What you can change and what you can't: human experience in computer network defenses

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

IMT Atlantique, Lab-STICC,
Université Bretagne Loire, Rennes, France
vivrooney@gmail.com simon.foley@imt-atlantique.fr

Abstract. The work of Computer Network Defense conducted, for instance, in Security Operations Centers and by Computer Security Incident Teams, is dependent not alone on technology, but also on people. Understanding how people experience these environments is an essential component toward achieving optimal functioning. This paper describes a qualitative research study on the human experience of working in these environments. Using Grounded Theory, a psychological understanding of the experience is developed. Results suggest that positive and negative aspects of the work are either amenable or not amenable to change. Areas of tension are identified, and posited as the focus for improving experience. For this purpose, psychological theories of Social Identity Theory, Relational Dialectics, and Cognitive Dissonance, provide a way of understanding and interpreting these components of Computer Network Defence work, and can be used to assess the experience of staff.

1 Introduction

The technical tools and skills associated with individuals working in Security Operations Centres, Computer Security Incident Response Teams, and other Computer Network Defense environments [18], are well understood in terms of being leveraged to improve operational functionality. How these individuals experience their role is not well understood and is an understudied facet of cybersecurity. Operationally, technology tends to be the focus, while the issues concerning people and processes tend to be sidelined [18]. Among the issues that we do know are that there is a high staff turnover and that the work environment is characterized by multiple tensions [11, 12]. As a consequence, there is a loss of expertise and damage to team cohesion, as well as a need to have a constant supply of new staff being trained. Focussing on the psychology of the experience of these individuals has the potential to develop insights that can be applied to improve their experience of work. Thus, while understanding the technical tools and skills remains an essential part of understanding the environment in which Computer Network Defenders work, what is also essential is that we understand the human experience. The application of this knowledge provides an opportunity to improve the functionality of such work environments.

This paper describes an Applied Psychology research project with people who work in Security Operations Centres and Computer Security Incident Response Teams. Hereafter, we refer to these individuals as *computer network defenders*, who are engaged in *"the practice of defense against unauthorized activity within computer networks, including monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities"* [18]. The purpose of this qualitative research was developing a psychological understanding of the experience of people working in these environments, with the aim of applying this knowledge to improve that experience and thereby improving functioning.

Methodologically, the project draws on Grounded Theory [2] which facilitates gaining an understanding of everyday experience while at the same time supporting development of theory. The analysis identified the factors that interplay and comprise the experience of the staff, such as situational and organizational components, providing insights into what working in these environments entails.

The primary contribution of the paper is five themes that emerged from the study, as listed in Table 1. The results suggest that there are positive and negative challenges intrinsic to the work being conducted that, as such, either need not, or cannot, be altered. These intrinsic aspects can provide a learning opportunity. For instance, emergent within-team communication was identified. Theoretically, this is framed by Relational Dialectics, and is described as dialogical discussion. The application of the knowledge gained in the research to the development of a training platform would enable new staff to learn, and existing staff to improve, this technique, and thereby support the goal of improving overall performance. Another example is understanding the team's social identity. The significance of social identity facilitates understanding the meaning of, for instance, team membership, or the tensions and norms associated with being part of a community. Furthermore, improvement in functioning can be achieved in areas where uncertainty and ambiguity are a source of psychological stress. A focus on the areas where alteration is possible would alleviate the associated additional and avoidable burden. The relevant psychological theories are Social Identity Theory, Relational Dialectics, and Cognitive Dissonance.

The paper is structured as follows. Section 2 reviews related research and Section 3 provides an overview of the methodology. The five themes identified in the study are explained in Section 4, and Section 5 considers how we can interpret, and affect change, by drawing on existing psychological theory.

2 Related work

Research on the work conducted by Computer Security Incident Response Teams has adopted a largely cognitive perspective. For instance, research on Cyber Security Analysts [8] has focussed on the formalization of the process of sense making, describing the components as a series of four steps that take place against a backdrop of experience. These are information seeking, observation analysis, insight development and result production. While experience is regarded as playing an important role in sense-making, the researchers report on the lack of a

Theme	Description	Amenable to change	Applicable theory
Intrinsic Positive	regarded as being inherently positive, not needing explanation, therefore less salient to creating identity	don't want to change	social identity
Created Positive	explained as positive, therefore highly salient to creating identity	don't need to change	social identity relational dialectics
Intrinsic Negative	inherent aspects of the work, negatively regarded, less salient for team identity	can't change	social identity cognitive dissonance
Created Negative	negative aspects of the work less relevant to creating team identity	want to change	social identity
Areas of Tension	aspects of work regarded with ambivalence, highly salient for team identity	want to change	social identity cognitive dissonance

Table 1. Emergent themes and theories of Computer Network Defenders

clear definition of experience in the literature. A similar approach to understanding people working in Computer Security Incident Response Teams focusses on Situation Awareness. This concerns a state of knowledge within the context of a dynamic system, typically involving three stages. The stages identified are perception, comprehension and projection [10]. The first stage concerns information about the status, attributes and dynamics of relevant elements within the environment. The second stage concerns how people combine, interpret, store and retain that information. The final stage concerns predictions based on the knowledge perceived and comprehended [5].

Adopting the perspective of organizational psychology in their research on Computer Security Incident Response Teams, [3] report that people need blended technical and interpersonal skills, such as the ability to know when and how a problem being dealt with at the individual level ought to escalate and be dealt with at team level. At the team level, they report that there is a need to collaborate both within and outside of an organization. The necessary cognitive tasks for staff that the researchers identified are remembering, understanding, evaluating and analyzing. Similar to the Situation Awareness research [5, 10], this is detailed as the detection of patterns, focussing attention, combining pieces of information to reach conclusions, and multitasking. The authors report that effective information sharing and collective problem solving are required for a successful Computer Security Incident Response. Thus, there is a need to understand each other's knowledge, skills and abilities. What is required is identified as curiosity, investigative skills, the desire to acquire and share new knowledge with others, problem solving ability and attention to detail.

There has been limited qualitative research undertaken in this area, for example, [15], have focussed on improving tool development for use by system administrators, identifying the work environment as being complex and risky, and having unique information system requirements. Werlinger [17] used qualitative research methods to study tool improvement, and identified the organizational, technological and human challenges in the context of information security. Kandogan and Haber [6] used qualitative research to understand, describe and interpret the meaning and significance of the work of security administrators, reporting that, with experience, the event driven work is accomplished intuitively.

Taking a different perspective, [11,12] reported recently on their longitudinal in-depth study of five Security Operations Centres, using qualitative research methods. The authors report the existence of multiple tensions and contradictions in the work environment, existing between different types of staff, between staff and systems, as well as between staff and technology. Furthermore, it is reported that because new working conditions are accompanied by new tensions, it is necessary to address these issues on an on-going basis. For instance, new tools create new problems, hence the need for on-going attention to the ensuing tensions. Another example of tension concerns the role of metrics, specifically, how their generation may seem like a goal in itself, rather than a reflection of the work accomplished in the Security Operations Centre. Reported also is a lack of awareness or understanding of the goals and challenges of staff both at an interdisciplinary level, with financial, managerial and technical among the examples. Within disciplines, there is also scope for lack of understanding, as different levels of technicians and analysts are unaware of the difficulties, challenges and goals of other levels. Such difficulties are linked to burnout by the authors, and the high staff attrition that is characteristic of Security Operations Centres. The researchers also noted that Security Operations Centres can be very different, and that generalization may be unwarranted and misguided. A particularist approach, whereby Security Operations Centres are individually studied, may be warranted [11,12].

3 Approach and Methodology: Qualitative Research

The objective is to understand the experience of Computer Network Defenders. Qualitative research methods facilitate understanding experience, thereby avoiding limiting understanding to what is simply observable. Experience is comprised of a broad range of interrelated components, such as personal values, beliefs and social components. A Grounded Theory approach [2] was selected as the most appropriate for a number of reasons. For instance, the topic is likely to have been considered in depth by participants, which is particularly appropriate for Grounded Theory data analysis. In addition, the approach facilitates iterative data gathering and analysis, as it was anticipated that participant recruitment for semi-structured interviewing [7] would continue throughout the duration of the project. Figure 1 provides an overview of features of Grounded Theory.

Ethics and recruitment An ethical self-evaluation was conducted, following the principles for research projects involving human participants recommended by [14], and made available to participating organizations. This included protocols for data privacy and informed consent while being cognizant of Intellectual Property and other rights of participating organizations. Given the ethical requirements for informed consent in the project, recruitment was envisaged as being a negotiated process. In line with the informed consent agreement, any information that could lead to identification of participants is excluded.

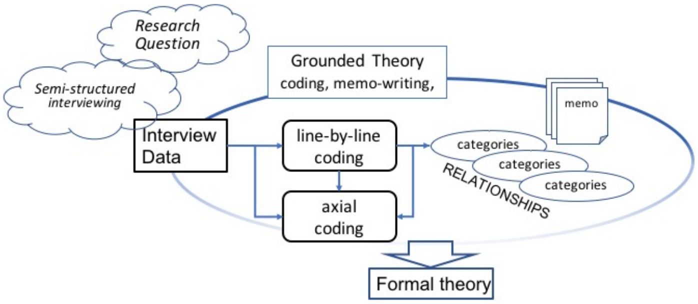

Fig. 1. Overview of the Grounded Theory process

Data gathering The qualitative research method of semi-structured one-to-one interviewing [7] was used. Interviews were conducted and transcribed according to [9] in light of the Grounded Theory analytic process to be applied.

Data analysis: initial coding Using the TAMS software tool, line-by-line codes were assigned (markup) to the text. The objective is the generation of codes encapsulating the meaning of each piece of data, lending transparency and validity to the analytic process and findings. A total of 231 codes were generated.

Data analysis: memo writing Memos record the research process, analytic ideas and direction, and potential theoretical development. Forty-four memos were compiled, documenting the analytic process from the construction of the interview schedules to development of a theoretical interpretation of the data.

Data analysis: categories and codes The purpose of this step is developing the analytic direction. A total of 24 categories were identified, under which the 231 codes were grouped. The categories are described in Memos.

Data analysis: axial coding This facilitates identifying and exploring connections between categories, and the development of themes. During the analysis, factors influencing the phenomena of interest emerge. These may be conditions around phenomena, the particular context of the actions and their consequences.

4 Results of the study

Uncertainty and change are intrinsic characteristics of the experience of working in cybersecurity. From the perspective of the Computer Network Defenders working in these specialized environments, the connotations of these intrinsic qualities are both positive and negative. The positive aspects of uncertainty and change mean that the work is always interesting, and that learning is part of their everyday working life. Both of these aspects are highly salient to the choice made to work in these environments. The negative aspects of uncertainty and change are the additional stress that these unknowns bring to their working life. The Computer Network Defenders are aware of the intrinsic benefits and difficulties. In reconciling these opposing qualities, they are also aware that the demands of their chosen field means that the work can be undertaken successfully only on a short term basis. This duration is envisaged as being approximately two years. Being intrinsic to the work, it is not possible to envisage how these positive and negative qualities can be altered. However, there are factors that exacerbate the aspects of the work that are intrinsically negative. Therefore, focussing efforts on improvement on what it is possible to alter may provide a means of understanding how best to ameliorate the difficulties faced. Taking steps to ameliorate the negative aspects of the working conditions for Computer Network Defenders has the potential to lessen the challenges of the work, therefore lowering the stress levels experienced, and ultimately extending the period of time that staff are willing to continue in their role. The benefit that can accrue with the attendant loss of expertise is improved functioning of the working environment.

Setting. The working environments of Computer Network Defenders have emerged in recent years in response to the need to deal with cyber threats and attacks. Working in these areas means that circumstances change rapidly. New problems arise, and, typically, the form that the new problem takes differs from the previous event. Firstly, there is a process during which a new event must be recognized and identified as such. Secondly, the particular form and substance of an event must be apprehended and understood. Thirdly, the most appropriate method for dealing with the particular event must be ascertained and formulated. Fourthly, the effectiveness of this process must be monitored on an ongoing basis. Finally, a determination on when an event can be deemed to have ended must be reached. As the foregoing illustrates, the nature of the work undertaken by Computer Network Defenders is that it is characterized by processes where change and uncertainty are intrinsic. As cyber attacks readily change their form and substance, corresponding change in both the form and substance of cyber defence work is a necessary and intrinsic quality.

In addition to the constant change that Computer Network Defenders encounter, uncertainty is also characteristic. For instance, along with the unpredictability of the form of cyber attacks as outlined above, the ordinary working experience is of relative calm during which there is no crisis, punctuated by periods when a crisis is taking place. During periods of calm, an attack is anticipated. However, rather than being discrete, periods of crisis/non-crisis exist on a continuum. During a crisis, the stakes for problem solving are high, and finding a solution is imperative. A problem without a solution is not an option. The uncertainty that is part of many aspects of the work presents challenges at the individual as well at the team level, and hampers the process of optimal decision-making that needs to be achieved. There are, however, tensions that it is possible to address, such as those emerging from the uncertainty around the use of intuition in problem solving, when the certainty of adhering to procedures is what is prescribed. The work is changing, complex and challenging. The paradox is that it is these intrinsic qualities of the work that make it attractive and satisfying for Computer Network Defenders, while at the same time being the reason that such work is not envisaged as being long term.

Main Themes. There are five main themes emerging from the analysis. (1) Intrinsic Positive, (2) Created Positive, (3) Intrinsic Negative, (4) Created Positive, and (5) Areas of Tension, as summarized in Table 1. Themes 1 to 4 concern matters that tend to be definite, these are matters that can be termed black and white in how they are explained and viewed by the Computer Network Defence workers. While this dichotomy reflects how the individuals experience aspects of their work in negative and positive terms, these aspects do not constitute a source of additional stress for staff. Rather, the Computer Network Defenders are aware that the work is stressful per se, and this is acknowledged and accepted. Theme 5, however, concerns areas that do contribute additional stress to the individuals and teams who work in Computer Network Defence. These areas are characterized by ambivalence, and the uncertainty surrounding them is a site of tension. These grey areas provide insights into areas where improvement in the experience of the work may be achieved. Figure 2 provides an overview of these themes with their identified code-categories. Themes are described discretely in this section, while the links between them are also noted.

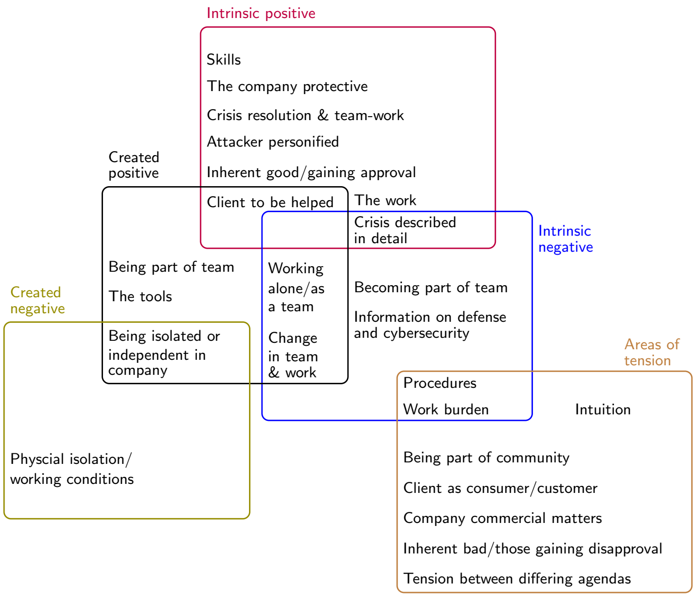
Intrinsic positive
Skills
The company protective
Crisis resolution & team-work
Attacker personified
Inherent good/gaining approval
Created positive
Client to be helped
The work
Crisis described in detail
Intrinsic negative
Being part of team
The tools
Working alone/as a team
Becoming part of team
Information on defense and cybersecurity
Created negative
Being isolated or independent in company
Change in team & work
Areas of tension
Procedures
Work burden
Intuition
Physcial isolation/ working conditions
Being part of community
Client as consumer/customer
Company commercial matters
Inherent bad/those gaining disapproval
Tension between differing agendas

Fig. 2. The emergent themes and their code categories

4.1 Intrinsic Positive

There are components that are intrinsic to the work, and are regarded as being inherently positive. This means that staff regard these aspects as being good in themselves, assigning them a high moral status. Being interested in the work for its own sake is part of this, as is enjoying problem solving and being curious; work that is boring is an anathema. The demanding and complex work means that people are busy, with individuals playing multiple roles within the team. There is enjoyment also in this variety, and having the freedom to approach complex problem solving flexibly, including, for example, using intuition to conduct the work, or choose to solve a problem, in a particular way. Understanding the processes, and products and how these fit into the team's work is also satisfying. One of the most interesting aspects of the work is the nitty-gritty of getting your hands dirty, devising a workaround, or building a solution to a problem.

Having and acquiring skills is regarded very positively, and this plays a dual role for the creation of identity. The practical role is being able to learn and apply skills to problem solving, and help in building solutions faster. The symbolic role is that the acquisition of skills indicates proficiency and, as such, is a step in becoming a fully integrated team member.

The crisis is the reason for the team's existence, and the experience of crises is positive. The crisis is not a source of enjoyment in itself, rather, the absorbing and energizing challenge it presents is a positive aspect of the work for Computer Network Defenders. The significance of the crisis is that other tasks are dropped and attention is focussed on problem solving. During communication, challenges and confrontations are part of how the individual team members bring their unique strengths into play. Solving a crisis can be satisfying, particularly if achieved quickly. The epitome of team cohesion is combining skills, experience and minds to work on resolution, and this is enjoyable and satisfying. The process of a crisis is engagaging, energising, and as such is a positive, even an enjoyable part of the work of the Computer Network Defenders. Resolution, nevertheless, is marked by a feeling of relief. Along with enjoying this aspect of the work for its interesting and challenging qualities, there is an awareness that attacks impact on people, who will suffer as a consequence. The altruistic motivation to help and protect people is a very positive component in the work, and in creating identity. As such this motivation, as well as the other positive components described, are how the Computer Network Defenders reconcile the choice they make to engage in work that they know is burdensome and demanding. Other positive aspects of the work concern how an attacker can provoke emotion, such as being detested, or playing a part in global terrorism. On a lighter note, a potential attack can also be a source of fun, or tension relief, among the team, and one example discussed is a potential attack being classified as innocuous.

4.2 Created Positive

There are aspects of the work that are deemed by participants as being positive. The contrast with the preceding section is that these aspects are not regarded as inherently positive, rather the participants choose that they are so, and therefore, in explaining how and why this is the case, they create their social identity. Being part of the team is regarded as being important and positive. As a team member, social norms apply, for example, that team cohesiveness is approved. Team cohesiveness is essential to the success of the how the team work. Being able to leverage team cohesiveness to engage in optimal ways of constructive argument is an approved activity, and one that is highly salient to the communication within the team, and hence, its functionality. This can mean that, for instance, during a crisis, even if going against one person's intuition, another team member's suggestion will be taken on board. At such times, the team will democratically confront and challenge proposed workarounds, as a way of reaching the best solution. Communication within the team is easy, for instance, it is easy to explain a question to another team member, in contrast to an outsider. This is important when on call, and especially important during a crisis. Another example of the usefulness of the approved social norm of team cohesion is that when people are on call they do not feel alone, they identify themselves as part of the team, being able to rely on each other for help and advice. Being alone in this context is a norm for the team that is entirely negative, in the sense of not having support when dealing with a crisis or potential crisis. Being able to rely on other team members is evidence of the mutual trust that the team place in each other, and this is salient to the effectiveness and identity of the team. Nevertheless, another part of the creation of the identity of the team is being aware of themselves as individuals, holding differing views, for example, on professional satisfaction, or having different skill sets, and strengths. Both the fact of, and having knowledge of each individual's strengths and weaknesses are considered as positive norms. For the team's social identity, understanding each other as individuals is an approved norm, facilitating successful functionality.

4.3 Intrinsic Negative

Some components of the work cannot be altered, being an intrinsic part of the Computer Network Defence work itself. These particular components are inherently negative, and accepted as being so by the staff. While these components are a source of stress, this is accepted as being part of the work, without rancour. There is, therefore, no expectation that these components could possibly be altered. Staff are reconciled to the stress they add to the burden of the work, and are a part of the reason why the work is regarded as being something that can be done successfully only in the shorter term. One component that is regarded negatively, yet as being unavoidable, is the process of becoming accepted by, and earning a place in, the team. As noted above, skills have a dual role and, similarly, the state of being alone in the context of Computer Network Defense work also has a dual role. Being alone, meaning being on call, or having to deal with a crisis without other team members, is regarded as being negative. A second meaning is that if you are on call alone, then this signals that you are trusted by the team, and this is a necessary step in becoming an accepted member of the team. Membership, as noted earlier, is important to the creation of social identity. The process of becoming a fully fledged member, while being negative, is, nevertheless, accepted as part of the process of entering into the group.

The demands associated with a crisis are accepted as being stressful, and this is negative. The uncertainty of duration, occurrence and resolution are negatively regarded as creating stress, yet at the same time, accepted as an intrinsic part of the work that they choose. A crisis can occur at any time, and at the initial stage of a crisis, its duration an unknown. Rather than being dichotomous, the crisis is described as a continuous state. A crisis is a spectrum of how the system is functioning. This state can range from where a service is not provided, or it may be a process of returning to the normal state, a service being re-established, fixed, or working, although not as it was designed. The restoration to normal may require time, hence a workaround might be used in order to achieve a functioning system. Change is a feature of the crisis, rather than a dichotomy of existing/not existing, and this, along with uncertainty, is accepted as an intrinsically negative characteristic of the work. Change is intrinsic to the experience of Computer Network Defence workers. This can encompass to the work itself, as described above, as well as more mundane matters, such as the expansion of the team, or the physical conditions of the work environment. Change can encompass what is anticipated for the future of a team, its work, or its conditions.

Regarded as a necessary evil, procedures are important in linking the activities conducted by the staff to those outside of the team. The links are with management and with other teams. Procedures can be a tool in the assessment of responses to crises, and as such are regarded as a means of retrospectively judging decisions made or actions taken during a crisis. This is significant because adherence to procedures can have legal or financial consequences. Procedures are regarded negatively for this, and other reasons as the work per se requires creative responses, in time critical situations. For instance, during a crisis, there is a need to be able to communicate and research. In such circumstances, procedures can slow down the process, and be regarded negatively, as a burden. There is, however, ambivalence concerning procedures that stems from their usefulness, as they can be effective as a memory aid, and are accepted as being necessary. Similarly, the process for changing procedures is regarded as being onerous, yet also necessary to ensure that any such changes are valid.

The demands of the work mean that while people enjoy some parts, they reconcile themselves to being in the post for only a finite amount of time. The work of the Computer Network Defenders can have a high profile within an organization, with correspondingly high expectations for performance to be excellent. With the work itself being characterized by change, as discussed earlier, this intrinsic characteristic compounds the requirement to meet the high expectations of those outside the team. This is an area where the work that is accomplished can be misunderstood, as can what it is possible to achieve, or the time frame required to achieve a task. The demands of the actual work are high also, for instance, being on call following a crisis, in the words of one participant, can be draining. Similarly, the volume of information that is available is large, and ensuring that what is what is not relevant is disregarded, and what is relevant is apprehended and managed correctly, presents a challenge. Demands such as these are an integral part of the work, and as such, are not expected to change. What the Computer Network Defenders can change is their own position in relation to the work. While participants view components of their work in a very positive way, as discussed earlier, they, nevertheless, do not envisage the job as being a long term proposition. The choice that the individuals make is to engage with work that they know is interesting and enjoyable, yet demanding, in the knowledge that these very characteristics mean that their choice is for remaining in the role for a limited duration.

4.4 Created Negative

There are aspects of the work that are deemed by participants as being negative. The contrast with the previous section is that these aspects are not regarded as inherent to the work, rather the participants highlight these as negative components that it is possible to alter. While regarding a certain amount of independence as positive, for instance, in managing some aspects of the work themselves, or in generating a fix for a problem, there is the negative corollary of feeling somewhat isolated from other teams. While physical isolation of the work environment is necessary because of the need to be in an environment where they can communicate freely, especially in relation to crises, this isolation is linked to a negative sense of being apart from other teams in the organization. The physical spaces that the teams occupy tend to be crowded and noisy, with people working in close proximity. This is beneficial in facilitating communication when needed, for example, during a crisis, however, the noise generated can be distracting to doing one's work, and hence can be draining for individuals. The rotas and hours worked are also noted somewhat negatively. While their importance is the requirement for cover at all times, any improvement in planning these would lessen the challenges faced as part of the work.

4.5 Areas of Tension

This theme focusses on the aspects of the work where there is ambivalence, where duality is required in order to reconcile their role, and as such, this creates additional and unnecessary tension for individuals and teams.

The Computer Network Defence workers construct their identity in the context of the global fight against cyber terrorism. Creation of this identity is a positive aspect of the work. The terms used to create this identity are likening themselves to, for instance, firefighters. This conceptualization creates a positive identity and belonging to a community that engenders pride in their work. Part of this identity is the adoption of a protective role, as seen also in the context of protecting and helping those who are suffering the consequences of an attack. The membership of this team of fighters means, however, that it also exists externally to the organizational work environment. This team exists in a wider community of experts, who are united in a global fight against attackers. As part of the fight that they are engaged with, their advantage lies in the strength that being united as a team entails. Their strategy to exploit this strength is the sharing of information. Membership of this wider community creates the social norm of being able to trust each other, as team membership requires. Team members might be, for instance, people with expertise, working in other organizations, who may know each other well. This enables information sharing to be practiced within an environment of trust, and being able to do so is regarded as being their main advantage in the fight against attackers. Herein lies the grey area that is source of tension. The need to search for, discuss, gather, share and manage information is regarded as a vital part of the work of Computer Network Defenders. Managing information in this way is a delicate process, where trust in people outside of the organization is a factor. There is, at the same time, an awareness of the need to protect the interests of the company when information is being sought and managed. The tension is in the links with those in the wider global community, yet who are external to an organization. While there is a formal procedure for making contact, this is a time consuming process, and as noted earlier, this can hamper problem solving, especially when the need for information is time sensitive. Consequently, an informal contact is more useful, and is used despite doing so being a grey area. Negotiating this delicate process constitutes a grey area in the work of Computer Network Defence workers, and the ambivalence around needing to act informally, despite formality being required, is a source of tension. Information per se can create difficulties in other ways, and to alleviate its management, and therefore streamline the associated work, obfuscating around information is a useful tactic. This is the case when disclosing information may be counter productive for the team in terms of creating additional work for themselves with less time being available for their primary team work of fighting against attackers. This is another grey area and as such a source of additional tension for the staff.

Another area where the contrasting positions of uncertainty and certainty is a source of tension in the work of Computer Network Defence teams is the use of intuition. The uncertainty associated with intuition contrasts with the certainty that procedures provide. Hence, the use of intuition is a grey area, and as such, a source of additional tension for staff. As discussed above, the work that is accomplished is always changing by necessity, as new attacks require new solutions. Solutions are arrived at through a creative process that takes place against a backdrop of the synthesis of, for instance, experience, insight, communication and technical skills. As we have seen, procedures are useful as a memory aid and also to provide certainty for those for whom how and when solutions to crises are provided may have legal and financial consequences. However, as we have also seen, procedures can be a means of slowing down problem solving. Slowing down a creative process hampers solutions to time sensitive problems. Not using the resource that intuition constitutes when dealing with crises would not cohere with the identity of the team as doing their utmost to protect and help those in need, nor with the openness that is also part of the team ethos. The need to downplay, or qualify the use of intuition in the work is another grey area that creates additional stress for staff.

Tension also stems from the two differing concepts of the work of Computer Network Defence teams. In reconciling these two concepts, a tension emerges as part of the experience, which centres around the difference between the rhetoric of the work, and the work as enacted. The rhetoric of the work is that there is certainty in what can be achieved. In the commercial enterprise context, certainty is an advantage, for marketing or financial purposes. This is particularly so when those outside of the Computer Network Defence work area do not fully understand the problems and their solutions at a technical level, and the reassurance that they desire can be provided. Misunderstanding the work of Computer Network Defence teams can create difficulties, such as when there is simplification in order to explain the work to non technical people. The enacted reality of the work is that there are elements of uncertainty in terms of what is available from the team, what is required in a particular situation, and what can be accomplished. The process of developing technical solutions may not be amenable to the certainty that is desired, or a particular solution may be inappropriate in a particular situation. This aspect of the work can be obfuscated by those whose agendas differ from the Computer Network Defence workers. Part of the social identity created by Computer Network Defence workers is altruistic, of being protectors, like firefighters, helping those in need. Their identity encompasses an ethos of protection, of seeing a crisis as a puzzle to be solved, and the enjoyment, learning and interesting nature of the work is rooted in the reality of the work they do, and an important part of creating their identity. Any obfuscation of the enacted reality that conflicts with their moral stance, the altruistic ethos, is a source of tension. Those with differing concepts of the work, or differing agendas, are a source of tension. The need for the reconciliation of these opposing tensions in the conduct of their day to day work creates an additional stress for the staff.

5 Changing the experience

What links the areas of tension discussed in Theme 5 is the need to reconcile the rhetoric of what ought to be done, with the enacted reality of practice. In these areas, a blind eye is turned to the reality when this does not cohere with what is prescribed. These grey areas are associated with uncertainty, when, for instance, people need to make important decisions in time sensitive situations. The necessity to cohere with a rhetoric of certainty, such as procedures and rules, creates a tension when people use what is uncertain, such as intuition.

What we have learned from studying the experience of Computer Network Defenders, is that these areas of uncertainty are a source of additional tension in an environment already experienced as being demanding. With the goal of improving the experience of these environments, the focus of resources on the reduction of tension would be of practical benefit. This in turn could provide a means of improving the functionality of the work environment. The application of theories from Psychology sheds light on the results, and how they might be interpreted in order to understand as well as improve the experience of this work.

Social Identity Theory [13] as a framework for the findings, illustrates how and why identity is created at three differing levels. Team membership is the core identity in Computer Network Defense. What is created at the individual level is identity that is subsidiary to that at the team level. Similarly, the process of attaining membership of the team is regarded as being intrinsically negative, and thereby creates the corollary, of not being in the team, as subsidiary. The social identity of being a team member is created in a very positive way, and as such, the centrality of its role in relation to the other two levels is underscored.

How and why identity is created, as discussed, illustrates the varied components that are important for the successful functioning of individuals and teams in Computer Network Defense work. Understanding, developing and fostering best practice in Computer Network Defense can be achieved by understanding the significance of the components that establish team and individual identity, and how they interrelate.

Relational Dialectical Theory [1] provides a way of understanding how communication, a core activity in the work, is experienced within teams. The emergent activity that is described in the findings once again foregrounds the importance of team membership, as the participants describe the constructive and democratic discussion engaged in to create workarounds and solutions to problems. The dialogue they engage in is open, constructive, and all voices are heard.

Engaging in a dialectical way means that assumptions are questioned, the certainty of one perspective is not accepted, rather, argument and discussion is oppositional and multi-vocal. The advantage of this way of communicating in Computer Network Defence is that it encourages the articulation of all ideas, even those opposed to what is dominant or accepted. In this way, the technique provides a means of accessing, utilizing and benefiting from the depth and range of skills and experiences available. This activity is linked to team cohesion, and as such is regarded as being very positive. It is noteworthy that recent research [16] on the development of applications for mobile software proposes dialectics to improve the process. The context is the difference between how engineers and attackers think, and the aim is lessening consensus and blind spots. The current findings show problem solving in Computer Network Defence is not ordinary discussion, rather it is active listening, valuing oppositional views, democratically taking account of all input, and where trust is a given. The team goal is problem solving, and within this context, the tensions associated with commercial and organizational goals are sidelined so as to facilitate the work. Relational Dialectical Theory regards dialogue as a creative social process, rather than a means of conveying information. Conceptualizing the emergent team communication activity in this way provides a framework for understanding this as part of optimal functioning. Applying this knowledge to enable the necessary skills to be developed and learned is an opportunity to improve how a core aspect of Computer Network Defense work is undertaken.

Despite the accomplished communication techniques that are emerging, there is a remaining area of tension, linked to problem solving. This area is the use of intuition, which, as we have seen, is at variance with procedural requirements.

Cognitive Dissonance [4] provides a useful theoretical framework for understanding such tension, or psychological stress generated, and why its reduction could be a means of ameliorating the stress associated with Computer Network Defense work, and thereby improve the work environment. In terms of the use of intuition, what is required can be seen as a contradiction in terms, thereby generating psychological stress. For instance, if there is a requirement for a flexible and imaginative approach in a crisis, and the use of intuition is part of this, while simultaneously, adherence to procedures needs to be demonstrated in retrospect, then there is cognitive dissonance. The rhetoric of what is required from staff contrasts with the enacted reality that they experience, and the result is psychological stress. This can impact on the functioning of teams. This tension that is not inherent to the work per se, and as such is an area that can be amended. Therefore, reducing the occurrence, or the impact of grey areas, provides a valuable opportunity for the goal of achieving optimal functioning.

Cognitive Dissonance Theory can also be applied to another source of tension. This relates to the identity of Computer Network Defence workers as part of a global team battling attacks. The creation of this very positive social identity engenders a sense of an altruistic community, and is a source of pride. The grey area that is part of this identity, and where Cognitive Dissonance Theory is useful, is in the links within this community, as they can extend beyond the organizational structure. The duality that creates psychological stress is the grey area of trusting the community, with the reciprocal exchange of information that is an essential component of the work. While formal procedures exist to facilitate communication outside an organization, they are cumbersome. In a time-sensitive situation, informality is effective, and can be essential to optimal functioning of a team. As with the use of intuition, any means of lessening the psychological stress that this site of tension generates would be beneficial.

6 Conclusion

People working in Computer Network Defence are aware of what is entailed in the choice they make to engage in high demand, high interest work. Part of this is knowing that such an engagement will necessarily be of short duration. The intrinsic qualities of the work render it unsustainable for longer duration, and people factor this into their choice to engage shorter term. Hence, there is no silver bullet that can be applied to the problem of staff attrition. While changing the intrinsic qualities of the work is not possible, there are opportunities to alleviate the stress experienced by staff. Paying attention to the experience of Computer Network Defenders, and acting on what is learned could pay dividends in reducing stress, and enable a longer term engagement with the work. The particularity of work environments varies, and Computer Network Defence is no exception. Nevertheless, the current findings are a useful resource. Using the theoretical framework of the five themes allows for the assessment of what is happening in a work environment. Areas where change can be effected, and that would be productive, can be identified. In this way, the findings provide a focus for the most effective deployment of resources to improve the experience of working in Computer Network Defence.

Acknowledgement. This work was supported by the Cyber CNI Chair of Institute Mines-Télécom which is held by IMT Atlantique and supported by Airbus

Defence and Space, Amossys, BNP Parisbas, EDF, Orange, La Poste, Nokia, Société Générale and the Regional Council of Brittany; it has been acknowledged by the French Centre of Excellence in Cybersecurity.

References

1. Baxter, L., Braithwaite, D.: Relational dialectics theory. In: Engaging theories in interpersonal communication: Multiple perspectives, pp. 349–361. Sage (2008)
2. Charmaz, K.: Constructing Grounded Theory. Sage Publications, London (2006)
3. Chen, T., Shore, D., S.J. Zaccaro, R.D., Tetrick, L., Gorab., A.: An organizational psychology perspective to examining computer security incident response teams. Security and Privacy **5**(12), 61–67 (2014)
4. Festinger, L.: A Theory of Cognitive Dissonance. Stanford University Press (1957)
5. Jajodia, S., Albanese, M.: An Integrated Framework for Cyber Situation Awareness, pp. 29–46. Lecture Notes in Computer Science 10030, Springer (2017)
6. Kandogan, E., Haber, E.: Security administration tools and practices. In: Security and Usability: Designing Secure Systems that People Can Use. (2006)
7. Kvale, S., Brinkmann, S.: InterViews. Learning the Craft of Qualitative Research Interviewing. Sage Publications, London, 2 edn. (2009)
8. Liu, P., et al.: Human subject research protocol: Computer-aided human centric cyber situation awareness: Understanding cognitive processes of cyber analysts. Tech. Rep. ARL-TR-6731, Army Research Laboratory, MD, USA (2013)
9. O'Connell, D., Kowal, S.: Basic principles of transcription. In: Rethinking Methods in Psychology. Part II, Discourse as Topic, chap. 7. Sage, London (1995)
10. 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)
11. Sundaramurthy, S., et al.: A human capital model for mitigating security analyst burnout. In: Symposium On Usable Privacy and Security. USENIX (2015)
12. Sundaramurthy, S., et al.: 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)
13. Tajfel, H., Turner, J.: An integrative theory of intergroup conflict. In: The social psychology of intergroup relations, pp. 33–47 (1979)
14. UK Economic and Social Research Council: Research ethics - ESRC, `http://www.esrc.ac.uk/funding/guidance-for-applicants/research-ethics/`
15. Velasquez, N., Weisband, S.: Work practices of system administrators: Implications for tool design. In: Symposium on Computer Human Interaction for Management of Information Technology. ACM (2008)
16. Weir, C., Rashid, A., Noble, J.: I'd like to have an argument, please: Using dialectic for effective app security. In: EuroUSEC 2017. Internet Society (April 2017)
17. Werlinger, R., Hawkey, K., Beznosov, K.: An integrated view of human, organizational, and technological challenges of it security management. Information Management & Computer Security **17**(1), 4–19 (2009)
18. Zimmerman, C.: Ten strategies of a world-class cybersecurity operations center. Tech. rep., The MITRE Corporation, Bedford, MA, USA (2014)