Analyzing Cybersecurity Definitions for Non-experts

Lorenzo Neil[1][0009−0001−3084−7451], Julie M. Haney[2][0000−0002−6017−9693], Kerrianne Buchanan[2][0000−0002−2735−8809], and Charlotte Healy[3]

[1] North Carolina State University, Raleigh, NC, USA
lcneil@ncsu.edu
[2] National Institute of Standards and Technology, Gaithersburg, MD, USA
{julie.haney, kerrianne.buchanan}@nist.gov
[3] University of Maryland, College Park, MD, USA
chealy@umd.edu

Abstract. Current definitions of cybersecurity are not standardized and are often targeted towards cybersecurity experts and academics. There has been little evaluation about the appropriateness and understandability of these definitions for non-experts (individuals without cybersecurity expertise). This poses a challenge for practitioners and researchers when trying to communicate the meaning and importance of cybersecurity to non-experts. We take an initial step towards addressing this challenge by building a corpus of cybersecurity definitions likely to be encountered by non-experts, unlike prior efforts that only consider definitions from authoritative sources. We observed several issues that may impede non-experts' understanding, including cybersecurity definitions: being inconsistent in describing what cybersecurity is and does; often using overly-technical terminology; and varying greatly in the components of cybersecurity (e.g., objects of protection, who is responsible, threats) included in the definitions. Our findings illustrate the full landscape of cybersecurity definitions and provide a basis for investigating which definitions and terminology may be best for non-experts.

Keywords: cybersecurity · definitions · non-experts.

1 Introduction

Despite the importance of cybersecurity, there is no standard definition for this term [14,23]. Moreover, since existing definitions largely target professionals with expertise in cybersecurity [11,23], there is little understanding of what definitions may be most useful for explaining cybersecurity to non-experts (those without cybersecurity proficiency). This may pose a challenge for security practitioners and researchers when trying to communicate the meaning and importance of cybersecurity to non-experts, including general public users, organizational employees, and small businesses that lack dedicated information technology (IT) or cybersecurity staff [12,22].

Our own initial exposure to this challenge occurred during research experiences investigating people's cybersecurity perceptions and behaviors. Repeatedly, we struggled to find a standard cybersecurity definition appropriate for non-experts for use within our own interview and survey protocols. For example, in one survey, we developed a series of questions about cybersecurity concerns followed by a similar set about privacy concerns. To differentiate the two concepts and ensure that participants understood the focus of the questioning and provided relevant responses, we wished to define both cybersecurity and privacy in the survey. However, when we searched for cybersecurity definitions, we found that many used highly technical language that may not be suitable for our general public audience or was incomplete or limited (e.g., only mentioning cybersecurity in the context of financially-motivated cyber crime). These observations were supported by other researchers who highlighted the inconsistency in cybersecurity terminology [2,14,22]. The use of technical jargon not familiar to lay people is further indicative of communications and translation gaps between experts and non-experts and the consequences of those (e.g., loss of interest and motivation, not being able to take appropriate action) in cybersecurity [15,19,20] and other technical and scientific [7,24] contexts.

This issue's relevance goes beyond a research application. The importance of defining and describing cybersecurity in terms understandable to non-experts extends into people's everyday encounters with technology and online services and their cybersecurity responsibilities [15]. Therefore, for the practitioners who ultimately communicate cybersecurity concepts to non-experts, it is imperative to understand which terms used within definitions may potentially be unfamiliar, unclear, or incomplete to their audience and, therefore, may necessitate additional explanation or a different choice of terminology.

Researchers have addressed the lack of consistency in cybersecurity definitions by analyzing cybersecurity definitions from authoritative sources (e.g., standards bodies, governments) [6,16] and, sometimes, developing their own composite definitions [9,11,23]. However, these efforts were typically targeted at an audience of cybersecurity and IT practitioners or academics. To the best of our knowledge, no definitions have been thoroughly evaluated for their appropriateness to individuals with limited or no cybersecurity expertise.

In the study presented in this paper, we take an initial step toward addressing this gap. Before evaluating definitions, we first needed to survey the current corpus of definitions available to non-experts. To that end, we performed a systematic search and analysis of publicly available, online cybersecurity definitions to investigate the following research questions (RQs):

RQ1: What terms and components (e.g., references to threats, security principles, and objects protected by cybersecurity) are commonly included in cybersecurity definitions likely to be accessed by non-experts?

RQ2: How do cybersecurity definitions differ depending on their source type?

Our study makes several contributions. Our findings – for the first time – illustrate the full landscape of cybersecurity definitions, not just the authoritative definitions intended for experts. Differing from prior research that analyzed

themes or relied on expert elicitation (e.g., [9,11]), we conducted a novel analysis of the components frequently used to define cybersecurity and provide new insights into statistically significant differences among distinct types of definition sources. This more comprehensive picture can be used as a basis to: 1) evaluate the appropriateness of current definitions and common cybersecurity terminology used in those definitions for a non-expert audience, 2) identify potential cybersecurity concepts and terminology causing confusion to non-experts, and 3) offer guidance for cybersecurity practitioners and researchers when communicating to non-experts.

2 Related Work

2.1 Non-Experts and Cybersecurity

Cybersecurity is a term that people who use technology have likely heard of, yet may understand differently [3,8,10,30]. As compared to cybersecurity experts, non-experts often rely on multiple mental models that may be incomplete, inaccurate, oversimplified, or contradictory [3,10,21,27]. These misconceptions can lead to non-experts taking inadequate cybersecurity actions [5,8]. For example, Theofanos et al. [27] discovered that non-experts' ill-informed mental models contributed to their avoidant and reactive approach to cybersecurity. Similarly, Wash [30] found that untrained users use mental models to justify ignoring computer security experts' advice; without an accurate and complete understanding of security threats, non-experts choose to ignore advice that they do not believe will help them. Emami et al. [13] showed that Internet of Things users' limited and often incomplete knowledge about cybersecurity impacted their ability to make informed security decisions.

Misconceptions may be partially rooted in a failure of experts to describe cybersecurity in non-technical terms, as exemplified by DiStaso et al. [12], who highlighted how organizations fail to perceive cybersecurity as a communications challenge and mostly only consider it from an information technology angle. Furthermore, when organizations engage in security risk communications, they use a technocratic approach by broadcasting facts to general audiences, which has been criticized as ineffective and inefficient [25]. Often experts use jargon in communication with non-experts, which Bullock et al. [7] found significantly affects lay persons' processing fluency, the ease or difficulty with which information is processed, and therefore affects their conceptions of and support for emerging science and technologies. Shulman et al. [24] confirmed these findings and discovered that the use of jargon's negative effect on processing fluency and comprehension was not mitigated by providing definitions and explanations to technical language.

2.2 Cybersecurity Definitions

Even for experts, the definition and scope of cybersecurity vary widely across sources. The European Union Agency for Cybersecurity [6] analyzed the use

of the cybersecurity term by various stakeholders, concluding that there are marked differences and gaps among available standards. Luiif et al. [16] compared 18 national cybersecurity strategies, of which only ten either define or describe cybersecurity. Some nations define cybersecurity as information security properties to be safeguarded. Other nations cite protection against threats from cyberspace or use descriptive text rather than a concise definition.

Closely-related concepts may also be incorrectly equated to cybersecurity. For example, Azmi et al. [4] and von Solms et al. [28] highlighted the confusion between *cybersecurity* and *information security,* which are often used interchangeably but are not completely analogous. Specifically, cybersecurity goes beyond the boundaries of traditional information security – protecting information resources – to also include the protection of digital assets and identities.

Several researchers attempted to address inconsistencies in cybersecurity definitions by proposing their own definitions. Craigen et al. [11] crafted a new definition after identifying a subset of nine cybersecurity definitions via an academic literature search and conducting group discussions with cybersecurity practitioners, academics, and graduate students. Cains et al. [9] developed a composite definition of cybersecurity after interviewing cybersecurity researchers and professionals and identifying overarching themes (e.g., "bad use or attacker," "machines are easier than humans") expressed in the experts' own definitions. Schatz et al. [23] analyzed 28 definitions from authoritative sources by calculating word frequencies, correlations between terms, and semantic similarities to develop a representative cybersecurity definition. New definitions have also been considered for other related concepts. For example, Wang et al. [29] performed an in-depth literature survey and Google search of definitions of social engineering to propose a definition that reduced conceptual inconsistencies.

Since new definitions generated from these research efforts were based on a small subset of authoritative and expert definitions and were targeted at cybersecurity practitioners and academics, it remains unclear if they would be meaningful to non-experts. Moreover, these are not necessarily definitions that would be viewed by non-experts (e.g., from a Google search). Our work is differentiated from these prior efforts in our focus on definitions most likely to be accessed by non-experts, regardless of authoritativeness of the source. Also, our study focuses more on the individual terms and components that are commonly used within cybersecurity definitions. These insights can serve as a basis for developing guidance to help clarify cybersecurity concepts to non-experts.

3 Methods

3.1 Systematic Search

From September-November 2022, we performed a systematic search to find cybersecurity definitions. We first conducted searches in Google and research databases (IEEE, ACM, Engineering Village, and Web of Science). To capture recent portrayals of cybersecurity, we searched for sources from the prior five

years (2017 – 2022). We used the following queries in Google searches: cybersecurity AROUND(3) definition; cybersecurity AROUND(3) "what is"; cybersecurity AROUND(3) glossary. We also substituted "cyber security" for "cybersecurity" in the search terms to account for different spelling conventions. We captured the first 50 Google search results for each query plus sources referenced in the initial "People also search" items on the first page of the web search results. For the research databases, we used similar queries tailored to the query language of each database. We then conducted backwards reference crawling from identified research sources, not limiting these sources to the last five years but attempting to find the most recent updates of documents since being cited. For all search sources, we applied the following inclusion and exclusion criteria:

Inclusion criteria:

- Sources available in English
- Sources clearly intended to provide an explicit definition of cybersecurity [23]
- Sources we could access from our institutional computers

Exclusion criteria:

- Sources that provided no clear or explicit definition of cybersecurity [23]
- Sources that only defined terms or concepts other than cybersecurity, for example information security, cybersecurity risk, or social engineering
- For research sources: sources that only contained definitions from other backwards references already included in the corpus
- Duplicate definitions already included in the corpus

In contrast to prior efforts to identify and characterize cybersecurity definitions [6,11,16,23], we did not exclude sources that lacked peer review or authority (e.g., from governmental or respected professional bodies) because we wished to examine definitions that non-experts would be able to readily access, regardless of source credibility.

Figure 1 shows our systematic search process and the number of sources emerging from each step. Our final corpus consisted of ***152 sources containing 167 distinct definitions***. We further classified each definition as being from one of six source types, which are described in Table 1.

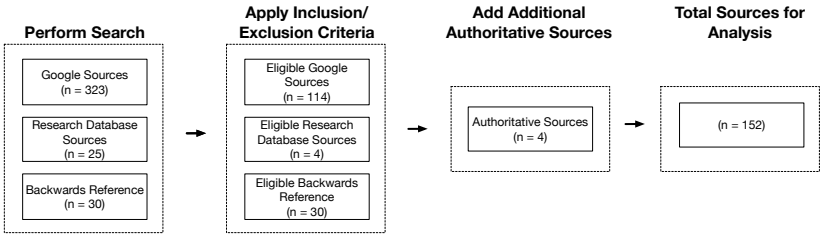

Fig. 1. Systematic search process

Table 1. Source types and number of definitions (n) in each.

Type	Description	n (%)
Education	an educational (.edu) organization (e.g., a university offering a cybersecurity degree) but not based on research content	8 (5%)
General	a general domain website for information, such as a dictionary or encyclopedia	6 (4%)
Government	a national or international government body or agency	36 (21%)
Industry	a company, industry forum, or non-profit organization	107 (64%)
Research	a research institution such as a university, with source content within a research context	8 (5%)
Standards	a national or international standards organization	2 (1%)

3.2 Analysis

Coding. We examined each source's "core definition," which most often was one sentence succinctly answering the question "what is cybersecurity?" Although many sources contained additional details or descriptions of cybersecurity, we scoped our analysis to only the core definitions.

When first conceptualizing our study, we compiled an initial set of cybersecurity definitions from research papers and government documents. We met as a team several times to discuss the definitions, components of the definitions (e.g., action words, mentions of threats, objects/assets protected by cybersecurity), and how we might analyze these. During these discussions, we developed a list of definition components. Once we performed our systematic search and finalized a corpus, we used this list of components as the basis for an initial codebook to conduct qualitative coding of the core definitions.

In our coding process, we started with a set of 25 definitions that two researchers coded individually. The researchers then met to discuss code application, resolve coding conflicts, and refine the codebook. The two researchers then individually coded a second set of 25 definitions, again meeting to discuss coding conflicts. In this round, we achieved a Cohen's Kappa inter-rater reliability score of 0.95, which is considered almost perfect agreement [18]. We then divided the remaining definitions between the two researchers for coding. The final codebook for the definitions included the seven codes shown in Table 2.

Statistical Analysis. We calculated descriptive statistics to determine the frequency of each coded component in the cybersecurity definitions in our corpus. We also examined word frequencies to see if there were patterns in words across definitions as well as those used for each type of definition component. Word frequencies considered stemmed words (e.g., protect, protection).

We performed inferential statistics using R to determine if the types of coding categories applied to each definition differed depending on the definition's source type. Because the small number of definitions in some source types (e.g., Standards) prevented us from performing statistical analysis for all six source

Table 2. Definition codes (components)

Code	Description
Action	answers the question of what cybersecurity does in general
How	cybersecurity actions taken
Object	what the action is taken on
Security Principles	tenets of cybersecurity
Threats	mentions of actors involved in cyber attacks, cyber risks, or means by which cybersecurity can be compromised
What	the thing(s) that cybersecurity is
Who	the actor(s) responsible for cybersecurity practices

groups, we collapsed the sources into two categories: ***institutional*** (research, standards, government, education, general) and ***industry***. We conducted Chi-Square analyses, crossing each of the seven components with the two source types with a significance level of $p < 0.05$. In cases where the expected frequencies were insufficient to conduct a Chi-Square test, we computed the Fisher's Exact Test [1]. We also report Cramer's V effect size for which less than 0.3 is a small effect, 0.3 - 0.7 is a medium effect, and over 0.7 is a large effect [26].

4 Results

We describe commonly referenced words and provide examples of trends in coded phrases across all definitions and then for each definition component, including source IDs for quoted definitions[4]. Source IDs beginning with *R* (e.g., R6) are from our initial academic paper database search, IDs beginning with *B* are from the backwards searching, and IDs beginning with *G* are from the Google searches. When applicable, we provide counts in parentheses to indicate the number of definitions containing a word. We also report significant statistical analysis to compare definition composition across institutional and industry sources.

4.1 Word Frequencies and Trends

All Definitions. The top five words occurring across all definitions were: *protect* (112 definitions), *systems* (83), *networks* (82), *data* (81), and *attacks* (75). Some cybersecurity definitions were quite short: "*preservation of confidentiality, integrity and availability in the Cyberspace*" (B4) and "*the practice of protecting sensitive data and IT networks from unauthorized access and cyber attacks*" (GJ137). Other definitions were longer. For example, an industry definition found through a Google search was "*the safeguarding of computer systems and networks against information disclosure, theft or damage to their hardware, software, or electronic data, as well as disruption or misdirection of the services they provide*" (GL28). A U.S. Government source defined cybersecurity as "*an approach*

[4] Definition source list available at: https://bit.ly/42HGWLI.

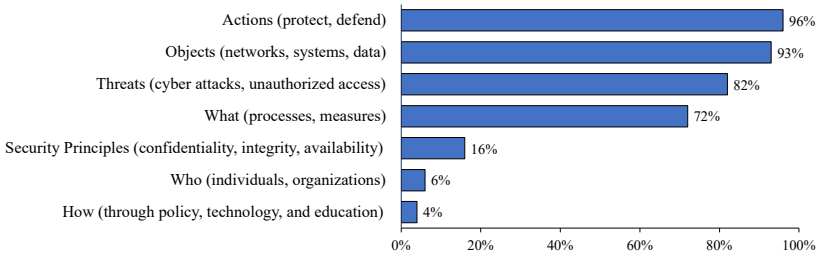

Fig. 2. Percentage of definitions with each component (n = 167 definitions). Examples of words and phrases included in each component are provided within parentheses.

or series of steps to prevent or manage the risk of damage to, unauthorized use of, exploitation of, and—if needed—to restore electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity, and availability of these systems" (GJ117).

We found varying technical complexity within the definitions. A source specifically targeted at individuals and families simply defined cybersecurity as "*the means by which individuals and organisations reduce the risk of being affected by cyber crime*" (A1). A website providing information for small businesses said that cybersecurity is "*protecting individual computer systems and networks from cyber-attacks*" (GJ88). Other definitions used technical jargon, for example, "*the process of protecting information and information systems by preventing, detecting, and responding to unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability*" (B12). Fifteen definitions contained the term *cyberspace*. One definition, crafted after analysis of other cybersecurity definitions, contained language not in the common vernacular: "*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*" (R4).

We further explored the percentages of definitions containing each of the seven components (see Fig. 2). Over 90% of definitions had an Action or Object component. Over 70% had Threats or What components. Few included Who and How components.

Actions. For the Actions code, the most commonly used word was *protect* (or variation like *protection*), which was mentioned 141 times in the Actions-coded text. Other action words were used less frequently, with *defend* (21 instances), *prevention* (14), *safeguard* (14), and *securing* (14) rounding out the top five. While many definitions had a single action word, a few included multiple words, for example, "*preventing, detecting, and responding*" (B12) and "*responding to and recovering from*" (B23).

How. Only six definitions contained a component describing how cybersecurity is enacted. The word *network* was present in four of these. The text coded as

How ranged from high-level (e.g., "*through policy, technology, and education*" (B6)) to more comprehensive (e.g., "*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*" (GJ8)). We also observed that the How component, although not common in the core definitions, was often expanded upon in other sections of the web sources, most often as a list of good cybersecurity practices.

Objects. The top five words in our Objects code were *data* (105 instances), *systems* (99), *networks* (97), *computer* (68), and *information* (62). Most definitions included both a system and data component, for example, "*computer systems, networks and data*" (GL109) and "*internet-connected systems (to include hardware, software, and associated infrastructure), the data on them, and the services they provide*" (GJ132). However, eight definitions limited cybersecurity to being for systems only (e.g., "*a computer or computer system*" (B2)). Seven definitions only mentioned information or data (e.g., " *information during collection, transit, exchange and storage*" (B9)), which is in line with the related, but different definition of information security [23]. Furthermore, four definitions only included the more generic objects *cyberspace* or *cyber assets*.

Security Principles. The most frequently mentioned tenets of cybersecurity were *integrity* (36 instances), *confidentiality* (33), and *availability* (30). For example, an industry source defined cybersecurity as the "*collective methods, technologies, and processes that help protect the confidentiality, integrity, and connectivity of computer systems, networks and data, against cyber-attacks or unauthorized access*" (GL109). All other words (e.g., *nonrepudiation*, *authentication*) appeared no more than five times, as in IEEE's Cybersecurity Glossary definition, "*the availability, integrity, authentication, confidentiality, and nonrepudiation of electronic communications*" (R16). Interestingly, while the components of the well-known CIA triad (confidentiality, integrity, availability) were usually mentioned together, this was not always the case, with the word *integrity* being more likely to be referenced on its own.

Threats. The top five words in Threats were *attacks* (89 instances), *access* (69), *unauthorized* (61), *cyber* (38), and *malicious* (28). Threats were often generally mentioned as *unauthorized access, cyber attacks*, or "*malicious digital attacks*" (GJ75). Other definitions clarified what was meant by cyber attacks within the cybersecurity definition itself: "*cyber attacks, which refer to attacks that target an institution's IT systems and networks with an aim to disrupt, disable, destroy or maliciously control an IT system/network, to destroy the integrity of the institution's data, or to steal information from it*" (B9). Some included specifics about unauthorized use, such as "*unauthorized disclosure, modification or destruction*" (B16). The types of cyber actors were briefly described in several definitions: "*electronic attacks by nefarious actors such as hackers, spammers, and cybercriminals*" (GJ62). Most focused on intentional actions taken by "*malicious*" actors without acknowledging unintentional threats due to negligence or

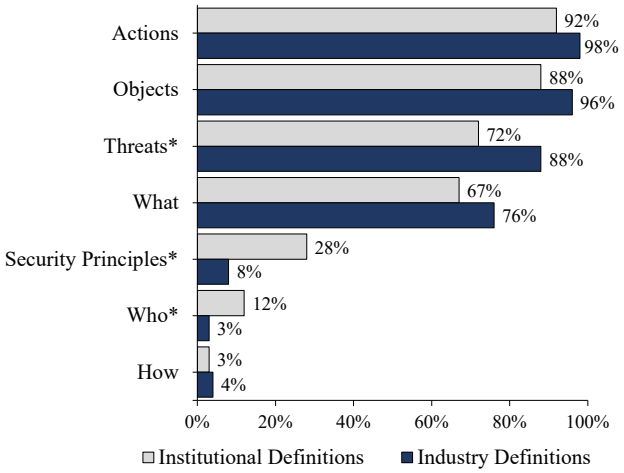

Fig. 3. Percentage of institutional definitions (n = 60) and industry (n = 107) per definition component. * indicates a statistically significant difference between the Institutional and Industry definitions.

accidents. Finally, threats were sometimes described in relation to security principles, for example, "*events in cyberspace that may compromise the availability, integrity or confidentiality of data*" (B11).

What. Cybersecurity was most frequently described as a *practice* (59 instances), a *process* or *set of processes* (43), *technologies* (36), or *measures* (25). Most often the What component was shorter (e.g., "*the state of*" (GJ1) and "*the entirety of measures*" (B20)). However, over 30 definitions described the What as being multi-faceted, for example: "*the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies*" (B5).

Who. Only 10 definitions included a Who component to indicate which entity is responsible for cybersecurity. Eight mentioned *organisations/organizations*, *business* or *company*, for example, "*a process that enables organizations to protect their applications, data, programs, networks, and systems from cyberattacks and unauthorized access*" (GJ33). Five included *individuals*. Three definitions mentioned both *individuals and organizations*: "*how individuals and organisations reduce the risk of cyber attack*" (GJ55).

4.2 Source Type Differences

Fig. 3 shows the percentages of industry and institutional definitions having each component. While 12% of institutional definitions had a Who component, only 3% of industry definitions did. This difference was significant (Fisher Exact,

Cramer's V = 0.18). Over a fourth of the institutional definitions had Security Principles (28%), but only 8% of industry definitions did, which was also significant ($\chi^2 = 11.61$, degrees of freedom = 1, V = 0.26). Significantly more industry definitions were coded as having Threats in the definitions compared to institutional definitions ($\chi^2 = 6.83$, df = 1, V = 0.20), though over 70% of both source types had Threats coded in their definitions. There were no significant differences for Actions, How, What, or Objects components.

5 Discussion

In this section, we discuss our results for each research question and then offer ideas for how this initial research can be leveraged to further explore the appropriateness of cybersecurity definitions for non-experts.

5.1 RQ1: Terms and Components Commonly Used in Definitions

Similar to prior definitions analysis efforts (e.g., [4,6]) we found that cybersecurity definitions are inconsistent in their components and terminology. We extend this prior work by analyzing and offering insights into the components of these definitions. Most definitions were action-oriented, mentioning words such as *protect*. However, it was unclear who is doing the protecting or how they are protecting. Because of this omission, non-experts may not recognize that they have responsibility for cybersecurity if the "who" is not identified. Additionally, most definitions only use the generic term *protect* and have inconsistent descriptions of what cybersecurity is (e.g., a set of processes and technologies). Threats were often referenced generically or only included one type of threat. For example, reducing cyber threats simply to "*cyber crime*" (A1) fails to account for other threats, such as nation-states, hacktivism, or terrorism. These observations suggest that existing definitions may be limited, leaving non-experts unaware of how to appropriately protect themselves from all relevant threats.

Considering the Related Work in section 2.1 that identified non-experts' struggles with cybersecurity concepts and jargon, we also observed multiple terms that may be difficult for non-experts to understand. For example, it is unclear as to how non-experts understand generic terms such as *cyber* or *cyberspace*, an issue also highlighted in Azmi et al. [4]. Another example is the CIA triad (confidentiality, integrity, and availability) frequently used in definitions. While people may be familiar with terms such as integrity and availability in the course of daily life, they may not have a good understanding of what these mean in the cybersecurity context. In addition, Lundgren et al. [17] questioned the appropriateness of using the triad in a definition since it may be more useful in describing security goals.

5.2 RQ2: Differences Based on Source Type

In contrast to prior work that largely considered authoritative definitions and performed no source analysis [6,9,11,16,23], we uniquely identified differences

between industry and institutional definitions. Industry definitions are more threat-focused. This may be the case because the definitions were largely from vendors of security products that directly respond to threats. Institutional definitions were more likely to include security principles, which may be because these sources are typically more formal and reliant on standards. However, we note that, since there were no differences for the Action and Object components, this may positively indicate that institutional and industry sources do have substantial overlap and that the areas of difference may have more to do with the audiences that consult those types of sources.

5.3 Future Work

Our findings can be used as a basis for future work that identifies best practices for how to communicate cybersecurity concepts and terminology to non-expert audiences in ways that are meaningful and easily understandable to them. Future research can test for non-experts' understanding of frequently-used terms in definitions (e.g., *cyberspace*, *integrity*). These efforts could also examine which components should be included in a cybersecurity definition to best aid non-experts in their understanding.

Other investigations could address some of the limitations of our study. We did not evaluate if the definitions we found and the components they contained were correct. Future research should seek to use terminology and components that are both easy to understand and technically correct. Also, beyond the core definitions, we did not analyze the additional information included in many of the industry Google web sources. This information likely can help non-experts better understand what cybersecurity is, for example, through more detailed examples of cybersecurity protections and threats. Future work may include analysis of the types of additional information (e.g., best practices, components of cybersecurity, threats), the complexity (e.g., measured via reading level scores), and the tone (e.g., measured via sentiment analysis). In addition, in many cases, it was difficult to determine the target audience of the definition, especially for sources found via Google web searches; therefore, we were not able to conduct an analysis comparing definitions based on audience. Future investigations could analyze definitions with known audiences to identify potential differences.

6 Conclusion

We conducted a systematic search of cybersecurity definitions non-experts are likely to encounter, rather than only focusing on authoritative and organizationally-focused cybersecurity definitions explored in prior work [6,11,16,23]. We analyzed the definitions in a novel way, using qualitative coding to identify the components of the definitions and comparing definitions from institutional and industry sources. By building and analyzing this corpus of definitions, we provide a foundation for future research to identify potential areas of confusion or inconsistencies that may impact non-experts' understanding so as to guide cybersecurity researcher and practitioner communications to non-experts.

Disclaimer

Identification of commercial companies or products in this paper is to foster understanding and does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that these are necessarily the best available for the purpose.

Acknowledgements

This material is based upon work supported by the North Carolina State University NIST Graduate Student Measurement Science and Engineering Fellowship Program under Award Number 70NANB21H090 and the University of Maryland NIST Professional Research Experience Program under Award Number 70NANB18H165.

References

1. Agresti, A.: An introduction to categorical data analysis. John Wiley & Sons, Inc, Hoboken, NJ, 3rd edn. (2018)
2. Althonayan, A., Andronache, A.: Shifting from information security towards a cybersecurity paradigm. In: Proceedings of the 2018 10th International Conference on Information Management and Engineering. pp. 68–79 (2018)
3. Asgharpour, F., Liu, D., Camp, L.J.: Mental models of security risks. In: Financial Cryptography and Data Security: 11th International Conference (FC 2007) and 1st International Workshop on Usable Security (USEC 2007). pp. 367–377 (2007)
4. Azmi, R., et al.: Revisiting cyber definition. In: European Conference on Cyber Warfare and Security. pp. 22–30. Academic Conferences International Limited (2019)
5. Bravo-Lillo, C., Cranor, L., Downs, J., Komanduri, S.: Bridging the gap in computer security warnings: A mental model approach. IEEE Security & Privacy **9**, 18 – 26 (2011)
6. Brookson, C., Cadzow, S., Eckmaier, R., Eschweiler, J., Gerber, B., Guarino, A., Rannenberg, K., Shamah, J., Górniak, S.: Definition of cybersecurity-gaps and overlaps in standardisation. Heraklion, ENISA (2015)
7. Bullock, O.M., Amill, D.C., Shulman, H.C., Dixon, G.N.: Jargon as a barrier to effective science communication: Evidence from metacognition. Public Understanding of Science **28**(7), 845–853 (2019)
8. Busse, K., Schäfer, J., Smith, M.: Replication: '. . . no one can hack my mind' - revisiting a study on expert and non-expert security practices and advice. In: Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019). pp. 117–136 (2019)
9. Cains, M.G., Flora, L., Taber, D., King, Z., Henshel, D.S.: Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. Risk Analysis **42**(8), 1643–1669 (2022)
10. Camp, L.J., Asgharpour, F., Liu, D.: Experimental evaluations of expert and non-expert computer users' mental models of security risks. In: Proceedings of the Workshop on the Econonomics of Information Security (WEIS 2012). pp. 1–24 (2012)

11. Craigen, D., Diakun-Thibault, N., Purse, R.: Defining cybersecurity. Technology Innovation Management Review **4**(10) (2014)
12. DiStaso, M.W.: Communication challenges in cybersecurity. Journal of Communication Technology **1**(1), 43–60 (2018)
13. Emami-Naeini, P., Dixon, H., Agarwal, Y., Cranor, L.F.: Exploring how privacy and security factor into iot device purchase behavior. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. pp. 1–12 (2019)
14. Furnell, S., Collins, E.: Cyber security: what are we talking about? Computer Fraud & Security **2021**(7), 6–11 (2021)
15. Haney, J.M., Lutters, W.G.: 'It's scary... it's confusing... it's dull': How cybersecurity advocates overcome negative perceptions of security. In: 2018 Symposium on Usable Privacy and Security. pp. 411–425 (2018)
16. Luiijf, E., Besseling, K., De Graaf, P.: Nineteen national cyber security strategies. International Journal of Critical Infrastructures 6 **9**(1-2), 3–31 (2013)
17. Lundgren, B., Möller, N.: Defining information security. Science and engineering ethics **25**, 419–441 (2019)
18. McHugh, M.L.: Interrater reliability: the kappa statistic. Biochemia Medica **22**(3), 276–282 (2012)
19. Nicholson, J., Coventry, L., Briggs, P.: 'If it's important it will be a headline' cybersecurity information seeking in older adults. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. pp. 1–11 (2019)
20. Nurse, J.R., Creese, S., Goldsmith, M., Lamberts, K.: Trustworthy and effective communication of cybersecurity risks: A review. In: 2011 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST). pp. 60–68 (2011)
21. Prettyman, S.S., Furman, S., Theofanos, M., Stanton, B.: Privacy and security in the brave new world: The use of multiple mental models. In: Intl Conference on Human Aspects of Information Security, Privacy, and Trust. pp. 260–270 (2015)
22. Renaud, K., Weir, G.R.: Cybersecurity and the unbearability of uncertainty. In: 2016 IEEE Cybersecurity and Cyberforensics Conference (CCC). pp. 137–143 (2016)
23. Schatz, D., Bashroush, R., Wall, J.: Towards a more representative definition of cyber security. Journal of Digital Forensics, Security and Law **12**(2), 8 (2017)
24. Shulman, H.C., Dixon, G.N., Bullock, O.M., Amill, D.C.: The effects of jargon on processing fluency, self-perceptions, and scientific engagement. Journal of Language and Social Psychology **39**(5-6), 579–597 (2020)
25. Stewart, G., Lacey, D.: Death by a thousand facts: Criticising the technocratic approach to information security awareness. Information Management & Computer Security **20**(1), 29–38 (2012)
26. The Comprehensive R Archive Network: Desctools r package (2022), `https://cran.r-project.org/web/packages/DescTools/DescTools.pdf`
27. Theofanos, M., Stanton, B., Furman, S., Prettyman, S.S., Garfinkel, S.: Be prepared: How US government experts think about cybersecurity. In: Workshop on Usable Security (USEC) (2017)
28. Von Solms, R., Van Niekerk, J.: From information security to cyber security. computers & security **38**, 97–102 (2013)
29. Wang, Z., Sun, L., Zhu, H.: Defining social engineering in cybersecurity. IEEE Access **8**, 85094–85115 (2020)
30. Wash, R.: Folk models of home computer security. In: Sixth Symposium on Usable Privacy and Security (SOUPS 2010). pp. 11–26 (2010)