage process. The first stage begins with a random generation of a number of terrorist scenarios, which make up the first population of terrorist scenarios. They are subsequently evaluated by considering their potential impacts. That is accomplished using an available simulation model of a given infrastructure system (for example, a model of the flow of traffic in a given transportation system, or a model of the flow of water in a given water distribution system). In the same stage, a number of security plans are randomly generated, with these

becoming the first population of security plans. They are also evaluated against the worst terrorist scenario of the first stage using the available simulation model of the infrastructure system being considered. The results of the both evaluations are then used to determine the surviving members of both populations. In the second evolution stage, both populations are evolved and again evaluated to determine members of surviving populations. The process is repeated as many times as changes are observed, or simply up to the moment when no more time is available or various stopping criteria terminate the co-evolutionary process.

3. Terrorist Scenarios Generation: Conceptual Design Approach

In the proposed concept of proactive security, parallel and concurrent generation of terrorist scenarios and security plans takes place. Both generation processes can be considered as equivalent to the concept generation process in the engineering conceptual design, as discussed below. In this way, methods and models of conceptual design, including those of co-evolutionary design, can be utilized and appropriate tools developed in a relatively short time period to support infrastructure security professionals such that they can directly benefit from use of these tools. From a computational point of view, the generation of security plans is identical to the generation of terrorist scenarios, which are more critical for infrastructure security professionals as much more difficult for them to develop. Therefore, in this paper we focus only on the generation of terrorist scenarios in the context of engineering conceptual design.

A brief discussion of the conceptual design process, on which much of this effort is based, is provided in (Arciszewski, 2002). A conceptual design process is a part of the engineering design process. In computational terms, it can be described as a search process through the conceptual design space, which produces the best design concept, or a class of concepts, satisfying all imposed requirements and constraints. A design concept is understood as a description of a future engineering system, actual or abstract, in terms of symbolic attributes (for example, a bridge will be a “truss

bridge"). ***A design concept can be formally presented as a feasible combination of symbolic attributes and their values.*** After the conceptual design process is completed, a given design concept is used next in the detailed design process to produce a detailed design, i.e. a detailed description of a future engineering system in terms of both symbolic and numerical attributes (dimensions, weights, etc.)

A terrorism scenario can be understood as a feasible combination of decisions to be taken by a terrorist attack planner that may lead to a terrorist act, i.e. to an event interrupting or negatively impacting the operations of a given infrastructure system. ***A terrorism scenario can be formally presented as a combination of symbolic attributes and values of these attributes.*** In this context, the process of a scenario generation is fundamentally equivalent to that of a design concept generation and the generation of terrorist scenarios is considered as an engineering design problem. A specific scenario may involve, for example, the locations of explosives in the various parts of a given infrastructure system and a sequence of their detonations.

4. TerrorMax/Capitol Hill

The concept of proactive security is quite complex, both conceptually and computationally. Therefore, its complete development and implementation require time. However, during the first 3 weeks of our research, an initial demonstration system has been developed and it is briefly described in this section. The developed system is intended for the general professional audience to demonstrate the potential of proactive security and to illustrate in a dynamic way the basic principles behind it as related to the generation of terrorist scenarios.

The system illustrates the evolutionary generation of terrorist scenarios for the Capitol Hill in Washington D.C. The purpose of this evolution is to produce a terrorist scenario with the maximum terror impact on the Capitol Hill, therefore it is called TerrorMax/Capitol Hill. The system has been developed making a number of assumptions, which may ultimately oversimplify the problem of terrorist attacks on the Capitol Hill. The intention, however, was never to produce a

system which could be used for actual security purposes, only to show the feasibility of building such system.

It has been assumed that at a given location terrorists may conduct various attacks. The list of considered terrorist attack types is provided below:

0. Starting fire
1. Causing an explosion
2. Using a dirty radioactive bomb
3. Using a biological weapon
4. Using a chemical weapon

For each type of a terrorist attack, a visual symbol has been selected, as shown in Figure 2. It has been also assumed that the terrorists may be suicidal terrorists and that their attacks will be conducted with a total disregard for human lives, including their own lives.

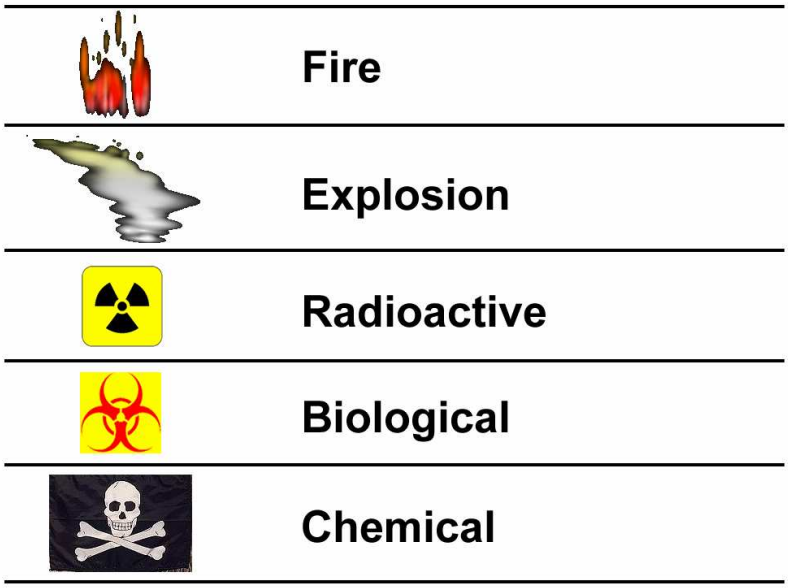

Figure 2. Symbols used to visualize specific terrorist attacks in TerrorMax/Capitol Hill.

Another important assumption is that at most four terrorist teams will attack the area at the same time and that these attacks will occur at most at four different locations out of the arbitrarily selected seven potential terrorist attack places. Also, it has been assumed

that at most three different attack types will take place at a given location.

Seven potential attack sites have been selected in the federal core of Washington DC (in the National Mall area) considering their infrastructure, security, and psychological and political impact. The selection illustrates a diverse target set with multiple stakeholders and thus with the potential to establish a spectrum of types of terror response in government, in the media and thus the public, and among the first and second responder machinery. The individual attack sites are listed here with the factors that drove their selection for the demonstration:

1. At the Capitol Building, at or adjacent to the east steps ascending to the Rotunda
    a. High global symbolic value
    b. Establishes the fear that even the highest level of security cannot secure a public access area
    c. Will create maximum response by first responders

2. At Pennsylvania Avenue and Constitution Avenue, adjacent to the National Gallery of Art and the Canadian Embassy
    a. High global symbolic value (Pennsylvania is the Nation's symbolic main street – joins Legislature (Capitol) to Executive (White House))
    b. An unsecured area with high traffic
    c. Priceless art is threatened
    d. May generate perception of multiple nations as targets and will exercise the diplomatic corps

3. NASA Headquarters (old location on Independence Avenue)
    a. High global symbolic value
    b. Draws in a new stakeholder
    c. Will escalate alert at all NASA facilities around the USA and abroad

4. FEMA Headquarters (10th and Independence Avenue)
    a. Moderate national symbolic value
    b. Create disruption within an existing stakeholder/responder

c. Potentially impact the second wave of response and the recovery

5. Smithsonian Metro Station (on the Orange/Blue trunk line of the Metro downtown system with entrances on the National Mall and at the Agriculture Department)
    a. High tourist use Metro station, serving the Smithsonian Institution
    b. East and westbound tunnels are open to each other in line sections adjacent to station and thus cannot be isolated (gas attack would shut down Orange/Blue Line operations in both directions)
    c. High potential for precipitating disruption to urban transport networks

6. Washington Monument
    a. Very high symbolic value
    b. Close to the White House
    c. Draws in the National Park Service and their police as a new stakeholder

7. Memorial Bridge across the Potomac River (one of the central arches)
    a. High symbolic value
    b. Close to Pentagon and Arlington Cemetery
    c. Key road transport artery for commuter access/egress
    d. Draws in additional water-based stakeholder/responder resources

The situation described above is relatively straightforward because of a number of simplifying assumptions made. However, even in this case the number of feasible terrorist scenarios is more than 14 millions. No human expert would be able to generate, not to mention to explore, such a number of scenario while a computer tool utilizing evolutionary computation will provide useful results in a short time.

The impact of the individual terrorist scenarios has been determined to obtain a synthetic fitness function. Such a function is sufficient to demonstrate system behavior, but in a system to be developed for actual security purposes, it will not be used since … a

precise fitness function will be employed whose values will be produced using various domain-specific simulation programs. The values of the synthetic fitness function for the individual scenarios have been determined in a two-stage process. First, a number of terrorist scenarios have been identified (approximately 50) and to each scenario a measure of its impact (fitness function value) was subjectively assigned. It has been done exclusively using our background knowledge without any formal studies conducted. Next, a special computer tool has been developed for the estimation of the impact of all remaining terrorist scenarios, which have not been evaluated by us. The program that generates these estimates uses similarity and complexity of various terrorist scenarios to estimate their impact and to create values of the fitness function for all feasible terrorist scenarios.

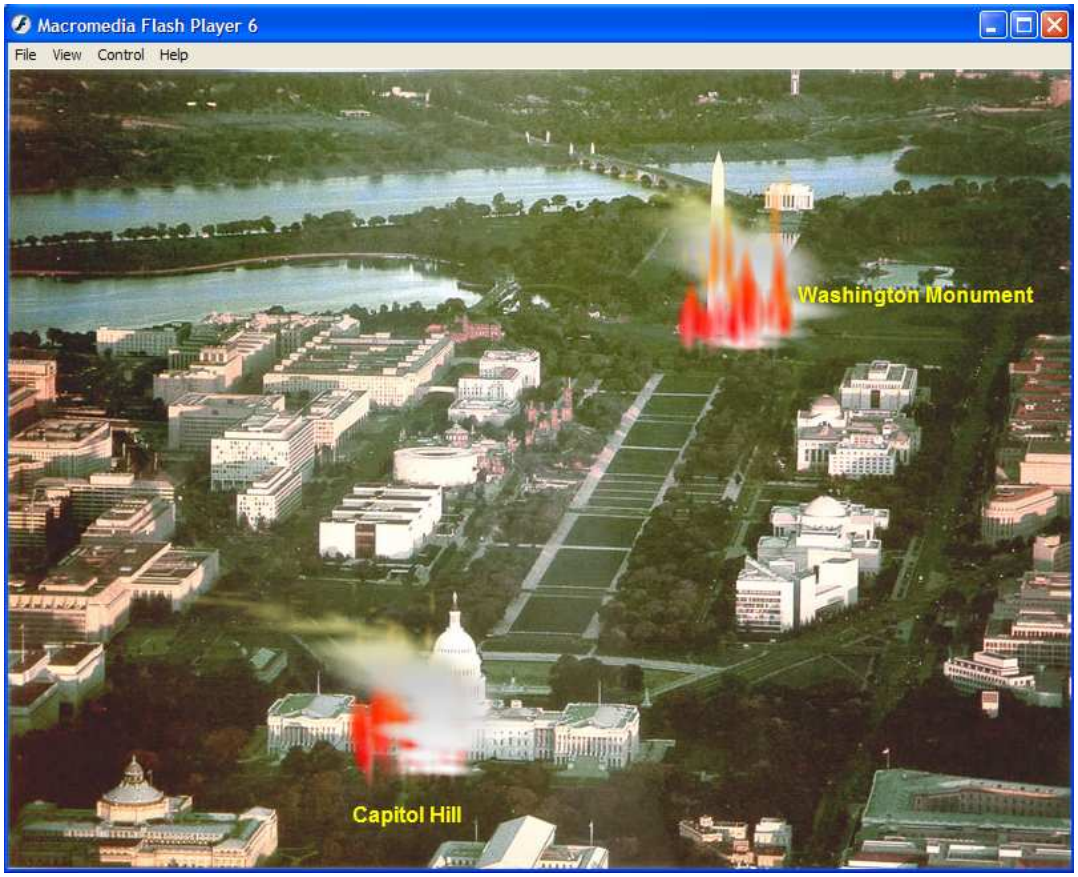

Figure 3. A sample terrorist scenario where an attack is conducted by two terrorist teams on the Washington Monument and on the Building of Congress.

In one of terrorist scenarios prepared by the authors to initiate the evolution process, it has been assumed that two terrorist teams would attack simultaneously. One attack would be on the Washington Monument causing an explosion and a fire while the second one would be on the Building of Congress, also causing an explosion and a fire as shown in Fig. 3.

Fig. 4 shows one of the terrorist scenarios generated by TerrorMax/Capitol Hill. The figure shows an abstract/computational representation of this terrorist scenario in the left top corner in the background. The central part of the picture shows four simultaneous attacks. In this case, a fire is started on the Memorial Bridge with a simultaneous use of a dirty bomb and biological weapons. At the Smithsonian Metro Station, a bomb is detonated while in the area around the Washington Monument a chemical attack is conducted. At the same time, the FEMA Headquarters is attacked with a combination of chemical and radioactive weapons.

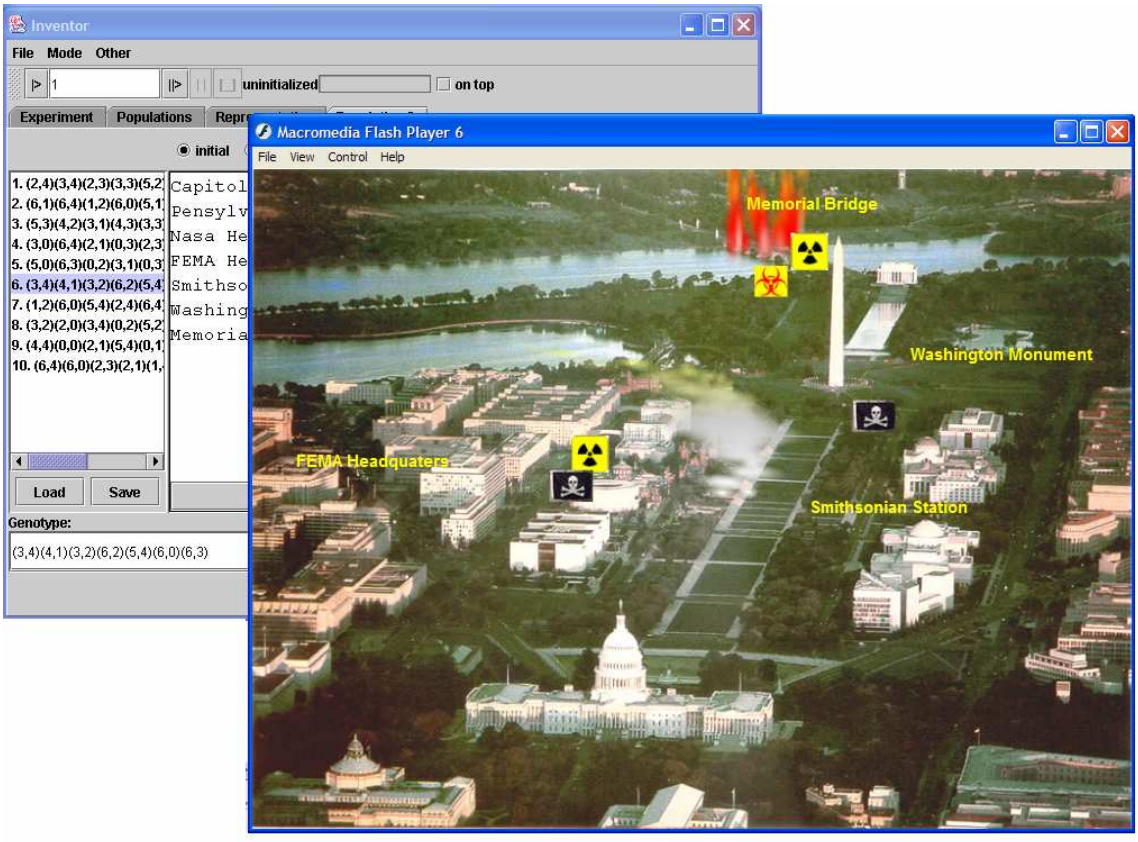

Figure 4. A terrorist scenario generated by TerrorMax/Capitol Hill.

The model of the evolution of terrorist scenarios has been implemented as a domain module in Inventor 2003 (Pullmann et al., 2003). Inventor uses ECKit (Potter, 1998) as an underlying evolutionary computation engine which was designed to support co-evolutionary models. Each terrorist scenario has been represented as a variable-length list of genes. Each gene in a list consists of two attributes. First one defines a location of a terrorist attack (e.g. the Capitol, or the Memorial Bridge) and can assume an integer value from 0 to 6. These values correspond to seven arbitrarily selected potential attack places described above. The second attribute specifies the type of attack that will be conducted at the location specified by the first attribute. It can assume one of five possible integer values (from 0 to 4) corresponding to previously selected types of terrorists attacks that have been described above.

The visualization module for Capitol Hill domain has been implemented in Macromedia Flash. A stand-alone Macromedia Flash Player is invoked from Inventor 2003 user interface and passed the values encoded in a genotype representing a terrorist scenario. The names of the locations where terrorist attacks occurred in that scenario are displayed during the visualization. Also, specific types of attacks conducted at these locations are visualized using symbols shown in Figure 2.

5. Initial Commentary

The reported research has been initiated only recently (July 1, 2003). Therefore, our commentary must be only preliminary and most likely will evolve as our research progresses.

There is no question that infrastructure systems in this country are highly vulnerable to asymmetric terrorist attacks and their security must be improved soon. The authors believe that the long-term solution is to design and construct new and replacement infrastructure systems in a way that satisfies all security requirements. Unfortunately, that will not improve the security of the existing infrastructure systems. In this case, the authors propose "Proactive Security." It is understood as a class of methods, models and tools, which have to be used in a systematic way in order to maximize the security of existing infrastructure systems. The

proposed proactive security will be based on a co-evolutionary approach in which terrorist scenarios and security plans are co-evolved. In the process, terrorist scenarios are evolved to maximize their impact on a given infrastructure system while security plans are evolved to minimize the impact of the generated terrorist scenarios on the infrastructure systems. The members of both populations are evaluated using the same simulation program for the infrastructure system being considered. The proposed vision requires significant amount of research and development before it may be operationally implemented in the form of various computer tools for proactive security. However, the process has already been initiated in the IT&E School at George Mason University. Our research utilizes results of design research on conceptual design, particularly of that on co-evolutionary conceptual design, which has been conducted by several of the authors.

The developed demonstration system, named TerrorMax/Capitol Hill, illustrates the principles behind proactive security, although it is currently limited only to the evolutionary generation of scenarios. The system should ideally demonstrate to infrastructure security professionals the feasibility of building co-evolutionary-based computer tools for determining proactive security measures for actual infrastructure systems.

Infrastructure security is a fascinating research area, and also one of major national interest and importance. The authors hope that this introductory paper will stimulate a productive discussion about fundamentally new approaches to security and ultimately will contribute to the improvements of security of infrastructure systems.

References

Angeline, P. J., & Pollack, J. (1993). *Competitive environments evolve better solutions for complex tasks.* Proceedings of the 5th International Conference on Genetic Algorithms (ICGA-93), University of Illinois at Urbana-Champaign.

Arciszewski, T. (2002). *Design and inventive engineering: lecture notes*. Fairfax, VA: IT&E School, George Mason University.

Arciszewski, T., & De Jong, K. A. (2001). *Evolutionary computation in civil engineering: research frontiers.* Proceedings of the Eight International Conference on Civil and Structural Engineering Computing, Eisenstadt, Vienna, Austria.

De Jong, K. A. (to appear). *Evolutionary computation: a unified approach*. Cambridge, Mass.: MIT Press.

Fogel, L. J., Owens, A. J., & Walsh, M. J. (1966). *Artificial Intelligence through simulated evolution*. Chichester, UK: John Wiley.

Holland, J. H. (1975). *Adaptation in natural and artificial systems*. Ann Arbor, Michigan: University of Michigan Press.

National Research Council (2002). *Making the nation safer: the role of science and technology in countering terrorism*. Washington, DC: National Academies Press.

Potter, M. A. (1998). Overview of the evolutionary computation toolkit. *Unpublished document*.

Potter, M. A., & De Jong, K. A. (1994). *A cooperative coevolutionary approach to function optimization.* Proceedings of the 3rd International Conference on Evolutionary Computation and 3rd Conference on Parallel Problem Solving From Nature, Jerusalem.

Pullmann, T., Skolicki, Z., Freischlad, M., Arciszewski, T., De Jong, K. A., & Schnellenbach-Held, M. (2003). *Structural design of reinforced concrete tall buildings: evolutionary computation approach using fuzzy sets.* Proceedings of the 10th European Group for Intelligent Computing in Engineering EG-ICE, Delft, The Netherlands.

Rechenberg, I. (1973). *Evolutionsstrategie; Optimierung technischer Systeme nach Prinzipien der biologischen Evolution*. Stuttgart-Bad Cannstatt: Frommann-Holzboog.

Shelton, K. (2003). *Conceptual design: co-evolutionary approach.* Ph.D. Proposal, George Mason University, Fairfax.