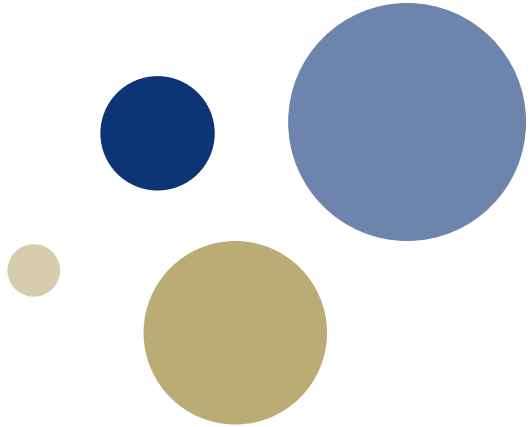
NTNU

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)

CCIS

NorCert Security Forum, Oslo, June 2019

COUNCIL on FOREIGN RELATIONS

Trending Yemen Brexit Refugees North Korea Rohi

from Net Politics *and* Digital and Cyberspace Policy Program

The Challenges Facing Computer Security Incident Response Teams

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?

...e fightback against security risks is very real -

...t Luke Jennings, head of research and

c|net 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.

Security

by Lance Whitney

13 March 2014 3:36 pm GMT

@lancewhit

Target

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

CSO FROM IDG

INSIDER Sign

IN DEPTH

Avoiding burnout: Ten tips for hackers working incident response

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

By Steve Ragan

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

SECURITY MANAGEMENT

FEBRUARY 2017

A PUBLICATION OF ASIS INTERNATIONAL

Issue & Beyond

× *Driverless Cars* Experts assess the risks.

× *Privacy* Government use of facial recognition.

×40 HEALTHCARE

×44 SUPPLY CHAIN

×56 TRADE SECRETS

×32 BEATING BURNOUT

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*]

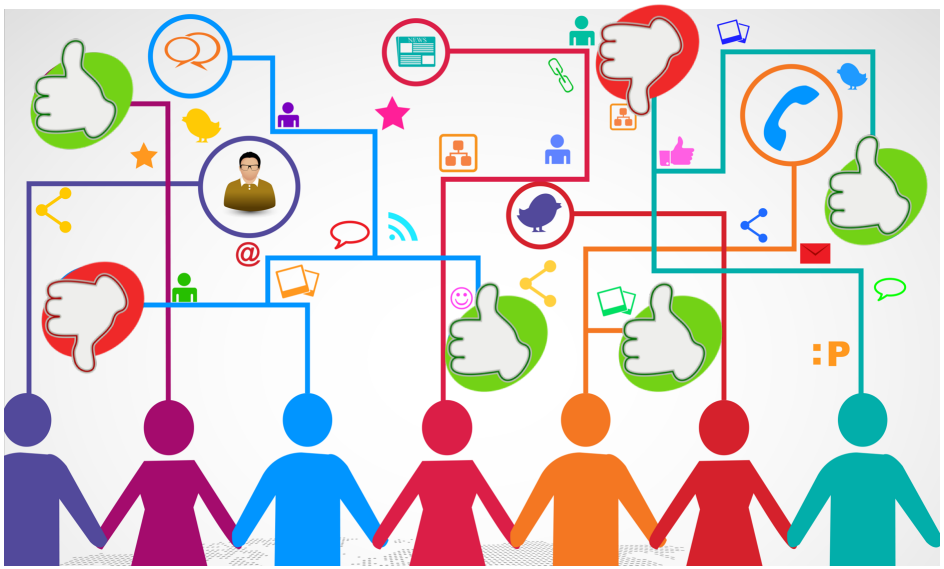
Conducting the study

A qualitative study of human experience in computer network defense

Communication within teams

An example of a result from the study

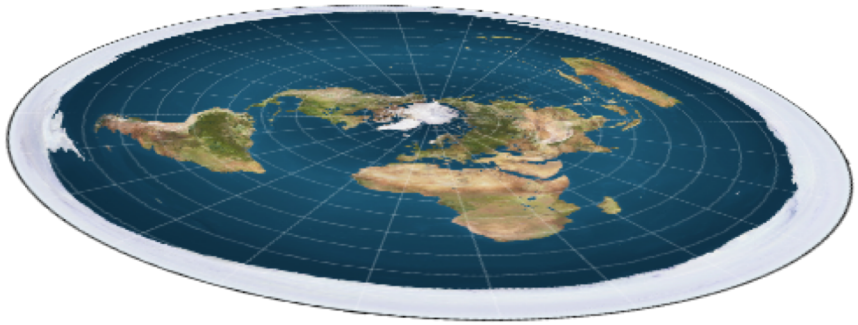
- Arguing & problem solving
  - Assumptions questioned
  - Certainty of one perspective not accepted
- Relational Dialectics in action
  - Dialogue as creative social process
  - Lessens consensus & blind spots
  - Helps build team cohesion
- A positive aspect of the work



How to reliably arrive at such conclusions?

Qualitative research methods

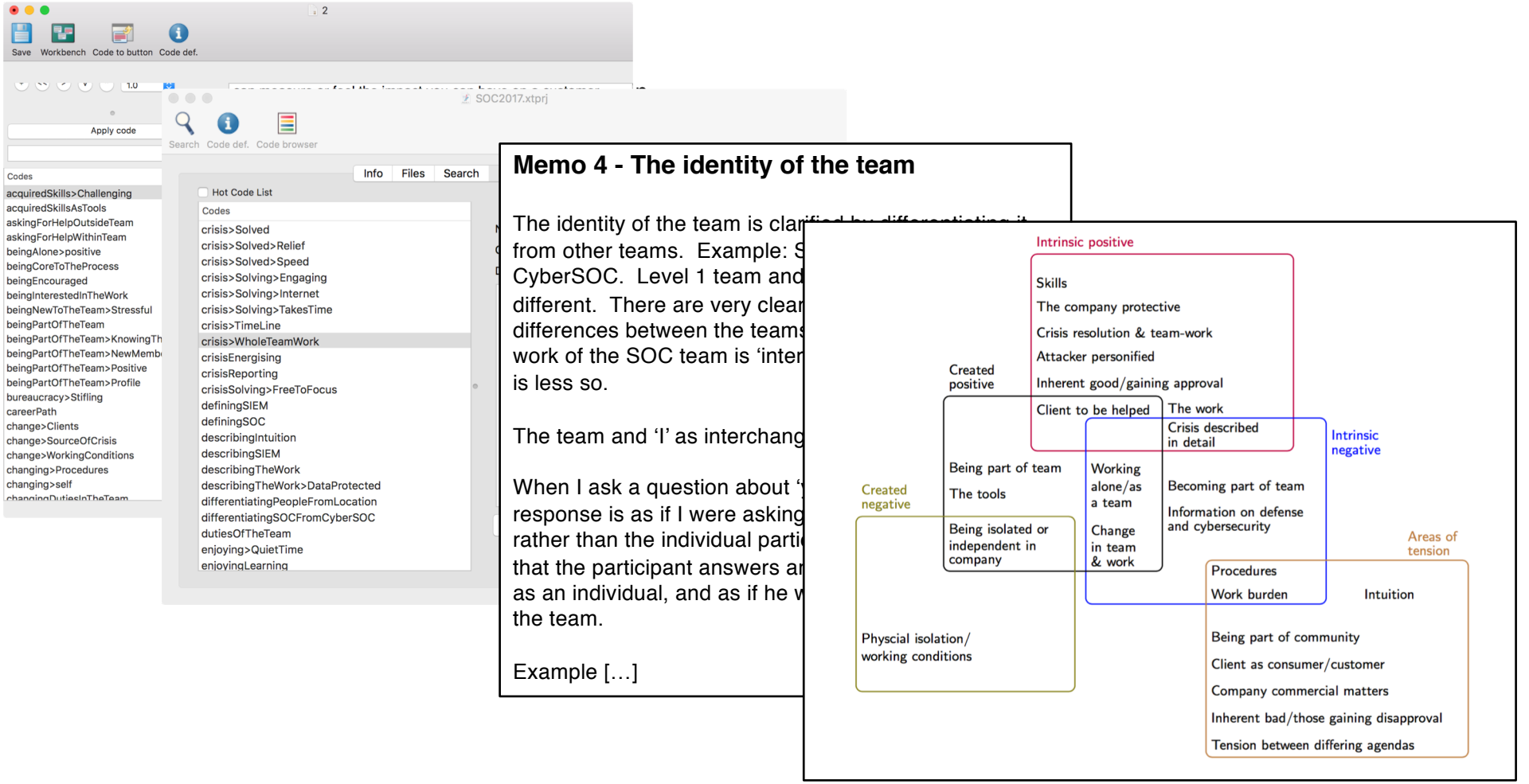
- Qualitative Research Methods
  - Techniques to uncover what is happening among people
- Study the psychology of the human in the loop
  - Understand what people do and why they do it
- Good for discovering unknown knowns



Qualitative Research methods

A way to undertand human experience

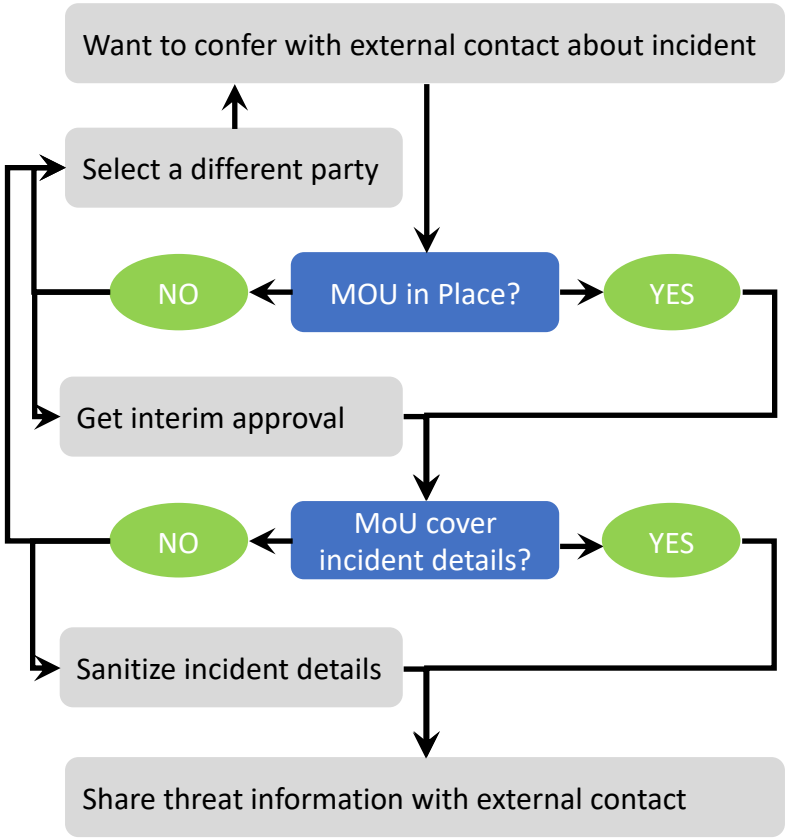
What is it like to do Grounded Theory?



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:

[…]

A: *they are r… …ve an issue, the quickest … …o is working on the issue, … …il, I'm really, it's sometim… …s also, so I just call then…*

Q: that's not … …s you send an email, an…

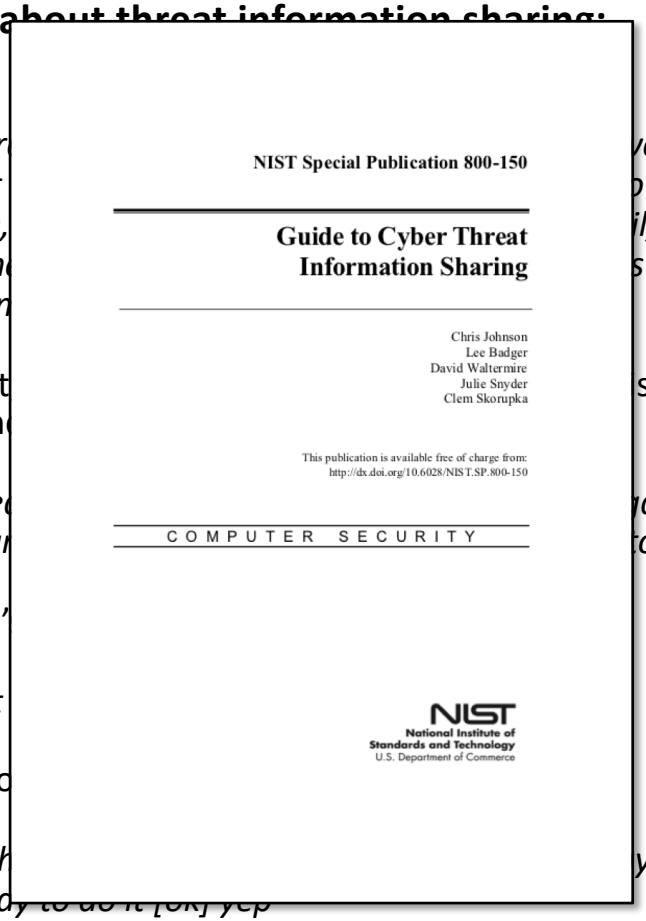
A: *the proce… …anisation] the procedu… …o call*

Q: ok, but it'…

A: *yeah, but…*

Q; they enco…

A: *most of th… …y to do it, there is a wa… …yep*



NIST Special Publication 800-150

Guide to Cyber Threat Information Sharing

Chris Johnson
Lee Badger
David Waltermire
Julie Snyder
Clem Skorupka

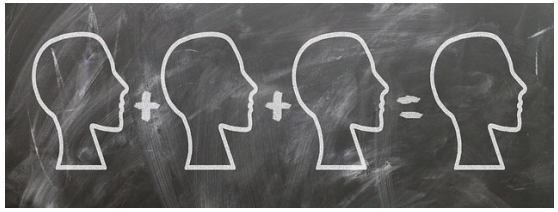
This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-150

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

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
- …

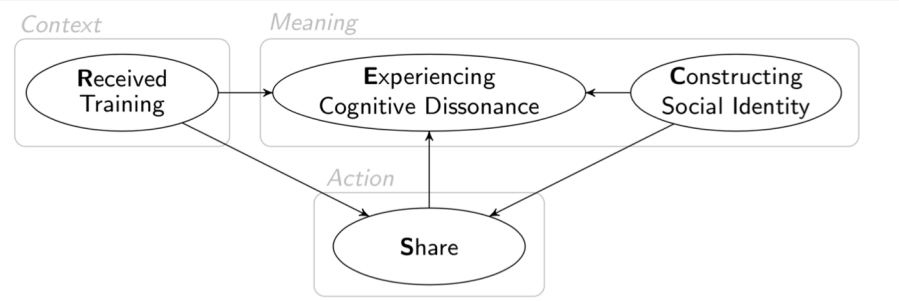
Member of a global community

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

Threat Information Sharing

Procedures as an area of tension

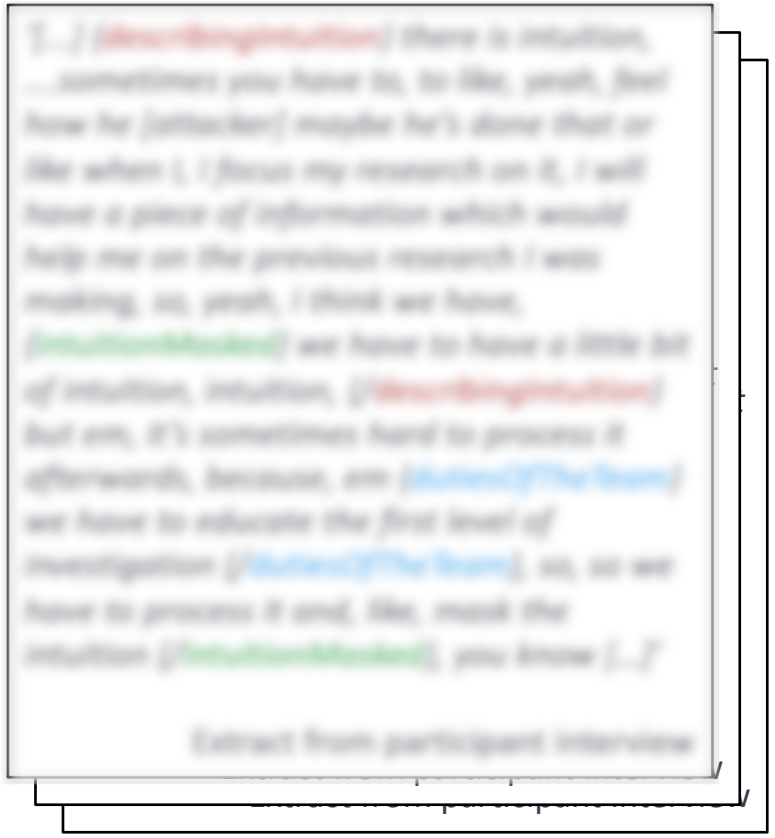
- Social Identity theory explains how and why identity is created
- Cognitive Dissonance occurs because multiple realities exist
- Relief from associated stress achieved through reconciling multiple realities



The use of intuition by defenders

Intuition as an area of tension

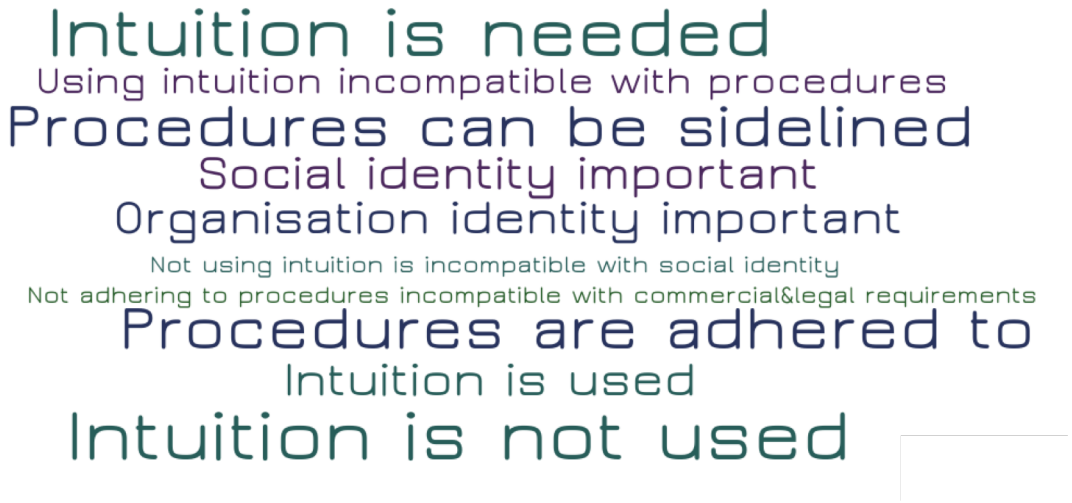
- Positive
  - Intuition is a useful resource based on experience
  - Can expedite a workaround to get system functioning
  - Can help build a solution during an attack
  - Is needed
- And negative….
  - Can be wrong
  - Even if not wrong, might need to be concealed
  - Problematic for retrospective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

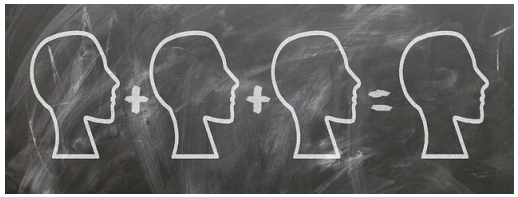


Understanding the ambivalence around intuition

Experience of defenders

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





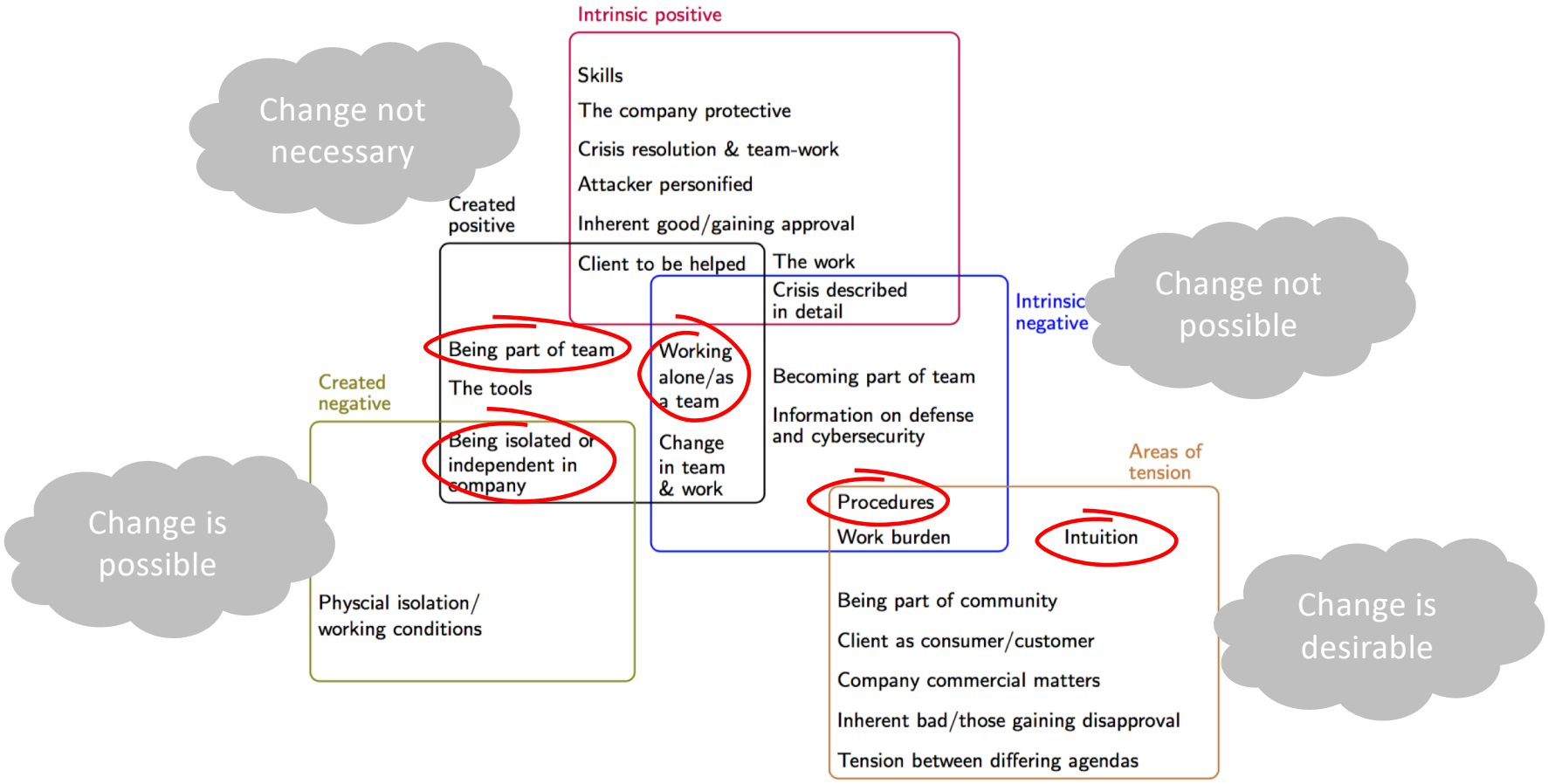
Understanding the ambivalence around intuition

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.