Social Constructionism in security protocols

A position on human experience, psychology and security

Simon N. Foley[0000−0002−0183−1215] and Vivien M. Rooney[0000−0001−9983−5443]

Department of Information Security and Communication Technology
Norwegian University of Science and Technology
Gjøvik, N-2815, Norway

Abstract. Understanding the human in computer security through Qualitative Research aims at a conceptual repositioning. The aim is to leverage individual human experience to understand and improve the impact of humans in computer security. Embracing what is particular, complex and subtle in the human social experience means understanding precisely what is happening when people transgress protocols. Repositioning transgression as normal, by researching what people working in Computer Network Defense do, how they construct an understanding of what they do, and why they do it, facilitates addressing the human aspects of this work on its own terms. Leveraging the insights developed through Qualitative Research means that it is possible to envisage and develop appropriate remedies using Applied Psychology, and thereby improve computer security.

Keywords: Social aspects of security and privacy · Security requirements · Psychology · Qualitative Research methods · Computer Network Defence · Threat Intelligence

1 Introduction

A variety of approaches have been considered when analysing how user behaviour can influence the objectives of a security protocol. For instance, at the most basic level, a separation of duty protocol can be verified as protecting a transaction should one of the subscribing parties misbehave [10]. Approaches, such as security ceremonies, are intended to model complex patterns of human-system interaction and how user-(mis)behaviour might impact the objective of the security protocol in which they play a part [2, 8]. Such approaches have tended to focus on modeling the observable behavior of the users. More recently, it has been suggested that this analysis should be extended to incorporate the user as a human, and consider the human persona, societal norms, and so forth [5,13,14]. For example, does a separation of duty protocol achieve its objective if the users involved have a casual regard to rules which they may circumvent in order to help each other out? Notwithstanding the technical challenges of developing and reasoning about such models, there has been little consideration of what it means to use these models and how we come to understand and diagnose the human participation in security protocols.

Our position is that Social Constructionism provides a means to help understand and diagnose how humans experience security protocols. We argue that Qualitative Research methods can be used to systematically discover what it means to the participants to engage in a security protocol. This meaning can be in terms of their emotional, sensory, physical, volition and intellectual experiences. This presents the reality of how the participant experiences the security protocol. For example, how ambivalence or a stressful situation might lead to a perfunctory check of a separation of duty requirement. We are interested in using psychological theories to help diagnose and understand these experiences of participants in a security protocol and how these experiences may impact the protocol objectives; these insights may in turn help identify potential remedies. We are also interested in systematically developing rigorous models of this human experience that could be used as part of a formal analysis of the interoperation between human experience and protocol operation.

In this paper we explore this position through a use-case concerning a protocol for sharing threat information among computer network defenders.

2 Social constructionism and the human experience of technology

As social beings, humans make sense of the world around them in a social context, in interaction with others. In the process of describing and explaining a situation, or a series of events, the process of doing so is how we create that situation or those events. Our understanding of a situation or events is developed in the same way. This approach to understanding how people make sense of their world is a Social Constructionist one. Adopting this approach to understanding an experience with technology means that people construct that experience in dialogue. As people explain and describe their experience with technology, or with a particular aspect of technology, such as in their work environment, they are constructing its meaning. In the same way, if technology is part of a particular experience, or if it is the aspect of experience that we are particularly interested in, then the framework for researching and understanding that technology, or that aspect of technology, is a social framework.

Experience is something that continues to elude concise definition [17], however, for practical purposes, there are several interrelated components of which it is comprised:

- *Emotional* responses to, for example, people, spaces, events, outcomes, processes, memories.
- *Sensory* apprehension of the environment.
- *Physical* factors of the body and how they interrelate with the environment.
- *Volition* of individual desires and choices, taking account of, for instance, wishes, needs and values.
- *Intellectual* reasoning based on knowledge and beliefs.

These components of experience interrelate, for instance, take the example of a person making a difficult decision in a high stress environment. Their experience of making that decision can encompass all of the components, perhaps in conflict with each other, perhaps as inseparable from each other, as a decision is reached, and as the person makes sense of the process at the same time.

When we want to understand what is happening between people and technology, adopting a focus on human experience, rather than on what is observable, facilitates delving into the meaning that an artifact has for an individual. This approach allows us to uncover how the components of experience can interplay, for instance, how intellectual and volitional components can be in conflict with each other, and how such conflicts are given meaning as individuals reconcile them in dialogue. We can uncover that physical and intellectual components of the same experience are intertwined, and what this means for the individual. Thus, rather than being limited in our understanding to a cognitive approach of what is observable, or focusing on facilitating ease of interaction with technology, as a Human-Computer Interaction approach might, we can understand how and why a *human being* constructs meaning of their experience of technology.

3 Use case: cyber threat information sharing

The exchange of threat information within sharing communities is a recommended practice for individuals working in Computer Network Defence, such as Security Operations Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs). Studies report that effective information sharing and collective problem solving are required for a successful security incident response [1,18–20]. There are risks when sharing communities span multiple organizations and it is important that sensitive information about threats, their remediation and legal and organizational requirements are safeguarded. NIST special publication 800-150 [15] provides guidelines on sharing cyber threat information, with recommendations on how sharing relationships should be established and how individuals should participate in these sharing relationships. This collection of procedural and technical controls are regarded as a security protocol intended to mitigate the risks associated with the human-intensive information sharing activity.

For the purposes of exploring our position in this paper we propose a security protocol that provides a (very much simplified) interpretation of the spirit of NIST 800-150. Figure 1 defines this protocol as follows:

- The organization approves a Memorandum of Understanding (MoU) setting the constraints for exchanging threat information in a sharing community involving external parties who are considered trustworthy. The organization should proactively establish such sharing communities as part of its security processes and is discouraged from setting up new MoUs during security incidents.
- In the course of an ongoing security incident, a computer network defender wishes to confer with an external contact who is believed to be defending a similar incident:

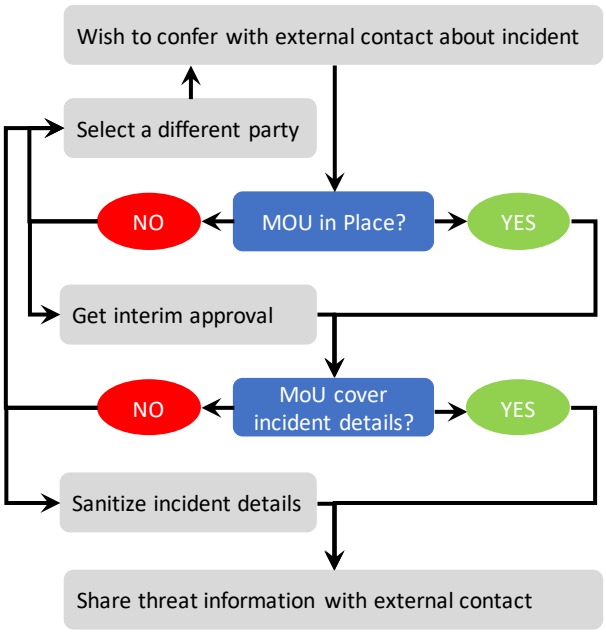


Fig. 1. Simplified threat information sharing protocol.

- If an MoU exists for the external party, then information sharing may proceed subject to the constraints of the MoU.
- If the MoU does not exist for the desired external party then the defender should seek a different party for which an MoU exists.
- An exception to this procedure is possible. If the trusted sharing communities cannot provide useful threat intelligence then the defender either requests an MoU to be established or else obtains interim approval from a line-manager to share limited information with the external party with careful recording of information disclosed.

4 Uncovering human security experience

From the Social Constructionist perspective, research findings are regarded as a situated interpretation, applicable to its particular context, and therefore open to subsequent reinterpretation. This contrasts with the Positivist perspective, where findings are regarded as a universal truth. The Social Constructionist approach being advocated in this paper has been used to research experiences with technology. One example is a project concerning the experience of Computer Network Defenders. The constructionist approach to Grounded Theory [6] was adopted, as an inductive approach to methodology is appropriate [22]. The data gathering technique of semi-structured interviewing was used [16], also cohering with the Social Constructionist perspective [22]. In this research project on the

experience of Computer Network Defense, semi-structured interviews were conducted with people working in Security Operations Centres and in Computer Security Incident Response Teams. The focus was on each individual's experience of work. The transcribed interviews were analysed using Grounded Theory techniques, such as line by line coding, the development of categories and themes, and memo writing. The theoretical analysis resulted in five themes [19].

In order to illustrate the outcome of the research, our focus in the current paper is on one particular phenomena that emerged during the Grounded Theory analysis of the transcribed interview data. This is the experience of information sharing in the context of the work of Computer Network Defenders. The Appendix gives examples of categories and line by line codes relevant to the context, action and meaning around the phenomena of sharing threat information by Computer Network Defenders in the course of their work. The following describes the experience of information sharing, and some of the components that interplay to create that experience. Line by line sample codes from the Appendix are included for convenience. In the following description of the phenomena surrounding threat information sharing, the relevant Grounded Theory codes are identified using a sans-serif font.

How the phenomena of information sharing is constructed by the Computer Network Defenders draws on multiple components of their experience. One component is procedures, and these are regarded variously as being: inflexible, something that slows you down during a crisis, yet as being important in an organisational context, and useful (proceduresSlowYouDown).

Another component of the experience of information sharing is the crisis itself, where speed in developing a workaround and a solution is critically important (workaroundNotInProcedures)(crisisSolvedSpeed). The importance of achieving this is bound up not alone in deploying one's skills and knowledge individually and as part of the team within the organisation (crisisWholeTeamWork), (crisisBeingAlone), it is also bound up in the social identity that is created by being part of the wider community of defenders (cyberDefendersCommunity). The span of this community of defenders extends beyond the organisational boundary (communicationWithNonTeam), and herein lies the tension of sharing information (cyberDefendersTension).

Being part of the community of Computer Network Defenders is regarded as akin to being a firefighter, and the fight is a global one against cyber attacks and cyber terrorism (cyberDefendersUnited), (cyberThreatsGlobal). Creating this identity is a very positive aspect of the experience of Computer Network Defense work. As such, being a member of this global community is important, and solving a problem during a crisis, an attack, means that people want to employ all of the resources at their disposal, including sharing and obtaining information outside of the organisation (externalLinksImportant), (linksWithOthersImportant). In this way, while procedures remain important, the membership of the global community can outweigh adherence to procedures. The ensuing dilemma around information sharing that is faced during a crisis (informationRequired), (informationSortingImportant), is rooted in these var-

ied factors, and simultaneously in a context where other tensions are also at play. Examples are tensions between different organisational agendas, such as those tensions between legal (regulatorsLegalAgenda), marketing and financial (crisisAssigningResponsibility).

For Computer Network Defenders, the experience of information sharing is characterised by contradictions, conflicts and unresolved tensions. The experience that is constructed is particular, complex and subtle, embedded in multiple overlapping contexts.

5 Explaining human security experience

We take two perspectives on the Grounded Theory analysis of the human experience of the security protocol. Firstly, we draw upon existing psychological theories related to the identified phenomena in order to better understand the human experience: this can help identify potential remedies for improving the protocol, helping the individual or simply accepting that something cannot be changed. Secondly, we consider how the Grounded Theory analysis might be used to develop rigorous models of aspects of the human experience for the purposes of understanding and diagnosing how an individual impacts the objectives of security protocol and vice-versa.

5.1 A psychological perspective

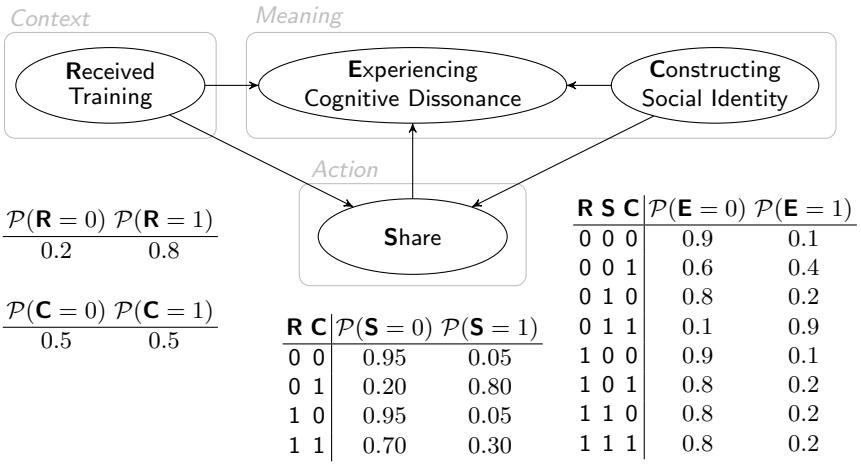
Understanding how Computer Network Defenders construct their experience of work provides insights into the process of how sense is made of the actions that people take in a particular situation. We can understand how a person perceived what they were doing, from their perspective, how this act made sense to them. We understand how, for instance, a protocol may be transgressed, and how sense was made of this act by the transgressor. This Social Constructionist approach facilitates the explanation and interpretation of experience in an abstract way, meaning that we can delve into the process of sense making, and develop a theoretical model that is valid in a particular situated context. This way of understanding the experience of Computer Network Defenders contrasts with Positivism, in that a predictive model is not possible. What is possible is the application of theory from Social Psychology to the emerging phenomena as a way of positioning the results of the study for practical purposes.

In [19] we proposed that Social Identity Theory [21], Relational Dialectics Theory [3,4] and Cognitive Dissonance [9] could be used in order to shed light on how people make sense of their experience of Computer Network Defense work. The potential of Social Identity Theory is to provide all stakeholders with the means of understanding, for instance, the components, significance and means of establishing Social Identity in the context of individuals and teams engaged in Computer Network Defense. Another phenomena that emerged from the research project concerned the manner of communication within the Security Operations Centre and Computer Security Incident Response Teams. We proposed [19] that

this constructive and democratic way of communicating be incorporated into staff training, framing what is an emerging team activity by Relational Dialectics Theory [3]. Other aspects of experience that emerged in the research project centred around Areas of Tension, the fifth theme that was identified during data analysis. This concerns the phenomena of information sharing as discussed above, and among other areas of tension identified is the use of intuition. The generation of psychological stress for Computer Network Defenders is associated with such areas, and it was proposed that Cognitive Dissonance Theory would be a useful way of understanding and ameliorating these issues [19].

5.2 Towards a socio-technical perspective

Recognising that the codes uncovered during a Grounded Theory analysis of semi-structured interview data can be interpreted as probabilistic variables [11], a qualitative elicitation methodology has been developed [12] whereby a Bayesian Network can be systematically built from a Grounded Theory analysis of interview data. The resulting model represents a machine-interpretable encoding of the identified phenomena. It is used in [12] as a means to elicit Attribute Based Access Control policies where the codes/variables uncovered during analysis represent the policy attributes.



$\mathcal{P}(\mathbf{R}=0)$	$\mathcal{P}(\mathbf{R}=1)$
0.2	0.8

$\mathcal{P}(\mathbf{C}=0)$	$\mathcal{P}(\mathbf{C}=1)$
0.5	0.5

R	C	$\mathcal{P}(\mathbf{S}=0)$	$\mathcal{P}(\mathbf{S}=1)$
0	0	0.95	0.05
0	1	0.20	0.80
1	0	0.95	0.05
1	1	0.70	0.30

R	S	C	$\mathcal{P}(\mathbf{E}=0)$	$\mathcal{P}(\mathbf{E}=1)$
0	0	0	0.9	0.1
0	0	1	0.6	0.4
0	1	0	0.8	0.2
0	1	1	0.1	0.9
1	0	0	0.9	0.1
1	0	1	0.8	0.2
1	1	0	0.8	0.2
1	1	1	0.8	0.2

Fig. 2. Simplified Bayesian Network of sharing experience

We are exploring how this approach might be adapted to develop machine-interpretable models that represent some part of the human experience of security protocols. Figure 2 depicts a Bayesian Network of aspects of the human

experience concerning the sharing of cyber-threat information. For the purposes of this paper we present it as a thought-experiment whereby the model represents what might be constructed from a Grounded Theory analysis carried out in our study of computer network defenders [19]. The probabilistic variables correspond to some of the codes uncovered during the study and their relationship (dependencies and transitional probabilities) is intended to represent the human experience of the participant interacting with the security protocol. These include

- Constructing Social Identity: the defender is constructing their Social Identity, making sense of what they are doing by being part of a community defending against threat. The community may be a specialised technical community, known personally to the defender. The community may be a global community of defenders who fight against cyber terrorism. In this context they are especially likely to do this when there's a potential crisis unfolding, and they wish to confer with other community members, sharing, seeking and comparing information about the phenomena that are being observed.
- Experiencing Cognitive Dissonance: disquiet arising from the experience of multiple realities that conflict with each other. This generates psychological stress; an additional burden on people working in the already high pressure environments of SOCs and CSIRTs. Lessening Cognitive Dissonance can help to improve functioning. For example, when conflicting realities have differing interpretations of procedures (in this case, whether or not an MoU is in place).
- Share: sharing threat information with colleagues outside the organization and contrary to procedure. More likely coincides with the defender enacting multiple realities and experiencing cognitive dissonance owing to procedure violation.

How the Bayesian Network might be systematically generated in practice using the approach in [12] is a topic of ongoing research. In the generated model three kinds of variables are identified:

- *Context* variables that represent participant beliefs about the context of the actions in which they engage. For example, whether there is an MoU in Place with an external party or whether the defender has recently Received Training to help them recognise and address cognitive dissonance.
- *Action* variables that represent the decisions that can be made by a participant to engage in an action. For example, the decision to contact and Share threat information with an outside party.
- *Meaning* variables represent the meaning of the experience by the participant when engaging, or otherwise, in an action in some context. For example, the participant is Constructing Social Identity or Experiencing Cognitive Dissonance.

The Bayesian Network can be used as a tool to help explore and diagnose the human experience of interacting with the security protocol. We used the SamIam

tool [7] to explore sharing based on the Bayesian Network defined in Figure 2. Computing directly from this network, and in the absence of any particular observations, the likelihood of external sharing is relatively low ($\mathcal{P}(\mathbf{S}{=}1) = 0.22$) as is the likelihood of staff experiencing cognitive dissonance ($\mathcal{P}(\mathbf{E}{=}1) = 0.21$). If specific phenomena (variables) have been observed then we can use the most probable explanation (MPE) for remaining unobserved variables by computing the maximum a-posteriori probability instantiation of all the variables given the evidence. For example, if we have evidence of external sharing ($\mathcal{P}(\mathbf{S}{=}1) = 1$) then, in the absence of any other observations, the most probable explanation is that defender(s) are constructing their social identities ($\mathcal{P}(\mathbf{C}{=}1) = 0.89$) and it is less likely that they are experiencing cognitive dissonance ($\mathcal{P}(\mathbf{E}{=}1) = 0.45$) since they are usually trained ($\mathcal{P}(\mathbf{R}{=}1) = 0.8$). However, if a compliance audit determines that they have not received training ($\mathcal{P}(\mathbf{R}{=}1) = 0$), then the most probable explanation is that they are experiencing cognitive dissonance ($\mathcal{P}(\mathbf{E}{=}1) = 0.86$) in the course of constructing their social identities ($\mathcal{P}(\mathbf{C}{=}1) = 0.94$).

In addition to helping to understand the human-experience of interacting with a security protocol, the Bayesian Network provides a machine-interpretable model that could play a role in the analysis of how human-experience can impact the objectives of the security protocol itself. For example, by providing a means to 'program' aspects for personas in Behavorial Computer Science [14] or for the human aspects of security ceremonies at Levels V (Communal) and IV (Personal) in the Bella-Coles-Kemp model [5]. These are future directions for the research.

6 Conclusion

In this paper we consider the elicitation and analysis of human experience in security protocols and the role that this plays in achieving the objective of the protocol. In the course of our research we observe that contemporary systems merit and require nuanced methodologies in order to better understand the user experience in what is a convoluted socio-technical context. Analysis of the phenomena using the psychological theories may help in remediation at a particular level, however they also point to the immutability of some practices and activities. This leads to the conclusion that notwithstanding the goals of user-centred security, sometimes human transgression might more usefully be re-conceptualized as a normal part of the status-quo.

Acknowledgement. This work was initiated at IMT Atlantique and completed at NTNU. It was supported, in part, by the Cyber CNI Chair of Institute Mines-Télécom which is held by IMT Atlantique and the Norwegian National Security Authority.

References

1. Albanese, M., Cooke, N., Coty, G., Hall, D., Healey, C., Jajodia, S., Liu, P., McNeese, M.D., Ning, P., Reeves, D., Subrahmanian, V.S., Wang, C., Yen, J.:

Computer-aided human centric cyber situation awareness. In: Liu, P., Jajodia, S., Wang, C. (eds.) Theory and Models for Cyber Situation Awareness, pp. 3–25. LNCS 10030, Springer (2017). https://doi.org/10.1007/978-3-319-61152-5_1
2. Basin, D.A., Radomirovic, S., Schmid, L.: Modeling human errors in security protocols. In: IEEE 29th Computer Security Foundations Symposium, CSF 2016, Lisbon, Portugal, June 27 - July 1, 2016. pp. 325–340 (2016). https://doi.org/10.1109/CSF.2016.30
3. Baxter, L.A.: Voicing Relationships. Sage Publications, London, UK (2011)
4. Baxter, L.A., Braithwaite, D.O.: Relational dialectics theory. In: Baxter, L.A., Braithwaite, D.O. (eds.) Engaging theories in interpersonal communication: Multiple perspectives, pp. 349–361. Sage Publications, London, UK (2008)
5. Bella, G., Coles-Kemp, L.: Layered analysis of security ceremonies. In: Information Security and Privacy Research - 27th IFIP TC 11 Information Security and Privacy Conference, SEC 2012, Heraklion, Crete, Greece, June 4-6, 2012. Proceedings. pp. 273–286 (2012). https://doi.org/10.1007/978-3-642-30436-1_23
6. Charmaz, K.: Constructing Grounded Theory. Sage Publications, London (2006)
7. Darwiche, A., et al.: Samiam: Sensitivity analysis, modeling, inference and more. http://reasoning.cs.ucla.edu/samiam, UCLA Automated Reasoning Group (accessed on 05/08/2019)
8. Ellison, C.M.: Ceremony design and analysis. IACR Cryptology ePrint Archive **2007**, 399 (2007), http://eprint.iacr.org/2007/399
9. Festinger, L.: A Theory of Cognitive Dissonance. Stanford University Press, CA, USA (1957)
10. Foley, S.N.: A nonfunctional approach to system integrity. IEEE Journal on Selected Areas in Communications **21**(1), 36–43 (2003). https://doi.org/10.1109/JSAC.2002.806124
11. Foley, S.N., Rooney, V.M.: Qualitative analysis for trust management. In: Christianson, B., Malcolm, J.A., Matyáš, V., Roe, M. (eds.) Security Protocols XVII. pp. 298–307. LNCS 7028, Springer Berlin Heidelberg, Berlin, Heidelberg (2009)
12. Foley, S.N., Rooney, V.M.: A Grounded Theory approach to security policy elicitation. Inf. & Comput. Security **26**(4), 454–471 (2018). https://doi.org/10.1108/ICS-12-2017-0086
13. Johansen, C., Jøsang, A.: Probabilistic modelling of humans in security ceremonies. In: Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance - 9th International Workshop, DPM 2014, 7th International Workshop, SETOP 2014, and 3rd International Workshop, QASA 2014, Wroclaw, Poland, September 10-11, 2014. Revised Selected Papers. pp. 277–292 (2014). https://doi.org/10.1007/978-3-319-17016-9_18
14. Johansen, C., Pedersen, T., Jøsang, A.: Towards behavioural computer science. In: Trust Management X - 10th IFIP WG 11.11 International Conference, IFIPTM 2016, Darmstadt, Germany, July 18-22, 2016, Proceedings. pp. 154–163 (2016). https://doi.org/10.1007/978-3-319-41354-9_12
15. Johnson, C., Badger, L., Waltermire, D., Snyder, J., Skorupka, C.: Guide to cyber threat information sharing. Tech. Rep. NIST Special Publication 800-150, National Institute of Standards and Technology, MD, USA (2016), https://csrc.nist.gov/publications/detail/sp/800-150/final
16. Kvale, S.: InterViews. An Introduction to Qualitative Research Interviewing. Sage Publications, London (1996)
17. Lallemanda, C., Groniera, G., Koenig, V.: User experience: A concept without consensus? exploring practitioners' perspectives through an interna-

tional survey. Computers in Human Behavior **43**, 35–48 (February 2015). https://doi.org/10.1016/j.chb.2014.10.048
18. Paul, C., Whitley, K.: A taxonomy of cyber awareness questions for the user-centered design of cyber situation awareness. In: Human Aspects of Information Security, Privacy, and Trust, LNCS, vol. 8030. Springer (2013). https://doi.org/10.1007/978-3-642-39345-7_16
19. Rooney, V.M., Foley, S.N.: What you can change and what you can't: Human experience in computer network defenses. In: Secure IT Systems - 23rd Nordic Conference, NordSec 2018, Oslo, Norway, November 28-30, 2018, Proceedings. pp. 219–235 (2018). https://doi.org/10.1007/978-3-030-03638-6_14
20. Sundaramurthy, S., McHugh, J., Ou, X., Wesch, M., Bardas, A., Rajagopalan, S.: Turning contradictions into innovations or: How we learned to stop whining and improve security operations. In: Symposium on Usable Privacy and Security (SOUPS). USENIX (2016)
21. Tajfel, H., Turner, J.: An integrative theory of intergroup conflict. In: Austin, W.G., Worchel, S. (eds.) The social psychology of intergroup relations, pp. 33–47. Brooks/Cole publishing, Monterey, CA (1979)
22. Twining, P., Heller, R.S., Nussbaum, M., Tsai, C.C.: Some guidance on conducting and reporting qualitative studies. Computers and Education **106**, A1–A9 (2017). https://doi.org/10.1016/j.compedu.2016.12.002

A Some categories and codes from the use case

The following provides examples of some of the uncovered categories and codes that are relevant to the phenomena of cyber-threat information sharing that emerged during Grounded Theory analysis, as part of a study on cyber network defenders.

A.1 Category: Procedures

Line by Line code (number of occurrences)
procedures/Absence/Creativity (2)
procedures/ImportanceOf (5)
proceduresSlowYouDown (1)

A.2 Category: Crisis resolution and team work

Line by Line code (number of occurrences)
crisis/WholeTeamWork (3)
work/CrisisBeingAlone (3)
workaround/NotInProcedures (2)

A.3 Category: Inherent Goods/Those gaining approval

Line by Line code (number of occurrences)
crisis/Solved (5)
crisis/Solved/Speed (2)
intuition/roleInTheWork (2)
procedures/Absence/Creativity (2)

A.4 Category: Crises described in detail

Line by Line code (number of occurrences)
crisis/Solved/Relief (3)
crisis/Solving/TakesTime (1)
crisis/Solved/Speed (2)
crisis/TimeLine (3)
identifyingTheCrisis (2)
identifyingTheCrisisEnd (8)
work/CrisisBeingAlone (3)

A.5 Category: Tension between differing agendas

Line by Line code (number of occurrences)
communicatingWithNonTeam (4)
regulatorsLegalAgenda (8)
tension/QualityServiceCommercialGoal (5)

A.6 Category: The company commercial matters

Line by Line code (number of occurrences)
askingForHelpOutsideTeam (2)
crisis/AssigningResponsibility (3)

A.7 Category: Being part of community

Line by Line code (number of occurrences in the data)
cyberDefendersCommunity (3)
cyberDefendersTension (2)
cyberDefendersUnited (6)
cyberThreatsGlobal (16)
externalContextImportant (5)
externalLinksImportant (8)
firefighterMercenariesRole (13)
informationSharingImportant (13)
informationToConfirmIncident (4)
linksWithOther[deleted]sImportant (6)

A.8 Category: Information on cyber security and defense

Line by Line code (number of occurrences in the data)
informationRequired [deleted] (11)
informationRequired[deleted]Burden (1)
informationSecurityImportant (8)
informationSharingManaged (11)
informationSortingImportant (13)