Human-Centered Study of a Network Operations Center: Experience Report and Lessons Learned

Celeste Lyn Paul
Department of Defense
clpaul@tycho.ncsc.mil

ABSTRACT
Network operations centers are notoriously difficult places to conduct human-centered research. The intense pace and sensitive information environment creates a number of hurdles for researchers. This paper shares the experiences from human-centered research of a government network operations center. The lessons learned from conducting interviews, field observations, and a card sorting study offer guidance to those who may study network operations centers in the future.

Categories and Subject Descriptors
C.2.3 [**Computer-Communication Networks**]: Network Operations – *network management, network monitoring*.

General Terms
Human Factors, Management, Security.

Keywords
Card sorting; ethnography; field observations; interviews; network operations center; security information workers.

1. INTRODUCTION
There is a growing need for human-centered research of security information workers, especially those in computer network defense [1, 2, 3, 5]. Network defense analysts work in a dynamic, always changing, complex environment, with intense time pressures and a need-to-act [3, 5]. Ethnographic methods, such a field observation and interviews [1, 2, 4, 5, 7], have been favored as a way to understand this rich, complex environment.

However, the study of network defense analysts poses a number of challenges. Simply finding and recruiting security information workers can be a challenge [1, 7]. Even once they are recruited, they are always very busy, overworked, and have limited time that they can dedicate away from their responsibilities to participate in research [1]. Perhaps one of the most limiting challenges is the sensitivity of the information environment of a large network and the hesitation of sharing that information with outsiders [1, 4, 7].

These challenges extend to the study of network operations centers. Network operations centers (NOCs) are the nerve center of any large network's defense. Networks utilize operations centers as the command site for coordinating network security. These are highly collaborative, high-stakes environments where network defense analysts must work together to observe, identify, characterize, and defend against computer security threats. While there is a history of research on other types of operations centers, there is very little human-centered research of NOCs ([2] is one of the few known examples). With the growing acknowledgement that computer security is as much of a human challenge as a technology challenge, there is a clear need for more human-centered research in this area.

The goal of this research was to develop an understanding of a government NOC as a basis for future network situation awareness research. Although I had a good background in computer network defense, I had little experience in an operational environment. In order to obtain a holistic understanding of the NOC environment, I studied its people, work processes, and technology *in situ*.

However as previously discussed, human-centered research of security information workers has a number of challenges. In this experience report, I describe the considerations made when designing my research plan and the lessons learned while conducting the research at the NOC. Given the known challenges of studying NOCs, I needed methods that were exploratory with the ability to target specific research questions when identified. I also needed methods that supported both breadth and depth of investigation. Finally, I needed non-invasive techniques that would not disrupt operations. In this experience report, I describe a case study of research conducted at a government NOC. Lessons learned from this experience offer guidance to those who may study NOCs in future research.

2. CASE STUDY
The target environment was an operations center responsible for the security and defense of a large government network. The NOC was a 24/7 operation with two shifts (day and night) of network defense analysts and managers. Floor analysts are responsible for identifying, analyzing, and reporting events that occurred on the network. Shift managers are responsible for general situation awareness of the network, management of analyst resources, and operational decision-making about event escalation and defensive measures. As with most computer security environments, the NOC is a very busy, high-stress environment.

The NOC is considered a sensitive information environment and access is restricted to those who worked on the operations floor. In order to gain access to the NOC for research, someone from the NOC or supporting organization needed to sponsor me to visit. Visits are normally limited to control interruptions and distractions in a very busy environment.

When considering methods and techniques for use in this research, I opted for an ethnographic approach that utilized multiple field-based methods. Ethnography is the qualitative study of people and their culture. It is often used in information technology environments for studying and understanding a user's

SIW'14, November 07 2014, Scottsdale, AZ, USA
ACM 978-1-4503-3152-4/14/11…$15.00
http://dx.doi.org/10.1145/2663887.2663899

work environment, their work processes and tools, and their interactions and collaborations with other users.

Because of the challenging research environment, I needed methods that were flexible with minimum impact on the environment. Interviews, field observations, and card sorting were conducted over the period of 12 months. This approach is similar to the one used by Brown et al. in their NOC study [2].

2.1 Interviews

Initial interviews were conducted to develop an understanding of the NOC environment before visiting. It was important to gain basic knowledge before visiting the NOC to minimize the researcher impact on the environment. Basic information about the NOC environment are facts that someone with experience with the NOC could provide outside the environment (e.g., "What is the NOC responsible for?", "What tools do NOC analysts use?", and "How is the NOC organized?"). Even though these topics are often good ice breakers when meeting a subject for the first time, it was necessary to minimize the impact of research activities in a high-stakes operational environment. Asking analysts to describe basic mission function was not an effective use of their time at the cost of interrupting their work, especially if that information could be learned outside of the NOC.

Seven interviews were conducted with people (all male) who had experience working with or in the NOC. Interviews were open-ended with no structured topics except to probe about their individual experiences with or in the NOC. Interviews lasted between 45 minutes to 1.5 hours.

The first four interviews were conducted with *surrogate users*. I use the term *surrogate users* to describe people who are similar to the target user population through shared knowledge or experiences. They may have at some point been the target users, worked closely with the target users, or have the same knowledge or training as the target users. Surrogate users are utilized when target users are unavailable or inaccessible, as is often the case with very busy network defense analysts. It is important to note that surrogate users are not the target user and are at risk of projecting their own biases on their ideas of what the target user might do or think. However, surrogate users offer an alternative to few or no interviews with a subject matter expert as long as the researcher considers the possible bias in the data.

The first two interviews were with researchers in a research organization associated with the NOC's parent agency. These researchers had spent one year or longer working with the NOC and supporting organization. While the researchers' knowledge and experiences were limited to the problems they had worked on, they were able to provide general information about the NOC mission and operations, and their opinions on what they thought are the NOC's research problems.

The third and fourth interviews were with people who worked in an organization that supported the NOC. They frequently worked with NOC analysts and managers. The purpose of their organization was to provide technology and analytic support to the NOC. They were able to provide an organizational perspective of the NOC's mission and its current challenges.

The last three interviews were with people who actually worked in the NOC. These people were NOC shift managers who are in charge or all operational tasking and decision-making during their shifts. These interviews overlapped with the beginning of the field observation period. They were able to provide a unique operational perspective that never emerged in the previous interviews. This perspective may have never emerged if most of the interview time was spent covering basic information about the NOC rather than deeper-level topics.

One of these last interviews was with who would become my "research advocate". His role as a NOC shift manager enabled him to provide me access to the NOC as needed. His role as a shift manager also gave him a unique perspective on the NOC that I was not able to gain from the other interviews. His interest in my research led him to advocate for my work to other NOC teams that helped me establish new research contacts.

The progressive nature of these interviews allowed me to build up an understanding of the purpose of the NOC and how it operates before I entered the environment. Combined, the information gained from the interviews also provided the necessary background knowledge to be able to identify events in the environment and understand what I was observing.

2.2 Observations

Approximately 30 hours of initial observations in the NOC were conducted over the course of 12 months. Observations occurred once a month at two to four hour periods. This time does not include the three interviews conducted at the NOC or the time for conducting the card sorting study.

While 30 hours is not a long time for observing an environment, the nature of NOCs makes long term and continued access a challenge. Due to the complexity and nature of the NOC, I opted for fewer observations over a longer period of time, rather than observing all at once in a short period of time. Although deep integration into the environment (such as "working" at the NOC full-time for a week) can provide valuable insight to how it operates, it can also be overwhelming. In-frequent, but regular visits were more productive for developing relationships with analysts and managers in the NOC for continued access. Additionally, a smaller view over time gives extra time to analyze field notes in between visits and conduct background research on new or unfamiliar concepts.

The NOC rotates teams of analysts and managers for 24/7 coverage. I observed the work of four different teams but spent most of my time with my research advocate's team. Observations occurred mostly during the night shift. Day shift is very busy with visitors and extra meetings and the impact of a researcher was greater than during the night shift. The night shift is quieter and sometimes offered an opportunity to interact with analysts with less impact on operations than the busy day shift.

Observed NOC activities included:

- Day-to-day operations, including the collaboration and communication between analysts and managers.
- Scheduled meetings, situation briefings, and technical demonstrations.
- Training exercises of simulated cyber events.

A typical observation session was based on the following format. First, I would arrive to the NOC and greet the shift manager, usually one or two hours into the shift. The shift handoff period is a very busy period for shift managers who are concerned with knowledge transfer between teams and event briefings. I was

asked by shift managers to come later in the shift after the handoff, but was invited to observe shift handoff several times to understand knowledge transfer between teams.

Next, I would ask the shift manager if there were any events happening on the network. This was important to know as the observer in order to gauge how much I could or should interact with the analysts and managers. If there was a major network event happening, analysts would be very busy and should not be disturbed. If it was a relatively quite night, then I could use it as an opportunity to interact more with analysts.

I would also ask if anything was different or new since the last time I visited. This was useful because my visits were infrequent, but over a long period of time. There were a number of analysis tools or management dashboards that were introduced, updated, or phased out during the course of the study. Knowing why certain tools succeeded or failed provided insight to the challenges the NOC faced and what successful solutions might look like.

Occasionally there were scheduled events, such as meetings, presentations, or technology demonstrations that I would attend. On two occasions, there were training exercises that simulated cyber events. The NOC practiced coordination amongst the analysts and managers, as well as coordinating with outside entities. These training exercises are meant to test new policies and procedures, as well as offer practice for uncommon events.

Finally, I would settle in to the observation period. This was a time where I quietly observed the communication and coordination between analysts and managers. On slower nights, the floor was quiet, with occasional pockets of analysts chatting in between tasks. On busier nights, the floor was buzzing with activity as analysts got in and out of their chairs to share information with other analysts and report to the shift manager.

Overall, there was moderate interaction with ops center managers and limited interaction with NOC analysts and managers. However, as the analysts and managers got to know me, they often volunteered information without being prompted. This was beneficial to me, because it provided important context if it was convenient. If they were in an important conversation, they would not be as inclined to self-interrupt.

To supplement my understanding of the NOC, I visited three other smaller government NOCs and one commercial NOC. These visits were not field observations but guided tours with the ability to ask limited questions about the NOC's organization, mission, and operations. This provided an opportunity to compare and contrast my experiences with the primary NOC with those in other NOCs. Visits lasted from one to two hours each.

These observations gave me valuable insight to NOC operations, its strengths and weaknesses, and potential areas for future research. One particular insight that the observations were able to provide was a sense of "battle rhythm" during a shift—not observable through interviews and card sorting.

2.3 Card Sorting

Near the end of the initial NOC observation period a card sorting exercise was conducted with analysts and managers. Card sorting is a knowledge elicitation method that helps people describe relationships between and hierarchy among concepts [9]. The purpose of the card sorting study was to explore mental models of cyber situation awareness in the NOC.

An open-style card sorting study was conducted with 12 NOC analysts and managers (all male) using 44 cyber situation awareness questions. Each question was written on an index card. Participants were asked to sort the questions into logical piles, using whatever method they felt was most appropriate. After the cards were sorted, participants wrote a topic title on blank index cards to label each pile. When a participant was finished sorting the cards and labeling the piles, he described each pile and explained why it was created.

The cyber situation awareness questions were derived from the interviews and observation data. These were questions analysts and managers used to describe the analytic challenges of the NOC environment. For example, a NOC analyst might ask himself "Does this attack matter?" when determining the severity and priority for analyzing an event.

Analysts and managers enjoyed participating in this activity. After weeks of being observed, they finally felt that they were part of the research. Several participants mentioned that they thought that the card sort was challenging in a positive, intellectual way—forcing them to think abstractly about a subject area that they were intimately familiar with.

What is most interesting about the cart sorting study results were the differences between explicit (participant-generated) topics and the implicit (analysis-derived) topic. The explicit topics generated by each participant seemed to be influenced by their specific job role in the NOC. However, there was high agreement between certain question pairs of analysis-derived implicit topics across participants, suggesting a cohesive mental model across the NOC.

The results of the card sorting study provided supporting evidence to related work on cyber analytic work processes as well as valuable insight as to what analysts and managers feel are the most important situation awareness questions. A more detailed report of this study, including the list of cyber situation awareness questions and resulting taxonomy, is described in [11].

3. DISCUSSION

Conducting human-centered research in network operations centers remains a challenge. The intensity of analysts' work, sensitivity of the information environment, and access to the environment and its people create barriers to conducting human-centered research in a NOC. The following provides a summary of major findings from this research, how the results of this research have been used to date, and lessons learned that could support the design of future research in this area.

3.1 Major Findings

The NOC is a **highly collaborative work environment**. While each analyst has his own responsibilities, work in the NOC is a team effort. Analysts interact with other NOC analysts and people outside the NOC on a regular basis. The preferred method for sharing information was through verbal and physically co-located interactions. It was common for an analyst to walk over to another analyst's desk to share information, for several analysts and a shift manager to discuss an event while looking at the same screen, or for an analyst to call out to the entire NOC floor when sharing urgent, high-priority information. This style of collaboration was very efficient, but also produced few artifacts that could be shared with the next shift. Virtual means for sharing and communicating existed, but were used for low priority requests and FYIs.

The preference for verbal and physical communication and lack of virtual artifacts posed **challenges for knowledge transfer** between shifts. Ticket systems and event reporting maintained a record of the work, but there was no method for recording the tacit knowledge gained during the shift. The most effective means of documenting this tacit knowledge was through a "captain's log" maintained by the shift manager. However, the ability to record these notes was dependent on the availability of the shift managers and how busy the shift is.

The most challenging aspect of the NOC shift manager's job was maintaining a **"mission-level" situation awareness** of the health and status of the network. Managers are aware of the events analysts were working on and how those events affect the network. However, it is challenging for shift managers to put together how all of these individual actions fit together in a higher-level story of how the network is operating. This mission-level situation awareness is critical for an ongoing narrative of the health and status of the network. This narrative is used to frame reports to higher-level management and for effective knowledge transfer between shifts. While the NOC is effective at its mission, this is where shift managers felt the greatest improvements could be made through the use of new tools or artifacts.

3.2 Application of Results

To date, I have utilized the results of this research in several ways. The general knowledge gained from field observations was used to create a realistic narrative for a design-focused visualization challenge [12]. An in-depth analysis of the card sorting study led to a taxonomy of cyber situation awareness questions that can be utilized in user-centered design of NOC technology [11]. The identification of the NOC's "mission-level" situation awareness challenge inspired a visualization prototype to help manage human activities during a network event [10]. Finally, the lessons learned from this research have influenced the methodology of follow-on work with other security information workers [6].

3.3 Lessons Learned

Longtitudinal study. Develop a research plan that is executed over a long period of time. One visit is not enough and a few hours is not enough. Rather than embedding yourself into the NOC, conduct regular, but in-frequent visits. This will minimize your impact on operations, but also provide a long-term view of how the NOC works. Visit often enough to maintain relationships and keep up on changes in the environment, but not so frequent that you become a distraction to the NOC.

Mix methods. Choose to conduct several studies with methodologies that have a low impact on the environment. One large invasive study might yield more data faster, but is also more intrusive, less likely to be welcome in a busy NOC, and is more likely to be postponed or cancelled. Several smaller studies can be done over time and adjusted as the research project and results evolve. Diversity in techniques is good methodology and supports triangulation of results.

Make friends. Develop and maintain a friendly professional relationship with the people you are studying. While getting too friendly can be a conflict of interest, not making and maintaining relationships will have a greater effect on your research. Finding a research advocate is especially important for access to and information about the NOC. These relationships are critical to the ever changing environment, especially when the NOC rotates teams in an out or off the schedule. You do not want to set up a productive research arrangement only to lose your contact when he or she rotates out of the NOC.

4. REFERENCES

[1] Botta, D., Werlinger, R., Gagné, A., Beznosov, K., Iverson, L., Fels, S. and Fisher, B. Towards Understanding IT Security Professionals and Their Tools. Proceedings of ACM SOUPS 2007, 100-111.

[2] Brown, J.M., Greenspan, S. and Biddle, R. Complex activities in an Operations Center: A Case Study and Model for Engineering Interaction. Proceedings of ACM EICS 2013, 265-274.

[3] Cummings, M.L., Bruni, S., Mitchell, P.J. Human Supervisory Control Challenges in Network-Centric Operations. *Reviews of Human Factors and Ergonomics*, 6(1), May 2010, 34-78.

[4] D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., Roth, E. Achieving Cyber Defense Situational Awareness: A Cognitive Task Analysis of Information Assurance Analysts. Proceedings of HFES 2005, 229-233.

[5] Gagné, A., Muldner, K., Beznosov, K. Identifying Difference between Security and other IT Professionals: a Qualitative Analysis. Proceedings of HAISA 2008, 69-80.

[6] Gersh, J.R. and Bos, N. Cognitive and organizational challenges of Big Data in Cyber Defense. Proceedings of HCBDR 2014, 4-8.

[7] Goodall, J.R., Lutters, W.G., and Komlodi, A. I Know My Network: Collaboration and Expertise in Intrusion Detection. Proceedings of ACM CHI 2005, 342-345.

[8] Horn, C. and D'Amico, A. Visual Analysis of Goal-Directed Network Defense Decisions. Proceedings of VizSec 2011.

[9] Hudson, W. Card Sorting. In, Soegaard, M. and Dam, R. (eds.) *The Encyclopedia of Human-Computer Interaction*, 2nd ed. Aarhus, Denmark: The Interaction Design Foundation, 2013.

[10] Paul, C.L., Rohrer, R., Sponaugle, P., Huston, J. and Nebesh, B. CyberSAVI: A Cyber Situation Awareness Visual Interface for Mission-Level Situation Network Situation Awareness. Proceedings of VizSec 2013, Poster.

[11] Paul, C. and Whitley, K. A Taxonomy of Cyber Awareness Question for the User-Centered Design of Cyber Situation Awareness. Proceedings of HCII 2013, HAS, 145-154.

[12] Whiting, M., Cook, K., Paul, C.L., Whitley, K., Grinstein, G., Nebesh, B., Liggett, K., Cooper, M. and Fallon, J. VAST Challenge 2013: Situation Awareness and Prospective Analysis. Proceedings of IEEE VAST 2013.