STSD-CSTE

A Socio-Technical Framework to Improve cyber security training: A Work in Progress

Grethe Østby
PhD researcher
NTNU

Lars Berg
Lawyer
Telenor

Mazaher Kianpour
PhD researcher
NTNU

Basel Katt
Associate professor
NTNU

Stewart James Kowalski
Professor
NTNU

Norwegian University of Science and Technology

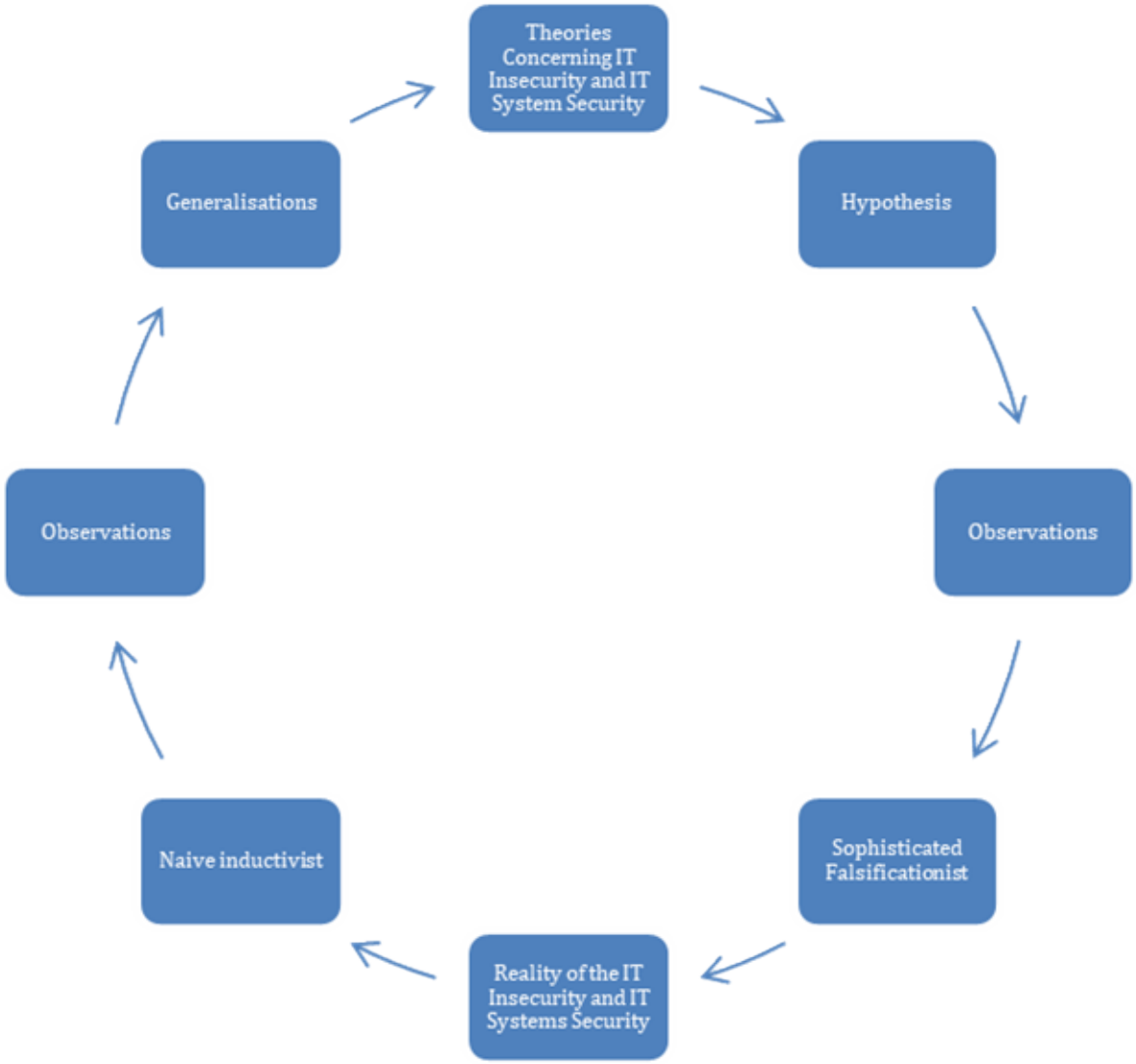
Problem: Lack of trained personel

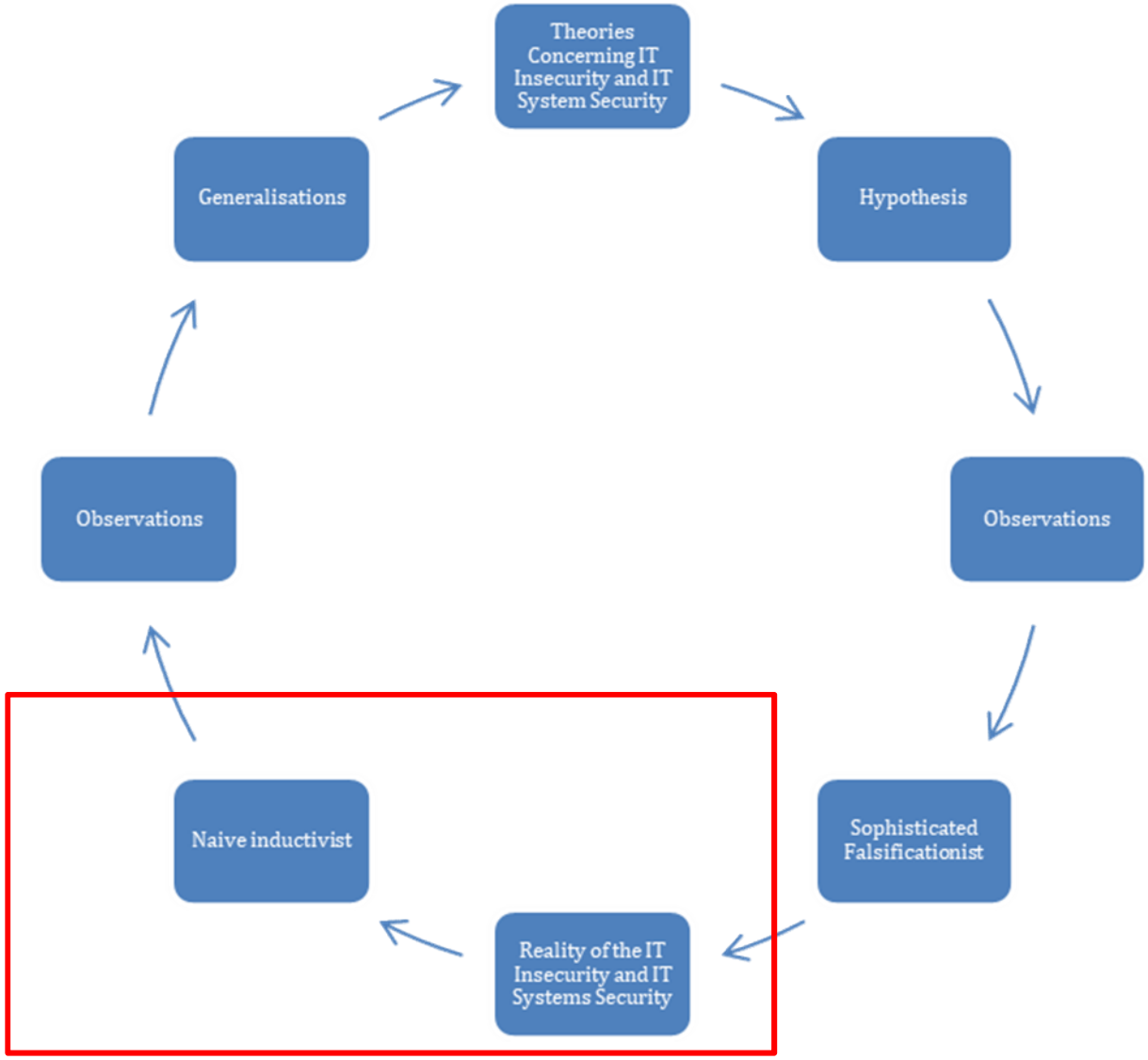
- According to the Cisco 2018 annual Cyber Security report, the lack of trained cyber security personnel is one of the key issue challenging security management (Cisco, 2018).

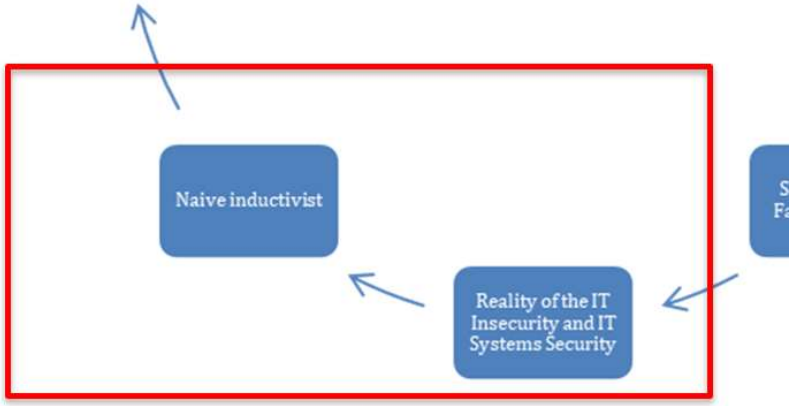
*“The focus is no longer prevention: you can’t stop attacks. It’s now about better **detection** and **readiness** for the inevitable in order to survive in today’s complex world.”*

www.ey.com

Naive inductivist Approach




Theories Concerning IT Insecurity and IT System Security
Hypothesis
Observations
Sophisticated Falsificationist
Reality of the IT Insecurity and IT Systems Security
Naive inductivist
Observations
Generalisations



"A characteristic of inductive arguments that distinguishes them from deductive ones is that, by proceeding as they do from statements about ***some*** *to statements about* ***all*** *events of a particular kind, they go beyond what is contained in the premises.»*

Alan Chalmers

Table 2. Three Kinds of Inference

	Abduction	Deduction	Induction
Premiss	Fact	Rule	Case
Premiss	Rule	Case	Fact
Outcome	Case	Fact	Rule

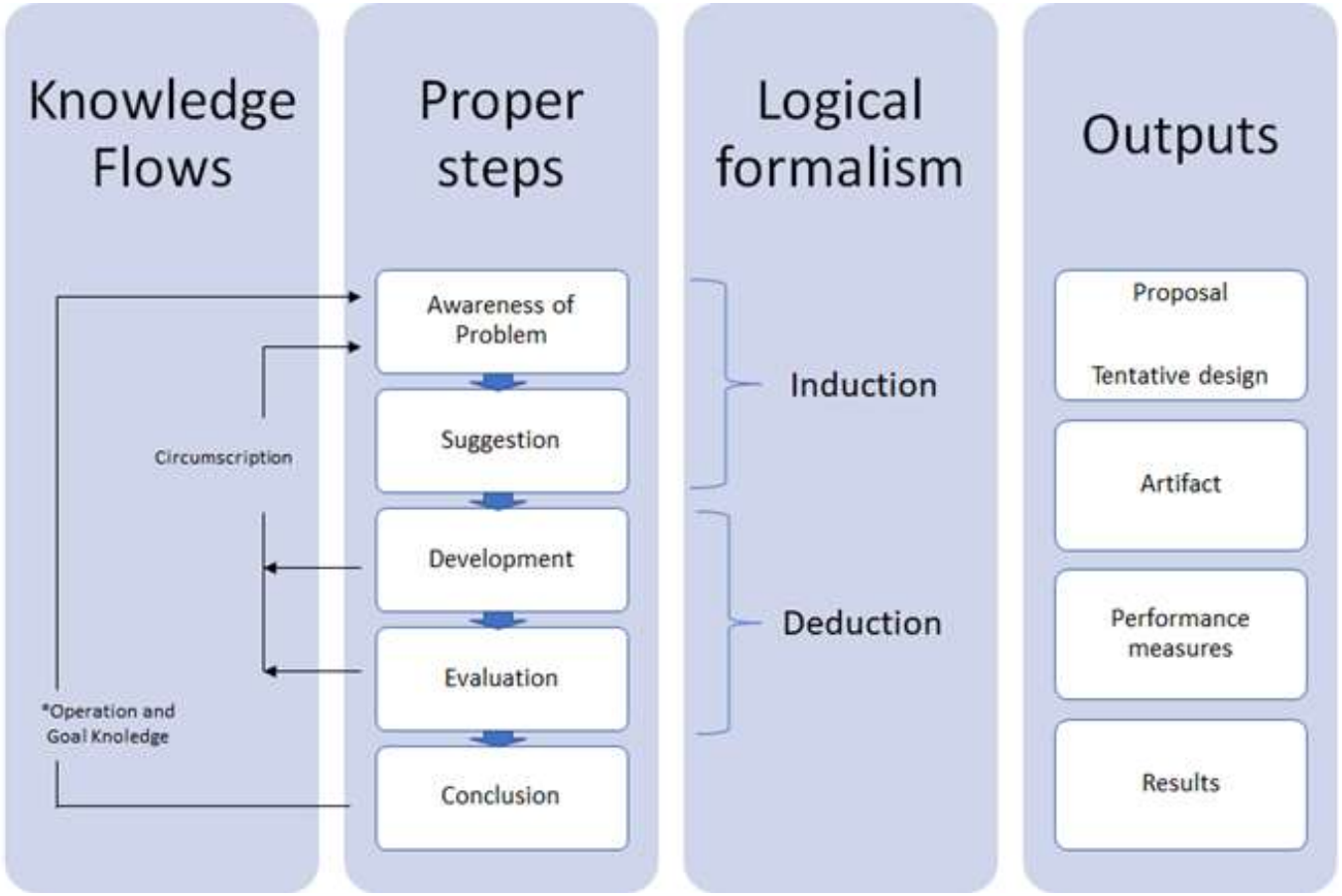
https://seansturm.wordpress.com/2011/05/23/deduction-induction-and-abduction/

Design Science Recearch

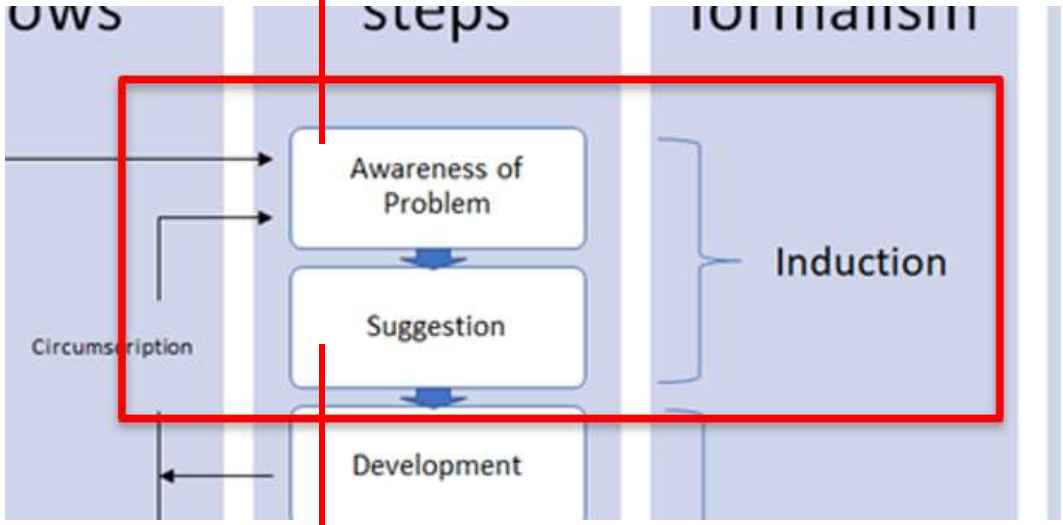
“Design science research in information systems (DSRIS) uses artifact design and construction (learning through building) to generate new knowledge and insights into a class of problems.”

Kuechler & Vaishnavi, 2012

Design Science Research – practical approach



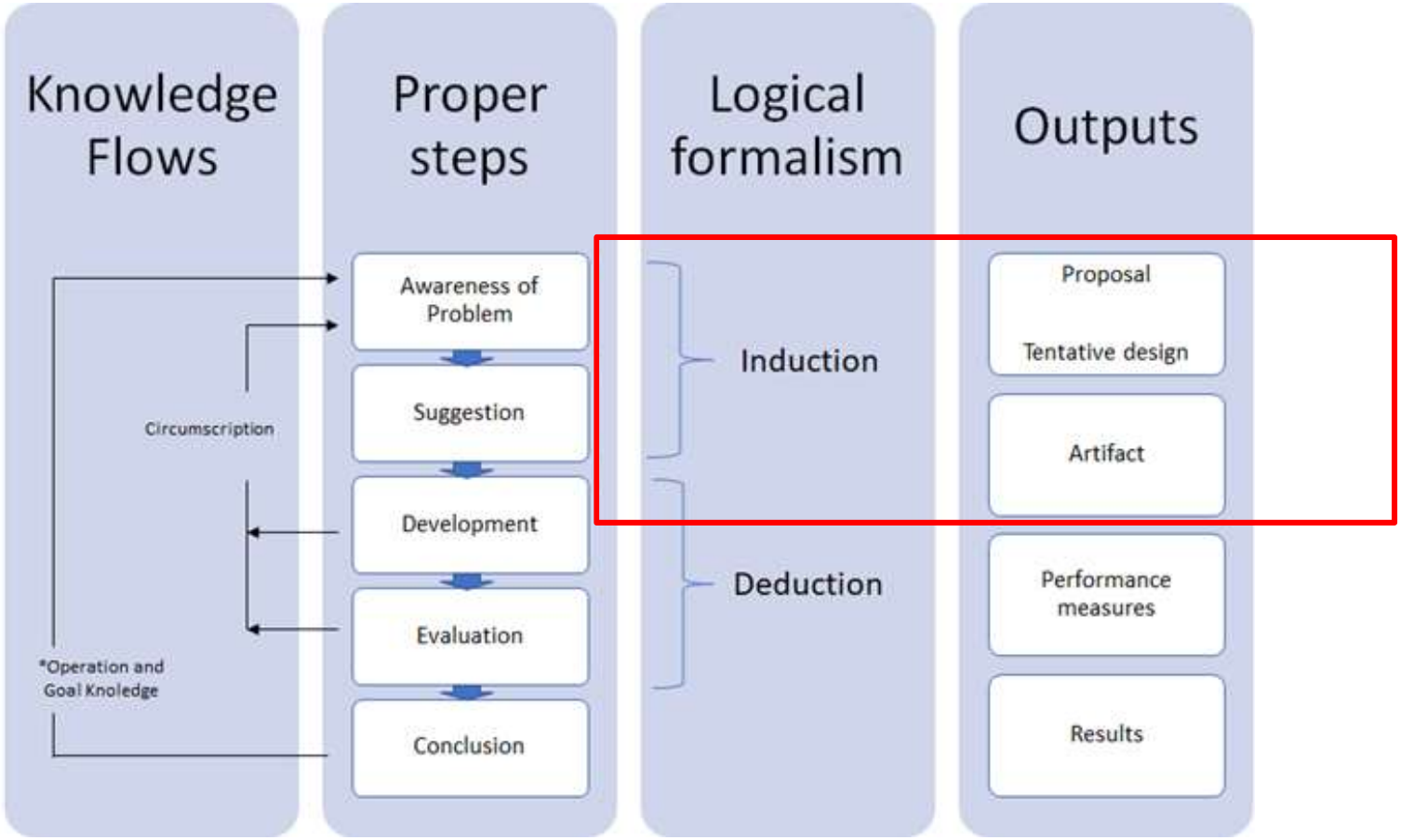
Karokola 2012, modified



Use Real Cases to Design Scenarios for Exercises

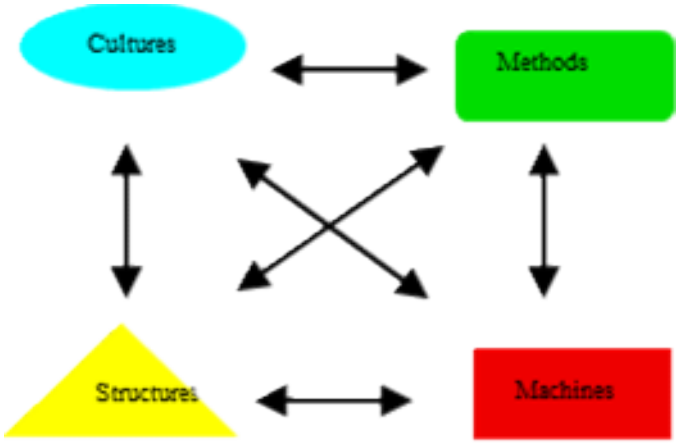
Use different ST-analyzis to approach different exercises

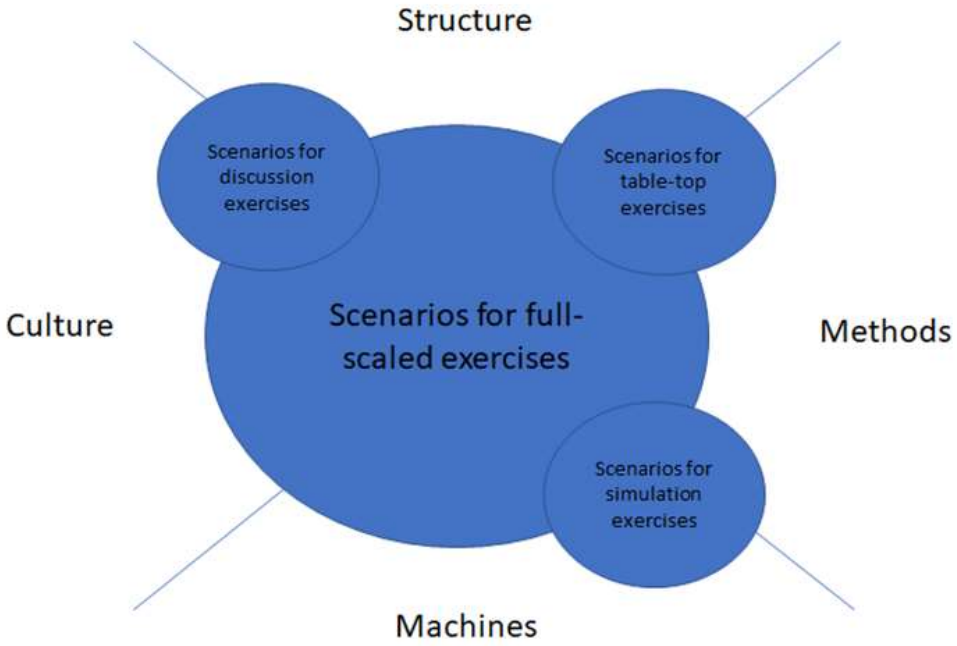
Practical testing NCR



Karokola 2012, modified

Socio-technical exercises to meet the demand of trained personel



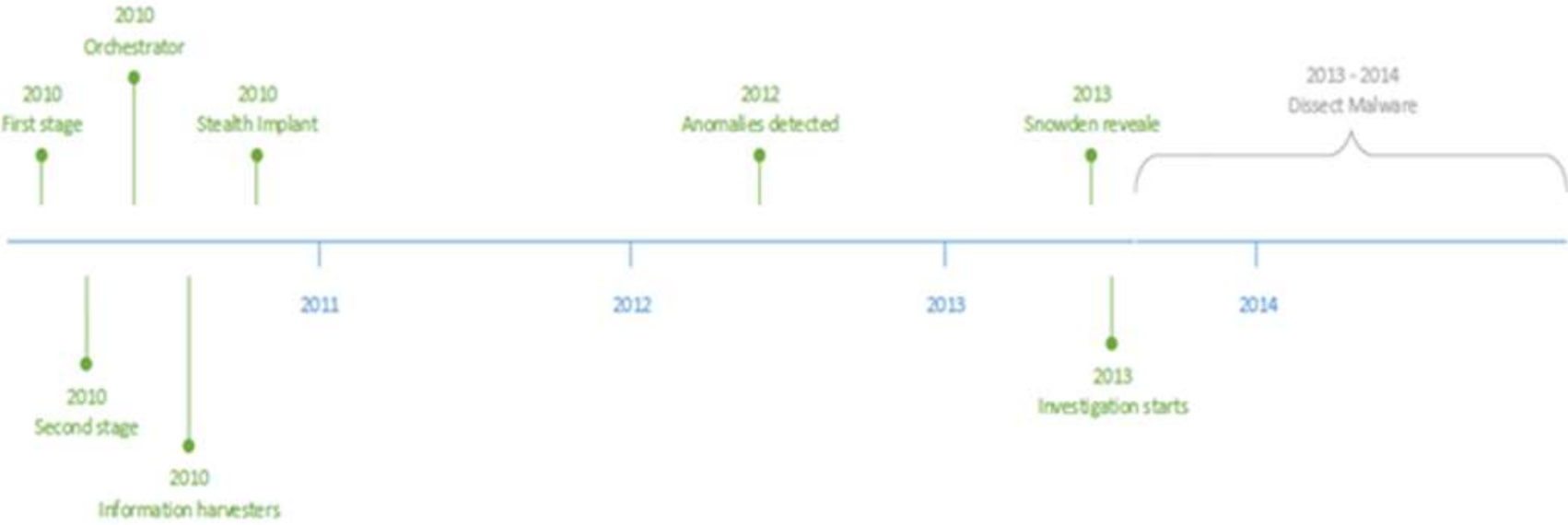


Case: Advanced Persistent Threat (APT)

"Advanced Persistent Threat (APT) is a term for a breed of insidious threats that use multiple attack techniques and vectors and that are conducted by stealth to avoid detection so that hackers can retain control over target systems unnoticed for long periods of time."

Colin Tankard, 2011

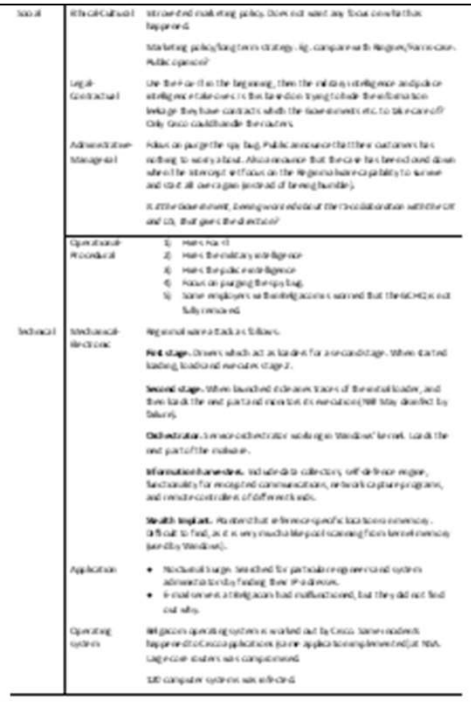
Operation Socialist – GCHQ infiltration on Belgacom



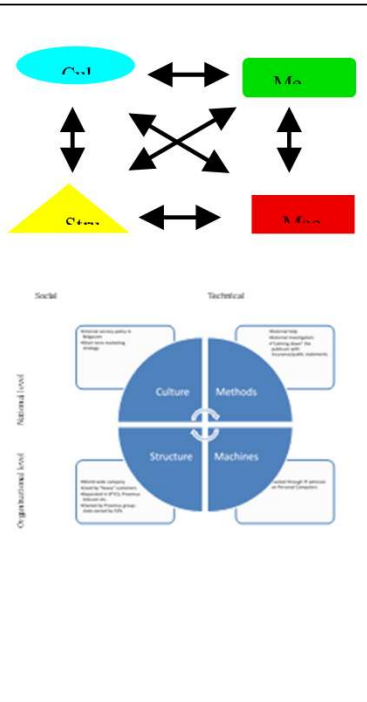
Root cause analyzis – models used

Withford

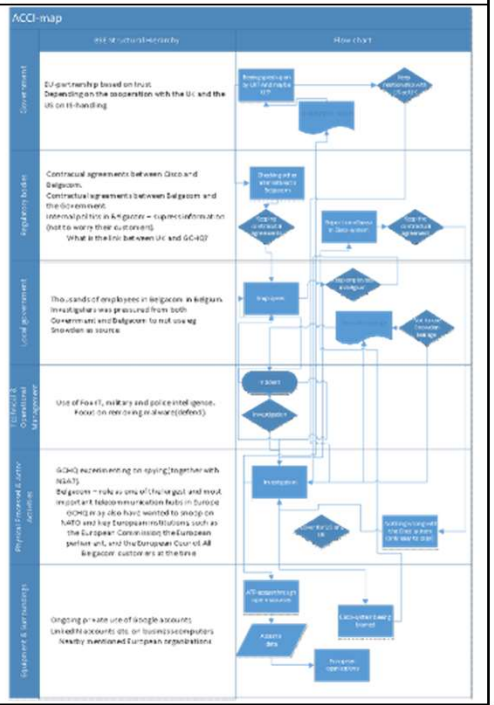
SBC-model



Kowalski

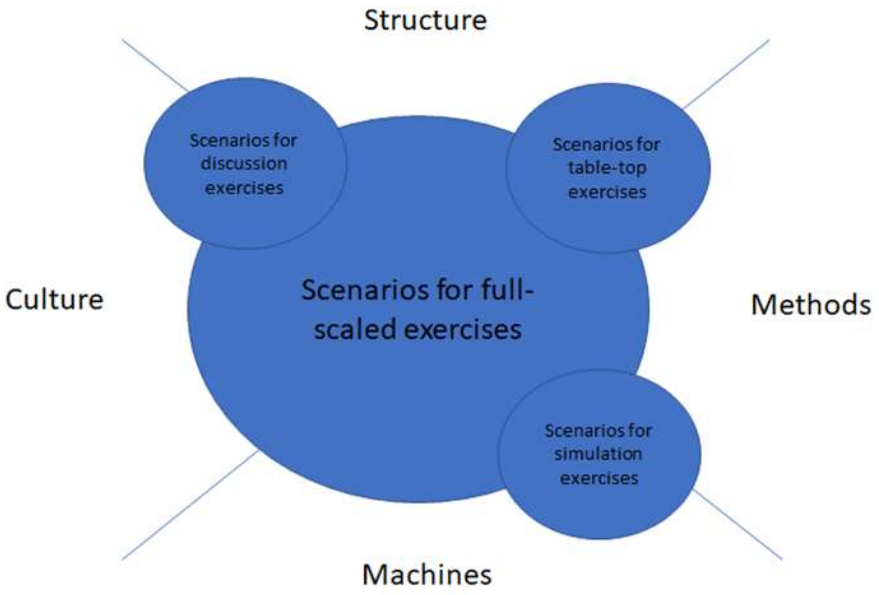


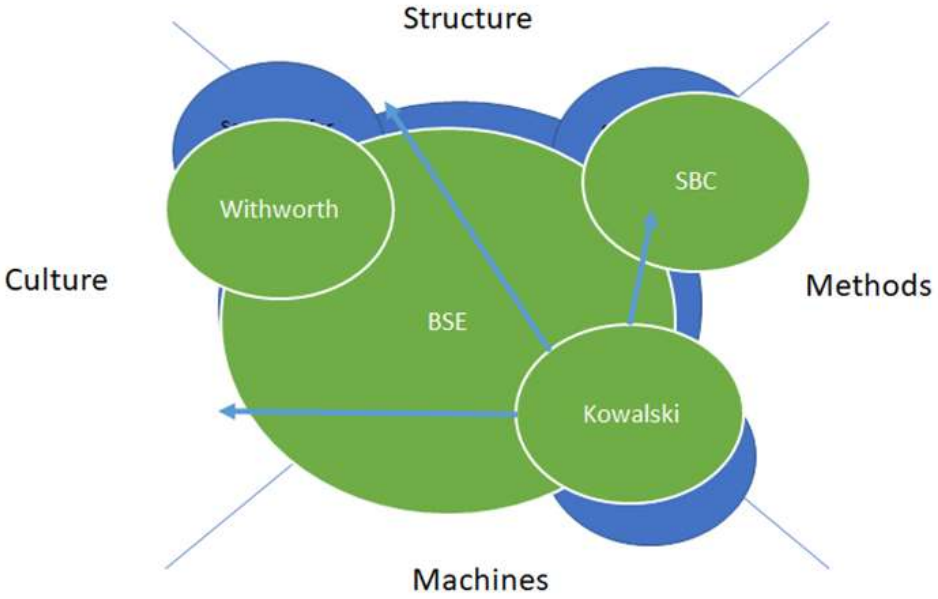
BSE-model



NTNU

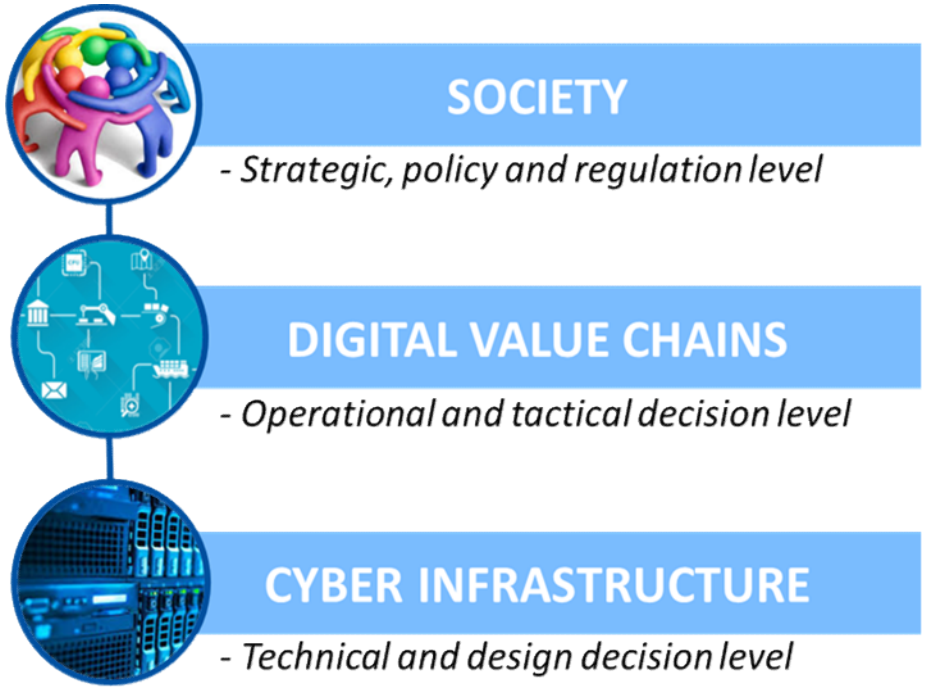
Socio-technical modelling ➡ exercises





Future work

- Test at Norwegian Cyber Range (NCR)



"NCR will be an arena where testing, training, and exercise will be used to expose individuals, public and private organizations and government agencies to simulate socio-technical cyber security events and situations in a realistic but safe environment."

Other future options

- Other socio-technical models?
- Ethical-Machine exercises?
- Capacity levels exercises – financial ?

“Almost every crisis contains within itself the seeds of success as well as the roots of failure.” Harvard Business Review

THANK YOU

Grethe Østby
grethe.ostby@ntnu.no