Qualitative Approaches to Cybersecurity Research

Katie Shilton[1], Mega Subramaniam[1], Jessica Vitak[1], Susan Winter[1]
[1]College of Information Studies, University of Maryland, College Park

Abstract
Although billions of dollars are spent each year securing network infrastructure, devices, and resources against threats, the impact of cybersecurity arrangements on individuals remains largely unexamined. Unless cybersecurity technologies, policies, and processes are built with people, and their diversity, in mind, the needs of wide swaths of society—including children and teens, the elderly, women, low-income families, and people with disabilities—are unlikely to be addressed. Though many methods are important for investigating motivations, practices, and affect, *qualitative methods* are particularly necessary for nuanced ways of knowing about these phenomena. But qualitative research constitutes just a fraction of cybersecurity research. This fishbowl session will focus on research to enable usable, livable, and inclusive cybersecurity by exploring qualitative ways of knowing in cybersecurity research.
Keywords: Cybersecurity; qualitative methods; policy
doi: 10.9776/16495

Contact: kshilton@umd.edu

1 Description

1.1 Organizers and Key Participants

Katie Shilton, Assistant Professor, University of Maryland College Park
Mega Subramaniam, Associate Professor, University of Maryland College Park
Jessica Vitak, Assistant Professor, University of Maryland College Park
Susan Winter, Associate Dean for Research, University of Maryland, College Park

1.2 Purpose

Although billions of dollars are spent each year securing network infrastructure, devices, and resources against threats, the impact of cybersecurity arrangements on individuals remains largely unexamined (U.S. Department of Homeland Security, 2009). As a result, the affect, motivations, and practices of people are weak points for most cybersecurity initiatives. Populations that have struggled to gain access to critical technologies and information are often disenfranchised, while values such as autonomy, adaptability, privacy, and access to information tend to be treated as afterthoughts—if considered at all. Unless cybersecurity technologies, policies, and processes are built with people, and their diversity, in mind, the needs of wide swaths of society—including children and teens, the elderly, women, low-income families, and people with disabilities—are unlikely to be addressed.

Though many methods are important for investigating motivations, practices, and affect, *qualitative methods* are particularly necessary for nuanced ways of knowing about these phenomena (Creswell, 2002; Patton, 2001). But qualitative research constitutes just a fraction of cybersecurity research. This fishbowl session will focus on research to enable usable, livable, and inclusive cybersecurity by exploring qualitative ways of knowing in cybersecurity research. Research perspectives that utilize qualitative ways of knowing include: human-computer interaction (HCI), digital and information literacy, values and design, information and technology policy, engineering ethics, and diversity and inclusion all. Linking these fields to cybersecurity will improve our understanding of deeply human questions within cybersecurity research.

1.3 Intended Audience

The intended audience will be researchers (faculty, students, and industry participants) interested in the intersection of qualitative methods and cybersecurity research.

1.4 Proposed Activities

Session leaders Shilton, Vitak, Subramaniam, and Winter will seed the discussion by informally presenting their early-stage qualitative research in cybersecurity (5 minutes per presenter). Shilton will discuss discourse analyses of factors motivating attention to cybersecurity among mobile application

developers. Vitak will discuss interviews with parents and their tween children about balancing security goals with ICT use. Subramaniam will discuss the coverage of cybersecurity instruction and skills in middle schools (grades 6 through 8), using multiple case study method to analyze cybercivility curriculum from several counties. Winter will discuss some of the challenges of integrating qualitative and quantitative research within federal research initiatives and funding opportunities in cybersecurity.

We will then open the fishbowl for brainstorming. A fishbowl session arranges the room in concentric circles, with one chair or speaker in the middle. As individuals would like to speak, they work their way towards the center of the circle. The person in the middle of the circle has the floor for a maximum of two minutes before the room reshuffles.

A major advantage of the fishbowl format is that it encourages the group to moderate itself, resulting in a natural flow from one participant to the next, with relatively little need for top-down intervention on the part of the organizers. The use of time limits along with the physical flow of the fishbowl will ensure that a single participant, group of participants, or organizers do not dominate the conversation, allowing sufficient time and space for all participants to contribute to the discussion. The organizers will move through the room as participants gather before the event to encourage everyone to participate. Depending on turnout and the degree of enthusiasm among participants, one option will be to encourage “ringers” if needed: participants who are ready to share their experiences and perspectives. Each participant will be encouraged to share either their own ideas for qualitative cybersecurity research, or to provide their perspective on ideas that have already been shared. In this way, we will overlay a broad range of experiences and perspectives, generating a research agenda for this important emerging research area.

A graduate student scribe from the University of Maryland will record the brainstorming session and share these notes via an online collaborative document, to which all participants will be invited to contribute.

1.5 Relevance to the iConference

Cybersecurity is an issue of growing importance in the information field, and information researchers have unique experience and methods to contribute to this issue of national and international importance. This event will be highly interactive and will explicitly encourage participation from everyone in the room based on both the format and the topic.

1.6 Length of the event

We propose a 90-minutes session to allow for ample discussion and brainstorming.

2 References

Creswell, J. W. (2002). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (2nd ed.). Thousand Oaks, CA: Sage Publications, Inc.

Patton, M. Q. (2001). Qualitative Research & Evaluation Methods (3rd edition). Thousand Oaks, Calif: SAGE Publications, Inc.

U.S. Department of Homeland Security. (2009). A roadmap for cybersecurity research. Washington, DC: Department of Homeland Security.