2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)

A Task Analysis toward Characterizing Cyber-Cognitive Situation Awareness (CCSA) in Cyber Defense Analysts

Robert S. Gutzwiller, Sarah M. Hunt, Douglas S. Lange, *Member IEEE*

***Abstract*—Cyberspace is an increasingly crucial part of everyday living. We have long recognized that defending this space is complex, requiring information integration, and decisions of man and machine to coalesce in a dynamic environment full of shifting priorities. These properties suggest that, as in other domains with similar characteristics, situation awareness (SA) of a human cyber defender is paramount to the quality of decision outcomes in cyber defense.**

The majority of existing research in cyber situation awareness, centers on information systems and computers, which piece together disparate data. Fused data from multiple sources, for example, is necessary for cyberspace visualization efforts. The judgment for successful cyber SA from this perspective is different from one that is human-centered. In comparison, we rarely assess *human* cognitive awareness in cyberspace. In part, this reflects a need, based on prior theory, to first define critical elements of information that the human must perceive, work to elucidate how humans combine these elements to comprehend the state of the network, and how together, this awareness helps analysts predict the future state of the network. In other words, although data fusion can provide value by reducing the cognitive load created to piece together disparate sources of information, human awareness of the network (cyber-cognitive situation awareness – CCSA) is perhaps the ultimate intermediary for defense performance.

Toward such an understanding, we discuss the results of a cognitive task analysis (CTA) which sought to determine the goals and abstracted elements of awareness that cyber analysts seek in network defense. We present the foundation for a series of planned experiments that establishes CCSA measurement, and baselines the efforts of cyber defenders. Once assessed, we can then begin to consider the help offered by fusion systems, automation of defensive capabilities, and cyber visualizations in a methodologically rigorous manner that has been lacking.

Keywords—cyber network defense; cyber-cognitive situation awareness; cyber situation awareness; decision-making; cognitive task analysis

I. Introduction

CYBERSPACE has been the realm of technologists, but the relative need for technological contribution is shifting. Technological advances are responsible for the improved connection and flows of information between devices over networks, and for many of the methods used to both attack and defend these spaces. However, at no point have these solutions provided an end-all for cyber defense. Humans are required to monitor and defend the networks and devices. Such protection has an increasingly vital role in contemporary life. Attacks are increasing in rate [1], scope, and criticality [2] with no end in sight. Increasing threats now effect powerful organizations, and in particular the military. With the recent breach of Sony Pictures [3] and the Office of Personnel Management [4], adversarial power in cyberspace is outwardly unlimited.

Although much of the work of defense occurs behind the scenes, the impacts when it fails can be widespread. Such expansion of malice is not, after all, limited to computers and server systems. With the advent of Web 2.0, traditionally unconnected devices and vehicles are now part of the network, or use services that expose attackable surfaces. Medical devices, for example, now present security risks to patients [5], the least of which is unwanted disclosure of personal information, and the worst of which are directly life-threatening through compromised device functionality and reporting. The brittle security of these systems greatly contradicts the need for resilience – something which humans are asked to consistently provide.

Indeed, it is no easy matter to control cyberspace, even with state of the art systems and technology. Cyber defense is very asymmetric, meaning, the advantages for the attacker are far more numerous [6] than for the defender. In this case, because attacker actions occur in vast noise in data, capabilities and intent are difficult to determine [7], and while defenders are under constant network exposure, relying on peers to succeed, attackers are successful as lone wolves, and only need one vulnerability for victory.

Promisingly, industries are turning to humans to mitigate cyber threats, because the promises of automated defenses are not enough [8]. Planted between malicious actors and the data being protected within organizations, are human cyber network defenders. These analysts (we use the term *defender* and *analyst*

Final paper submitted January 13th 2016. This work was supported by a Naval Innovative Science and Engineering grant from the Space and Naval Warfare Systems Center Pacific. This manuscript is submitted with the understanding that it is the work of a U.S. government employee done as part of his/her official duties and may not be copyrighted.

The views and opinions expressed in this article are solely those of the authors, and do not reflect the official policy or position of any agency of the U.S. government.

R. S. Gutzwiller,PhD, S. M. Hunt, and D. S. Lange, PhD, are with the Space and Naval Warfare Systems Center Pacific, San Diego, CA (92106) USA (e-mail:robert.s.gutzwiller1@navy.mil; sarah.hunt@navy.mil; doug.lange@navy.mil).

interchangeably here) perform the difficult jobs of determining whether a network is under attack, how to mitigate that attack and in many cases determining how the attack was possible. Cyber analysts operate in large organizations. Organizational structures differ widely, resulting in different analyst roles. Analysts are generally understudied in the search for effective cyber security (though recent efforts are improving our understanding, e.g., [9]).

Signature-based security methods may not require direct human detection. Many efforts seek to automate those defensive procedures even as they require some oversight by analysts. But despite this seeming "win", only highly trained human analysts are able to detect subtle attacks and insider threats.

In the effort to mitigate threats, the analyst needs to build situation awareness of the critical elements relevant to defending the network. A cognitive perspective on situation awareness [10], is that a human operator in a dynamic environment will seek to perceive the relevant, critical elements of information, attempt to comprehend their meaning and use this knowledge to make predictions in the near future about the state of the environment. The label of *cyber situation awareness* [11] has often been used to represent data fusion and integration, the kind that could provide integrated, common operational picture for an operator. However, the term has decayed in richness, and is now taken to mean the dealings of the cyber system itself, such as how data fusion efforts are created in architectures, and displayed on screens – rather than referring to analyst awareness in cyber defense [12, 13].

A new label, **cyber-cognitive situation awareness** (**CCSA**) differentiates from the data fusion concepts to avoid confusion, and helps reiterate the importance of studying and improving the situation awareness of the human cyber defender [14].

A. Current State of Cyber-Cognitive Situation Awareness

CCSA is a critical issue to address [14–18]. A recent review assessed the state of CCSA in cyber defense, found several cognitive task analyses but a shortage of experimental work [13]. There is not yet a well-developed understanding of the elements of CCSA, or their measurement.

Difficulty arises due to the unique challenges in cyber defense. For example, analysts are using a large number of different software tools to accomplish their task. Silva and colleagues [19] observed 75 unique software tools in use. These ad-hoc combinations can be unique to analysts, networks and/or organizations, and increase the difficulty of researchers determining the elements of CCSA.

While aspects of cyber-cognitive SA for defense may be generalizable, others will rely on a given toolset or policy implementation, the network itself, and even the organizational structure.

The goal of the current work was to conduct a preliminary cyber-defender cognitive task analysis to identify key elements of information analysts must attend to during operations to guide their decision-making. Existing cognitive task analyses provided starting points [20], [21]. With the amalgamation of tools and interfaces available, awareness metrics need to be agnostic to particular software. Instead, they must be pinpointing the key elements of information that help detect and diagnose cyber threats, which can be present in a variety of different cyber tools. Such measurement can help establish baselines, and used to assess new cyberspace tools and visualizations, new processes, training, and teaming.

II. Cognitive Task Analysis

This section present the methods and results for our cognitive task analysis, focusing on the information and CCSA process of one subset of cyber analysts.

A. Methods

One theme in the literature is the ability of networks and tasks to vary greatly both inside a single organization, and between organizations. Any generalization of findings from CTAs of cyber defenders is difficult. Therefore, prior work is unlikely to meet our requirements for the unique position of the Navy. Several priori cognitive task analyses informed our methodology. D'Amico and colleagues [21] succeeded in assessing the tasks of cyber defense analysts in multiple government agencies. They suggested that the phases of cyber analysis aligned with situation awareness phases of perception, comprehension, and projection. Others [22] focused on an observation of intrusion detection system (IDS) analysts, who completed a card-sorting task based on categories of potential operations activities.

1) Choosing a Task Analysis Method

In selecting the appropriate cognitive task analysis methodologies, we made several considerations.

First, we gathered general information such as organizational structure, physical environment, and the participant's personal understanding of their roles and responsibilities in a general demographic survey, and in a semi-structured interview.

Second, while our goal was to determine situation awareness as it related to intrusion detection and cyber defense in general, the more obvious choice of conducting a Goal Directed Task Analysis required expert knowledge concerning the tasks and work environment. This expertise was not available in the literature, nor to us through personnel..

Third, even though the Critical Decision Method (CDM) is used in safety-critical domains, which have parallels to cyber defense, the primary assumptions require the decision maker to be aware of the specific critical decision, and, works best when recounting a real-time incident. Both of these assumptions were unclear for this environment. The CDM method was set aside in favor of a Knowledge Audit [23]. A Knowledge Audit involves collecting vignettes of incidents while addressing multiple dimensions of expertise. This allowed the flexibility to capture an uncertain environment along multiple dimensions, increasing our understanding of how analysts develop awareness in contextualized systems.

Fourth, experimenters were concerned with the magnitude of domain knowledge. The interactive method of Concept Mapping [23] was selected to prompt participants to visualize and interrelate their knowledge.

2) Participants:

All seven participants were cyber analysts with experience or familiarity with cyber defense, and some knowledge of blue team activities (Table I). The subset discussed here included six participants from the same Navy facility. All had worked on these networks from less than one year, to a maximum of five. Five of the six participants reported experience on other Navy networks. All had spent a minimum of 7 years in government service and had multiple cyber accreditations.

3) Procedure:

Experimenters spent three days in 2015 conducting a three-part cognitive task analysis at a Navy facility. A single moderator led participants through a three-step interview process. Due to time constrains, not every participant was able to answer every question.

Step 1 consisted of a semi-structured interview covering workplace environment and structure, their job description, and tools (Table II). Probing from the moderator elicited further details from the participants.

Step 2 was a knowledge audit, a series of in depth questions targeting expertise, training, decision-making, tasks, and workarounds (Table III). The knowledge audit is a streamlined interview technique focusing on collecting vignettes of incidents while addressing multiple dimensions of expertise. We designed the audit for breadth of data collection, focusing on expertise in the following areas: the past and future, big picture, noticing, job smarts, improvising and spotting opportunities, self-monitoring, anomalies, and equipment difficulties [24]. Breadth can be especially useful in the first round of interviews or a new domain. After initial data collection, unproductive questions could be removed and the audit focused on the most productive areas [24].

In addition to expertise, the knowledge audit afforded the opportunity to collect multiple incident accounts, when one critical example may not be identifiable [23]. The knowledge audit questions developed for this research using a template [found in 25]. The knowledge audit followed a structured format, preventing the moderator from interjecting bias but did allow for clarifying questions by the moderator elicit knowledge from the participants.

Step 3 was an interactive concept mapping activity. During this period, participants interacted with the moderator and note-takers as they mapped concepts and relationships concerning intrusion detection onto butcher paper using note-cards, markers, and tape.

TABLE I: PARTICIPANT DEMOGRAPHICS

Participant Number	Blue Team Experience	Years of Govt Service	Time on Current Naval Network	Experience on Other Naval Networks?	Screens Typically Used in Work Activities
301	Yes	7	1-5 years	Yes	4
302	Yes	16	Less than 1 year	Blank	2-3
303	Yes	17	Less than 1 year	Yes	2-3
304	–	12	1-5 years	Yes	2-3
305	Yes	8	1-5 years	Yes	1
306	Yes	18	1-5 years	Yes	2

TABLE II: GENERAL INTERVIEW QUESTIONS

Interview Questions in Order Presented
*Job description (e.g., forensics, admin, etc)
*Job reiteration to confirm
*Do you typically work in a team, or individually?
*So as a [job title], what tools / software do you generally use?
*What do you use each [tool] for?
*What types of products / documentation do the [tools] produce?
*Can you tell me about some types of events that typically occur in IDS that are important to detect?
*Are some [IDS events] more important than others?
*Are some types of [threat] events more difficult to detect than others? (What are you keying off of when the data comes in)
*Are your awareness needs different for the different types of threats?
*After you identify a threat, what is your next step?

TABLE III: KNOWLEDGE AUDIT QUESTIONS**d**

Knowledge Audit Questions in Order Presented
*Can you walk me through your routine for when you first sit down at your desk at the beginning of the day?
*What do you do first?
*Walk me through checking on the state of your network.
*So when you dig into your network traffic, are you also keeping tabs on the big picture of your network?
*Can you give me an example? (or) Why not?
*How are the tools assisting you with this?
*What about your alerts?
*Can you describe to me how you set up your system / alerts for your network?
*How important is it for an operator new to a network to specify their alerts themselves, versus being handed a set of existing alerts?
*Can you walk me through your most recent successful intrusion detection (if it's not classified)? Start from when you first started noticing something was wrong in your network traffic.
*How do you determine whether a threat is a false alarm, or has real threat potential?
*Are there certain categories of events that more frequently fall into "real threats" versus "false alarms" than others?
*What is the procedure for the "false alarms"?
*Are there any strategies, work-arounds, or shortcuts you find especially useful for this job or network?
*Have you ever paused in the middle of tracking down an intrusion and realized you had to change tactics, or that something else was going on?
*Can you give me an example?
*Are some people just a "natural" when it comes to this kind of work? (if yes) Can you give me an example of what you think makes them naturals?

After an introduction to concept mapping using material reproduced from [26], participants were given a focus question for their map: "What variables (like information or patterns) are necessary for you to successfully detect intrusions in your network?" One participant (302) used help from a previously developed "parking lot" of concept terms. Participant 306 chose not to complete a concept map.

B. Results - Findings from CTA

1) Physical Work Environment

As part of good data practices in reporting task analysis results, we provide some information on the physical environment below. The current set of participants worked at a twenty-four hour facility with a watch floor. As such, we found an open layout, with banks of workstations. *"We encourage them to talk and work together. It can be kind of chatty. That is why the watch officer is there."*

Analysts were co-located with other analysts on the watch floor as well as several large television screens on the wall; *"… a matrix display across the front [is used] for impromptu training, presentations, if someone finds something, we pop them up on the screen so junior [analysts] can follow along"*

There was an adjoining conference room, and cubicles for management stations. On the watch floor itself, there were no high walls between workstations obstructing the view. As seen in Table I, all but one participant reported using more than two computer screens to complete their work.

2) Three Major Areas for CCSA in Cyber Defense

The data reported here is a subset of a larger collection process targeting multiple locations. The initial findings focus on elements of cyber-cognitive situation awareness for cyber defense practices, which reveal three major domains of defense awareness: the network, the world, and internal organization.

We highlight up front one point of interest, which is that these analysts worked "cradle to grave" with cyber incidents. This differs from some of the more distributed, large-scale work in Network Operations Centers (NOC) as reported by Paul and Whitley [22, 27]. In each section, we also highlight the similarities to prior work in this area.

a) The Network

Analysts must maintain their understanding and awareness of the network itself. Of course, networks have multiple attributes which we break down here according to our CTA results.

i) *Network Architecture and State* – the network's software and hardware components are important to know in order to understand vulnerabilities, as well as having this information merged with real time information about patches and updates. Comprehension of this information is a key noise filter when deciding to elevate threats. For example, if a threat targets an unpatched system, and the analyst's network already received the patch, the threat is null.

ii) *Behavior for the Network* – every network has different behavior and traffic depending on what mission it supports, and the characteristics of the people using it. In order to detect abnormal behavior, an analyst must learn the normal patterns of activity on the network. Participants related this to a beat cop knowing his beat and what is normal, implicitly suggesting abnormal behavior for one network is not abnormal for another. For example, a network that supports a business office, closed on the weekends, would see Sunday activity as abnormal unless the analyst is aware that the accounting manager goes in every Sunday for a few hours. Analyst analysis revealed that awareness of the information contained in personnel activity logs should link to information about activity on the network (a form of level 2, comprehension CCSA). Such awareness relating the network data with the comings and goings of real people helps inform analyst decisions about whether activities are malicious; either stream of information in isolation does not provide a clear answer.

Relation to previous CTA - The awareness needs we identified under Network Architecture and State and Behavior of the Network above are closely related to a domain analysis done by Mahoney and colleagues [20]. The categories derived by Mahoney of element *Health Awareness*, *Activity Awareness*, and *Connectivity Awareness* gain support from our current findings. We provide quotations taken from the interviews that support each.

- *Element Health Awareness* – the actual components comprising the network and their current capability or state. *"One of the things we try to work with our team on is understanding what our current state is. Do we still have XP [operating system] in the environment? We may see IDS alerts fire on things that might indicate an attack, [but] if the end device is not an XP device, do we really want our analysts concerned with that chatter?"*
- *Element Activity Awareness* – the normal activity of a network, including timing and patterns of behavior. *"Abnormal traffic, which in order for you to know what that is, you have to go and see the normal events fire over and over to establish a mental baseline. […] Analysts are assigned a beat, a sensor, they know the traffic and when something is off they investigate, do peer review."*
- *Element Connectivity Awareness* – connections or dependencies, both within a network, and between potentially compromised networks. *"You need to know if the networks are connected and the defenses between networks, if I can get into one, can I get into something else?"*

The lack of an exact one-to-one match is expected, as organizational cultures affect how analysts approach the workspace. Our sample of six analysts is also in comparison to Mahoney's single subject matter expert. The distinction may also be that our analysts view these elements as interconnected, mediated by a proprietary common operating picture tool called Phoenix. One analyst commented, for example, *"The actual health, packets flowing. I partner with [organization redacted] to tell me that. […] we have a dashboard to track [health], a status on Phoenix that will tell you."*

iii) *Customer Activities* – this attribute of awareness relies heavily on communication between the defense analyst and their customer. This is awareness of typically abnormal activities that are normal due to special circumstances, like a 24-hour hackathon or inventory. It can also cover technical changes to the network such as upgrades and equipment changes, and awareness of these issues helps an analyst update their mental model of the network state.

iv) *Network Targets* - identifying and protecting the high value target in a network requires understanding what the target is, and what type of attacker might want that information. Thus, awareness of an attacker's intent, and being able to comprehend the goal of linked sets of actions. Health networks have high value personally identifiable information, while a retailer might store

credit card information.

Relation to previous CTAs - The 'Customer Activities' category described here is very similar to *Social / Organizational / Behavioral Awareness* – a customer organization's activity that affects the network's health or persistent behavioral traits [20], especially activities or procedures which are decided arbitrarily by the customer as to what is acceptable. *"We are trying to [get] pretty regular communication with the customer. Most of that happens in the morning, [we] get on the phone with the big customers and get a feel [for] what has happened in the last week, and get a feel for any tasks that are customer driven."*

b) The World

Cyber defense analysts not only must maintain awareness of their own network, but also how they may be affecting or affected by the cyber defense community.

i) *Emergent Threats*– On a regular basis threats are reported through public and private forums and news sources. Outside of strict cyber news, some events may suggest a likely actor or likely intent. Defense analysts must be aware of this information in terms of both the existence of the threat and the time and effort to check the network.

ii) *Abnormal Behavior and Attack Signatures*– Some event management on a network is based on signatures. Systems can automatically thwart some attacks and protect against them. While one community or organization may be equipped and safe, another may not be. Understanding these interconnections and being aware of them may help guide analyst decision-making. "*... it's hard to see the signal […]. Is any of this stuff getting through? Do I have protection mechanisms in place? Do I care that they are constantly scanning me?"* Another analyst commented, *"Having the info on the front end helps us weed out the noise by just knowing what is on the distant end. [for example], knowing when java updates are pushed and our systems are compliant."*

c) The Team

Not all cyber defense analysts work in a team, but all personnel surveyed here indicated a team is critical to their success. Situation awareness in the team-critical environment has been the topic of study, even in the cyber domain [28]–[30]. The team dynamic brings several additional awareness requirements, uncovered in our analysis of cyber defenders.

i) *Work and Handoff Requirements*– the cyber defense analyst working in a team acquires awareness of the work completed and in-progress on their network by other team members. *Completed work* has implications for similar events (How was it solved before? Is the problem truly resolved?). *In-progress work* required an analyst to understand the process and conclusions of the first analyst for a successful transfer. These sometimes must consider the information gathering and sharing requirements across organizations, a recognized struggle of cyber analysts. The process itself has even come under fire in wake of the OPM breach [31].

ii) *Team Processes*– The analyst working in a team also must follow the team processes. For example, to hand off an event ticket: what information is required and what documentation is necessary to share his or her awareness with another analyst? Presumably, needs are generated from the critical elements of information in the environment that helps an analyst diagnose or solve a particular issue. The need to fill in gaps in ticket-sharing interfaces may further influence what an analyst attends to or attempts to record during their work in the future. Several analysts mentioned the centrality of this interface in their work.

iii) *Bootstrapping*– Inter-agency communications between "red" and "blue" teams keeps both on their toes. Although this is not a direct awareness element, it can alter elements that each team or analyst looks for both in defense and offense network actions. Thus, bootstrapping has a place in the CCSA model as providing new knowledge.

C. Results - Concept Map Preliminary Findings

As mentioned, we had analysts generate concept mappings. Our preliminary analysis highlights trends and overlap between the five participants who produced a concept map during the exercise.

1) Concept Map

Fig 1 is a concept map produced by one participant. Multiple concepts are interrelated as part of the analysts' goal-oriented process. One can see the large role that a common operating picture such as the *Phoenix* tool serves as a hub for accessing information both on the system, and on the processes ongoing at the center (e.g., analyst activity found in queues and communications).

Two participants chose to complete the concept map from a red team perspective. Therefore, only the three maps completed from a blue team perspective, are the focus of the remaining analyses here. Their maps included 16, 24, and 23 unique concepts, suggesting some variety (but also, the limitations of the exercise). As was shown elsewhere, analysts may use as many as 75 different tools, each to be consulted for different aspects of the overall network picture [19].

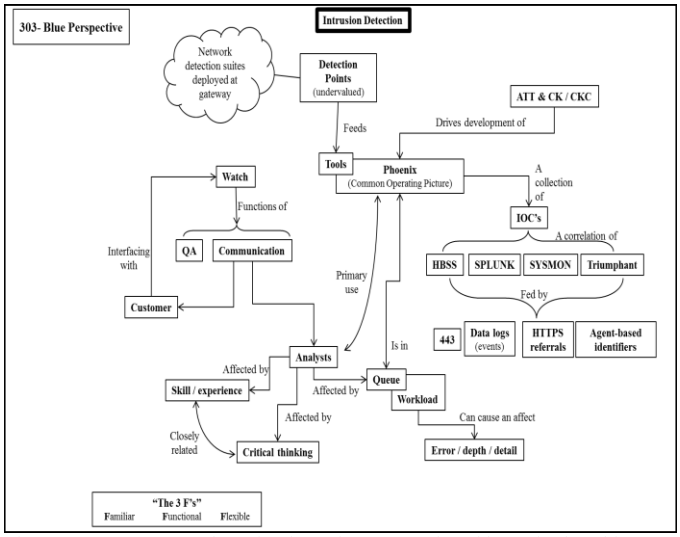

Fig 1. Concept map on detecting intrusions as produced by a single subject matter expert.

2) Concept Map Descriptives

Because the concepts used were often similar but sometimes lexically different, grouping categories were created (Table IV).

TABLE IV: GROUPING CATEGORIES FOR CONCEPT MAP ELEMENTS

Group	Criteria
Action	Any action taken by an analyst, such as 'Implement' or 'Isolate.'
Alert	Any concept referencing an alert, such as 'Firewall Alert.'
Analyst	Any concept box containing 'Analyst' or any pluralization.
Data	Concepts concerning data sources, including logs or specific data element queries.
Environment	Concepts concerning the working environment of the analyst, such as 'Watch' or 'Network.'
Interpersonal	Concepts concerning interactions with customers and team members, such as 'Customer' or 'Communication.'
Phoenix	The Phoenix common operating tool.
Question	Concepts where the analyst is asking a question (to themselves or others) such as 'Event?" or 'Abnormal?'
Reporting	Concepts involved in reporting out, such as 'High level Notification' or 'Reporting (all the details).'
Skill	Concepts related to skills or attributes of the analyst, such as 'Critical Thinking' or 'Skill / Experience.'
Tool	Concepts containing a tool that is not Phoenix, such as 'Triumphant' or 'SPLUNK.'

Fig 2 is a graph of the frequency of each of these concept groupings, with Data, Tool, Question and Action having the greatest prevalence. A broad need exists for analysts to access the various data sources (e.g., router logs).

We plan for additional analyses on linking phrases, similar to assessing the connections in propositional networks. These analyses are likely to reveal dependencies and references between categories as revealed to us here. Linkages will become more important as we look across organizations and tiers of cyber defense. However, they are very dependent on the elements revealed through CTA, and may not be dependable – this assumption should be tested.

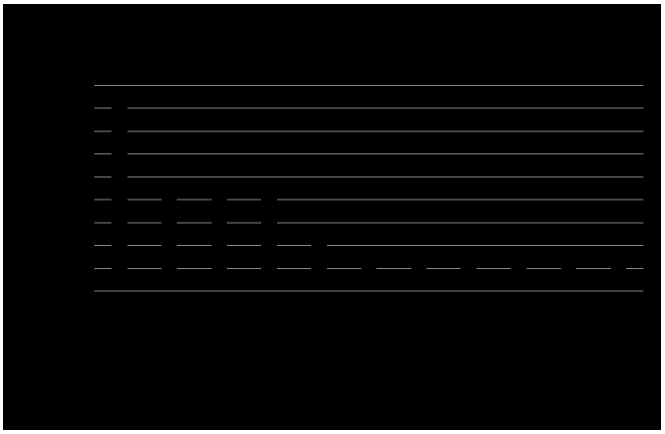
Fig *2*: Total counts of the 11 grouped categories.

III. CONCLUSIONS AND FUTURE PLANS

The number of concepts identified by each participant throughout the CTA suggests that cyber defense is indeed a complex, cognitively demanding environment. Analysts need to perceive multiple data sources, comprehend relationships between them, and build a representation not just of the network, but also of the social elements surrounding it. We and others [14, 18, 32] have confirmed that the defensive environment in particular is ripe for the study of cyber-cognitive situation awareness (CCSA).

From our assessment of the concept maps, we find a large impact of noticing different types of data, and the *interconnected* nature of the data itself (Fig. 2, Fig. 3, and Table IV). Many of the linkage phrases connect sources of data, indicating, in a cognitively insightful way, the intrinsic value data-fusion methods provide. However, analysts need awareness information in the moment of formulating decisions, and often this means holding information "in the mind" rather than "in the world," a testable assumption that future work can address.

One novel finding is that our analysts worked cradle to grave. In other environments and tiers of service, this may be unfeasible due to the sheer amount of incoming information (to a NOC, for example). The work structure may create unique challenges to cyber-cognitive situation awareness by requiring more skill, and potentially more interaction with other organizations, and multiple tool sets as defense analysts move through phases (c.f., [21]). Thus, different tiers are more or less taxed due to differences in available human resources.

Another difference is that our analysts helped to establish their own unique set of processes and training to deal with their environment. One of their main tools, in fact, was developed in-house with their direct involvement, highlighting the power of user-centered design to address the specific needs of a population. Of course, users are not always accurate judges of whether a display actually helps them (see [33]).

We recognize some limitations to our methods. A wide variety of potential methods for CTA exists. In this domain, and moving forward, we hope to conduct a goal-oriented task analysis. We believe such a method will elucidate the elements for CCSA assessment in cyber defense. As a final note on the

future of CTAs in this area, a more robust and rapid method for soliciting and reporting knowledge from cyber analysts needs to be implemented. Even a complete cognitive task model may become stale as new threats emerge, and policy changes alter the *how* and *when* of sharing information. Developing a way to update and maintain fidelity of CTAs will directly influence the utility of interface designs, for example.

We expect to use the knowledge derived here to shape experiments on humans in cyber network defense. Both creating and validating CCSA measures in defensive scenarios, in which the analysts are engaged in active tasks, hinges on the existence of a platform for human-in-the-loop experimentation and measurement [14]. While these platforms are emerging, the available work in them is limited and the platforms may not always be ecologically valid, due to the complexities of the cyber defense task.

REFERENCES

[1] M. Garnaeva, V. Chebyshev, D. Makrushin, R. Unuchek, and A. Ivanov, "Kaspersky security bulletin 2014: Overall statistics for 2014," *Kaspersky Lab*, pp. 1–31, 2014.

[2] DHS, "Incident Response Activity: Trends in incident response in 2013," *ICT-CERT Monit.*, no. December, pp. 1–14, 2013.

[3] L. Grisham, "Timeline: North Korea and the Sony Pictures hack," *USA Today*, pp. 1–3, 2015.

[4] D. Bisson, "The OPM breach: Timeline of a hack," *Tripwire*, pp. 1–8, 2015.

[5] J. Sametinger, J. Rozenblit, R. Lysecky, and P. Ott, "Security challenges for medical devices," *Commun. ACM*, vol. 58, no. 4, pp. 74–82, Mar. 2015.

[6] W. Yurcik, J. Barlow, and J. Rosendale, "Maintaining perspective on who is the enemy in the security systems administration of computer networks," *ACM CHI Work. Syst. Adm. Are Users*, 2003.

[7] J. Li, X. Ou, and R. Rajagopalan, "Uncertainty and Risk Management in Cyber Situational Awareness Abstract," *ARO Work. Cyber Situational Aware.*, 2009.

[8] M. Line, A. Zand, G. Stringhini, and R. Kemmerer, "Targeted Attacks against Industrial Control Systems: Is the Power Industry Prepared?," *Proc. ACM Work. Smart Energy Grid Secur.*, pp. 13–22, 2014.

[9] S. Hunt, R. S. Gutzwiller, D. Rousseau, and R. Iden, "Characterizing the human limitations and impediments to cyber situation awareness," *Appl. Hum. Factors Ergon. Annu. Meet.*, Poster, 2015.

[10] M. R. Endsley, "Toward a theory of situation awareness in dynamic systems," *Hum. Factors*, vol. 37, no. 1, pp. 32–64, 1995.

[11] T. Bass, "Intrusion detection systems & multisensor data fusion: Creating cyberspace situational awareness," *Commun. ACM*, pp. 99–105, 2000.

[12] U. Franke and J. Brynielsson, "Cyber situational awareness – a systematic review of the literature," *Comput. Secur.*, vol. 46, pp. 18–31, Jul. 2014.

[13] R. S. Gutzwiller, "Cyber-cognitive situation awareness: A review and future directions."*Under Review*

[14] R. S. Gutzwiller, S. Fugate, B. D. Sawyer, and P. A. Hancock, "The human factors of cyber network defense," *Proc. Hum. Factors Ergon. Soc.*, vol. 59, pp. 322-326, 2015.

[15] M. Boyce, K. Duma, L. Hettinger, T. Malone, D. Wilson, and J. Lockett-Reynolds, "Human Performance in Cybersecurity: A Research Agenda," *Proc. Hum. Factors Ergon. Soc. Annu. Meet.*, vol. 55, pp. 1115–1119, 2011.

[16] Y. Tenney and R. Pew, "Situation awareness catches on: What? So what? Now what?," *Rev. Hum. Factors Ergon.*, 2006.

[17] R. E. T. Jones, E. S. Connors, and M. R. Endsley, "A framework for representing agent and human situation awareness," *IEEE Int. Inter-Disciplinary Conf. Cogn. Methods Situat. Aware. Decis. Support*, pp. 226–233, Feb. 2011.

[18] B. A. Knott, V. F. Mancuso, K. B. Bennett, V. Finomore, M. McNeese, J. A. McKneely, and M. Beecher, "Human factors in cyber warfare: Alternative perspectives," *Proc. Hum. Factors Ergon. Soc. Annu. Meet.*, vol. 57, pp. 399–403, 2013.

[19] A. Silva, J. Mcclain, T. Reed, B. Anderson, K. Nauer, R. Abbott, and C. Forsythe, "Factors impacting performance in competitive cyber exercises," *Proc. Interservice/Interagency Training, Simul. Educ. Conf.*, 2014.

[20] S. Mahoney, E. Roth, K. Steinke, J. Pfautz, C. Wu, and M. Farry, "A cognitive task analysis for cyber situational awareness," *Proc. Hum. Factors Ergon. Soc. Annu. Meet.*, vol. 54, pp. 279–283, 2010.

[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," *Proc. Hum. Factors Ergon. Soc. Annu. Meet.*, vol. 49, pp. 229–233, 2005.

[22] C. Paul and K. Whitley, "A taxonomy of cyber awareness questions for the user-centered design of cyber situation awareness," in *Lecture Notes on Computer Science: HAS/HCII 2013*, L. Marinos and I. Askoxylakis, Eds. Springer-Verlag Berlin Heidelberg, 2013, pp. 145–154.

[23] B. W. Crandall, G. A. Klein, and R. Hoffman, *Working minds: A practitioner's guide to cognitive task analysis*. Cambridge, MA: MIT Press, 2006.

[24] L. G. Militello and R. J. B. Hutton, "Applied cognitive task analysis (ACTA): A practitioner's toolkit for understanding cognitive task," *Ergonomics*, vol. 41, no. 11, pp. 1618–1641, 1998.

[25] R. R. Hoffman, "Protocols for cognitive task analysis," *Inst. Hum. Mach. Cogn.*, 2005.

[26] J. Novak and A. Canas, "The theory underlying concept maps and how to construct and use them," *IHMC Tech. Rep. 2006-01 Rev 2008-01, C.*, 2008.

[27] C. Paul, "Human-centered study of a network operations center: experience report and lessons learned," *Proc. ACM Work. Secur. Inf. Work.*, pp. 39–42, 2014.

[28] K. Sulistyawati, C. D. Wickens, and Y. P. Chui, "Exploring the concept of team situation awareness in a simulated air combat environment," *J. Cogn. Eng. Decis. Mak.*, vol. 3, no. 4, pp. 309–330, 2009.

[29] D. B. Kaber and M. R. Endsley, "Team situation awareness for process control safety and performance," *Process Saf. Prog.*, vol. 17, no. 1, pp. 43–48, 1998.

[30] M. Champion, P. Rajivan, N. J. Cooke, and S. Jariwala, "Team-based cyber defense analysis," *Cogn. Methods Situat. Aware. Decis. Support*, pp. 218–221, 2012.

[31] J. Moore, "Watchdog: DHS still struggles with cyber response," *Nextgov*, 2015.

[32] P. Barford, M. Dacier, T. G. Dietterich, M. Fredrikson, J. Giffin, S. Jajodia, S. Jha, J. Li, P. Liu, P. Ning, X. Ou, D. Song, L. Strater, V. Swarup, G. Tadda, C. Wang, and J. Yen, "Cyber SA: situational awareness for cyber defense," in *Cyber Situational Awareness*, 2010, pp. 3–14.

[33] H. S. Smallman and M. B. Cook, "Naïve Realism: Folk fallacies in the design and use of visual displays," *Top. Cogn. Sci.*, vol. 3, no. 3, pp. 579–608, Jul. 2011.