Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation

Mariana G. Cains, Liberty Flora, Danica Taber, Zoe King, and Diane S. Henshel

It is important to have and use standardized terminology and develop a comprehensive common understanding of what is meant by cyber security and cyber security risk given the multidisciplinary nature of cyber security and the pervasiveness of cyber security concerns throughout society. Using expert elicitation methods, collaborating cyber researchers from multiple disciplines and two sectors (academia, government–military) were individually interviewed and asked to define cyber security and cyber security risk. Data-driven thematic analysis was used to identify the most salient themes within each definition, sector, and cyber expert group as a whole with results compared to current standards definitions. Network analysis was employed to visualize the interconnection of salient themes within and across sectors and disciplines. When examined as a whole group, “context-driven,” “resilient system functionality,” and “maintenance of CIA (confidentiality, integrity, availability)” were the most salient themes and influential network nodes for the definition of cyber security, while “impacts of CIA vulnerabilities,” “probabilities of outcomes,” and “context-driven” were the most salient themes for cyber security risk. We used this expert elicitation process to develop comprehensive definitions of cyber security (cybersecurity) and cyber security risk that encompass the contextual frameworks of all the disciplines represented in the collaboration and explicitly incorporates human factors as significant cyber security risk factors.

KEY WORDS: Cross-disciplinary; human factors; network analysis; system; thematic analysis

1. INTRODUCTION

Cyber security risk models have traditionally focused on machine-based threat, deterrence, mitigation, and recovery. However, human factors contribute to many cyber risks via the creation and deployment of malicious-acting software, increased attacker use of social engineering, and the lack of protective behaviors, such as password encryption or the use of antivirus software. Humans play a role in the creation, exacerbation, propagation, and mitigation of cyber security risk as users, defenders, and attackers (Henshel, Cains, Hoffman, & Kelley, 2015; Henshel, Sample, Cains, & Hoffman, 2016; King et al., 2018). In recent years, researchers have begun to include human factors such as maliciousness and expertise in cyber security risk models to provide additional insight into the human behaviors that induce or mitigate cyber security breaches (Bowen, Devarajan, & Stolfo, 2011; Cherdantseva et al., 2016; Mittu & Lawless, 2015; Oltramari, Henshel, Cains, & Hoffman, 2015). This human-inclusive approach challenges the current machine-focused definition of cyber security as it incorporates fields such as sociology, psychology, risk and decision science, and many others (Cebula, Popeck, & Young, 2014; NIST, 2018; Oltramari & Kott, 2018). However, the increasingly interdisciplinary nature of cyber security...
research also complicates discussion between stakeholders from diverse disciplines as they define key concepts such as cyber security and cyber security risk differently.

This article examines the definitions of cyber security and cyber security risk, as defined by principal investigators, researchers, and practitioners who are a part of the Army Research Laboratory funded Cyber Security Collaborative Research Alliance (CSec CRA). The CSec CRA was first formed in 2013 with a mission to:

…the development of a fundamental understanding of cyber phenomena, including aspects of human attackers, cyber defenders, and end users, so that fundamental laws, theories, and theoretically grounded and empirically validated models can be applied to a broad range of Army domains, applications, and environments. ARL [Army Research Laboratory] envisions the alliance bringing together government, industry, and academia through this basic research program to develop and advance the state of the art of Cyber Security. (ARL, 2013)

The different lenses through which practitioners, researchers, and users interact with the notions of cyber security and cyber security risk influence their perception and conceptualization of either term (Craigen, Diakun-Thibault, & Purse, 2014). Therefore, as experts from the diverse fields of information science, computer science, risk and decision science, organizational management, and behavioral psychology converge to advance the science of cyber security in the face of ever advanced and persistent threats, it is crucial for all parties to have a shared and cohesive definition of cyber security and cyber security risk.

The background section of this article demonstrates risk communication issues that result from the varying definitions and perceptions surrounding cyber security and cyber security risk. The background section also analyzes similar risk communication and risk perception issues in other interdisciplinary fields to understand how these problems have been identified and addressed. The methods and analysis sections detail the qualitative processes used to identify salient themes from individual cyber experts’ definitions of cyber security and cyber security risk gathered from semistructured interviews with both academic and U.S. Army Research Laboratory (ARL) participants in the CSec CRA. This article includes five analyses: expert elicitation, thematic analysis, network analysis, a comparative content analysis between these expert elicitation definitions and prior analysis of cyber language in formal cyber ontologies, and a comparison of the derived expert elicitation definition to definitions from national and international standards and best practices. Each analysis presents both visual and tabular data representations. The final discussion section compares the results of these analyses and highlights the challenges associated with expert elicitation and thematic analysis and concludes with the implications of this research.

Using both sectoral and disciplinary subgroupings, the thematic analysis of the expert elicitation-based cyber security and cyber security risk definitions indicated that while there were clear inconsistencies between the subgroupings, the main commonality was the need to maintain confidentiality, integrity, and availability (CIA; cyber security) and reduce CIA vulnerabilities (cyber security risk). Both academia and ARL interviewees expressed that perfect cyber security is unattainable and that cyber security risk is exacerbated by a lack of understanding of human factors in cyber security. None of the reviewed cyber security risk definitions from standard developing organizations included either human factors or the element of time control, the latter of which is becoming more critical as cyber systems control more and more time-dependent societal functions and processes. In contrast, only the Merriam-Webster definition for “security risk” acknowledges the human element.

2. BACKGROUND

2.1. Current Definitions in Cyber Security Research

The Merriam-Webster dictionary defines cyber security as “measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack” (Merriam-Webster, 2020). The International Telecommunications Union (ITU) defines cyber security as “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets” within the cyber security focus of confidentiality, availability, and integrity (CIA) objectives (ITU, 2008). The department of Homeland Security’s National Initiative for Cybersecurity Careers and Studies glossary defines cybersecurity as an activity or process that protects and/or defends information and systems against damage, unauthorized

¹Term is spelled as defined in the original source.
use or modification, or exploitation (DHS, 2020). Although these definitions express the need to protect assets, they are hardware and software focused and fail to consider human aspects of cyber security. Further, cyber security and the risk associated with cyber security is impacted by a multidisciplinary and multistressor system. The physical environment and human/social interactions components are omitted from these definitions which hinders the ability for cyber researchers and risk analysts to holistically assess the risk posed to systems, networks, and users in a cyber domain. This translates to ineffective communication between cyber security experts, whether they are academic researchers or applied practitioners.

Cyber security strategies and perspectives also differ between nations. Some nations use a top–down approach in which they believe the purpose of cyber security is to protect against threats from cyberspace while other nations use a bottom–up approach in which security properties must be safeguarded and guaranteed (Luijij, Besseling, & De Graaf, 2013). As a response to international differences, the Russian-US bilateral working group of the East West Institute and Lomonosov Moscow State University created a terminology framework in which they defined cyber security as “a property of cyber space that is an ability to resist intentional and unintentional threats and respond and recover” (ISI, 2014). However, this definition still focuses on hardware and software and fails to address the human aspects of cyber security.

While some researchers have investigated trends within the current definitions and uses of risk within cyber security, few have presented formalized definitions of cyber security risk. For example, Oltramari and Kott (2018) suggest practitioners describe cyber risk2 in terms of a configuration of a system instead of the probability of harm occurring. Researchers have also investigated the process of identifying specific risks for various systems. A study on the risks to supervisory control and data acquisition (SCADA) systems defined risk management as “coordinated activities to direct and control an organization with regard to risk” and risk assessment as the “overall process of risk identification, risk analysis and risk evaluation” (Cherdantseva et al., 2016).

There has also been some research on differences in cyber security risk perceptions. Quigley, Burns, and Stallard (2013) suggest there are discrepancies in the way cyber security risk is perceived among individuals in different sectors. The study consisted of a rhetorical analysis on 10 writing samples to determine how cyber security-related topics are portrayed by “management gurus,” which consisted of journalists as well as professionals in academia and consulting fields. A rhetorical analysis is an evaluation of the relationship between the writer, message, and audience. The results of this analysis demonstrated that management gurus enhance the perception of cyber security risk by using rhetorical devices (persuasion) and heuristics to create fear among readers and clients.

The various definitions of cyber security and the lack of explicit definitions of cyber security risk demonstrate that these key terms are not standardized, although two research teams have recently presented integrated definitions (Craigen et al., 2014; Ramirez & Choucri, 2016). Since both terms can be used in a wide array of disciplines and applied to various systems, a universal or standardized definition of cyber security and cyber security risk may not be possible. However, it is still important to create standardized definitions of cyber security and cyber security risk in order to mitigate the problems that arise when members of diverse disciplines work together.

2.2. Multidisciplinary Effects on Communication

Technological, sociological, and organizational challenges associated with risk communication are due to the unfamiliar nature and severity of crises (Kellens, Terpstra, & De Maeyer, 2012; Slovic, Fischhoff, & Lichtenstein, 1982) and lack of established mutually agreed upon terms, which diminishes the ability for information to be efficiently and effectively disseminated (Manoj & Baker, 2007). When faced with uncertainty, humans often use heuristics, such as emotions, to make decisions (Gigerenzer & Gaissmaier, 2011). These decisions are often justified using risk as feelings, rather than quantified risk analysis, which is based in logic and measurement (Quigley et al., 2013). Researchers suggest that humans are unable to interpret risk-relevant numbers if terms are not defined in a clear and conceptual manner (Cox, 2008; Gaissmaier & Gigerenzer, 2008).

Cognitive biases also create ineffective risk communication. For example, doctors and nurses often have differing cognitive biases (Blumenthal-Barby & Krieger, 2015; Sladek et al, Bond, & Phillips, 2010). These biases affect their ability to communicate as they have different conceptions of patient care goals. Reader et al. (2007) found that the differing

2Term is spelled as defined in the original source.
conceptions between doctors and nurses are rarely addressed as nurses may report feeling embarrassed by their differences with senior doctors. These issues contribute to a lack of safety precautions and a decline in the quality of patient care. Cognitive biases can be exacerbated in multidisciplinary work as different disciplines have different approaches to risk management (Zinn, 2006). It is therefore important to address these cognitive biases components of the human factor both as risk assessors and as a contributor or mitigator of cyber risk.

Issues in risk communication associated with cognitive biases are worsened by a lack of standardized vocabulary (Manoj & Baker, 2007). The importance of standardized terminology has been demonstrated across disciplines and in cross-disciplinary work. For example, a lack of standardized vocabulary contributed to reduced innovation in fish reproduction studies as scientists and resource managers could not accurately compare their work due to differences in the terms used (Bowen et al., 2011). Standardization of vocabulary is commonly established by creating a formalized, systematic nomenclature that facilitates communication among stakeholders from various disciplines (Ramirez & Choucri, 2016). Ramirez and Choucri (2016) argue that a standardized cyber security vocabulary starts with increased research efforts focusing on identifying trends in terminology standards. Ramirez further suggests there are four subdisciplines of cyber security: public policy, computer science, management, and social science (Ramirez, 2017). In order to facilitate cyber security communication, Ramirez recommends professionals (such as the ARL and academic counterparts in the CSec CRA) initiate change using technical language that is compatible across disciplines.

The presented research used expert elicitation, data-driven thematic analysis, network analysis, and a content analysis comparison to identify patterns and salient themes within interviewees’ definitions of cyber security and cyber security risk. The salient themes were further examined with ARL- and academia-derived themes as a single group and then as two subgroups. Network analysis was used to understand the relationship between the identified themes and across the two sectors (e.g., academia and government–military) and the interviewee disciplines. Content analysis was used to compare the interviewees’ definitions (not the salient themes) to the vocabulary used in cyber ontologies (Oltramari & Kott, 2018).

3. EXPERT ELICITATION AND ANALYSIS

The research methods consisted of four components: expert elicitation through semistructured interviews, data-driven thematic analysis, network analysis, and a content analysis comparison. This study utilized the knowledge of a group of self-selecting cyber experts who were members of the CSec CRA at the time of the interview. The data collected during the expert elicitation were systematically analyzed using data-driven thematic analysis to identify patterns and salient themes within interviewees’ definitions of cyber security and cyber security risk. The salient themes were further examined with ARL- and academia-derived themes as a single group and then as two subgroups. Network analysis was used to understand the relationship between the identified themes and across the two sectors (e.g., academia and government–military) and the interviewee disciplines. Content analysis was used to compare the interviewees’ definitions (not the salient themes) to the vocabulary used in cyber ontologies (Oltramari & Kott, 2018).

3.1. Expert Elicitation Protocol

3.1.1. Outreach

Forty-four (22 ARL, 22 academia) CSec CRA principal investigators, researchers, and professionals were contacted via email asking for their participation in a semistructured interview to collect cyber security risk assessment goals, risk factors, and risk metrics. All research institutes associated with the CSec CRA (at the time of the interviews) were represented in the 27 self-selected interview participants; 10 participants from ARL and 17 from academia. Participants from both ARL and academia self-identified as having multiple sub-areas of expertise, including security informatics, intrusion detection, social and decision sciences, and risk assessment (See Table I).

3.1.2. Semistructured Interviews

The semistructured interview consisted of the interviewer, a scribe, and the interviewee. The same interviewer and scribe were present for all interviews. At the start of the interview, the interviewer described the need for the interview and how it fit into the overall risk assessment process. The first step in any risk assessment is problem formulation and the identification of information, that is what question(s) is the cyber security risk assessment trying to answer and what information is available to answer those questions. The semistructured interview consisted of

Pennsylvania State University, Carnegie Mellon University, Indiana University, The University of California at Davis, The University of California Riverside, and the U.S. Army Research Laboratory.
Defining Cyber Security and Cyber Security Risk within a Multidisciplinary

Table I. Disciplines and Research Areas of Interviewed Cyber Security Collaborative Research Alliance Participants (CSec CRA)

| Behavioral Psychology | Cognitive Neuroscience | Computer Engineering |
|-----------------------|------------------------|-----------------------|
| Computer Science      | Computer Security      | Human Factors Engineering |
| Network Science and Engineering | Risk Assessment | Security Informatics |
| Security Monitoring and Intrusion Detection | Social and Decision Sciences | Software Engineering |
| Systems and Network Security | Tactical Mobile and Strategic networks | Wireless Systems and Networks |

questions about the tasks and management goals necessary to achieve progress in each interviewee’s respective research area and the types of risks posed to each research area. Interviewees were also asked for their definitions of cyber security and cyber security risk. Each semistructured interview lasted approximately 30–60 minutes. The interviews of academic participants were recorded for transcription purposes. However, audio recording was not permitted in Army Research Laboratory buildings, so the interviews were transcribed in situ by the same scribe for all interviews.

3.2. Data Analysis and Discussion

3.2.1. Thematic Analysis

Thematic analysis is commonly used in qualitative research to identify overarching patterns, or themes, that are expressed both implicitly and explicitly across qualitative data sets such as narratives and interviews (Braun & Clarke, 2006). The data-driven method of thematic analysis draws on the practice of developing theory from trends arising from the data via systematic investigation, while the theory-driven method examines the data for predetermined trends or theories (Clarke & Braun, 2014).

Data-driven thematic analysis was performed on the transcripts of interviewees’ responses to the questions “What is your definition of cyber security?” and “What is your definition of cyber security risk?” to identify and organize similar concepts into representative themes. All 27 interview participants were asked the same “definitions” question, however, two individuals’ responses were removed from “cyber security” thematic analysis due to (1) stated uncertainty about how to answer the question, and (2) a demonstrated lack of understanding of the prompt due to variable English proficiency. All 27 interview participants’ responses for “cyber security risk” were appropriate for thematic analysis. The cyber security and cyber security risk definitions of the interview transcripts were analyzed using data-driven thematic analysis; Table II is an example of this process.

Using the data-driven thematic analysis methodology detailed by Braun and Clark (2006), the entirety of each interview (all questions and answers) was independently read and coded by three researchers (doctorate, master’s, and undergraduate level). The researchers then coded the responses to the “definitions” questions to identify the core concepts of each answer (e.g., Table II: “Code” column). Once individually read and coded, the three researchers (with input from other authors of this article) gathered as a group to refine the codes for the “definitions” answers into first-order themes (e.g., Table II: “1° Theme” column). Themes “[reflect] a pattern of shared meaning, organized around a core concept or idea, a central organizing concept.” (Braun, Clarke, Hayfield, & Terry, 2018). The first-order themes were then compared to the interviewees’ original “definitions” answers to ensure the theme was representative of the response. The researchers than individually collated the first-order themes into the second-order themes and regrouped to (1) compare the individually identified second-order themes and (2) come to a consensus on how the first-order themes were refined into second-order themes (Table II: “2° Theme” column). This process was repeated for a third time resulting in third-order themes (Table II: “3° Theme” column).

When read left to right, Table II exemplifies the sequential order of the response-code-theme refining process of thematic analysis and illustrates how more than one theme can be identified in a single definition. Table II presents verbatim excerpts from three interviewees (marked A, B, and C). The two entries for Interviewee A demonstrate how thematic analysis researchers can identify different themes, in this case first-order themes, from the same definition extract and code. The two entries for interviewee B illustrate how multiple codes and themes can be identified in a single definition. Through the deliberation process described in the previous paragraph
Table II. Excerpt of Coding Progression via Thematic Analysis of Responses to “What is your Definition of Cyber Security Risk?”

| Interviewee | Definition Extract                                                                 | Code                                | 1° Theme                          | 2° Theme                                | 3° Theme                                          |
|-------------|-------------------------------------------------------------------------------------|-------------------------------------|-----------------------------------|------------------------------------------|---------------------------------------------------|
| A           | “To me, it is the humans that are the biggest risk.”                                | humans are the biggest risk         | Bad user or attacker              | Unknown of human behavior                | Uncertainties introduced by human factors          |
| A           | “…humans that are the biggest risk.”                                               | humans are the biggest risk         | Humans are a source of risk       | Unknows of human behavior               |                                                   |
| B           | “…humans will be hard such as insider threat.”                                     | humans are hard to quantify         |                                  |                                        |                                                   |
| C           | “…attackers don’t follow rules in reality…”                                       | attackers don’t follow rules        |                                  |                                        |                                                   |
| B           | “Risk in terms of machine may be easier to quantify.”                              | machine risk is easier to quantify than human |                                  |                                        |                                                   |

and in detail by Braun and Clark (2006) and Braun et al. (2018), the second-order theme and third-order theme columns show how the identified first-order themes and second-themes were collated, respectively, into more inclusive (i.e., higher order) themes.

Thematic analysis results. The theme refining process in thematic analysis is visualized in the thematic butterfly diagrams below (Figs. 1 and 2). The systematic consolidation of similar ideas (i.e., patterns of thought) into representative themes is illustrated by the grouping of several themes into a unifying theme (moving from the edges of the diagram inward). The research presented is a comparison of the thematic butterfly diagrams for CSec CRA academics and ARL researchers and practitioners. The results of the refined thematic butterfly diagrams are useful in distilling and relating commonly held perceptions of cyber security and cyber security risk across diverse issues and stakeholder groups.

The thematic butterfly diagrams below provide a comparison of the first, second, and third-order cyber security and cyber security risk themes identified from interviews across the disciplines of ARL practice and academic research. The outermost themes (far left for ARL and far right for academia) are first-order themes. Moving toward the spine of the thematic butterfly diagram, the themes are refined from first-order, second-order, and third-order themes. A handful of second order themes also serve as third-order themes as some themes could not be consolidated with other themes without losing the context of the answered definition. Green themes were identified in both sectors (ARL and academia), blue themes were expressed by only one sector, and yellow themes represent differing first or second-order themes that were refined into the same second and third-order themes, respectively.

Eighty-two first-order “cyber security” themes were identified across the 25 cyber security definitions provided by the CSec CRA expert elicitation participants. The 82 first-order themes were refined into 33 second order themes, which were further refined into 19 third-order themes (Fig. 1; Tables SI–SIII). Eighty first-order “cyber security risk” themes were identified across the 27 cyber security risk definitions provided by the CSec CRA expert elicitation participants. The 80 first-order themes were refined into 36 second-order themes, which were further refined into 26 third-order themes (Fig. 2; Tables SIV–SVI).

To build the composite cyber security and cyber security risk definitions, the identified third-order themes were reexamined within the context of the interviewees’ stated definitions from the interviews and the greater the context of the CSec CRA mission. The themes were then pieced together into coherent, contextually sensible definitions for cyber security and cyber security risk. Using the 19 third-order “cyber security” themes (Fig. 1; Table SIII), the interviewees’ composite definition of cyber security

...the iterative process of maintaining quantifiable levels of cyber system dependability and control over verifiable data provenance, confidentiality, integrity, and accessibility (CIA) via comprehensive system
Defining Cyber Security and Cyber Security Risk within a Multidisciplinary

Fig. 1. Thematic butterfly map of first, second, and third-order themes from thematic analysis of the answers to “What is your definition of cyber security?” Green themes were expressed by both sectors (U.S. Army Research Laboratory [ARL] and academia), blue themes were expressed by only one sector, and yellow themes represent differing first or second-order themes that consolidate into the same second and third-order themes, respectively. Image best viewed in color and enlarged via online journal.

Fig. 3 illustrates the frequency of the top five third-order themes inferred from the interviewees’ answers to the question: “What is your definition of cyber security?” A full list and frequencies of the first-, second-, and third-order themes is provided in the Supporting Information Tables SI–SIII.

Using the 26 third-order “cyber security risk” themes (Fig. 2, Table SVI), the interviewees’ composite definition of cyber security risk

...the context-driven, agility-dependent, and goal-dependent probability of sociotechnical system harm or failure due to known and unknown factors including human behavior, level of risk perception, and system physical and cyber vulnerabilities across multiple dimensions and scales that affect resource prioritization, control, and/or system functionality.

Fig. 4 illustrates the frequency of the top five third-order themes inferred from the interviewees’ answers to the question: “What is your definition of cyber security risk?” A full list and frequencies of the...
Fig 2. Thematic map of first, second, and third-order themes from thematic analysis of the answers to “What is your definition of cybersecurity risk?” Green themes were expressed by both sectors (U.S. Army Research Laboratory [ARL] and academia), blue themes were expressed by only one sector, and yellow themes represent differing first or second-order themes that consolidate into the same second and third-order themes, respectively. Image best viewed in color and enlarged via online journal.
Defining Cyber Security and Cyber Security Risk within a Multidisciplinary

First-, second-, and third-order themes is provided in the Supporting Information Tables SIV–SVI.

Thematic analysis discussion. The thematic butterfly diagrams (Figs. 1 and 2) visualize the theme refining process across the ARL and academic subgroups of the larger CSec CRA participants. All of the respective third-order themes were used to build the composite definitions for cyber security and cyber security risk.

The cyber security themes indicate that experts in both sectors recognize cyber security is context-driven (e.g., what is being secured for whom at what cost) and requires resilient system functionality. System functionality can be maintained through the maintenance of the traditional cyber security vulnerabilities (CIA), threat prediction and prevention, and the protection of resources. The themes identified and refined from the academic expert elicitation suggest defenders are able to mitigate risks associated with system functionality; the themes derived from the ARL expert elicitation suggest cyber security is dependent on the human factor as an attacker, but the defender is not specifically addressed as a risk mitigator. Further, the academics view cyber security as a multidimensional, complex framework. ARL experts, on the other hand, focus on specific resources that need to be protected to ensure a cyber secure environment. Neither sector, ARL nor academia, think perfect cyber security is attainable; however, academia definitions implied that cyber security was complicated (Fig. 1), while ARL definitions implied that cyber security risk was complicated (Fig. 2).

The thematic analysis suggests that although both ARL and academia experts consider the scope and context of cyber security risk, they approach cyber security risk in a different manner. Both sectors think that cyber security risk is exacerbated by a lack of understanding of human factors effects on cyber security. The ARL interviewees expressed that the majority of cyber security risk is captured within the traditional information vulnerability triad of CIA, while academics expressed that the CIA triad does not comprise all risk factors (e.g., human factors, timing). When analyzing and discussing risks, computer scientists focus on CIA attributes (Confidentiality of information, Integrity or maintaining the trustworthiness of data, and Availability or providing information access to authorized personnel only) as the sole indicators of risk; Von Solms & Van Niekerk, 2013). Oltramari et al. (2015) suggest a holistic cyber security risk model incorporates variables other than solely CIA, specifically time and humans as crucial factors in evaluating risk to a system, network, or user.

Academics attempt to list the multitude of external factors that influence a problem, address the uncertainty, and then attempt to identify the source of uncertainty. ARL experts generalize the uncertainty and focus on agility as a means to overcome risk. Both groups either explicitly stated or implied that cyber security risk is exacerbated by a lack of under-
standing of humans as risk contributors or mitigators. The academia definitions included the impact on humans, whereas the negative impacts are not explicitly specified, thus not inferred, in the ARL analysis. The academia perspective attempts to understand cyber security risk as it relates to cyber security and human factors, both as defenders and attackers. This holistic view corresponds to the cyber security analysis, in which the themes inferred from academic expert language revolve around the characterization of cyber security as a complex framework.

3.2.2. Network Analysis

Network analysis and visualization examines the relationship (e.g., coexistence) between entities (e.g., interviewees’ definition themes). Network analysis was performed to understand the relationships between the definition-derived third-order themes analyzed by interviewee sector and discipline. In this setting, the visualizations that result from network analysis of the third-order themes can provide answers to the questions such as, “Which third-order theme was used the most in conjunction with other third-order themes?”; “Which third-order theme is isolated from the corpus of third-order themes, that is a theme that only represents a solitary definition?”; or “What third-order themes were identified across all disciplines?”

Network analysis was performed using Gephi (Bastian, Heymann, & Jacomy, 2009) on each of the third-order themes for cyber security and cyber security risk comparing across academic and ARL interviewees’ individual definitions (see section on sector-based network analysis) and across the interviewee corpus by discipline (see section 3.2.2.2.).

**Sector-based network analysis.** Sector-based network analysis was used to explore the relationships between the third-order themes within any given interviewee definition. Given the complex nature of the resulting networks, Fig. 5 is presented as a simplified network to facilitate interpretation of Figs. 6, 7, and 8.

**Interpreting sector-based networks:** The nodes (i.e., circles) are the representative third-order themes derived from interviewees’ respective definitions, and the size of the node corresponds to the number of degrees (i.e., connections) to other nodes. The color of the nodes represents the modularity of communities within the constructed network, that is nodes of the same color within a network are more densely connected to each other than other nodes in the network (Blondel, Guillaume, Lambiotte, & Lefebvre, 2008). Within Figs. 5–8, the node colors signify communities of themes frequently expressed together in the same definition. For example, within Fig. 5, themes A, C, and D are all green because they were expressed together in the same or multiple definitions, while B (purple) was only expressed with A in one definition, and E (gray) is an isolated node and represents a definition with one theme. An isolated node has no connections to another node, versus a network component that is connected by least one path of edges (e.g., Fig. 5: B-A-C-D-A).

The edges (i.e., connection, line) between two nodes (i.e., themes) illustrates the pairing of those two themes within a single interviewee definition. For example, themes A and B were found in the same definition and themes C and D were found in the same definition. The color of the edge indicates the interviewee’s sector (gold for academia and blue for ARL), for example themes A and B were found in an one academia definition, while themes C and D were found in a second academia definition, while themes A, C, and D were found in either one (C-A-D) or two ARL definitions (A-C, A-D).

**Constructed networks:** The third-order theme and interviewee sector networks were constructed using the following layout protocol: Force Atlas > No Overlap > Label Adjust > Expansion. The sector-based network analysis resulted in two undirected parent networks, one for cyber security third-order
themes and one for cyber security risk third-order themes (see Fig. 6). Each parent network was further visualized as two child networks (i.e., sector-parsed), one network of academic third-order themes and one network of ARL third-order themes (see Figs. 7 and 8). Figs. 6, 7, and 8 are the network visualizations of the network analysis performed on the cyber security and cyber security risk thematic analysis third-order themes.

Fig. 6 contains the network structure of cyber security (left network) and cyber security risk (right network) third-order themes identified from interviewed cyber experts’ definitions of cyber security and cyber security risk, respectively. Fig. 7 contains the network structure of cyber security third-order themes parsed into the interviewees sector, academia (left network) and ARL (right network). Fig. 8 contains the network structure of cyber security risk third-order themes parsed into the interviewees sector, academia (left network), and ARL (right network). The emergent structure and interconnectedness of the sector-based networks (Figs. 6, 7, and 8) were evaluated for the following network properties: node and edge count, connected components, graph density, influential nodes, isolated nodes, modularity, and hanging edges.

Connected components: Each of the networks (parents: Fig. 6 and sector-parsed: Figs. 7 and 8) have one main cohesive network structure (i.e., component), with the exception of two isolated nodes in the ARL cyber security risk network (Fig. 8, right network). A single cohesive network means that all the interviewees’ definitions share common themes with cyber experts within their sector and across the two sectors. Several fragmented networks would be indicative of wholly dissimilar definitions.
Node and edge count: The academic and ARL participants’ cyber security and cyber security risk definitions produced approximately the same number of themes (i.e., nodes), 18 versus 15 and 22 versus 17, respectively (Table III). The number of edges in the academic cyber security network is 94, more than twice that of the ARL cyber security network with 42 edges. Also, the number of edges in the academic cyber security risk network is 68, which is nearly twice that of the ARL cyber security risk network with 35 edges. The academic subgroup tended to explore the multitudes of implications, more than ARL researchers, as illustrated by the increased number of identified themes and fewer academic definitions converging on unifying themes. Fewer themes were identified within any given ARL definition as compared to the multiple themes identified within a majority of the academic definitions. The pontification of academics compared to the directness of the ARL participants supports the basic research perspective of academics and the generalizing and operationalizing objective for the ARL. Additionally, the ARL subgroup themes are more management focused with a common understanding of the mission within the ARL and an emphasis on the crucial components they believe are required to attain cyber security. Some may argue this is a more practical approach, but all factors must be considered in order to holistically quantify cyber risk.

Graph density: Graph density measures, on a scale from 0 to 1, the completeness of a network (Bastian, 2015). If all of the nodes connected to all of the other nodes in the network, graph density would be 1. The less connected (i.e., complete) a network, the closer the graph density is to 0. If a third-order theme network were to have a graph density of 1, all of the definitions would have contained all of the identified third-order themes. If a third-order theme network were to have a graph density of 0, each of the definitions could contain a single third-order theme that was unique to each definition, that is, no shared understanding. The corpus network for cyber security has the higher graph density of 0.795, while the corpus network for cyber security risk only has a graph density of 0.317 (Table III). The definitions provided for cyber security shared more third-
Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Framework

Fig 8. Sector-parsed networks of cyber security risk third-order themes identified from the interview corpus using thematic analysis. Nodes (i.e., circles) are the third-order theme and edges (i.e., connecting lines) signify interviewee definitions from which both themes were identified. The nodes of the same color are more densely connected to each other than other nodes in the network, that is community of nodes. The edge color denotes the interviewees sector, Academia (gold; left network) and U.S. Army Research Laboratory (ARL; blue, right network). Image best viewed in color and enlarged via online journal.

order themes across the interviewees than the cyber security risk definitions. The graph density of the cyber security sector-parsed network is 0.4 for ARL and 0.614 for academia; the cyber security risk sector-parsed network is 0.435 for ARL and 0.294 for academia. The academia definitions of cyber security shared more third-order themes than ARL, while the ARL definitions of cyber security risk shared more third-order themes than academia.

Influential nodes: Table III details the most and least influential nodes in each network. The most influential node is the node connected to the most nodes, that is the third-order theme that was identified within the most definitions and definitions from which more than one third-order theme was identified. Within the corpus and both sector cyber security networks, the third-order theme of “Context-driven” is the most influential node with 43 connections (i.e., degrees) in the corpus network, 27 connections in the academia network, and 16 connections in the ARL network. “Impacts of CIA vulnerabilities” is the most influential node in the cyber security risk corpus and academia network with 28 and 23 connections, respectively. “Probability of outcomes” is the most influential node in the cyber security risk ARL network with nine connections.

Isolated nodes: Isolated nodes are nodes that have no connecting edges to any other node. Isolated nodes represent definitions that contained one third-order theme that was not identified in any other interviewee definition. The ARL network for cyber se-
Table III. Minimum and Maximum Number of Degrees, with Respective Node (i.e., Third-Theme) for Each Parent Networks and Parsed Sector Networks. The Degree is the Number of Edges (i.e., connections) Connecting to Other Nodes

| Network                  | Number of | Total N | Total E | GD     | Min D | Theme(s)                                                                 | Max D   | Theme                  |
|--------------------------|-----------|---------|---------|--------|-------|---------------------------------------------------------------------------|---------|------------------------|
| Cyber Security           |           |         |         |        |       |                                                                            |         |                        |
| Corpus                   | 3         | 19      | 136     | 0.795  | 2     | Systemic solutions                                                        | 43      | Context-driven          |
| Academia                 | 2         | 18      | 94      | 0.614  | 1     | Verifiable information provenance                                         | 27      | Context-driven          |
| ARL                      | 3         | 15      | 42      | 0.4    | 2     | Accurate intrusion detection; Comprehensive system awareness; Resource management; Systemic solutions | 16      | Context-driven          |
| Cyber Security Risk      |           |         |         |        |       |                                                                            |         |                        |
| Corpus                   | 3         | 26      | 103     | 0.317  | 1     | Goal dependent                                                            | 28      | Impacts of CIA vulnerabilities                                       |
| Academia                 | 3         | 22      | 68      | 0.294  | 1     | Goal dependent; Multiple realms of threats; Sociotechnical exploitation    | 23      | Impacts of CIA vulnerabilities                                       |
| ARL                      | 6         | 17      | 35      | 0.435  | 0     | Absolute and relative resource valuation; Scope of risk perception         | 9       | Probability of outcomes                                             |

Comm. = communities, N = nodes, E = edges, GD = graph density, D = degrees.

...security risk, (Fig. 8) has two isolated nodes: “Scope of risk perception” in the upper left section of the network and “Absolute and relative valuation” in the middle right section of the network.

**Modularity:** Modularity is a measure of connectedness within the network and is represented by node color. The more densely interconnected nodes, in comparison to the rest of the network, share the same color. Modularity can be used to identify communities of nodes, which represent connections between themes of those that share similar pairings or groupings.

**Hanging Edges:** Hanging edges represent definitions from which only one third-order theme was identified. If a node has a hanging edge, it will be on the right side of node parallel to the legend text, for example “Maintenance of CIA” in the academia network for cyber security (Fig. 7, left network). Hanging edges are present in all networks except for the ARL network for cyber security (Fig. 7, right network).

**Discipline-based network analysis.** The discipline-based network (Fig. 9) visualizes the cross-tabulation of interviewees per discipline per cyber security (left) and cyber security risk (right) third-order theme. Tables SVII and SVIII are the tabular form of the data used to produce Fig. 9. The discipline nodes were anchored in the center as the spine of the network with the cyber security third-order theme nodes alphabetically radiating to the left and the cyber security risk third-order theme nodes to the right (Fig. 9). The disciplines and research areas listed in Table I were grouped into six representative disciplines: cognition and human factors (e.g., behavioral psychology, cognitive neuroscience, and human factors engineering); computer and cyber security (e.g., computer engineering, computer science, computer security, security informatics, and security monitoring and intrusion protection); decision sciences (risk assessment and social and decision sciences), network science, security, and engineering (e.g., network science and engineering, systems and network security, tactical mobile and strategic networks, and wireless systems and networks); software engineering; and user privacy and security.

The size of the discipline nodes corresponds to the number of interviewees per discipline and the size of the third-order theme nodes corresponds to the number of interviewees whose definition contained the theme. The thickness of the edge connecting a representative discipline and third-order theme is proportional to the number of interviewees from the discipline whose definition contain the connected theme. The color of the edges identifies the interviewees' representative discipline. Since the structure of the discipline-based network was predetermined (i.e., no algorithm was used to determine nodal relationships), the structural network properties were not analyzed.

While the 14 of the 19 cyber security third-order themes and 19 of the 26 cyber security risk third-order themes were “multidisciplinary” (i.e., more...
than one discipline), only one theme per definition question encompassed all disciplines. All six disciplines were represented in the 10 interviewees’ whose cyber security definition contained the third-order theme “maintenance of CIA” and the 10 interviewees’ whose cyber security risk definition contained the third-order theme “impacts of CIA vulnerabilities.” These cross-disciplinary references to CIA reflect the pervasiveness and historical emphasis on CIA and the protected data in the cyber security field. All disciplines except for software engineering and user privacy and security were represented in the top cyber security third-order theme “context-driven” (13 interviewees). Additionally, all disciplines except for software engineering and user privacy and security were represented in the top cyber security risk third order theme “probability of outcomes” (11 interviewees). Despite the fact that three of the six disciplines are human focused, and the other three acknowledge the importance of human factors in their work, humans’ role in cyber security and cyber security risk is implied rather than directly cited by interviewees in most disciplines.

3.2.3. Content Analysis

In addition to thematic text analysis, semantic text analysis methods can qualitatively and quantitatively...
tively evaluate the relationships between vocabulary and themes appearing in text (Roberts, 2000). Oltramari and Kott (2018) conducted a semantic text analysis to evaluate the number of risk-related concepts incorporated into cyber ontologies. These authors developed a cyber risk vocabulary list consisting of 45 terms found in the literature and determined the frequency of occurrence each term appeared in 10 cyber security risk-related ontologies. 4

Using the cyber risk vocabulary list compiled by Oltramari and Kott, a content analysis was performed on the original full-length definitions provided by each expert elicitation participant. The content analysis determined the number of definitions that used each vocabulary term, not the frequency of the vocabulary term within the definitions. The content analysis was then compared to the “frequency of occurrence” conducted by Oltramari and Kott (Table III), which measures the number of ontologies containing the specific terms. When two terms were listed together by Oltramari and Kott (2018), for example source/origin, the frequency was determined for each term and then summed, ensuring that no ontologies were counted twice.

The percentage of interview participants’ definitions that contained each vocabulary term was calculated for cyber security ($N = 25$) and cyber security risk ($N = 27$) and compared against the “frequency of occurrence” (represented as a percentage; $N = 9$) calculated by Oltramari and Kott (2018). For this comparison, the interview participants were not separated into ARL and academia subgroups. For each definition (i.e., cyber security and cyber security risk) and each vocabulary term, the percentage was computed using the number of interview participant definitions that contained each vocabulary term and the total CSec CRA expert elicitation participants.

Several cyber risk vocabulary terms and concepts were modified by the adjectives “cyber” or “risk” and consequently, the full term, for example cyber attack, rarely, if ever, appeared in the expert elicitations. An additional content analysis was performed with adjectives removed and the stem form of the term, for example “vulnerab” rather than “cyber vulnerability.” Using the stem form of the term ensures that all possible forms of the term are captured in the content analysis, for example “vulnerable,” “vulnerability,” and “vulnerabilities.”

4Ontologies provide “a model of concepts in the domain of interest in a more elaborate, formal, and exhaustive manner than conventional definitions.” (Oltramari & Kott, 2018)

Content analysis results. The content analysis of the interviewees’ original definition based on the cyber risk vocabulary compiled by Oltramari and Kott (2018) is detailed in Table IV. The content analysis comparison determines whether the expert elicitation participants used the same language as cyber ontology developers when defining cyber security and cyber security risk. Table IV provides the vocabulary percentage breakdown for the ontologies identified by Oltramari and Kott (2018) and the expert elicitation definitions provided for cyber security and cyber security risk.

The top cyber risk vocabulary terms for cyber ontology developers were “cyber attack,” “asset,” and “cyber vulnerability,” while the top terms for expert elicitation participants were “network,” “control,” and “consequences” for cyber security and “risk,” “network,” and “likelihood” for cyber security risk (Table IV). However, when the expert elicitation were evaluated for the nonadjectival stem forms of the vocabulary term, the top terms for cyber security were “network,” “attack” (stemmed from “cyber attack”), and “identi” (stemmed from “risk identification); the top terms for cyber security risk were “risk,” “attack” (stemmed from “cyber attack”), and “vulnerab” (stemmed from “cyber vulnerability”) (Table V). The majority of vocabulary terms appeared in a greater percentage of the cyber risk ontologies than of the expert elicitation definitions. “Cyber attack,” “cyber vulnerability,” and “asset” were the top vocabulary terms used by the cyber risk ontology developers.

Of the 45 cyber risk vocabulary terms and concepts identified by Oltramari and Kott, only 19 terms/concepts were used during the expert elicitation to define cyber security and cyber security risk. This number increased to 29 when the nonadjectival stemmed forms of terms/concepts were used. The terms/concepts that appear in cyber security risk ontologies but were not found in the expert elicitation are listed in Table VI. The nonadjectival stemmed forms of terms/concepts with the asterisks were found in the expert elicitation.

Content analysis discussion. The content analysis compared the cyber security and cyber security risk terms used by CSec CRA expert elicitation participants (from this study) versus the cyber security and cyber security risk terms used in cyber ontologies (Oltramari & Kott, 2018). The results of this analysis suggest ontology developers and cyber experts
Table IV. Expert Elicitation Use of Cyber Security Terms and Concepts by Percentage. The Cyber Risk Ontology (CR Ont; N = 9) Columns is the Percentage of Select Ontologies that Contain the Cyber Risk Specific Vocabulary Terms and as Determined by Oltramari and Kott. The Cyber Security Expert Elicitation (CS EE; N = 25) and Cyber Security Risk Expert Elicitation (CSR EE; N = 27) Columns are Percentage of Experts Who Used the Term Within Their Definition of Cyber Security and Cyber Security Risk, Respectively

| Term/Concept       | CR Ont | CS EE | CSR EE | Term/Concept       | CR Ont | CS EE | CSR EE |
|--------------------|--------|-------|--------|--------------------|--------|-------|--------|
| Alert              | 22.2   | 0.0   | 0.0    | Impact             | 44.4   | 0.0   | 7.4    |
| Asset              | 66.7   | 0.0   | 3.7    | Intent             | 22.2   | 0.0   | 3.7    |
| Benefit            | 11.1   | 0.0   | 3.7    | Likelihood         | 33.3   | 0.0   | 14.8   |
| Configuration      | 33.3   | 0.0   | 0.0    | Mission            | 33.3   | 0.0   | 0.0    |
| Consequence        | 55.6   | 4.0   | 7.4    | Network            | 33.3   | 32.0  | 22.2   |
| Control            | 11.1   | 8.0   | 3.7    | Origin/Source      | 55.6   | 20.0  | 11.1   |
| Cost               | 22.2   | 4.0   | 3.7    | Payload            | 22.2   | 0.0   | 0.0    |
| Countermeasure     | 44.4   | 0.0   | 0.0    | Report             | 22.2   | 0.0   | 0.0    |
| Credential         | 22.2   | 4.0   | 0.0    | Risk               | 33.3   | 0.0   | 81.5   |
| Cyber attack       | 88.9   | 0.0   | 0.0    | Risk assessment    | 33.3   | 0.0   | 11.1   |
| Cyber defense      | 22.2   | 0.0   | 0.0    | Risk factor        | 33.3   | 0.0   | 0.0    |
| Cyber exploitation | 44.4   | 0.0   | 0.0    | Risk identification| 11.1   | 0.0   | 0.0    |
| Cyber incident     | 22.2   | 0.0   | 0.0    | Risk metric        | 33.3   | 0.0   | 0.0    |
| Cyber operation    | 22.2   | 0.0   | 0.0    | Risk mitigation    | 11.1   | 0.0   | 0.0    |
| Cyber response     | 22.2   | 0.0   | 3.7    | Risk monitoring    | 11.1   | 0.0   | 0.0    |
| Cyber threat       | 22.2   | 4.0   | 0.0    | Security/Protocol  | 33.3   | 0.0   | 0.0    |
| Cyber vulnerability| 66.7   | 0.0   | 0.0    | Service            | 55.6   | 4.0   | 3.7    |
| Dependability      | 22.2   | 0.0   | 0.0    | Situation          | 33.3   | 0.0   | 0.0    |
| Detection          | 55.6   | 0.0   | 3.7    | Stakeholder        | 22.2   | 0.0   | 0.0    |
| Failure            | 33.3   | 0.0   | 3.7    | Target             | 44.4   | 0.0   | 0.0    |
| Fault              | 33.3   | 0.0   | 0.0    | Threat             | 44.4   | 12.0  | 18.5   |
|                    |        |       |        | Treatment          | 11.1   | 0.0   | 0.0    |

Table V. Content Analysis of Expert Elicitation for Cyber Risk Vocabulary Without Adjectives and Using Stem Form of Vocabulary Terms. The Cyber Risk Vocabulary Terms is the Full Form of the Vocabulary Term/Concept Identified by Oltramari and Kott. The Stemmed Vocabulary Terms Are the Stem (i.e., base) Form of the Word without Any Adjective. The Cyber Risk Ontology (CR Ont; N = 9) columns is the Percentage of Select Ontologies that Contain the Cyber Risk Specific Vocabulary Terms and as Determined by Oltramari and Kott. The Cyber Security Expert Elicitation (CS EE; N = 25) and Cyber Security Risk Expert Elicitation (CSR EE; N = 27) Columns are Percentage of Experts Who Used the Term Within Their Definition of Cyber Security and Cyber Security Risk, Respectively

| Cyber Risk Vocabulary Terms | CR Ont | CS EE % | CSR EE % | Stemmed Vocabulary Terms | CS EE % | CSR EE % |
|-----------------------------|--------|---------|----------|--------------------------|---------|----------|
| Cyber attack                | 88.9   | 0.0     | 0.0      | Attack                   | 24.0    | 29.6     |
| Cyber defense               | 22.2   | 0.0     | 0.0      | Defen                    | 8.0     | 0.0      |
| Cyber exploitation          | 44.4   | 0.0     | 0.0      | Exploit                  | 0.0     | 11.1     |
| Cyber operation             | 22.2   | 0.0     | 0.0      | Operat                   | 16.0    | 7.4      |
| Cyber response              | 22.2   | 0.0     | 0.0      | Respon                   | 4.0     | 0.0      |
| Cyber vulnerability         | 66.7   | 0.0     | 0.0      | Vulnerab                 | 4.0     | 25.9     |
| Dependability               | 22.2   | 0.0     | 0.0      | Dependab                 | 4.0     | 0.0      |
| Risk identification         | 11.1   | 0.0     | 0.0      | Identiti                 | 24.0    | 14.8     |
| Risk metric                 | 33.3   | 0.0     | 0.0      | Metric                   | 4.0     | 3.7      |
| Risk mitigation             | 11.1   | 0.0     | 0.0      | Mitigat                  | 8.0     | 0.0      |

(researchers and practitioners) do not use the same terms to operationalize cyber security risk. A number of terms used in ontologies to describe cyber security risk were not included in the definitions of cyber security and cyber security risk generated during the expert elicitation (Table VI); however, both groups focused on “attack” as a key term. Other top terms used by ontology developers to describe cyber security risk include “vulnerability” and “target.” Other top terms used by expert elicitation interviewees include “network” and “threat.” The results from the final analysis indicates that there is reason to believe that experts in different disciplines and sectors, each working in some aspect of cyber security, focus on
different aspects of the complex cyber risk universe or use different terms to describe similar concepts (Stemler, 2001).

### 3.3. Comparison to Standards and Best Practices

Cyber security definitions have changed over time in part due to the increasing dependence of global society on cyber systems. The third-order themes used to build the composite definitions of cyber security (CS) and cyber security risk (CSR) were compared against a selection of national and international standards and best practices (Table VII). The comparisons in Tables VIII and IX illustrate the congruencies and inconsistencies across state-of-the-art and regulatory definitions and emphasize the common themes that are highlighted. The comparisons also highlight expert-identified important themes that are not included in any of the current definitions. The following sources of definitions were used: Federal Information Security Modernization Act of 2014 (U.S. Congress, 2014), International Organization for Standardization (ISO, 2012), International Telecommunication Union (ITU, 2008; 2011), National Institute of Standards and Technology (NIST, 2018), National Initiative for Cybersecurity Careers and Studies (NICCS; DHS, 2020), Committee on National Security Systems (CNSS, 2015), and the World Economic Forum (WEF, 2012). The Merriam-Webster Dictionary (MW, 2020) and Craigen et al. (2014) sources are not a standard or best practice, however, they provide context for nontechnical general definitions. Additionally, the European Network and Information Security Agency (ENISA) uses the abbreviated United States Department of Homeland Security (DHS) NICCS glossary definition (DHS, 2020), while the presented comparison evaluates the “extended definition” provided by the glossary (Brookson et al., 2015).

3.3.1. Comparison of Definitions Results

The NICCS cyber security definition was the most complete definition of the nine definitions analyzed. In the NICCS definition, 14 of the 19 cyber security third-order themes were identified (Table VIII). The CNSS cyber security risk definition was the most complete of the six analyzed definitions, with 14 of the 26 cyber security risk third-order themes identified (Table IX).

None of the standards or best practices contained all of the third-order themes for either cyber security or cyber security risk. For the cyber security definition, “protection of resources” and “resource management” were either explicit or implicit in all nine definitions, while threat prediction and/or prevention was explicit in only three definitions, and implied in another five. Only five of nine definitions explicitly referred to or implied “maintenance of confidentiality, integrity, and availability” and “resilient system functionality,” while the critical aspects of intrusion detection, concerns about information provenance, and the need for a systemic solution were only mentioned in one and inferred in two additional definitions. The security state of any connected cyber system or even any single machine is constantly in flux, thus any definition of cyber security should reflect this dynamic situation. Yet despite this very broadly acknowledged phenomenon (Heard, Heard, & Adams, 2016; Xu, 2019), only three of the nine definitions even implied the ever-changing nature of functional cyber security, and only one referred in any way to the human elements inherent in cyber networks, and thus in cyber security.

The approaches to defining cyber security risk, in the six definitions analyzed, tended toward considering risk as a probability of harmful outcomes. Of these, only one considered human impacts of cyber security, but only one of these was an explicit consideration.
### Table VII. Select Definitions of Cyber/Information Security and Risk from National and International Standards and Best Practices. Merriam-Webster (MW) and Craigen et al., 2014 Are Standard or Best Practice, however it Provides Context for a Nontechnical General Definition

| Source          | Security definition                                                                 | Risk definition                                                                 |
|-----------------|--------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| MW              | Cybersecurity: “Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.” | Security risk: 1) “someone who could damage an organization by giving information to an enemy or competitor” 2) “someone or something that is a risk to safety” |
| Craigen et al., 2014 | Cybersecurity: “…the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights.” | No explicit definition for cyber or information security risk. |
| FISMA           | Information security: “The term ‘information security’ means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide: (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (C) availability, which means ensuring timely and reliable access to and use of information.” | No explicit definition for cyber or information security risk. |
| ISO             | Cybersecurity: “Preservation of confidentiality, integrity and availability of information in the Cyberspace. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.” | No explicit definition for cyber or information security risk. |
| ITU             | Cybersecurity: “The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets. Organization and user’s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user’s assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability; Integrity, which may include authenticity and nonrepudiation; Confidentiality.” | Security risk: “The probability that a threat will exploit a vulnerability to breach the security of an asset.” |

(Continued)
| Source    | Security definition                                                                                                                                                                                                                                                                                                                                 | Risk                                                                                                                                                                                                                           |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NICCS     | “Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.” | “The potential for an unwanted or adverse outcome resulting from an incident, event, or occurrence, as determined by the likelihood that a particular threat will exploit a particular vulnerability, with the associated consequences.” |
| NIST      | “The process of protecting information by preventing, detecting, and responding to attacks.”                                                                                                                                                                                                                                                     | “A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.”           |
| CNSS      | “Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.”                                                                                                                                           | “A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. Adverse impacts to the Nation include, for example, compromises to information systems that support critical infrastructure applications or are paramount to government continuity of operations as defined by the Department of Homeland Security.” |
| WEF       | “Cybersecurity’ refers to analysis, warning, information sharing, vulnerability reduction, risk mitigation and recovery efforts for networked information systems.”                                                                                                                                                                              | ‘Cyber risks’ are defined as the combination of the probability of an event within the realm of networked information systems and the consequences of this event on assets and reputation.”                                                                 |

security risk, and none included humans as risk creators or inducers, that is attackers, malicious users, or incompetent users or defenders. And despite the common reliance on monetization as a means of normalizing the quantified impacts of cyber security breaches (IBM Security, 2019; Verizon, 2020), none of the six cyber security risk definitions included financial valuation.

3.3.2. Comparison of Definitions Discussion

The European Network and Information Secu-
Table VIII. Comparison of third-order thematic Analysis Themes Identified in the Definition of Cyber/Information Security for US and International Standards and Best Practices

| Third-Order Theme (Expert Elicitation Interviewee Count; Percent) | MW et al., 2014 | FISMA | ISO | ITU | NICCS | NIST | CNSS | WEF |
|---------------------------------------------------------------|-----------------|-------|-----|-----|-------|------|------|-----|
| Context-driven (13; 52%)                                       |                 | x     | x   | x   | x     | x    |      |     |
| Resilient system functionality (12; 48%)                       |                 | x     | x   |     |       | x    |      |     |
| Maintenance of CIA (10; 40%)                                   |                 |       |     |     |       |      |      |     |
| Threat prediction and prevention (7; 28%)                      | (x)             |       |     |     |       | x    |      |     |
| Protection of resources (6; 24%)                               | x               |       |     |     |       | x    |      |     |
| Sociotechnical system (5; 20%)                                 | x               | x     |     |     | (x)   | x    |      | x   |
| Unattainable (4; 16%)                                          | x               |       |     |     |       |      |      |     |
| Resource management (4; 6%)                                    | (x)             | (x)   |     |     | (x)   | x    |      | x   |
| Comprehensive system awareness (3; 12%)                        |                 |       |     |     |       |      |      |     |
| Evolving security standards (3; 12%)                           |                 |       |     |     |       | (x)  |      |     |
| Iterative (and/or active) process (2; 8%)                      | (x)             | (x)   |     |     | ~     | (x)  |      |     |
| Accurate intrusion detection (2; 8%)                           |                 |       |     |     |       |      |      |     |
| Security competence (2; 8%)                                    |                 |       |     |     |       |      |      |     |
| Verifiable information provenance (2; 8%)                      |                 |       |     |     |       |      |      |     |
| Characterization and effects of human factor (2; 8%)           |                 |       |     |     |       |      |      |     |
| Diverse dimensions and factors (2; 8%)                         |                 |       |     |     |       |      |      |     |
| Quantifiable security (2; 8%)                                  |                 |       |     |     |       |      |      |     |
| Complicated (1; 4%)                                            |                 |       |     |     |       |      |      |     |
| Systemic solutions (1; 4%)                                     | X               |       |     |     |       |      |      |     |

x = Third-order theme concept and or words explicitly included in definition; (x) = third-order theme concept is implicit in definition, ~ = required assumption for definition context.

* Source of definition is not a standard or best practice, however it provides context for a nontechnical general definition.

MW, 2020: Merriam-Webster Dictionary; FISMA: United States Federal Information Security Modernization Act of 2014 (ISO, 2012; U.S. Congress, 2014); International Organization for Standardization; ITU: International Telecommunication Union, 2008, 2011; NICCS: National Initiative for Cybersecurity Careers and Studies (DHS, 2020); NIST, 2018: United States National Institute of Standards and Technology; CNSS, 2015: United States Committee on National Security Systems; WEF, 2012: World Economic Forum.
| Third-Order Theme (Expert Elicitation Interviewee Count; Percent) | MW* | Craigen et al., 2014* | FISMA | ISO | ITU | NICCS | NIST | CNSS | WEF |
|---------------------------------------------------------------|------|----------------------|------|-----|-----|-------|------|------|-----|
| Probability of outcomes (11; 41%)                            | N/A  | N/A                  | N/A  | x   | x   | (x)   | x    | x    |     |
| Impacts of CIA Vulnerabilities (10; 37%)                      |      |                      |      |     |     |       |      |      |     |
| Context-driven (6; 22%)                                       |      |                      |      |     |     |       |      |      | x   |
| Uncertainties introduced by human factors (5; 19%)            | x    |                      |      |     |     |       |      |      |     |
| Vulnerabilities (known and unknown) (4; 15%)                  |      |                      |      |     |     |       |      |      |     |
| Negative consequences (4; 15%)                                | x    |                      |      |     |     | (x)   | x    | x    |     |
| Absolute and relative resource valuation (4; 15%)             |      |                      |      |     |     |       |      |      |     |
| Monetization (3; 11%)                                        |      |                      |      |     |     |       |      |      |     |
| Negative consequences for humans (3; 11%)                     | (x)  |                      |      |     |     |       |      |      |     |
| Multiple dimensions and scales (3; 11%)                       |      |                      |      |     |     |       |      |      | x   |
| Vulnerabilities introduced by human factors (3; 11%)          | x    |                      |      |     |     |       |      |      |     |
| Classical elements of risk (3; 11%)                           |      |                      |      |     |     |       |      |      | (x) |
| Sociotechnical exploitation (2; 7%)                            | ~    |                      |      |     |     |       |      |      |     |
| Complicated (2; 7%)                                           |      |                      |      |     |     |       |      |      |     |
| Interference with physical components (2; 7%)                 |      |                      |      |     |     |       |      |      |     |
| Interference with cyber security (2; 7%)                       | (x)  |                      |      |     |     |       |      |      |     |
| Probability of vulnerability (2; 7%)                           | x    |                      |      |     |     | (x)   | x    |     |     |
| Scope of risk perception (2; 7%)                               |      |                      |      |     |     |       |      |      | x   |
| Vulnerabilities in first line of defense (1; 4%)              |      |                      |      |     |     |       |      |      |     |
| Limits of detection (1; 4%)                                   |      |                      |      |     |     |       |      |      |     |
| Risk Quantification (1; 4%)                                   |      |                      |      |     |     |       |      |      | (x) |
| Agility is paramount (1; 4%)                                  |      |                      |      |     |     |       |      |      |     |
| Agility-dependent (1; 4%)                                     |      |                      |      |     |     |       |      |      |     |
| Beyond CIA (1; 4%)                                           |      |                      |      |     |     |       |      |      |     |
| Goal dependent (1; 4%)                                        |      |                      |      |     |     |       |      |      |     |
| Multiple realms of threats (1; 4%)                            | x    |                      |      |     |     |       |      |      |     |

*Source of definition is not a standard or best practice, however it provides context for a nontechnical general definition.

MW, 2020: Merriam-Webster Dictionary; FISMA: United States Federal Information Security Modernization Act of 2014 (U.S. Congress); ISO, 2012: International Organization for Standardization; ITU: International Telecommunication Union, 2008, 2011; NICCS, 2020: National Initiative for Cybersecurity Careers and Studies; NIST, 2018: United States National Institute of Standards and Technology; CNSS, 2015: United States Committee on National Security Systems; WEF, 2012: World Economic Forum.
Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Agency (ENISA) performed a similar “cybersecurity” definition comparison to identify gaps in the standardization of the terminology (Brookson et al., 2015). The gap analysis evaluated the use and definition, or lack thereof, of cyber security as defined by the Oxford dictionary, the Merriam–Webster dictionary, European Telecommunications Standards Institute (ESTI), ISO, ITU, NIST, North Atlantic Treaty Organization (NATO), and CNSS. Despite ESTI’s cyber related activities and initiatives and NATO’s Cooperative Cyber Defence Centre of Excellence, neither organization formally defines their use of cyber security. Since cyber security is an “enveloping term,” ENISA does not recommend having a singular definition, rather that each fit-for-purpose definition is unambiguous and explicit in scope and application (Brookson et al., 2015).

Schatz, Bashroush, & Wall, 2017 computational linguistic analysis of existing definitions highlighted the common thread of CIA of information, the high-level management of networks by organizations and states, clearly refers to human users (and by implication, defenders) and the need for training of the human elements. It is an inwardly looking definition, providing a shell of protection around information assets, but does not include reference to attackers or any form of malware or “bad actors”—human or not.

Over the last 20 years the use of cyber networks has expanded from communications and control systems to become the underpinning of societal “critical infrastructure” (such as water systems controls and the electrical grid) and manufacturing as well as of social and commercial communications and interactions, and the control of small microscale Internet of Things networks. Humans are inevitable parts of the current cyber security framework, as users, defenders, and attackers. Thus, in any definition of cyber security and cyber security risk, human connection needs to be acknowledged, the inherent complexity needs to be taken into account and the dynamic nature of cyber technology and its integration into our society and social structures needs to be implied if not actually included in the definition.

4. DISCUSSION

Cyber experts from different sectors across multiple disciplines and research areas were asked via expert elicitation to define cyber security and cyber security risk. The results of the expert elicitation were analyzed using data-driven thematic analysis and content analysis and the results were compared to current national and international standards and best practices. The output of the thematic analysis was visualized using butterfly diagrams and network analysis. The use of network analysis led to additional points of analysis regarding the interconnectedness of themes across (e.g., ARL to academia) and within sectors (e.g., amongst ARL interviewees). The results suggest: (1) definitions of cyber security and cyber security risk vary across and within ARL and academic sectors, and (2) definitions of cyber security and cyber security risk differ between cyber experts and ontology developers. Furthermore, some experts had interdependent definitions of cyber security and cyber security risk, using one term to define the other.

4.1. Analysis and Interpretation Challenges

4.1.1. Interpretation Challenges

Although data-driven thematic analysis is useful in determining collective concepts associated with cyber security and cyber security risk, the analysis method is subject to the following challenges:

(1) Semistructured interviews are subject to inconsistencies in communication efficiency and senses of mutual understanding (Margaret, 1994); for example, an expert feels s/he has expressed a concept, while the interviewer may not register or interpret that concept in the analysis.

(2) Expert elicitation is a subjective measure, that is beliefs of an individual or a group of experts impact the results (O’Hagan, 2019).

(3) Thematic analysis is qualitative and vulnerable to analyst subjectivity (Usher & Strachan, 2013).

(4) The results of the expert elicitation and subsequent thematic analysis only represent those interviewed and not the entirety of the expertise domains of cyber security and cyber security risk.

In essence, the analysis of an expert elicitation is a function of both the experts’ beliefs as well as the researchers’ interpretation of the data. To reduce any researcher bias and enhance the reliability of the analysis, this analysis had three researchers independently transcribe the interviews from the interview corpus, and the thematic and network analyses used all three sets of transcriptions. Research suggests experts are less susceptible than other individuals to the bias that is exaggerated by popular media or cultural
nuances, for example the influence of peer networks as experts rely on data analysis rather than inference from hearsay (Quigley et al., 2013).

Some differences in the analysis of the two sectors (academia and ARL) were due to differences in the expert elicitation procedures. The ARL interviews were not allowed to be recorded and thus were dually transcribed in situ by the interviewer and a scribe, while the audio of the academic interviews was recorded for later transcription and verification. This procedural difference may have influenced the amount of detail retained within the definitions provided by the ARL participants, however the duplicate notetaking was intended to reduce the loss of information.

Cyber experts, like other humans, are subject to cognitive biases. Experts typically use experience and intuition to make decisions about cyber security and cyber security risk (Oltramari & Kott, 2018; Tversky & Kahneman, 1974). These biases are affected by personal judgement and experience as well as cultural influence, meaning formulations of subjective probabilities vary between individuals and across disciplines (Henrie, 2013; O’Hagan, 2019; Tversky & Kahneman, 1974). Similarly, humans often fail to incorporate numbers as probabilities into their decision-making processes, which has resulted in unclear understandings of security risk (Cox, 2008). Similarly, Oltramari and Kott (2018) determined that practitioners define cyber risk in terms of a configuration of a system instead of the probability of harm occurring. This helps explain the discrepancy between definitions and the perception of cyber security and cyber security risk.

Cyber networks, and therefore cyber security, are now inherent within all disciplines, from science through social science and even into the humanities and arts. Nonstandard definitions result in contrary or oblique uses of the language in different papers and research. When cyber security and cyber security risk are being newly considered within a broaden disciplinary scope, the lack of common definitions are even more problematic. Researchers and people applying the results can find themselves in discussions and disagreements that are based on a lack of language clarity rather than an inherent disagreement, which results in inefficient use of time and effort. As language is dynamic and evolves over time, these standard definitions can be revisited as new technology, research, application, or governance expand the use of the terms: cyber security and cyber security risk.

4.1.2. Multidisciplinary Communication Challenges

McPhillips et al. (2018) discuss the need for common terminology when addressing phenomena (in their study: extreme events) that affect and are studied by (and within) multiple disciplines in order to ensure that these complex phenomena can be managed holistically, using effective cross-disciplinary communication. Disciplinary training involves developing a set of disciplinary heuristics used to view and analyze the world. In order to communicate in a true cross disciplinary way, the team members have to get out of their own heads and away from their hard-built disciplinary heuristics (cf. O’Rourke et al, 2013). Each discipline, each disciplinary language has inherently unique biases and assumptions. For example, engineers look at a system and immediately try to simplify the system to a few critical components or at least a greatly simplified network (Harte, 1988). The first assumption is that interactions are straight-forward and easily modeled. Ecologists will also try to identify the key components that other parts of the system depend on, the drivers or keystone nodes (Suter, 2007). However, ecologists also assume that interactions are complex and both time- and population (density)-based. Creating common definitions that engender the assumptions of the different disciplines creates a communication-based common ground that acts as the nexus for effective cross-disciplinary communication (c.f. Aagaard-Hansen, 2007; Li et al., 2008; Pennington, Simpson, McConnell, Fair, & Baker, 2013)

5. CONCLUSIONS

Terminology standardization facilitates efficient communication. The results of this research suggest there is a communication gap across disciplines which can be partially bridged by developing and applying standardized language. The potential benefits associated with standardizing terminology (in this case cyber-related vocabulary) include effective laws and policies, “repeatable, mutually intelligible, comparable, and interdisciplinary research” and improved data management that facilitates searchability and usability of cyber-related research (Ramirez, 2017).

Despite the aforementioned challenges of qualitative data and thematic analysis, the present research is the first known effort to determine a cross-disciplinary working definition of cyber security and cyber security risk. While similarities can be drawn
between the composite definitions above and the National Initiative for Cybersecurity Careers and Studies definitions (DHS, 2020) for cyber security and risk, visual analysis of the thematic maps (see Figs. 1 and 2 for example) highlights both the disparate and recurrent themes that make cyber security and cyber security risk complex concepts.

Although the composite definitions presented above are not formally accepted by the greater discipline of cyber research, the definitions offer useful information regarding the current expert perceptions of cyber security and cyber security risk. Like other cyber terminology researchers (Ramirez & Choucri, 2016), we believe a standardized cyber security vocabulary starts by identifying terminology standards. The methods to conduct a comparative content analysis described in this article are useful in determining cyber experts’ baseline understanding of cyber security and cyber security risk.

Current definitions are disciplinarily narrow and do not take into account how cyber networks and therefore cyber security have infiltrated virtually all aspects of society. Multidisciplinary research fields use nuanced language influenced by the researchers’ parent discipline. Disagreements based on undefined and unspoken vocabulary meanings can result from otherwise unclarified underlying disciplinary assumptions. Therefore, using more comprehensive definitions for key actionable terms within multidisciplinary research facilitates shared understanding, respect for collaborators’ disciplinary perspective, increased productivity of multidisciplinary collaboration, and reduces unproductive linguistic obstacles to functional research.

Additionally, the third-order themes emphasize the diversity of thought across disciplines conducting cyber security and cyber security research and the ubiquity of fundamental concepts (e.g., CIA). The number of third-order themes also illustrates that the definitions of cyber security and cyber security risk cannot be distilled down to a single concept. The third-order themes also reflect cultural differences between the two sectors, academia and ARL. Academia as a culture pushes the researcher toward analysis and context consideration, whereas the cultural focus of applied cyber security specialists is on the protection against constant and dynamic threats throughout the network. Given the necessary collaboration across these sectors, it is all the more important for common definitions to encompass the use of these terms within both sectors.

We argue that:

- The current definitions of cyber security and cyber security risk are inadequate due to the lack of inclusion of human factors,
- No standardized cyber security terminology exists across disciplines, and
- Communication to develop interdisciplinary definitions for cyber security and cyber security risk is lacking.

Time is a functional aspect of cyber security and cyber security risk beyond the long-recognized vulnerabilities of CIA of information. At the time of the expert elicitation (2014) and of the recent reviews of cyber security definitions (Craigen et al., 2014; Schatz et al., 2017), the critical nature of time dependence and time windows in the cyber control of critical infrastructure and communication had not yet been acknowledged, although an ENISA guidance points out time as a critical cyber vulnerability (ENISA, 2006). Therefore, a more state-of-the-art definition would expand security objectives beyond CIA to include time control. The formalization of key terms facilitates interdisciplinary cyber risk modeling, risk communication, and ultimately improve cyber security.

Given the multidisciplinary nature of cyber security and the complexities associated with quantifying and managing cyber risk, it is important that researchers, from collaborating fields share a common understanding of what is meant by cyber security and cyber security risk. This common understanding can help move cyber security from a multidisciplinary effort to a truly interdisciplinary domain.

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 Indiana University, 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 hereon.
REFERENCES

Aagaard-Hansen, J. (2007). The challenges of cross-disciplinary research. Social Epistemology, 21(4), 425–438.

Bastian, M., Heymann, S., & Jacomy, M. (2009). Gephi: An open source software for exploring and manipulating networks. Paper presented at Third International AAAI Conference on Weblogs and Social Media, San Jose, CA. Retrieved from https://www.aaai.org/ocs/index.php/ICWSM/09/paper/view/154/1009

Blondel, V. D., Guillaume, J. L., Lambiotte, R., & Lefebvre, E. (2008). Fast unfolding of communities in large networks. Journal of Statistical Mechanics: Theory and Experiment, 2008(10), P10008.

Blumenthal-Barby, J. S., & Krieger, H. (2015). Cognitive biases and heuristics in medical decision making: A critical review using a systematic search strategy. Medical Decision Making, 35(4), 539–557.

Bowen, B. M., Devarajan, R., & Stolfo, S. (2011). Measuring the human factor of cyber security. Paper presented at 2011 IEEE International Conference on Technologies for Homeland Security (HST), Boston, MA. (230–235). IEEE. https://ieeexplore.ieee.org/document/6107876

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. Retrieved from http://doi.org/10.1191/1478088706 qp063oa

Braun, V., Clarke, V., Hayfield, N., & Terry, G. (2018). Thematic analysis. In P. Liamputtong (Ed) Handbook of research methods in health social sciences (pp. 1–18). Singapore: Springer Singapore.

Brookson, C., Cadzow, S., Eckmaier, R., Escheiwer, J., Gerber, B., Guarino, A., ... Gorniak, S. (2015). Definition of cybersecurity-gaps and overlaps in standardisation. Heraklion, ENISA. Retrieved from https://www.enisa.europa.eu/publications/definition-of-cybersecurity

Cebula, J. J., Popeck, M. E., & Young, L. R. (2014). A taxonomy of operational cyber security risks version 2 (Report No. CMU/SEI-2014-TN-006). Carnegie-Mellon University Pittsburgh Pa Software Engineering Institute. https://resources. sci.cmu.edu/library/asset-view.cfm?assetid=91013

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. Computers & Security, 56, 1–27.

Clarke, V., & Braun, V. (2014). Thematic analysis. In T. Teo (Ed.), Encyclopedia of critical psychology (pp. 1947–1952). New York: Springer.

Committee on National Security Systems (CNSS). (2015). Committee on National Security Systems (CNSS) glossary. CNSSI No. 4009. Retrieved from https://rfm.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

Cox, Jr., L. A. (2008). Some limitations of “Risk = Threat × Vulnerability × Consequence” for risk analysis of terrorist attacks. Risk Analysis, 28(6), 1749–1761. https://doi.org/10.1111/j.1539-6924.2008.01142.x

Craigien, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. Technology Innovation Management Review, 4(10), 13–21. Retrieved from http://doi.org/10.22215/timreview/835

European Network and Information Security Agency (ENISA). (2006). Proposal for a directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection. European Critical Infrastructure Directive. Retrieved from http://eur-lex.europa.eu/LexUriServ/

Gaismaier, W., & Gigerenzer, G. (2008). Statistical illiteracy undermines informed shared decision making. Zeitschrift für Ev-

idenz, Fortbildung und Qualität im Gesundheitswesen, 102(7), 411–413.

Gigerenzer, G., & Gaissmaier, W. (2011). Heuristic decision making. Annual Review of Psychology, 62, 451–482.

Harte, J. (1988). Consider a spherical cow: A course in environmental problem solving. Sausalito, CA: University Science Books.ISBN 0-935702-58-X.

Heard, N. A., Heard, N. A., & Adams, N. M. (2016). Dynamic networks and cyber-security New Jersey. Imperial College Press.ISBN 9781783269044.

Henrici, M. (2013). Cyber security risk management in the SCADA critical infrastructure environment. Engineering Management Journal, 25(2), 38–45. https://doi.org/10.1080/10429247.2013.11431973

Henshel, D., Cains, M. G., Hoffman, B., & Kelley, T. (2015). Trust as a human factor in holistic cyber security risk assessment. Procedia Manufacturing, 3, 1117–1124.

Henshel, D., Sample, C., Cains, M., & Hoffman, B. (2016). Integrating cultural factors into human factors framework and ontology for cyber attackers. In D. Nicholson (Ed.), Advances in human factors in cybersecurity (pp. 123–137). Cham, Switzerland: Springer.

IMB Security. (2019). Cost of a data breach report 2019. Retrieved from https://www.ibm.com/downloads/cas/ZBZLY7KL?_ga=2.147493559.1631301142.1592590885-1159380929.1592590885

Information Security Institute (ISI). (2014). Critical terminology foundations 2: Russia-U.S. bilateral on cybersecurity. East West Institute. Retrieved from https://www.files.ethz.ch/isn/178418/terminology2.pdf

International Organization for Standardization (ISO). (2012). Information technology – Security techniques – Guidelines for cybersecurity 4: terms and definitions. ISO/IEC 27032:2012. Retrieved from https://www.iso.org/obp/ui/?iso=std;iso-iec:27032:eD-1:v1:en

International Telecommunications Union (ITU). (2008). X.J205 Overview of cybersecurity. Series X: Data Networks, Open System Communications and Security – Telecommunication Security. Retrieved from https://www.itu.int/rec/T-REC-X.2005-200804-I

International Telecommunications Union (ITU). (2011). ITU national cybersecurity strategy guide. Retrieved from https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

Kellens, W., Terpstra, T., & De Maeyer, P. (2012). Perception and communication of flood risks: A systematic review of empirical research. Risk Analysis, 33(1), 24–49.

King, Z., Henshel, D., Flora, L., Cains, M. G., Hoffman, B., & Sample, C. (2018). Characterizing and measuring maliciousness for cybersecurity risk assessment. Frontiers in Psychology, 9(39). Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5807417/#B26

Li, X., Liu, G., Ling, A., Zhan, J., An, N., Li, L., & Sha, Y. (2008). Building a practical ontology for emergency response systems. In 2008 International Conference on Computer Science and Software Engineering (Vol. 4, 222–225). Piscataway, NJ: IEEE.

Luijff, E., Besseling, K., & De Graaf, P. (2013). Nineteen national cybersecurity strategies. International Journal of Critical Infrastructures 6, 9(1–2), 3–31.

Manoj, B., & Baker, A. (2007). Communication challenges in emergency response. Communications of the ACM, 50(3), 51–53.

Margaret, T. (1994). Establishing mutual understanding in systems engineering and designation of European Critical Infrastructure and emergency response. (pp. 1–18). Singapore: Springer Singapore.

McPhillips, L. E., Chang, H., Chester, M. V., Depietri, Y., Friedman, E., Grimm, N. B., ... Shafei Shiva, J. (2018). Defining extreme events: A cross-disciplinary review. Earth’s Future, 6(3), 441–455.
Defining Cyber Security and Cyber Security Risk within a Multidisciplinary 1669

Merriam-Webster Dictionary (MW). (2020). Cybersecurity. Retrieved from https://www.merriam-webster.com/dictionary/cybersecurity.

Mittu, R., & Lawless, W. F. (2015). Human factors in cybersecurity and the role for AI. In Palo Alto, California, USA: 2015 AAAI Spring Symposium Series. https://www.aaai.org/ocs/index.php/SSS/SSS15/paper/view/10248/10054

National Institute of Standards and Technology (NIST). (2018). Framework for improving critical infrastructure cybersecurity. Version 1.1. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP04162018.pdf

O’Hagan, A. (2019). Expert knowledge elicitation: Subjective but scientific. The American Statistician, 73(1), 69–81. https://doi.org/10.1080/00031305.2018.1518265

Oltramari, A., & Kott, A. (2018). Towards a reconceptualisation of cyber risk: An empirical and ontological study. Journal of Information Warfare, 17(1). arXiv preprint arXiv:1806.08349.

Oltramari, A., Henshel, D. S., Cains, M., & Hoffman, B. (2015). Towards a human factors ontology for cyber security. Proceedings of the Tenth Conference on Semantic Technology for Intelligence, Defense, and Security, Fairfax, VA. pp 26–33. http://ceur-ws.org/Vol-1523/STIDS_2015_T04_Oltramari_etal.pdf

O’Rourke, M., Crowley, S., Eigenbrode, S. D., & Wulfhorst, J. D. (Eds.). (2013). Information Intelligence, Defense, and Security, Fairfax, VA. pp 26–33. http://ceur-ws.org/Vol-1523/STIDS_2015_T04_Oltramari_etal.pdf

Pennington, D. D., Simpson, G. L., McConnell, M. S., Fair, J. M., & Baker, R. J. (2013). Transdisciplinary research, transformative learning, and transformative science. Bioscience, 63(7), 564–573. https://doi.org/10.1525/bio.2013.63.7.9

Quigley, K., Burns, C., & Stallard, K. (2013). Communicating effectively about cyber-security risks: Probabilities, peer networks and a longer term education program. Halifax, NS: Critical Infrastructure Protection Initiative, Dalhousie University. http://cip.management.dal.ca/wp-content/uploads/2013/04/Quigley-Burns-Stallard-Cyber-Security-Paper-Final-1.pdf

Ramirez, R. B. (2017). Making cyber security interdisciplinary: Recommendations for a novel curriculum and terminology harmonization (Thesis, Massachusetts Institute of Technology). http://hdl.handle.net/1721.1/111232

Ramirez, R., & Choucri, N. (2016). Improving interdisciplinary communication with standardized cyber security terminology: A literature review. IEEE Access, 4, 2216–2243.

Reader, T. W., Flin, R., Mearms, K., & Cuthbertson, B. H. (2007). Interdisciplinary communication in the intensive care unit. British Journal of Anaesthesia, 98(3), 347–352.

Roberts, C. W. (2000). A conceptual framework for quantitative text analysis. Quality and Quantity, 34(3), 259–274.

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. Journal of Digital Forensics, Security and Law, 12(2), 53–74.

Sladek, R. M., Bond, M. J., & Phillips, P. A. (2010). Do doctors, nurses and managers have different thinking styles? Australian Health Review, 34(3), 375–380.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1982). Why study risk perception? Risk Analysis, 2(2), 83–93.

Stemler, S. (2001). An overview of content analysis. Practical Assessment, Research & Evaluation, 7(17), 137–146.

Suter, I. G. W. (2007). Ecological risk assessment (2nd ed.). Baton Rouge, FL: CRC Press.

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. Science, 185(4157), 1124–1131.

U.S. Army Research Laboratory (ARL). (2013). Cyber security research alliance. Retrieved from https://www.arl.army.mil/www/default.cfm?page=1417

U.S. Congress (2014). Federal Information Security Modernization Act of 2014. Public Law 113–283. 113th Congress. Retrieved from https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

U.S. Department of Homeland Security (DHS). (2020). National Initiative for Cybersecurity Careers and Studies. Glossary. Retrieved from https://nics.us-cert.gov/glossary

Usher, W., & Strachan, N. (2013). An expert elicitation of climate, energy and economic uncertainties. Energy Policy, 61, 811–821. https://doi.org/10.1016/j.enpol.2013.06.110

Verizon. (2020). 2020 Data breach investigations report. Retrieved from https://www.ericsson.com/res/docs/2020-data-breach-investigations-report.pdf

von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102.

World Economic Forum (WEF). (2012). Partnering for cyber resilience. Retrieved from http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf

Xu, S. (2019). Cybersecurity dynamics: A foundation for the science of cybersecurity. In C. Wang & Z. Lu (Eds.) Proactive and dynamic network defense (pp. 1–31). Cham, Switzerland: Springer.

Zinn, J. (2006). Risk as an interdisciplinary research area. Risk in Social Science, 1, 20–53. Retrieved from http://hdl.handle.net/11345/28526

SUPPORTING INFORMATION

Additional supporting information may be found online in the Supporting Information section at the end of the article.

Table SI. First-order themes from responses to “What is your definition of cyber security?”

Table SII. Second-order themes from responses to “What is your definition of cyber security?”

Table SIII. Third-order themes from responses to “What is your definition of cyber security?”

Table SIV. First-order themes from responses to “What is your definition of cyber security risk?”

Table SV. Second-order themes from responses to “What is your definition of cyber security risk?”

Table SVI. Third-order themes from responses to “What is your definition of cyber security risk?”

Table SVII. Cross-tabulation of interviewees by discipline per cybersecurity third-order theme.

Table SVIII. Cross-tabulation of interviewees per discipline per cybersecurity risk third-order theme.