Modeling the Design of Death:

Adaptive, Predictive Rapid-Response Knowledge Systems and Communications in support of Strategic and Tactical Responses to Biological and Chemical Threats

Martin J. Dudziak, PhD

Silicon Dominion Computing, Inc.

under contract to Defense Advanced Projects Research Agency

Draft in Progress – Not for Public Release

1. INTRODUCTION

Several major research initiatives undertaken by the United States and other governments in recent years are focused upon providing improved deterrents to very critical and high-probability threats of terrorist and other actions using biological and chemical weapons of mass destruction. These threats have, as in the case of the AUM Shinrikyo attacks using sarin gas against civilians in the Tokyo subway system (1995), emerged into reality from not only government sponsored and sanctioned military and paramilitary operations but also from relatively autonomous independent groups with a variety of political, religious, and (as in the Oklahoma City Federal Building massacre) personal motivations.

The purpose of this paper is not to analyze or critique in depth such "asymmetric" and non-standard threats or actions that have occurred in the past, nor the information and knowledge-based systems that have been the subject of much research and development over the past several years, nor operational methods and actions that have been employed in the gathering of intelligence and the development of pre-emptive and attributory investigations by intelligence, military, and civilian law enforcement agencies.

The goal here is to present and to discuss various approaches, both analytical and operational, that are perhaps somewhat novel and different from those that have been developed thus far. These new approaches are seen to be complementary, supportive, and valuable for the successful design and deployment of knowledge systems that will help in the future prevention of biological and chemical warfare incidents, particularly in the very near-term (1999) when there are several conceivable "Y2K" threats that may be expected to occur.

There are indeed serious concerns to be raised concerning events that may occur on or shortly after Midnight, January 1, 2000 in not only the chem/bio domain but in the form of acts of information warfare and sabotage, actions that can be expected from a variety of groups some of which operate under religious and quasi-political "millenium apocalypse" philosophies. Certain acts of information warfare may be designed and executed to not merely disrupt sensitive global or national computer systems but to disrupt certain chemical, biological, or nuclear installations that would result in a catastrophe which could be ascribed by the group and its advocates as being some form of apocalyptic or doomsday event that was predestined or otherwise of supernatural origin.

This context of a "Y2K" chem/bio/info terrorist strike can, therefore, provide more than simply a realistic scenario for use in modeling how a knowledge discovery, data mining, and reasoning system (complete with processes and methods leading to the formation of testable hypotheses and their use by analysts, strategists, and operatives) can be designed. It can provide the basis for a tactical toolset to be used in circumventing a very real threat that can be expected and which under certain circumstances could be a joint effort of several groups working together, albeit not necessarily sharing the same motives and rationales.

Two suggested scenario are presented in Chapter 2, both based upon this context and introductory groundwork. Alpha Scenario concerns a suggested "challenge problem" topic of interest to DARPA ISO, DSO groups and to other US agencies, namely the planning and construction of a biological weapons strike capability including a production plant, storage, and delivery mechanisms. The scenario is presented rigorously not from the perspective of the analyst looking towards and for a terrorist group but rather from that of a committed "Y2K Apocalypse" terrorist cadre that is already (3/99) organized and engaged in their planning activities.

Alpha Scenario, and the entire development of information technology and related BWD technology that will serve as the architectural building blocks and tools for an adequate, reliable response system to deal with such a scenario, is all presented in the light of an evolutionary approach to solving problems that face current response tools including knowledge engineering technology that has been under development for several years and more.

An alternative is the Beta Scenario. This may be combined with Alpha for the study, modeling, and development of countermeasures to defeat a multi-pronged strike intended to kill and injure thousands of people and to do so with relative ease because of an event such as New Year's on Times Square. By itself Beta Scenario concerns the use of small private airplanes, loaded with ANFO or FAE type explosive devices, for targeting high-profile skyscrapers such as the World Trade Center in New York (an obvious target because of the 1993 terrorist attack and an "incomplete job" in the minds of the perpetrators), or a comparable high-rise or complex of high-rises (Sears or Hancock Towers in Chicago, the ARCO twin towers in Los Angeles, the Transamerica building in San Francisco, the cluster of high-rises in Houston, Atlanta, or even downtown Boston).
.

What is presented in this paper is intended as an extension and evolution of concepts and architectures defined in the course of work to date in Project Genoa and related efforts by US agencies, including High Performance Knowledge Base (HPKB), Intelligent Integration of Information Technology (I3), Knowledge Discovery and Data Mining (KDD), and Rapid Knowledge Formation (RKF) projects. What is somewhat different and novel is the emphasis upon two fundamental tenets, one having to do with information science, computation, and the attainment of knowledge engineering goals, and the other having to do with sources of information, models, and expertise that are needed for such a knowledge enterprise.

These can be briefly described as:

(1) Emergent complexity and self-organization as a means toward increasing and accelerating knowledge.

- ♦ The use of self-organizing dynamical systems theory, and computational methods developed for nonlinear learning systems including but not limited to neural networks, cellular automata, and massive parallel "field" computing, applied to the problem of pattern discovery and detection, uncertainty resolution, and the reduction of search strategies.
- ♦ The use of both models and physical devices in BWD sensor technology and information gathering that incorporate principles of emergent, complex, hierarchical behavior, some of which are subjects of active research along different tracks and for different purposes within other DARPA organizations (e.g., ITO Ultrascalar Computing).

(2) The role of first-person agent modeling and simulated thinking for generating accurate axioms and patterns of reasoning within the knowledge bases that are to be employed by agents and analysts and policy makers.

- ♦ The orientation of challenge problem definition and modeling to fit the mindset and methods or modus operandi of individuals and groups that are engaged in the sponsorship and execution of programs for biological and chemical warfare.
- ♦ The generation of logics and axiomatic elements that reflect the thinking and framework of both known and conjectured groups that would be likely to conduct missions of chemical and

biological warfare in the context of transnational or intranational threats for political, religious, or economic motivations.

2. The Scenario

2.1 The Modern-day “SS” – The Seventh Seal Organization

2.1.1 Origins of the Group

2.2.2 Personal History of the Founder

2.1.3 Leadership Echelon

2.1.4 Philosophical Tenets

2.1.5 Genesis of the Group

2.1.6 Cadre Formation

2.1.7 Interpersonal Dynamics

2.1.8 Economic Structure

2.1.9 Informational Dynamics

2.1.10 Security and Paramilitary Practice

2.1.11 Training
Alpha Scenario – biological weapon/agent secural, preparation, handling, delivery

Beta Scenario – private flight training, licensing, route planning, logistics

2.1.12 Counter-countermeasures
Defeating security circumspect to large public gatherings

Defeating air control security

2.2. The Mission

2.2.1 Jan. 1, 2000, 12:00:01

Initiation of the Project

Long-Term Planning

Project Schedule

Distribution of Responsibilities and Authorities

2.2.2 Countdown 1999

Infrastructure and Fail-Safe Definition

3. Evolutionary and Emergent Self-Organization and Cognition

3.1 Theoretical and Mathematical Foundations

3.2 Rosen, Kampis and Categorical Bases

3.2 Origins and Relations with Cognitive Science and Psychology

3.2 Geometrical Modeling of Organizational and Group Thought Processes

3.3 Atkin and Simplicial Complex Models

3.4 Casti and Geometrical Paradigms for Social Process

3.5 Surprise Theory and Building Surprise Predictors

3.6 Application of Geometric Algebra and "Knowledge-Plane Tiling" Concepts

3.7 Detectable Features and Patterns

3.8 Arbitrary and Deliberate Incompleteness

3.9 Tags, Broken Needles, and Stray Fingerprints

4. Computational Modeling Issues and Approaches

4.1 Differences in Modeling and Testing Requirements

4.2 Selective Technologies of Merit

4.3 HAL – Holographic Associative Learning

4.4 SONON – Self-Organizing Nonlinear Oscillator Networks

4.5 TCL – Topological Classification and Learning

5. Integration with Reasoning Systems and Knowledge Bases

5.1 Axiom-Based Reasoning and Prediction Systems

5.2 Nonlinear Complexity and Pattern Recognition As Enhancements for Knowledge Discovery

5.3 Rapid Hypothesis Generation and Explication

5.4 Hypothesis Pruning and Conjecture-Space Reduction

5.5 Not Throwing Out the Pearls with the Dishwater

6. Tactical Systems Development Topics

6.1 Information Acquisition and Field Communications

6.2 HUMINT, ELINT, and "BIOINT" Coordination

6.2.1 CBD Field Arrays and Amorphous Networks

6.2.2 Appropriate Distribution and Interpretation

6.2.3 Getting the Knowledge to the Operative

6.2.4 Distributing the Knowledge to the Aware-Sensitive Community

6.3 Application of Mobile and Autonomous Collection Models and Technologies

6.4 Integration with Incidence Response Forces and Authorities

6.5 Weeding Out the False Alarms

6.6 Circumvention and Attribution

6.7 Second-Guessing and Staying Ahead

6.8 Matching the Brains of the SS

7. System and Project Modeling Approaches

7.1 UML-Based Methods for Component Design and Development

7.2 Document and Program Structure and Coordination

7.3 Experiments and Challenge Problems

7.4 How Does a Constructed 1M-Axiom Knowledge Base Become Adaptive?

7.5 How Does A Collective Brain Learn About What It Should Pay Attention?

7.6 What is the Right Measure of Success in the Model?

8. Conclusions and Next Steps

