2006 CCRTS
The State of the Art and the State of the Practice

Situation Awareness for Cyber Defense

Topics: Cyber Defense, Situation Awareness, Information Assurance

Leslie D. Cumiford, PhD, PE
Knowledge Discovery and Extraction
Defense Systems and Assessments
Sandia National Laboratories
P.O. Box 5800
MS 0455
Albuquerque, New Mexico 87185-0455
v (505) 844-0670
f (505) 844-9641
ldcumif@sandia.gov

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2006		**00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Situation Awareness for Cyber Defense	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Sandai National Laboratories,PO Box 5800,Albuquerque,NM,87185-0455**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**28**	

Situation Awareness for Cyber Defense

Leslie D. Cumiford, PhD, PE
Knowledge Discovery and Extraction
Defense Systems and Assessments
Sandia National Laboratories*
ldcumif@sandia.gov
(505) 844-0670

Abstract
Situation awareness (SA), or the ability to assess situations and prepare timely responses, has long been acknowledged as an important aspect of theater operations for defensive purposes. Likewise, SA is critical in the cyber world. The focus of this paper is SA in the cyber domain with respect to defensive capabilities. The cyber defense domain has an important characteristic in common with related domains such as analysis of terrorism, protection of infrastructure, and IED defense: the domains are characterized by sets of complex, interacting issues that are ill-defined, ambiguous, and evolving in time. Solutions for such problems must be integrative, handle domain complexity, and incorporate and address the element of surprise. A list of the capabilities needed to accomplish effective cyber SA is provided, along with an architecture for cyber SA reasoning. Most cyber SA architectures attempt to mirror the complexity of the domain. Surprisingly, the latest brain research does not support this approach. Notional information is provided regarding a new approach to cyber situation awareness, taking into account the lessons learned from the way humans process such information.

Introduction: Situation Awareness

Situation awareness (SA) has long been acknowledged as an important aspect of theater operations for defensive purposes. Likewise, SA is critical in the cyber world. The focus of this paper is SA for cyber defense.

At the most basic level, situation awareness is defined as the ability to rapidly and effectively address incoming stimuli with appropriate responses. SA impacts defensive operations at the tactical level since it provides the ability to recognize and respond to enemy actions. SA also impacts the strategic level, since feedback from the tactical level of operations feeds into the strategic planning process. Likewise, a good understanding of strategic operations and planning contributes to effective SA in handling tactical situations.

Endsley (1988, 1995) defines SA as "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future". Klein (1997) ties the notions of goals, cue salience, expectations, and identification of typical actions to SA, and believes that it is

* Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

central to the decision-making process. Rasmussen (1983) describes a hierarchically-organized system for SA consisting of three levels: skill-based, rule-based, and knowledge-based. Pew (2000) proposes that SA should integrate the environment, goals, system, available physical and human resources, and other actors. Rousseau, Tremblay, and Breton (2004) state that most SA researchers and practitioners agree that SA represents a body of knowledge with a set of processes (or functions) that serve to develop and update that knowledge.

SA can be broken down into several different components. The first component is that of being aware of the current environment. The second component is that of ascertaining the significance of certain events and aspects of the current environment. Third, one must be able to tie the awareness to timely and appropriate responses. In many situations, "appropriate" responses are determined by the degree of their success in accomplishing a particular goal. The goals can be a work goal, such as "navigate the channel to deliver the goods" or "hold the defensive position". Sometimes it is simply necessary to understand or interpret the environment and report what is seen or note anomalies.

The notion of time is critical to SA. It is almost always important to note the time at which actions occur in the environment or at which the environment takes on particular characteristics. Sequences, trends, deadlines, overlapping events, and similar notions are typically a very important part of understanding the environment and tying stimulus with response to effectively achieve goals.

Another important consideration for SA is that of selective attention. At any given point in time in a crowded environment, some information is more important than other information. Additionally, the relative importance of a particular datum changes with time. Selective attention boosts situational awareness for persons and reasoners that interact with physical systems. Selective attention is the ability to intelligently direct the reasoning/planning focus in order to dynamically respond to changing events in the physical system. Selective attention is both reactive a proactive in nature. It forms the basis of a tightly-integrated feedback loop between the current state of the physical system and the reasoning processes used to monitor and control the physical system. Selective attention provides a reasoner with two types of knowledge:

1. Identification of critical or significant sensor data at a given point in time, and
2. Identification of the points in time (in the immediate future) which are critical for accessing sensor data (Interrante, 1991).

In busy or crowded environments, having a high degree of SA requires sifting and focusing both the effort required to recognize stimuli and that needed to determine responses. In such cases, it is this very quality that determines those with a high degree of SA. In busy environments, a higher degree of SA leads to efficiency in assessing the environment, providing more cognitive "room" to process incoming information, determine what to expect in the near future, and determine appropriate responses.

The cyber defense domain is next described, with particular emphasis on the fact that it is a difficult domain to characterize. Next, the means to address cyber defense domain complexity is described, followed by the architecture and capabilities needed to achieve cyber situation awareness for defensive operations. A notional description of a new approach to SA is provided that reduces complexity as compared to most similar systems. Finally, a discussion of the open issues and benefits of the approach described herein is provided. This paper does not contain an explicit discussion of human-cyber interactions in defensive operations, but alludes to such interactions. It is the author's position that a tight integration between both systems is necessary to accomplish effective situation awareness, even in the cyber defense domain.

Cyber Defense Domain

The cyber defense domain has an important characteristic in common with related domains such as analysis of terrorism, protection of infrastructure, and IED defense: the domains are characterized by sets of complex, interacting issues that are ill-defined, ambiguous, and evolving in time. Within this domain, the cyber agent system may be defending itself, related information systems, control systems for a physical system such as a pipeline or power line, a human force or operation, allied forces or systems, or some combination of these elements.

The following discussion, based on the hypothesis that terrorism is an emergent phenomenon of complex systems, is largely drawn from Hayden (2006). Note that most, if not all, of the characteristics of the terrorism domain described below are relevant to the domain of cyber defense. In fact, defense against terrorism is necessary in the cyber world. Terrorism is an emergent phenomenon of complex, dynamically interacting social, technological, and institutional systems. Terrorist organizations and cells meet changes in economic, political, and security environments with innovation and adaptation in targets, operations, and strategies. "Small world" phenomena emerge through decentralized terrorist networks and facilitate resiliency in operations, diffusion of ideology and innovation, and distribution of resources and information (Barabasi 1999; Watts 2003). To defend against such an opponent, cyber systems must address the critical problem of discerning differentiating behavioral characteristics amidst ambiguity and complexity. Post-9/11 review has identified the need for collection, synthesis, and sense-making of information from multiple (and often contradictory) sources and perspectives. This information must be interpreted, hypothesized about, and responded to in the context of diverse social, behavioral, technical, political, and institutional models to support a spectrum of counterterrorism decision-making policies and actions.

Hayden (2006) delineates a number of characteristics of the problem of understanding and responding to terrorism, listed in part below:

1. no definitive formulation of the problem
2. no end to the problem
3. solutions are not true/false, but good/bad
4. no immediate and no ultimate test of a problem solution
5. solutions are one-shot operations, with no opportunity to learn by trial and error

6. every attempt at a solution counts significantly
7. every instantiation of the problem is essentially unique
8. a problem may actually be a symptom of another problem

The multiplicity of factors and conditions that impinge on such problems ensure that no two of them are alike, and that the solutions to them will always be custom designed and fitted (Rittel 1973).

According to Hayden (2006), "We must cease to ask questions about *explicitly predicting* future events . . . , and instead ask questions that seek to *explore possibilities* of future behaviors and the key indicators for those behaviors in terms of dynamic patterns of interactions and the underlying structures upon which those transactions take place". Hayden advocates the use of self-organizing complex systems for enabling actionable discernment into differentiating patterns of behaviors. She emphasizes that complex systems such as that of terrorism exhibit emergence. One consequence of this quality is that system properties cannot be predicted *a priori*; cause and effect are almost always only evident in retrospect.

Hayden (2006) emphasizes the importance of *communication* and *association* across interfaces in a complex system. She states, "Communication – the means by which it occurs and the speed by which it occurs – establishes what information is known by each system in the whole. . . At the same time, associations between parts of the system establish a network of interactions . . . Together, the amount of communication and association among systems partially determines the behavior of the whole system."

The *level of system complexity* and the *timeframe of relevance* are important choices to be made when addressing emergent, complex domains such as terrorism (Hayden 2006). She defines the level of complexity as falling somewhere on the spectrum between order and chaos (or randomness). The relevant timeframe encompasses the rate of information transmission and the periodicity associated with system behavior in response to the information. The nature of information in dynamic systems is such that its periodicity is measured by the characteristic rhythms and iterations associated with environmental changes and agent behavior.

Addressing Complexity

What can we conclude about cyber SA for defensive operations based on Hayden's (2006) description of the complexities and characteristics of the terrorism domain? At the heart of accomplishing cyber SA is the need to build discernment and associated spontaneity into the reasoning capability of the system. The use of templates, schema, and/or frames in the traditional sense is ill-advised in such an environment. One would end up with a fairly low level of SA in a cyber system that depends on such formalisms; a system that behaves as if it is always a few steps behind the curve, since the system would have no ability to predict and/or respond to novel situations. The domains in which a cyber SA system is needed are filled with such novel situations, created by the dynamic confluence of interacting, complex subsystems as described by Hayden (2006) with

respect to terrorism. At best, an understanding of past events would be useful only as a starting place for determining an appropriate response.

A defensive cyber SA system must track the status and capability of the enemy's cyber system; predict and defend against attacks and related enemy operations; maintain an understanding of its own defensive capabilities, status, and plans; stay aware of allied operations, and keep in mind the influence of other environmental factors such as the weather, communications, and hardware or software malfunctions or failures. All such awareness must be dynamically maintained over time.

Many of the same concepts that are applied to military applications apply in the cyber context. The cyber SA system must keep pace with the battle tempo. The cyber system must perform cyber battle damage assessment of self and friendly systems in a timely manner and plan for ongoing defense in the face of possibly diminishing network or processing assets.

Many aspects of modern warfare occur too rapidly, involve too much data, or both for unaided human processing, necessitating information system support. There is an intricate linking between the more traditional, physical business of defense and that of the information system, taxing the cyber SA system in at least two dimensions – defense of its own computing capability for conducting defensive operations and the provision of information system support for the physical counterpart.

Cyber Situation Awareness

To begin with, a cyber SA system must process incoming data. Such data is likely to be asynchronous, disparate in composition and source, and high in volume. This information comes, most generally, from the world external to the cyber SA system. Figure 1 depicts the SA feedback loop at the most basic level. The cyber SA system must have command of actions to affect its own state and that of the environment as a result of its reasoning and goal-seeking behavior. For example, implementation of a particular cyber defense may repel future attacks from an opponent's information system. The external world may

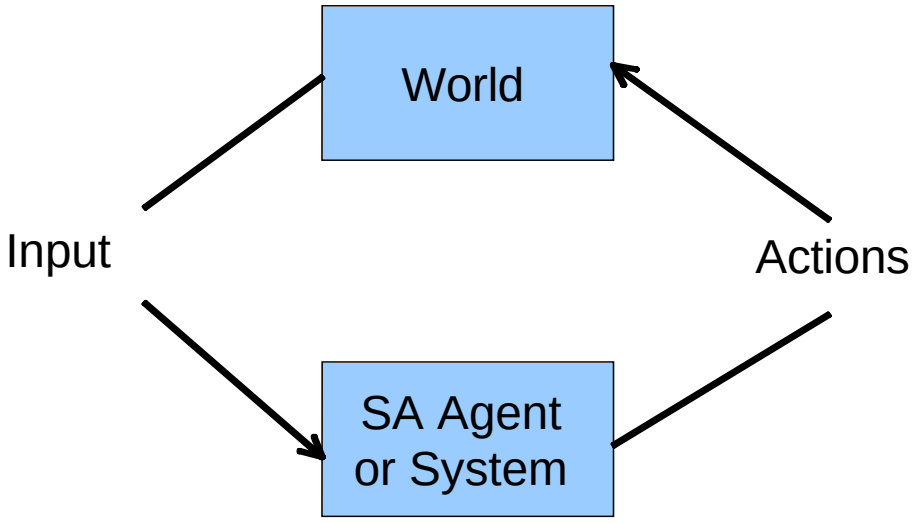


Figure 1. Simple Situational Awareness Feedback Loop

be digital or physical. For example, provision of real-time monitoring data may aid forces in accomplishing effective defense against a physical attack.

A cyber SA system must be able to abstract low-level details into higher-level models. A number of the models necessary for cyber SA are provided in Figure 2. The cyber SA system must capture and reason about past, current, and future states in its models. It must maintain a representation of self and the environment. It must model other actors in the environment, including friendly and opposition elements. The system must be able to bootstrap – build new models (or modify existing ones) based on new information combined with older information. Goals must be represented in the models, along with tracking of progress to goals and the impact of specific stimuli-response sets on goal progress. Models are updated based on input from the world, self status, and/or planning and reasoning outputs.

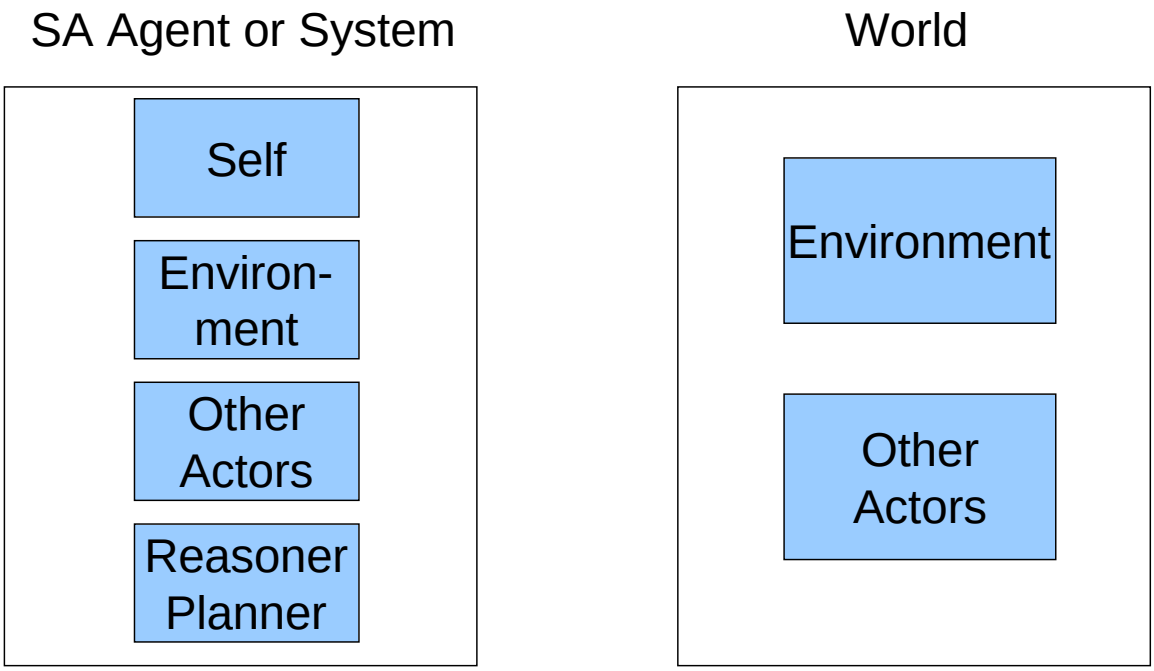


Figure 2. Cyber Situation Awareness Models vs External World

The ability to reason, specifically, to plan, is required in such a system, including the following capabilities:

1. recognition of particular situations, including novel situations
2. determination of the significance of particular situations
3. ability to tie situations with appropriate responses (reactive capability)
4. ability to anticipate future events (proactive capability)
5. ability to handle uncertainty and incompleteness
6. understanding of effects of actions on the world
7. knowledge of goals (regarding self, environment, other entities)

8. ability to break down goals into constituent parts.

Figure 3 depicts the use of goals to incrementally transition the environment from a beginning state to an end state.

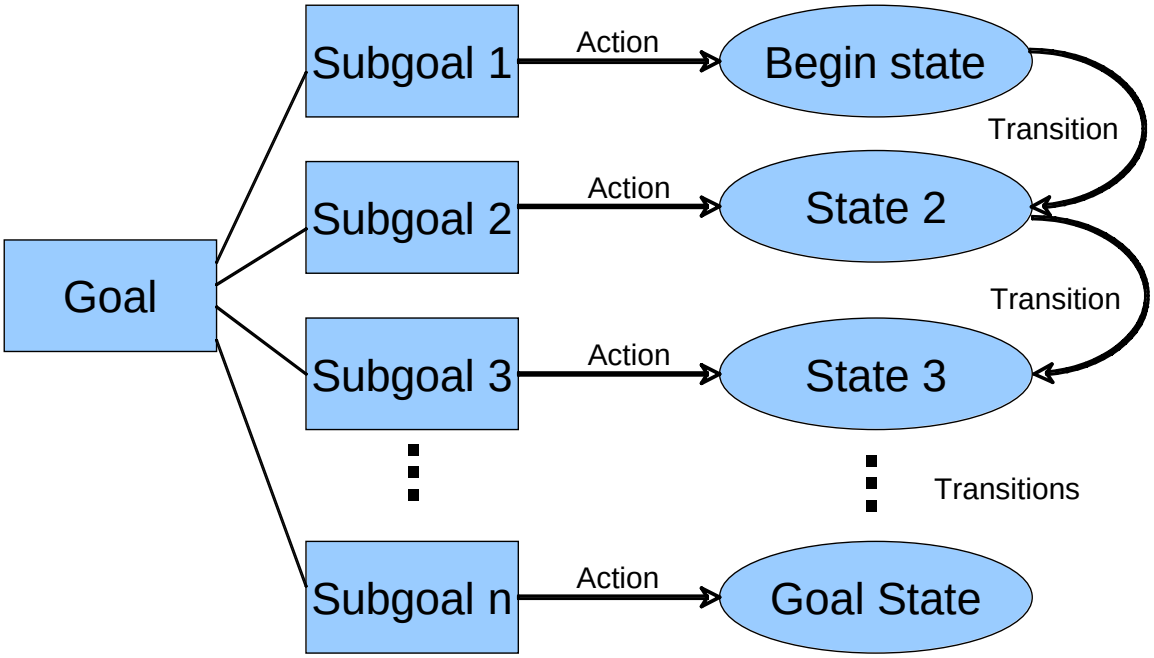


Figure 3. Incremental Goal Satisfaction

For higher-level SA performance, four additional capabilities are necessary. Temporal reasoning is needed since situations occur in time, including modal logic. Depending on the features of the domain, spatial reasoning and other specialized reasoning is likely needed as well. Truth maintenance, or the ability to know what facts no longer hold to be true in the world at a given time, is necessary in order to retract any inferences or decisions based on the facts, thus syncing reality with the SA models. Selective attention, mentioned earlier in this paper, is necessary since some data is more important than other data and the significance changes with time. Selective attention is necessary to reduce information overload in crowded or busy domains. It is closely tied to the efficacy of reasoning and the ability to anticipate events. Learning allows a cyber SA system to benefit from past experience, thus providing for better predictive capability, allowing more time for the reasoner to take evasive action or create countermeasure plans.

Other actors in the system may be benevolent, in which case the additional communication and coordination associated with team situational awareness may be necessary. On the other hand, other actors may be malevolent, in which case modeling takes on the flavor of game theory with antagonistic players. In some cases, the domain may involve both kinds of other actors. Identification becomes more significant in such cases to avoid spoofing and to identify the source of hostile attacks. Additionally, it is important for the cyber SA system to know what portions of the system are controllable

(to a lesser degree able to be influenced), those that are assessable (or knowable), and those that are unknowable and/or unpredictable. Figure 4 shows a more complex cyber SA feedback loop, in which friendly agents, hostile agents, and the cyber SA system interact with each other and the environment in a number of ways.

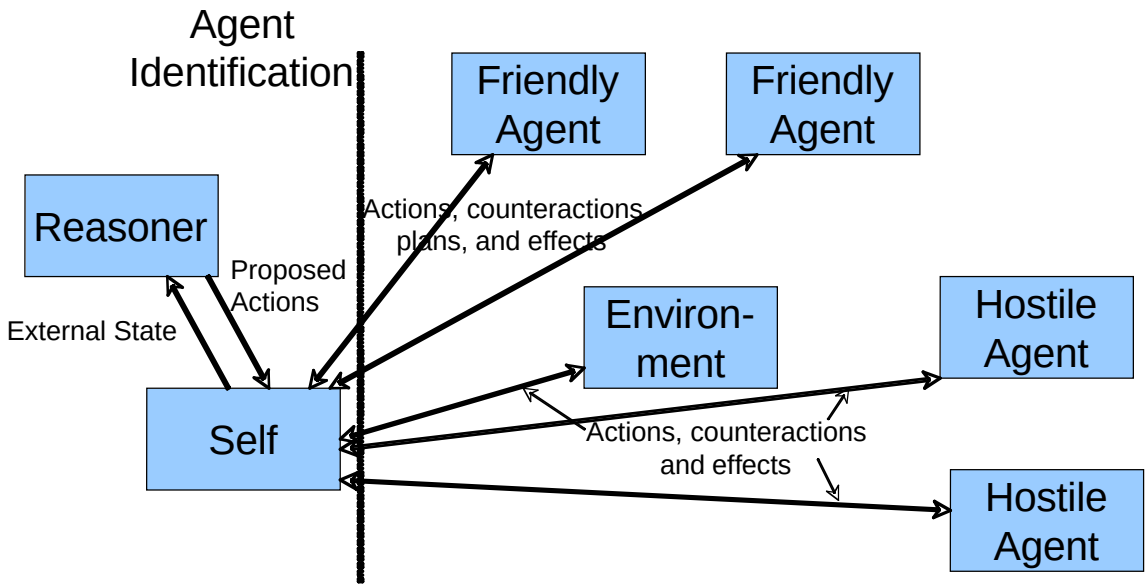


Figure 4. More Complex Depiction of Situation Awareness

The architecture for the cyber SA reasoner/planner is depicted in Figure 5. This architecture embodies the notions of communication, association, level of complexity, and timeframe of relevance as recommended by Hayden (2006). The assumption upon which the reasoner is based is that of time relevance – all events are modeled as occurring in time, and an explicit time representation is employed (Shoham 1988). Events, actions, and actors in the environment are described in terms of the time at which they apply, occur, or are active/relevant. Communication vias describe channels across which a kind of communication can occur. For example, encrypted or protected communication occurs within a particular via. Likewise, even though communication among hostile agents may not be fully knowable, the via may be identifiable at some point during an operation. The notion of a communication via is a familiar one for the cyber world. Associational patterns describe the interactions among actors and/or the environment. An understanding of each of these aspects of the cyber system and the physical system, particularly as patterns are related to one another and as they evolve over time, contributes to cyber situational awareness for defense. An abstractional hierarchy allows the reasoner to process information at a particular level of fidelity and associated complexity, providing the capability for fast, selective matching of patterns and associations and assuring a variety of different means for reasoning about the environment and associated actors. The next section will delineate why the latter two capabilities hold promise for the improvement of cyber situational awareness.

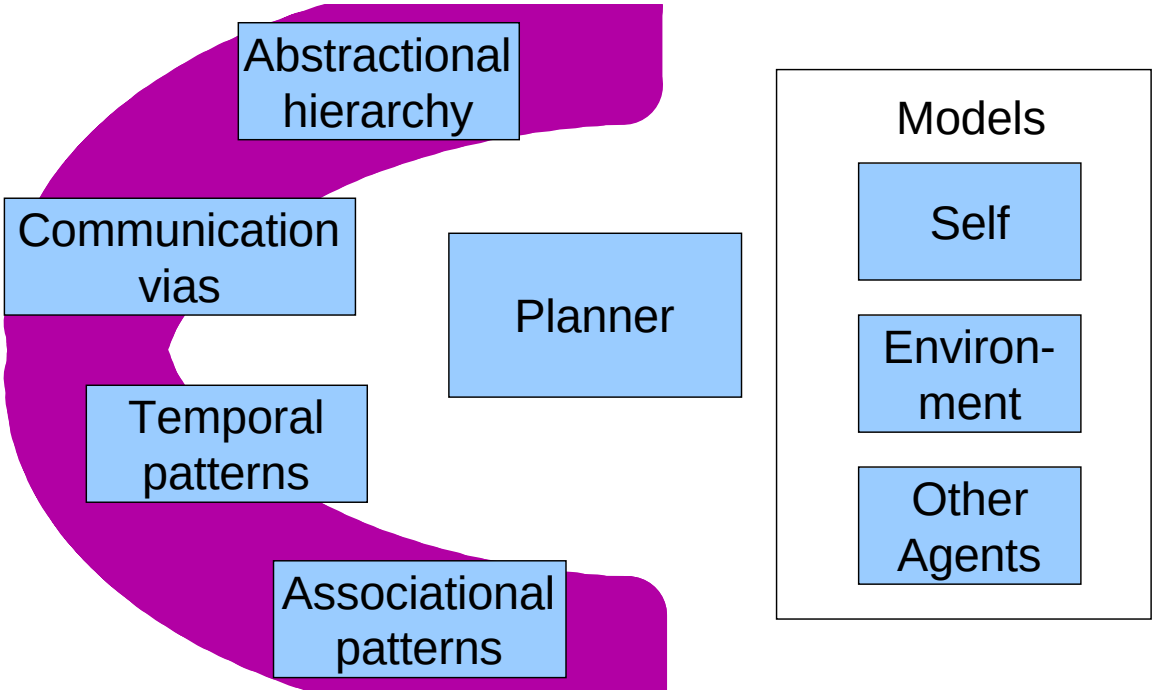


Figure 5. Situation Awareness Reasoning

Reduction of Complexity

The description of the mechanisms and characteristics of the human brain in this section is based on Hawkins (2004). The human brain knows about the world through human senses. Our senses can only detect parts of the absolute world. Patterns are created of the input from our senses that are processed by the cortex of the brain. Regardless of the particular sense (e.g., taste, vision) employed, it is believed that the cortex uses the same cortical algorithm to create a model of the world. Thus, fundamentally different kinds of data coming in through the senses are thought to be translated into a common representation in the brain. This model of the world is held in memory.

Cortical memory seems to store information in temporal sequences. Humans are capable of auto-associative recall – they can recall complete patterns when given only partial or distorted inputs. Humans can accomplish this capability for both spatial and temporal patterns. For example, humans can complete an image in their minds when provided with a partially-occluded picture. Finally, humans seem to store invariant representations – ones that are general enough to be able to match with a wide variety of specific instantiations. In other words, we store patterns with less than complete fidelity in order to remember the important relationships of the world, independent of the details. This capability allows us to, for example, match a person's face with our memory of the person's image, regardless of their orientation with respect to our position (Hawkins 2004).

What are the implications of this research for the improvement of cyber SA systems? The majority of SA systems developed for reasoning about complex domains tend to exhibit a complexity that approaches that of the domain being modeled. It seems intuitive that one must represent and process complex problems with complex systems. However, that is not the path suggested by the latest brain research. Rather, it makes more sense to build a fairly simple mechanism for processing patterns, and focus instead on the content of the patterns when it comes to representing, comparing, and processing complexity. Such a data-driven approach is in line with many successful models of complex systems in other domains.

Input from disparate sources does not necessarily have to remain disparate in format as it is processed. If one wants to achieve the kind of cyber SA system that can handle discernment, spontaneity, and the ability to deal with novel situations and surprise, it is necessary to carefully design the specific patterns for representing situations and the manner in which they are stored and retrieved. On the one hand, the patterns should be specific enough to achieve differentiation and discernment of situations. On the other hand, the patterns should be general enough to allow for recall and application to a number of variants of particular situations, with post-recall adjustments to meet the needs of a specific situation. The author believes that time spent in carefully designing the transformation of incoming patterns to represent situations such that:

1. patterns from unlike sources can be analyzed together
2. after transformation, the patterns will easily exhibit critical information

is more fruitful than time devoted to increasing levels of complexity in the structure or processing of a cyber SA system for complex domains such as cyber defense.

Conclusion

To achieve cyber situational awareness for defensive capabilities in the face of hostile attacks, it is critical to understand the complexity of such a domain. Typically, the domain is characterized by sets of complex, interacting issues that are ill-defined, ambiguous, and evolving in time. This paper has described essential characteristics for the achievement of cyber SA capability, as well as characteristics for approaching higher-level SA behavior. An architecture is posed for reasoning in such a system. In spite of the complexity of the cyber defense domain, building complexity into the cyber SA system is not necessarily the answer to solving the hard problems of the domain. In fact, recent brain research suggests a different approach – maintaining simplicity in cyber system design and processing, and carefully thinking about how to represent patterns stored in memory such that they can be readily recalled to apply to later, perhaps novel, situations. A number of dichotomies have been introduced herein: predictability versus handling the novel; control of an asset versus assessment or characterization; benevolent versus malevolent actors; specialized versus generalized patterns; and complex versus simple designs. The achievement of cyber situational awareness rests in the ability to judiciously balance these notions as we design cyber systems able to handle the complexities of defensive operations.

References

Endsley, M.R. (1988), *Design and Evaluation for Situation Awareness Enhancement*, paper presented at the Human Factor Society 32nd Annual Meeting, Santa Monica.

Endsley, M.R. (1995), 'Toward a Theory of Situation Awareness in Dynamic Systems', *Human Factors*, vol. 37(1), pp. 32-64.

Klein, G. (1997), 'The Recognition-Primed Decision (RPD) Model: Looking Back, Looking Forward', in C.E. Zsambock and G. Klein (eds), *Naturalistic Decision Making*, Lawrence Erlbaum Associates, Mahwah, pp. 285-292.

Rasmussen, J. (1983), 'Skills, Rules, and Knowledge: Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models', *IEEE Transactions on Systems, Man and Cybernetics*, vol. 13(3), pp. 257-266.

Pew, R.W. (2000), 'The State of Situation Awareness Measurement: Heading Toward the Next Century', in M.R. Endsley and D.J. Garland (eds), *Situation Awareness Analysis and Measurement*, Lawrence Erlbaum Associates Inc., Mahwah, pp. 33-47.

Rousseau, R., Tremblay, S., and Breton, R. (2004), 'Defining and Modeling Situation Awareness: A Critical Review', in S. Banbury and S. Tremblay (eds.), *A Cognitive Approach to Situation Awareness: Theory and Application*, Ashgate Publishing Company, Burlington, pp. 3-21.

Interrante [Cumiford], L.D. (1991), 'A Model for Selective Attention in Monitoring and Control Reasoning Tasks', in *1991 Proceedings of the IEEE Systems, Man and Cybernetics Conference*, Institute of Electrical and Electronics Engineers.

Hayden, N.K. (2006), *The Complexity of Terrorism: Social and Behavioral Understanding, Trends for the Future*, Draft Document, to be published by Routledge Press, February 7, 2006.

Barabasi, , A.-L. and Albert, R. (1999), 'Emergence of Scaling in Random Networks', *Science*, vol. 286, pp. 509-512.

Watts, D. (2003), *Six Degrees – The Science of a Connected Age*, W.W. Norton & Company, New York.

Rittel, H. and Weber, M. (1973), 'Dilemmas in a General Theory of Planning', *Policy Sciences*, vol. 4, pp. 155-169.

Hawkins, J. (2004), *On Intelligence*, Henry Holt and Company, LLC, New York.

Shoham, Y. (1988), *Reasoning about Change*, MIT Press, Cambridge.

Situation Awareness for Cyber Defense

June 20-22, 2006

Leslie D. Cumiford, PhD, PE
Knowledge Discovery and Extraction
Defense Systems and Assessments
Sandia National Laboratories
ldcumif@sandia.gov

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Overview

- Situation awareness (SA)
- Cyber defense domain
- Addressing of complexity
- Cyber situation awareness
- Reduction of complexity
- Conclusions

Situation Awareness (SA)

The ability to rapidly and effectively address incoming stimuli with appropriate responses.

- **Awareness of current environment**
- **Ability to assess and impact environment**
- **Ability to accomplish goals**
- **Reasoning about time**
- **Selective attention for crowded environments**

Cyber Defense Domain

- **Characteristics in common with domains of terrorism analysis, infrastructure protection, and IED defense**
- **Complex, interacting issues are ill-defined, ambiguous, and evolving**
- **Patterns of communication and association across interfaces**
- **Level of system complexity and timeframe of relevance are important choices**

(Hayden 2006)

Cyber Agents for Defensive Operations

Defend:

- **Self**
- **Related information systems**
- **Control systems for physical systems**
- **Human force or operation**
- **Allied forces or systems**
- **A combination of the above**

Cyber Defense Domain Complexity

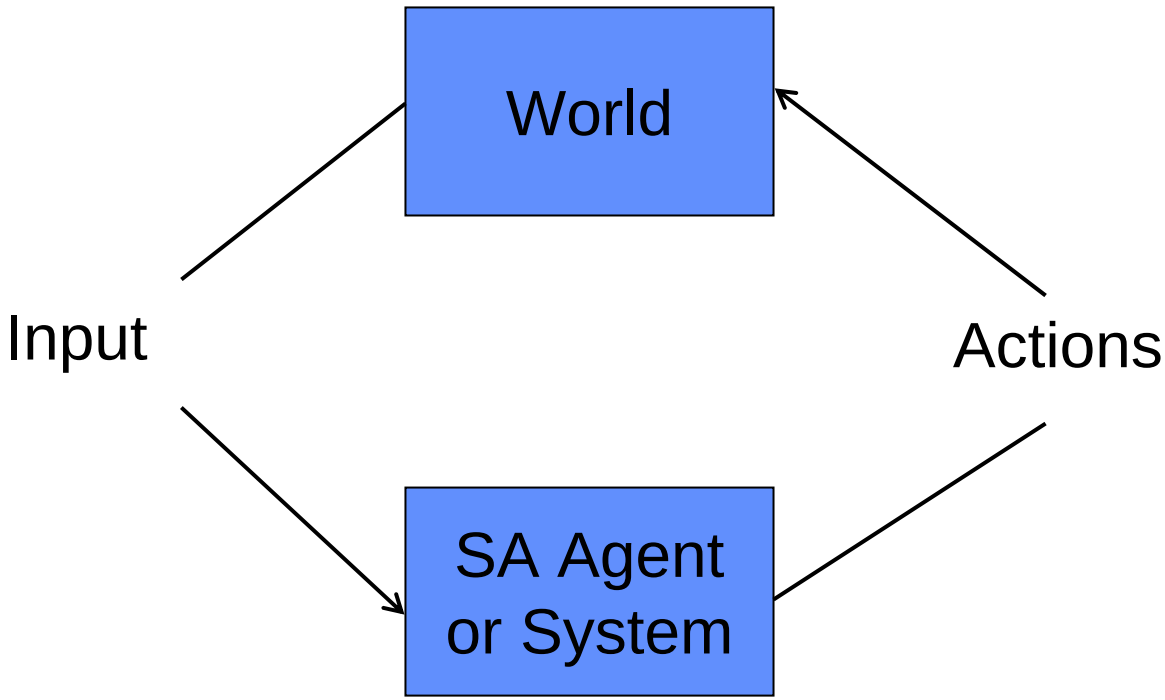
Cyber SA: need discernment and spontaneity

- **Two dimensions: digital and physical defense**
- **Tasks, to be dynamically conducted over time:**
  - **Assess and track enemy's cyber capabilities**
  - **Predict and defend against attacks**
  - **Assess and track own defense capabilities**
  - **Coordinate with allied operations**
  - **Note influence of environmental factors (e.g., hardware failures)**
  - **Maintain tempo faster than that of hostile attacking systems**
  - **Battle damage assessment of self and friendly systems**

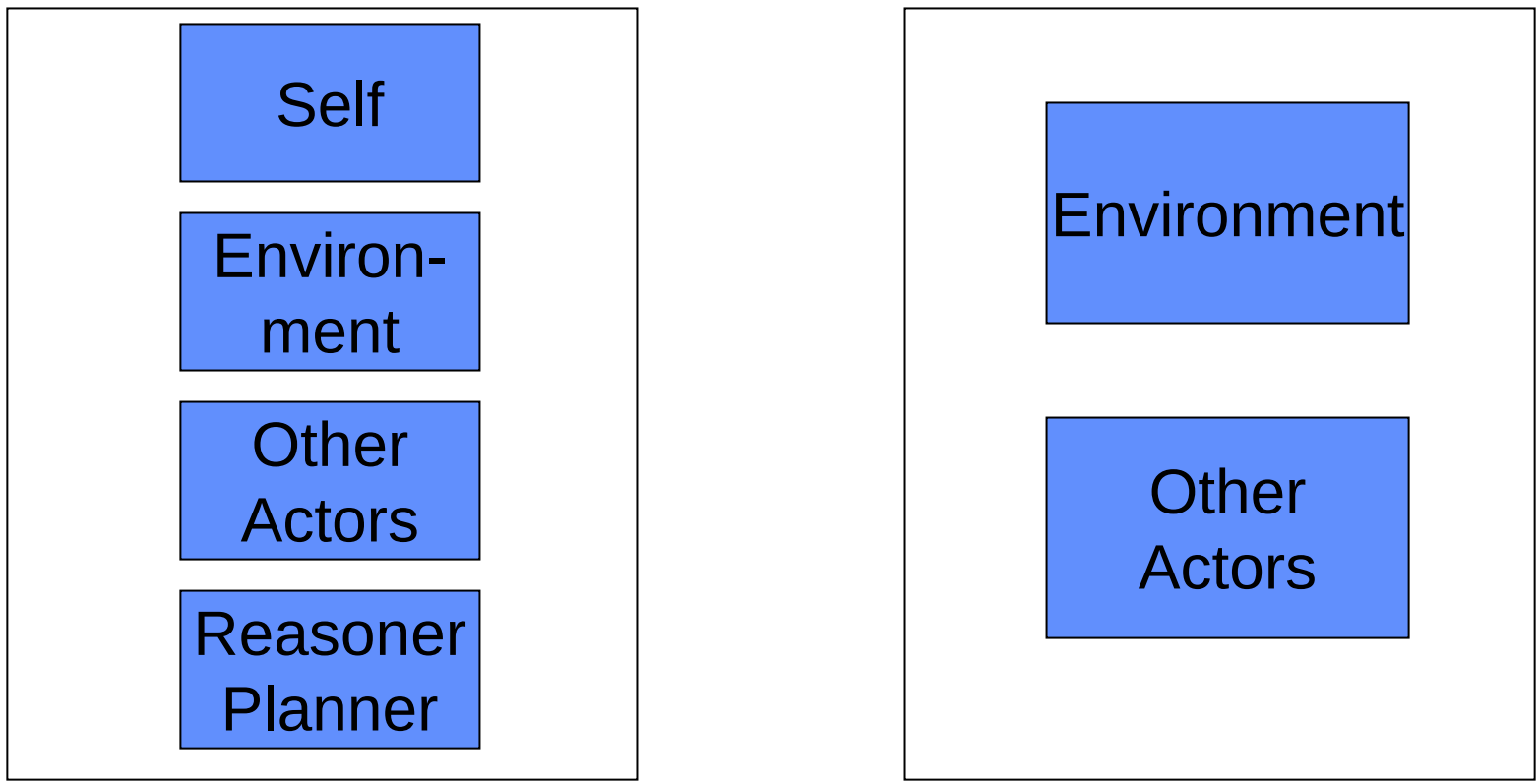
Cyber Situation Awareness

- **Process incoming data**
  - **Asynchronous**
  - **Disparate in composition and source**
  - **High in volume**
- **Abstract low-level details into higher-level models**
- **Capture and reason about past, present, and future states**
- **Bootstrap to evolve models**
- **Track progress to goals**

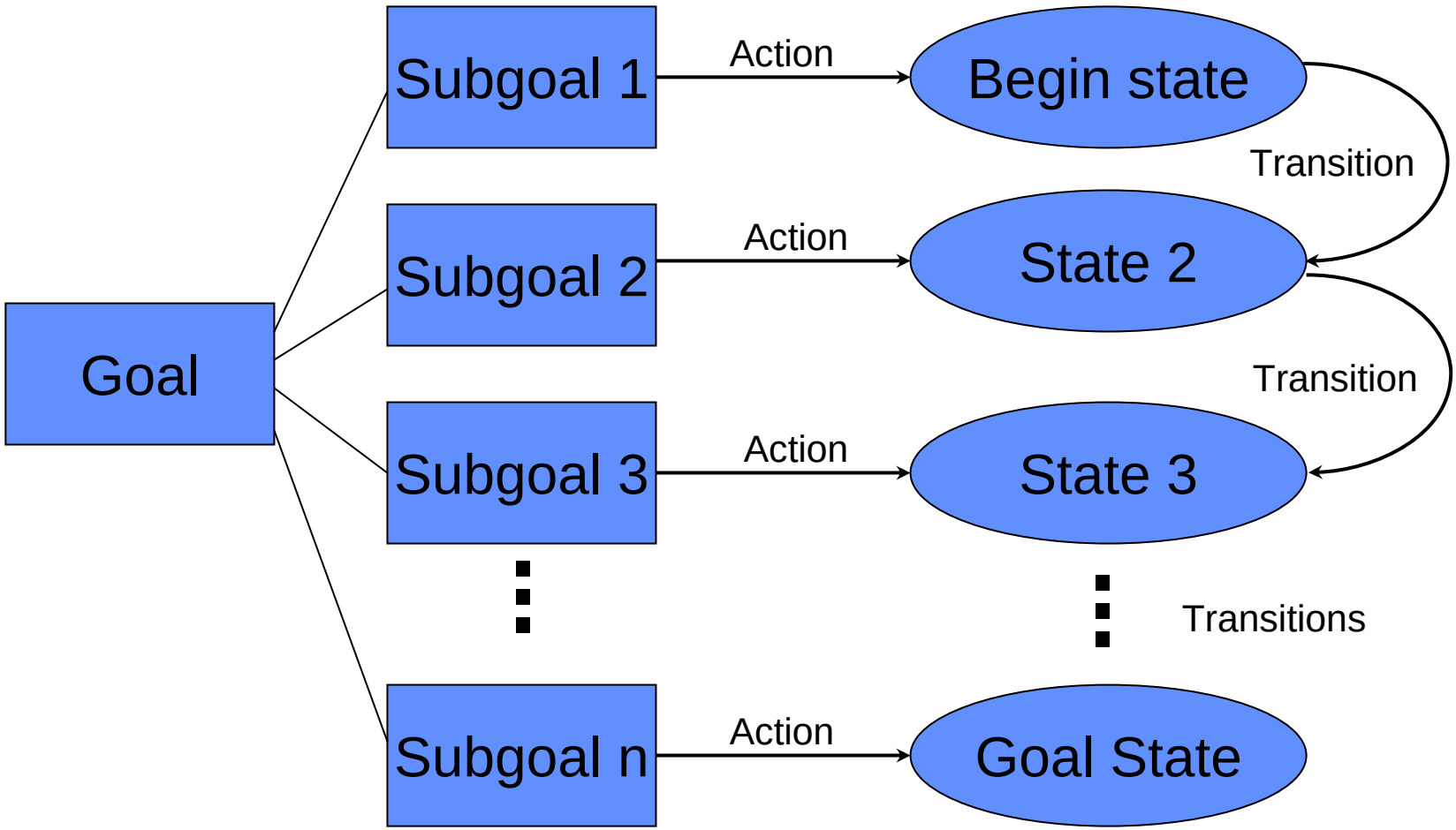
Simple SA Feedback Loop



Situation Awareness Models



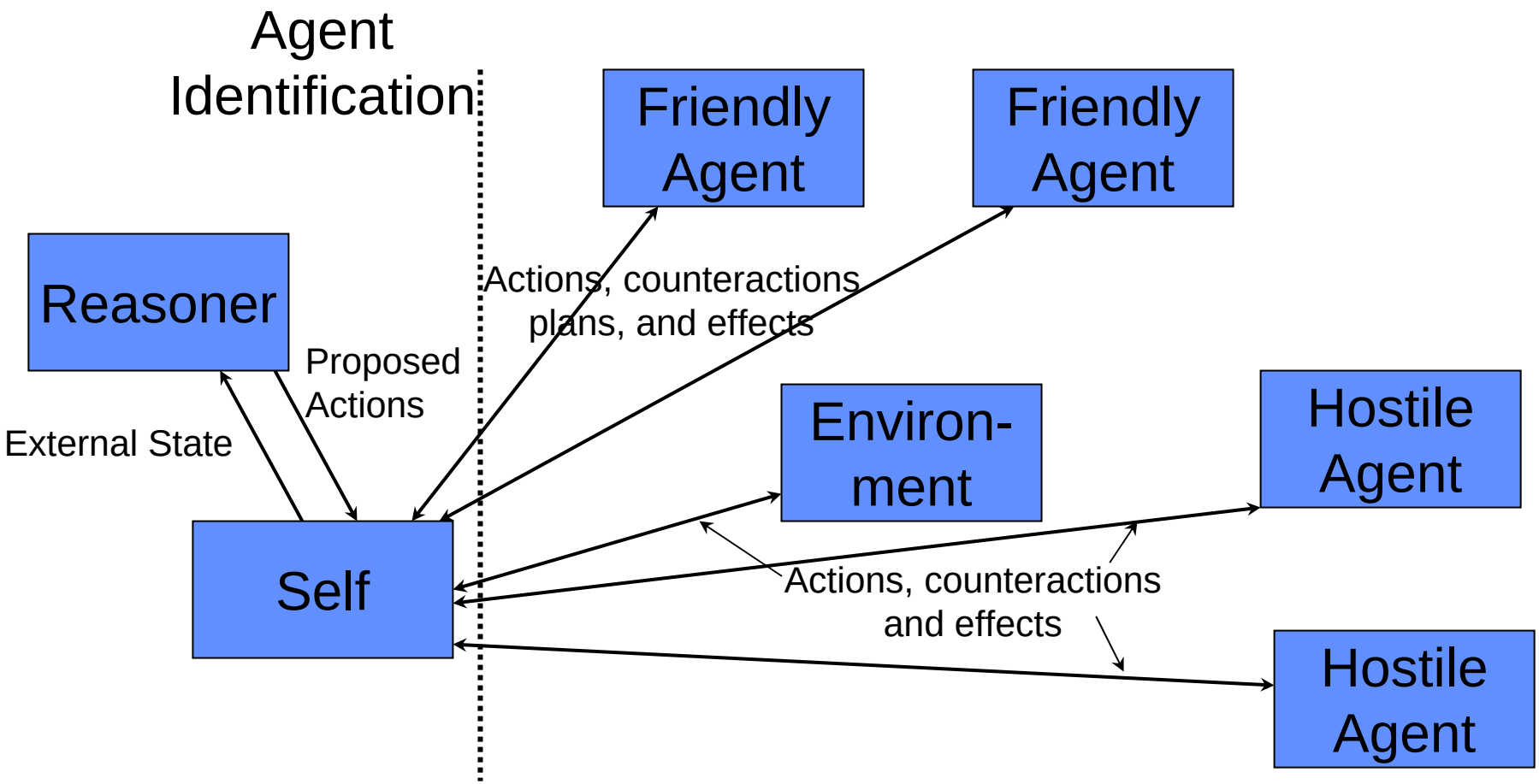
Incremental Goal Satisfaction



Higher-Level SA Capability

- Explicit temporal reasoning (modal logic)
  - To see deadlines, coincident events, etc.
- Domain may require spatial or other specialized reasoning
- Truth maintenance
  - To sync reality with models
- Selective attention
  - To reduce information overload in crowded environments
- Learning
  - To benefit from past experience

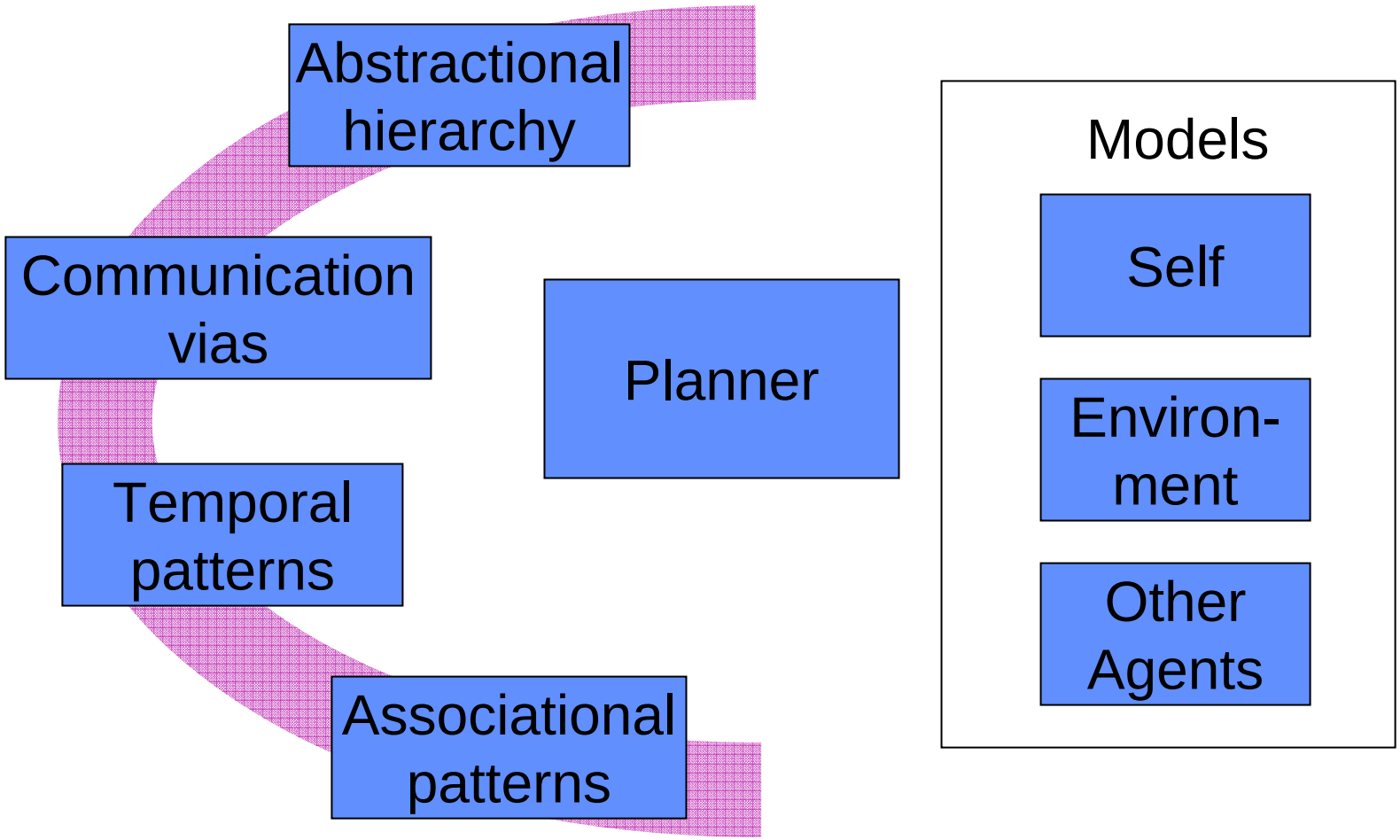
More Complex SA Feedback Loop



Cyber SA Agent: Handling Other Actors

- **Benevolent other actors**
  - **communication and coordination associated with team SA**
- **Malevolent other actors**
  - **game theory with antagonistic players**
- **Domain may include both**
  - **Authentication of communication sources and identity of other actors**
    - **Avoid spoofing**
    - **Identify source of attack**

Situation Awareness Reasoning



Reduction of Complexity

Lessons from brain research (Hawkins 2004)

- Different kinds of data from our senses are made into common patterns for cortex processing
- Patterns are stored in memory as temporal sequences by the cortex
- Auto-associative recall
- Invariant representations

Conclusion for cyber SA: Focus on transformation of incoming patterns more fruitful than matching of complexity in system structure to that of the domain

Conclusions

- Understand the complexity of the cyber defense domain
- Mirroring the complexity in the cyber SA system is not necessarily the answer
- Focus on patterns and memory
- Judiciously balance dichotomies in the design:
  - Prediction vs novel events
  - Control vs assessment
  - Benevolent vs malevolent other actors
  - Specialized vs generalized patterns
  - Complex vs simple