Towards a Human Factors Ontology for Cyber Security

Alessandro Oltramari
Carnegie Mellon University
Pittsburgh, USA

Diane Henshel & Mariana Cains
Indiana University
Bloomington, USA

Blaine Hoffman
Army Research Laboratory
Aberdeen, USA

***Abstract*— Traditional cybersecurity risk assessment is reactive and based on business risk assessment approach. The 2014 NIST Cybersecurity Framework provides businesses with an organizational tool to catalog cybersecurity efforts and areas that need additional support. As part of an on-going effort to develop a holistic, predictive cyber security risk assessment model, the characterization of human factors, which includes human behavior, is needed to understand how the actions of users, defenders (IT personnel), and attackers affect cybersecurity risk. Trust has been found to be a crucial element affecting an individual's role within a cyber system. The use of trust as a human factor in holistic cybersecurity risk assessment relies on an understanding how differing mental models, risk postures, and social biases impact the level trust given to an individual and the biases affecting the ability to give said trust. The Human Factors Ontology illustrates the individual characteristics, situational characteristics, and relationships that influence the trust *given* to an individual. Furthering the incorporation of ontologies into the science of cybersecurity will help decision-makers build the foundation needed for predictive and quantitative risk assessments.**

Keywords*— *cyber security, risk assessment, human factors, cyber operations

I. INTRODUCTION

A. The Holistic Cybersecurity Risk Framework

The science of cybersecurity risk assessment has been reactive, narrow in focus, and based on a business risk assessment approach. More recently, the National Institute of Science and Technology (NIST) responded to the 2013 "Improving Critical Infrastructure Cybersecurity" Executive Order with the development of the 2014 NIST Cybersecurity Framework [1,2]. The NIST framework aims to provide organizations and businesses with best risk management practices that can be implemented to improve the security and resilience of critical infrastructure. NIST recognizes that risk management is an iterative process of risk identification, risk assessment, and risk mitigation. While the NIST framework provides businesses and organizations with a neatly organized account of their cybersecurity efforts, the framework fails to capture the concept that humans are an inherent risk to any system in which they directly or indirectly participate.

To go beyond the current risk framework promulgated by NIST [1,2], risk assessment needs to be more holistic. In order to enable cybersecurity risk assessment to become more predictive, the process and models need to incorporate humans and risk factors together in a single model and use metrics that go beyond the direct assessment of classical vulnerabilities (confidentiality, integrity, accessibility, or CIA).

First, when considering CIA, the actual measurement or evaluation of these vulnerabilities will depend on the situation being modeled. Situations requiring cybersecurity risk assessment can include baseline assessments of network protection, but must also include situations in which the network is being used actively. The actual metrics for, say, protection of an SQL database containing personal information (social security numbers, for example) may be very different than the metrics needed to be assessed when evaluating risk related to a field operation using radios, walkie talkies or cell phones to convey information.

Second, other variables beyond CIA may be the relevant risk variables that need to be analyzed in a risk model. Take, for example, a situation in which information being used, generated in, or relayed by one network needs to be received in a specific time window either for another operation to begin or so that the information can be used maybe by the human who will receive the information. Within a military or other time critical context, the evaluation goes beyond time to access information; it must include time to act on the accessed information and can include time for completion of actions within a critical time window. In this example, time to completion of a task is the critical metric that must be tracked, and so must be incorporated into the risk model.

Third, humans are a part of virtually all networks, whether as users, defenders (and IT personnel) or attackers. All humans can introduce risk into the network, not just attackers, a consideration acknowledged when users are asked how they use the system (and system components) as part of the NIST risk management and risk assessment process. Defenders or IT personnel can also increase cyber risk if they are, for example, less skilled, or tired, or inside threats. Humans can also reduce risk in a cybersecurity system. Defenders put in place baseline protections, and then track attacks on the system to assess whether the protections have been breached and what needs to be done to increase system hardening (protections), counteract

malware that may have introduced access to the system (or otherwise compromised the system and system assets), and repair damage to the system. Users can decrease risk by being aware of (and not being hooked by) spam or phishing efforts, ensuring their personal system assets are appropriately protected, and by not downloading infected files or accessing malware-linked websites. Therefore, human-dependent metrics must be included in a holistic risk analysis of cyber security.

A fully predictive cyber security risk assessment model will take into account humans as risk factors, and as risk mitigators, and will enable the incorporation of metrics that go beyond the classic CIA vulnerabilities. In order to develop such a model, we have been characterizing the universe of cybersecurity by framing the characteristics, attributes and, ultimately, metrics that can be use to describe the risks associated with any cyber network. The framework has multiple pieces, and metrics that are assessed at different levels.

Three main parts to the Cybersecurity Risk Framework identifies system level metrics, policy related metrics, and asset related metrics. System level metrics are evaluated at the full system level, such as probability of completion of a mission or a system level task. Policy level metrics evaluate the risks associated with the policies that govern the network and network assets. Asset level metrics are evaluated at the asset level, such as metrics to assess risks associated with specific machines, a virtual network, or an operating system. One piece of the asset level framework characterizes the Human Factors that introduce or mitigate risk in a cyber network [3], which is then being incorporated into an ontology. One goal of this framework and ontology is to identify the factors that contribute to a key aspect of human-related cyber risk, trust.

B. An ontological approach to risk modeling

A recent report on quantification of cyber threats highlights the intrinsic complexity of the cyber domain [4]: in this document experts pinpoint the bottleneck of cyber threat assessment on the lack of "standardization and benchmarking of input variables", as conversely accomplished – they add – "by the car insurance industry" (p.16). But if agreeing on the meaning of notions like 'age' and 'gender' of drivers, 'weight' and 'year of built' of cars, 'claims history', etc. seems mostly straightforward, specifying the semantics of concepts like 'system vulnerability', 'software usability', 'trust', 'password strength', etc. requires advanced technical knowledge, fine-grained modeling primitives, and non-trivial metrics.

Little effort has been put into this standardization process. For instance, Fenz and Ekelhart propose an ontology based on four parts, i.e. security and dependability taxonomy, the underlying risk analysis methodology, the concepts of the IT infrastructure domain and a simulation enabling enterprises to analyze various policy scenarios [5]. Notwithstanding the comprehensive investigation, the work presented in [5] is affected by an underspecified notion of risk, conceived as "the probability that a successful attack occurs", which clearly fails to account for the mutual dependence between profiles of attackers, system vulnerabilities, level of expertise of the defenders, monetization of information loss resulting from data breaches, etc. In general, a too-coarse representation of risk is a pervasive problem in the state of the art on ontologies of cyber security: it's the case of [6] and [7] where the in-depth conceptual distinctions adopted to model cyber attacks are not matched by a corresponding level of detail in defining cyber threats and risk assessment procedures.

The most popular modeling solution in risk-related ontology research seems to be the reification of risk-assessment and threat-quantification into the process of 'rating', whose attributes are expressed either qualitatively (e.g., by means of high, medium and low dimensions in the Likert scale) or quantitatively (measuring the probability of a risk). Note that in ontology modeling, reification of properties is commonly adopted as a method to bypass language expressivity limits: in RDF, for instance, a relation with arity $n > 2$ can be represented with a statement about those n entities. Thus, for instance, we could represent the fact that a set of n cyber vulnerabilities exposes a system to a certain risk factor, by asserting a risk-rating statement about those known n vulnerabilities [8]. An alternative approach comes from Enterprise Risk Management (ERM), an area that concerns the identification, assessment and mitigation of operational risk: for instance, Lykourentzou and colleagues focus on seven subclasses of events, i.e. 'Failure', 'Infrastructure disruption', 'Occupational incident', 'Fraud', 'Disaster', 'Attack', binding each of these event types to a wide spectrum of 'Root causes' and 'Treatment plans' to address risk factors [9]. ERM's approaches can be effective not only to identify risk-related event patterns, but also to elicit the behavioral patterns in the adoption of risk management practices. In this context, ontologies supply an axiomatic infrastructure to mental models of risk-related patterns.

The rest of the paper is organized as follows: Section II makes the case for a holistic approach to risk in cyber security, introducing the role of trust ontologies; Section III focuses on the Human Factors Ontology (HUFO); finally, Section IV draws preliminary conclusions and sets an agenda for future research.

II. RELATED WORK

A. Ontologies of cyber security

The U.S faces cyber attacks by rogue states and terrorist organizations on a daily basis. While greatly increased use of information systems has contributed enormously to economic growth, it has also made the U.S. vulnerable to a variety of cyber threats that are difficult to contrast and prevent. There are numerous factors that make cyber defense, and cyber security in general, especially problematic. The kinds of threats are diverse and span a wide spectrum of private and public interests: destruction or

theft of data, interference with computer networks and information systems, disruption of the power grid and telecommunications, denial of services, etc. The legal and ethical status of cyber attacks or counterattacks by states are also unclear, at least when deaths or permanent destruction of physical objects does not result. It is still an open question what U.S. policy is or should be, and how cyber threats are analogous to traditional threats and policies—for example whether "first use" deterrence, and in-kind responses apply, and whether a policy of pure cyber defense does not put the far greater burden on attacked rather than attacking nations [10].

As these arguments suggest, untangling the complexity of cyber security does not solely depend on pinning down the computational elements into play, but demands a thorough analysis of the human factors involved. In this regard, cyber security must be studied in the context of "sociotechnical systems" [11], where the interaction between people and technology in workplace is central. Ontology analysis has recently proved to be an effective tool for investigating the defining aspects of that interaction [12].

Informed decisions emerge when a cyber analyst projects her observations into a broad context that factors in threat and attack types, space of defensive maneuvers, system vulnerabilities, risk assessment and mitigation under time constraints. Obrst and colleagues [13] provide the most systematic description of a wide-ranging ontology of cyber security, but only a small portion of this large-scale project is devoted to the human component. Various agencies and corporations (NIST [1,2], MITRE [14], and Verizon [15]) have formulated enumerations of types of malware, vulnerabilities, and exploitations: MITRE, which has been very active in this field, maintains two dictionaries, namely CVE (Common Vulnerabilities and Exposure[1]) and CWE (Common Weakness Enumeration[2]) and a classification of attack patterns (CAPEC - Common Attack Pattern Enumeration and Classification [3]). Regardless of the important issues covered by these initiatives, they have two major problems: 1) machine-readability is not supported, making them ineffectual as computational models of cyber security; 2) the human component is mostly overlooked, making the resulting models partial in scope.

In order to overcome these problems, in the context of the Cyber Collaborative Research Alliance we are developing CRATELO, a three-level modular ontology of cyber security. In the next section we are going to describe the general features of CRATELO, focusing on the Human Factors Trust Ontology module (HUFO).

B. *Trust ontologies*

Ontology-based models of trust have been studied in various domains [16]. In [17], the authors propose an intelligent and dynamic Service Level Agreement (SLA) based on a probabilistic ontology that detects warnings in a cloud computing environment. A generic service-oriented framework of trust ontologies is described in [18]. A trust ontology aiming at improving the semantic specification of trust networks in the context of social institutions and ecosystems is discussed in [19]. In [20], the author focuses on six general areas to derive trust for a system, namely user, hardware, software, network, machines, and the applications, mapping trust associated with each area to specific attributes. An ontology-based approach to integrate semantic web based trust networks with provenance information to evaluate and filter a set of assertions is presented in [21]. In [22], a reference ontology to develop privacy preserving negotiation systems is delineated.

III. The Human Factors Trust Ontology

A. *The Human Factors Trust Ontology*

Adopting a standard understanding and definition of terms and concepts is a foundational requirement for good cyber security practice, owing to the nature of the space and the need for rapid, efficient decision-making. Cyber security is an adversarial space, where defenders must project possibilities and be ahead of their opposition in order to be successful. Enacting strategies favors selecting a suitable course of action in minimal time over exhaustively searching [23,24]. Furthermore, the data available is not always straightforward, requiring collection and parsing in order to construct an understanding of the situation(s) at hand. Numerous sources of relevant information are often applicable, including network monitoring tools, logs, system statuses, and hardware monitors. Analysts are situated at the center of a large-scale data fusion process, identifying and defining information through patterns and relationships to perceive the ground truth of the cyber systems and assets they are defending and monitoring [25,26,27]. Once collected, the information must be appropriately combined, categorized, and communicated in order to provide a useful and accurate picture of the world on which future strategies can be based. Simply stated, cyber defense is heavily focused on the human analysts and agents involved in a data fusion and situation awareness process.

Through processing of data, defenders can draw conclusions and decide how to respond to evolving scenarios. Implicit within the workload is a desire and preference for information that can be *trusted*, a concept that requires a lot of unpacking to properly understand. In fact, conceptualizing trust in order to evaluate its role and presence within a system is itself a difficult problem; there are literally hundreds of definitions of trust covering interpersonal trust, trust in automation (system trust), and human-machine interaction [28]. However, that variety only strengthens the argument for constructing and supporting an ontological representation of cyber security. The core similarities of cyber security and the tasks involved are essentially the same [29], which also supports the creation

[1] https://cve.mitre.org/
[2] https://cwe.mitre.org/
[3] https://capec.mitre.org/

of a standard ontology. Thus we should be able to describe the human factors that influence trust in a way that can be applicable regardless of the specific cyber environment or organization involved and that will help explicate the role of trust in risk assessment and evaluation.

Assessing cyber security risks is a multi-component, multi-tiered problem that involves hardware, software, environmental, and human factors. Effective and successful efforts must consider impacts beyond the computer assets and network, taking a more holistic approach that considers the users, defenders, and attackers involved [3]. Exploring the differences among human roles and human factors includes exploring how trust permeates risk assessment, such as trust in information, in people, or in security policies. Information is not uniformly trusted and incorporated into situation awareness and defender responses automatically, but it is built over time as those involved develop relationships, progress through training, and gain experience [30]. Individuals grow trust in one another through working together, and people gain trust in systems as they continue to demonstrate consistent behavior. Previous definitions of trust aggregate characteristics into a whole sum, including concepts such as competence, benevolence, integrity, predictability, attitude, intention, behavior, reliability, dependability, and faith [31] [32] [20]. The human factors trust ontology aims to map these concepts into understood and explicit relationships that tie together risk assessment across the human and human-system interactions within the cyber security space.

As part of an ongoing development of holistic cyber security risk assessment, we have been creating a framework that enables predictive and proactive defenses [33,34,35]. A critical component of this process has been the characterization of human factors, such as trust, and mapping the relevant risk attributes to the risk spaces involved in cyber security. Overall, this is a process of creating, enumerating, and solidifying risk characteristics and factors, and in many cases refining them and relating them to the human factors. The latter are broken into three main categories of attacker, defender, and user with a shared core of spaces (their *behavioral characteristics*, *knowledge and skill characteristics*, *situational characteristics*, and traits that influence behavior) that create the definition of each [3]. The framework (see Figure 1) can be navigated from top to bottom, the lower tiers breaking out into the more specific metrics and concepts that, collectively, describe and detail these core spaces, which allows for the mapping of attributes to measures and data that can be used to create risk evaluations.

Situational Characteristics focus on where in the system/network the individual is positioned and the level of insider access they possess, denoting when this access is authorized or unauthorized. A person's situational characteristics also influence the knowledge they can access and may influence the attention they bring to a situation. For example, a user who is an executive of a company may have significant authorized access to assets but lack the same level of attentiveness to security concerns and information that a network analyst possesses. *Knowledge and skill characteristics* call to attention the experience, expertise, and situational awareness capabilities of the individual, including demographics such as years working in a position and training as well as their proficiency with relevant tools and techniques. *Behavioral Characteristics* are split into spaces such as motivation, rationality, malevolence vs. benevolence, and integrity. For example, a defender who is rational, benevolent, and has a record of following through with work and being accountable for his or her responsibilities will likely exhibit persistence in defending assets and building appropriate situational awareness. We have expanded the framework to include traits that influence the behavioral characteristics, including ideology, ethical attributes, risk averseness, and personality traits. Each of these may scale the behavioral characteristics in some fashion or serve as the driving force behind a person's integrity, benevolence, or rational approach to cyber security situations. Collectively, these characteristics and traits impact the individual's interactions with mission assets and play a role in determining risk. For example, defender with poor motivation and integrity, insufficient knowledge, and appropriate insider access can present a higher risk, whereas an attacker with high motivation and knowledge despite limited insider access also poses higher risk.

Trust also comes through across these spaces. The predictability and reliability of an individual generates a sense of trust in his or her actions and creates a reputation for that individual. The expertise and knowledge possessed can instill a faith or confidence in the work a defender will do, and users with sufficient integrity will be trusted to follow security policy and not act maliciously within the network. In effect, the human factors of trust directly associates with risk evaluation of cyber situations, and we can explore the relationships across the human factors of cyber security to discover *where* risk manifests and how trust is generated and influenced. Integrating the human factors framework into a cyber security ontology provides a logical means to explicate relationships both obvious and unintuitive, follow their connections, and evaluate trust's presence and impact on the risk present within a given network.

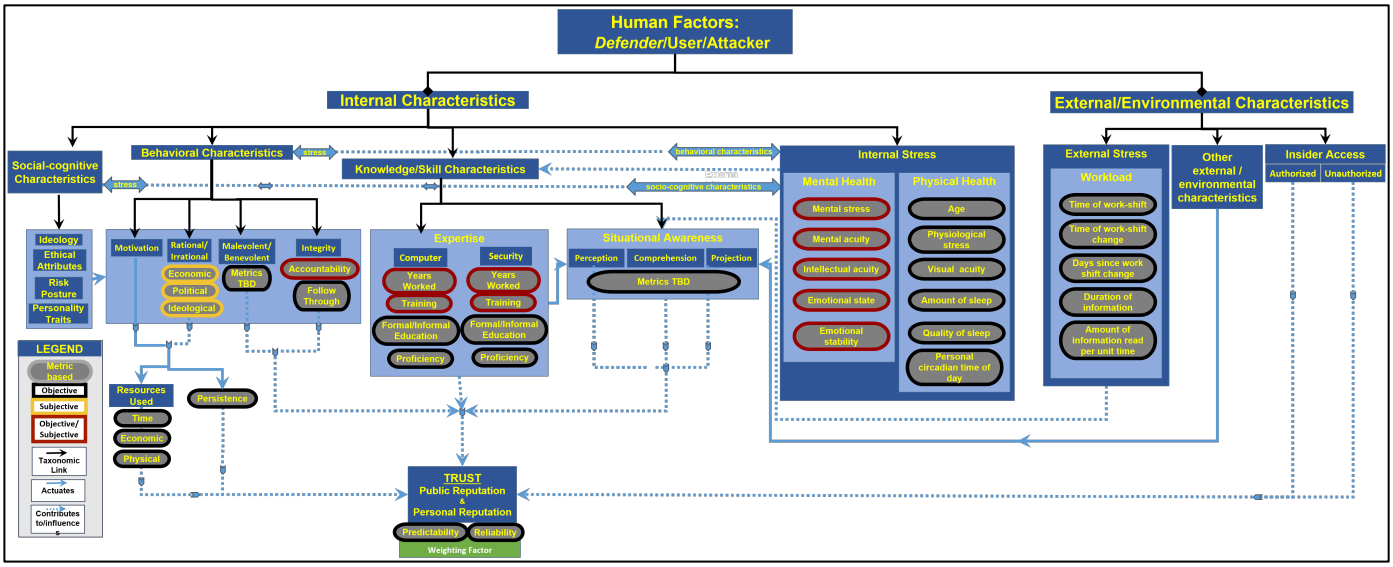

Figure 1 – Trust Framework of Human Factors in Cyber Security.

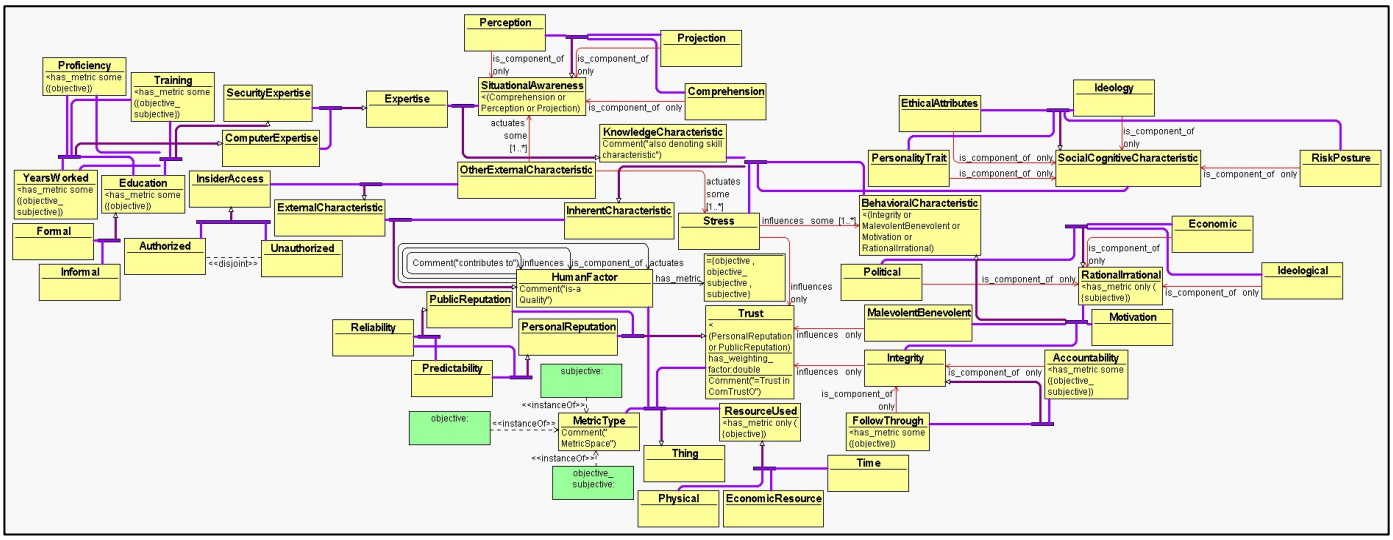

Figure 2 – A visualization of HUFO.

B. *HUFO and Trust: an overview*

HUFO (see Figure 2 above) is part of CRATELO [36], a suite of integrated ontologies of cyber security, designed on the basis of DOLCE top level [37], extended with a security-related middle ontology. These top, middle and domain level ontologies currently add up to 330 classes, connected by 162 relationships (132 object properties and 30 datatype properties) and encoded in OWL-DL. The logical expressivity of CRATELO is SRIQ, a decidable extension of the description logic SHIN (for more details see [38]).

The relation holding between the human factors and the metrics used to assess them is captured by the semantic characterization of 'qualities' and 'quality spaces', which has been originally formulated by [39] and subsequently formalized in DOLCE ontology [37]. Intuitively, a quality corresponds to an individual attribute of a specific entity, as 'predictability' or 'reliability' can be considered attributes of 'trust'; a quality space is the abstract representation of an attribute's semantics, e.g. a boolean space that denotes the 'reliable/unreliable' dichotomy. An important topological property of quality spaces is that their dimensional structure can vary. For instance, the 'reliability space' can be more complex than a bidimensional configuration: in particular, this is the case when reliability is conceptualized as probabilistic distribution between maximum reliability (100%) and complete unrealibility (0%). The atomic parts of a quality space, which collectively denote the range of

values used to specify an attribute's semantics, are called 'quality regions'. Note that quality regions of a linear space reduce to points.

As mentioned above, 'predictability' and 'reliability' are conceived in HUFO as components of 'trust', a complex factor that is influenced by inherent and external characteristics, in combination with measures of human performance in a given situation. Hence, trust is not only associated to human characteristics, but emerges as an essential aspect of sociotechnical systems: the hybrid nature of trust is particularly evident in the cyber security domain, where a trustworthy interaction with computer network systems is the '*conditio sine qua non*' for a defender/attacker to accomplish a mission in cyberspace[4].

Figure 2 represents an overview of HUFO generated using OWLGrEd[5]: the purple links represent subsumption relationship between classes, whereas the dotted arrows indicate either the 'component-of' or the 'influenced-by' property (textual labels in the figure disambiguate the equivalent graphical notations); classes are depicted as yellow boxes, instances as green boxes. The object property 'component of', holding between attributes and qualities, is modeled as a generic 'part-of' relation [40], whereas the 'influenced-by' relation reflects DOLCE's characterization of general dependence, to highlight the strong connection between the assessment (existence) of proper internal and external characteristics and the computation of the derived trust level. Note that *objective*, *subjective*, and *objective-subjective* designate the sorts of metrics that can be predicated to each human factor (represented in Figure 1). An *objective* metric represents characteristics that are based in quantifiable and unbiased facts such as highest level of education completed. A *subjective* metric represents characteristics based in human decision-making and assumptions such as political rationality. An *objective-subjective* metric represents characteristics that are based in fact while also influenced by human decision-making such as emotional state. These metrics types are modeled as instances in HUFO: the use of meta-classes would have required OWL-Full, which is the undecidable fragment of OWL, and therefore unfit for reasoning. Consequently, we opted for modeling the three types of metrics as a collection of individual instances (range) associated to human factors classes (domain) through the object property 'has metric'.

IV. Conclusions And Future Work

In this paper we examined the effort of building a human factors ontology (HUFO) as part of a broader ontology of cyber security (CRATELO). In particular, we focused on the notion of trust, showing its ties with the inherent and external characteristics of humans interacting with computer networks. In the long term, we envision to apply HUFO in support of risk assessment and risk prioritazion in cyber operations.

The semantic model outlined in this paper is only a first, preliminary step in the process of porting a larger model of the cyber security ecosystem into a computational ontology. The holistic nature of our approach makes the task exceptionally challenging and, to the best of our knowledge, uniquely systematic in cyber security research. Despite the complex problems we are trying to solve, we're also convinced that, in the forward-looking vision of the ARL Cyber Security Collaborative Research Alliance, our approach sets a realistic and crucial milestone toward the foundation of a science of cyber security.

[4] This is the case, for instance, when a cyber analyst uses a network-based intrusion prevention system (or NIPS) to monitor and protect a given network environment from cyber attacks.

[5] http://owlgred.lumii.lv/

Acknowledgments

This 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.

Bibliography

[1] Technology, National Institute of Standards and, "Framework for Improving Critical Infrastructure Cybersecurity", Dept. of Commerce, NIST, Ver. 1 2014.

[2] Technology, National Institute of Standards and, "Guide for Conducting Risk Assessments", US Dept. of Commerce, NIST, Special Publication 800-30 2012.

[3] M., Hoffman, B., Kelley, T., and Henshel, D. Cains, "Trust as a Human Factor in Holistic Cyber Security Risk Assessment", in *6th International Conference on Applied Human Factors and Ergonomics (AHFE)*, 2015.

[4] World Economic, Deloitte Forum. (2015) weforum.org.[Online]. http://www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf

[5] S., Ekelhart, A. Fenz, "Formalizing Information Security Knowledg" in *the International Symposium on Information, Computer, and Communications Security (ASIACCS '09)*, New York, pp. 183-194.

[6] 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.

[7] A., Lenne, D., Debray, B. Assali, "Ontology Development for Industrial Risk Analysis", in *IEEE*

International Conference on Information & Communication Technologies: from Theory to Applications., Damascus, 2008.

[8] B. McBride, "Jena: Implementing the RDF Model and Syntax Specification", in *SemWeb*, Chicago, 2001.

[9] I. , Papadaki, K. Lykourentzou and A., Djaghloul, Y., Latour, T., Charalabis, I., Kapetanios, E. Kalliakmanis, "Ontology-based Operational Risk Management", in *13th Conference on Commerce and Enterprise Computing (CEC).*

[10] R. Dipert, "The Essential Features of an Ontology for Cyber Warfare", in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, A. Lowther and P. Yannakogeorgos, Eds.: Air Force Press (by Taylor & Francis), 2013.

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

[12] 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.

[13] L. Obrst, P. Chase, and R. Markeloff, "Developing an Ontology of the Cyber Security Domain", in *STIDS 2012*, Fairfax, VA, 2012.

[14] MITRE. Common Malware Enumeration list. [Online]. http://cme.mitre.org/data/list.html

[15] Verizon. (2015) Data Breach Investigation Report. [Online]. http://www.verizonenterprise.com/DBIR/2015/?utm_source=pr&utm_medium=pr&utm_campaign=dbir2015

[16] L. Viljanen, "Towards an Ontology of Trust", in *Trust, Privacy, and Security in Digital Business*. Berlin-Heidelberg: Springer-Verlag, 2005, vol. 3592, pp. 175–184.

[17] O, Hafid, A. and M.A. Serhani Jules, "Bayesian network, and probabilistic ontology driven trust model for sla management of cloud services", in *3rd IEEE International Conference on Cloud Networking*, 2014.

[18] E., Dillon, T. S., Hussain, F. Chang, "Trust ontologies for e-service environments", *International Journal of Intelligent Systems*, vol. 22, pp. 519-545, 2007.

[19] N. and Matskin, M. I, pages Papeete, France, 4-9 Nov. 2007. Dokoohaki, "Structural determination of ontology-driven trust networks in semantic social institutions and ecosystems", in *International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies*, 2007, pp. 263–268.

[20] E. Blasch, "Trust metrics in information fusion", in *SPIE 9119 - Machine Intelligence and Bio-inspired Computation: Theory and Applications VIII,* 2014.

[21] J., Parsia, B. Goldbeck, "Trust network-based filtering of aggregated claims", *International Journal of Metadata, Semantics and Ontologies* , vol. 1, no. 1, pp. 58-65, 2006.

[22] A.C., Bertino, E. Ferrari Squicciarini, "Achieving privacy in trust negotiations with an ontology based approach", *IEEE Transactions on Dependable and Secure Computing*, vol. 3, no. 1, pp. 13-30, Jan-Mar 2006.

[23] G. A. Klein, "Recognition-primed-decision". In W.B. Rouse (Ed.), Advances of Machine-System Reserch. Greenwich, CT: JAI Press, 1989, vol. 5, pp. 47-92.

[24] G.A., Calderwood, R., & Clinton-Cirocco, A. Klein, "Rapid decision making on the fire ground", in *Human Factors Society 30th Annual Meeting,* pp. 576-580.

[25] E. Blasch, "Introduction to Level 5 Fusion: the Role of the User", in *Handbook of Multisensor Data Fusion*, D. Hall, and J. Llinas. M. E. Liggins, Ed.: CRC Press, 2008, pp. 503-535, .

[26] N. A. Giacobe, "Application of the JDL Data Fusion Process Model for Cyber Security" , 2010.

[27] E.P., Breton, R., and Valin, P. Blasch, "User Information Fusion Decision Making Analysis with the C-OODA Model", in *14th International Conference on Information Fusion*, 2011, pp. 2082-2089.

[28] D. R. Billings, K. E. Schaefer, N. Llorens, and P. A. Hancock, "What Is Trust? Defining the Construct Across Domains", in *American Psychological Association Conference (Division 21)*, Orlando, FL, 2012.

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

[30] A. Jøsang, J. Dezert, P.C.G. Costa, and A.-L. Jousselme. E. Blasch, "URREF self-confidence in information fusion trust", in *In 17th International Conference on Information Fusion (FUSION'2014)*, Salamanca, Spain, 2014, pp. 1-8, .

[31] D.H., and Chervany, N.L. McKnight, "Trust in Cyber-societies: Integrating the Human and Artificial Perspectives", in *Lecture Notes in Computer Science*, M. Singh, Y.-H. Tan R. Falcone, Ed. New York: Springer, 2001, pp. 27-54, .

[32] B., Moray, N. Muir, "Trust in automation: Part II. Experimental studies of trust and human Intervention in a process control simulation", *Ergonomics*, vol. 39, no. 3, pp. 429-460, 1996.

[33] D.S. Henshel, A. Alexeev, P. Rajivan M.G. Cains, "Human Actors' Roles in Holistic Cyber Security Risk Assessment", in *World Congress on Risk* , Singapore, 2015.

[34] A. Alexeev, M.G. Cains, P. Rajivan. D.S. Henshel, "Risk Parameters in Holistic Cyber Security Risk Assessment", in *World Congress on Risk* , Singapore, 2015.

[35] D. S. Henshel M.G. Cains, "Holistic Cyber Security Risk Assessment", in *Society for Risk Analysis, Denver*, Denver (CO), 2014.

[36] Oltramari, A., Cranor, L.F, Walls, R., McDaniel, P., "Building an Ontology of Cyber Security", in *STIDS 2014 (9th International Conference on Semantic Technology for Intelligence, Defense, and Security*, 2014.

[37] Masolo, C., Borgo, S., Gangemi, A., Guarino, N., Oltramari, A., Schneider, L., "The WonderWeb Library of Foundational Ontologies and the DOLCE ontology," Laboratory For Applied Ontology, ISTC-CNR, Technical Report 2002.

[38] Kutz, O., Lücke,D., and Mossakowski, T., "Heterogeneously Structured Ontologies—Integration, Connection, and Refinement", in *Knowledge Representation Ontology. Workshop*, 2008, pp. 41-50.

[39] Gärdenfors, P. "Conceptual Spaces: The Geometry of Thought", p. 2004.

[40] Simons, P. "Parts: a study on ontology" , 1987.