CHAPTER 11

CONDUCTING ETHICAL RESEARCH IN SENSITIVE SECURITY DOMAINS: UNDERSTANDING THREATS AND THE IMPORTANCE OF BUILDING TRUST

Alex Stedmon and Daniel Paul

ABSTRACT

In many security domains, the 'human in the system' is often a critical line of defence in identifying, preventing and responding to any threats (Saikayasit, Stedmon, & Lawson, 2015). Traditionally, such security domains are often focussed on mainstream public safety within crowded spaces and border controls, through to identifying suspicious behaviours, hostile reconnaissance and implementing counter-terrorism initiatives. More recently, with growing insecurity around the world, organisations have looked to improve their security risk management frameworks, developing concepts which originated in the health and safety field to deal with more pressing risks such as terrorist acts, abduction and piracy (Paul, 2018). In these instances, security is usually the specific responsibility of frontline personnel with defined roles and responsibilities operating in accordance with organisational protocols (Saikayasit, Stedmon, Lawson, & Fussey, 2012; Stedmon, Saikayasit, Lawson, & Fussey, 2013). However,

Ethical Issues in Covert, Security and Surveillance Research
Advances in Research Ethics and Integrity, Volume 8, 159–176

Copyright © 2022 by Alex Stedmon and Daniel Paul. Published by Emerald Publishing Limited. These works are published under the Creative Commons Attribution (CC BY 4.0) licence. Anyone may reproduce, distribute, translate and create derivative works of these works (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this licence may be seen at http://creativecommons.org/licences/by/4.0/legalcode
ISSN: 2398-6018/doi:10.1108/S2398-601820210000008012

understanding the knowledge that frontline security workers might possess and use requires sensitive investigation in equally sensitive security domains.

This chapter considers how to investigate knowledge elicitation in these sensitive security domains and underlying ethics in research design that supports and protects the nature of investigation and end-users alike. This chapter also discusses the criteria used for ensuring trustworthiness as well as assessing the relative merits of the range of methods adopted.

Keywords: Ethical research; sensitive security domains; establishing trust; knowledge elicitation methods; deductive and inductive reasoning; stakeholders and end-users

INTRODUCTION: RESEARCH IN SENSITIVE DOMAINS

The lack of literature on security is not only down to the relative youth of the field as an academic discipline ('critical security studies' only really becoming a field in the 1990s, Buzan & Hansen, 2009), but also due to the way organisations protect such information and the difficulties in openly sharing it (Williams & McDonald, 2018). Organisations working in the security sector will carefully protect what data and information are publicly available both to ensure the safety of their staff and operations, and also because the reality is that processes are often far from optimal and could reveal potential shortcomings in management and practice (Harmer & Schreter, 2013). Such issues underpin research in sensitive domains by impacting the quality of data that can be collected in primary research and limiting the information available for meta-analyses (Barnard, Geber, & McCosker, 2001).

Though sensitive domains are often associated with health and safety research or specific investigations with vulnerable populations (Cowles, 1988; Sieber & Stanley, 1988), Lee (1993) uses an extended definition to include any domain that possesses three specific characteristics:

- *An intrusive threat* – where the research may cause strong emotional responses from participants. An intrusive threat is any subject which is highly personal to participants and has the potential to cause a negative emotional response (Cowles, 1988). Such typology is fitting to topics in which death and traumatic experiences are discussed, especially if the participant has been directly involved or has emotional links to those involved (Lee, 1993). To highlight the prevalence of death and trauma, between 2007 and 2016 there was a mean of 104 deaths a year in the humanitarian sector (Czwarno, Harmer, & Stoddard, 2017). It is not just death itself or major attack against a field worker, but the experience of being in a developing country, hostile environment or post-disaster setting that can have a negative emotional effect (Brewer, 2017). Such emotions can be re-experienced during the conduct of research and likely to pose an intrinsic threat as it may deal with concepts such as death and trauma by nature of the subject.

- *The threat of sanctions* – where participants fear that in revealing information there will be repercussions on them. For example, this may include situations where participants may have broken rules or committed wrongdoings and with the threat of sanctions this can limit what participants might want to openly say or admit to (Lee, 1993). As the security management has moved to a systems-based approach, a greater number of rules have been imposed on workers (Brunderlein & Grassmann, 2006). These rules give managers the power to impose disciplinary procedures on staff who go against the security measures (Harmer, Haver, & Stoddard, 2010). However, these remove the human aspect of decision making, meaning staff could face discipline for taking actions that were appropriate for the time and place but were contrary to the established rules (Beerli & Weissman, 2016). This is even more likely, where those in the field have little input into the rules imposed (Daudin & Merkelbach, 2011). Therefore, where participants admit to situations where they went against rules, there can be the underlying threat of sanction in the form of disciplinary action.
- *Political threat* – in the broadest sense where data collected might be used for negative purposes by powerful people or organisations (Lee, 1993). This is particularly the case where the research may reveal flaws in security measures which can then be exploited by aggressive actors (Brewers, 1990). For example, with the rise in the kidnapping threat, where aggressive actors conduct surveillance against targets to identify weaknesses (Harmer, Stoddard, & Toth, 2013) and any useful intelligence gleaned from research could be used against security workers themselves. Another aspect of political threat is the loss of funding from donors, for which many humanitarian organisations are critically dependent (Martin, Metcalfe, & Pantuliano, 2011). Humanitarian organisations may limit the information they share about their capabilities and weaknesses, so that donors are more likely to support them (Bollentino, 2008). Such competition for funding means that organisations often obscure the risks they are exposed to and may be reluctant to be fully transparent in the information they do share. Revealing information on security weaknesses can therefore cause a political threat, limiting transparency and producing a culture where participants are less likely to reveal information on operational weaknesses (Lee, 1993).

These characteristics help keep researchers aware of key issues associated with accessing and collecting data within sensitive domains. In doing so, it provides critical reflection on acceptability and ethics – whether the methods are acceptable to the participants and fit for the purpose of the research, and how the methods limit any potential negative effects on those involved in the research (Wilson, 2005).

DEDUCTIVE AND INDUCTIVE REASONING

Research in this domain usually takes an inductive, rather than a deductive, approach. Whilst there are merits to choosing a deductive approach, it suffers

from the assumption that the solution lies within the problem and therefore the problem statement must be known to all involved in some way (Wilson, 2010). In simple terms, if a statement cannot be known, then it is seen to be 'deductively' untrue. This is based on 'closed-world assumptions' where any statement which is true is there to be discovered and known to be true, and vice versa (Fox, 2008; Kelly, 2014).

Deductive research can produce strong and reliable conclusions, best suited to quantitative research methods where theories, hypotheses and specific variables can be tested and investigated (Lewis, Saunders, & Thornhill, 2009). However, it is problematic employing deductive reasoning when there are many unknowns (Babbie, 2011). This is often the case in security investigations, especially when investigating the effects of knowledge management on operational security (where established theories and foundational assumptions are lacking).

Inductive research is more suited to new or unexplored fields, as its greatest strength is that it can 'generate theory' where little data exist (Babbie, 2011). Inductive reasoning allows for, and helps to foster, emergent designs and grounded theory approaches (Given, 2008a; Pailthorpe, 2017). Although a theory may be disproven later, it can stimulate discussion and provide a basis for new theories to arise, or for the original theory to be refined through future deductive reasoning (Kelly, 2014). It is therefore important that inductive reasoning remains flexible and open to re-interpretation so that emergent themes can develop freely (Merriam & Tisdell, 2016).

Inductive research often begins with a specific focus and through data gathering identifies patterns and generates new understandings for why particular patterns exist (Bryman & Bell, 2011). In this way, general principles are developed from specific observations (Babbie, 2011). The starting point for inductive research often lies in collecting relevant data, employing mixed methods such as interviews or observations (Fox, 2008). Mixed methods allow the phenomenon to be viewed and tackled from multiple, complementary, angles and triangulated for greater scientific rigour (Milton, 2012).

Inductive reasoning is often employed within the discipline of human factors, which seeks to understand the interactions between humans and the systems they operate within (Stanton, Salmon, Walker, Baber, & Jenkins, 2005; Wilson, 2005). Human factors takes a user-centred perspective when investigating complex socio-technical systems that are typical of security settings (Stanton et al., 2013; Stedmon et al., 2013). By focussing on the individual, and employing knowledge elicitation methodologies, it is possible to identify and capture knowledge necessary for systems to work more effectively (Hoffman, 1987).

DEVELOPING AN ETHICAL RESEARCH APPROACH

Safeguarding those involved in research is paramount in any investigation. It is crucial that critical reflection of the methodologies to be used is applied to the research in order to help identify the inherent risks and how complementary methods can be used (Wilson, 2005). It can also help identify, at an early stage,

how the inductive approach can be developed to provide better results (Stanton et al., 2005). A primary concern in sensitive security domains is gaining access and promoting open and transparent data collection processes. This improves the critical reflection on the dependability, and therefore trustworthiness, of the approach and data collected in any investigation (Shenton, 2004). Several techniques can be applied to gain access to sensitive security domains and promote openness from participants:

- *Relationships and building rapport* – it is common for researchers to act as external observers, staying separated and not divulging personal lives to participants (Creswell, 2003). This builds into the concept of non-reactivity in that the researcher has as small an impact as possible on participants and the research (Wilson, 2005). Sensitive domain research requires an alternative approach where researchers develop trusting relationships and a trusted rapport with participants (Clark & Kotulic, 2004). This is often done by demonstrating a shared identity and purpose (Cowles, 1988) and sharing personal accounts relevant to the area of inquiry (Lee & Renzetti, 1990). In doing so, participants can identify the researcher who can promote more open and honest exchanges (Barton, 2015; Dickenson-Swift, James, & Liamputtong, 2007).
- *Recording data and alternatives to recording/transcribing* – both Clark and Kotulic (2004) and Cowles (1988) state that the use of digital recording can often deter participants from feeling open to answer sensitive questions. Therefore, alternative methods of recording data are necessary (Clark & Kotulic, 2004). Cowles (1988) suggests that whilst alternatives may be available, fully explaining the use of any data recorder, and making it known that the recorder can be turned off at any point allows the data to be captured for analysis, but also for the participant to maintain control of the exchange and to state things 'off the record' where appropriate (Cowles, 1988). Where this might occur, for accuracy and ethical reassurance, close written transcripts should be written at the time, reflecting both what is said as well as the context in which it was said.
- *Ensuring confidentiality and non-reactivity* – in any research, it is ethically vital that issues of confidentiality are dealt with sympathetically. It is important to take steps to remove the possibility of deductive-disclosure (i.e. identification of any data and/or individuals from what participants say or through job details) (Kaiser, 2009). In order for data to keep its rich description whilst ensuring privacy to those involved, techniques such as paraphrasing over verbatim transcribing may be necessary. In this way, researchers have a duty and participants have control in the way data are interpreted. Before data are collected, the protocols need to be explained to participants in order to allow them to decide what data can be used, and ensuring they are fully aware of how their data will be used, who will have access to it and how identities may be kept confidential (Adams & Cox, 2008). For a more detailed discussion of privacy in research see Chapter 3 in this volume.
- *Purposive sampling* – Clark and Kotulic (2004) suggest that limiting the number of participants involved in research allows greater time to be spent developing

relationships and trust. Purposive sampling is a common technique in qualitative inquiry, where the quantity of participants is secondary to the quality of data they can provide (Cochran & Quinn-Patton, 2007). To a degree, all sampling should have a purpose and should be representative of the wider population under investigation. Within the sensitive domain, participants are identified based on their relevance to the investigation rather than employing random sampling techniques (Bryman & Bell, 2011).

- *Recruitment of participants through professional networks* – in sensitive or in hard-to-reach domains, snowball or chain referral sampling methods are particularly successful in engaging with a target audience (Atkinson & Flint, 2004). This approach relies on cumulative referrals made by those who share knowledge or interact with others at an operational level or share specific interests for the investigation (Biernacki & Waldorf, 1981). Each successive referral further expands the possible number of people reached by the researcher (Atkinson & Flint, 2004). In this way, snowball sampling increases the possible sample size and accesses participants that other techniques may not allow (Atkinson & Flint, 2001). This method is predicted to be particularly effective in the humanitarian domain where there are strong informal networks (Kuhanendran & Micheni, 2010; Schneiker, 2015). This sampling method is useful where security agencies and organisations might be reluctant to share confidential and sensitive information with those they perceive to be 'outsiders'. This method has been used in the areas of drug use and addiction research (see Sims & Iphofen, 2003a, 2003b, 2003c) where information is limited and where the snowball approach can be initiated with a personal contact or through an informant (Biernacki & Waldorf, 1981). However, one of the problems with such a method of sampling is that the eligibility of participants can be difficult to verify as investigators rely on the referral process, and the sample includes only one sub-set of the relevant user population (Biernacki & Waldorf, 1981).
- *Safeguarding participants and researchers* – perhaps one of the most obvious concerns arising from ethics in research is safeguarding participants. Whilst this is seen as a critical element of the ethics appraisal or review process, it also serves to safeguard the researcher. In this way, a robust ethics application process and a knowledgeable and facilitative ethics review committee can make informed judgements on the methodological approach being fit for purpose and the procedure being appropriate to investigate the research question. It is also important to assess any risks of the research for all those involved so that suitable measures and contingencies are in place. In order to protect the safety of the researcher, protocols for researcher safety should be used, in which the potential safety risks are assessed prior to any in-person activities (i.e. interviews) being conducted (Gregory, Paterson, & Thorne, 1999). This also extends to the safety of the researcher after the research, where the sensitive data they hold might be sought after by hostile actors. The process of conducting research on sensitive issues can also have an emotional effect on participants or researchers (Clark & Kotulic, 2004; Lee, 1993). Support networks and training in psychological first aid can be of benefit in these instances.

Discussing sensitive issues can elicit emotional responses, that participants have not previously recounted (Cowles, 1988). Therefore, it is important that researchers are prepared to deal with these situations and can assist participants in finding any further support they might require (Clarke & Johnson, 2003). Such training may allow the researcher to sensitively approach difficult topics and provide access to information that participants may not otherwise disclose (Cowles, 1988).

Ultimately, the responsibility of ethics review in research is to protect researchers and participants alike (Cowles, 1988). As Wilson (1995) states, research should be based on non-reactivity principles, such that the research should not negatively impact those involved in collecting or providing data. Whilst research activities should ensure no one is put in any danger, this limits some applications and research settings (Gregory et al., 1999). For instance, research might be extremely challenging in high-risk environments with a very real threat to life or where participants may become vulnerable simply through the activity of providing data. Extreme care is needed to safeguard those providing what might be the richest data, without compromising their safety.

Core to this, issues of privacy and confidentiality underpin many of the ethical challenges of knowledge elicitation, where investigators must ensure that:

- end-users and stakeholders are comfortable with the type of information they are sharing and how the information might be used and
- end-users are not required to breach any agreements and obligations with their employers or associated organisations.

In many ways, these ethical concerns are governed by professional codes of conduct (in the UK this would be regulated by professional bodies such as the British Psychological Society) but it is important that investigators clearly identify the purpose of an investigation and set clear and legitimate boundaries for intended usage and communication of collected data.

CONDUCTING KNOWLEDGE ELICITATION

Whilst methods exist for knowledge elicitation in the security domain, they are relatively underdeveloped (Paul, 2018). It is only recently that security aspects of interactive systems have begun to be systematically analysed (Cerone & Shaikh, 2008, chapter 25). However, little research has been published on understanding the work of security personnel and systems, which leads to the lack of case studies or guidance on how methods can be adopted or have been used in different security settings (Hancock & Hart, 2002; Kraemer, Carayon, & Sanquist, 2009). As a result, it is necessary to re-visit the fundamental issues of conducting knowledge elicitation that can then be applied to security research.

Knowledge elicitation presents several challenges to investigators, not least in recruiting representative end-users and other stakeholders upon which the whole

process depends (Lawson & D'Cruz, 2011). Equally important, it is necessary to elicit and categorise/prioritise the relevant expertise and knowledge, and communicate this forward to designers and policy makers, as well as back to the end-users and other stakeholders.

One of the first steps in conducting knowledge elicitation is to understand that there can be different levels of end-users or stakeholders. Whilst the terms 'end-user' and 'stakeholder' are often confused, stakeholders are not always the end-users of a product or process, but have a particular investment or interest in the outcome and its effect on users or wider community (Mitchell, Agle, & Wood, 1997). The term 'end-user' or 'primary user' is commonly defined as someone who will make use of a particular product or process (Eason, 1987). In many cases, users and stakeholders will have different needs and often their goals or expectations of the product or process can be conflicting (Nuseibeh & Easterbrook, 2000). These distinctions and background information about users, stakeholders and specific contexts of use allow researchers to arrive at informed outcomes (Maguire & Bevan, 2002).

Whilst knowledge elicitation tends to be conducted amongst a wide range of users and stakeholders some of these domains are more restricted and challenging than others in terms of confidentiality, anonymity and privacy. These sensitive domains can include those involving children, elderly or disabled users, healthcare systems, staff/patient environments, commerce and other domains where information is often beyond public access (Gaver, Dunne, & Pacenti, 1999). In addition, some organisations restrict how much information employees can share with regard to their tasks, roles, strategies, technology use and future visions with external parties to protect commercial or competitive standpoints (Nonaka & Takeuchi, 1995). Security organisations may be particularly sensitive of any vulnerabilities that could then be perceived by the public as a lack of security awareness or exploited by competitors or aggressors for their own benefit. Security domains can also add further complications in reporting findings to support the wider understanding of user needs across this sector (Crabtree et al., 2003; Lawson, Sharples, Cobb, & Clarke, 2009), or where there are information sharing hurdles across agencies or countries (Williams & McDonald, 2018).

KNOWLEDGE ELICITATION METHODS

The human factors approach has made extensive and effective use of established social science methods such as questionnaires, surveys, interviews, focus groups, observations and ethnographic reviews and formal task or link analyses that can be used as the foundations to knowledge elicitation (Crabtree et al., 2003; Preece, Rogers, & Sharp, 2007). These methods provide different opportunities for interaction between the investigator and target audience, and hence provide different types and levels of data (Saikayasit et al., 2012). A range of complementary methods are often selected to enhance the detail of the issues explored. For example, interviews and focus groups might be employed to gain further insights or highlight problems that have been initially identified in questionnaires or surveys.

In comparison to direct interaction between the investigator and participant (e.g. interviews) indirect methods (e.g. questionnaires) can reach a larger number of respondents and are cheaper to administer but are not efficient for probing complicated issues or experience-based knowledge (Sinclair, 2005).

Focus groups can also be used, where the interviewer acts as a group organiser and facilitator to encourage discussion across several issues around pre-defined themes (Sinclair, 2005). However, focus groups can be resource intensive and difficult to arrange depending on the degree of anonymity required for the research. They are also notoriously 'hit and miss' depending on the availability of participants for particular sessions (Stedmon et al., 2013). In addition, they need effective management so that all participants have an opportunity to contribute without specific individuals dominating the interaction or people being affected by peer pressure to not voice particular issues (Friedrich & van der Poll, 2007). As with many qualitative analyses, care is also needed in how results are fed into the requirements capture. When using interactive methods, it is important that opportunities are provided for participants to express their knowledge spontaneously, rather than only responding to directed questions from the investigator. This is because there is a danger that direct questions could be biased by preconceptions that may prevent investigators exploring issues they have not already identified. On this basis, investigators should assume the role of 'learners' rather than 'hypothesis testers' (McNeese, Zaff, Citera, Brown, & Whitaker, 1995).

Observational and ethnographic methods can also be used to allow investigators to gather insights into socio-technical factors such as the impact of gate-keepers, moderators or more formal mechanisms in security. However, observation and ethnographic reviews can be intrusive, especially in sensitive domains where privacy and confidentially are important. In addition, the presence of observers can elicit behaviours that are not normal for the individual or group being viewed as they purposely follow formal procedures and act in a socially desirable manner (Crabtree et al., 2003; Stanton et al., 2005). Furthermore, this method provides a large amount of rich data, which can be time consuming to analyse. However, when used correctly, and when the investigator has a clear understanding of the domain being observed, this method can provide rich qualitative and quantitative real-world data (Sinclair, 2005).

Investigators often focus on the tasks that users perform in order to elicit tacit experience-based information or to understand the context of work (Nuseibeh & Easterbrook, 2000). Thus, the use of task analysis methods to identify problems and the influence of user interaction on system performance is a major approach within human factors (Kirwan & Ainsworth, 1992). A task analysis is defined as a study of what the user/system operation is required to do, including physical activities and cognitive processes, in order to achieve a specified goal (Kirwan & Ainsworth, 1992). Scenarios are often used to illustrate or describe typical tasks or roles in a particular context (Sutcliffe, 1998). There are generally two types of scenarios: those that represent and capture aspects of real work settings so that investigators and users can communicate their understanding of tasks to aid the development process; and those used to portray how users might envisage using a future system that is being developed (Sutcliffe, 1998). In the latter case,

investigators often develop 'user personas' that represent how different classes of user might interact with the future system and/or how the system will fit into an intended context of use. This is sometimes communicated through story-board techniques either presented as scripts, link-diagrams or conceptual diagrams to illustrate processes and decision points of interest.

Whilst various methods are available for researchers trying to elicit knowledge, research methods where the researcher and participant are seen as equals trying to overcome a problem together, are often more effective for sensitive domain research (Paul, 2018). Such methods are often described as 'contrived' (Milton, 2007) and expand upon methods where the participant simply describes how they accomplish a task, such as verbal protocol analysis (Shadbolt & Smart, 2015). Contrived methods, such as those highlighted in the figure above, allow the participant and the researcher to explore the issue together, as co-investigators, helping create more open conversations (Paul, 2018). They might therefore be seen as more appropriate for sensitive domain research.

COMMUNICATING KNOWLEDGE BACK TO END-USERS AND STAKEHOLDERS

Whilst various methods assist investigators in knowledge elicitation, it is important to communicate the findings back to relevant users and stakeholders. Several techniques exist in user experience and user-centered design to communicate the vision between investigators and users. These generally include scenario-based modelling (e.g. tabular text narratives, user personas, sketches and informal media) and concept mapping (e.g. scripts, sequences of events and link and task analyses) including actions and objects during the design phase (Sutcliffe, 1998). Scenario-based modelling can be used to represent the tasks, roles, systems and how they interact and influence task goals, as well as identify connections and dependencies between the user, system and the environment (Sutcliffe, 1998). Concept mapping is a technique that represents the objects, actions, events (or even emotions and feelings) so that both the investigators and users form a common understanding in order to identify gaps in knowledge (Freeman & Jessup, 2004; McNeese et al., 1995). The visual representations of connections between events and objects in a concept map or link analysis can help identify conflicting needs, create mutual understandings and enhance recall and memory of critical events (Freeman & Jessup, 2004). Use-cases can also be used to represent typical interactions, including profiles, interests, job descriptions and skills as part of the knowledge elicitation representation (Lanfranchi & Ireson, 2009). Scenarios with personas can be used to describe how users might behave in specific situations in order to provide a richer understanding of the context of use. Personas typically provide a profile of a specific user, stakeholder or role based on information from a number of sources (e.g. a typical child using a chat-room, a parent trying to govern the safety of their child's on-line presence, a shopper and a person using a home-banking interface). What is then communicated is a composite and synthesis of key features within a single profile that can then be used as a single point of

reference (e.g. Mary is an 8-year-old girl with no clear understanding of internet grooming techniques; Malcolm is a 60-year-old man with no awareness of phishing tactics). In some cases, personas are given names and background information such as age, education, recent training courses attended and even generic images/photos to make them more realistic or representative of a typical user. In other cases, personas are used anonymously in order to communicate generic characteristics that may be applicable to a wider demographic.

Knowledge elicitation with users working in sensitive domains also presents issues of personal anonymity and data confidentiality (Kavakli, Kalloniatis, & Gritzalis, 2005). In order to safeguard these, anonymity and pseudonymity can be used to disguise individuals, roles and relationships between roles (Pfitzmann & Hansen, 2005). In this way, identifying features of participants should not be associated with the data or approaches should be used that specifically use fictitious personas to illustrate and integrate observations across a number of participants. If done correctly, these personas can then be used as an effective communication tool without compromising the trust that has been built during the elicitation process.

Using a variety of human factors methods provides investigators with a clearer understanding of how security, as a process, can operate based on the perspective of socio-technical systems. Without a range of methods to employ and without picking those most suitable for a specific inquiry, there is a danger that the best data will be missed. In addition, without using the tools for communicating the findings of knowledge elicitation activities, the overall process would be incomplete and end-users and other stakeholders will miss opportunities to learn about security and/or contribute further insights into their roles. Such approaches allow investigators to develop a much better understanding of the bigger picture such as the context and wider systems, as well as more detailed understandings of specific tasks and goals.

ESTABLISHING THE TRUSTWORTHINESS OF QUALITATIVE DATA

Historically, the trustworthiness of qualitative research has always been challenged by positivist researchers. However, frameworks exist to improve the integrity, credibility and reliability of qualitative data (Lincoln, 1995; Silverman, 2011). An analytical approach to research not only increases the trustworthiness of the inquiry (Annett, 2005; Wilson, 2005) but is also necessary and useful for human factors research that sits between academia and praxis (Milton, 2012; Stanton et al., 2005). In this way, it allows an understanding of both how research contributes to the knowledge base and also its real-world application (Annett, 2005; Stanton et al., 2005).

Several authors have proposed principles for establishing trustworthiness in qualitative inquiry (Denzin & Lincoln, 2000; Given, 2008b; Guba, 1981; Lincoln, 1995; Silverman, 2011). It has become a central pillar of qualitative research, and particularly in exploratory investigations that are not guided by previous research

(Lincoln, 1995). Shenton (2004) provided a synthesis to ensure trustworthiness, which condenses four well-accepted constructs first posed by Guba (1981) and developed further by Guba and Lincoln (1985).

Credibility

Credibility is concerned with ensuring the findings are a true reflection of the research which has been conducted (Shenton, 2004). Denzin and Lincoln (2000) state that credibility is central to ensuring trustworthiness in qualitative research. Shenton (2004) proposed several constructs for credibility:

- Well-established research methods should be adopted. Less common methods may be used in conjunction to help extend the reach of the inquiry.
- Familiarity with the field under investigation is necessary, both through the researcher's professional involvement (where possible) but also through analysis of previous findings and appropriate review of existing research and knowledge.
- Where possible, purposive sampling should be employed to reduce any bias in data collection.
- Triangulation of mixed methods allows the research to be understood from multiple angles and compensates for any weaknesses inherent to certain methods.
- Methods to promote honesty should be used, including the opportunity for participants to refuse to be part of the investigation as well as the ethical basis of the research being stressed prior to data collection. This form of preventative measure reduces the possibility of participants lying or deceiving during data collection and assures them that they are in control of the data collection process. This is further supported with iterative questioning, in which the participants are asked to confirm information provided previously, and where information provided is rephrased later in the data collection session. This necessitates training and practice in the methods used but allows more transparent and honest datasets.
- Thick description has been used to provide detail for results and how they help develop knowledge and conclusions. Though this method is often lengthy, it allows readers to understand the way in which the data have been synthesised.

Transferability

The ability to transfer the interpretation of results to groups wider than the sample studied is an important aspect of both qualitative research (Silverman, 2011) as well as human factors methods, which are inherently practitioner-focussed (Wilson, 2005). In order to achieve this, thick descriptions of the results can be used that allow the reader to draw their own conclusions about how the results can be transferred (Shenton, 2004). It is also necessary, for research replication, to provide a full account of how the data were collected, and the approach taken,

including inclusion criteria, the methods used to collect data, the number of sessions conducted and how long these took (Guba, 1981; Shenton, 2004).

Dependability

Whilst quantitative, positivist research is concerned with empirical reliability, or how data collection should yield the same results every time (Silverman, 2011), qualitative research is mindful that the phenomenon under investigation may change over time (Shenton, 2004). Qualitative research usually only claims to present a view at a given time when the data were collected or in relation to the context they were collected in (Shenton, 2004). Instead, qualitative research may provide a 'prototype model', allowing the same methods to be employed by other researchers, understanding that the same conclusions may not be drawn and that understandings may evolve over time (Shenton, 2004).

Confirmability

Qualitative research does not rely on objective methods used by positivists as the collection and processing of data revolve around the researcher (Shenton, 2004). Researcher subjectivity and bias can be a major challenge and influence on the trustworthiness of qualitative research (Denzin & Lincoln, 2000). The use of triangulation in data collection is an important step in reducing bias and allows other researchers to scrutinise how the data were collected and analysed (Shenton, 2004).

Using these principles, it is important that research is designed based on the selection and use of appropriate methods that safeguard those involved and also that the method of communication is equally sensitive to issues of privacy and confidentiality. These factors also help identify how human factors methods (borrowed and developed from the social sciences) are designed to not only produce academically relevant data but also data can be used to tailor practical solutions to security threats (Stanton et al., 2005). Furthermore, by providing recommendations it is possible to review the transferability and trustworthiness of research findings beyond the sample studied (Shenton, 2004).

TOWARDS AN INTEGRATED UNDERSTANDING OF ETHICAL RESEARCH IN SENSITIVE SECURITY DOMAINS

Having reviewed the concepts underpinning ethical research in sensitive security domains, it is possible to provide an integrated view of these factors (Fig. 1).

In this configuration, we see that ethics is bounded by a number of typical threats to research in relation to intrusion, sanctions and political impacts of the work. It is important to be aware of the potential effects of these factors before starting out on a particular research activity as this may later impact on the trustworthiness of the research, or prevent data being collected in the first place.

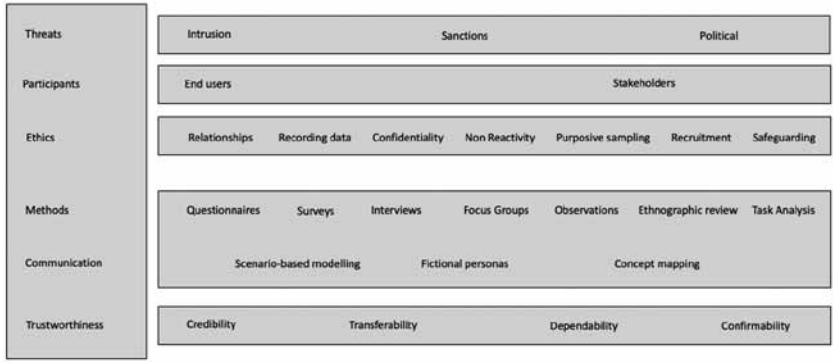

Fig. 1. Integrated Approach to Ethical Research.

With regard to knowledge elicitation as a methodological approach it is also important to understand who the end-users and stakeholders might be. We have seen already that these different actors within the problem space will have different perspectives and levels of investment in helping to find solutions.

A range of ethical issues have been introduced in this chapter which are relevant to participants (both end-users and stakeholders), embodied in the development of trusted relationships, how data may be recorded for sensitivity, confidentiality, non-reactivity, purposive sampling, recruitment of participants and safeguarding those involved.

A range of established methods from the social sciences are readily available for conducting knowledge elicitation and these need to be matched with appropriate communication techniques for sensitive data. Methods where the participant and researcher are seen as co-investigators, both exploring a solution to an issue (opposed to methods where information is being drawn out from the participant) are potentially more appropriate in sensitive domains.

Finally, the trustworthiness of the data needs to be considered prior to the research being conducted, so that responsible research is designed from the outset. This not only underpins the credibility, transferability, dependability and confirmability of research, but also fundamental concepts such as validity and reliability of what is often qualitative research.

Many of these concepts are inter-related and relevant to both end-users and stakeholders. By using this framework as a general tool for assisting with the design, conduct and communication of research in sensitive domains, it also provides a basis for reflecting on the success of different approaches so that lessons can be learned about the process of ethics as much as the conduct of ethics.

CONCLUSION

Security research usually takes an inductive approach, seeking to identify new theoretical principles through the collection of new data. In order to conduct

research within sensitive domains that is equally sensitive to the needs of those involved, a user-centred approach is important for understanding security from a human factors perspective. It is also important to understand the contexts in which investigations are situated so that ethical principles are upheld throughout the research process. There are many formal and established methodologies that are of use and it is essential that the researcher considers key issues as outlined in this chapter before choosing a particular approach. Whilst various methods and tools can indeed be helpful in gaining insight into particular aspects of knowledge elicitation for security, caution must be at the forefront as a valid model for eliciting such data does not exist specifically for security research at present. At the moment, investigations rely on the experience, understanding and skill of the investigator in deciding which approach is best to adopt in order to collect robust data that can then be fed back into the system process. Alongside this, it is important to establish the trustworthiness of qualitative data based on principles of credibility, transferability, dependability and confirmability. In this way, the ethical basis of research in this domain reaches beyond the actual activity of conducting the research but also what the research contributes to the wider knowledge base and understanding. Doing so allows a more structured approach for such research to be taken in the future and provides further opportunities for other researchers to access both the humanitarian security domain, as well as other security domains in which access to information could be limited.

REFERENCES

Adams, A., & Cox, A. (2008). Questionnaires, in-depth interviews and focus groups. In P. Cairns & A. Cox (Eds.), *Research methods for human–computer interaction* (pp. 17–34). Cambridge: Cambridge University Press.

Annett, J. (2005). A note on the validity and reliability of ergonomics methods. *Theoretical Issues in Ergonomics Science*, *3*, 228–232.

Atkinson, R., & Flint, J. (2001). Accessing hidden and hard-to-reach populations: Snowball research strategies. In N. Gilbert (Ed.), *Social research update* (p. 33). Guilford: University of Surrey.

Atkinson, R., & Flint, J. (2004). Snowball sampling. In A. Bryman, M. Lewis-Beck, & T. Liao (Eds.), *The SAGE encyclopaedia of social science research methods* (pp. 1043–1044). Thousand Oaks, CA: SAGE Publications, Inc.

Babbie, E. (2011). *The practice of social research.* Belmont, CA: Wadsworth, Cengage Learning.

Barnard, A., Geber, R., & McCosker, H. (2001). Undertaking sensitive research: Issues and strategies for meeting the safety needs of all participants. *Forum: Qualitative Social Research*, *2*(1), 1–14. Retrieved from http://nbn-resolving.de/urn:nbn:de:0114-fqs0101220. Accessed on May 26, 2021.

Barton, K. (2015). Elicitation techniques: Getting people to talk about ideas they don't usually talk about. *Theory and Research in Social Education*, *43*(2), 179–205.

Beerli, M., & Weissman, F. (2016). Humanitarian security manuals: Neutralising the human factor in humanitarian action. In M. Neuman & F. Weissman (Eds.), *Saving lives and staying alive: Humanitarian security in the age of risk management* (pp. 71–81). London: C. Hurst & Co.

Biernacki, P., & Waldorf, D. (1981). Snowball sampling. Problems and techniques of chain referral sampling. *Sociological Methods & Research*, *10*(2), 141–163.

Bollentino, V. (2008). Understanding the security management practices of humanitarian organisations. *Disasters*, *32*(2), 263–279.

Brewer, C. (2017). Aid workers: What overseas volunteers need to know. *Independent Nurse*, *11*, 16–18.

Brewers, J. (1990). Sensitivity as a problem in field research: A study of routine policing in Northern Ireland. *American Behavioural Scientist*, *33*(5), 578–593.

Brunderlein, C., & Grassmann, P. (2006). Managing risks in hazardous missions: The challenges of securing United Nations access to vulnerable groups. *Harvard Human Rights Journal*, *19*(1), 63–94.

Bryman, A., & Bell, E. (2011). *Business research methods* (3rd ed.). Oxford: Oxford University Press.

Buzan, B., & Hansen, L. (2009). *The evolution of international security studies.* Cambridge: Cambridge University Press.

Cerone, A., & Shaikh, S. A. (2008). Formal analysis of security in interactive systems. In M. Gupta & R. Sharman (Eds.), *Handbook of research on social and organizational liabilities in information security* (pp. 415–432). Hershey, PA: IGI-Global.

Clark, J., & Kotulic, A. (2004). Why there aren't more information security research studies. *Information and Management*, *41*, 597–607.

Clarke, J., & Johnson, B. (2003). Collecting sensitive data: The impact on researchers. *Qualitative Health Research*, *13*(3), 421–434.

Cochran, M., & Quinn-Patton, M. (2007). *A guide to using qualitative research methodology.* Geneva: Medicines Sans Frontier.

Cowles, K. (1988). Issues in qualitative research on sensitive topics. *Western Journal of Nursing Research*, *10*(2), 163–179.

Crabtree, A., Hemmings, T., Rodden, T., Cheverst, K., Clarke, K., Dewsbury, G., … Rouncefield, M. (2003). Designing with care: Adapting cultural probes to inform design in sensitive settings. In *Proceedings of OzCHI 2003*, University of Queensland, Brisbane Australia (pp. 4–13).

Creswell, J. (2003, November 18–26). *Research design: Qualitative, quantitative, and mixed methods approach* (2nd ed.). London: SAGE Publications Ltd.

Czwarno, M., Harmer, A., & Stoddard, A. (2017). *Aid worker security report 2017. Behind the attacks: A look at the perpetrators of violence against aid workers.* London: Humanitarian Outcomes.

Daudin, P., & Merkelbach, M. (2011). *From security management to risk management: Critical reflections on aid agency security management and the ISO risk management guidelines*. Geneva: Security Management Initiative.

Denzin, N., & Lincoln, Y. (Eds.). (2000). *The SAGE handbook of qualitative research* (2nd ed.). Thousand Oaks, CA: SAGE Publications, Inc.

Dickenson-Swift, V., James, E., & Liamputtong, P. (2007). Doing sensitive research: What challenges do qualitative researchers face?. *Qualitative Research*, *7*(3), 327–353.

Eason, K. (1987). *Information technology and organizational change*. London: Taylor and Francis.

Fox, N. (2008). Induction. In L. Given (Ed.), *The SAGE encyclopaedia of qualitative research methods* (pp. 429–430). London: SAGE Publications, Ltd.

Freeman, L. A., & Jessup, L. M. (2004). The power and benefits of concept mapping: Measuring use, usefulness, ease of use, and satisfaction. *International Journal of Science Education*, *26*(2), 151–169.

Friedrich, W. R., & van der Poll, J. A. (2007). Towards a methodology to elicit tacit domain knowledge from users. *Interdisciplinary Journal of Information, Knowledge and Management*, *2*, 179–193.

Gaver, B., Dunne, T., & Pacenti, E. (1999). Design: Cultural probes. *Interaction*, *6*(1), 21–29.

Given, L. (2008a). Emergent design. In L. Given (Ed.), *The SAGE encyclopaedia of qualitative research methods* (pp. 245–248). London: SAGE Publications, Ltd.

Given, L. (Ed.) (2008b). *The SAGE encyclopaedia of qualitative research methods*. London: SAGE Publications, Ltd.

Gregory, D., Paterson, B., & Thorne, S. (1999). A protocol for researcher safety. *Qualitative Health Research*, *9*(2), 259–269.

Guba, E. (1981). Criteria for assessing the trustworthiness of naturalistic inquiries. *Educational Communication and Technology Journal*, *29*, 75–91.

Guba, E., & Lincoln, Y. (1985). *Naturalistic inquiry.* Beverly Hills, CA: SAGE.

Hancock, P. A., & Hart, S. G. (2002). Defeating terrorism: What can human factors/ergonomics offer?. *Ergonomics in Design*, *10*, 6–16.

Harmer, A., Haver, K., & Stoddard, A. (2010). *Good practice review 8: Operational security management in violent environments* (rev. ed.). London: Overseas Development Institute.

Harmer, A., & Schreter, L. (2013). *Delivering aid in highly insecure environments: A critical review of literature, 2002–2012.* London: Humanitarian Outcomes.

Harmer, A., Stoddard, A., & Toth, K. (2013). *Aid worker security report 2013. The new normal: Coping with the kidnapping threat.* London: Humanitarian Outcomes.

Hoffman, R. (1987). The problem of extracting the knowledge of experts from the perspective of experimental psychology. *AI Magazine*, *8*(2), 53–66.

Kaiser, K. (2009). Protecting respondent confidentiality in qualitative research. *Qualitative Health Research*, *19*(11), 1632–1641.

Kavakli, E., Kalloniatis, C., & Gritzalis, S. (2005). Addressing privacy: Matching user requirements to implementation techniques. In *7th Hellenic European research on computer mathematics and its applications conference (HERCMA 2005)*, Athens, Greece, 22–24 September.

Kelly, D. (2014). *The art of reasoning: An introduction to reason and critical thinking*. New York, NY: W.W. Norton & Company, Inc.

Kirwan, B., & Ainsworth, L. K. (1992). *A guide to task analysis.* Boca Raton, FL: CRC Press, Taylor & Francis Group.

Kraemer, S., Carayon, P., & Sanquist, T. F. (2009). Human and organisational factors in security screening and inspection systems: Conceptual framework and key research needs. *Cognition, Technology and Work*, *11*(1), 29–41.

Kuhanendran, J., & Micheni, K. (2010). Saving lives together: A review of security collaboration between the United Nations and humanitarian actors on the ground. Retrieved from http://www.alnap.org/resource/9859 Accessed on May 26, 2021.

Lanfranchi, V., & Ireson, N. (2009, September 1–5). User requirements for a collective intelligence emergency response system. In *Proceedings of the 23rd British HCI group annual conference on people and computers: Celebrating people and technology*, Cambridge, UK (pp. 198–203).

Lawson, G., & D'Cruz, M. (2011). Ergonomics methods and the digital factory. In L. Canetta, C. Redaelli, & M. Flores (Eds.), *Intelligent manufacturing system DiFac* (pp. 23–34). London: Springer.

Lawson, G., Sharples, S., Cobb, S., & Clarke, D. (2009). Predicting the human response to an emergency. In P. D. Bust (Ed.), *Contemporary ergonomics 2009* (pp. 525–532). London: Taylor and Francis.

Lee, R. (1993). *Doing research on sensitive topics*. London: SAGE Publications, Ltd.

Lee, R., & Renzetti, C. (1990). The problems of researching sensitive topics: An overview and introduction. *American Behavioural Scientist*, *33*(5), 510–528.

Lewis, P., Saunders, M., & Thornhill, A. (2009). *Research methods for business students* (5th ed.). Harlow: Pearson Education Ltd.

Lincoln, Y. (1995). Emerging criteria for quality in qualitative and interpretive research. *Qualitative Inquiry*, *1*, 275–289.

Maguire, M., & Bevan, N. (2002). User requirements analysis. A review of supporting methods. In *Proceedings of IFIP 17th world computer congress*, Montereal, Canada, 25–30 August (pp. 133–148). Dordrecht: Kluwer Academic Publishers.

Martin, E., Metcalfe, V., & Pantuliano, S. (2011). *Risk in humanitarian action: Towards a common approach?*. Humanitarian Policy Group Report 39. Overseas Development Institute, London.

McNeese, M. C., Zaff, B. S., Citera, M., Brown, C. E., & Whitaker, R. (1995). AKADAM: Eliciting user knowledge to support participatory ergonomics. *International Journal of Industrial Ergonomics*, *15*, 345–363.

Merriam, S., & Tisdell, E. (2016). *Qualitative research: A guide to design and implementation.* San Francisco, CA: John Wiley & Sons, Inc.

Milton, N. (2007). *Knowledge acquisition in practice: A step-by-step guide*. London: Springer-Verlag.

Milton, N. (2012). Acquiring knowledge from subject matter experts. In J. Kantola & W. Karwowski (Eds.), *Knowledge service engineering handbook* (pp. 253–278). Boca Raton, FL: CRC Press.

Mitchell, R. K., Agle, B., & Wood, D. J. (1997). Toward a theory of stakeholder identification and salience: Defining the principle of who and what really counts. *The Academy of Management Review*, *22*(4), 853–886.

Nonaka, I., & Takeuchi, H. (1995). *The knowledge-creating company: How Japanese companies create the dynamics of innovation*. New York, NY: Oxford University Press, Inc.

Nuseibeh, B., & Easterbrook, S. (2000). Requirements engineering: A roadmap. In *Proceedings of international conference of software engineering (ICSE-2000)*, Limerick, Ireland, 4–11 July (pp. 37–46). New York, NY: ACM Press.

Pailthorpe, B. (2017). Emergent design. In C. Davis, J. Mattes, & R. Potter (Eds.), *The international encyclopaedia of communication research methods* (pp. 1–2) Hoboken, NJ: Wiley-Blackwell.

Paul, D. (2018). *A knowledge elicitation approach to improving security management systems in the humanitarian sector*. Unpublished Ph.D. thesis, Coventry University.

Pfitzmann, A., & Hansen, M. (2005). *Anonymity, unlinkability, unobservability, pseudonymity and identify management: A consolidated proposal for terminology*, version v0.25, December 6, 2005. Retrieved from http://dud.inf.tu-dresden.de/Anon_Terminology.shtml. Accessed May 26, 2021.

Preece, J., Rogers, Y., & Sharp, H. (2007). *Interaction design: Beyond human–computer interaction* (2nd ed.). Hoboken NJ: John Wiley & Sons Ltd.

Saikayasit, R., Stedmon, A., & Lawson, G. (2015). A macro-ergonomics perspective on security: A rail case study. In A. W. Stedmon & G. Lawson (Eds.). *Hostile intent and counter-terrorism: Human factors theory and application* (pp. 277–294). Aldershot: Ashgate Publishing Limited.

Saikayasit, R., Stedmon, A. W., Lawson, G., & Fussey, P. (2012). User requirements for security and counter-terrorism initiatives. In P. Vink (Ed.), *Advances in social and organisational factors* (pp. 256–265). Boca Raton, FL: CRC Press.

Schneiker, A. (2015). Humanitarian NGOs security networks and organisational learning: Identity matters and matters of identity. *International Journal of Voluntary and Nonprofit Organisations*, *26*(1), 144.

Shadbolt, N., & Smart, P. (2015). Knowledge elicitation: Methods, tools and techniques. In S. Sharples & J. Wilson (Eds.), *Evaluation of human work* (4th ed., pp. 163–200). Boca Raton, FL: CRC Press.

Shenton, A. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information*, *22*, 63–74.

Sieber, J., & Stanley, B. (1988). Ethical and professional dimensions of socially sensitive research. *The American Psychologist*, *43*(1), 49–55.

Silverman, D. (2011). *Interpreting qualitative data* (4th ed.). London: SAGE Publications, Ltd.

Sims, J., & Iphofen, R. (2003a). Parental substance use and its effects on children. *The Drug and Alcohol Professional*, *3*(3), 33–40.

Sims, J., & Iphofen, R. (2003b). The primary care assessment of hazardous and harmful drinkers. *Journal of Substance Use*, *8*(3), 1–6.

Sims, J., & Iphofen, R. (2003c). Women and substance misuse (monograph). The British Library Catalogue Number M03/37596 Special Acquisitions.

Sinclair, M. A. (2005). Participative assessment. In J. R. Wilson & E. N. Corlett (Eds.), *Evaluation of human work: A practical ergonomics methodology* (3rd ed., pp. 83–112). London: CRC Press, Taylor & Francis Group.

Stanton, N., Salmon, P. M., Rafferty, L. A., Walker, G. H., Baber, C., & Jenkins, D. P. (2013). *Human factors methods: A practical guide for engineering and design* (2nd ed.). Boca Raton, FL: CRC Press LLC.

Stanton, N. A., Salmon, P. M., Walker, G. H., Baber, C., & Jenkins, D. P. (2005). *Human factors methods: A practical guide for engineering and design* (pp. 21–44). Aldershot: Ashgate Publishing Limited.

Stedmon, A. W., Saikayasit, R., Lawson, G., & Fussey, P. (2013). User requirements and training needs within security applications: Methods for capture and communication. In B. Akhgar & S. Yates (Eds.), *Strategic intelligence management* (pp. 120–133). Oxford: Butterworth-Heinemann.

Sutcliffe, A. (1998). Scenario-based requirements analysis. *Requirements Engineering*, *3*, 48–65.

Williams, P., & McDonald, M. (Eds.). (2018). *Security studies: An introduction* (3rd ed.). Oxon: Routledge.

Wilson, J. (2010). *Essentials of business research: A guide to doing your research project*. London: SAGE Publications, Ltd.

Wilson, J. R. (1995). Ergonomics and participation. In J. R. Wilson & E. N. Corlett (Eds.), *Evaluation of human work: A practical ergonomics methodology* (2nd and rev. ed.). London: Taylor & Francis.

Wilson, J. R. (2005). Methods in the understanding of human factors. In N. Corlett & J. R. Wilson (Eds.), *Evaluation of human work: A practical ergonomics methodology* (3rd ed., pp. 1–31). London: Taylor & Francis.