

# **Computational Intelligence and Threat Assessment**

**Fuzzy Logic and Computational Intelligence  
in Threat Detection, Validation, and Interdiction.**

©2001 Earl Cox



1289 North Fordham Blvd. Suite A312  
Chapel Hill, NC 27517

(919) 678-0477  
[www.scianta.com](http://www.scianta.com)

Who dares wins.

Motto of the British Special Air Service regiment, from 1942.

See J. L. Collins *Elite Forces: the SAS* (1986), *Introduction*.

Rien n'est plus dangereux qu'une idee,  
quand on n'a qu'une idee.

*Nothing is more dangerous than an idea,*

*when you have only one idea.*

--Alain (Emile-Auguste Chartier, 1868-1951)

*Propos sur la religion* (1938) no. 74

There are two parts to the human dilemma. One is the belief that the end justifies the means. That push-button philosophy, that deliberate deafness to suffering, has become the monster in the war machine. The other is the betrayal of the human spirit – the assertion of dogma that closes the mind and turns a nation, a civilization, into a regiment of ghosts – obedient ghosts or tortured ghosts.

It is said that science will dehumanize people and turn them into numbers. That is false, tragically false.

Look for yourself. This is the concentration camp and crematorium at Auschwitz. This is where people were turned into numbers. Into this pond were flushed the ashes of some four million people. And that was not done by gas. It was done by ignorance. When people believe that they have absolute knowledge, with no test in reality, this is how they behave. This is what men do when they aspire to the knowledge of gods.

Jacob Brownowski (1908-1974)

*The Ascent of Man*

In the thirtieth century BCE, Babylonian couriers carried encrypted messages along the Tigris and Euphrates rivers. The encryption was simple – like Leonardo Da Vinci a millennia or two later, they simply reversed the message's cuneiform symbols. Many examples of such tablets, scattered between prayers to Ishtar and the Epic of Gilgamesh have been found in the ruins of Mesopotamian cities. Here we find the condition of river marshes, the movement of troops, and early examples of weather forecasts (probably just as inaccurate then as now.) In those early days of The First Cities, the threat to civilization was real and persistent. Removed by only a few thousands years from the last vestiges of the great Ice Ages, these fragile rectangular cities of mud bricks and timbers, scattered along the silt banks of a few rivers in Asia Minor, held tenuously to law and societal order against the wild tribes of hunter/gathers that still roamed the wilds of a sparsely populated world. The loss of a single city could end civilization in the region for a millennium.

Today, civilization has come under renewed attacks by determined enemies very similar to those that poured out of the mountains into the flood plains of Babylon five thousand years ago. But unlike the early protectors of civilization, we cannot rely on spies in mountain passages watching for camp fires, dust clouds, or thunder storms. Nor, apparently, can we rely on our equivalent to the high walls and cleared approach fields of Babylonian cities – remoteness from enemies, spy satellites, and tactical and strategic weapons. In our modern global but highly heterogeneous society, security stems from knowledge and intelligence. Such a reliance on intangibles should come as no surprise to anyone who considers the immense cultural, economic, and technological complexity of our world –

- it's confusion of beliefs that polarize entire subcultures into defending their version of "truth:"
- it's open, collective and unfiltered sharing of immense amounts of information of vastly varying degrees of purpose, certainty, civility, and accuracy.
- it's imbalance in the distribution of critical land, financial, economic, and opportunity resources
- it's steady evolution into a blend of societies united by their dependence on highly vulnerable computer technologies
- it's near uniform coherence as a world village – allowing huge numbers of anonymous people to easily move around its continents in time frames of hours and days

In such a village universe populated with dense cities connected by weakly supervised air, land, and sea lanes, the ideas of a few can be translated into aggression against the many. Physical barriers are ineffective. Militaries are ineffective. Even the unified purposes of member nations opposing the ideas of these few are ineffective. Thus, the future strategic security of a nation will increasingly depend on its ability to collect, correlate, interpret, connect, and evaluate a wide spectrum of intelligence sources. Unlike the intelligence gathering objectives of just a few years ago, this new intelligence perspective attempts to find weakly expressed, weakly emerging, and weakly supported behavior, movement, and asset acquisition patterns in the ordinary workings of our culture – including but not limited to banking and financial transactions, credit card purchases, insurance and re-insurance policies, local, state and federal licensing, accident reports, government agency supervisory reports, shipping and transportation waybills, pre-lodge, and container manifests, voice communications, and electronic mail.

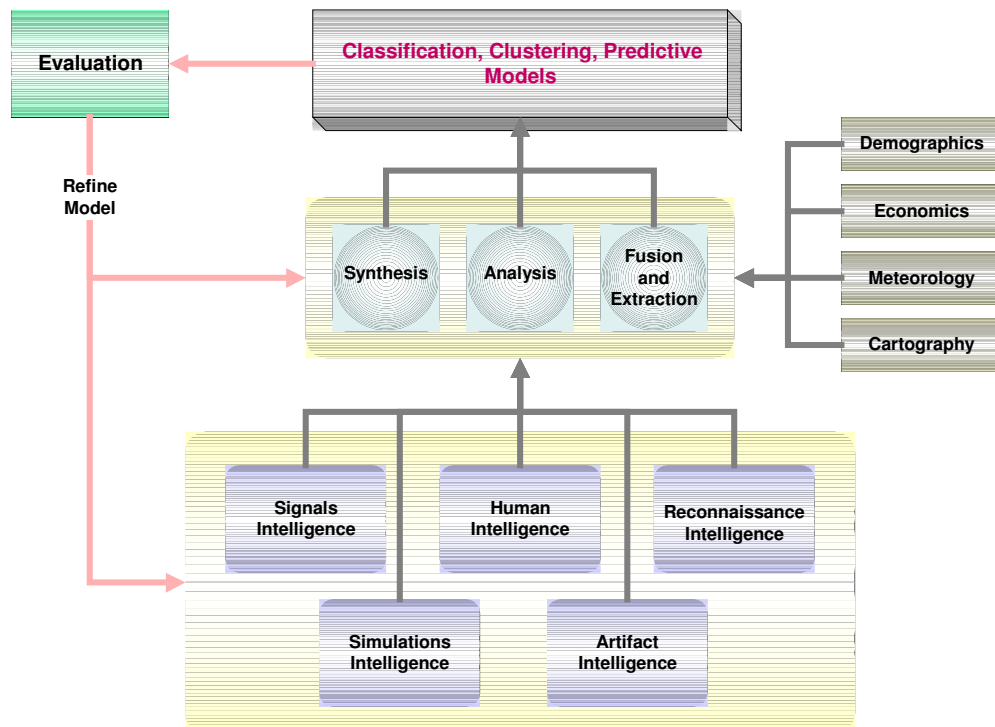
Also not surprisingly, the use of computational intelligence to augment or even replace many forms of standard knowledge and intelligence analysis has increased dramatically. In today's marketplace of ideas there is no room for technology agoraphobia. In this article we examine some of the ways in which advanced artificial intelligence techniques and methods are fused with traditional national security issues to create a new, powerful and more robust intelligence service.

## The Intelligence Process

Intelligence is concerned with recognizing the unusual. Often the unusual is in the form of hidden patterns – implicit and explicit connections between events, processes, things and concepts. And just as often, these patterns are very weak and are scattered over long periods of time. To find, collect, and organize and analyze these patterns the intelligence community employs a wide variety of sensors. These sensors are involved with gathering intelligence from agents in the field (human intelligence or *humint*), from intercepting and analyzing communications (signal intelligence or *sigint*), and from photographic, in a general sense, sources (reconnaissance intelligence or *recon* data). From these and other sources, the intelligence analysts apply a broad spectrum of analytical tools and techniques to create models that explain as well as predict behavior.

## Data Fusion and Intelligence Models

Threat assessment – the heart of an intelligence model – is an exercise in data fusion (often, in engineering parlance, called sensor fusion.) Nearly all military command systems involved with tactical operations include a wide spectrum of data fusion parameters – thermal and acoustic energy levels, pulse and broad band electromagnetic radiation, ground trembling harmonics, ambient radiation levels, and so forth. Intelligence models use a kind of knowledge fusion to create an accurate estimate of the threat based on an extremely wide range of possible sensor data (where, of course, “sensor” is used to mean any source of input.) Figure 1 illustrates schematically how this modeling process works,



**Figure 1.** The Intelligence Analysis and Modeling Process

As we see, intelligence models at the analysis and synthesis level also fuse incoming data – *sigint*, *humint*, and *recon* data – with specific and general knowledge about the world at large. Strategic and tactical intelligence models must incorporate knowledge about a region or country’s political structure, military capabilities, demographics, economics, weather, and terrain. These statistics are critical in making sense of the model’s raw data, interpreting their meaning, and predicting a future course of action.

Figure 1 also shows two other common sources of intelligence data – artifacts and simulations. Artifacts comprise an entire sea of miscellaneous and often seemingly unrelated data points including news paper and journal extracts, acquired photographs, local bus, train and airline schedules, average costs for services (meals, taxi tips, grocery purchases, and so forth). Although sometimes lumped into signals or reconnaissance intelligence, artifact information is treated and processed quite differently both in terms of its evidence value and its applicability to the analyst’ objective function.

Simulation intelligence – an odd way of looking at knowledge gathering - provides insight into possible scenarios and causal relationships between events and processes. Simulating a car bomb explosion,

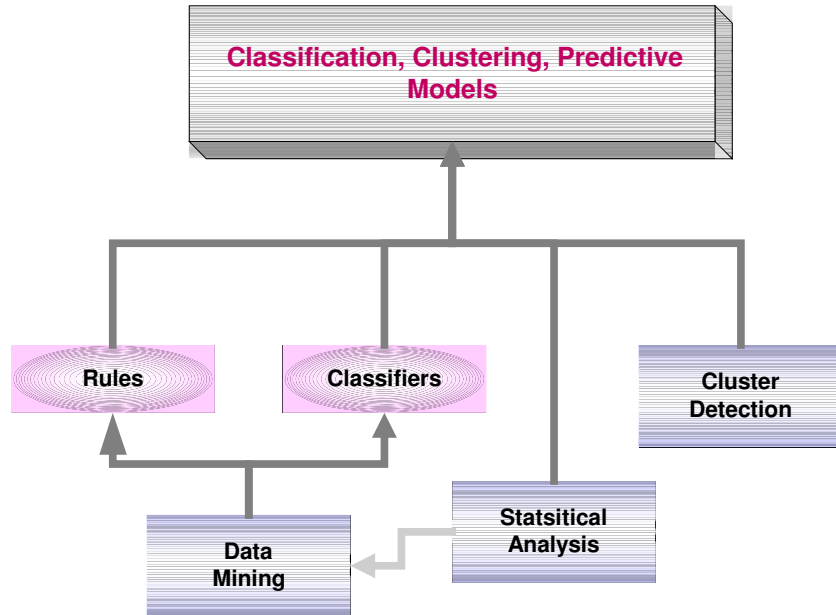
as an example, provides, over thousands of runs, statistical information about material scattering, types and degrees of collateral damage, concussion (blast) effects, and injury as well as fatality radiating patterns. The results of these simulations -- used with pattern matching and principal component analysis techniques -- add robustness and high degrees of selectivity to models that must interpret, classify, and explain unusual phenomena.

Commercial threat simulators using expert system technologies are already available. These systems, in effect, model such events as bombs and airline crashes in order to understand both risk and degree of threat. An example is *Rampart*, built by Sandia National Laboratories. Developed following the Oklahoma City bombing in April, 1995, Rampart estimates the tolerance buildings have for similar disasters. Rampart has a database of possible threat scenarios. These are used by its integrated expert system to predict how various threats -- earthquakes, tornadoes, hurricanes, and bombs of various kinds -- will effect the structural integrity of a building. At its heart Rampart borrows risk assessment and mitigation methods from those employed to assure the safety of our nuclear weapon stockpiles. Modeling software like Rampart are routinely used to simulate and study the characteristics and effects of everything from highway traffic patterns during extreme emergencies to bombs (nuclear and conventional) to chemical and biological attacks in highly populated centers.

## Building Intelligence Models

The degree to which the analyst selects the proper sources, provides the correct correlation between intelligence elements, removes noise (that is, deals with the signal to noise ratio) and applies the best analysis architecture will determine the final strength of the model. A good, robust model reduces ambiguity and strives to provide evidence for its conclusions in forms that are consistent with the reliability, certainty, and accuracy of the underlying sources. It is then up to the analysts to understand the implications of the model (this is often the weakest link in the intelligence chain and the place where a powerful model combining conventional statistical techniques with computational intelligence often yields a very high payoff.)

Even at its low level of granularity, Figure 1 illustrates the complexity of today's intelligence models. Combining high quantities of raw and processed data of varying degrees of coherence, completeness, and trustworthiness, simulations, artifacts, demographics, climatology, geography, and economics an intelligence model must evolve a consistent, complete, and understandable picture of the underlying patterns. Thus today, more than ever, knowledge discovery (data mining) and other artificial intelligence technologies form the core tools for such models. Figure 2 shows some of the important components of these models.



**Figure 2.** Components of the Basic Intelligence Model

At the core of modern intelligence models we find several important artificial intelligence technologies. While the intelligence community has long used a wide spectrum of statistical techniques (no surprises there), rule based expert systems (to capture the knowledge of such rare and critical skills as photo interpreters and logistics analysts) and neural networks, the next generation of intelligence models employ and have an increased reliance on fuzzy logic, genetic algorithms, and evolutionary programming. In modern intelligence models we find a consortium of interlocking technologies.

- Data mining or knowledge discovery has become an essential element, generating *if-then* rules or complex decision tree classifiers. In many cases the classifier is, in fact, the data mining process itself and is associated with a form of unsupervised neural networks (such as self-organizing maps also known as Kohonen Nets.) The use of rule induction algorithms coupled with fuzzy logic gives these next generation data mining systems a very powerful and highly robust method of automatically generating fuzzy expert systems that describe the behavior of multiple patterns within the same collection of data.
- Both separately and as part of the data mining process, descriptive statistics as well as statistical learning theory plays a vital role in understanding and interpreting the organization and meaning of data. In particular, statistical learning theory provides modelers with an adaptive feedback capability which detects and exploits period behavior sin time-varying data. Multiple models can be extracted, each representing different levels of granularity and periodicity in the data (that is, daily, weekly, monthly, or semi-annual patterns.)
- Multi-dimensional cluster analysis also plays an ever increasing role in understanding the relationship between sets of data points. Fuzzy clustering algorithms such as the extended fuzzy c-means and the Gustafson-Kessel algorithms allow data points to reside in multiple clusters each with its own degree of membership in the cluster. Overlapping and non-unique cluster memberships provide a powerful and easy to use way of finding weakly occurring patterns in the data.

It is often surprising to find, in fact, that fuzzy models play an ever more critical role in building high performance intelligence models (where performance, of course, is measured in a model's ability to detect and illuminate very weak patterns emerging from background noise.) These models take the form of both rule-based expert systems and, in an evolving intelligence community trend, in the form of case-based reasoning (CBR) systems. Fuzzy CBR systems have the ability to form solutions – often in the form of a dynamically created rule-base - by finding cases that are similar to the current problem state based on fuzzy measurements. In this way the strength of the similar function as well as the degree of evidence is directly reflected in the fuzzy parameters of the model.

## Detecting Anomalous Behavior

Anomalous behavior of aluminum near the melting temperature: transition  
in the rate controlling mechanism of yielding and realization  
of superheated solid states under tension

*Micromechanisms of Deformation and Fracture.*

*Gennady Kanel, Sergey Razorenov*

*(Institute of Problems of Chemical Physics, Chernogolovka, Russia),*

*Kurt Baumung, Josef Singer (Forschungszentrum Karlsruhe, Germany)*

Researchers in metallurgy are concerned with state transition anomalies. Security vendors and IT managers are concerned with anomalous behaviors caused by network intruders. Intelligence analysts are concerned with a wider and much more difficult to quantify aspect of aberrant behavior. In the world of intelligence, anomalous behavior means behavior directly associated with a threat and takes many, many forms, not all of which are easy to understand let alone detect.

Scientists at the Nanyang Technological University in Singapore have developed a neural network system that sounds an alarm when it detects suspicious or unusual behavior such as people shouting, running, or making violent gestures. Yet tuning the system to perhaps distinguish airline workers from terrorists in such places as cargo area is still an unattainable goal. “Anomalous”, however, means more than unusual and extends beyond human behavior. In detecting *anomalousness*, a system must employ sophisticated learning algorithms that can distinguish between routine behavior in various contexts and truly anomalous behavior. Several commercial AI-based systems are adept at finding and quantifying anomalous behaviors. As an example, a recent Business Week article by Otis Port describes a version of HNC's Falcon software (used to detect credit card fraud) that monitors banking transaction looking for anomalous transactions – many small deposits, unusual international cash transfers or numerous similar deposits of cash from questionable sources. Such a system could conceivably uncover the movement of financial assets used by terrorist cells.

In intelligence models, anomalous behavior is not strictly associated with people, although identifying the strange or unexplained behavior of many related individuals would be a critical component of isolating and pinning down terrorists. In fact, behavior is an emergent property of the analysis – becoming visible when many perhaps seemingly unrelated data elements are brought together and properly correlated. In this respect computational intelligence techniques powered by fuzzy logic and neural networks provide the analysts with a deep insight into patterns associated with such events and processes as,

- The movement of containers and cargo by truck outside the secure facilities of the receiving depot.
- The purchase of chemicals, building materials, hardware that, by itself would not be unusual, but taken together and related by a common transaction mechanism (e.g. a credit card)

# Computational Intelligence and Threat Assessment



- The attempt to license or purchase hazardous materials
- The attempt to acquire potential delivery systems for chemical or biological warfare agents (such as crop dusters, highway asphalt or insecticide spraying trucks)
- An attempt to gain a common set of rare or unusual skills (such as the recent attempt by the World Trade Center attackers to gain pilot certification)
- The theft of particular classes of vehicles - a mixture of UPS or Federal Express trucks as an example. These vehicles are so ubiquitous in our society that they are effectively invisible in large metropolitan areas.
- The recent acquisition of commercial or private driver's licenses (associated with other factors)
- Unusual but often sporadic, sparse, and low impact financial activity (some forms of this were covered in the previous discussion of HNC's falcon system.)

Many of the intelligence indicators used in threat assessment models may violate or at least threaten our sense of due process and privacy. Consequently most national security models used in the intelligence field work in a definite cascading pattern – recognizing significant anomalies with sufficient evidence to acquire court sanctions. In this regard computational intelligence models that aggregate and systematically process evidence (such as fuzzy systems), although not meeting the standards of our judicial system, do provide the analyst with faith that they have discovered a real behavior and not a statistical fluctuation in the background noise.

## And In Conclusion....

Artificial intelligence techniques have long played a part in conventional intelligence models – supporting voice recognition, image and pattern detection, text (document) analysis, and, to a somewhat lesser degree, cryptographic key management. But today they are becoming the essential backbone for a new generation of intelligence models whose aims are more aligned with domestic terrorism than conventional battlefield wars. These new models are significantly constrained by the huge number of variables, the faceless anonymity of the enemy, the enormous amount of background clutter, and our long standing social and legal history that often mitigates against the collection and use of data that would compromise our constitutional safeguards. It is unlikely (but not totally unthinkable) that we would willingly give up our freedoms even in a protracted war against terrorism – thus the new family of intelligence models must make the most out of their available data sources. In order to accomplish this task, analysts are turning to powerful fuzzy logic and neural network models often augmented by genetic algorithms that rapidly tune the model based on historical data as well as adaptive feedback from the model itself. The future belongs to models that think for themselves.

## Intelligence Sites:

The Central Intelligence Agency  
National Intelligence Council  
National Security Agency  
Defense Intelligence Agency  
National Reconnaissance Office  
National Imagery and Mapping Agency  
National Counter Intelligence Center  
Center for the Study of Intelligence

<http://www.cia.gov/>  
<http://www.cia.gov/nic/index.htm>  
<http://www.nsa.gov/>  
<http://www.dia.mil>  
<http://www.nro.gov/>  
<http://www.nima.mil>  
<http://www.ncix.gov/index2.html>  
<http://www.odci.gov/csi/index.html>

# Computational Intelligence and Threat Assessment

---



President's Foreign Intelligence Advisory Board  
The Centre for Counterintelligence and Security

<http://www.whitehouse.gov/pfiab/index.html>  
<http://cicentre.com/>

(State Dept.) Office of the Coordinator for Counterterrorism  
<http://www.state.gov/www/global/terrorism/index.html>

Justice Dept. Office of Intelligence Policy and Review [http://www.usdoj.gov/jmd/mps/mission.htm#N\\_OIPR\\_](http://www.usdoj.gov/jmd/mps/mission.htm#N_OIPR_)

Association of Former Intelligence Officers

<http://www.afio.org/>

Earl Cox is the founder, Chief Technology Officer, and sole employee of newly formed Scianta Intelligence Corporation an advanced business intelligence and data mining company. Earl is the author of *The Fuzzy Systems Handbook* (1994,1998, Academic Press Professional), *Fuzzy Logic for Business and Industry* (1995, Charles River Media), and, with Greg Paul, the award winning *Beyond Humanity: CyberEvolution and Future Minds* (1997, Charles River Media). He can be reached at [earldcox1@home.com](mailto:earldcox1@home.com).

---

For more information or to schedule a presentation call (919) 678-0477 or visit [www.scianta.com](http://www.scianta.com)

# Computational Intelligence and Threat Assessment

---



©2004 Scianta Intelligence, LLC  
AR-PA-013