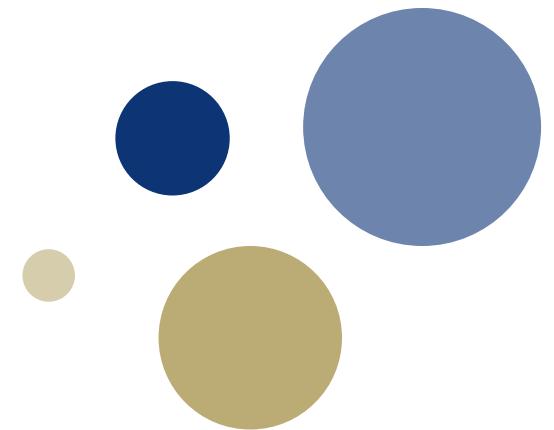




Norwegian University of  
Science and Technology



# Human experience in computer network defense

Simon Foley,  
Department of Information Security and Communication Technology,  
NTNU Gjøvik  
*(Joint work with Vivien Rooney)*

*NorCert Security Forum, Oslo, June 2019*



Trending Yemen Brexit Refugees North Korea Rohi

from Net Politics and Digital and  
Cyberspace Policy Program

## The Challenges Facing Computer Security Incident Response Teams



REVIEWS NEWS VIDEO HOW TO SMART HOME CARS GAMES DOWNLOAD

SEARCH

## How Target detected hack but failed to act -- Bloomberg

Despite alerts received through a \$1.6 million malware detection system, Target failed to stop hackers from stealing credit card numbers and personal information of millions of customers, Bloomberg reports.

CSC et HPE Enterprise Services  
forment désormais DXC Technology.

EN SAVOIR PLUS ▶

Security



by Lance Whitney  
13 March 2014 3:36 pm GMT  
@lancewhitney



Target



SUBSCRIBE  
from just £1 per issue

# NewStatesman

Follow us  
on Twitter

NS

POLITICS

CULTURE

WORLD

SCIENCE & TECH LONG READS NEW TIMES MAGAZINE EVENTS JUNE 2017

SUBSCRIBE



BY LUKE JENNINGS

CYBER 9 MARCH 2016

## Why are SOCs failing?

The fightback against security risks is very real –  
t Luke Jennings, head of research and

QUICK LINKS: State of cybercrime 2018 · Reviews · Video · Newsletters · CSO50 Awards ·

CSO  
FROM IDG

INSIDER Sign In

IN DEPTH

## Avoiding burnout: Ten tips for hackers working incident response

Recent security graduates entering the world of incident response, or those with a strong security background making a career move, face a challenging environment that often leads to frustration and burnout.



By Steve Ragan

Senior Staff Writer, CSO | APR 30, 2014 8:51 AM PT



# Ways of understanding computer defense work

Security Operations Centers Computer | Computer Security Incident Response Teams

- Technological
  - Tools, sensors, visualisation
- Human-Computer Interaction
  - Use of tools, interoperability, cognition
- Socio-technical experience
  - The human experience of working in a Socio-Technical Environment



# Working in a Socio-Technical Environment

- Previous study on Security Operations Centers:

*"There are tensions and contradictions within the SOC ... **tensions** between analysis and the tools used ... **conflicts** between analysts and operating rules ... **burnout** leading to poor judgements and frequent personnel turnover ... **vicious cycles** affecting the morale of analysts"*

[Sundaramurthy et al 2016]

- We want to develop an in-depth understanding of the human experience in computer network defense.

# What do we mean by Human Experience?

- Emotional responses to people, environment and situations
- Sensory awareness and influence
- Physical factors of the body and the environment
- Volition of individual desires and choices
- Intellectual reasoning



[Munch, *The Dance of Life*, 1900]

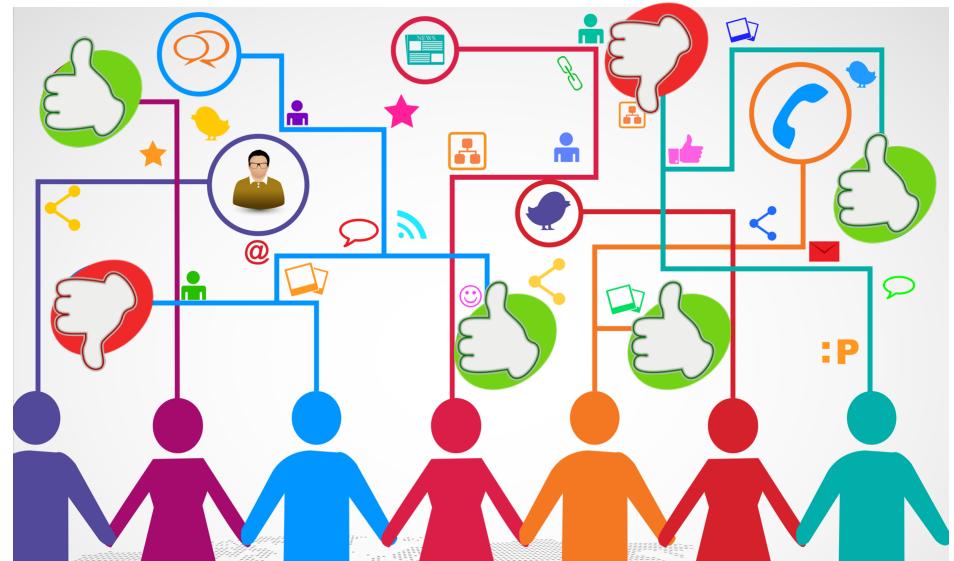
# Conducting the study

A qualitative study of human experience in computer network defense

# Communication within teams

An example of a result from the study

- Arguing & problem solving
  - Assumptions questioned
  - Certainty of one perspective not accepted
- Relational Dialectics in action
  - Dialogue as creative social process
  - Lessens consensus & blind spots
  - Helps build team cohesion
- A positive aspect of the work



# How to reliably arrive at such conclusions?

## Qualitative research methods

- Qualitative Research Methods
  - Techniques to uncover what is happening among people
- Study the psychology of the human in the loop
  - Understand what people do and why they do it
- Good for discovering unknown knowns

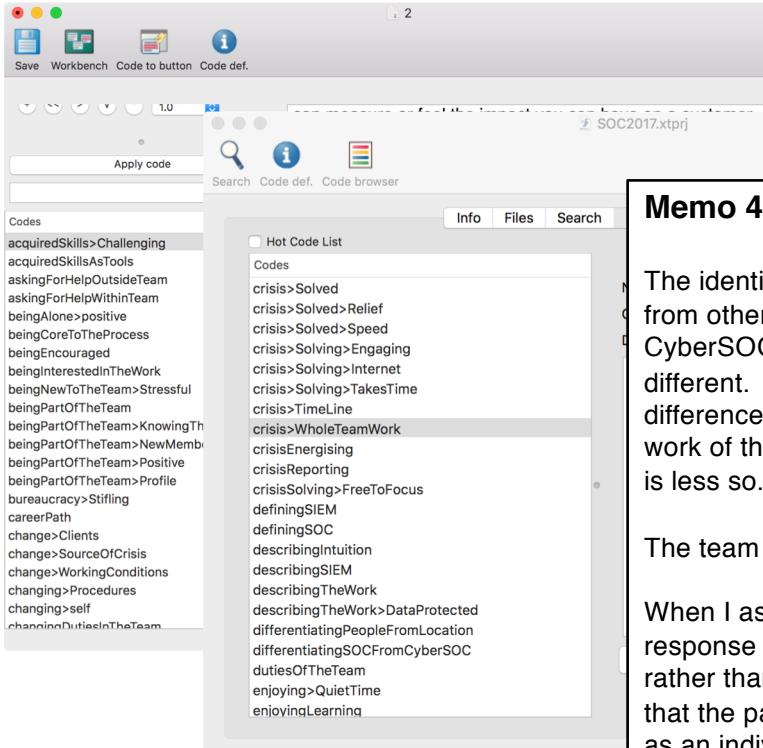


# Qualitative Research methods

A way to understand human experience



# What is it like to do Grounded Theory?



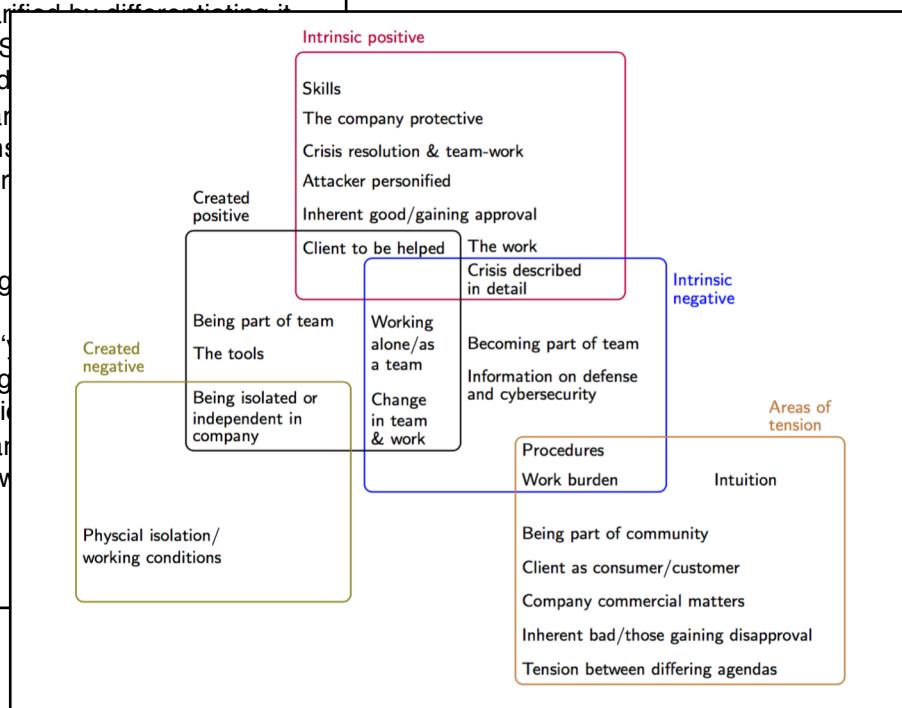
## Memo 4 - The identity of the team

The identity of the team is clearly different from other teams. Example: SOC vs CyberSOC. Level 1 team and different. There are very clear differences between the teams. The work of the SOC team is 'interesting' is less so.

The team and 'I' as interchangeable

When I ask a question about 'I', the response is as if I were asking 'the team' rather than the individual participant. That the participant answers as if he were an individual, and as if he were part of the team.

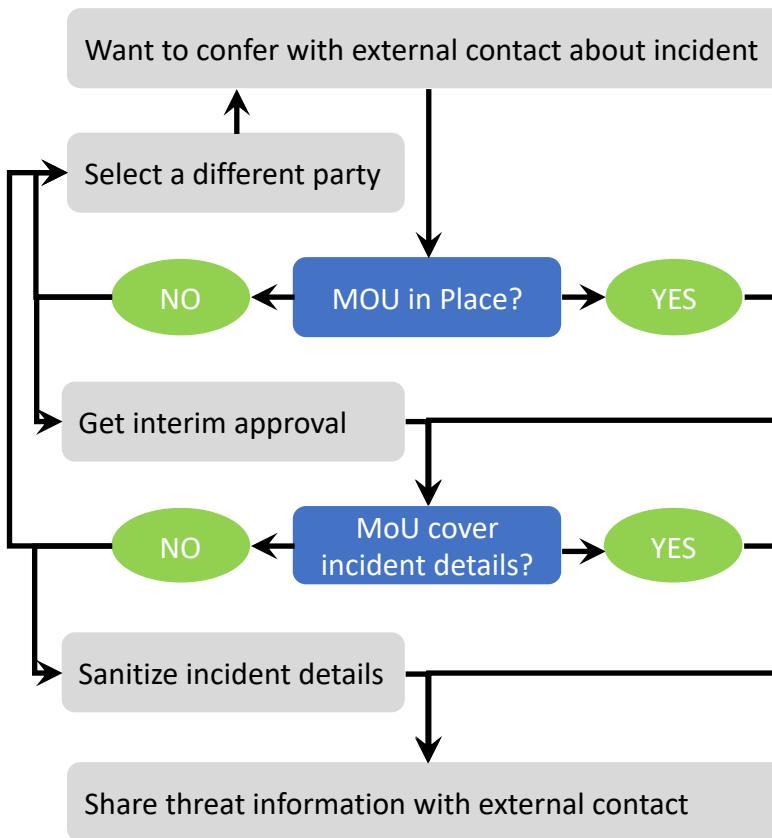
Example [...]



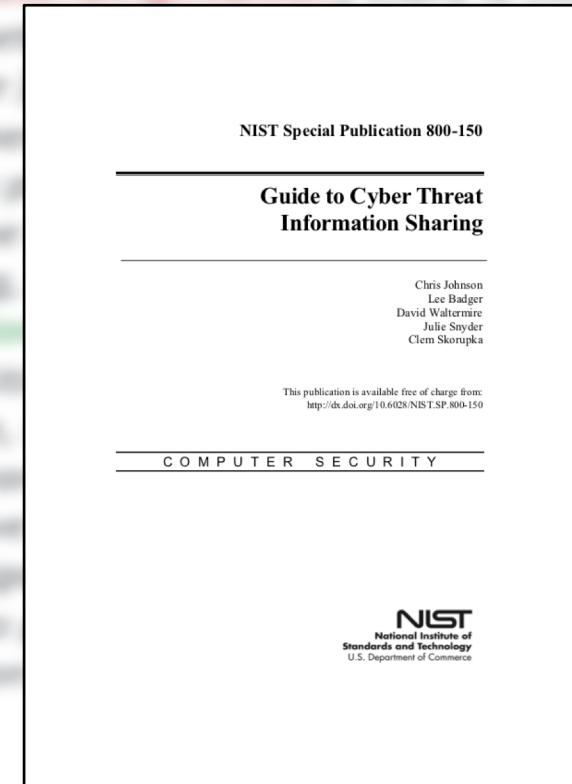
# Some results from the study

A qualitative study of human experience in computer network defense

# Threat information sharing



## Extract of semi-structured interview with cyber defender about threat information sharing:



# Threat Information Sharing

Making sense of experience by constructing multiple identities



## **Member of the organization**

- Procedures are important
- Procedures help you to work
- Procedures are followed
- ...

## **Team member**

- In a crisis, procedures are at a remove from the problem-solving activity
- mindful of team when reporting how procedures were followed
- ...

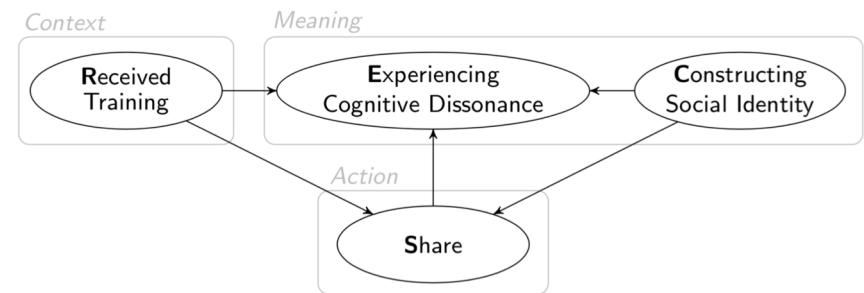
## **Member of a global community**

- Sharing information is important
- Procedures slow you down
- Procedures are sidelined
- ...

# Threat Information Sharing

Procedures as an area of tension

- Social Identity theory explains how and why identity is created
- Cognitive Dissonance occurs because multiple realities exist
- Relief from associated stress achieved through reconciling multiple realities



# The use of intuition by defenders

## Intuition as an area of tension

- Positive
  - Intuition is a useful resource based on experience
  - Can expedite a workaround to get system functioning
  - Can help build a solution during an attack
  - Is needed
- And negative....
  - Can be wrong
  - Even if not wrong, might need to be concealed
  - Problematic for retrospective analysis of crisis
  - Is a 'grey' area where a blind eye is turned

[redacted] There is intuition, [redacted] you know it, in the youth, that how the [intuition] member has done that or [redacted] when I, I think my research on it, I will have a point of information which would help me on the previous research I was doing on youth, I think we have, [green/redacted] we have to have a little bit of intuition, intuition, [redacted] but yes, it's sometimes hard to process it afterwards, because, with [blue/redacted] we have to evaluate the first level of interpretation [redacted], so, we can have to process it and like, most the intuition [green/redacted], you know [...]'

Extract from participant interview

# Understanding the ambivalence around intuition

## Experience of defenders

- Defenders experience multiple realities around intuition use
- Multiple realities are incompatible, Cognitive Dissonance occurs
- This increases stress

**Intuition is needed**

Using intuition incompatible with procedures

**Procedures can be sidelined**

Social identity important

Organisation identity important

Not using intuition is incompatible with social identity

Not adhering to procedures incompatible with commercial&legal requirements

**Procedures are adhered to**

Intuition is used

**Intuition is not used**



# Understanding the ambivalence around intuition

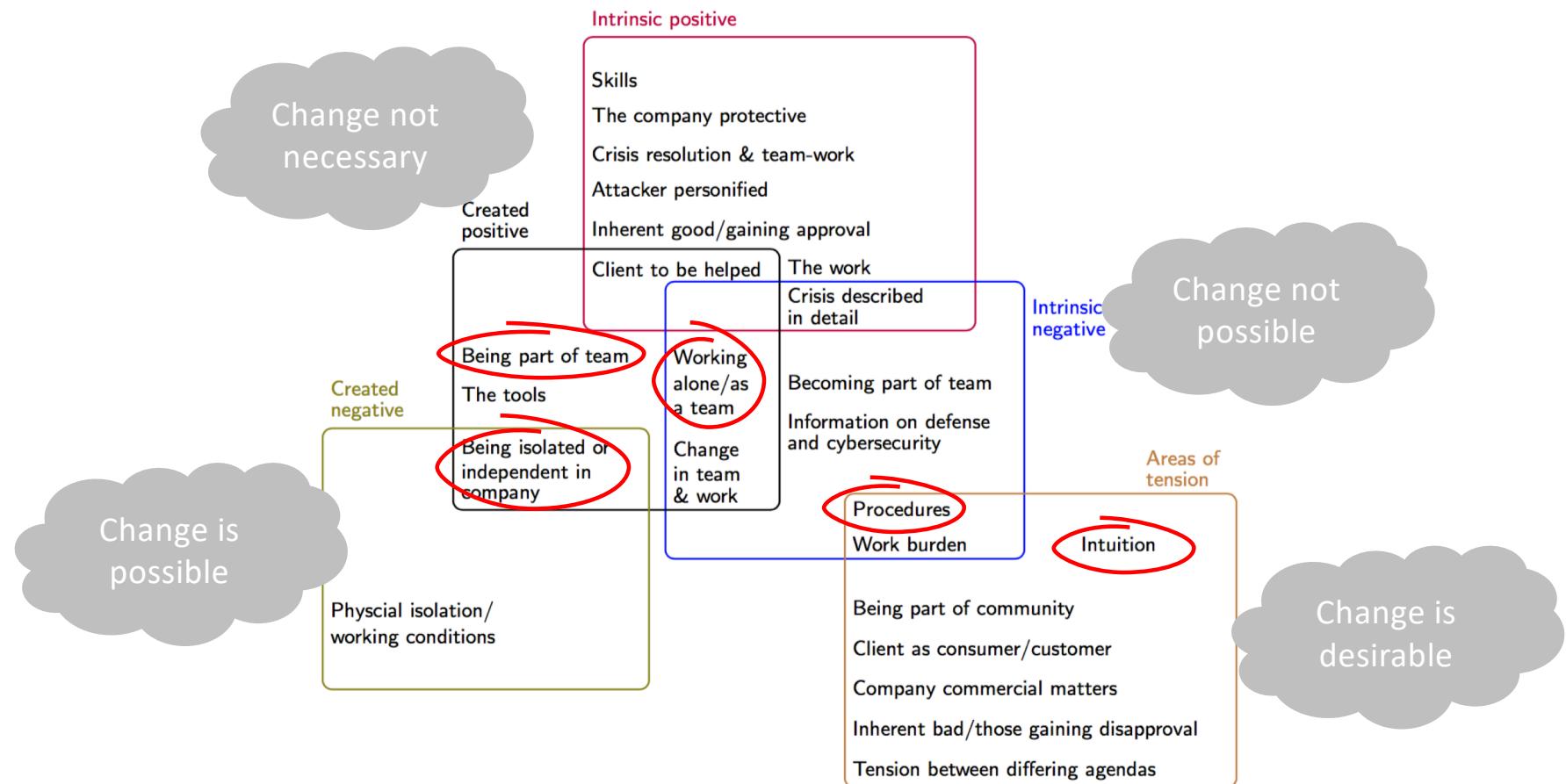
## Suggested Remedy | Outcome

- Investigate rhetoric and practice of intuition use at organization level
- Research how, when and why particular realities are privileged over others
- Alleviate stress of Cognitive Dissonance by altering the meaning of intuition use



# Overview of results

## A model of human experience of Computer Network Defenders



# Overview of results

## A model of human experience of Computer Network Defenders

Theme	Description (by participants)	Salience for creating identity	Amenable to change	Applicable psychological theory
Intrinsic Positive	Explanation not required	Low	Not necessary	Social Identity
Created Positive	Explained as positive	High	Not necessary	Social Identity Relational Dialectics
Intrinsic Negative	Explanation not required	Low	Not possible	Social Identity Cognitive Dissonance
Created Negative	Explained as negative	Low	Possible	Social Identity
Areas of Tension	Regarded with ambivalence	High	Desirable	Social Identity Cognitive Dissonance

# Conclusion

- A psychological understanding of Computer Network Defenders
- Change: what can change, what should change, what cannot change
- Studying the human experience of security is worthwhile

# Postscript

Practical challenges of  
conducting these studies

- Individual versus organization
  - Human experience
- Ethical considerations
  - Voluntary, confidential
- Social Constructionism
  - Insights based on participants



Harald Sohlberg, "Winter Night in the Mountains", 1914

# Questions

Further information:

V.M. Rooney & S.N. Foley, ["What You Can Change and What You Can't: Human Experience in Computer Network Defenses"](#), NordSec 2018: Secure IT Systems, Springer LNCS 11252.