Cybersecurity Definitions for Non-Experts

Lorenzo Neil
North Carolina State University

Julie Haney
National Institute of Standards and Technology

Kerrianne Buchanan
National Institute of Standards and Technology

Charlotte Healy
University of Maryland

1 Introduction

There is no standard definition nor common terminology for explaining cybersecurity [1, 6], with existing definitions largely targeting academics or technical experts [2,3,8] but not non-experts (those without cybersecurity proficiency). This poses a challenge for security practitioners and researchers when trying to communicate the meaning and importance of cybersecurity to non-experts [4], potentially contributing to misconceptions of cybersecurity that impact people's ability to make informed security decisions or provide appropriate responses during their involvement in human-centered cybersecurity research studies [5, 7, 9].

In this work-in-progress research effort, we take an initial step toward developing guidance on how to define and describe cybersecurity to non-experts. In the first phase of our research, we performed a systematic search and analysis of publicly available, online cybersecurity definitions from different types of sources. *We investigated what terms are used to define cybersecurity, as well as what current definitions have in common with each other.* As opposed to prior work focusing on technical definitions, this work provides a deeper understanding of cybersecurity definitions non-experts are likely to encounter. We conducted a novel analysis of the terms and components (e.g., references to threats, security principles, and objects protected by cybersecurity) frequently used to define cybersecurity. Furthermore, we observed significant structural differences in definitions between distinct types of sources. Our findings – for the first time – illustrate the full landscape of cybersecurity definitions, not just the authoritative definitions created by and intended for experts. **This more comprehensive picture will be used to inform an in-progress interview study to investigate which definitions non-experts understand and which terminology aids their understanding.**

USENIX Symposium on Usable Privacy and Security (SOUPS) 2023.
August 6–8, 2023, Anaheim, CA, United States.

2 Systematic Search

Methods. To understand how cybersecurity is defined and commonalities among definitions, we systematically searched for and analyzed definitions from Google and research databases (IEEE, ACM, Engineering Village, and Web of Science) from the prior five years. Sources that provided explicit definitions [8] in English that could be accessed from our institutional computers were included in our dataset. We examined each source's core definition, which was typically one sentence. In contrast to Schatz et al. [8], we did not exclude sources that lacked peer review or authority (e.g., from governmental or 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 consist of ***152 sources containing 167 distinct definitions***. We classified each definition as being from one of six source types (Table 1).

Through an iterative qualitative coding process, we developed a codebook of definition components. The final codebook included seven codes, as described in Table 2: Actions, How, Objects, Security Principles, Threats, What, and Who. We conducted iterative rounds of coding with two researchers, checking for agreement and discussing areas of disagreement.

We calculated descriptive statistics to determine the frequency of each coded component in the cybersecurity definitions in our corpus. We performed Chi-Square or Fisher's Exact tests (significance level $p < 0.05$) with Cramer's V effect size 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 groups, we collapsed the sources into two categories: ***institutional*** (research, standards, government, education, general) and ***industry***. We also examined word frequencies to look for trends across definitions.

Results. We describe commonly referenced words and provide examples of trends in coded phrases across all definitions, including source IDs for quoted definitions[1]. 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.

The top five words occurring across all definitions were: *protect* (112 definitions), *systems* (83), *networks* (82), *data* (81), and *attacks* (75). 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). Other definitions used more 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).

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. Very few included Who and How components. 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.

Discussion. We found terms used to define cybersecurity are inconsistent and use generic references when describing threats, for example, limiting threats to "*cyber crime*" (A1). Cybersecurity definitions were also mostly action oriented, mentioning words such as *protect*, yet rarely mentioned who performs the protecting or how they are protecting, leaving open interpretation of non-experts' responsibility for cybersecurity. This ambiguity may not matter as much for definitions aimed at experts, but communications targeted at non-experts may benefit from being more specific to their context. It is also unclear how technical jargon (e.g., *confidentiality, integrity, availability*) or vague terminology (e.g., *cyberspace*) might be understood by non-experts.

We also 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 who consult those types of sources.

3 Interview Study

Purpose. The systematic search is informing an in-progress interview study to answer the following research questions:

- How do non-experts describe and define cybersecurity?
- How do non-experts understand published cybersecurity definitions, including the common terms and concepts in those definitions?
- Which representative cybersecurity definitions do people prefer, and for what reasons?

Methods. We will conduct virtual interviews with 30 non-experts of differing ages, genders, and education levels from across the U.S. to explore thier understanding of cybersecurity and reactions to several cybersecurity definitions. The definitions are from the corpus of definitions compiled in our systematic search and were selected to be representative of the trends we observed in our analysis. In the interview, we will first ask participants about their current understanding of cybersecurity and their own definition. Then we will step through two cybersecurity definitions in detail, asking participants about their opinions and potentially confusing terminology. We will next engage participants in a sorting exercise with three institutional and three industry definitions. Participants will select definitions that they think are favorites, easy to understand, comprehensive, and useful and will explain their reasoning behind those selections. Finally, we will reveal the sources of the definitions and ask if their opinions have changed.

4 Anticipated Contributions

The ultimate purpose of our research effort is to evaluate the appropriateness of current definitions for non-experts, identify potential areas of confusion, and offer guidance for cybersecurity practitioners and researchers when communicating to non-experts. We plan to conduct one more phase after the interviews involving a large-scale survey to explore differences based on demographics (gender, age, education level, etc.).

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

Disclaimer

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

References

[1] Charles Brookson, Scott Cadzow, Ralph Eckmaier, Jörg Eschweiler, Berthold Gerber, Alessandro Guarino, Kai Rannenberg, Jon Shamah, and Sławomir Górniak. Definition of cybersecurity-gaps and overlaps in standardisation. *Heraklion, ENISA*, 2015.

[2] Mariana G. Cains, Liberty Flora, Danica Taber, Zoe King, and Diane S. Henshel. Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. *Risk Analysis*, 42(8):1643–1669, 2022.

[3] Dan Craigen, Nadia Diakun-Thibault, and Randy Purse. Defining cybersecurity. *Technology Innovation Management Review*, 4(10), 2014.

[4] Marcia W DiStaso. Communication challenges in cybersecurity. *Journal of Communication Technology*, 1(1):43–60, 2018.

[5] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. Exploring how privacy and security factor into iot device purchase behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2019.

[6] Steven Furnell and Emily Collins. Cyber security: what are we talking about? *Computer Fraud & Security*, 2021(7):6–11, 2021.

[7] Sandra Spickard Prettyman, Susanne Furman, Mary Theofanos, and Brian Stanton. 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*, pages 260–270, 2015.

[8] Daniel Schatz, Rabih Bashroush, and Julie Wall. Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, 12(2):8, 2017.

[9] Rick Wash. Folk models of home computer security. In *Sixth Symposium on Usable Privacy and Security (SOUPS 2010)*, pages 11–26, 2010.

A Systematic Search Process

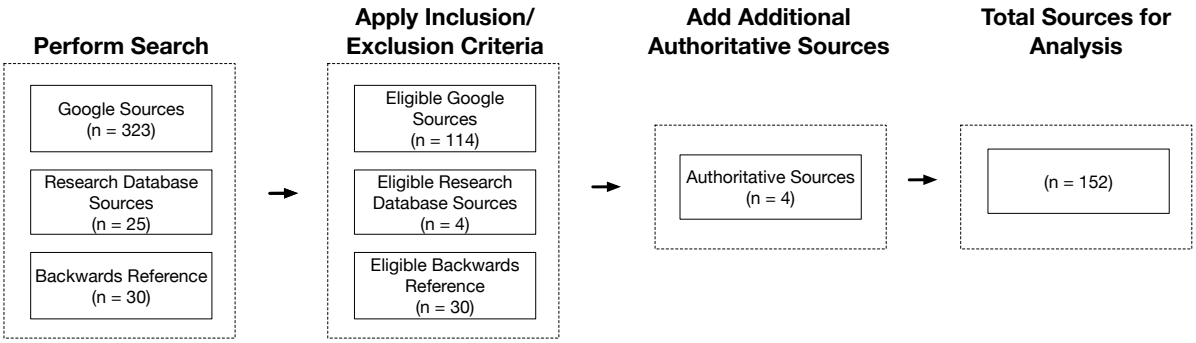

Figure 1: Systematic search process methodology

B Source Types

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%)

C Codebook

Table 2: Definition codes (components)

Code	**Description**
Actions	answers the question of what cybersecurity does in general
How	cybersecurity actions taken
Objects	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

D Definition Component Percentages

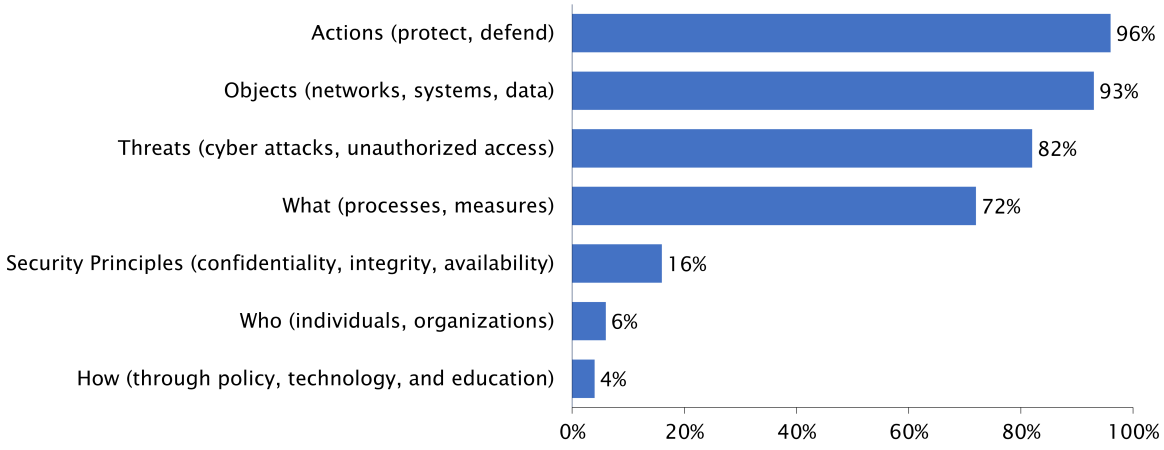

Figure 2: Percentage of definitions with each component (n = 167 definitions). Examples of words coded to each component are included within parentheses.

E Industry vs. Institutional Definitions

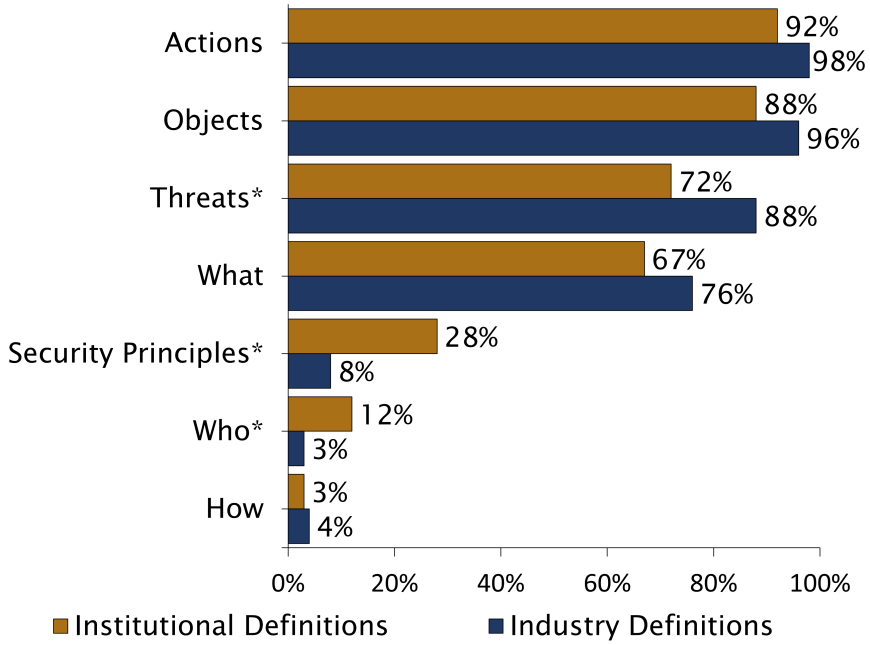

Figure 3: Percentage of industry (n = 107) and institutional definitions (n = 60) per definition component. *Statistically significant differences (Chi-Square or Fisher's Exact)