Externalizing Expert Mental Models for Cyber Visualization Design

Diane Staheli
MIT Lincoln Laboratory

Vincent F. Mancuso
MIT Lincoln Laboratory

Jared Chandler
Tufts University

Steven R. Gomez
MIT Lincoln Laboratory

Sean McKenna
University of Utah

Cody Fulcher
MIT Lincoln Laboratory

Lane Harrison
Worcester Polytechnic Institute

ABSTRACT

Understanding the mental model of the analyst is an important consideration in the design of cyber security visualizations to assist the sensemaking process. This paper discusses an exploratory study aimed at understanding the elements of an expert's mental model of network activity. We contribute a demonstration of a methodology that utilizes sketching to elicit information about the analyst's mental model and an analysis of the resulting drawings. In general, we found that trained experimenters can reliably categorize the shape elements of the drawings, but analyzing the domain semantics of representations in the drawings is more challenging. We discuss the results of our analysis process, as well as insights gleaned from qualitative observations made about the drawings. We suggest implications for cyber security visualization and future directions for mental model research.

Keywords: Mental model, cyber security, visualization.

1 INTRODUCTION

Through years of experience, cyber security analysts gain a detailed understanding of the networks they work on. This understanding contributes to an internalized representation that facilitates reasoning, called a "mental model" in cognitive psychology [1]. The mental models of cyber analysts help them to react appropriately in time-critical situations, to prioritize patches and improvements in their networks, and in many other operational tasks that keep their organizations secure. This paper focuses on the relationship between analysts' mental models and how visual representations elicited from them can inform the design of visual sense-making tools, like data visualizations, that analysts use. In fact, the goal of data visualization in cyber security is to help analysts process and make sense of large heterogeneous datasets produced by organizations. Security analysts use data in many ways: finding threats and attacks in their organizations, or for creating a common perspective on a security issue to share with other teams and decision-makers.

Few security visualizations are designed with analysts' mental models in mind, however. Visualization research typically focuses primarily on the technique, and evaluation with users is an afterthought [2]. This approach is not without benefit. Early innovations in visualization for cyber security included the use of parallel coordinate plots to represent packet or network flow data, for example, which proved useful in helping analysts detect malware and scanning activity [3, 4].

Technique-focused visualization research has benefitted significantly from innovations in design processes for problem-driven work. Visualizations can be considered cognitive tools to facilitate discovery, reduce memory load, and encourage collaboration [5]. To best support these processes, when building a visualization system, it is important to consider the needs and abilities of the users. Following a specific design process can help ensure the utility and efficacy of the visualization. Several design models exist in the visualization community, such as the nine-stage framework for design studies [6], the design activity framework [7], and the nested model [8]. These design methodologies focus on tasks external to the data itself. Organizational context, environmental conditions, and user experiences all shape user interpretations of data, and influence analytic conclusions drawn from the data.

One approach to bridging the gap between analysts' mental models and visualization techniques is through the elicitation, operationalization and application of mental models during the design process. There is a critical need in the VizSec community to better understand how analysts internalize the relationships between network entities so that we can work towards a common set of cognitive design principles for cyber security visualization. In pursuit of this, we aim to (1) explore a methodology for eliciting, capturing and analyzing information related to analyst mental models, (2) improve our understanding of said mental models for the purpose of informing the design of visualization systems to support cyber operations, and (3) suggest directions for future mental model research in cyber security.

Following previously established methodologies from human-computer interaction and cognitive psychology, we conducted an exploratory study with IT security professionals at one organization to examine their mental models of the organization's networks and assets. Our contributions include:

- a demonstration of a methodology that elicits artifacts about a cyber analyst's mental model through sketching,
- findings from applying a closed-coding analysis to the drawings with respect to the form, or shape, of each mark and its representation semantics, and
- a discussion of implications for visualization, and future directions for mental model research in the area of security visualization.

2 BACKGROUND

The core theory of mental models was formed from work in the psychology and cognitive science communities. Foundational studies in these areas facilitated later work on the applications of mental models in data visualization (e.g. [5]) and in cyber security. Because the goal of our study is to evaluate the utility of mental models in data visualization for cyber security, we begin by discussing and contrasting prior results in these areas.

2.1 Mental Models in Data Visualization

Mental models have been a long discussed topic in the visualization research community. In their research, Tversky et al. [5] discuss an approach to reveal mental representations through sketching, and use these representations to derive cognitive design principles. Two studies eliciting mental representations in different domains are discussed as exemplar use cases for the

approach – route maps and furniture assembly instructions. Wessel et al. [9] describe a similar study to the route map study, utilizing sketch mapping to externalize a mental model. They describe an experiment in which users are asked to navigate an unfamiliar environment using different navigation aids, and sketch a map of the area traversed. The results suggest that user recall is imperfect in a complex environment, but improves as users construct a cognitive map of an environment integrating both spatial understanding and semantic information: the spatial framework provides a means to organize semantic or contextual understanding. However, these use cases are confined to relatively simple tasks. Our work explores a more abstract task of providing visual answers to questions about a complex enterprise computer network that has little or inherent spatial component.

Previous examples of research into visual cognition include study of spontaneous visualization to discover how people use visuals to think [10] and analysis of hand-drawn artifacts across academic disciplines to derive information visualization design principles [11]. More broadly, it is generally accepted that effective visualizations represent information the way our minds do [12] and that interactive visualizations can serve to amplify and augment cognition [13, 14].

Mental models have appeared in several threads of research in visualization. Taking an abstract approach, Liu and Stasko [14] describe the role of mental models in data visualization [5]. Their efforts provide language beyond the common definition of mental models (i.e. an "internal representation"). Instead, they relate mental models directly to well-defined aspects of the data visualization, such as the encoding, interactions, and the tasks undertaken using the visualization. Also covering common elicitation techniques for mental models (sketching, prototyping, and think-aloud protocol), their work provides a suitable baseline from which designers can use information about mental models in the design of novel visualizations, but does not discuss discovery of conceptual understanding in a given domain. In contrast to Liu and Stasko [14], we focus on the relationship between the broader analytical context in organizations and analysts' corresponding mental models.

2.2 Mental Models in Networking and Cyber Security

The cyber security visualization research community has undertaken several mental model studies, many of which utilize sketching as an elicitation technique. Kang et al. [15] provides a comprehensive overview of studies related to mental models of home networking, Wi-Fi, security threats, web security, and personal firewalls [16-19] and describes a user study of mental models of how the Internet functions [15]. Mental model studies have been used with significant success to understand differences between experts' and lay-persons' understanding of cyber security concepts; participants examining privacy in the Kang [15] study produced vague and inconsistent representations, which was found to correlate to users with low-expertise in computing. In a creative take on knowledge elicitation, Hall et al. [20] describe a participatory design methodology utilizing Lego building blocks as a means of eliciting information about social, technical, and infrastructural components of a cyber security scenario.

D'Amico and Whitley [21] describe a detailed cognitive task analysis with expert analysts, and present a model for how analysts use their mental models to transform data into analytic conclusions and situation awareness. However, this work focuses on work process: it characterizes the role of the mental model and how it is utilized to perform analytic tasks, rather than trying to understand its formation or structure. The research methodology as described does not incorporate elements of visual cognition, and relies on other knowledge elicitation techniques: semi-structured interviews, observations, review of critical incidents, and hypothetical scenario construction.

In this study, we apply existing mental model elicitation techniques to address this fundamental gap in mental model research. We utilize the sketching methodology to elicit how expert security analysts conceptualize the network that they work on every day. While previous studies discuss knowledge gained from these activities, they do not provide a blueprint for how to analyze the drawings generated; as such, we explored both quantitative and qualitative analysis techniques.

3 Methods

We generally followed the methodology described in Tversky et al. [5] to conduct our exploratory study. In the Tversky study, users were asked to create a drawing of a route to a local landmark; a relatively simple task with a finite number of sensible outcomes. To make our study task-agnostic, we modified the protocol to ask open-ended questions, and users sketched out their responses. In order to encourage reflection in different directions and to generate as many drawings as possible, we asked users multiple questions about different aspects of the network. The questions asked are enumerated below:

- How do you picture the network you work on every day in your head?
- How does your network connect to other networks?
- How do users utilize the network?
- How would you describe the network to a new analyst?
- What are the major features of your network?
- How do you picture the details of activity on the network?
- How would you navigate between a high-level view of the network and a detailed view of the data?

3.1 Participants

Eight participants were recruited for the study. At the time of the study, all participants worked in IT security for the same organization and used the same network. While they had overlapping responsibility in maintaining the security of the network, they represented multiple roles (network operations, threat analysis, compliance, traffic analysis, and malware analysis) with varying daily tasks.

3.2 Sketching Procedure

Following a brief demographic survey, participants were asked a series of seven open-ended questions about their views of the network. Following the questions, they were given markers and papers, and asked to create a sketch as a response to each of the questions.

While they were drawing, participants were asked to describe their drawings to the research team; either as concurrent think-aloud or after the drawing was complete. Follow-up clarifying questions were asked at the discretion of the study moderator. Each session lasted approximately 45 minutes.

3.3 Analysis

We analyzed the study data primarily through a coding process that aimed to categorize and count meaningful features in the drawings related to the network concepts and marks. Notes from the user interviews were used as a reference to clarify the content of the drawings.

3.3.1 Coding Process

Four members of the research team performed a closed-coding process in which pre-selected codes were assigned to individual items across all the drawings. Items are defined as marks in the drawing that represent units of shape (e.g., an arrow) or network concepts (e.g., a host in the network). For example, if a participant draws two computers connected by a line, the drawing includes three items: the two computers and the connecting line. We developed and used a computer-based coding tool (described in section 3.3.3) for this process.

To maintain consistency and ensure equivalent data points across coders, each individual used the coding tool to define items. For each item, coders were asked to assign a singular value based on the form and representation.

Following completion of the coding, interrater reliability was assessed using Fleiss' kappa [22], a statistical measure of the reliability of agreement between more than two coders. Disputes were settled based on a majority vote, or a third party judgment.

Throughout the coding process, coders noted aspects of the drawings or verbal explanations that were interesting examples of mental-model illustration, but that did not fit into the formal categories of the coding scheme, which we describe next.

3.3.2 Coding Scheme

To assess the drawings we employed both a top-down (a priori) and bottom-up (derived from data) coding approach, utilizing a set of a priori codes across two levels based on the syntax of the drawing and its intended representation. For the syntax, a set of geometric shapes were identified from the drawings, as seen in Table 1.

Table 1: Labels and descriptions for syntax-based codes

Labels	Descriptor
Polygon	Shape bounded together by straight edges (e.g. square, triangle, pentagon).
Line	Connector between two elements without any implied directionality
Arrow	Connector between two elements with directionality in a single direction
Bi-Directional Arrow	Connector between two elements with directionality in two directions
Text	Label with semantic meaning
Cloud	Shape with puffy Extrusions
Circle	A round object
Other	Anything that does not fall into the above categories

The second coding structure focused on the cyber-specific item the drawing was attempting to represent. For this categorization, we developed a simplified structure based on the Cisco Systems Corporate Iconography [23], a popular standard across cyber security products, as seen in Table 2.

Table 2: Labels and descriptions for representation-based codes

Labels	Descriptor
Network Infrastructure	A device attached to the network with the purpose of providing delivery of network traffic (e.g. switch, router)
Security Infrastructure	A device attached to the network with the purpose of providing cyber security.
Server	A server accessed over the network by other computers
Computer	A computer used by a user on the network
End User	Human who uses computers
Physical Infrastructure	An object which supports the network (e.g. building, door, table)
Connection	A connection between two elements on the network
Attacker	An adversary or threat
Other	Something recognized but not listed above
Unknown	Something unrecognizable

3.3.3 Coding Tool

The coding tool is a web application running either locally on a researcher's personal computer or on a network server. The tool is implemented in Python with data stored in a SQL database. When run from a network server, multiple coders can use the tool simultaneously.

Subject drawings are scanned from paper and uploaded into the system as either JPEG or PNG format. An entry for each drawing to be coded is added to the system database. Researchers define a bounding region for each feature in the drawing. This is done through the web interface directly over the scanned image and saved to the database, as seen in Figure 1. Coders are able to adjust regions in several ways, including resize, reposition, and remove. The tool supports intersecting and nested bounding regions.

Users perform coding for all features contained in each drawing. The researcher first selects a drawing to code from a menu. The drawing is then displayed. Colored borders visually differentiate features of the drawing. These regions are color coded to indicate whether they are yet to be coded, are partially coded or are complete. Coders have immediate visual feedback of the state of coding for a given subject drawing as seen in Figure 2. Once complete, the coding results were exported in a comma separated value (CSV) format for data analysis in other software tools.

4 Results

In this section, we discuss the results of our coding process, as well as observations we made about the drawings external to our coding scheme.

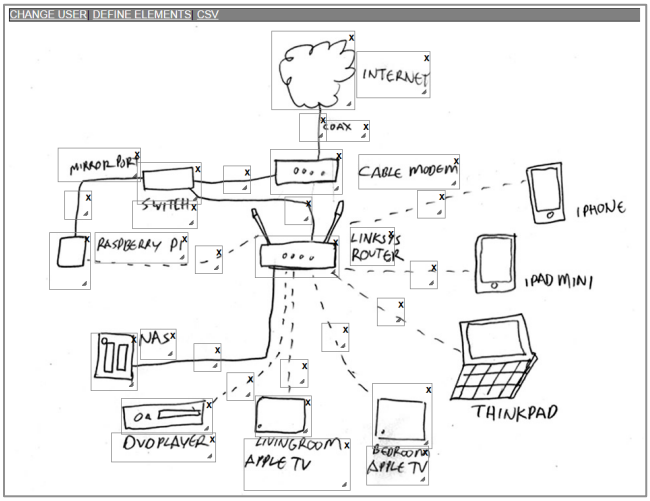


Figure 1: Coding tool region definition

4.1 Coding Analysis

Participants generated 47 drawings. A subset of 27 drawings was selected for analysis, resulting in 144 visual elements coded. In this section, we discuss the analysis and results of the coding exercise.

4.1.1 Syntax Coding Analysis

The interrater reliability (Fleiss' kappa, [22]) of the four coders on the syntax coding analysis was .78, which indicates substantial agreement [24]. The results showed that almost all items that were drawn had a corresponding line or arrow attaching them to another item. Additionally, of the lines with arrows, over 90% of them were directed.

Of the drawings created by subjects, 11 of them exhibited use of one or more cloud shapes. The cloud shape was given a text label in 9 of those, always placed within. In one drawing the contents of the cloud shape was a smaller network diagram and in only one drawing was the cloud shape unlabeled. In three drawings multiple clouds shapes were depicted. The use of a cloud shape to depict an abstract network is well known convention in the area of computer networking and its appearance supports the idea that the subjects are familiar and feel comfortable employing this visual convention.

Other items across the network were represented with simplistic polygon shapes. These were more difficult to hone in on, as they were used to represent numerous categories from the representations, thus without text or context from the drawing, they could be difficult to decipher.

4.1.2 Representation Coding Analysis

After multiple attempts at coding, involving repeated training sessions, the coders were only able to achieve a kappa value of .4 for the representation dimension, signifying Fair to Moderate agreement [24], well below the typical threshold of acceptable agreement (kappa > .6). Given the substantial agreement for the syntax coding, we assume that the lack of agreement was not necessarily a result of the coders, but rather the lack of robustness of the code set.

In follow up discussions, we found that the coding scheme was both too simple and not robust enough. On average, across all coders, the representation scores for the "connection" and "network infrastructure" codes represented 47.2% of the final data set (SD = 0.13). At the same time, we found that 39.92% (SD = 0.19) of the data was coded as other.

Rather than simplifying the code set, which would artificially increase the kappa value [25], or increasing it with bottom-up codes, which would decrease generalizability, we performed an additional qualitative analysis on the drawings. The qualitative analysis, discussed in the next section, revealed new insights about the possible development of analysts' mental models and how models differ between analysts.

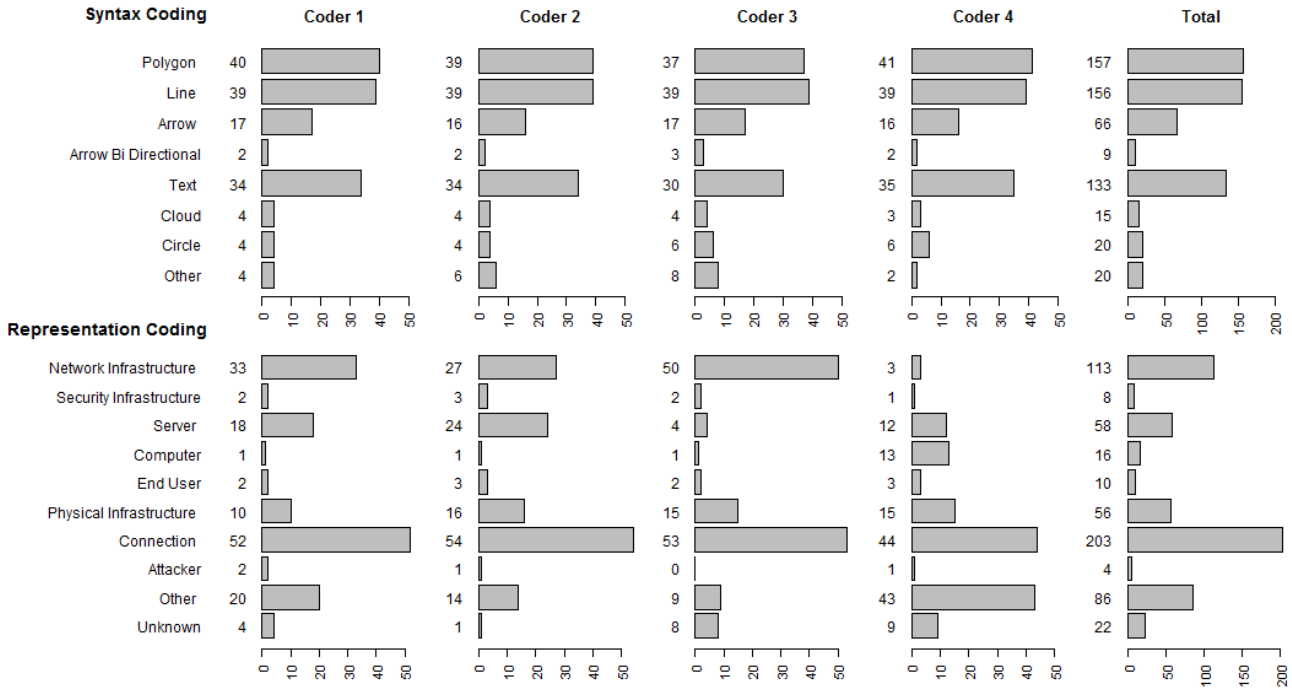
4.1.3 Observations Outside the Coding Scheme

In addition to the coding exercise, we also analyzed the drawings qualitatively in cases where coders observed interesting illustration techniques or network concepts that did not fit into the closed-coding categories. We identified two themes in the dataset that stood out. First, participants mixed metaphors, both visual and verbal, when drawing and explaining their response. Second, participants rarely drew people in their diagrams, or indicated malicious activities or vulnerabilities, despite their IT security job duties. These themes are discussed further in Section 5.

4.1.4 The Network Diagram as Common Ground

The first question posed to users was "How do you picture the network you work on every day in your head?" Most (5 of 8) participants drew a notional enterprise network diagram, intended to represent network topology, as a response. We characterize a network diagram as having the following features: standard symbology sets, attempts at representing all significant network infrastructure, and lines representing connections between infrastructure elements. An example is presented in Figure 3. Generally the topology depicted in the drawings was similar to the logical topology of the network (as verified against the most recent network diagram provided by the organization). Responses diverged for all subsequent questions. Other responses employed metaphors, geospatial drawings, and typical visualization conventions (such as line graphs, scatter plots, Venn diagrams) to convey key concepts. This finding reinforces our previous assumption that the network diagram is a canonical

Table 3: Coding counts for syntax-based and representation-based coding



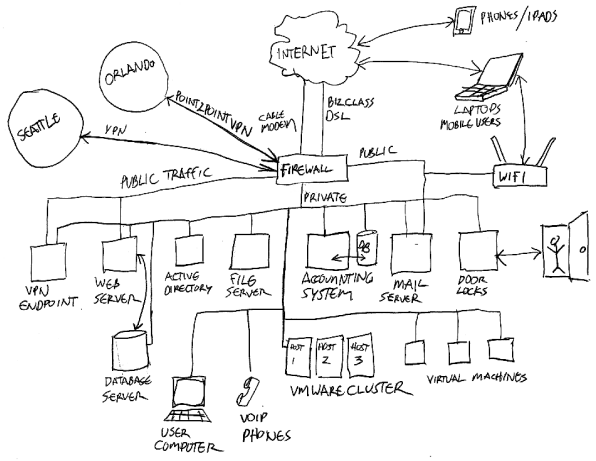


Figure 3: Example of Enterprise Network Drawing

representation, and provides common cognitive ground for a team.

Several participants used metaphors other than the network diagram. One participant, for example, drew the network as a city, with walls and gates representing entry points into the organization. Another participant drew a door in between the world and the enterprise IT services of the organization. The diversity of alternative representations suggests that limiting visual representations to network devices may be inadequate to represent all the ways in which an analyst conceives of network activity.

5 Discussion

The following section discusses implications for cyber visualization design based on our qualitative findings and the results of our coding analysis.

5.1 Accuracy & Consistency Between Drawings

Upon examining the drawings that resembled traditional network diagrams, we noted many variations and inconsistencies between subjects that drew the same portion of the network. There were 6 drawings that represented the same segment of the network, and only 2 of those drawings portrayed identical network assets in the same order. This observation could be interpreted in two ways:

(1) Analysts have different understandings of how infrastructure is configured and cannot recall the details correctly. This interpretation is consistent with prior research in the geospatial domain suggests that recall may be imperfect in the face of system complexity [9].

(2) Analysts are intentionally abstracting away unnecessary detail, and recalling only the details that are relevant to their particular task. For example, sensor locations are important information that a traffic analyst might need to understand the relationships that between entities present in the data.

The latter interpretation – analysts were making deliberate choices to focus scope – is supported by additional observations; there are other instances in the drawings where participants abstract away details into drawn elements that are less precise but still accurate. Individual end hosts were not represented very often, even in aggregate. The amount of detail depicted in drawings of conceptually similar objects varied greatly; in many instances the resolutions differ between objects at the same hierarchical levels of the system. For example, one drawing depicted a network segment with 9 squares and a cloud connected to it. The cloud was labeled "Internet". 4 of the squares were labeled as "server" and the remaining 5 squares were unlabeled. Several other drawings depicted clouds representing the Internet or other network segments at the same hierarchical level and visual scale as routers, servers, and other concrete devices.

5.2 Abstract Themes in Drawings

5.2.1 Use of Metaphor

In several drawings, participants mixed visual metaphors with concrete representations of network devices. Metaphor refers to the understanding of one experience or concept in terms of another – typically, the understanding of a more abstract concept is expressed in terms of more concrete [26]. For example, one user drew a door with doorknob between a pair of network sections to help illustrate the behavior and function of the firewall device between these sections. In another case, a participant drew the network as a city, with walls and gates representing entry points into the organization. Overall, metaphors were used more frequently in the words that subjects used to explain their drawings, rather than in the drawings themselves. Common metaphors from explanations included: doors, gates, cities, roads, intersections, and traffic. These metaphors can provide inspiration for future network visualization tools or symbologies.

5.2.2 Depiction of the Human User

One question asked: "How do users interact with the network"? Despite this direct inquiry into user behavior, only 3 of the 27 drawings coded contained an explicit representation of a human user. The drawings that did contain a human user depicted them interacting with individual devices, presumably to indicate where the subject imagined humans interacting with the network. For example, one computer is shown on a table with a human next to it. Some objects are depicted with affordances for human input, such as keyboards or touchpads. This lack of attention towards the individual user is surprising, given the current level of concern over insider threat. Related to this, although we did not directly inquire about potentially malicious user activity, no drawings included representations of an adversary or a hacker. A possible explanation is that analysts conceive of networks as autonomous systems, rather than as systems that humans utilize for various tasks.

5.3 Visual Taxonomies for Cyber

Developing and converging on a coding scheme that could be applied robustly, with generalizability, and in a repeatable fashion was a significant challenge in this study. Given our results, where coders' responses fell into one of two categories, or "other", we determined that the scheme we identified was both too general and not complex enough. This was particularly surprising considering the coding scheme was based off a common cyber symbology set from Cisco.

When taking a qualitative look at the drawings, it was apparent that not only was the coding scheme developed by the researchers adequate, but the mental models of cyber symbology for the participants was also very coarse. In the absence of good iconography, or visual vocabulary, participants defaulted to labeled text boxes and arrows to describe concepts. This is consistent with previous research: meanings of simple geometric features (lines, crosses, arrows, etc.) are related readily understood in context [5]. For example, lines can represent either connections or boundaries between network assets. Cyber may be a realm where concepts cannot be adequately expressed using a visual

vocabulary, and as a result subjects resort to metaphor and combinations of icon and text as the fundamental unit of expression. This divide created a gap between how the users internalized and utilized metaphors to represent cyber when compared to current conventions. Where the users rely on more simple, geometric shapes, but current conventions rely on more representative iconography.

When we took a step back from the individual symbologies and assessed the drawings at a macro level, we found some more interesting commonalities across drawings. Participant drawings represented network structure (what are the major infrastructural components, how devices are arranged), semantics (zones of trust, services available, entities using the network), and temporal behaviors (regular and irregular patterns, functions performed) of the network. The relationship between these kinds of elements on a network is much more closely coupled than in the physical world and are much more fluid (for example, the structure or topology of a network can change to establish a trusted relationship between two entities). Because of the interconnected nature of these relationships, it may be difficult to definitively place an element into one category or another, without a sufficiently rich schema. We suggest that the variety of elements we found in our drawing dataset could serve as a starting point to develop such a taxonomy.

5.4 Mental Model Research as a Design Activity

Based on our qualitative observations, we have formed new hypotheses for cyber visualization design that we identified following the findings of our exploratory study. We believe targeting these hypotheses with controlled studies could lead to design guidelines and tools that better support the cognitive needs of cyber analysts.

We noted the analyst mental model is not always consistent or accurate between analysts – while we did not specifically ask participants to draw for accuracy, this finding is nevertheless concerning, as it implies that analysts could be misinterpreting data or making decisions based on information that is incorrect. Further study could illuminate the impact of this finding – impact of mental model on error rates could lead to additional insight. To assist analysts in orienting correctly in relation to the network environment, visualizations tools should contain explicit representations of major infrastructure elements relative to the data source under analysis. However the fact that this structure was the most common type of drawing in our study implies that it is the most important element of an expert's mental model.

The structure of the network diagram, particularly in the case of a large enterprise, can be overwhelmingly complex and difficult to reproduce accurately from memory. The inconsistency of analyst representations may or may not be intentional as a means to reduce complexity; regardless, we hypothesize that visualization interaction mechanisms that abstract away and reveal the details of network structure as needed (e.g., expand and collapse design pattern) will help cyber analysts to better understand network structure and improve efficiency and accuracy of analysis results. For example, incorporating accurate sensor position information will help establish the provenance of network activity data, which is useful in understanding activity of interest. Providing a cognitively-informed taxonomy of network structures and behaviors will help cyber analysts understand their data and better communicate their findings better to others.

While network diagrams and schematics are useful conventions to describe the logical, or literal, structure of a network, they are not adequate to describe behaviors or reason about functions of network devices. Lakoff and Johnson [26] argue that the human conceptual system is "fundamentally metaphorical in nature". This implies that metaphor for cyber security is a useful device to translate the abstract behaviors that are occurring on a network in a way that is more accessible to the analyst, and in a way that better fits their innate conceptualization. The metaphors gathered using the sketching methodology are a rich source of information that can be mined and explored to build interactive visualizations.

By conducting this study, we have started to make progress into how we might characterize the expert mental model, and provided thoughts on how we might design visualization tools to fit this model. Looking ahead, we envision the use of systematic mental model elicitation as a design activity to understand the cognitive requirements as well as the task requirements of a visualization system. It is well documented in research that network analysis is requires support for cognition as well as support for tasks [21]. By repeating these studies in each of the areas we have highlighted in our discussion (network structure, symbology, abstraction, metaphor), we can start to understand how these elements are conceptualized and how they fit together. By gaining an understanding of how experts conceptualize a network, we can move towards more task-independent visual representations in the cyber domain, which would be applicable and presumably more useful across many tasks and roles.

5.5 Study Limitations

5.5.1 Externalizing Mental Models

We asked participants to draw diagrams of networks by hand in order to better understand cyber analysts' mental models of these data structures. In doing so, we assume that an analyst's drawing of a network is a good proxy for her mental model of that network. While this process has been used before to elicit and analyze drawn representations of networks and abstract systems (i.e., [10]) there are a few limitations to this approach.

First, it is possible that one's knowledge of a network is more similar to *imperative knowledge*, which is expressed through the ability to perform tasks, than *declarative knowledge*, which can be written down or drawn. In other words, one's understanding of a network might be difficult for them to externalize on paper. Therefore, conclusions from these drawings might apply only to parts of one's mental model that can be written down or drawn, and other parts could exist.

Second, the task of drawing one's model of a network imposes constraints on how the model is externalized. For example, the color and size of marks we observed were guided by the physical materials we provided for this task. In addition, there is usually little that is inherently 2D about how a computer network functions, but the drawing task essentially asks participants to project models of networks onto 2D, space-constrained pages. Because maps are commonplace, we believe the 2D projection is an intuitive way for analysts to externalize and visualize their models. Other methods for "drawing" a network model, like modeling it in 3D or drawing on transparent pages that can be layered, could help participants externalize their models as well or better than drawing on paper.

5.5.2 Study Scale and Scope

Though it was representative of the organization from which participants were drawn, our sample size was small given the variety of participants' cyber roles and the freeform nature of the study tasks. With a small sample size, significant quantifiable patterns in how cyber analysts understand networks might be difficult to observe, even if true patterns exist and the coding

scheme is expressive and applied perfectly. Unfortunately, due to the sensitive nature of cyber analysts' work, it is difficult to recruit participants at a scale larger than ours. Narrowing the scope of the study and research questions could make it easier to draw specific quantitative conclusions.

6 Research Opportunities

In this section, we discuss areas for further study that build on our exploratory findings. We break down these opportunities into two types of work: 1) refining the experiment we performed in order to target more specific hypotheses about cyber analysts, and 2) developing new tools for externalizing mental models that enable new analyses.

6.1 Additional User Studies

We envision several directions for extending the exploratory study we performed.

Repetition of the sketching protocol with additional participants – The study could be repeated with a similar organization of similar size, to determine if findings were consistent, or repeated with a larger organization, to determine if findings were statistically significant.

Reduction in scope of the study – The study described here was exploratory, and intentionally broad. From our taxonomy discussion, we hypothesizing that reducing the scope of the study to focus on analysis of one aspect of the network in question (structure, semantics, behavior) in isolation will yield rich data about the problem space.

Further analysis of user roles – While we did collect data on user roles and contribution to the organization, the small sample size precluded analysis based on user roles. If the study could be repeated with a larger organization, we could examine individual differences between drawings, and draw meaningful conclusions based on role.

Validation of coding schema – The coding exercise could be repeated with participants external to the study team as a means of testing new taxonomies or coding schemas. The analysis of drawings could be crowd-sourced to both cyber security experts and non-experts to see how well the schema generalizes, and how broadly understandable it is.

6.2 Coding Tools for Mental Models

Following our study, we identified new requirements for the coding tool that could enable deeper analysis of cyber analysts' mental models. More broadly, a full-featured coding tool could be used by the visualization research community at large to study multiple aspects of visual cognition.

Live capture of mark-making – Directly capturing the subject's drawing using a digital interface, like a tablet computer, would let us more easily analyze the sequence by which visual elements are drawn and the time spent on each element. We believe this data would offer insight into the relative importance of different elements of a mental model, as well as workload involved in externalizing its different parts. Aggregating this data from multiple study participants could help us test whether there are similarities in the sequences and timing across a group of analysts, and whether these model-drawing patterns are specific to the cyber domain.

Annotation and revision – We identified a need for supporting further participation of subjects during the coding process. It could be helpful for subjects to return to their drawing and self-code features that were ambiguous to coders. More generally, self-coding could validate the schema that evaluators choose, or help refine it during an open coding process. In addition, we believe it would be helpful for subjects to annotate how uncertain they feel about parts of their drawings for the coders, or for automated analysis. This could be done using a software interface in order to avoid mixing subjects' annotations with their mental-model marks.

Towards quantitative measurement – For the cyber domain, we identified a use case for a tool that automatically captures, interprets, and encodes the graph properties in subjects' drawn network diagrams. Collecting this data manually is time-consuming and error-prone, however, with the recent widespread availability of tablet computers this is now feasible. The data could shed light on whether network scale and topology as commonly understood and communicated by analysts, and could yield more quantitative information about the accuracy and completeness of the network diagrams.

7 Conclusion

Mental models are important to consider during the visualization design process. Experts have a standard means to generally represent the structure of a network and its underlying infrastructure, though problematic areas remain: inadequate symbology, and the accuracy and completeness of the mental model. Experts also lack a shared understanding of how to visually represent network semantics, relationships, behaviors – our study has highlighted that this is a rich field for research. We have provided a methodology for how these areas might be researched, and have provided some insight into future study.

Acknowledgements

The authors wish to thank Kristen Liggett and Caroline Ziemkiewicz for their insights and discussions pertaining to the study.

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.
This material is based upon work supported by the Assistant Secretary of Defense for Research and Engineering under Air Force Contract No. FA8721-05-C-0002 and/or FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Assistant Secretary of Defense for Research and Engineering.

References

[1] P. N. Johnson‐Laird, "Mental models in cognitive science," *Cognitive Science,* vol. 4, pp. 71-115, 1980.

[2] D. Staheli, T. Yu, R. J. Crouser, S. Damodaran, K. Nam, D. O'Gwynn, *et al.*, "Visualization evaluation for cyber security: trends and future directions," in *Proceedings of the Eleventh Workshop on Visualization for Cyber Security*, Paris, France, 2014, pp. 49-56.

[3] X. Yin, W. Yurcik, M. Treaster, Y. Li, and K. Lakkaraju, "VisFlowConnect: netflow visualizations of link relationships for security situational awareness," in *Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security*, Washington, DC, 2004, pp. 26-34.

[4] H. Choi, H. Lee, and H. Kim, "Fast detection and visualization of network attacks on parallel coordinates," *computers & security,* vol. 28, pp. 276-288, 2009.

[5] B. Tversky, M. Agrawala, J. Heiser, P. Lee, P. Hanrahan, D. Phan, *et al*., "Cognitive design principles: From cognitive models to computer models," in *Model-based reasoning in science and engineering*. vol. 2, L. Magnani, Ed., ed London: King's College, 2006.

[6] M. Sedlmair, M. Meyer, and T. Munzner, "Design study methodology: Reflections from the trenches and the stacks," *IEEE Transactions on Visualization and Computer Graphics,* vol. 18, pp. 2431-2440, 2012.

[7] S. McKenna, D. Mazur, J. Agutter, and M. Meyer, "Design activity framework for visualization design," *IEEE transactions on visualization and computer graphics,* vol. 20, pp. 2191-2200, 2014.

[8] T. Munzner, "A nested model for visualization design and validation," *IEEE transactions on visualization and computer graphics,* vol. 15, pp. 921-928, 2009.

[9] G. Wessel, C. Ziemkiewicz, R. Chang, and E. Sauda, "GPS and road map navigation: the case for a spatial framework for semantic information," in *Proceedings of the International Conference on Advanced Visual Interfaces*, Roma, Italy, 2010, pp. 207-214.

[10] J. Walny, S. Carpendale, N. H. Riche, G. Venolia, and P. Fawcett, "Visual thinking in action: Visualizations as used on whiteboards," *IEEE Transactions on Visualization and Computer Graphics,* vol. 17, pp. 2508-2517, 2011.

[11] S. R. Gomez, R. Jianu, C. Ziemkiewicz, H. Guo, and D. Laidlaw, "Different strokes for different folks: visual presentation design between disciplines," *IEEE Transactions on Visualization and Computer Graphics,* vol. 18, pp. 2411-2420, 2012.

[12] C. F. Chabris and S. M. Kosslyn, "Representational correspondence as a basic principle of diagram design," in *Knowledge and information visualization*. vol. 3426, S.-O. Tergan and T. Keller, Eds., ed Germany: Springer, 2005, pp. 36-57.

[13] S. K. Card, J. D. Mackinlay, and B. Shneiderman, *Readings in information visualization: using vision to think*. San Francisco, CA: Morgan Kaufmann, 1999.

[14] Z. Liu and J. Stasko, "Mental models, visual reasoning and interaction in information visualization: A top-down perspective," *IEEE Transactions on Visualization and Computer Graphics,* vol. 16, pp. 999-1008, 2010.

[15] R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler, "“My Data Just Goes Everywhere:” User Mental Models of the Internet and Implications for Privacy and Security," in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, Ottawa, Canada, 2015, pp. 39-52.

[16] E. S. Poole, M. Chetty, R. E. Grinter, and W. K. Edwards, "More than meets the eye: transforming the user experience of home network management," in *Proceedings of the 7th ACM conference on Designing Interactive Systems*, Cape Town, South Africa, 2008, pp. 455-464.

[17] P. Klasnja, S. Consolvo, J. Jung, B. M. Greenstein, L. LeGrand, P. Powledge, *et al*., "When i am on wi-fi, i am fearless: privacy concerns & practices in eeryday wi-fi use," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Boston, MA, 2009, pp. 1993-2002.

[18] R. Wash and E. Rader, "Influencing mental models of security: a research agenda," in *Proceedings of the 2011 Workshop on New Security Paradigms*, Marin County, CA, 2011, pp. 57-66.

[19] F. Raja, K. Hawkey, and K. Beznosov, "Revealing hidden context: improving mental models of personal firewall users," in *Proceedings of the 5th Symposium on Usable Privacy and Security*, Mountain View, CA, 2009, p. 1.

[20] P. Hall, C. Heath, and L. Coles-Kemp, "Critical visualization: a case for rethinking how we visualize risk and security," *Journal of Cybersecurity,* vol. 1, pp. 93-108, 2015.

[21] A. D'Amico, K. Whitley, D. Tesone, B. O'Brien, and E. Roth, "Achieving cyber defense situational awareness: A cognitive task analysis of information assurance analysts," in *Proceedings of the Human Factors and Ergonomics Society annual meeting*, Orlando, FL, 2005, pp. 229-233.

[22] J. L. Fleiss, "Measuring nominal scale agreement among many raters," *Psychological bulletin,* vol. 76, p. 378, 1971.

[23] Cisco, "Cisco Systems Corporate Iconography " n.d.

[24] J. R. Landis and G. G. Koch, "The measurement of observer agreement for categorical data," *biometrics,* pp. 159-174, 1977.

[25] J. Sim and C. C. Wright, "The kappa statistic in reliability studies: use, interpretation, and sample size requirements," *Physical therapy,* vol. 85, pp. 257-268, 2005.

[26] G. Lakoff and M. Johnson, "Conceptual metaphor in everyday language," *The journal of Philosophy,* vol. 77, pp. 453-486, 1980.