General Requirements of a Hybrid-Modeling Framework for Cyber Security

Alessandro Oltramari, Noam Ben-Asher, Lorrie Cranor, Lujo Bauer, Nicolas Christin
Carnegie Mellon University
Pittsburgh, USA

Abstract— **Understanding human dynamics of cyber security is a critical step for enhancing situation awareness of analysts. To this end, in this paper we focus on the requirements for building a comprehensive model of cyber analyst's decision making processes: we embrace an approach that leverages on cognitive aspects and knowledge representation to define the core elements of such model. In particular, we make the case for investigating the interplay between ontological underpinnings of cyber security and cognitive mechanisms of decision making in cyber operations. We claim that, by integrating ontologies and cognitive architectures in a hybrid-modeling framework, it's possible to rigorously characterize and simulate the core structures that govern the decisions of defenders and attackers and mediate interactions among them in the cyberspace.**

Keywords—ontology, cognitive architecture, cyber security, situation awareness

I. Introduction

The cyberspace is populated by a variegate range of hybrid entities, emerging as intertwined digital structures out from the physical substratum of computer networks. But, first of all, the cyberspace is a complex technological infrastructure built by humans to store, access and share information. In this regard, "the cyberspace is defined as much by the cognitive realm as by the physical or digital" [1]. As a result of this *multilayeredness*, "cyber security", namely the security of all those entities – including humans – that operate in cyberspace, has become an increasingly complicated problem, that demands scientific understanding both in terms of theoretically-grounded and empirically validated models [2]: a rigorous approach is thus needed to learn how to deploy defensive mechanisms in compliance with security policies to contrast diverse and variable kinds of attacks, from destruction or theft of data to interference with information systems and disruption of computer networks, across a spectrum of private and public interests. In order to recognize, comprehend and properly respond to cyber threats, a rigorous analysis of the cognitive dynamics of decision making is also necessary: in this respect, a central objective of a "science of cyber security" is to improve situation awareness of analysts [3] and reduce their "cognitive load" i.e. factoring in the distinctive cognitive elements into play, such as attention, memory, experience, reasoning capabilities, expectations, confidence, performance, etc.

Far from being exhaustive, this paper aims at introducing some of the core aspects that a comprehensive model needs to specify in order to meet the complexity of cyber security. To this end, we refer to the paradigm of "socio-technical system" [4], which emphasizes social and cognitive aspects of the interactions between humans and technologies. Ontologies have proved to be powerful tools for specifying knowledge and rules embedded in socio-technical systems [5], but they are not suitable to model human behavior in cyber operations, which needs to be studied as a genuinely dynamic cognitive phenomenon. In this perspective, the two key components of the hybrid-modeling framework we propose are:

- Ontologies – to serve as formal specifications of the entities involved in cyber security, e.g. classes of attacks, defenses, policies, etc. [6].
- Cognitive architectures – to serve as dynamic models of human decision making in cyber security. These models, based on ACT-R[1] cognitive architecture [7], will focus on learning mechanisms, memory and attentional limitations, defense and attack strategies, risk perception, and trusted judgments.

By integrating ontologies and cognitive architectures, we aim at unraveling the complex structures that govern the behavior of defenders and attackers and mediate interactions among them in the cyberspace.

Combining detailed information structures that semantically maps the cyber security domain with the dynamic and adaptive reasoning mechanisms of cognitive architectures, opens a wide range of possibilities spanning from decision support systems and simulations of what-if scenarios, to training environments.

Research was sponsored by the Army Research Laboratory and was accomplished under Cooperative Agreement Number W911NF-13-2-0045 (ARL Cyber Security CRA). The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation here on.

[1] Pronounced, "act-ARE", the acronym stands for "Adaptive Control of Thought—Rational".

The rest of the paper is organized as follows: Section II outlines ontologies and cognitive architectures, focusing on their role as components of a unified model of cyber analyst's decision making processes; Section III sketches a preliminary empirical paradigm for testing the proposed framework in a scalable experimental settings.

II. Towards a Hybrid-Modeling Framework for Cyber Security

A. *Ontologies of cyber security*

Ontology, 'the study of being as such' – as Aristotle named it – originated as a philosophical discipline and evolved into a modern science in the computer era [26]. According to a widely-accepted contemporary definition, an "ontology" is "a language-dependent cognitive artifact committed to a certain conceptualization of the world by means of a given language" [8]. In other terms, an ontology[2] corresponds to a semantic model of the world: when the model is simply described in natural language, an ontology reduces to a *dictionary, thesaurus,* or *terminology*; when the model is expressed as an axiomatic theory (e.g., in first order logics), it is called a *formal ontology*; ultimately, if logical constraints are encoded into machine-readable formats, formal ontologies take the form of *computational ontologies* and become software components, entering *de facto* in the spectrum of *semantic technologies*. For the sake of applications, ontologies seldom deal with the whole world[3]: they are built to represent specific *domains*, like agriculture or genomics. But, despite fine-grained concepts being important, it's a good practice to design domain ontologies by means of well-grounded *top-level* distinctions (e.g., the difference between objects and events, including the corresponding attributes and mutual relationships) and *middle-level* distinctions, (e.g., distinguishing attack strategies from defensive maneuvers in a warfare scenario). Computational ontologies have found application in a growing variety of areas, such as biomedical informatics, robotics, natural language processing, sentiment analysis, etc. [39]. In particular, they have recently attracted great interest thanks to the vision of the "Semantic Web", the effort to develop scalable semantic models and technologies for representing, sharing, and reasoning over structured data in the World Wide Web (e.g., the W3C Ontology Web Language - OWL[4]).

The development of computational ontologies of cyber security is a critical step in the transformation of cyber security to a science. In 2010, the DoD sponsored a study to examine the theory and practice of cyber security, and evaluate whether there are underlying fundamental principles that would make it possible to adopt a more scientific approach. The study team concluded that:

The most important attributes would be the construction of a common language and a set of basic concepts about which the security community can develop a shared understanding. A common language and agreed-upon experimental protocols will facilitate the testing of hypotheses and validation of concepts [9].

The need for controlled vocabularies and ontologies to make progress toward a science of cyber security is recognized in [10] and [11] as well. In the domain of cyber security, ontologies would include, among other things, the classification of cyber attacks, cyber incidents, and malicious and impacted software programs. From our point of view, where the human component of cyber security is also crucial, we expand our analysis to the different roles that attackers, users, defenders and policy makers play in the context of cyber security, and to the different tasks that the members of a team are assigned to by the team leader, and the knowledge, skills and abilities needed to fulfill them. In order to reduce the level of effort, we will reuse existing ontologies when possible[5] and only create new ontologies to support novel use cases if needed. As a matter of fact, there has been little work on ontologies for cyber security and cyber warfare. Within a broader paper, there is a brief discussion of an ontology for DDoS attacks [12] and a general ontology for cyber warfare is discussed in [13]. Obrst and colleagues [14] provide the best sketch of a cyber warfare ontology, and the scale of the project and its difficulties are discussed by Dipert in [11]. By and large, efforts that have been made toward developing computational ontologies of cyber security, even when expressed in OWL, RDF or other XML-based formats, typically do not utilize existing military domain or middle-level ontologies such UCORE-SL[6]. With regard to human users and human computer interaction (HCI), the most important step in understanding a complex new domain involves producing accessible terminological definitions and classifications of entities and phenomena: Mundie and colleagues stressed this point in [10]. Discussions of cyber warfare and cyber security often begin with the difficulties created by misused terminology (such as characterizing cyber espionage as a attack): in this regard, the Joint Chiefs of Staff created a list of cyber term definitions that has been further developed and improved in a classified version[7]. None of these definitions, however, are structured as an ontology. Likewise, various agencies and corporations (NIST[8], MITRE[9], Verizon[10]) have formulated enumerations of types of malware, vulnerabilities, and exploitations, sometimes expressed in XML-based semantics. In particular MITRE, which has been

[2] Note that the lowercase differentiates the "artifact" (ontology) from the "discipline" (Ontology).

[3] The most comprehensive and long-lived attempt of building an "ontology of the world" is reflected by Doug Lenat's project Cyc, which commits to represent everyday commonsense knowledge [27].

[4] OWL is based on description logics; description logics are *decidable* fragment of First-Order Logics (http://www.w3.org/TR/owl-features/).

[5] For instance, exploiting material from this portal: http://militaryontology.com/cyber-security-ontology.html

[6] http://www.slideshare.net/BarrySmith3/universal-core-semantic-layer-ucoresl

[7] http://publicintelligence.net/dod-joint-cyber-terms/

[8] http://www.nist.gov/

[9] http://www.mitre.org/

[10]http://www.verizon.com/

very active in this field, maintains two dictionaries, namely CVE (Common Vulnereabilities and Exposures[11]) and CWE (Common Weakness Enumeration[12]), a classification of attack patterns (CAPEC - Common Attack Pattern Enumeration and Classification [13]), and an XML-structured language to represent cyber threat information (STIX - structure Threat Information Expression[14]). Despite the intrinsic value of these resources, without a "shared semantics", their sprawling English descriptions in large, incompatible databases are hard to maintain and port into machine-usable formats.

B. Cognitive architectures for cyber security

Modeling decision-making in cyber security requires multiple factors to be investigated: (*i*) the size and the variety of *knowledge* which is necessary to classify and analyze attacks, defensive actions and policies; (*ii*) the *flexible behavior* required by coupling alternative strategies of response to specific cyber threats, updating and revising strategies when the circumstances of the attack or the environmental conditions evolve; (*iii*) *learning by experience* how to deal with cyber attacks; (*iv*) *interacting* in a team by building a mental representation of the co-workers as well as of the adversaries. These factors can be mapped to the criteria distilled in [15] (from the original list compiled by Newell in [16]) that a "cognitive architecture" would have to satisfy in order to achieve human-level functionality. In general, cognitive architectures attempt to capture at the computational level the invariant mechanisms of human cognition, including those underlying the functions of control, learning, memory, adaptivity, perception, decision-making, and action. In these regards, cognition is not considered as a "tool" for optimal problem solving but, rather, as a set of limited information processing capacities (so-called 'bounded rationality' [17]). In a similar fashion, Wooldridge identified the requirements that an agent fulfills when acting on a rational basis [18], namely: *reactivity*, the capacity of properly reacting to perceptual stimuli; *proactivity*, the capacity of operating to pursue a goal; *autonomy*, implying an unsupervised decision making process; *social ability*, the capacity of interacting with other agents and revising mental states accordingly. State-of-the-art research on cognitive architectures (SOAR, ACT-R, CLARION, OpenCog, LIDA, etc.) has produced a significant amount of results on specifying this extensive range of functions: by and large, ACT-R has accounted for the broadest portion of them at a high level of fidelity, reproducing aspects of behavioral data such as learning, errors, latencies, eye movements and patterns of brain activity [7]. However, these results have often involved relatively narrow and predictable tasks. Moreover, research in cognitive architectures have just started to address the problem of how to model *social ability* [19], whose fundamental feature is "mindreading" [20], i.e. to understand and predict the actions of others by means of hypothesizing their intentions, goals and expectations: this process of interpretation is feasible only if an agent can learn to *represent* the mental states of others on the basis of cumulative experience and background knowledge, combining the resulting mental model with the continuous stream of data from the environment, aiming at replicating the cognitive processes that have likely motivated the other agents to perform the observed actions. Social ability is clearly an important feature to be included in models of cyber operations, e.g. the choice of a defensive strategy is more effective when the intentions of the attacker are pondered in first place.

C. Replicating cognitive mechanisms with ACT-R

ACT-R [7] is a modular cognitive architecture including perceptual, motor and declarative memory components, synchronized by a procedural module through limited capacity buffers (see figure 1). Declarative memory (DM) plays an important role in the ACT-R system. At the symbolic level, ACT-R agents perform two major operations on DM: 1) accumulating knowledge "chunks" learned from internal operations or from interacting with objects and other agents populating the environment and 2) retrieving chunks that provide needed information. ACT-R distinguishes "declarative knowledge" from "procedural knowledge", the latter being conceived as a set of procedures (or production rules) which coordinate information processing between its various modules [7]: according to this framework, agents accomplish their goals on the basis of declarative representations (semantic contents) elaborated through procedural steps (in the form of *if-then* clauses). This dissociation between semantic and procedural knowledge is grounded in experimental cognitive psychology; major studies in cognitive neuroscience also indicate a specific role of the hippocampus in "forming permanent declarative memories" and of the basal ganglia in production processes (see [21], pp. 96-99, for a general mapping of ACT-R modules and buffers to brain areas and [22] for a detailed neural model of the basal ganglia's role in controlling information flow between cortical regions). In summary, ACT-R simulates cognitive tasks by combining rules and representations: for reasons of space, a complete analysis of how the architecture instantiates this cognitive-based processing is not suitable here. Nevertheless, two core mechanisms need to be mentioned: *a) partial matching,* the probability of association between two distinct declarative knowledge chunks, computed on the basis of adequate similarity measures (e.g. a "computer virus" is more likely to share some characteristics with a a "computer worm" rather than with an "anti-spyware software"); *b) spreading activation*, the phenomenon by which a chunk distributionally activates the different contexts in which it occurs ("Stuxnet" can evoke "SCADA systems", "Malware", "PLCs of Iranian nuclear centrifuges", "Windows operating systems", etc.). Partial matching and spreading activation belong to the general sub-symbolic computations underlying chunk activation, which in ACT-R control the retrieval of declarative knowledge elements by procedural rules. The intertwined connection between declarative and procedural knowledge, weighted by stochastic computations, denotes the necessary substrate for realizing at the computational level the functionalities outlined at the beginning of this section: more

[11] https://cve.mitre.org/

[12] http://cwe.mitre.org/

[13] https://capec.mitre.org/

[14] https://stix.mitre.org/language/version1.1.1/

specifically, we claim that ACT-R can successfully be employed to emulate human behavior in selecting and executing defense strategies, matching input data from ongoing cyber attacks to deeply structured background knowledge of cyber operations (in the past, ACT-R architecture has been successfully used in contexts where integrating declarative and procedural knowledge was also a fundamental issue, e.g. air traffic control simulations [23]). Scaling up ACT-R to account for extensive multi-agent scenarios can help to build comprehensive models[15] of social conflict and cooperation, which are critical to discern the governing dynamics of cyber operations.

But if ACT-R is typically sufficient to replicate the *mechanisms* described in section *B* by (*ii*)-(*iv*), (*i*) can only be accomplished by "injecting" a fair amount of domain knowledge into the architecture: in this respect, "ontologies of cyber security" can be an adequate source of formalized semantic structures to be integrated into ACT-R declarative memory [24].

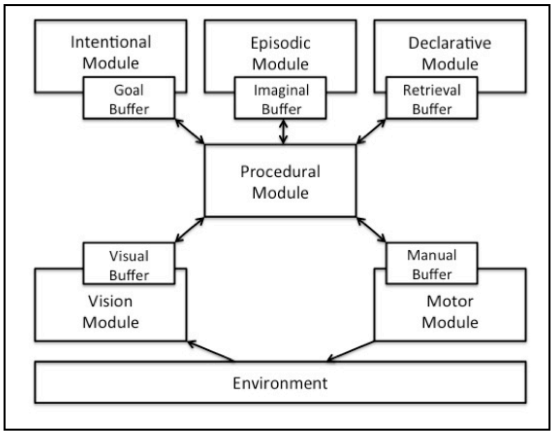

Figure 1 ACT-R Modular Structures

D. *Enhancing ACT-R with ontologies of cyber security*

Whilst the separation between declarative and procedural knowledge in ACT-R is experimentally grounded in psychological studies on "knowledge dissociation" [7], this distinction has been the bedrock of artificial intelligence over the last thirty years. In 1980 McCarthy first realized that, in order to enable full-fledged reasoning capabilities, logic-based intelligent systems must incorporate "re-usable declarative representations that correspond to objects and processes of the world" [25]. Therefore, in the context of cognitive architectures ontologies can clearly play the role of long-term memory structures, namely semantic extensions of the declarative knowledge at the disposal of a particular agent. Although these kinds of extensions are not usually required by ACT-R models to replicate relatively limited cognitive tasks, declarative memory needs to be properly designed to encompass a rich spectrum of concepts and relations when dealing with complex scenarios like cyber operations, including types of attacks, risks, policies, system's functionalities and vulnerabilities, human responsibilities, as well as all the interconnections.

Widening the scope beyond ACT-R, state of the art work has also focused on mapping ontologies to the declarative memory of cognitive systems (see [28], [29] and [30]), aiming to enhance not only the "capability" of representing information but also the functionality of automatically deriving implications from known facts. In this regard, and following the research path described in [3], ontologies can be used to 1) characterize knowledge in long-term memory that depicts prototypical situations and goals, and that dictate decision making and action performance and 2) foster *automaticity* of certain cognitive tasks, "that significantly benefit situation awareness by providing a mechanism for overcoming limited attention".

As [28], [29], and [31] show, most research efforts have focused on designing methods for mapping large knowledge bases to ACT-R declarative module, but with scarce success due to the heavy computational costs. A more efficient approach deals with "modular ontologies", which have become a key issue in ontology engineering ([32] gives a good overview of it). Modularity guarantees wide coverage and "maintainability": in our context, for instance, instead of tying ACT-R to a single large ontology, which is hard to manage, update and query, a *suite of* ontologies would reliably combine different dimensions of the cyber security, e.g. representation of secure information systems at different levels of granularity (system requirements, user guidelines, core functions, etc.); categorization of attacks, viruses, malware, spyware, worms, bots; descriptions of defense strategies; representations of the attacker's mental attitudes, and so on.

III. COGNITIVE SIMULATIONS OF CYBER OPERATIONS: AN EVALUATION PLAN

As recent studies have shown [33], training users to identify cyber threats and to better protect themselves becomes effective only after several iterations. But this means that, until training starts producing the expected benefits, socio-technical systems remain dangereously exposed to attacks.

The hybrid framework outlined in the previous section aims precisely at supporting analysts to better understand cyber threats in combination with defense strategies and, eventually, to speed up the deployment of counter-measures. To this end, after identifying an adequate set of cyber operations to focus on[17], human behavioral data would need to be collected and analyzed. Subsequently, on the basis of ACT-R cognitive architecture augmented with cyber security ontologies, hybrid models of the identified cyber operations will be built. Our plan is to examine the cognitive mechanisms that govern the

[15] Note that the distinction between 'model' and 'agent' when dealing with cognitive architectures is a blurred one. In general, cognitive agents can be conceived as cognitive models that dynamically interacts in the environment.

[17] At the time of writing, a task group within the ARL program that sponsors this work is conducting a study on 60 typologies of cyber operations: the authors are planning to rely on the outcome of this study for future evaluation of models.

identification of the relevant attributes of cyber operations, and study how these attributes are "glued" together into "patterns" when cyber-attacks are recognized by analysts. In order to achieve the required degree of robustness and dependability, we envisage behavioral experiments and simulations at different levels of complexity and scale, as follows:

- **SDTE** – *Synthetic Defender Training Environment*: in this simulation environment an ACT-R agent is repeatedly interacting with a set of predefined attacker strategies. As a defender, the ACT-R agent learns to identify the relevant attributes and the relationships between them from repeated experiences with a strategy. Interacting with different strategies will familiarize the agent with a range of cyber-attacks. Here, the use of a predefined strategy provides control over the learning process. Each strategy represents a sequence of attacks that brings about a change in the environment (e.g., network state). The ACT-R agent monitors and identifies how different combinations of attributes can provide indication whether a cyber-attack occurred or not. Once a cyber-attack is recognized, the agent has to learn which countermeasures are able to mitigate the associated risk. When the training is completed, it is possible to evaluate the process of learning and examine the ability of the agent to detect and respond to novel variants of the training strategies.
- **SATE** – *Synthetic Attacker Training Environment*: in this environment an ACT-R agent interacts with predefined strategies. However, here the ACT-R agent serves as an attacker who learns to identify and exploit the vulnerabilities of the defender.

To validate the models for each of the above environments, we will use behavioral experiments where humans (basically students with expertise in cyber security) replace ACT-R agents in interacting with offensive and defensive strategies. Data collected at this stage will be used to calibrate and enhance the ecological validity of the models, both in terms of strategies used and baseline performance.

- **SME** – *Synthetic Match Environment*: The match environment aims to test the ability of a trained defender ACT-R agent to detect cyber-attacks generated by an attacker ACT-R agent and respond appropriately. This stage focuses on the dyadic interactions between the attacker and the defender, incorporating social aspects like reciprocity, evolvement of trust, deception, etc.

Cyber defense is usually performed by a group of analysts whose main task is to protect an organization's computer network [34]. Effective teamwork and collaboration are critical in such situation where misdiagnosis and wrong decisions can have severe consequences: among other things, this involves good team communication and collaboration, reliable information sharing and a strong transactive memory [35]. In this respect, the next phase extends the dyadic interactions to group interaction by having a team of ACT-R agents that serves as defenders, each agent with its own memory and decision making capabilities.

- **SGE** – *Synthetic Group Environment*: A set of two teams, each constituted by ACT-R agents face each other playing the role of assailant and defender. Defenders collaborate when detecting cyber-attacks and selecting how to respond to an attack. Each synthetic defender can have a unique set of past experiences that depend on its training and influence its future decisions. Agents can share information and consider the information provided by other agents. This can improve the ability of the group to detect attacks, though conflicting information and opinions can also disrupt the detection process. The within-group interactions are modeled through mechanisms of in-group power [36].

In order to run these incremental simulations, we will preliminary collect a large dataset of cyber attacks, to be split into training and test set (a common practice in state-of-the-art data mining and machine learning applications). In particular, we will focus on DDoS, information theft and spear phishing attacks. At the **SDTE** and **SATE** levels, the simulations aim at assessing the soundness of the cognitive mechanisms executed by the agent, serving also as a system debugging and evaluation of experimental settings. In **SME**, "mindreading" capabilities of the individual agents will be tested. The **SGE** scenario will scale up in complexity by shifting to a multi-agent framework, where a group of synthetic defenders will have to collaborate and learn intra-group cooperation, building mental representation of the opponent as a group (whose members act complementarily and collectively to harm the defending team).

In the delineated experimental setting we plan to expand our previous work on applying cognitive architectures to decision-making in non-zero sum games [37]: cooperative and conflicting phenomena have been comprehensively studied using game theory [38], in which multifaceted social dynamics are narrowed down to relatively simplified frameworks of strategic interaction. Valid models of real-world phenomena can provide better understanding of the socio-cognitive variables that influence strategic interaction: these models need to be consistent with the structural characteristics of games, and with the actual everyday situations at hand.

IV. Conclusion

This paper described a general framework to study decision-making of cyber analysts by leveraging computational agents in "gamified" attack scenarios. The novelty of our approach stems from grounding a computational model of cyber security on a cognitive architecture informed by the domain knowledge structures contained in ontologies. This hybrid framework is initially devised for training purposes as a resource for augmenting situational awareness of cyber analysts; nevertheless, it also embodies the capability of imitating human analysts by simulating their cognitive mechanisms and decision procedures at the computational level. In this regard, by fulfilling the requirements of a hybrid-modeling framework for cyber security as we proposed in this paper, in future work we are not only aiming to realize a decision support system for human operators but also to foster – in synergy with the military community – the implementation of autonomous computational agents, to be tested and eventually deployed as synthetic team members in cyber armed forces.

Our approach clearly envisions the creation of a potentially autonomous, dependable and self-sustainable cyber defense infrastructure for the U.S.: paraphrasing [1], “cybersecurity may seem a story of technology, but understanding and shaping human incentives and *cognitive dimensions*[18] matters the most in any effective defense”.

Bibliography

[1] P.W. Singer and A. Friedman, Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, 2014.

[2] A. Kott, "Towards Fundamental Science of Cyber Security," in Network Science and Cybersecurity, R. E. Pino, Ed. New York, 2014, vol. 55.

[3] M.R. Endsley, "Toward a Theory of Situation Awareness in Dynamic Systems," Human Factors, vol. 37, no. 1, pp. 32-64, 1995.

[4] K. B. De Greene, Sociotechnical systems: factors in analysis, design, and management.: Prentice-Hall, 1973.

[5] N. Guarino, E. Bottazzi, R. Ferrario, and G. Sartor, "Open Ontology-Driven Sociotechnical Systems: Transparency as a Key for Business Resiliency," in Information Systems: Crossroads for Organization, Management, Accounting and Engineering., 2012, pp. 535-542.

[6] F.B. Schneider, "Blueprint for a science of cybersecurity," The Next Wave, vol. 19, no. 2, 2012.

[7] John R. Anderson and Christian J Lebiere, The Atomic Components of Thought.: Erlbaum, 1998.

[8] N. Guarino, "Formal ontology and information systems," in Formal ontology and information systems (FOIS), Trento, 1998, pp. 3-15.

[9] The MITRE Corporation, "Science of Cyber-Security," The MITRE Corporation, McLean, VA, Technical 2010.

[10] D. A. Mundie and D. M. McIntire, "The MAL: A Malware Analysis Lexicon," CERT® Program - Carnegie Mellon University , Technical 2013.

[11] R. Dipert, "The Essential Features of an Ontology for Cyberwarfare," in Conflict and Cooperation in Cyberspace - The Challenge to National Security, Panayotis A Yannakogeorgos and A. B. Lowther, Eds.: Taylor & Francis, 2013, pp. 35-48.

[12] I. Kotenko, "Agent-Based modeling and simulation of cyber-warfare between malefactors and security agents in internet". In Proceedings of the 19th European Conference on Modeling and Simulation, 2005.

[13] A., Buchanan, L., Goodall, J. & Walczak, P. D’Amico. (2009) Mission impact of cyber events: Scenarios and ontology to express the relationship between cyber assets. [Online]. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA517410

[14] L., Chase, P., & Markeloff, R. Obrst, "Developing an ontology of the cyber security domain". In Proceedings of the Seventh International Conference on Semantic Technologies for Intelligence, Defense, and Security, 2012, pp. 49-56).

[15] J. R. Anderson & C. Lebiere, "The Newell Test for a theory of cognition," Behavioral and Brain Sciences, vol. 26, no. 5, pp. 587-637, 2003.

[16] A. Newell, Unified Theories of Cognition. Cambridge, Massachusetts: Harvard University Press, 1990.

[17] H. Simon, "Bounded Rationality and Organizational Learning," Organization Science, vol. 2, no. 1, pp. 125-134.

[18] M. Wooldridge, Reasoning about Rational Agents. Cambridge, MA, United States of America: The MIT Press, 2000.

[19] R. Sun, Cognition and Multi-agent Interaction, R. Sun, Ed.: Cambridge University Press, 2006.

[20] Paul Bello, "Cognitive Foundations for a Computational Theory of Mindreading," Advances in Cognitive Systems, vol. 1, pp. 59-72, 2012.

[21] J. R. Anderson, How Can the Human Mind Occur in the Physical Universe? New York: Oxford University Press.

[22] A. Stocco, C. Lebiere, & J. R. Anderson, "Conditional Routing of Information to the Cortex: A Model of the Basal Ganglia's Role in Cognitive Coordination," Psychological Review, vol. 117, no. 2, pp. 541-574, 2010.

[23] C. Lebiere. Constrained Functionality: Application of the ACT-R Cognitive Architecture to the AMBR Modeling Comparison. Mahwah, NJ: Erlbaum, 2005.

[24] A. Oltramari & C. Lebiere, "Knowledge in Action: Integrating Cognitive Architectures and Ontologies," in New Trends of Research in Ontologies and Lexical Resources, Alessandro, Vossen, Piek Oltramari, Lu Qin, and Ed. Hovy, Eds.: Springer, pp. 135-154.

[25] J. McCarthy, "Circumscription – A form of non-monotonic reasoning," Artificial Intelligence, vol. 13, no. 1-2, pp. 27-39, 1980.

[26] J. F. Sowa, Conceptual structures: Information processing in mind and machine. Reading, MA: Addison Wesley, 1984.

[27] D. B., Prakash, M., & Shepherd, M. Lenat, "CYC: Using Common Sense Knowledge to Overcome Brittleness and Knowledge Acquisition Bottlenecks," Artificial Intelligence, vol. 6, no. 4, pp. 65-85, 1985.

[18] The words in italics are ours.

[28] J. Ball, S. Rodgers, & K. Gluck, "Integrating ACT-R and Cyc in a large-scale model of language comprehension for use in intelligent agents," in Papers from the AAAI Workshop, Menlo Park, CA, pp. 19-25.

[29] B. J. Best, N. Gerhart, & C. Lebiere, "Extracting the Ontological Structure of OpenCyc for Reuse and Portability of Cognitive Models. ," in Proceedings of the 17th Conference on Behavioral Representation in Modeling and Simulation, 2010.

[30] B. Emond, "WN-LEXICAL: An ACT-R module built from the WordNet lexical database ," in Seventh International Conference on Cognitive Modeling , 2006, pp. 359-360.

[31] S. Douglas, J. Ball, & S. Rodgers, "Large declarative memories in ACT-R". In Proceedings of the 9th International Conference of Cognitive Modeling, Manchester, UK.

[32] H. Stuckenschmidt, C. Parent, and S. Spaccapietra, "Modular Ontologies - Concepts, Theories and Techniques for Knowledge Modularization," , 2009.

[33] B. M. Bowen, D. Ramaswamy, & S. Stolfo, "Measuring the Human Factor of Cyber Security," Homeland Security Affairs, vol. 5, no. 2, 2012.

[34] A., Whitley, K. D'Amico, "The real work of computer network defense analysts," in Workshop on Visualization for Computer Security, 2008, pp. 19-37.

[35] N.J., Gorman, J.C., Winner, & J. Cooke, "Team cognition," in Handbook of Applied Cognition., 2007, pp. 239-268.

[36] I. Juvina, C. Lebiere, J.M. Martin, & C. Gonzalez, "Intergroup Prisoner’s Dilemma with Intragroup Power Dynamics," Games, vol. 2, pp. 21-51, 2011.

[37] A. Oltramari, C. Lebiere, N. Ben-Asher, & C. Gonzalez, "Strategic Dynamics Under Alternative Information Conditions," in Proceedings of ICCM 2013 (International Conference of Cognitive Modeling), Ottawa, 2013.

[38] A. Rapoport, M. J. Guyer, and D. G. Gordon, The 2 x 2 games. Ann Arbor, MI: University of Michigan Press, 1976.

[39] A. Oltramari, P. Vossen, L. Qin, E. Hovy. New Trends of Research in Ontologies and Lexical Resources: Springer-Verlag, 2013.