An Anthropological Approach to Studying CSIRTs

Sathya Chandran Sundaramurthy, John McHugh, Xinming Ou
S. Raj Rajagopalan, and Michael Wesch

In an apocryphal tale, it is widely believed that the big green button which is now ubiquitous on Xerox machines was invented by an anthropologist. In 1979, Xerox Parc asked anthropologist Lucy Suchman to study user interactions with a printer that had just been put on the market and widely disparaged by users as too complicated. With cameras in place to carefully track the movements and interactions of the machine's users, Suchman's footage would become most famous for the meme-like image which John Seely Brown used in a keynote address labeled "When User Hits Machine." As the story goes, Xerox watched Suchman's video and from her conclusions developed a new user interface – the big green button. As with many such tales, there is a grain of truth to the story, but it isn't entirely true. The true story, which we will return to in the conclusion reveals a great deal more about our relationship to the tools we use, and how they "use us." All of these, as we will explain in this article, has much to do with studying Computer Security Incident Response Teams, or CSIRTs.

1 Anthropology Today

Normally we imagine cultural anthropologists to be working at the far edges of the earth, working with exotic indigenous peoples still isolated from the rampant and rapid transformations of technology. But over the past several decades, more and more cultural anthropologists have been bringing their research methods to explore more familiar territory, often with surprisingly practical and productive results.

In the late 1990s, for example, Charles Leinbach and Ron Sears brought the methods of anthropology to the design of Recreation Vehicle (RV) campers. Their method was, of course, to become RV campers themselves, spending six months on the road with a giant RV and living in RV campsites. They learned that much of the design of the RV was completely inadequate for the actual needs and desires of everyday life within the RV culture. They found, for example, that most RV campers never use the shower on board (they prefer the high-pressure showers offered at the campgrounds that do not waste their limited water supply), and instead use the shower as an extra closet. Office-bound designers had designed what they imagined RV'ers would need – but had never actually lived with them to find out more about their culture. When Leinbach and Sears finished their study they had hundreds of ideas and built a prototype that was so successful that the company had to cancel the manufacture of all their other models to meet the demand of this new prototype. The prototype has now become one of the most copied in the history of the industry [11].

And there are many other success stories. Genevieve Bell, a cultural anthropologist at Intel explored the social and cultural aspects of ubiquitous computing with Paul Dourish [6]. Their work has significantly shaped the ubiquitous computing research methodologies. And Go-Gurt,

the handheld yogurt that children can enjoy like a popsicle while appeasing moms' interest in nutrition, was based on an anthropological study by Susan Squires [15].

What feeds the success of these endeavors is the anthropologist's hallmark approach, *participant observation.* Rather than standing back as mere observers, they feel and experience the world from the participant's perspective.

2 Bringing Anthropology to Studying CSIRTs

In contrast to the success stories mentioned above, the traditional approach taken by the cybersecurity research community for innovation is to read the current literature on a problem, identify areas for improvement, and then develop tools and methodologies that address those problems. While this process may result in "theoretically sound solutions," there has always been an issue of how usable these solutions are in the real world. The main reason for this problem, we believe, is the discrepancy between what the security practitioners actually need and what the researchers perceive as what they need. As a result, research results hardly find their way into practical use.

2.1 Why Anthropology?

For studying Computer Security Incident Response Teams (CSIRTs), adopting an anthropological approach is especially important, since the Security Operations Center (SOC)'s work and culture is very hard to understand from the outside. From multiple of the authors' past experience in designing cybersecurity technologies for SOC analysts, interviewing with the analysts can only scratch the surface of how they actually do their job. And with this limited understanding, it is extremely challenging to design algorithms and build tools to help the analysts' job. When research does lead to promising prototypes, the progress is invariantly stifled by "lack of cooperation" from the analysts in deploying the research prototypes in their work environment, since this is always something the analysts have to do "in extra" and they do not have the time. Research prototypes are rarely designed to be able to fit into the analysts' workflow; more often researchers ambitioned to provide an all-encompassing solution that can "automate" the analysts' job, only to find the tool to fall completely flat in the operational environment. There is no reason to expect that analysts would be willing to help the researchers to "fix" the tool and identify the problems, since most likely this would mean that they will have to stop what they are doing and help the researchers to improve a tool that has no real concrete prospect of being useful at all.

While researchers often times believe they have better ideas on how to address a practical problem, the truth is that jobs such as incident response and forensics analysis commonly found in SOCs have become so sophisticated and expertise-driven that it is nearly impossible to understand the processes and needs without doing the job by one's self. Nevertheless, few researchers are doing the "fieldwork" to understand the problem first hand, before attempting to design models and algorithms to help solve the problem.

From the research community's perspective, SOCs are often perceived as shrouded in secrecy. Researchers find it hard to get data for research, or get research prototypes deployed and "evaluated." SOC analysts are guarded when approached by researchers, who are perceived to be only interested in publications, not solving the real problems. Indeed, most academic research gets little credibility with and has little impact on the practitioners community. Studies conducted by researchers tend to be plagued by lack of scientific rigor and is largely divorced from reality. One

significant result of this state of affairs is a lack of effective technology transfer from the academic research to security practitioners.

The dynamics of the research, however, will change completely if researchers set their foot on the ground, by joining the analysts' community. This way the researchers can learn the job themselves, and also reflect on what is going on to identify the real gaps that need research to bridge. He/she can then design algorithms and tools that will be directly embedded in the day-to-day operations, and readily accepted by the SOC community — for one thing, the researcher is now part of it.

When anthropological methods are worked into a design process, you get what Paul Czyzewski, Jeff Johnson, and Eric Roberts have called "participatory design." In the following we illustrate three key characteristics of this approach, as outlined by Czyzewski, Johnson, and Roberts [5]: 1. Our research "turns the traditional designer-user relationship on its head, viewing the users as the experts – the ones with the most knowledge about what they do and what they need." 2. We view the tools we develop "not in isolation, but rather in the context of a workplace; as processes rather than products." and 3. Our work "rejects the assumption that the goal of computerization is to automate the skills of human workers, instead seeing it as an attempt to give workers better tools for doing their jobs."

2.2 The Real Experts (and Their Frustrations)

SOC analysts handle various types of cyber events that may be related to hacker breaches or other types of cyber attacks. They make use of numerous tools and follow a predefined set of procedures to handle a variety of incidents everyday. The authors have been talking with SOC analysts of various organizations and they all are quite unhappy with the current solutions for forensics and incident response. Commercial solutions like Security Information and Event Management (SIEM) systems often do not address the needs of the operational environment. The main reason seems to be that the vendors or the research community has not adequately understood how analysts do their jobs.

SOC analysts often need to perform sophisticated investigations and it is not uncommon that the exact process of connecting the dots to resolve an incident is not even clear to the people doing the job itself. Moreover, incident response is not just a technical problem; it involves people with a wide variety of skill sets interacting with each other and a predefined process being followed for each type of incidents. Current solutions do not understand these workflows and hence remain only partially helpful.

Another problem facing SOCs is that the analysts working in these organizations must obtain necessary trainings to conduct the job, the nature of which is highly dynamic and requires one to be able to deal with a variety of threats that are constantly evolving. How to do the job is more an art than a science these days. New analysts are trained on a rather *ad-hoc* basis. Many times the training is not structured but done on the job. Rookies are intentionally left to stand out in complicated tasks by themselves, even though the more experienced analysts could have provided the simple hint for the one suffering. The common wisdom in the profession is that one must learn the trade through the pain and it is regarded as a necessary "initiation" process for new analysts. Nevertheless, the lack of systematic training for new SOC analysts have become a critical bottleneck for SOCs to perform their jobs effectively.

2.3 The Root Cause

All these challenges of working in SOCs can be rooted at the difficulty of effective knowledge transfers: between analysts and from analysts to tool builders. It turns out that this phenomenon has long been studied in social sciences, especially anthropology. The term "tacit knowledge" [14] was coined by the philosopher of science Michael Polanyi[1]. In simple words, tacit knowledge means such knowledge that cannot easily be put into words. As an example, how to perform the various tasks in a CSIRT job could be very sophisticated; but there is no manual or textbook to explain this. Indeed even if one asks a very experienced analyst, he/she may find it hard to explain exactly how dots are connected in the investigations. From this perspective, the fact that new analysts get little help in training is not surprising, because the profession is so nascent that the how-to's have not been fully realized by even the people who have the knowledge.

Cultural and social anthropology could be described as the study of tacit knowledge [7]. Anthropologists do intensive long-term fieldwork in an attempt to reveal and make explicit the "native point of view," which is not just "what natives say" (explicit knowledge) but more importantly, the underlying concepts, presuppositions, and know-how that make up tacit knowledge. While the native point of view is never fully attainable [9], the foundational anthropological method of "participant observation" allows anthropologists to explore the subjects' perspectives and practices by actually taking part in their daily lives and activities (participation) while also standing back from them to gain new perspectives (observation) [1].

Over the past several decades, anthropologists have become increasingly aware that knowledge and expertise are not just to be found "inside people's heads." In a widely-cited study of tailors and their apprentices in Liberia, Jean Lave and Etienne Wenger developed the notion of "communities of practice," suggesting that contrary to common-sense perceptions of knowledge and learning, they are (1) not always explicit, (2) often embedded in or even "embodied" in practice, and (3) that there is often a social dimension to knowledge and learning, so that the knowledge may not necessarily even be said to be "in an individual," but is instead embedded and embodied in the community of practice [10]. The logical conclusion from these insights is that **if you want to gain access to these tacit forms of knowledge, you must become embedded in the community of practice yourself.**

3 Ethnographic Fieldwork at a University SOC

— Understanding Tools as Processes not Products

To gain access to the knowledge and expertise permeating a CSIRT, Sathya Chandran Sundaramurthy (lead author) has been conducting an enthnographic fieldwork at a higher-education institution SOC for the past year. By becoming part of the operation team, Sundaramurthy per-

[1]It is worth noting that Polanyi's formulation of tacit knowledge was partly spurred by a discussion in a 1949 symposium organized by the Department of Philosophy at the University of Manchester, on "Mind and Machine." Both Michael Polanyi and Alan Turing were among the attendants of the Symposium and they had some very interesting debate [2] on whether a machine can "think" like a human. A precursor to the notion of "tacit knowledge" was used by Polanyi to reject Turing's idea that it is possible to build a machine that can think like a human, which later led to Turing's seminal paper that set the stage for artificial intelligence [17]. Polanyi did not reject the idea of formalizing human knowledge for the purpose of automation, but he deeply believed that there is a fundamental difference between the way a human brain and a machine works. It is interesting to observe under this historical backdrop how the debate between two great minds helped shape the ideas presented in this article.

forms many of the same tasks as the analysts, and experiences the same pains, frustrations, as well as the occasional triumphs.

3.1 The Beginning of the Saga: Losing One's Perspective

More than anything, Sundaramurthy was immediately introduced to the tedium of the job's more frustratingly time-consuming and repetitive low-level tasks. The SOC receives alerts on malicious network traffic from a number of trusted sources as well as from their own intrusion detection system (IDS). The alerts contain the IP address of the infected host and the remote IP address it was communicating to. The IP address most of the times is of the border firewall since the internal hosts are NATed. Hence the internal IP address has to be extracted from the firewall logs. From the internal IP address the corresponding MAC address is obtained from ARP logs. The network generates approximately 70 GB of firewall log data on an average business day. Finding the connection log entry for a given timestamp, firewall IP address and port number sometimes took up to three minutes and the ARP lookup took another minute. Then looking up user information for that MAC address took another minute. So the whole process may take up to five minutes. And this repeats. Before long, Sundaramurthy was fully absorbed. He wasn't creating tools. He was a tool.

It is surprising to the researchers that such a simple event correlation problem does not find an easy solution in any of the off-the-shelf SIEM products we are aware of. Later on we also knew through both literatures and anecdotal stories that this type of problem does not exist only at the SOC we are studying, but in other SOCs (both commercial and educational) as well.

The typical thought process in the SOC is to get incidents processed quickly rather than thinking about the long-term vision on how to improve the efficiency, and the fieldworker was also consumed by this style of work. It wasn't until Sundaramurthy discussed his work with some external team members of this research that he realized a better way to do this.

3.2 The Breakthrough: Gaining the Trust

The fieldworker decided to speed up the lookup by building a database of connections along with IP address to MAC address mapping with timestamp. The challenge however was that one cannot keep adding data to this database as it would exhaust the available storage very quickly. But from the fieldworker's experience most of the alerts are no more than a week old. So he decided to build a caching database and keeps the mapping information for the latest seven days at any given time.

The fieldworker first built the database using MySQL but then the tool was falling behind on log collection from the firewall. The reason was that he was indexing on a few attributes for faster lookup and since the inserts are in real time the indexes have to be adjusted for each insert and also have to be committed to the disk. After reading a bit on database optimization he decided to adopt NoSQL solutions that are efficient in handling applications that have high real-time write throughput, such as log collection. He finally settled on MongoDB which stores data as JSON type (schema-less) objects.

Once the fieldworker built this database and found it to be stable, he asked the SOC analyst he was embedded with to use it. First of all, the analyst was extremely happy to see the speedup in incident response the tool has brought him: from five minutes down to two seconds. More importantly, and much to the fieldworker's pleasant surprise, the analyst started to talk much more to him. He became much more interested in talking to the fieldworker on how the tool

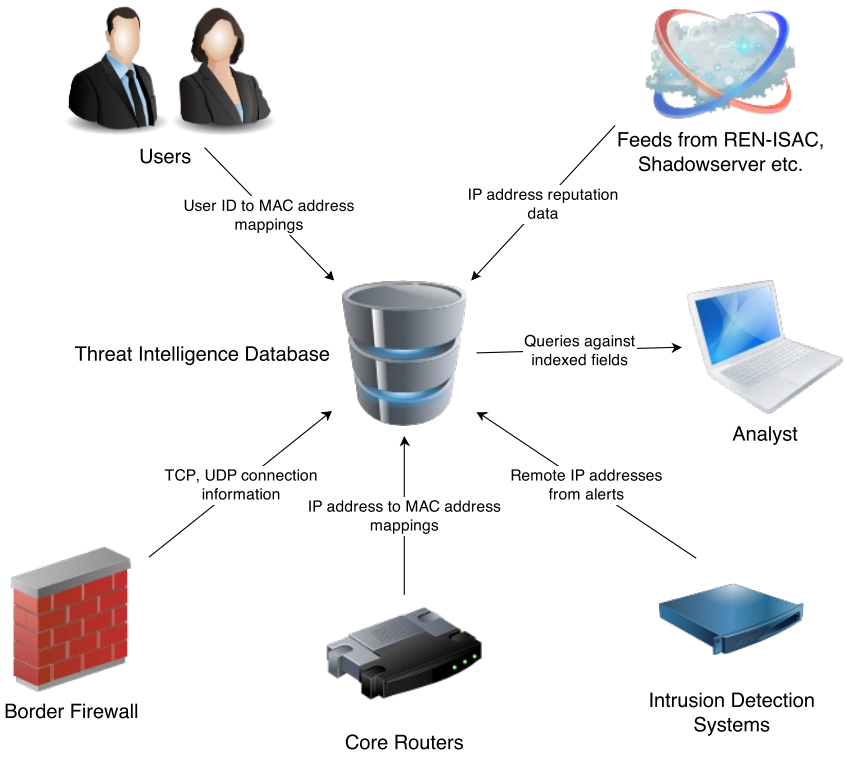


Figure 1: Threat Intelligence Framework

can be extended to do more things, and was willing to share more data to expand the database infrastructure. The two did a long brainstorming session on the whiteboard and arrived at a "Threat Intelligent Framework" based on the caching database.

This was what the fieldworker had wanted to do on day one but was not able to pull off until this moment. For all this time he had been frustrated by being completely consumed by the mundane and repetitive tasks and not feeling making any progress towards his real objective, which is to design better tools for SOC analysts. But once the analyst saw this first very simple tool he had built, he completely changed his attitude. The fieldworker found his first "informant," like an anthropologist working in a remote tribal area would be delighted about. The key to having this moment is to have the subject's trust, which in this case was done (nicely) by providing something useful for the analyst. This is not unlike what the anthropologist Clifford Geertz described in his famous article "Deep Play" [8] about how he gained acceptance among the "natives." This first success is a great example of how being "in the field" can actually allow one to see an opportunity to increase efficiency and to find the resources to actually accomplish the task. Now that he had this trust and acceptance, the fieldworker might also be able to see the world and the tasks more and more through the analyst's eyes and thereby be able to create even more sophisticated tools. In other words, we opened the door to truly access the "tacit knowledge" and make it more explicit.

3.3 To Be Betwixt and Between

This example also illustrates a paradox of fieldwork. On the one hand, *the farther you are from the community you want to study the more daring you are to try new ideas*, but without being part of the community, your ideas may lack relevance or otherwise not be able to be implemented. Fieldworkers have to step into the shoes of the members of the community they are studying but also remind themselves often that they are just observers not one among them.

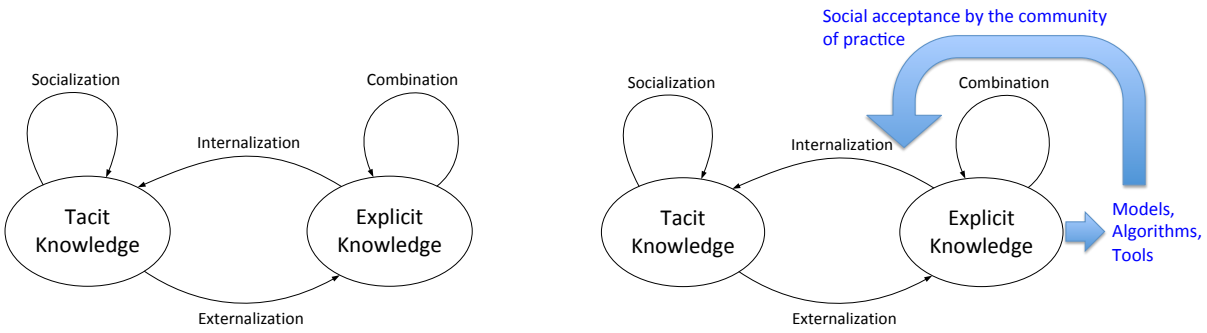
Anthropologists recognize that by becoming part of the research subjects, there will be inevitable subjectivity in the research finding. Thus it is important that researchers practice reflexivity — being able to step out of the shoes of the subjects to reflex upon and question what one does and how things are perceived. In other words, anthropologists exist "betwixt-and-between" the world of the researcher and subject. For the rich tacit knowledge existing in environments like CSIRTs, this approach is necessary since the subjects themselves cannot identify and articulate the critical relevant information. Observation *and participation* in the target environment by researchers are critical to understanding the problem.

It is also worth noting that the "tacit knowledge" includes not only the technical know-hows, but also organizational structure and processes and how they help or hinder the job. Such observations may not even be clear in the subjects' mind and can only be teased out if researchers get embedded with the subjects.

3.4 Bringing the Two Cultures Together Through Tool Co-Creation

3.4.1 The Chasm between Two Cultures

For the subject of cybersecurity, academic researchers tend to work in a world set apart from that of practitioners. They work under very different conditions, attend different conferences, and have developed a mutual feeling of distance from one another. Furthermore, academics are accustomed to creating, contesting, and sharing their knowledge and expertise, while practitioners have long worked on their own and created their own expertise without sharing any detailed expositions of



(a) SECI Diagram

(b) Tool-oriented SECI

Figure 2: Ethnography-guided Cybersecurity Research

that knowledge. This is because (i) the culture of cybersecurity practice is a closed one in that one is not encouraged to talk about attacks and how they were found, (ii) there is a mismatch between the kind of knowledge possessed by practitioners and the typical content of research papers, (in other words a practitioner would probably never get a paper published in academic conferences), and (iii) where practitioners do present (DefCon, Black Hat, *etc.*) the focus is more on the "wow" factor or "coolness" and less on scientific merit, relevance, and validity. These factors have led to a large chasm between the two communities because of which very little knowledge transfers between them.

Simply fostering conversations between the two camps does not automatically bring about knowledge transfers, due to the nature of the knowledge held by the practitioners. As Michael Polanyi famously noted [14], "We can know more than we can tell." Cybersecurity practitioners often work on what they perceive to be a "hunch" or an "intuition." They know what to do, where to look, and how to investigate a case, but they do not and perhaps cannot state this knowledge explicitly.

3.4.2 Knowledge-Conversion Model

Over the past 20 years, researchers in organizational studies have expanded upon and refined a model for how tacit knowledge can be accessed and ultimately transformed into explicit knowledge. Most prominent and relevant for our discussion is Ikujiro Nonaka's model of "knowledge conversion" (Figure 2(a)) which has come to be known by the acronym SECI, standing for the four modes of knowledge creation: Socialization (sharing tacit knowledge through apprenticeship and mentoring), Externalization (conversion from tacit to explicit through questioning, reflection, and reconstruction), Combination (accumulation of explicit knowledge), and Internalization (converting new forms of explicit knowledge into tacit knowledge) [12].

The model has been critiqued and refined over the past 18 years, so that today it is understood that tacit and explicit knowledge exist on a continuum [13], and that movement along this continuum from tacit to explicit is best achieved through reflection, ongoing practice, and above all, subjecting one's self to a diverse range of alternative experiences that can help disorient one's self just enough to see the tacit dimension — to stop taking for granted the taken-for-granted. In this regard, practice is essential. It is not enough to "join the community," for the elements of

knowledge are not necessarily shared across all members of a community; rather one must be fully engaged in the day-to-day practice [3].

3.4.3 Tool-oriented Knowledge Conversion

For studying CSIRTs, it seems that the most effective way of bringing the two cultures together is for researchers to conduct ethnographic fieldwork in SOCs for extended periods of time. This will enable the SECI knowledge conversion to reveal the deeply buried tacit knowledge in an SOC's operations. However, we would also like to argue that simply being embedded in a SOC and doing the tasks as an analyst may not be the most effective way for this knowledge conversion, since very likely the fieldworker will be relegated to a position where not much interesting observation can be made. To move from "peripheral participation" to "full participation," fieldworkers need to be fully accepted into the community. Since our research objective is to identify the performance bottleneck in a SOC and propose solutions, the most straightforward way for fieldworkers to gain full acceptance by the community is by designing tools that can help the analysts' job.

Based on this strategy, the ethnography-guided cybersecurity research method we adopt in studying CSIRTs works as follows (shown in Figure 2(b)): 1) researchers become apprentices of CSIRTs analysts (Socialization); 2) researchers reflect, question, and reconstruct what they do (Externalization); 3) researchers design models and algorithms and build tools to help the analysts' job (Combination); 4) researchers take the tool into the work and use the tool as a vehicle to open up more discussions with the analysts and identify more tacit knowledge (Internalization).

As an example of this process at work, after Sundaramurthy developed the Threat Intelligence Framework and released a tool for the analysts to use, the analyst wanted to enhance it with other features that might be helpful during some of the other incidents he handles often. Some usage of the tool was never imagined by the researcher who built the tool. As an example, among all the enhancements of the tool one of them is to help deal with stolen laptops. In such incidents the perpetrator is usually a student. If the victim knows the MAC address of his/her laptop and reports to the CSIRT, we could be lucky if the perpetrator uses the University's authenticated wireless service, since we can then associate his University ID against the MAC address of the stolen device and even catch him/her red-handed using the Access Point (AP) information. It gets interesting when the perpetrator uses the guest wireless system that does not require any authentication. Even in this case, there is an appliance used to monitor the user experience of web servers — it creates profiles of users by intercepting sessions between the user and the server. The University uses the appliance for the campus web servers, the most common among the students being the online course manager. Any student who needs to access it must authenticate to the web server and that means we can retrieve the unique University ID for that user along with the IP address and timestamp used in that access. Even if the perpetrator is using only the guest wireless network to access his/her course materials with the stolen laptop, we can still identify the suspect using the appliance's logs, together with the other information collected in the Threat Intelligence Framework. This feature also helps the analysts identify owners of compromised machines even after the Wireless Access Points flush the authentication information.

Analysts also applied the framework to phishing scam detection. Whenever a phishing email is received the CSIRT responds from a honeypot university email address. The CSIRT then watches for a login from that identifier in the future. The IP address associated with that activity is noted. This IP address is then matched against other logins made using the same address but for different identifiers within a time window. Usually it is the case that the attacker has harvested

many University accounts along with the honeypot account and is trying one by one in quick succession. The process of retrieving compromised accounts once this IP address is identified used to be a manual process. Using the framework, a watch can be placed for logins from the honeypot account and once that happens other accounts that are possibly compromised can be automatically identified. This significantly reduced the time the analysts spend in responding to phishing scams.

Users vs. Creators In this ongoing collaboration, the true "author" of the tool becomes blurred. The researcher develops a tool which is taken up by analysts and used in ways the researcher might never have imagined. This virtuous cycle produces findings and tools at the same time. This unique research methodology differs from both traditional cybersecurity research and anthropological research. Instead of building the algorithms and tools first, the researchers will base their model on concrete ethnographic fieldwork data, which will yield algorithms and tools that can actually help the analysts' job. Thus the CSIRTs community will no longer have resistance to adopting the research prototype, especially when the researchers are part of their team. Most importantly, the tool provides an opportunity for analysts to brainstorm with the researchers more practical problems that the tool could be enhanced to address, thus opening up more venues for sharing the tacit knowledge. In a few instances, we have observed that the analysts had to think hard to explain how they would like the tool to be enhanced, which is exactly the process of converting the "tacit" knowledge in their mind into explicit forms. We have observed that this knowledge conversion process seems to be most effective in this tool-oriented ethnographic fieldwork. From the cybersecurity researchers' perspective, we no longer view the practitioners' role as simply to help us evaluating our research prototype or providing data; rather, we view them as *the* experts who possess the knowledge that will inform the research and tool building. In some sense, the analysts are co-creating the tools with the researchers. The purpose of the research is not simply to automate the humans' tasks, but rather to give workers better tools for doing their jobs. The tool building process is not simply for the sake of having a better tool, but to reveal more tacit knowledge and make it explicit. In this iterative process, we identify and document the key findings regarding what are the main challenges in CSIRTs analysts' job, how they do the job, and how to make it better.

4 Closing Thoughts

When we started this work in 2012 at a K-State meeting of a subset of the authors, our motivation was two-fold. First, the fundamental question before us was how to make SOCs and in particular CSIRTs more effective (by any reasonable metric). The second question, which is related but not identical, was how cybersecurity researchers can play a significant role in the improvement of SOCs and CSIRTs. In the course of our work we have managed to make some progress on both fronts. The learning that we have obtained is described in this article and we provide these nuggets below in a succinct form to reinforce them in the minds of the reader.

4.1 Lessons Learned

- **The use of anthropology as an effective means to study the subject**

  When we started out, lacking a professional anthropologist in the team we had merely hypothesized based on our amateur understanding that anthropological methods would be effective

in understanding and studying the aforementioned questions. With the addition of a professional anthropologist (Wesch) to our team our methodology has been solidified and even revamped to some extent, and our experience thus far has left us with no doubt that we are on the right track. We have already uncovered new understanding of the reality of CSIRT operations that we have not encountered either in print or apocrypha. As this article is being written, we are still combing through the vast amount of fieldwork note we have accumulated and new findings will certainly continue to emerge as the research progresses. The anthropological concept of tacit knowledge helped us gain an initial understanding of the problems and then proceed on a trajectory to convert such tacit knowledge to explicit knowledge.

- **The importance of participation**

  Some of the authors have started out in the past with a (in hindsight, naive) notion that it is sufficient to understand the problems of CSIRTs by observing the environment and not actively participating in it. But, as the narrative above describes, we changed that model to one of robust participation where our fieldworker actively participates in the environment he is embedded in. Our experience has shown the effectiveness of the engagement as well as yielded immediate results in terms of rapport with the CSIRT staff.

- **The importance of tool co-creation**

  An obvious metric of our effectiveness is the level of acceptance of not only our embedded fieldworker but also the tools that are created jointly by the research team and the CSIRT staff in the process described in this article. A companion lesson to the previous one is that getting CSIRT staff to have co-ownership of the tools created not only enriches the tool but also enables its eventual acceptance in the CSIRT environment.

- **The criticality of tacit knowledge**

  Our experience has shown very clearly that the problems of CSIRT operations are not merely technological but rather dictated by the extreme demands of fast turnaround and high volume. None of our created and heavily used tools were high in technical sophistication; indeed many of the "more sophisticated" vendor tools present in the environment were ignored by the SOC team. The problem is intrinsically bound with the CSIRT personnel's internal model of the process that they undertake to achieve their goals. No tools can be effective until that internal model is made explicit, and as we discovered, every instance of tool acceptance in the CSIRT environment is an actual instance of conversion of this tacit knowledge into explicit form.

- **Open-ended nature of the learning process**

  As should be clear from the narrative, there are no definite endpoints to such a learning process. As we learn about the CSIRT, the external world keeps changing and the CSIRT has to continuously adapt. New knowledge that gets incorporated into the CSIRT is very likely to be tacit because of the experiential nature of the problem, which will have to be converted to explicit form as we go forward.

4.2 Future Work

In addition to deepening our fieldwork at K-State, we are now extending and expanding this effort to studying more SOCs, including commercial SOCs. We would like to find more partners to work

with us, so that our study can be more representative and valid. In particular, we will need help to access more SOCs to conduct the fieldwork. What we will need from our collaborators is to dedicate some human resources for doing this fieldwork. For academic collaborators, this could mean sending some students to SOC(s) and having regular meeting with the whole research team to exchange the findings produced from the fieldwork. For industry collaborators, this could mean having an analyst working with the student fieldworkers (apprentices) to train them in doing the job. The collaborating organizations will benefit from a third-party perspective of operational effectiveness, intra-team interactions, and other organizational attributes in the context of cybersecurity operations. They may also benefit from any tools that the fieldworkers build or help build specifically for the organization. At the end of the project, we expect to write a training manual with do's and don'ts for organizations employing cyber security operations personnel that are common to such organizations across businesses, academia, and governmental agencies. Collaborating organizations can also benefit by contributing to the framing and prioritization of issues to be addressed in such a manual as well as early access to learning.

4.3 Return to the Big Green Button

Xerox PARC really did ask Lucy Suchman, an anthropologist, to study users of their copy machines, and she did record the famous "when user hits machine" image [16]. However, the machine that user was hitting already had the big green button on it. It wasn't that users could not find the start button. It's that when they pushed it the machine would not do what they wanted it to do, if it did anything at all. From this, Suchman would make the point that no machine or tool is self-explanatory. "We need time to make unfamiliar devices our familiars," she explained. More importantly, as we make a tool our familiar we often change its use and function from that of its original intention. In this way, the users of tools are always in part also the authors of them. While traditional research methods like interviews and surveys might elicit somebody's explicit understandings, needs, and desires, only participant observation can help us understand the social context, underlying assumptions, and tacit practices that shape how tools might actually be used, adopted, and adapted in different work contexts. Likewise, as the tool is used it changes our routines and habits. It changes the way we think about and address problems. It might change who we collaborate with and how we collaborate with them. It might even be the catalyst for a complete restructuring of an organizational chart or workflow. As John Culkin (invoking the insight of his colleague, Marshall McLuhan) noted, "We shape our tools and thereafter our tools shape us." [4] The lasting lesson of the big green button is not that these complex problems demand simple solutions. Rather, it is the recognition that the relationship between humans and their tools is always going to be a complex one.

References

[1] H. Russell Bernard. *Research Methods in Anthropology: Qualitative and Quantitative Approaches*. AltaMira Press, 5th edition, 2011.

[2] Paul Richard Blum. Michael Polanyi: Can the mind be represented by a machine?, 2010. `http://existenceandanthropology.blogspot.com/2010/08/michael-polanyi-can-mind-be-represented.html`.

[3] J S Brown and P Duguid. Knowledge and organization: A social-practice perspective. *Organizational Science*, 12(2):198–213, 2001.

[4] John Culkin. A schoolman's guide to Marshall McLuhan. *Saturday Review*, March 18:51–53, 71–72, 1967.

[5] Paul Czyzewski, Jeff Johnson, and Eric Roberts. *Proceedings of the Conference on Participatory Design*. 1990.

[6] Paul Dourish and Genevieve Bell. *Divining a digital future: mess and mythology in ubiquitous computing*. MIT Press, 2011.

[7] Julia Elyachar. Before (and after) neoliberalism: Tacit knowledge, secrets of the trade, and the public sector in Egypt. *Cultural Anthropology*, 27(1):76–96, 2012.

[8] Clifford Geertz. Deep play: Notes on the Balinese cockfight. *Daedalus*, 101(1):1–37, 1972.

[9] Clifford Geertz. From the native's point of view: On the nature of anthropological understanding. *Bulletin of the American Academy of Arts and Sciences*, 28(1):26–45, 1974.

[10] Jean Lave and Etienne Wenger. *Situated Learning: Legitimate Peripheral Participation*. Cambridge University Press, 1991.

[11] Charles Leinbach. Managing for breakthroughs: A view from industrial design. In Susan Squires and Bryan Byrne, editors, *Creating Breakthrough Ideas: The Collaboration of Anthropologists and Designers in the Product Development Process*, pages 3–16. Greenwood Publishing, 2002.

[12] I Nonaka. A dynamic theory of organizational knowledge creation. *Organization Science*, 5(1):14–37, 1994.

[13] I Nonaka and G von Krogh. Tacit knowledge and knowledge conversion: Controversy and advancement in organizational knowledge creation theory. *Organization Science*, 20(3):635–652, 2009.

[14] Michael Polanyi. *The Tacit Dimension*. DoubleDay & Company, 1966.

[15] Susan Squires and Bryan Byrne. *Creating Breakthrough Ideas: The Collaboration of Anthropologists and Designers in the Product Development Industry*. Greenwood Publishing, 2002.

[16] Lucy Suchman. *Plans and Situated Actions: The Problem of Human-Machine Communication*. Cambridge University Press, 1987.

[17] Alan M. Turing. Computing machinery and intelligence. *Mind*, 59(236):433–460, Oct 1950.