Collaborative Data Analysis and Discovery for Cyber Security

Diane Staheli, Vincent Mancuso, Raul Harnasch, Cody Fulcher, Madeline Chmielinski, Adam Kearns, Stephen Kelly and Era Vuksani

MIT Lincoln Laboratory
Lexington, MA
{diane.staheli, vincent.mancuso, raul.harasch, cody.fulcher, madeline.chmielinski, akearns, stephen.kelly, era.vuksani}@ll.mit.edu

ABSTRACT
In this paper, we present the Cyber Analyst Real-Time Integrated Notebook Application (CARINA). CARINA is a collaborative investigation system that aids in decision making by co-locating the analysis environment with centralized cyber data sources, and providing next generation analysts with increased visibility to the work of others. In current generation cyber work, tools limit analyst's ability to collaborate, often relying on individual record keeping which hinders their ability to reflect on their own work and transition analytic insights to others. While online collaboration technologies have been shown to encourage and facilitate information sharing and group decision making in multiple contexts, no such technology exists today in cyber. Using visualization and annotation, CARINA leverages conversation and ad hoc thought to coordinate decisions across an organization. CARINA incorporates features designed to incentivize positive information-sharing behaviors, and provides a framework for incorporating recommendation engines and other analytics to guide analysts in the discovery of related data or analyses. In this paper, we present the user research that informed the development of CARINA, discuss the functionality of the system, and outline potential use cases. We also discuss future research trajectories and implications for cyber researchers and practitioners.

Keywords
cyber security, data analysis, collaboration, sensemaking, situational awareness

1. INTRODUCTION
Over the last several years, cyber security and operations have come to the forefront of the national discussion. With cyber attacks, data breaches, and information security threats occurring on a seemingly daily basis, it is no surprise that the Department of Defense has identified cyber as a key research trajectory for ensuring national security [1]. From the network defense perspective, cyber is a cognitively demanding task. Analysts are responsible for analyzing massive amounts of data to identify interesting or anomalous activity, a proverbial needle in the haystack. Analysts rely primarily on their own cognitive resources to interpret observed network activity using their mental model of what constitutes "normal" for a given network or adversary behavior based predominantly upon prior observations. The majority of this synthesis activity takes place internally to the human mind, placing a significant cognitive burden on the Analyst; "the cognitive skill involved in detecting relationships is so critical that any procedures or aids that can expedite or enhance it would improve the analysis process" [2]. In the event of an attack or threat, Analysts must identify the adversaries and their capabilities, the intended victims, and formulate a hypothesis of the intent of the attack [3]. This burden is magnified when scaling the analysis process to the team level, particularly when analysis must be conducted and decisions must be made across geographic and functional boundaries [4].

Currently, the majority of work in human-centered network defense focuses on the analytical and decision making processes of a singular Analyst, with less attention on collaboration, information sharing and team cognition. This lack of research in team cyber operations has created a significant gap in technology as Analysts are required to find ad-hoc methods to transition from individual to team decision making.

1.1 Team Decision making in Cyber Operations
Existing research in cyber mainly focuses on either analysis and decision making processes [e.g. 5, 6] or uses non-experts in their testing [7-9]. Currently, there is limited research that focuses on team decision making in cyber operations [7-10]. Much of this work focuses on the collaborative processes, rather than on how to improve such outcomes by supporting the collaboration.

Previous work in fields such as Human-Computer Interaction and Computer Supported Cooperative Work has found that the design of online collaboration systems can facilitate positive collaborative behaviors, and support distributed team decision making. These tools often focus on providing distributed teammates with an awareness of each other's activities within a given environment [11]. Though research has demonstrated that online collaboration systems can encourage and facilitate distributed teams in sharing information and group decision making [12], no such technology exists today for cyber defenders. Existing tools such as i2 Analyst Notebook provide basic data visualization and annotation capabilities, but have significant interaction problems [2] and do not have cyber-specific capabilities.

1.2 A User-Centered Design Approach
To improve decision making in cyber, at both the individual and team level, research must focus on better understanding their current ad-hoc practices, identifying the processes and pain points, and transitioning these practices into a system that can support and improve their work. In pursuit of this, we adopt a user-centered design approach. The International Usability Standard [13] specifies that a successful user-centered design approach must: be based upon explicit understanding of users, tasks and environments; involve users throughout the design and

development; be driven and refined by user-centered evaluation; be an iterative process; address the whole user experience; and include a team with multidisciplinary skills and perspective. Figure 1 illustrates the phases and notional activities of the user-centered design approach.

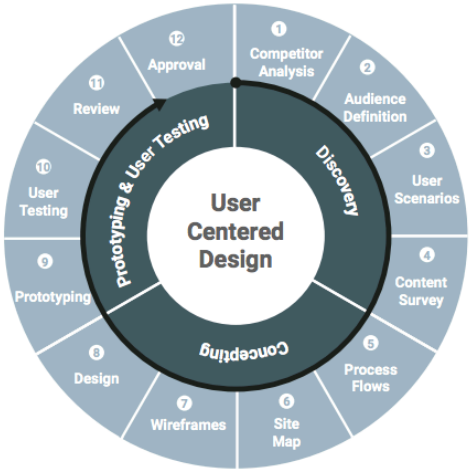

Figure 1: Visual depiction of User-Centered Design Approach

In this paper, we present a preliminary in situ research study with cyber analysts to examine the tools used for analysis and evidence collection, existing formal workflow and informal collaboration, mechanisms for data collection and storage, and the cognitive processes that transform data to insight. The data collected during this study will be used to design and prototype a visual analytics system to support cyber collaboration and analysis. From this approach, we present the Cyber Analysts-Real Time Integrated Notebook Application (CARINA). CARINA, developed using a user-centered design approach, is a collaborative system that aids in decision making by co-locating the analysis environment with centralized cyber data sources and providing analysts with increased visibility into the work of others. In the following paper, we present our research from the "discovery phase" of the user-centered design cycle. This research helped identify key requirements and functionality that informed the development of CARINA. Applying these requirements, we present a prototype of our system, and discuss future research.

2. DISCOVERY

2.1 Overview

The goal of the discovery phase is to learn about and model users, and to elicit and define clear product requirements. By incorporating the users at an early stage, we are able to focus on understanding the users themselves, as well as the tasks they will preform. This stage is critical in ensuring a comprehensive set of task related goals and understood constraints to guide future system development.

For this research effort, we conducted our field research with a global organization that federates the functions and responsibilities of cyber operations across its geographically distributed workforce. These work centers shared the responsibility for various functions of the organization's cyber security; staff must collaborate and share information across centers to perform their function effectively. We conducted on-site interviews at these operations centers, with cyber security staff at all levels of the organization. From the interviews, we utilized a data-driven approach to construct a set of user personas and scenarios that are representative of the environment.

2.2 Data Collection and Analysis

We utilized semi-structured interviews to elicit information from participants about their work. Questions consisted of six broad areas of interest relating to demographics (age, profession, work experience, certifications), job responsibilities (daily tasks, work load, tools used), collaboration (organizations contacted the most, means of communication), decision making (types of decisions made, how much information is needed to make a decision), and qualitative assessments of the working environment (what works well, areas of improvement). In total there were fourteen a priori questions, however interviewers were permitted to ask follow-up questions to ensure thorough responses. Interviews, which lasted thirty minutes to an hour, were conducted with 37 individuals spanning several job junctions, across 8 work centers, over the course of three months.

Based on the data gathered, the team produced a set of four data-driven user personas [14], organized by their job functions. These personas function as a means to clarify audience definition. They assist in modeling behavioral characteristics of target users, reasoning about user needs specific to the problem space, and mapping personas to software features. Individual interview responses were separated and mapped by persona onto Persona Scales [15] to extrapolate trends. For each persona, details surrounding their experience, certifications, goals, pain points and decision making behaviors were extracted.

From these findings a set of system requirements were extracted to inform the design of the CARINA prototype in the conceptual phase of the user-centered design process.

2.3 Personas

Based on the interviews, we synthesized roles into four main personas, Cyber Analyst, Supervisor, Manager and Director. These roles were designed to not only be representational of our findings in the discovery phase, but also to be generalizable for use in a variety of organizations and related contexts.

2.3.1 Cyber Analyst

Cyber Analysts are responsible for monitoring data from incoming indicators, reports, or sensors to identify malicious traffic. During the day, their goal is to develop insights into relationships between data points and recurring patterns to create more accurate and meaningful reports. To accomplish this, they are responsible for making decisions involving whether or not to produce a report, or pass along information that they deem important. During the interview, several pain points emerged: answering to multiple supervisors, lack of awareness of other Analysts' work, workflow inefficiencies, and lack of situational awareness of the overall efforts of the organization.

2.3.2 Supervisor

Supervisors are primarily responsible for delegating tasks and authorizing reports for higher-level review; however they also aid in mentoring Analysts. Their overall goal is to provide efficient and thorough analysis of malicious or anomalous activity. During their tasking, they make decisions based on whether or not a report is complete and accurate, and whether it should be passed on or reworked. Additionally, they have to make decisions on how to divide and delegate tasks amongst the Analysts. Their primary pain points center around inter- and intra-office collaboration, specifically, coordination between locations (inter-office), as well as communication and handoff of investigations within their own

teams (between shifts). Other pain points include being the sole bottleneck for report approval, and offering sufficient training opportunities to grow their Analysts.

2.3.3 Manager

Managers are responsible for coordinating activity across teams and organizations, and carrying out the goals of Director-level leadership (and above) for their own organization. Managers aim to unify the effort, provide situational awareness and ensure the smooth functioning of the organization. They are in charge of deciding on what information is presented to leadership and prioritizing the work of their immediate location. Their main points of pain include inconsistent reporting requirements across the role, lack of visibility and one-directional interactions with other locations.

2.3.4 Director

Directors often rely on the expertise of their workforce to gather essential elements of information in support of organizational decision making. Their overall goal is to execute cyber missions in support of the parent organization's goals. They are responsible for assessing risk, and prioritizing their actions in relation to the organization at large beyond their geophysical location. Pain points include lack of contingency plans, situational awareness, data overload, lack of information on issues, costs and resolutions, and need for backup plans.

2.4 Key Findings

Based on the interviews and the persona outputs, we present two key findings on the collaborative nature of the work, and the types of decisions that were made at the different levels of the organization.

Analysts Collaborate the Most: During the interviews, we asked Analysts to enumerate the organizations that they collaborated with or shared information with during a typical workday. We organized this information into communication graphs for analysis. Although we interviewed personnel at 8 locations, our analysis revealed 26 distinct organizations that were part of the information ecosystem. Most of the communication was taking place at the Analyst level; the higher the rank of the individual, the lower the degree of collaborative activity participation. This could be the result of established, formal channels of communication that exist at higher levels and higher ranks. Analysts, who collaborated the most, were required to work with the Supervisor above them, but also communicate with other Analysts in an attempt to develop situational awareness of observations being made at other locations. Supervisors primarily worked with their own Analysts, though occasionally discussed issues and coordinated across groups. Similarly, the Manager was responsible for communicating with Supervisors below, but many of their interactions were one-directional with limited collaboration. Finally, the Directors have many responsibilities and limited time and attention to devote to collaboration, resulting in a lack of bandwidth for communication and collaboration at their own level and below. This results in a system in which information is pushed up, and decisions were pushed down, all with limited collaboration, except at the lowest levels. Figure 2 demonstrates this collaborative hierarchy.

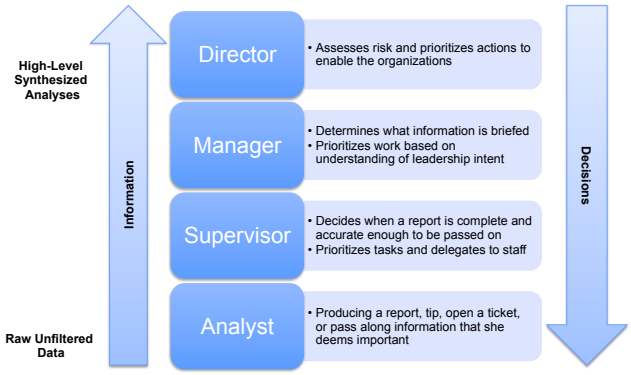

Figure 2: Personal Hierarchy and Interactions

This layout, consistent with a hierarchical organization has both positive and negative outcomes. While it facilitates collaboration across levels (up and down the hierarchy), it creates structural holes within each level. Structural holes, especially at the higher levels of an organization have been shown to have a negative impact on innovative behavior and result in a decrease in performance outcomes [16]. These holes can result in a lack of overall awareness of the organizational status at higher levels, and result in a decrease in coordinative behavior at lower levels

Polarity in Decision Making: A second key finding revolved around the polarity in decision making at all levels. Individuals described the decisions that they make on a regular basis as either very simple or very complex, with very little in-between. Simple decisions included atomic events that occurred within a single organization. These often had a low operational impact and financial cost, and had simple tradeoffs. Due to the simplicity of these decisions, the Analysts were often the final decision maker, with individuals above them having limited awareness of them even occurring. This is due largely to the establishment of standard operating procedures for incident handling and reporting. Examples include, whether or not to pass along a report, opening or closing a ticket, and remediation of a known vulnerability. On the other hand, complex decisions spanned multiple events and locations, and required involvement from people across the organization (both laterally and vertically in the management chain). These decisions often had high operational impact and financial cost, and many tradeoffs that needed to be considered. Interestingly, we found little evidence of decision making with medium complexity present at any level. This is consistent with the managerial literature which considers the complexity and size as binary, either major or minor [17]. Finally, and possibly the most troubling, was that we found no evidence of a chain or hierarchy of decisions from simple to complex.

Based on these findings, we suggest that improving the ability to collaborate and share information at the Analyst level will improve the quality of the analysis and speed at which information is distributed, both laterally and hierarchically.

2.5 System Requirements

We used the interview data, personas, and our findings to generate requirements for a tool to facilitate collaborative analysis. These requirements, defined in Figure 3, would be used with varied regularity depending on the individual and the complexity of their decision making task.

Figure 3: Matrix of Tool Requirements and Usage By Persona

These tool requirements were translated into six primary actions that had to be implemented into the system: (1) Analyze data, (2) Build an investigation, (3) Share an investigation, (4) Track an investigation, (5) Annotate an investigation, (6) Brief an investigation. These actions were then rolled into the prototype discussed more in the following sections.

3. CARINA

In the following section, we present a system concept called Cyber Analyst Real-time Integrated Notebook Application (CARINA). CARINA aims to positively impact decision making laterally and hierarchically by centralizing the analysis community. To achieve this, CARINA provides Analysts increased visibility into the actions of others, facilitates the discovery process, and promotes unity of effort among community.

We envision CARINA as a collaborative data analysis platform, integrated as a key component of a big data analytic infrastructure. Mature platforms tailored for the cyber environment have started to emerge, making this approach feasible. This design choice helps to focus Analysts on analysis by co-locating data with the tools. This ensures Analysts do not have to interrupt exploration to figure out how to find, capture, or export data from multiple tools, and can more readily focus on the task at hand. This integrated environment can function as an extension of an Analyst's cognition, making it easier for the Analyst to enter a flow state, and minimizing interruptions that have high cognitive cost.

3.1 Watchfloor Management

The Watchfloor Management screen (Figure 4) orients the Analyst to the days' tasks, and provides information from news/reporting sources that might be relevant to the tasks at hand. The Watchfloor Management screen assists Supervisors and Managers to identify roles present on the floor and monitor the activity stream of Analysts, providing greater transparency into tasking.

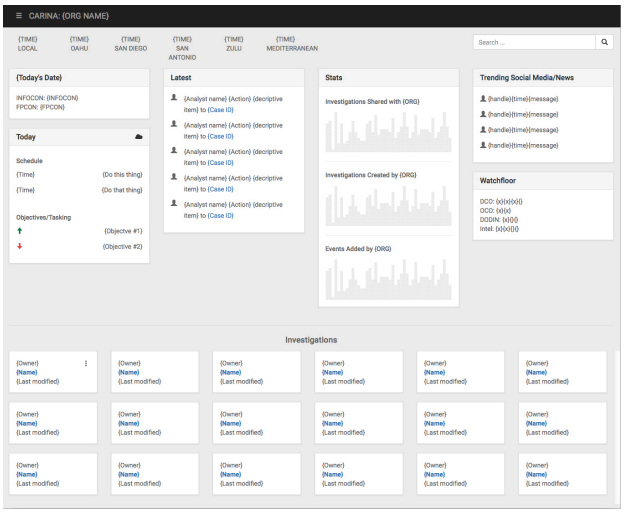

Figure 4: CARINA Watchfloor Management Screen

3.2 Organizational Leaderboard

The Organizational Leaderboard visualizes who the most active collaborators are, both on an individual and on an organizational level. The Leaderboard aims to provide greater visibility into collaborative insights and incentivize collaborative behaviors. Our user study revealed that Analysts are de-incentivized to share data or interim analyses as an expert Analyst's reputation is built upon being the one to find the needle in the haystack. Tools for collaboration must address this concern to be successfully adopted, and help to transform the behaviors of the intended audience. By exposing collaboration metrics in this fashion, we can provide ways to incentivize Analysts differently in more productive ways; measuring contributions to investigations, sharing of cases with others, and use the leaderboard model to rank Analysts along these dimensions.

3.3 Investigation Browser

The Investigation Browser (Figure 5) allows all users to view the current stream of investigations in the process. Each investigation is represented using a graphic snapshot that visualizes the data points contained within. The display also indicates the number of active users involved in an investigation, and highlights the organization that they represent.

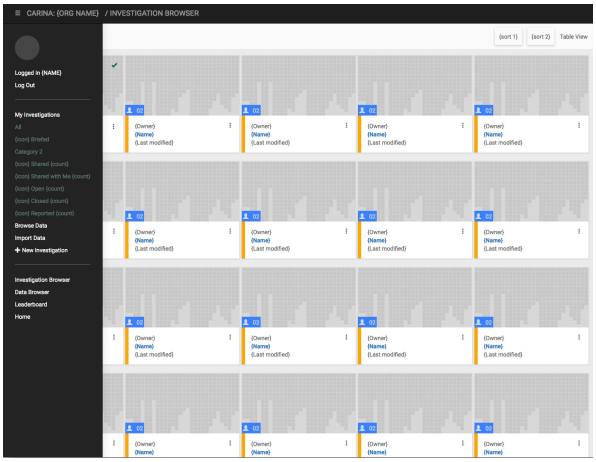

Figure 5: CARINA Investigation Browser

The investigation browser provides the ability to explore both internal and external investigations. Different organizations have different data sources and different points of visibility into network activity, as well as different baseline activity patterns. By unifying investigations into one platform, we aim to provide more complete insights into distributed networks.

3.4 Data Browsing and Search Capabilities

Data Browsing/Search (Figure 6) allows Analysts to construct complex queries and ask questions of multiple data sources to answer their analytic questions. As Analysts make meaningful discoveries in the data, they have the ability to "snip" data to save off into case files. They also have the option to save their search query to either revisit at a later date, or to receive notifications of new results.

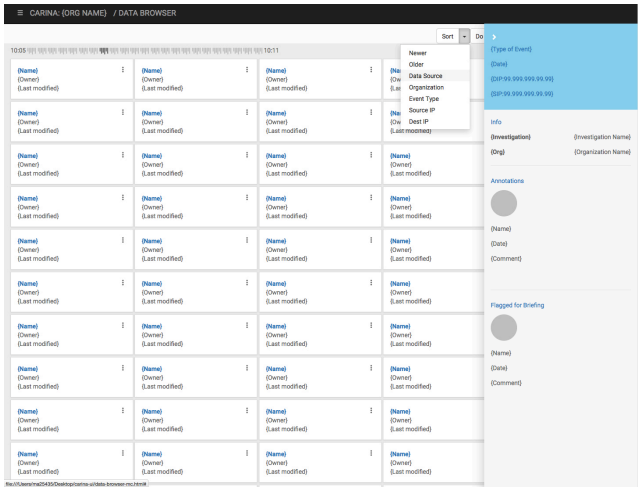

Figure 6: CARINA Data Browser and Search Screen

3.5 Analyst Sandbox

The Analyst Sandbox is designed to be a digital space equivalent to an Analyst's notebook or whiteboard, and comprises four elements to support the analytic process:

- Investigations: Analysts actively track work-in-progress as Investigations.
- Personal Data Library: Analysts create their own personalized views of available data, using multiple mechanisms such as saved searches, watch lists, targeted collection.
- Recommendations: Analysts receive recommendations from the system on similar cases or additional relevant data sources.
- Visualization and Analytics: Analysts can choose from a library of visualizations and analytics that can be applied to the data to assist sensemaking.

The CARINA system translates Analyst process from analog to digital by providing a framework for Analysts to capture both structured data and unstructured insights in the same space. By providing context alongside shared data, the process of sharing early-stage analysis becomes feasible and repeatable. Highlighting connections between cases helps Analysts to converge on major problems before they become larger problems. The initial implementation will be relatively simple, but will allow for more advanced analytics to be applied to the data and incorporated into the data stream.

3.6 Investigation Construction

Items of interest are organized into Investigations, which can be either simple tasks, or more complex activities such as kill chain analysis or comprehensive threat assessment. The primary organizational unit of the Investigation is the data "snippet." Snippets can be annotated and linked together to best reflect the analysis. From the Data Browser, Analysts are able to select the data snippets they are most interested in, and add them to an ongoing or new investigation (Figure 7).

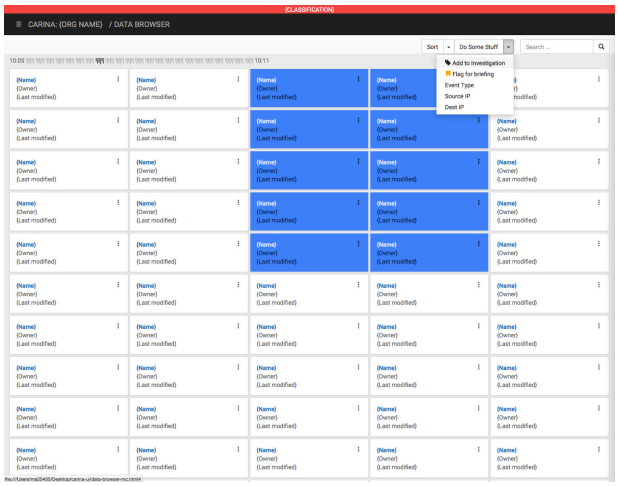

Figure 7: Example of Analyst adding Snippets to investigation in Data Browser

The Investigation is also the primary unit of sharing and collaboration, either laterally to other Analysts, or hierarchically to brief at the Director level. Investigations can be made discoverable by others or kept private until analysis is complete. Sharing analysis at an earlier stage of event workflow (vs. finalized reports and indicators) between Analysts and organizations enables earlier response to potentially malicious activity, reducing attack surface and potential mission impact.

By integrating briefing capabilities with the tool, CARINA helps automate the conversion of information between deep detail for Analysts and the "so what" for senior leaders. This helps by focusing Analyst time more efficiently on operational tasks rather than briefing tasks. Integrating briefing into the tool serves to provide de facto standards for the way cyber information is briefed, sets expectations for Directors, and reduces the need for personality-driven approaches.

3.7 Integration of Features

The overall goal of CARINA was to integrate and support the Pirolli and Card model of sensemaking [18], illustrated in Figure 5. This model is broken up into two major loops of activities, (1) the foraging loop, that supports information discovery, and (2) a sense making loop that supports the construction of a mental model. By leveraging this model, CARINA can support both top-down (from theory to data) and bottom-up (from data to theory) decision making. As seen in Figure 5, analysts can go between the top-down processes (top) and bottom-up processes, across numerous loops depending on the type of decision, and the current situation.

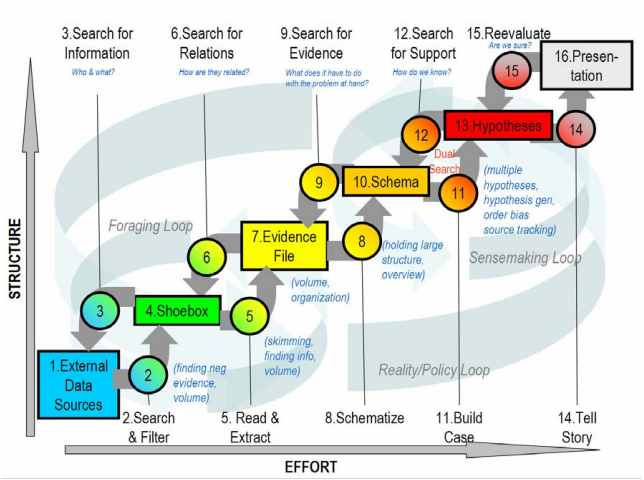

Figure 8: Pirolli and Card Model of Sensemaking (Figure taken from [18])

Leveraging this model, CARINA was designed to ensure that analysts were able to operate across the top-down and bottom-up processes, as well as work within the various loops that span the two. Together, the Data Browsing/Search, Analyst Sandbox, and Investigation Features provide the capability to support the above model while adding support for a team as described by Table 3.

Table 1: CARINA support for bottom-up sensemaking [18]

Model Element	*CARINA Feature*	*CARINA Support*
2, 3	*Search*	CARINA extends the scope of where evidence might be found. The current model contains an implicit assumption that the raw data sources are the only source of information. The CARINA model hypothesizes that shoeboxes and evidence files from other Analysts could also be valuable sources of information
5, 6	*Sandbox*	CARINA assists with the extraction of information by providing suggestions about appropriate related information and similar entities.
8, 9	*Investigation Visualization*	By sharing the same CARINA workspace, Analysts can develop a common schema for how they organize, represent and communicate information.
11, 12	*Investigation*	The collaboration features of CARINA facilitate the creation of cases by extending the generation of hypotheses from the individual Analyst to multiple Analysts. Multiple Analysts can be tasked to collect evidence in support of the case, or to produce counter-arguments, eventually converging on an agreed-conclusion.
14, 15	*Visualization, Annotations, Investigation Brief*	Self-service visualization, annotations, and the automated brief assist Analysts to tell the story that they see in the data, augmented by artifacts produced by other Analysts in other locations.

4. VISION

We envision CARINA as a first step towards a more intelligent approach for human-computer interaction in big data analysis. Enhanced capabilities enabled by CARINA, particularly in the Investigation, Brief, Search, and Sandboxing components, offer a rich set of interactions, data assessments, and feedback that can be utilized for improving analytic processes at both the individual and team level. This data is typically absent from big data analysis tools, and is essential for better integration of algorithmic and Analyst-driven data discovery, processing, and triage.

By capturing Analyst interactions with data, we create the potential to learn and model how an Analyst's current task aligns with data. These models can be used as an approximation of Analyst mental models, and can greatly improve identifying data relationships, relevance, and priority. When learned and applied correctly, these models can improve stand-alone components of the CARINA system including recommendation within the Data Search/Browsing tools, highlighting relevant portions of data in the Sandboxing tools, and pre-staging likely events within the Investigation tool.

Additionally, examining these models across teams could result in an improvement in collaborative tasks. Collection and linking of annotation results from the schema building phases (Figure 5) of analysis offers the potential for identifying complex relationships between how Analysts with varying levels of experience and expertise think of similar pieces of data. Generation of such connections could result in a number of new capabilities supporting collaborative tasks including the construction and utilization of knowledge-bases and automated contextualization of results in the presentation phases of the analytic process.

5. FUTURE WORK

In the future we plan to use CARINA as a research platform for not only understanding cyber decision making, but also team behaviors within cyber operations. As we continue to mature our designs, a key question that must be answered first and foremost, is how team-decision making can be evaluated in such a platform. This is key in understanding the usability, utility and efficacy of the technology. Capturing collaboration is a complex and difficult task due to the invisible nature of many of the constructs. However, we are confident that the data from the users within the system can inform us of the collaborative work that is occurring within CARINA. Using this data, we can return to the personas to answer questions about whether the size and scope of the individual decisions have changed, whether users have adopted new communication strategies, and how the role of each of the personas factors into a decision. For this evaluation, we plan to deploy CARINA in a real world cyber operations center, and capture data to mature and refine both the system and the personas.

In addition to refining the system and personas, the interactions mined from the system can be used to inform other cyber research. Communication has been cited as being the best insight into team cognitive and collaborative processes [19]. By capturing a detailed log of interactions within the system we hope to provide organizational level awareness on the current collaborations and work being done in CARINA. Managers can ultimately use this information for future tasking orders and/or policy changes. By understanding who is working on what tasking, and the division of labor in the organization, supervisors and managers may be able to more effectively delegate out work, ensuring that no individual becomes overloaded. Also, this may help remove bottlenecks by automating some of the information sharing, and created better visibility within each level and across levels.

We plan to use this system to help inform the design and deployment of cyber sensors, and data sources. Through the

collection of evidence data, we plan to develop a better understanding of how each data type is being utilized. This will shed light on whether certain data sources are not trusted, or if they have limited utility when compared to another source. This knowledge can then in turn be used to inform future installations of CARINA.

Finally, we plan to explore the use of CARINA in domains other than cyber security. Collaborative data analysis is not limited to the cyber realm, and we hope to pilot the capability to an additional domain to test the generalizability of the approach.

6. CONCLUSION

As cyber analysis and decision making increase in complexity and scale, it becomes important to have tools that can better integrate, automate, aggregate, and contextualize portions of the analytic and decision making process for an individual and across an organization. We view CARINA as a first step towards providing these capabilities and believe that annotations, interactions, and feedback collected from the use of the tool will unlock further developments in improving the state of the art in human-computer interaction.

ACKNOWLEDGEMENTS

This material is based upon work supported by the Department of the Navy 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 Department of the Navy.

REFERENCES

[1] M. Maybury, “Toward the Assured Cyberspace Advantage: Air Force Cyber Vision 2025,” IEEE Security & Privacy, 13(1), 49-56 (2015).

[2] A. D’Amico, D. Tesone, K. Whitley *et al.*, “Understanding the Cyber Defender: A Cognitive Task Analysis of Information Assurance Analysts,” Report CSA-CTA-1-1 under Contract No. F30602-03-C-0260 issued by USAF, AFMC Air Force Research Laboratory, (2005).

[3] S. Caltagirone, A. Pendergast, and C. Betz, [The Diamond Model of Intrusion Analysis] Center for Cyber Intellifence Analysis and Threat Research, Hanover, MD(2013).

[4] M. Tyworth, N. A. Giacobe, V. F. Mancuso *et al.*, “A human-in-the-loop approach to understanding situation awareness in cyber defence analysis,” EAI Endorsed Transactions on Security and Safety, 13(1-6), (2013).

[5] N. A. Giacobe, "A Picture is Worth a Thousand Alerts." 57, 172-176.

[6] V. F. Mancuso, G. Funke, A. Strang *et al.*, "Capturing Performance in Cyber Human Supervisory Control." 59.

[7] V. F. Mancuso, and M. D. McNeese, "Effects of Integrated and Differentiated Team Knowledge Structures on Distributed Team Cognition." 56, 388-392.

[8] S. Jariwala, M. Champion, P. Rajivan *et al.*, "Influence of Team Communication and Coordination on the Performance of Teams at the iCTF Competition." 56, 458-462.

[9] P. Rajivan, M. Champion, N. J. Cooke *et al.*, [Effects of teamwork versus group work on signal detection in cyber defense teams] Springer, Las Vegas, NV(2013).

[10] M. Champion, P. Rajivan, N. J. Cooke *et al.*, "Team-based cyber defense analysis." 218-221.

[11] C. Gutwin, S. Greenberg, R. Blum *et al.*, “Supporting Informal Collaboration in Shared-Workspace Groupware,” J. UCS, 14(9), 1411-1434 (2008).

[12] M. Schreiber, and T. Engelmann, “Knowledge and information awareness for initiating transactive memory system processes of computer-supported collaborating ad hoc groups,” Computers in Human Behavior, 26(6), 1701-1709 (2010).

[13] ISO 13407, [Human-centred design processes for interactive systems] ISO, Geneva(2010).

[14] J. J. McGinn, and N. Kotamraju, "Data-driven persona development." 1521-1524.

[15] D. Ogle, and A. Bloodworth, [Persona Scales], https://wiki.fluidproject.org/display/fluid/Persona+Scales(2014).

[16] G. Ahuja, “Collaboration networks, structural holes, and innovation: A longitudinal study,” Administrative science quarterly, 45(3), 425-455 (2000).

[17] P. C. Tripathi, and P. Reddy, [Principles of management] Tata McGraw Hill Education Private Limited, New Delhi(2012).

[18] P. Pirolli, and S. Card, "The sensemaking process and leverage points for analyst technology as identified through cognitive task analysis." 5, 2-4.

[19] N. J. Cooke, E. Salas, P. A. Kiekel *et al.*, [Advances in measuring team cognition] American Psychological Association, Washington, DC USA(2004).