An Outcome-Based Learning Model to Identify Emerging Threats: Experimental and Simulation Results

Ignacio J. Martinez-Moyano
Argonne National Laboratory
imartinez@anl.gov

Stephen H. Conrad
Sandia National Laboratories
shconra@sandia.gov

David F. Andersen
University at Albany
david.andersen@albany.edu

Abstract

The authors present experimental and simulation results of an outcome-based learning model as it applies to the identification of emerging threats. This model integrates judgment, decision making, and learning theories to provide an integrated framework for the behavioral study of emerging threats.

1. Introduction

In this paper, the authors expand on previous work regarding the behavioral aspects of emerging insider threat identification [22, 27] to include the analysis of experimental results[1]. Through experimentation, we conduct empirical validation of the dynamic theory to increase confidence in the usefulness of the model [30]. Our model, based on reinforcement learning theories, is used for the behavioral study of emerging threats [2].

2. Learning models

Learning models have been explored in many disciplines, including psychology, economics, educational research, and instructional systems development literature. Three main types of learning models have been identified and empirically explored: reinforcement models, belief-based models, and mixed models. Reinforcement models are based on the premise that people learn with experience [20]. Although it can be difficult to directly experience the consequences of many of our decisions [29], in these models, learning is achieved by identifying the different outcomes of peoples' decisions and by assigning utilities to those that promote change (improvement) in their experience. Good outcomes reinforce the strategies used, while bad outcomes generate pressures for change in strategies [7, 8, 14]. Belief-based learning models focus on the role of notions of past performance and expectations of future performance as drivers of change in strategies [9]. Mixed models use characteristics of both reinforcement models and belief-based models to capture a wider range of human learning processes than either model alone [6, 18].

3. Methods

We used system dynamics to develop the model presented here [10, 28, 30]. The system dynamics approach helps researchers gain insight into dynamic problems by providing a framework to identify the causal structure that conditions the observed behavior of systems [for examples of the use of system dynamics in the study of identification of threats, see 24, 26].

For many scientists, empirical validation is the gold standard for model validation. In system dynamics, we pose models that are theories about real systems that, "must not only reproduce/predict its behavior, but also *explain* how the behavior is generated" [1, pp. 185-186]. Therefore, in order to build confidence in our models, we conduct behavior reproduction tests, but only as one of many other types of tests [28, 30]. Behavior reproduction tests alone are considered fragile tests of confidence because several causal structures, with enough degrees of freedom, can generate almost any temporal behavioral pattern. However, empirical validation, paired with deep understanding of the causal structure that conditions the observed behavior, is extremely useful for enhancing system understanding and generating "the right output behavior for the right reasons" [1, p. 186].

Throughout the development of the model presented here, the authors conducted several confidence building tests as recommended in the system dynamics literature [10, 23, 28, 30].

[1] The work presented here builds on previous work developed with Thomas R. Stewart, Eliot H. Rich, and Elise Weaver from the University at Albany. The authors acknowledge their valuable contribution to this work. Additionally, the authors thank Ido Erev, Michael Samsa, and Bill Buehring for their constructive comments on earlier versions of this paper. All errors are responsibility of the authors.

1530-1605/07 $20.00 © 2007 IEEE

4. Model description

4.1 Model overview

The model focuses on the interaction of outcomes and the level of the decision threshold over time. Figure 1 shows a simplified version of the feedback structure of the model.

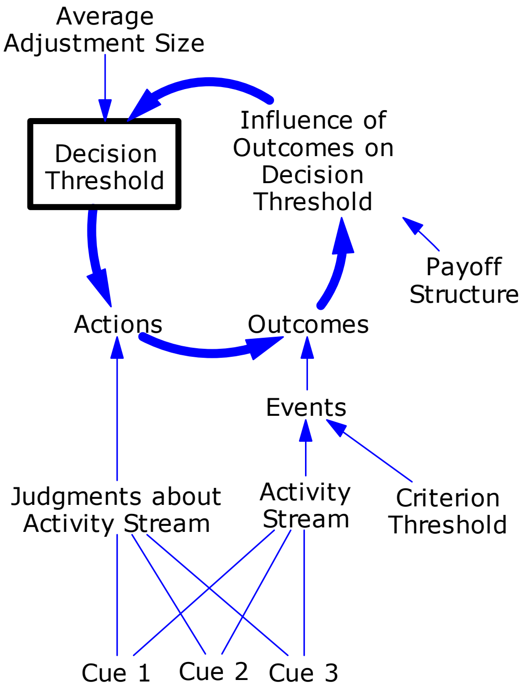

Figure 1. Model overview

The model has four main sectors: the judgment sector, the decision-making sector, the outcome-decomposition sector, and the outcome-based learning sector. These sectors are interconnected and are part of the same complete causal structure that represents a prototypical decision maker in a detection-selection-action process.

The learning model presented in this paper is the result of a theory integration effort to capture the main components of the judgment and decision making processes present in the detection of emergent threats in organizations.

In our model, we integrate concepts from social judgment theory [4, 5, 13, 15, 16], signal detection theory [12, 34, 35], and the psychology of learning, particularly reinforcement learning theories discussed both in the psychological and economics literature on human learning [6-8, 18].

Our learning model is a simplified version of Erev's [7] cutoff-reinforcement learning model. In our model, decision makers learn by making judgments and decisions, and by identifying the consequences of their decisions. In our model, individuals generate judgments about the world by using a linear additive model looking at multiple information cues, which are then compared to a decision threshold that determines the action to be taken. Additionally, in our model, events are generated by comparing the level of the activity stream to that of the criterion threshold (definition of what level constitutes an event). When the level of the activity stream is larger than the criterion threshold, a positive event is generated (a threat in this case); otherwise a negative event is generated (negative in the sense that it does not belong to the object class of the identification process). Subsequently, when an action is taken, and when the type of action is compared to the type of event that happens, one of four types of outcomes occurs: true-positive outcomes, false-positive outcomes, false-negative outcomes, and true-negative outcomes. Because these outcomes are identified and associated with a predefined payoff structure, decision makers adjust their decision threshold for decisions about future action, closing the learning feedback loop that allows them to increase their effectiveness in identification of emergent threats.

4.2 Judgment sector

The first sector of the model deals with how human judges in organizations integrate information to generate behaviorally-based judgments about the likelihood of threats emerging. Figure 2 shows the causal structure that captures a model of judgment that has been identified as robust enough to represent human judgment in general [13-17, 31-33]. This model of judgment uses a linear additive combination of information cues to represent the judgment process of decision makers in organizations. The model is of the form shown in see equation 1:

(1) $$Y = w_1 X_1 + w_2 X_2 + \ldots + w_n X_n + e$$

where Y represents the judgment of likelihood of threat, X_n represents the information cues used in the judgment process, w_n represents the relative weight that each information cue has on the judgment, and e represents the unavoidable uncertainty in the judgment process. In the model presented in this paper, the information cues represent cues used by security officers to recognize the emergent threat of a terrorist attack to an information system in an organization (*judgment about activity stream* in Figure 1 [generic definition] and *judgment of likelihood of terrorist behavior* in Figure 2 [specific definition in the context of threat identification]). The specific cues that the security officer uses to try to distinguish those cases that belong to the terrorists' population are: *level of weapons training*, *level of previous suspicious activity*, and *level of radicalism in religious practice*.

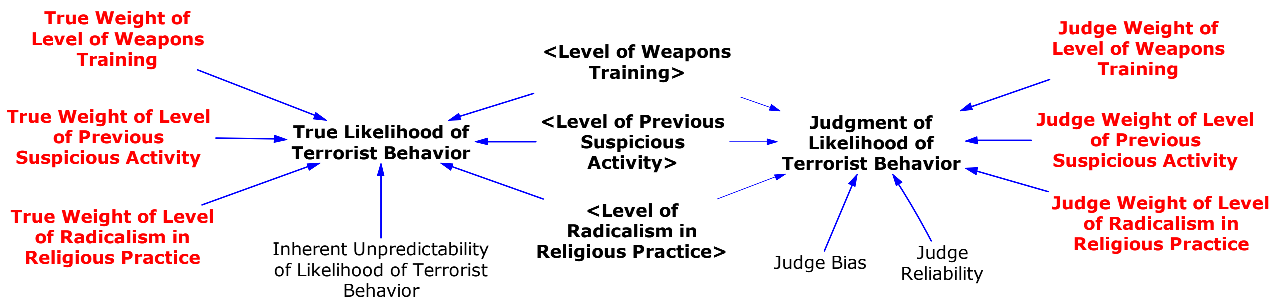

Figure 2. Judgment sector structure

4.3 Decision-making sector

Decision making in the model is captured by comparing the level of the judgment of the variable under study (in this case *judgment of likelihood of terrorist behavior*) with that of the associated decision threshold. If the judgment exceeds the threshold level, defensive action is considered warranted, and is performed. Figure 3 shows the causal structure of this process. The higher the level of the decision threshold, the less often action is granted because fewer judgments exceed the threshold level. Extremely vigilant decision makers, concerned with the emergence of threats, have low decision thresholds in place in their organizations. Following precepts from signal detection theory [12, 35], the optimal level for the decision threshold can be identified given a predetermined payoff matrix. The optimal level for the decision threshold is the one that maximizes payoff.

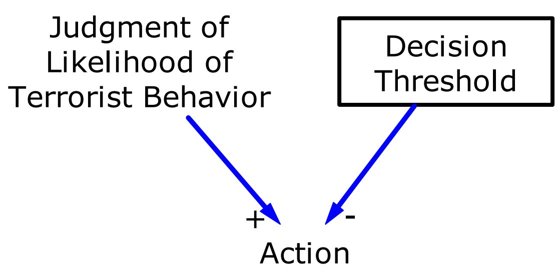

Figure 3. Decision-making structure

4.4 Outcome-decomposition sector

After decisions are made and actions are performed, outcomes are decomposed into four categories depending on whether actions correspond with the nature of the event that triggers them. Figure 4 shows the causal structure of this process.

For example, suppose security officers decide to take defense actions because they mistakenly believe these actions are warranted. After the fact, when it becomes clear that these actions were not needed, these are considered false-positive outcomes (also known as false alarms). Being able to decompose outcomes in the four basic categories that signal detection theory uses as a basis for performance analysis in selection-detection processes allows us to fully characterize this process in the model. In real-life decision processes, because decision makers normally confront incomplete and imperfect outcome feedback, it is difficult to have accurate knowledge of all four types of outcomes — making learning a difficult enterprise.

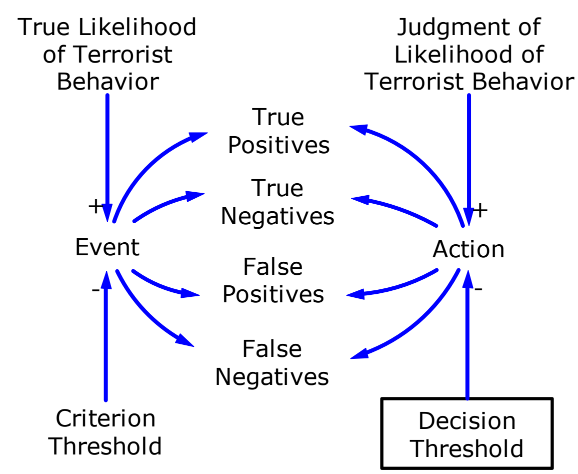

Figure 4. Outcome-decomposition structure

4.5 Outcome-based learning sector

The core learning process in the model is characterized as a reinforcement-learning process. When intended outcomes are obtained, they create reinforcing influences on the level of the decision threshold. When unintended outcomes (errors) are experienced, influences to change the level of the decision threshold are triggered. Reinforcement occurs via two important elements in the model: the payoff matrix and the size of the change of the decision threshold.

The payoff matrix captures the importance of each type of outcome to the decision maker. In our model, a symmetric payoff matrix is used. True-positive and true-negative outcomes (intended outcomes) represent a gain of \$1.00 US, and false-positive and false-negative outcomes (errors) cost \$1.00 US each (independently of the type of error). In certain contexts, as in the case of identification of terrorists, the payoff matrix might be asymmetric; in this case, the cost of a false-negative outcome compared with that of a false-positive would be enormous.

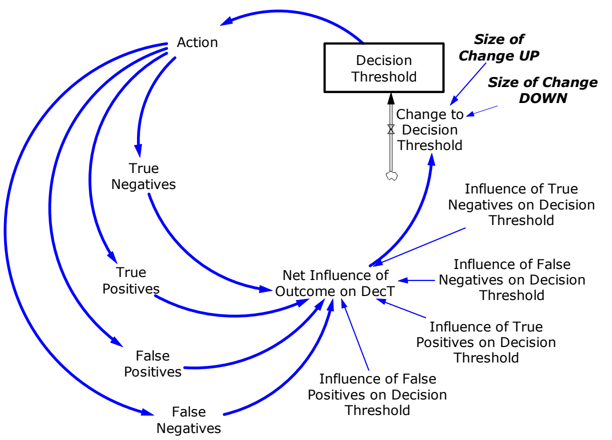

Figure 5. Outcome-based learning structure

In his cutoff-reinforcement learning model, Erev [7] introduces the concept of reinforcement relative to a dynamic reference value that, depending on whether it is going up or down, the decision threshold (DecT) changes more or less rapidly. In our model, we capture this process with two parameters that represent the size of the adjustment when the decision threshold is growing and declining: *size of change up* and *size of change down* (see Figure 5). When *size of change down* and *size of change up* are equal, a symmetric mechanism is represented. Alternatively, when these two parameters are different, an asymmetric mechanism is captured.

4.6 Behavior

The model is capable of generating converging behavior within the parameter space selected. Figures 6, 7, and 8 show simulated temporal evolution of decision thresholds given a symmetric payoff matrix (as in Erev [7]), symmetric directional size adjustments (following Erev's [7] use of 101 decision thresholds in his study, both *size of change up* and *size of change down* are parameterized to 1-unit change in a 100-unit range possible), and different initial levels of the decision threshold (for the three cases presented [*base*, *low initial*, and *high initial]*, the parameters used in the simulation are: 50, 30, and 70 decision-threshold units, respectively).

In the three cases presented, convergence to the criterion threshold (base rate of threat emergence and optimal decision threshold in this case) is achieved. In the base condition (Figure 6), convergence is achieved after 160 trials (where lines 3 and 4 meet). In the low-initial-decision-threshold condition (Figure 7), convergence is reached after 170 trials. In the high-initial-decision-threshold condition (Figure 8), it is reached after approximately 110 trials. In the model, one trial is performed by the security officer in each simulated time period.

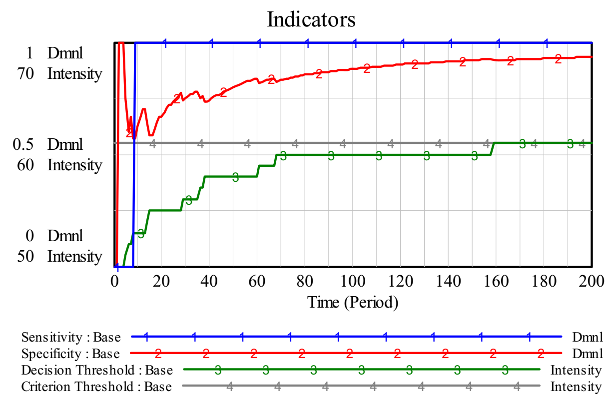

Figure 6. Behavior (base case)

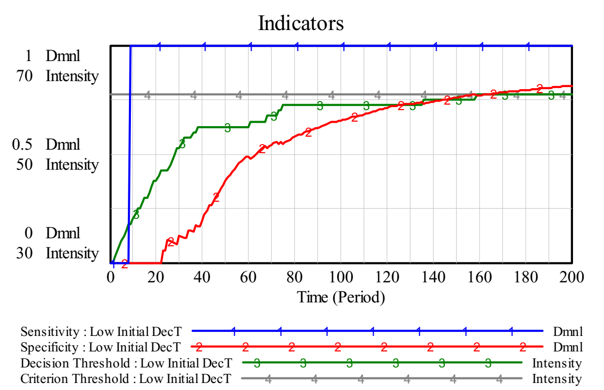

Figure 7. Behavior (low initial DecT case)

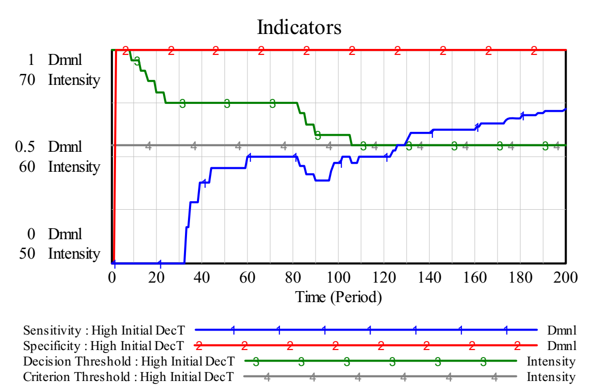

Figure 8. Behavior (high initial DecT case)

0-7695-2755-8/07 \$20.00

Figures 6, 7, and 8 also present the temporal evolution of sensitivity and specificity scores achieved by the simulated judge. These two scores are useful in understanding the effectiveness of the judging process and in understanding how learning is taking place over time. Theoretically, when learning occurs, these two scores grow over time and, eventually, reach their limit of 1 when a large number of trials are performed by the judge.

The sensitivity score (Figures 6–8, line 1) refers to the ability of the judge to correctly identify threats as a percentage of all threats generated over the simulated time (see Equation 2):

(2) $$Sensitivity_i = \sum_{i=1}^{n} \frac{TP_i}{\left(TP_i + FN_i\right)}$$

Where TP represent true-positive outcomes, FN false-negative outcomes, and n the number of trials performed. When sensitivity is 1, no false-negative outcomes are generated, and 100% of threats are correctly identified.

The specificity score (Figures 6–8, line 2) captures the accuracy of the judge in identifying non-threats as a percentage of all non-threats generated over the simulated time (see Equation 3):

(3) $$Specificity_i = \sum_{i=1}^{n} \frac{TN_i}{\left(TN_i + FP_i\right)}$$

Where TN represent true-negative outcomes, FP false-positive outcomes, and n the number of trials performed. When specificity is 1, no false-positive outcomes are generated, and 100% of non-threats are correctly identified.

A decision maker who is capable of finding the optimal decision threshold can, in theory, achieve sensitivity and specificity scores of 1. As shown in Figures 6 and 7, when the initial decision threshold is lower than the criterion threshold (in this case, the optimal too), representing a cautious security officer, and the adjustment toward the criterion threshold does not exhibit extreme changes that would produce oscillations around the optimal as convergence is achieved (as discussed in Weaver and Richardson [36]), the sensitivity score is higher than the specificity score. In these cases, the specificity score increases over time as decision makers learn about the right level of the decision threshold. Alternatively, when the initial decision threshold is higher than the criterion threshold, capturing the case of a not-vigilant-enough security officer (see Figure 8), and the adjustment is smooth, the specificity score is always higher than the sensitivity score because more false-negative outcomes are allowed through the detection process while the decision maker learns where the right level of the decision threshold should be.

5. Experiment

5.1 Description

Our model assumes that individuals learn how to improve detection of threats by paying attention to the results of their judgments and decisions in the past and consequently adjusting the decision threshold that produces these results. To gain confidence that the results of the model are a fair representation of human decision making and learning and to empirically test our theory, we designed and conducted the experiment described below.

We set up a judgment task of behaviorally-based identification of terrorists by using the three information cues described in Section 4.2: *level of weapons training*, *level of previous suspicious activity*, and *level of radicalism in religious practice*. The experiment was implemented in an Excel spreadsheet and carried out over a two-week period. Using purposive sampling [2, 3, 25], a non-probability sampling method used in exploratory research and pilot studies in the social sciences, we selected professionals from the field of decision and information sciences as subjects. Twelve subjects participated in three blocks each generating a total of 36 experimental blocks. We used purposive sampling to capture the learning processes of experienced decision scientists because the experimental task is related to threat identification. We decided that, in this context, the participation of experienced decision scientists could give us more representative information about this process than a pool of subjects obtained via a traditional random sampling technique.

In this experiment, trials were constructed by using a truncated normal random distribution for the information cues with the stochastic characterization that follows: mean of 50, standard deviation of 16.66, maximum of 100, and minimum of 0.

The judgment task included the judgment of 100 trials of terrorists' profiles using three information cues. Three blocks were used to account for the learning process over time and with increasing experience. In total, the subjects completed 300 trials each. The subjects were presented with one trial at a time. They were shown numerical scores for the three information cues (scores between 0 and 100) of the profile and an additional composite score that combined the information cues (again, between 0 and 100). The subjects were instructed that the composite score accurately combined the three information cues. Additionally, the subjects were presented with a predetermined initial level for the decision threshold (50 units in the base case) and, after being presented with the numerical information about the profile, they were asked to determine a new level for the decision threshold (subjects could change it based on experience or leave it at the same level). The decision to determine the level of the decision threshold was the only one that the subjects needed to make each trial.

After each trial, we provided the subjects with immediate, complete, accurate, fully decomposed feedback about their performance, explicitly specifying the type of outcome generated: this action allowed the subjects to know not only whether their response was correct or incorrect, but also why it was correct or incorrect. This type of feedback is richer than traditional outcome-based feedback (just stating if the outcome is correct or incorrect). Additionally, we allowed the subjects access to all previous results of their judgments and decisions — giving them a complete history of all their prior decisions and outcomes to help them in the learning process. With the feedback provided and the history of trials judged, the subjects adjusted their decision thresholds trying to maximize payoff and avoid error generation consistent with Maddox and Bohil's [21] competition between reward and accuracy (COBRA) hypothesis. The subjects were awarded one dollar for each correct response and were penalized one dollar for each incorrect one (regardless of the type of error incurred: false positive or false negative). If all responses were correct, subjects could achieve the maximum payoff of \$100 (US) per block (subjects did not receive any actual monetary compensation — just the satisfaction of identifying the terrorists, doing the right thing, and achieving imaginary payoffs).

5.2 Results

Figures 9 and 10 show some of the results of the experiment. The subjects exhibited learning during each block and over the set of three blocks. Payoffs grew over time, time to complete each block decreased and, as expected, error generation dropped.

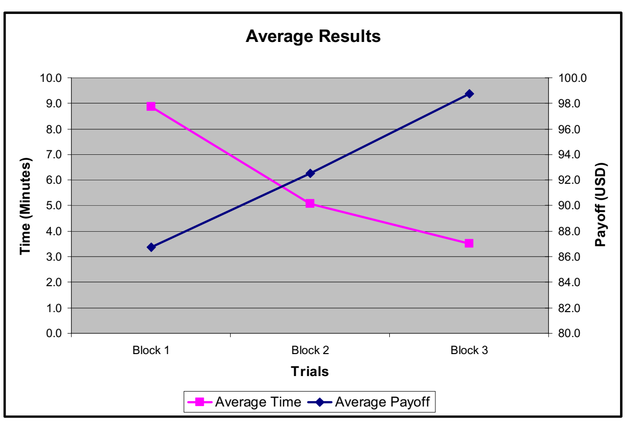

Figure 9. Average results

Due to learning, the total number of errors generated by the subjects declined from an average of 6.5 in the first block, to 3.5 in the second, to 0.5 in the final block. False-positive outcomes show the most dramatic adjustment in this process, changing from an average of 5.5 to less than one. False-negative outcomes, on the other hand, remained fairly unchanged across blocks.

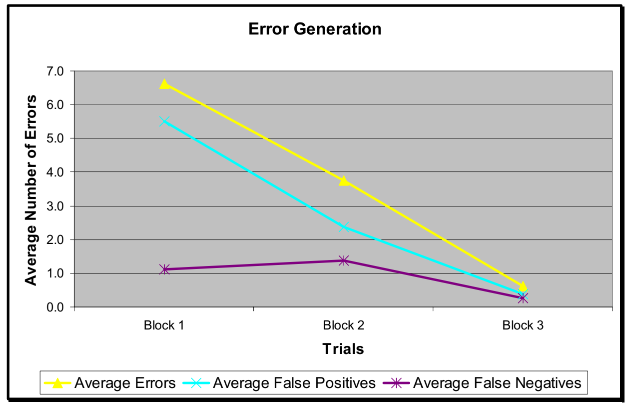

Figure 10. Error generation

In order to enhance our understanding of the learning process and to test whether the model is capable of capturing the way in which human subjects behave, we compared the human-generated temporal evolution of decision thresholds with model-generated data. The results are presented in Section 6.

6. Comparing experimental results with simulation

The human-generated decision thresholds and the model-generated decision thresholds were compared and analyzed by using Theil inequality statistical metrics [30]. Theil inequality statistics are extremely useful when assessing the degree to which two time series of data match each other because these statistics allow for the decomposition of the sources of error in the comparison: mean, variance, or covariance.

Simulated results were calibrated to the human-generated data by using Vensim® automated calibration capability (specialized simulation software used for system dynamics modeling), providing two parameters for the adjustment process: *size of adjustment up* and *size of adjustment down*. These parameters capture the size of the revision that human decision makers use when adjusting decision thresholds to find the optimal level. Figures 11 and 12 show results of different decision makers' behavior; Figures 13 and 14 show their corresponding sources of error according to Theil inequality statistics.

When the source of error is related to differences in mean, it indicates bias in the results. When the error source is variance, it indicates a failure of the model to capture the basic variability of the result. Covariance variation only indicates that there is not a point-to-point correspondence between the simulated data and the experimental data [30]. In the cases presented in Figures 13 and 14, most of the mean-squared error obtained when comparing the simulated time series data with the human-generated time series data is attributable to covariance differences. This means that the model accurately captures the variability of the human-generated results without bias.

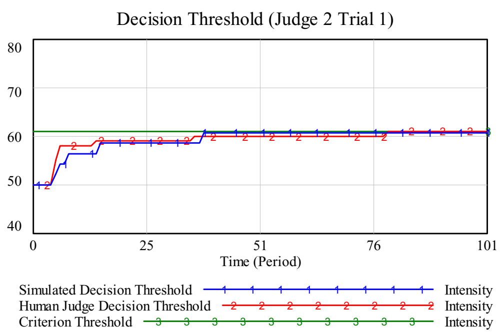

Figure 11. Comparative behavior I

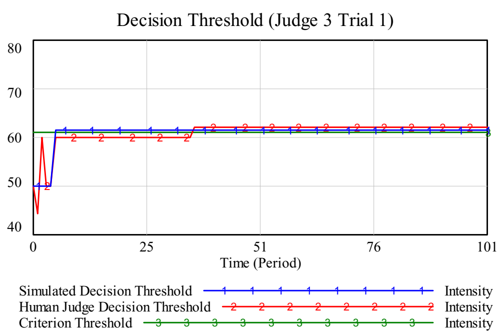

Figure 12. Comparative behavior II

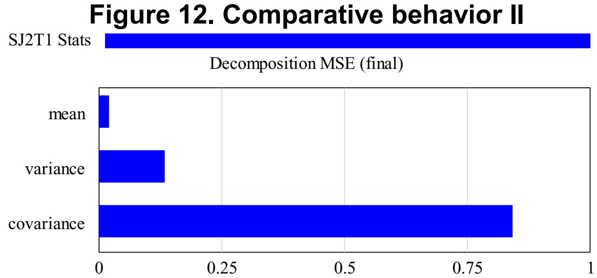

Figure 13. Sources of error I

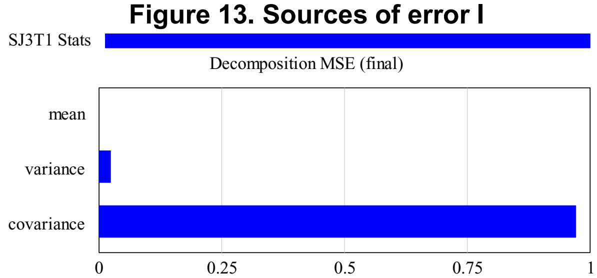

Figure 14. Sources of error II

Comparing experimental data with simulated data allows for increasing confidence in the usefulness of the model [10, 11, 28, 30]. The results of the calibration process are presented in Table 1.

Calibration Results	Mean	Min	Max	Standard Deviation
R^2	0.7301	0.5842	0.8862	0.1270
Mean Abs. Percent Error	0.0116	0.0036	0.0190	0.0065
Mean Square Error	1.6821	0.2082	4.2194	1.5185
Root Mean Square Error	1.1717	0.4563	2.0541	0.6092
Mean	0.0136	0.0008	0.0320	0.0138
Variance	0.0506	0.0135	0.1350	0.0440
Covariance	0.9358	0.8425	0.9842	0.0533

Table 1. Calibration results

7. Conclusions

Outcome-based learning models, such as the one described here, are useful in helping researchers to understand the emergence of threats. The model presented here integrates judgment, decision making, and learning theories to provide an integrated framework with which to behaviorally approach the study of threats.

This model is not complete by any means, further work is necessary. Further work includes performing additional tests of behavior, changing parametric definitions to include different stochastic characterizations of populations, increasing the sample size of subjects, varying the types of judgment tasks to test for robustness of the model across types of tasks, incorporating the use of memory stages in the learning process, and including elements of destabilization of correspondence between type of task and cognitive ability required [14], as in the case of threat emergence.

We also recognize that work related to cue discovery, as a critical part of the learning process [18, 19], is a natural next step in this investigation, along with endogenizing several parameters of the model to expand the learning paths present in the model. Some parameters to be endogenized include (1) the size of adjustment of the decision threshold, (2) the judgment weights on information cues, (3) the payoff structure, and (4) the base rate of events as expressed in the criterion threshold.

Acknowledgments

This work was funded in part by the U.S. Department of Homeland Security.

References

[1] Barlas, Y., "Formal aspects of model validity and validation in system dynamics", *System Dynamics Review*, 12 (3), 1996, pp. 183-210.

[2] Bernard, H. R., *Social Research Methods: Qualitative and Quantitative Approaches*, Sage Publications, Inc., Thousand Oaks, CA, 2000.

[3] Brewer, J., and A. Hunter, *Multimethod Research: A Synthesis of Styles*, Sage Publications Inc., Newbury Park, CA, 1989.

[4] Brunswik, E., "Organismic achievement and environmental probability", *Psychological Review*, 50, 1943, pp. 255-272.

[5] ———, *Perception and the Representative Design of Psychological Experiments*, University of California Press, Berkeley, CA, 1956.

[6] Camerer, C., and T. Ho, "Experienced-Weighted Attraction Learning in Normal Games", *Econometrica*, 67 (4), 1999, pp. 827-874.

[7] Erev, I., "Signal detection by human observers: A cutoff reinforcement learning model of categorization decisions under uncertainty", *Psychological Review*, 105, 1998, pp. 280-298.

[8] Erev, I., D. Gopher, R. Itkin, and Y. Greenshpan, "Toward a Generalization of Signal Detection Theory to N-Person Games: The Example of Two-Person Safety Problem", *Journal of Mathematical Psychology*, 39, 1995, pp. 360-375.

[9] Feltovich, N., "Reinforcement-Based vs. Belief-Based Learning Models in Experimental Asymmetric-Information Games", *Econometrica*, 68 (3), 2000, pp. 605-641.

[10] Forrester, J. W., *Industrial Dynamics*, Productivity Press, Cambridge MA, 1961.

[11] Forrester, J. W., and P. M. Senge, "Tests for building confidence in system dynamics models", *TIMS Studies in Management Sciences*, 14, 1980, pp. 209-228.

[12] Green, D. M., and J. A. Swets, *Signal Detection Theory and Psychophysics*, John Wiley, New York, 1966.

[13] Hammond, K. R., *Human Judgment and Social Policy: Irreducible Uncertainty, Inevitable Error, Unavoidable Injustice*, Oxford University Press, New York, 1996.

[14] ———, *Judgments Under Stress*, Oxford University Press, New York, 2000.

[15] Hammond, K. R., G. H. McClelland, and J. Mumpower, *Human Judgment and Decision Making: Theories, Methods, and Procedures*, Praeger, New York, 1980.

[16] Hammond, K. R., and T. R. Stewart, eds. *The Essential Brunswik: Beginnings, Explications, Applications*. Oxford University Press. New York. 2001.

[17] Hammond, K. R., T. R. Stewart, B. Brehmer, and D. O. Steinmann. "Social judgment theory". In *Human Judgment and Decision Processes* edited by M. F. Kaplan and S. Schwarts. Academic Press. New York. 1975.

[18] Klayman, J., "Learning from Feedback in Probabilistic Environments", *Acta Psychologica*, 56, 1984, pp. 81-92.

[19] ———, "Cue discovery in probabilistic environments: Uncertainty and experimentation", *Learning, Memory, and Cognition*, 14 (2), 1988, pp. 317-330.

[20] Kolb, D. A., *Experiential Learning: Experience as the Source of Learning and Development*, Prentice-Hall, New York, 1984.

[21] Maddox, W. T., and C. J. Bohil, "Base-rate and payoff effects in multidimensional perceptual categorization", *Journal of Experimental Psychology: Learning, Memory, and Cognition*, 24 (6), 1998, pp. 1459-1482.

[22] Martinez-Moyano, I. J., E. H. Rich, S. H. Conrad, D. F. Andersen, and T. R. Stewart, "A Behavioral Theory of Insider-Threat Risks: A System Dynamics Approach", *Transactions on Modeling and Computer Simulation (TOMACS)*, Forthcoming, pp. 1-36.

[23] Martinez-Moyano, I. J., and G. P. Richardson. "An Expert View of the System Dynamics Modeling Process: Concurrences and Divergences Searching for Best Practices in System Dynamics Modeling". Paper read at the *20th International Conference of the System Dynamics Society*, Palermo, Italy, 2002.

[24] Melara, C., J. M. Sarriegui, J. J. Gonzalez, A. Sawicka, and D. L. Cooke. "A system dynamics model of an insider attack on an information system". In *From Modeling to Managing Security: A System Dynamics Approach*, edited by J. J. Gonzalez. Høyskoleforlaget AS - Norwegian Academic Press. Kristiansand, Norway. 2003.

[25] Newman, I., and C. R. Benz, *Qualitative-Quantitative Research Methodology: Exploring the Interactive Continuum*, Southern Illinois University Press, Carbondale, IL, 1998.

[26] Rich, E., and J. J. Gonzalez. "Maintaining security and safety in high-threat e-operations transitions". Paper read at the *39th Hawaii International Conference on System Sciences*, Hawaii, 2006.

[27] Rich, E., I. J. Martinez-Moyano, S. Conrad, A. P. Moore, D. M. Cappelli, T. J. Shimeall, D. F. Andersen, J. J. Gonzalez, R. J. Ellison, H. F. Lipson, D. A. Mundie, J. M. Sarriegui, A. Sawicka, T. R. Stewart, J. M. Torres, E. A. Weaver, J. Wiik, and A. A. Zagonel. "Simulating insider cyber-threat risks: A model-based case and a case-based model". Paper read at the *International Conference of the System Dynamics Society*, Cambridge, MA, 2005.

[28] Richardson, G. P., and A. L. Pugh, *Introduction to System Dynamics Modeling*, *System Dynamics Series*, Pegasus Communications, Inc., Waltham, 1989.

[29] Senge, P. M., *The Fifth Discipline: The Art and Practice of the Learning Organization*. Revised edition, Currency Doubleday, New York, 2006.

[30] Sterman, J. D., *Business Dynamics: Systems Thinking and Modeling for a Complex World*, Irwin McGraw-Hill, Boston MA, 2000.

[31] Stewart, T. "Judgment analysis: procedures". In *Human Judgment: The SJT View*, edited by B. Brehmer and C. R. B. Joyce. North-Holland. Amsterdam. 1988.

[32] Stewart, T. R. "Uncertainty, judgment, and error in prediction". In *Prediction: Science, Decision Making, and the Future of Nature* edited by D. Sarewitz, R. A. Pielke and R. Byerly. Island Press. Washington, D.C. 2000.

[33] Stewart, T. R., and C. M. Lusk, "Seven components of judgmental forecasting skill: implications for research and the improvement of forecasts", *Journal of Forecasting*, 13, 1994, pp. 579-599.

[34] Swets, J., "The Science of Choosing the Right Decision Threshold in High-Stakes Diagnostics", *American Psychologist*, 47 (4), 1992, pp. 522-532.

[35] Swets, J. A., "The relative operating characteristic in psychology." *Science*, 182 (4116), 1973, pp. 990-1000.

[36] Weaver, E., and G. P. Richardson, "Threshold Setting and the Cycling of a Decision Threshold", *System Dynamics Review*, 22 (1), 2002, pp. 1-26.

Model equations

(001) Absolute Critical Error Rate = ZIDZ (Real Count of False Negatives, Real Count of Transactions) Units: Dmnl
(002) Accumulated Events = INTEG (Changes to Event Accumulation, Initial Events) Units: Event
(003) "Accumulated Payoff (v)" = INTEG (Change to Payoff, Initial Accumulated Payoff) Units: Utility
(004) Action = IF THEN ELSE (“Sampled Judgment of Distal Variable (x)" > Decision Threshold, 1, 0) Units: Audit
(005) Action Count Rate = IF THEN ELSE (Action = 1, Event Counter, 0) Units: Event/Period
(006) Adding Transactions = Sampling Flag / TIME STEP Units: Event/Period
(007) Average Event Base Rate = ZIDZ (Accumulated Events, Real Count of Transactions) Units: Dmnl
(008) Average Payoff = ZIDZ (“Accumulated Payoff (v)”, Real Count of Transactions) Units: Utility/Transaction
(009) Base Rate = ZIDZ (Accumulated Events, Real Count of Transactions) Units: Dmnl
(010) Calibration Data = DecTData[Judge 5,Trial 1] Units: Intensity
(011) Change to Decision Threshold = IF THEN ELSE (Net Influence of Outcome on DecThre > 0, ((Net Influence of Outcome on DecThre * Size of Change UP) / TIME STEP) , ((Net Influence of Outcome on DecThre * Size of Change DOWN) / TIME STEP)) Units: Intensity/Period
(012) Change to Payoff = Net Payoff / TIME STEP Units: Utility/Period
(013) Changes to Event Accumulation = Event * Count Multiplier Units: Event/Period
(014) Count Multiplier = 1 / TIME STEP Units: 1/Period
(015) Criterion Threshold = 61 + STEP (0, 10) Units: Intensity
(016) Cue1 Error Max = 3 Units: Intensity
(017) Cue1 Error Mean = 0 Units: Intensity
(018) Cue1 Error Min = -3 Units: Intensity
(019) Cue1 Error Seed = 32453 Units: Dmnl
(020) Cue1 Error StdD = 0 Units: Intensity
(021) Cue1 Max = 100 Units: Intensity
(022) Cue1 Mean = 50 Units: Intensity
(023) Cue1 Min = 0 Units: Intensity
(024) Cue1 Seed = 1234 Units: Dmnl
(025) Cue1 StdD = (50 / 3) Units: Intensity
(026) Cue2 Error Max = 3 Units: Intensity
(027) Cue2 Error Mean = 0 Units: Intensity
(028) Cue2 Error Min = -3 Units: Intensity
(029) Cue2 Error Seed = 4.75657e+009 Units: Dmnl
(030) Cue2 Error StdD = 0 Units: Intensity
(031) Cue2 Max = 100 Units: Intensity
(032) Cue2 Mean = 50 Units: Intensity
(033) Cue2 Min = 0 Units: Intensity
(034) Cue2 Seed = 123321 Units: Dmnl
(035) Cue2 STd = (50 / 3) Units: Intensity
(036) Cue3 Error Max = 3 Units: Intensity
(037) Cue3 Error Mean = 0 Units: Intensity
(038) Cue3 Error Min = -3 Units: Intensity
(039) Cue3 Error Seed = 3.42565e+008 Units: Dmnl
(040) Cue3 Error StdD = 0 Units: Intensity
(041) Cue3 Max = 100 Units: Intensity
(042) Cue3 Mean = 50 Units: Intensity
(043) Cue3 Min = 0 Units: Intensity
(044) Cue3 Seed = 345345 Units: Dmnl
(045) Cue3 StdD = (50 / 3) Units: Intensity
(046) Decision Threshold = INTEG (Change to Decision Threshold, Decision Threshold Initial) Units: Intensity
(047) Decision Threshold Initial = 50 Units: Intensity
(048) DecTData[Judge,Trial] Units: Intensity
(049) DecThre Range = Max Decision Threshold - Min Decision Threshold Units: Intensity
(050) Distal Variable = (Information Cue 1 * True Weight of Information Cue 1) + (Information Cue 2 * True Weight of Information Cue 2) + (Information Cue 3 * True Weight of Information Cue 3) + (Inherent Unpredictability of the Environment * True Weight of Unpredictability of the Environment) + Environment Natural Propensity Units: Intensity
(051) Environment Error Max = 3 Units: Intensity
(052) Environment Error Mean = 0 Units: Intensity
(053) Environment Error Min = -3 Units: Intensity
(054) Environment Error Seed = 9.86599e+008 Units: Dmnl
(055) Environment Error StdD = 1 Units: Intensity
(056) Environment Natural Propensity = 0 Units: Intensity
(057) Error Rate = ZIDZ (Errors Generated, Real Count of Transactions) Units: Dmnl
(058) Errors Generated = Real Count of False Positives + Real Count of False Negatives Units: Event
(059) Event = IF THEN ELSE (Sampled Distal Variable > Criterion Threshold, 1, 0) Units: Event
(060) Event Counter = Count Multiplier * Number of Events per DT Units: Event/Period
(061) External Fraud Threat Threshold = Criterion Threshold Units: Intensity
(062) False Negatives = IF THEN ELSE (Event = 1: AND: Action = 0: AND: Sampling Flag = 1, 1, 0) Units: Event
(063) False Negatives Count Rate = IF THEN ELSE (Event = 1: AND: Action = 0: AND: Sampling Flag = 1, Event Counter, 0)

Units: Event/Period
(064) False Negatives Payoff = -1 Units: Utility/Event
(065) False Positives = IF THEN ELSE (Event = 0: AND: Action = 1: AND: Sampling Flag = 1, 1, 0) Units: Event
(066) False Positives Count Rate = IF THEN ELSE (Event = 0: AND: Action = 1: AND: Sampling Flag = 1, Event Counter, 0) Units: Event/Period
(067) False Positives Payoff = -1 Units: Utility/Event
(068) FINAL TIME = 200 Units: Period
(069) Frequency of Sampling = 1 Units: Period
(070) Influence of False Negatives on Decision Threshold = -1 Units: Dmnl/Event
(071) Influence of False Positives on Decision Threshold = 1 Units: Dmnl/Event
(072) Influence of True Negatives on Decision Threshold = 0 Units: Dmnl/Event
(073) Influence of True Positives on Decision Threshold = 0 Units: Dmnl/Event
(074) Information Cue 1 = RANDOM NORMAL (Cue1 Min, Cue1 Max, Cue1 Mean, Cue1 StdD, Cue1 Seed) Units: Intensity
(075) Information Cue 2 = RANDOM NORMAL (Cue2 Min, Cue2 Max, Cue2 Mean, Cue2 STd, Cue2 Seed) Units: Intensity
(076) Information Cue 3 = RANDOM NORMAL (Cue3 Min, Cue3 Max, Cue3 Mean, Cue3 StdD, Cue3 Seed) Units: Intensity
(077) Inherent Unpredictability of the Environment = RANDOM NORMAL (Environment Error Min, Environment Error Max, Environment Error Mean, Environment Error StdD, Environment Error Seed) Units: Intensity
(078) Initial Accumulated Payoff = 0 Units: Utility
(079) Initial Events = 0 Units: Event
(080) Initial Real Count of False Negatives = 0 Units: Event
(081) Initial Real Count of False Positives = 0 Units: Event
(082) Initial Real Count of Transactions = 0 Units: Event
(083) Initial Real Count of True Negatives = 0 Units: Event
(084) Initial Real Count of True Positives = 0 Units: Event
(085) INITIAL TIME = 0 Units: Period
(086) Judge: Judge 1…Judge 12
(087) Judge Bias = 0 Units: Intensity
(088) Judge Error Max = 3 Units: Intensity
(089) Judge Error Mean = 0 Units: Intensity
(090) Judge Error Min = -3 Units: Intensity
(091) Judge Error Seed = 1234 Units: Dmnl
(092) Judge Error StdD = 1 Units: Intensity
(093) Judge Reliability = RANDOM NORMAL (Judge Error Min , Judge Error Max , Judge Error Mean , Judge Error StdD , Judge Error Seed) Units: Intensity
(094) Judge Reliability Weight = 0 Units: Dmnl
(095) Judge Weight of Information Cue 1 = (1 / 6) Units: Dmnl
(096) Judge Weight of Information Cue 2 = (2 / 6) Units: Dmnl
(097) Judge Weight of Information Cue 3 = (3 / 6) Units: Dmnl
(098) Judgment of Distal Variable = ((Knowledge about Information Cue 1 * Judge Weight of Information Cue 1) + (Knowledge about Information Cue 2 * Judge Weight of Information Cue 2) + (Knowledge about Information Cue 3 * Judge Weight of Information Cue 3) + (Judge Reliability * Judge Reliability Weight)) + Judge Bias Units: Intensity
(099) Knowledge about Information Cue 1 = Measurement Error of Information Cue 1 + Information Cue 1 Units: Intensity
(100) Knowledge about Information Cue 2 = Information Cue 2 + Measurement Error of Information Cue 2 Units: Intensity
(101) Knowledge about Information Cue 3 = Information Cue 3 + Measurement Error of Information Cue 3 Units: Intensity
(102) Max Decision Threshold = 100 Units: Intensity
(103) Measurement Error of Information Cue 1 = RANDOM NORMAL (Cue1 Error Min, Cue1 Error Max, Cue1 Error Mean, Cue1 Error StdD, Cue1 Error Seed) Units: Intensity
(104) Measurement Error of Information Cue 2 = RANDOM NORMAL (Cue2 Error Min, Cue2 Error Max, Cue2 Error Mean, Cue2 Error StdD, Cue2 Error Seed) Units: Intensity
(105) Measurement Error of Information Cue 3 = RANDOM NORMAL (Cue3 Error Min, Cue3 Error Max, Cue3 Error Mean, Cue3 Error StdD, Cue3 Error Seed) Units: Intensity
(106) Min Decision Threshold = 0 Units: Intensity
(107) Net Influence of Outcome on DecT = False Negatives * Influence of False Negatives on Decision Threshold + False Positives * Influence of False Positives on Decision Threshold + True Negatives * Influence of True Negatives on Decision Threshold + True Positives * Influence of True Positives on Decision Threshold Units: Dmnl
(108) Net Payoff = False Negatives * False Negatives Payoff + False Positives * False Positives Payoff + True Negatives * True Negatives Payoff + True Positives * True Positives Payoff Units: Utility
(109) "Non-Events" = Real Count of True Negatives + Real Count of False Positives Units: Event
(110) Number of Events per DT = 1 Units: Event
(111) Real Count of Actions = INTEG (Action Count Rate, 0) Units: Event
(112) Real Count of False Negatives = INTEG (False Negatives Count Rate, Initial Real Count of False Negatives) Units: Event
(113) Real Count of False Positives = INTEG (False Positives Count Rate, Initial Real Count of False Positives) Units: Event
(114) Real Count of Transactions = INTEG (Adding Transactions, Initial Real Count of Transactions) Units: Event
(115) Real Count of True Negatives = INTEG (True Negatives Count Rate, Initial Real Count of True Negatives) Units: Event
(116) Real Count of True Positives = INTEG (True Positives Count Rate, Initial Real Count of True Positives) Units: Event
(117) Relative Critical Error Rate = ZIDZ (Real Count of False Negatives, Errors Generated) Units: Dmnl
(118) Sampled Distal Variable = IF THEN ELSE (Sampling Flag = 1, Distal Variable, -5) Units: Intensity
(119) "Sampled Judgment of Distal Variable (x)" = IF THEN ELSE (Sampling Flag = 1, Judgment of Distal Variable, -5) Units: Intensity
(120) Sampling Flag = IF THEN ELSE (MODULO (Time, Frequency of Sampling) = 0: AND: Time <> 0, 1, 0) Units: Event
(121) SAVEPER = 1 Units: Period [0,?]
(122) Selection Rate = ZIDZ (Real Count of Actions, Real Count of Transactions) Units: Dmnl
(123) Sensitivity = ZIDZ (Real Count of True Positives, (Real Count of True Positives + Real Count of False Negatives)) Units: Dmnl
(124) Size of Change DOWN = DecThre Range / (“Total Number of DecThre Cutoffs (mDOWN)" - 1) Units: Period
(125) Size of Change UP = DecThre Range / (“Total Number of DecThre Cutoffs (mUP)" - 1) Units: Intensity
(126) Specificity = ZIDZ (Real Count of True Negatives, (Real Count of True Negatives + Real Count of False Positives)) Units: Dmnl
(127) TIME STEP = 0.0625 Units: Period [0,?]
(128) "Total Number of DecThre Cutoffs (mDOWN)" = 101 Units:Dmnl
(129) "Total Number of DecThre Cutoffs (mUP)" = 101 Units: Dmnl
(130) Trial: Trial 1, Trial 2, Trial 3
(131) True Negatives = IF THEN ELSE (Event = 0: AND: Action = 0: AND: Sampling Flag = 1, 1, 0) Units: Event
(132) True Negatives Count Rate = IF THEN ELSE (Event = 0: AND: Action = 0: AND: Sampling Flag = 1, Event Counter, 0) Units: Event/Period
(133) True Negatives Payoff = 1 Units: Utility/Event
(134) True Positives = IF THEN ELSE (Event = 1: AND: Action = 1: AND: Sampling Flag = 1, 1, 0) Units: Event
(135) True Positives Count Rate = IF THEN ELSE (Event = 1: AND: Action = 1: AND: Sampling Flag = 1, Event Counter, 0) Units: Event/Period
(136) True Positives Payoff = 1 Units: Utility/Event
(137) True Weight of Information Cue 1 = (1 / 6) Units: Dmnl
(138) True Weight of Information Cue 2 = (2 / 6) Units: Dmnl
(139) True Weight of Information Cue 3 = (3 / 6) Units: Dmnl
(140) True Weight of Unpredictability of the Environment = 0 Units: Dmnl