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

Grethe Østby1[0000-0002-7541-6233], Lars Berg2[0000-0001-8688-5759], Mazaher Kianpour1[0000-0003-2804-4630], Basel Katt 1[0000-0002-0177-9496], Stewart Kowalski1 [0000-0003-3601-8387],

[1] Norwegian University of Science and Technology, Postboks 191, 2802 Gjøvik
[2] Telenor Norge AS, Snarøyveien 30, 1331 Fornebu

lncs@springer.com

Abstract. In this paper we discuss a work in progress to create a socio-technical system design framework for cyber security training exercises (STSD-CSTE) to support the development of cyber security training in the Norwegian Cyber Range (NCR). The process to create the framework started by first performing a socio-technical systems root cause analysis of an Advanced Persistent Threat (APT) incident called “Operation Socialist”. Operation Socialist was the code name given by the British signals and communications agency Government Communications Headquarters (GCHQ) to an operation in which they successfully breached the infrastructure of the Belgian telecommunications company Belgacom (now Proximus Group) between 2010 and 2013. To extract relevant information from the case four socio-technical systems models were tested. The four models integrated into one framework were the Cassano-Piche Structural Hierarchy model, the “Security by Consensus” model, the Kowalski’s Socio-Technical systems dynamic model and the Withword’s 8 criterial model. After this framework has been reviewed by the socio-technical research community we plan to test the framework with exercises in the Norwegian Cyber Range environment. 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.

Keywords: Socio-technical models; Root cause analysis, Crisis-management, Cyber Security simulations, scenario exercises

1 Introduction

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). This lack of trained personnel is not a new problem. In 2017, 27 percent cited the lack of talent as a major obstacle, compared with 25 percent in 2016 and 22 percent in 2015. The gap between supply and demand for trained security personnel is growing.

In this paper, we outline our work in progress at the Norwegian Cyber Range to help fill this competence gap by using socio-technical models to construct training exercises and scenarios based on actual cyber incidents. In our work, we are attempting to combining socio-technical theory with didactic theory and crisis management training practices to cyber education and training.

The paper is structured as follows: After the introduction and background in section 1 and 2, in section 3 our research approach is discussed, together with our framework for building scenarios and exercises in cyber readiness based on real life incidents. In section 4, we review relevant literature. Then, in section 5 we present the case and one example of how we used socio-technical models to analyze the case, and in section 6 we exemplify the outcome of this application. In section 7 we end this paper by outline our prospects for further research.

2 Background

Several threat-actors are focusing on telecom services and infrastructure. According to Norwegian National Security Authority (NSM) in 2017 the NorCERT alarm on critical national infrastructure were triggered more than 22.000 times and more than 5.200 Norwegian entities were subject to advanced cyber-attacks (NSM, 2018). In the period May 2016 to May 2017 Telenor Norway managed 1800 cyber intrusion attempts in own and customers networks (Telenor, 2018). Private and public entities are facing new cyber threats day by day, and threat actors have different motivations. The most advanced cyber-attacks are often referred to as Advanced Persistent Threat (APT). Li defined APT as a cyber-attack launched by a group of sophisticated, determined, and coordinated attackers who systematically compromise the network of a specific target or entity for a prolonged period (Li, Lai, & Ddl, 2011). APTs have capacity, capability and motivation to run clandestine operations for months and years to achieve their objectives. Most organizations are not prepared to handle those kinds of advanced malicious cyber-attacks, and when it happens the repercussions are vast.

Detecting anomalies that occur only within individual variables is often trivial, while detecting correlation anomalies is much harder and is practically important in fault analysis of complicated dynamic systems (Idé, Lozano, Abe, & Liu, 2013). In a complex cyber-physical system, such as a smart grid, while some of the relationships between time series can be directly observed, other mutual dependencies are significantly complex to extract computationally. A typical cyber-physical system may include multiple process series with hundreds of mutual dependencies, where many of them are not directly observable (Rahman, Momtazpour, Zhang, Sharma, & Ramakrishnan, 2015).

To understand and manage cyber security situations, we suggest using socio-technical models to prepare for training and education based on real-life incidents. A sociotechnical system (STS) is the synergistic combination of humans, machines, environments, work activities and organizational structures and processes that comprise a given enterprise (Carayon et al., 2015). The goal of STS is a comprehension and accounting for the 'joint optimization of the social and technical systems', i.e. the different subsystems or different system components. Workers adapt to the sociotechnical system, but, in their turn, also serve to adapt the sociotechnical system itself.

3 Research Approach

In this paper, we approach the cyber security challenges using what can be referred to as a naive inductivist approach. The naïve inductivist approach starts by first observing a phenomenon and then generalizing the phenomenon which leads to theories that can be falsified or validated (Kowalski, 1994). This approach will use the methodology outline by design science research in information systems (DSRIS) (Kuechler & Vaishnavi, 2012). This methodology uses artifact design and construction (learning through building) to generate new knowledge and insights into a class of problems.

DSRIS requires three general activities: (1) construction of an artifact where construction is informed either by practice-based insight or theory, (2) the gathering of data on the functional performance of the artifact (i.e., evaluation), and (3) reflection on the construction process and on the implications the gathered data (from activity (2)) have for the artifact informing insight(s) or theory(s) (Kuechler & Vaishnavi, 2012).

How to work on these steps was presented in a thesis written by Karokola (Karokola, 2012). He visualized this approach as outlined in figure 1. As we are approaching our work in a naive inductivist approach, we modified the logical formalism in the model from abduction to induction.

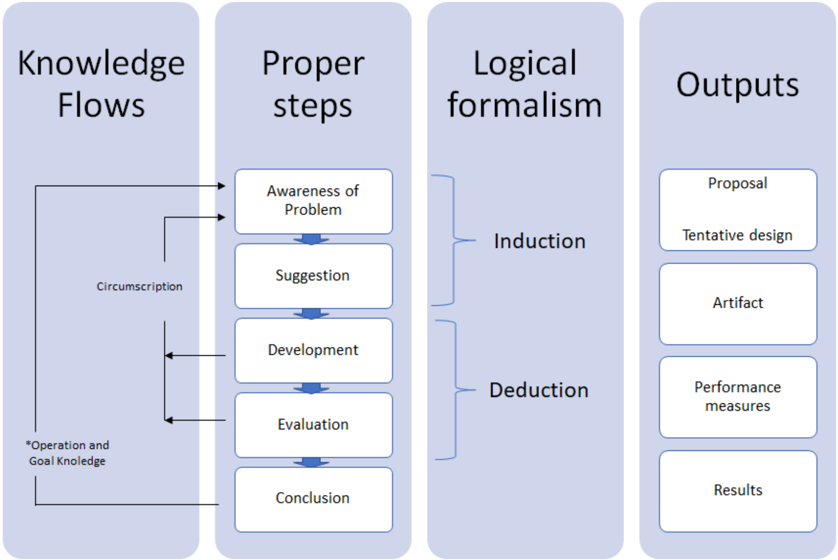


Figure 1, Design research methodology - modified

To propose an artifact in an inductive approach we started up by analyzing an actual cyber-incident to present the problem (first step in the 2nd column). For the next step in this work in progress paper we suggest a model based to deal with the problem in crisis management education in which different kind of exercises are needed to target different aspect in a socio-technical security system (second step in the 2nd column). The goal of the paper is to propose a tentative design (first step in the 4th column), in which we want to test when preparing for cyber exercises at the Norwegian Cyber Range.

3.1 Apply an Actual Incident Case study

The actual incident we chose for our first attempt to design a framework was the APT-attack “Operation Socialist” making international headlines in September 2013. Operation Socialist was the code name given by the British signals and communications agency Government Communications Headquarters (GCHQ) to an operation in which they successfully breached the infrastructure of the Belgian telecommunications company Belgacom (now Proximus Group) between 2010 and 2013.

We did a root cause analysis on this incident using four different socio-technical models. Those models were chosen based on the different approaches they have, to see if any or all of them could be relevant for making scenarios for exercises.

The responsible of the technical operations are often considered to be within the organization. However, most organizations today are complex and cannot perform all technical tasks by themselves. By entering into contracts and service level agreement of various sort, the companies have other people and organizations to run their technical operations and are therefore bounded by agreements and thereby regulations. Withford & Zaic describe four different system levels to analyze requirements for technical operation with WOSP (Web of System Performance) (Whitworth & Zaic, 2018): Hardware requirements, software requirements, human requirements and communal requirements. They define WOSP as a theoretical framework for the balanced design and evaluation of advanced information systems. The framework analyses performance via four fundamental system elements: Boundary, internal structure, effectors and receptors. As this is organizational issue, we considered this model relevant when designing scenarios for discussion exercises.

The four quadrants used in the proposed framework are modeled after the naive socio-technical system dynamic mental model proposed by Kowalski (Kowalski, 1994). Kowalski's mental model attempts to describe how systemic security weaknesses in socio-technical systems can be analogized as homeostatic imbalance. Homeostatic imbalance is the disability of the internal environment to remain in equilibrium in the face of internal, external and environmental changes (Pelletier, Guertin, Paige Pope, & Rocchi, 2016). Homeostatic imbalance is a concept that we suggest can also be used with scenario building to model the inability of an organization to face internal and external cyber threats.

The Security by Consensus model (SBC), is a model that attempt to capture the static and dynamic characteristics of ICT systems security (Kowalski, 1994). Moreover, the model sub-divides security measures into subclasses. The holistic approach required the issue of IT crime be examined, and the model was used to make computer abuse reports. Such reports are relevant on the strategic level and as a method to define action points in the organizations, and thereby likely to be relevant for table-top scenarios.

In the Norwegian Cyber Range project, we also plan to run full-scale exercises in Norway. Cassano-Piche et. al. Socio-technical systems analysis of the BSE Epidemic in the UK using the Rasmussen framework helped vertically integrate a socio-technical root cause analysis of Mad Cow Diseases across multiple levels and hierarchies of socio-technical system in the United Kingdom as a whole (Cassano-Piché, Vicente, & Jamieson, 2006). Consequently, we believe it can be used to design scenarios for large scale cyber security incidents and events in Norway.

Suggested modelling four quadrants used in the proposed framework are modeled after the naive socio-technical system dynamic mental model proposed d by Kowalski (Kowalski, 1994). As mentioned before, homeostatic imbalance concept can be used with scenario building. Therefore, the model suggested consists of the four socio-technical aspects suggested by Kowalski (Kowalski, 1994):

Table 1: Socio-technical aspects

Social	Structure
	Culture
Technical	Machine
	Methods

First, we tried to see where scenarios for **exercises** could fit our socio-technical model. There are several types of exercises, and in this paper, we have used the exercise-definitions outlined by the Norwegian Directorate for Civil Protection (DSB): discussion exercises, functional exercises, simulation exercises and full-scaled exercises. A *discussion exercise* is executed under different kind of names, for example, table-top, dilemma-exercises or seminar-exercises (DSB, 2016b, 2016c, 2016d, 2016a). In a discussion exercise, all participants gather in one room and all communication happens within this room. Inputs are given oral or on paper/screen/canvas sheets. All activity is to focus around discussion on concept and ideas and no concrete action or communication outside the exercise is needed. The participants are not to play or simulate, but to discuss specific and generic problems related to the scenario presented by the instructor. *Function exercises* is a collective name for exercises that test one or more functions within the organization (DSB, 2016b). It might be technique, organization or capabilities. Attending a function exercise, it is more about what to exercise than how the exercise is done. Function exercises are also referred to as procedure exercises. *A simulation exercise* consists of two elements: The attenders and the simulation counterparts (DSB, 2016d). A simulation exercise can be illustrated as if the game is running within a “closed bubble”, where the participants are staying in the inner bubble and the counterparts surrounding them. The participants will normally stay in their accustom premises, with their normally accessible tools and equipment. The simulation counterparts are staying in other premises, and control the game based on a planned scenario. The purpose is to convey a message with a certain effect to the participants. *A full-scale exercise* consists of all the elements in a simulation exercise, and functions, normally on a tactical level doing practical work (DSB, 2016a). A full-scale exercise is always real time. You use the same equipment as you normally have access to, and exercise in the places you normally are working.

For each kind of exercise, we need **relevant scenarios**. A scenario is a summary of the plot of a play, including information about its characters, scenes, or a predicted sequence of events (The free dictionary, by Farlex). The common way of making scenarios is to find out who is participating in the exercise and make the scenario relevant for the participants. For example, in 2017, a group from NTNU, CCIS, The Norwegian Cyber Defence and the Norwegian Civil Defence made a table-top cyber exercise for the Oppland County Office management group and for the county readiness council. We made the scenario based on the participants and their responsibility. The scenario was based on what can happen in the society more than what has happened, and it was all made up by ideas. As a reflection after the exercise we asked ourselves if there are relevant theories to approach these kinds of scenarios in a better way, and we could not find any relevant theories on this specific matter.

Large companies have a similar approach for creating scenarios to run exercises. Telenor is running annual full-scale cyber exercises including participants and observers from the Norwegian Armed Forces, The Norwegian Police, The Norwegian National Security Authority and other invited participants. The scenarios are meant to reflect true-to-life cyber incidents the organization faces and put the participants to the test. Experiences and lessons learned build operational, tactical and strategic competence and improve the participant's organizations in facing and managing cyber security incidents. Telenor has similar idea-based approach for making scenarios for exercises.

By considering either Structure, Methods, Machines or Ethical/Legal i.e. culture in the scenario for exercise build, we can determine where different exercises would be useful. Moreover, by having performed a root cause analysis and thus determined the underlying "real", that is major and sine qua non - reasons for the cyber-attack, building an appropriate scenario based on this could prove more accurate, give higher learning quality/effect and more cost effective.

To exemplify this approach, we have discussed the NATO exercise Trident juncture executed in and hosted by Norway in 2018. The main scenario was made for the full-scale exercise within a 3-week timeline. The strategic part of the exercise was kept outside the full-scale exercise and started instead at the end of the full-scale exercise timeline. The scenario for the strategic part of the exercise was in this case based only on structure and methods. The scenario for the NATO exercise would in this case be placed both in an overall context in the model, but the strategic part of the exercise would be placed in the upper right part of the model.

When planning for the annual exercise at the Oppland county readiness council in 2017, the exercise's theme was a cyber-attack against municipalities ICT-systems (Oppland Arbeiderblad, 2017). The county readiness council was given step-by-step information about the scenario and had round table discussions based on those inputs. The discussions were based on the structure in the organizations, laws and regulations and ethical issues (amongst others) – a typical discussion exercise that would be placed in the upper left corner in our model.

When testing systems such as fire alarm systems, it requires a certain methodology and actual use of machines. Fire-alarm exercises is typical functional exercises and you will be placed in the lower right corner in our model. Other known exercises that is based on methodology and machines is cyber mega games, better described as simulation games.

When analyzing the outlined DSB's definitions of exercises, we found that there is not any definition on cultural and machine exercises (lower left corner of our model). However, there are examples of real-life incidents which has been used in teaching strategic and ethical exercises, such as the Therax-25 case (Computing Cases, 1983). We consider this as an area of which can be developed better in combining exercise-definitions and scenarios and have presented this in our future research chapter.

Our scenario for exercise perception is shown in figure 2.

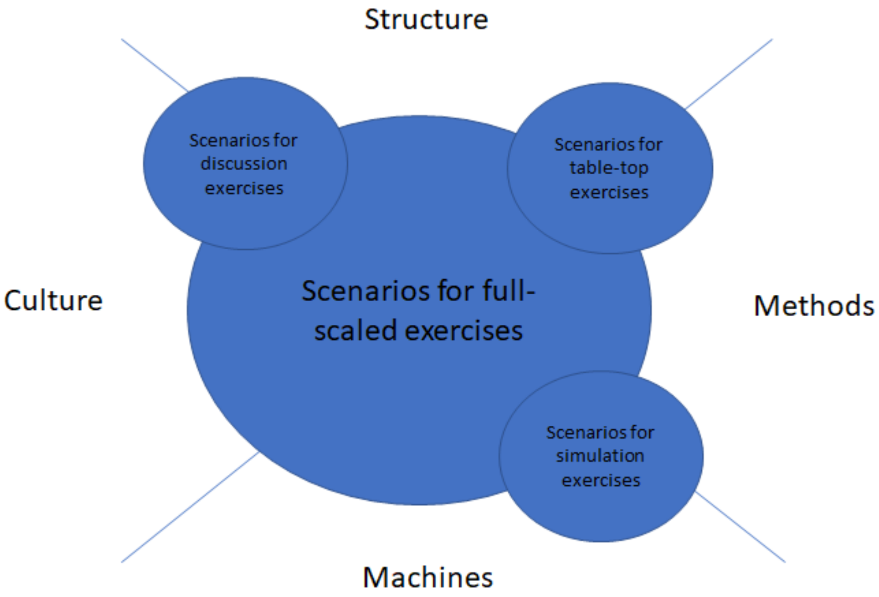

Structure
Scenarios for discussion exercises
Scenarios for table-top exercises
Culture
Scenarios for full-scaled exercises
Methods
Scenarios for simulation exercises
Machines

Figure 2: Placing different scenarios for exercises in a social-technical context

4 Relevant literature

Today we witness rapid developments of APT tools and systems. Future scenarios include attack vectors orchestrating sets of APT tools in mixed interaction with networks of military units and civilian infrastructures. Carlsson & Gustavsson state that we must prepare ourselves to cope with these threats through awareness and education (Carlsson & Gustavsson, 2018).

Most organizations are not prepared to handle the vast implications of these crises. A challenge in crises is to transfer the accumulated knowledge flowing from concrete experiences, well-documented by crisis management researchers, to learning models in which organizational actors will be **actively engaged**. One of the avenues to better integrate this learning can be found in organizational development approaches (Lalonde, 2007).

Since the start of the 1980s, the field of crisis management has been characterized by two main trends: planning in crisis management and the analysis of organizational contingencies during a crisis (Lalonde, 2007). Based on vast relevant research on crisis management, Lalonde created a synthesis of results from academic research and classified the results with reference to:

- types or contents of lessons, returning to the question *what have we learned?*, whether new information, the consolidation of existing organizational routines stemming either from crisis plans or routines learned within the organization, or tacit knowledge coming from socialization in a trade or profession or from an organizational cultural environment, etc.;

- learning conditions, returning to the question how or in what conditions *did we learn?*, including experimentation in real time in "real" situations, simulations of the experience, training, confrontation and sharing of experiences, etc.;
- the potential to transfer knowledge within the organization, aiming to respond to the question how can we incorporate this knowledge in an organizational learning model?

In our ongoing research, we use an actual APT-attack to extract the consequences from the attack and figure out what we can learn from such attacks, and how to implement lessons learned in exercises enable also other organizations learn from it.

Scenarios are tools for improving the decision-making process on a background of possible future environments. The scenarios should not be treated as predictions capable of influencing the future nor science fiction stories prepared merely to titillate the imagination (Schoemaker & van der Heijden, 2008). In a study to describe how scenarios used in an environmental science program function in terms of the type of questions they evoked, the results gave that questioning in different ways all bring learning to participants (Dahlgren & Öberg, 2001).

5 Case background and example

5.1 Operation Socialist

Belgacom operates a substantial number of data links internationally and it serves millions of people across Europe as well as officials from top institutions including the European Commission, the European Parliament, the European Council and the NATO HQ Europe. When Belgacom's internal security team began to suspect that their system was infected with a virus, they hired in outside experts, and after a while the Belgian military intelligence to handle the situation (Marquis-Boire, Guarnieri, & Gallagher, 2014). Some anomalies where detected already in 2012, but Belgacom's security team was unable to identify the cause.

The operation's existence were revealed in documents leaked by the former National Security Agency contractor Edward Snowden in 2013. The malware disguised as legitimate Microsoft software, where identified as the source of the problems. The leakage stated that it was the Government Communications Headquarters (GCHQ) who had infiltrated Belgacom's systems. GCHQ is the British intelligence and security organization responsible for providing signals intelligence (SIGINT) and information assurance to the government and armed forces of the United Kingdom. According to the leaked documents, from Snowden, GCHQ had probed Belgacom's infrastructure for years. Additionally, the documents suggested that Operation Socialist had been recognized by the head of the GCHQ's Network Analysis Centre as a success. Snowden subsequently described Operation Socialist as the "first documented example to show one EU member state executing a cyber-attack on another…" (Marquis-Boire et al., 2014).

According to the leakage, GCHQ had been able to get access to vital data within the mentioned organizations. This led to both political and organizational difficulties for multiple stakeholders.

GCHQ had allegedly used Quantum Inserts technology to target Belgacom and GPRS roaming exchange (GRX) providers like the Comfone, Syniverse, and Starhome. Quantum Insert is the process of injecting TCP sessions into a TPC stream and sending the victim in the wrong direction towards a malicious website that infects their computers with malware at lightning pace (Marquis-Boire et al., 2014). The combination of an IP address and a port is strictly known as an endpoint and is sometimes called a socket. A TCP connection is defined by two endpoints a.k.a. sockets. The Quantum Insert attack started by finding that way into the Belgacom systems by targeting their engineers use of passwords on LinkedIn (Marquis-Boire et al., 2014), the APT kill-chain was as follows:

- Reconnaissance: The APT choose targets of interest and surveil for a period their use of services on the internet, i.e. Belgacom system administrators active on LinkedIn.
- First stage: Drivers which act as loaders for a second stage. When started loading, loads and executes stage 2.
- Second stage: When launched it cleans traces of the initial loader, and then loads the next part and monitors its execution (NB! May disinfect by failure).
- Orchestrator: Service orchestrator working in Windows' kernel. Loads the next part of the malware.
- Information harvesters: Include data collectors, self-defense engine, functionality for encrypted communications, network capture programs, and remote controllers of different kinds.
- Stealth implants: *Pointers* that reference specific locations in memory. Difficult to find, as it is very much alike pool scanning from kernel memory (used by Windows).

Technically Quantum Inserts are categorized as “man-on-the-side attacks” which is a subcategory to “waterhole attacks”. As such APT-attacks are very difficult to discover, the exact time of when the stealth implants were in place is uncertain, but the investigators suggested an approximately startup in 2010. The Intercept summered up the story timewise in 2018 (Gallagher, 2018). The timeline of the incident is shown in figure 3.

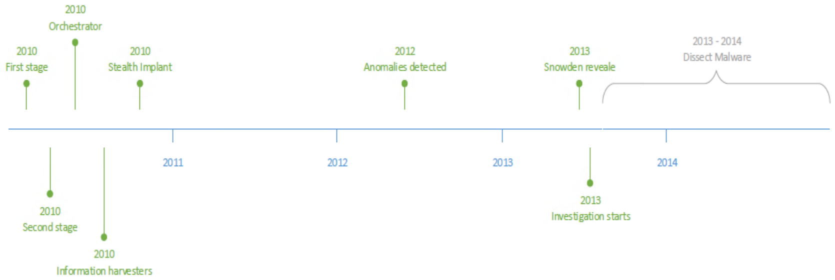
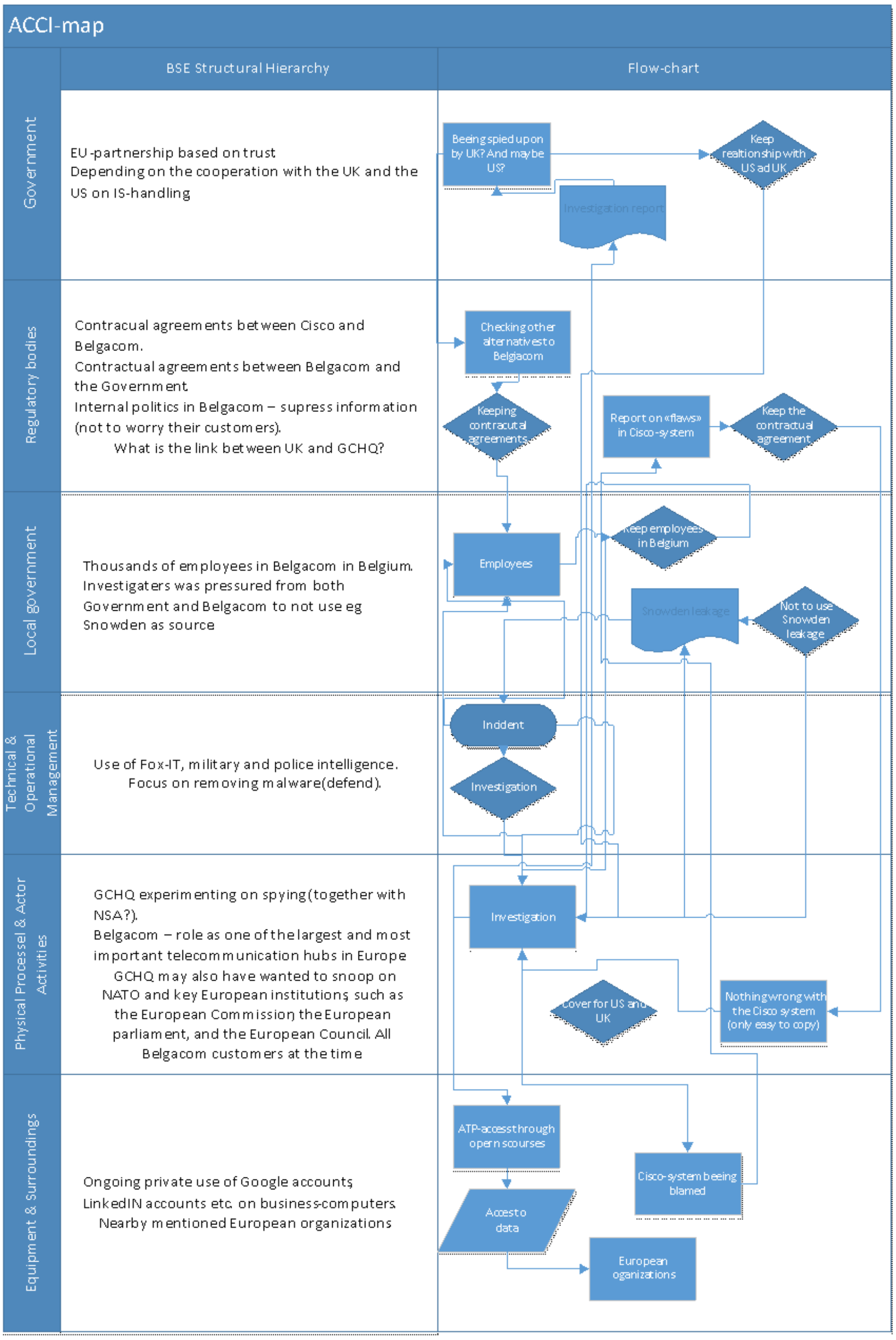


Figure 3: Quantum Insert escalation and period of detection, investigation and dissection

5.2 Example

One of the models we used for analyzing the case was the BSE Structural Hierarchy model based on Rasmussen structural hierarchy model (Cassano-Piché et al., 2006). In this paper it is presented as an acci-map. An acci-map is a systems-based technique for accident analysis, specifically for analyzing the causes of accidents and incidents that occur in complex Socio-technical systems. In figure 4 we present the different layers in the society in the left column, then some analyzed impacts in the second column and a flow-chart to show how events relate to each other in the right column.

We analyzed what impact the incident had on the different layers and moreover used the flowchart to show how decisions were made and had impact on other layers - both in Belgacom and in other societal organizations.



ACCI-map

	BSE Structural Hierarchy
Government	EU-partnership based on trust Depending on the cooperation with the UK and the US on IS-handling
Regulatory bodies	Contracual agreements between Cisco and Belgacom. Contractual agreements between Belgacom and the Government. Internal politics in Belgacom – supress information (not to worry their customers). What is the link between UK and GCHQ?
Local government	Thousands of employees in Belgacom in Belgium. Investigaters was pressured from both Government and Belgacom to not use eg Snowden as source
Technical & Operational Management	Use of Fox-IT, military and police intelligence. Focus on removing malware(defend).
Physical Processel & Actor Activities	GCHQ experimenting on spying (together with NSA?). Belgacom – role as one of the largest and most important telecommunication hubs in Europe GCHQ may also have wanted to snoop on NATO and key European institutions, such as the European Commission, the European parliament, and the European Council. All Belgacom customers at the time
Equipment & Surroundings	Ongoing private use of Google accounts, LinkedIN accounts etc. on business-computers. Nearby mentioned European organizations

Flow-chart
Beeing spied upon by UK? And maybe US?
Keep realtionship with US ad UK
Investigation report
Checking other alternativesto Belgiacom
Keeping contracutal agreements
Report on «flaws» in Cisco-system
Keep the contractual agreement
Employees
Keep employees in Belgium
Snowden leakage
Not to use Snowden leakage
Inddent
Investigation
Investigation
Cover for US and UK
Nothing wrong with the Cisco system (only easy to copy)
ATP-acessthrough opern scourses
Cisco-system beeing blamed
Accesto data
European oganizations

Figure 4: BSE Structural Hierarchy model analysis of Operation socialist

6 Current Conclusion

The socio-technical models appear useful in understanding and defining training scenarios as it gives us a good indication on both social and technical challenges from real life cases.

The **SBC Model** appears to be a good model for making scenarios for table top exercise regarding the Belgacom incident, since it helps to indicate were the organization is vulnerable from a strategic level within the organization. By using the SBC model, we can make exercise that show the relationship between different both technical and social functions within (in this case) Belgacom, and a scenario could be made to support this.

For **Kowalski's socio-technical model** we choose organizational and national level, but we think that for writing scenarios, we could have chosen both local government and other third-parties. We figured this model would be excellent for making scenarios for discussion exercises and table-top exercises. This model gives the instructors/trainers possibility to both focus and train the company and a third party. The idea of the model is though in a continual state of surface flux, it is also striving to reach a state of equilibrium or homeostasis (Kowalski, 1994). In our incident, this means that when we find the weakest link in the model, which might be the place to start modeling a scenario for exercise, by using this model, you may end up with different kind of scenarios and exercises.

The **BSE-model** with the flow-chart shows how well aligned the different events are between different levels in this hierarchy, and we also see a scenario involving all these levels. This model shows that all levels are connected and gives us the reason to believe that this model can be used for making scenarios for full-scaled exercises, but also be toned down and used for all other types of exercises.

When we analyzed the **Withword 8 criteria-model** we found that this is related to organizational level in first, and as the WOSP are made to follow up on strategic decisions, this model can be used for discussions exercises. This assumes Information Security as part of the WOSP's.

Below is a table outline the four different models and the type of exercise the actual incident can be applied.

Table 2: Using socio-technical models and real incident to build relevant scenarios for exercises

Socio-technical model	Withford	SBC-model	Kowalski	BSE-model
Scenario	Operation Socialist	Operation Socialist	Operation Socialist	Operation Socialist
Appropriate for exercise	Discussion exercise	Table-top exercise	Discussion exercise Table-top exercise Simulation exercise	Full-scale exercise

In figure 5 we map the different socio-technical models together with the scenarios for exercises mapped in figure 2, to attempt to visualize and compare. We may conclude that by changing the models in one or another direction, they will be more suitable for the different kind of exercises. For example, the Kowalski model can float across the diagram based on the situation in the organization, and by that approach decide what exercise to consider.

We are proposing to name this comparing model a socio-technical system design framework for cyber security training exercises (STSD-CSTE).

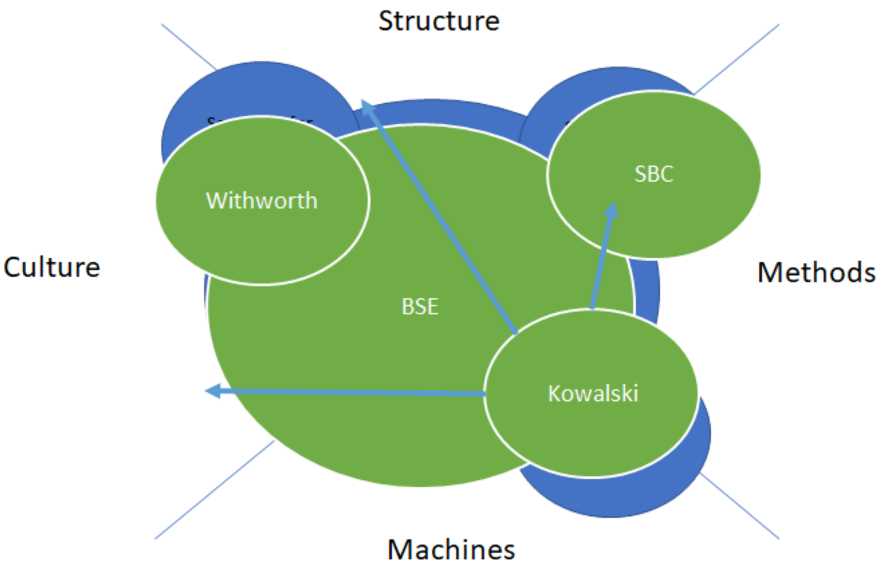


Figure 5: Framework for building relevant scenarios for exercises, based on socio-technical models to analyze real life incidents (STSD-CSTE)

7 Future Directions

Social-technical models enables us to introduce more holistic and near-to-life elements needed to be factored in designing scenarios. We need to verify and validate the findings we already have made, and to enhance and improve the STSD-CSTE model proposed. To validate the framework, we plan to test it when setting up exercises in the NCR environment. NCR will be an arena where testing, training, and exercise are tools to expose people, businesses, and units to realistic events and situations in a realistic but safe environment. The arena ensures efficient transfer of knowledge and building of real-world competence, that links together the strategic, operational, tactical and technical levels of decision making, by simulating the impacts of cyber security events on the levels of society, digital value chains and cyber infrastructure without harming the entities involved and their critical infrastructure.

In this paper we describe a root-cause analysis by using only four socio-technical models. In future work we will do a systematic-literature review of socio-technical modeling in general and select the models that best meets when designing exercise and scenario in the Norwegian Cyber Range.

To ensure the best possible effect in the cyber-range arena in Norway, current existing information systems tools used in the community will be, for example, ISCMS (information security crises management systems) systems, and facilitate accurate comprehension of scenarios fitted the different systems. Additionally, there will be need of preparedness learning based on real life incidents.

When analyzing the outlined DSB's definitions of exercises, we found that there is no clear definition on cultural and machine exercises (lower left corner of our model). However, as mentioned there are examples of real-life incidents which has been used in teaching strategic and ethical exercises. We consider this as an area of which can be developed better in combining exercise-definitions and scenarios and have a work in progress in this matter.

As illustrated in figure 6, the more complex and capabilities involved in the training exercise, the more effort and resources must be put into planning.

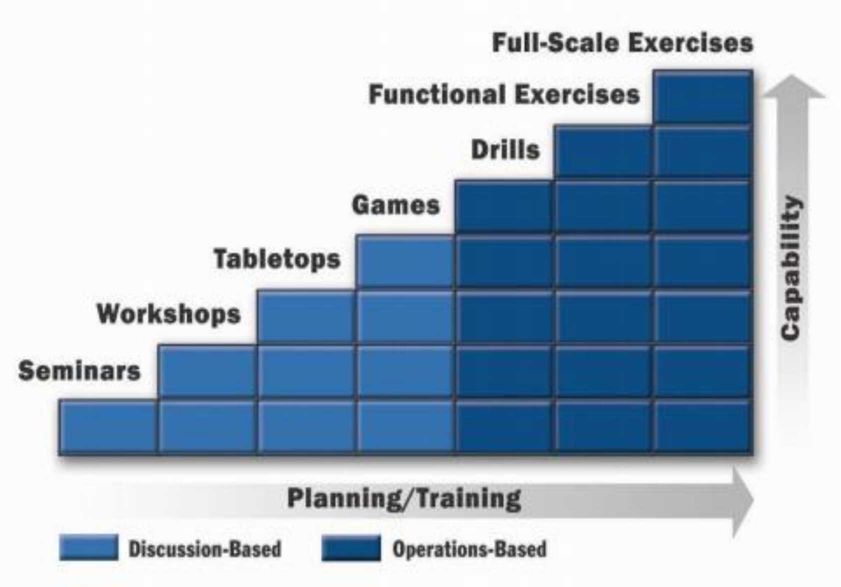


Figure 6: Exercise Types and Capacity Levels from (HSEEP, 2006)

Figure 6 also illustrates another adjacent topic; cost. A full-scale exercise requires far more resources than simple discussion meetings or tabletop exercises. By using a more granular (STSD-CTF) model, time and cost can be saved by facilitating management to help them identifying and choose appropriate test scenarios for the participating organization. By structured use of the (STSD-CTF) model scenario repository can be constructed. Scenario repository can be used to both re-use and exchange scenario and exercise. This may reduce costs of cyber security training and help to fill the existing competence gap for cyber security personnel in two ways: Directly to provide customized training exercise at low cost and secondly by allowing none security specialists to participate in organizational learning exercises. Moreover, consequently distribute the knowledge to handle the cyber security problem across the organization.

Being a working in progress paper it is difficult to have clear conclusions yet. However as indicate in figure 1 there are 5 distinct steps in the design science research process, problem analysis step, solutions suggestion step, development step, evaluations step and conclusion. This paper has outlined a work in progress in step 1 and step 2. In the next step we will develop scenario exercises and refine the evaluation criteria to measure the effectiveness of these exercise to help deal with the problem of fill the gap between the demand and supply of cyber security specialist and cyber security trained users.

8 References

Carayon, P., Hancock, P., Leveson, N., Noy, I., Sznelwar, L., & van Hootegem, G. (2015). Advancing a sociotechnical systems approach to workplace safety – developing the conceptual framework. *Ergonomics*. https://doi.org/10.1080/00140139.2015.1015623

Carlsson, A., & Gustavsson, R. (2018). The art of war in the cyber world. In *2017 4th International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S and T 2017 - Proceedings*. https://doi.org/10.1109/INFOCOMMST.2017.8246345

Cassano-Piché, A., Vicente, K. J., & Jamieson, G. A. (2006). *A SOCIOTECHNICAL SYSTEMS ANALYSIS OF THE BSE EPIDEMIC IN THE UK THROUGH CASE STUDY*.

Cisco. (2018). *Annual cyber security report*.

Computing Cases. (1983). Therac-25. Retrieved from https://computingcases.org/case_materials/therac/teaching_intro/Teaching_Intro.html

Dahlgren, M. A., & Öberg, G. (2001). *Questioning to learn and learning to question: Structure and function of problem-based learning scenarios in environmental science education*. *Higher Education* (Vol. 41).

DSB. (2016a). *Fullskalaøvelser*. Retrieved from https://www.dsb.no/globalassets/dokumenter/risiko-sarbarhet-og-beredskap/ovingsveileder/metodehefte_-fullskalaovelse.pdf

DSB. (2016b). *Funksjonsøvelser*. Retrieved from https://www.dsb.no/globalassets/dokumenter/risiko-sarbarhet-og-beredskap/ovingsveileder/metodehefte_funksjonsovelse.pdf

DSB. (2016c). *Metodehefte diskusjonsøvelse*. Retrieved from https://www.dsb.no/globalassets/dokumenter/risiko-sarbarhet-og-beredskap/ovingsveileder/metodehefte_diskusjonsovelse.pdf

DSB. (2016d). *Spilløvelser*. Retrieved from https://www.dsb.no/veiledere-handboker-og-informasjonsmateriell/metodehefte-spillovelse/

Gallagher, R. (2018, February 17). How U.K. spies hacked a European ally and got away with it. *The Intercept_*. Retrieved from https://theintercept.com/2018/02/17/gchq-belgacom-investigation-europe-hack/

Idé, T., Lozano, A. C., Abe, N., & Liu, Y. (2013). Proximity-Based Anomaly Detection using Sparse Structure Learning. https://doi.org/10.1137/1.9781611972795.9

Karokola, G. R. (2012). *A framework for Securing a-Government Services, The case of Tanzania*. Stockholm University.

Kowalski, S. (1994). *IT Insecurity: A Multi-disiplinary Inquiry*. Stockholm University.

Kuechler, W., & Vaishnavi, V. (2012). *A Framework for Theory Development in Design Science Research: Multiple Perspectives*. *Journal of the Association for Information Systems* (Vol. 13).

Lalonde, C. (2007). *Proceedings of OLKC 2007-"Learning Fusion" CRISIS MANAGEMENT AND ORGANIZATIONAL DEVELOPMENT: TOWARDS THE CONCEPTION OF A LEARNING MODEL IN CRISIS MANAGEMENT*.

Li, F., Lai, A., & Ddl, D. (2011). Evidence of advanced persistent threat: A case study of malware for political espionage. In *Proceedings of the 2011 6th International Conference on Malicious and Unwanted Software, Malware 2011*. https://doi.org/10.1109/MALWARE.2011.6112333

Marquis-Boire, M., Guarnieri, C., & Gallagher, R. (2014, November 24). Secret Malware in European Union Attack Liked to U.S. and British Intelligence. Retrieved from https://theintercept.com/2014/11/24/secret-regin-malware-belgacom-nsa-gchq/

NSM. (2018). *Et sikkert digitalt Norge-IKT-risikobilde 2018*.

Oppland Arbeiderblad. (2017). Øvelse på kritsk dataangrep. Retrieved from https://www.oa.no/fylkesmannen/beredskap/oppland/ovelse-pa-kritisk-dataangrep/s/5-35-545812

Pelletier, L. G., Guertin, C., Paige Pope, J., & Rocchi, M. (2016). Homeostasis balance, homeostasis imbalance or distinct motivational processes? Comments on marks (2015) ‘homeostatic theory of obesity.’ *Health Psychology Open*, *3*(1). https://doi.org/10.1177/2055102915624512

Rahman, S., Momtazpour, M., Zhang, J., Sharma, R., & Ramakrishnan, N. (2015). Analyzing Invariants in Cyber-Physical Systems using Latent Factor Regression. https://doi.org/10.1145/2783258.2788605

Schoemaker, P. J. H., & van der Heijden, C. A. J. M. (2008). Integrating scenarios into strategic planning at Royal Dutch/Shell. *Planning Review*. https://doi.org/10.1108/eb054360

Telenor. (2018). *Digital Sterkere sammen*.

Whitworth, B., & Zaic, M. (2018). The WOSP Model: Balanced Information System Design and Evaluation. *Communications of the Association for Information Systems*. https://doi.org/10.17705/1cais.01217