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

Østby, Grethe; Berg, Lars; Kianpour, Mazaher; Katt, Basel; Kowalski, Stewart

grethe.ostby@ntnu.no; lars.berg@telenor.no; mazaher.kianpour@ntnu.no; basel.katt@ntnu.no; stewart.kowalski@ntnu.no

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. 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 a Cassano-Piche Structural Hierarchy model, the "Security By Consensus" model, the Kowalski Socio-Technical systems dynamic model and 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 (NCR) 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

In the Cisco 2018 annual Cyber Security report confirms that trained personnel is the key constraints for security professionals when managing security (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 of 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 our methodological consideration are discussed. Next, we review relevant literature before we propose our framework for building scenarios and exercises in cyber readiness. A current actual incident that is used to apply our framework is presented with brief background and the outcome of this application is exemplified. 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 AND METHODOLOGY

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 about 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. He visualized this approach as outlined in figure 1.

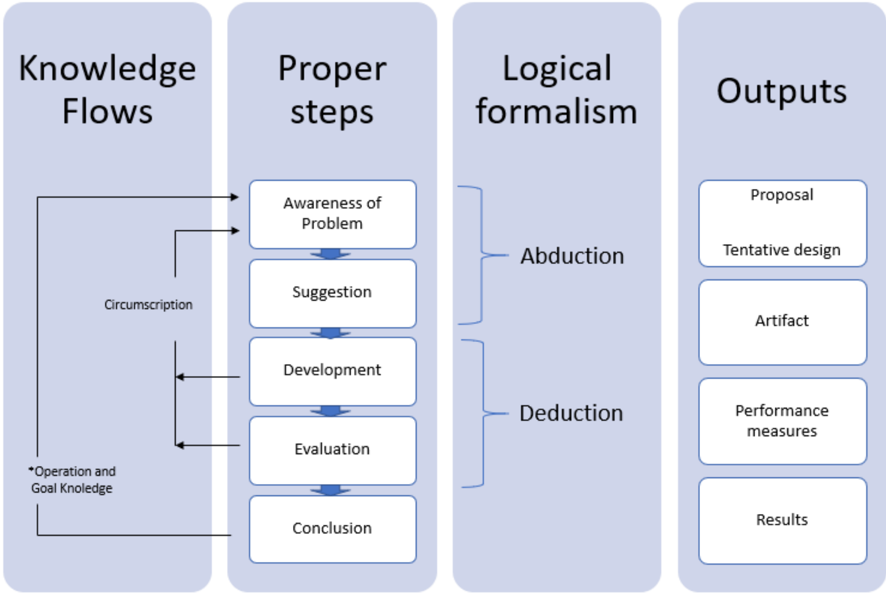

Figure 1, Design research methodology (Karokola, 2012)

Our proposed artifact in this work in progress paper is 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. The model consists of a figure dividing socio-technical approach in four concepts as suggested by Kowalski (Kowalski, 1994):

Social	Structure
	Culture
Technical	Machine
	Methods

Table 1: Socio-technical aspects

First, we tried to see where scenarios for **exercises** could fit our socio-technical model. Exercises can be different types, they can be 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, 2016a, 2016c, 2016d, 2016b). 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 testing 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 emphasizing 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.

Based on our general perception, the scenarios for discussion exercises at present are being create for for management/strategic of cyber security in organization and societies. Scenarios for table-top exercises will be placed in the area between structure and methodology. Scenarios for gaming exercises will be placed in the area between technical and methodology, and scenarios for full-scaled exercises should meet all levels of the model. We have shown this perception in figure 2:

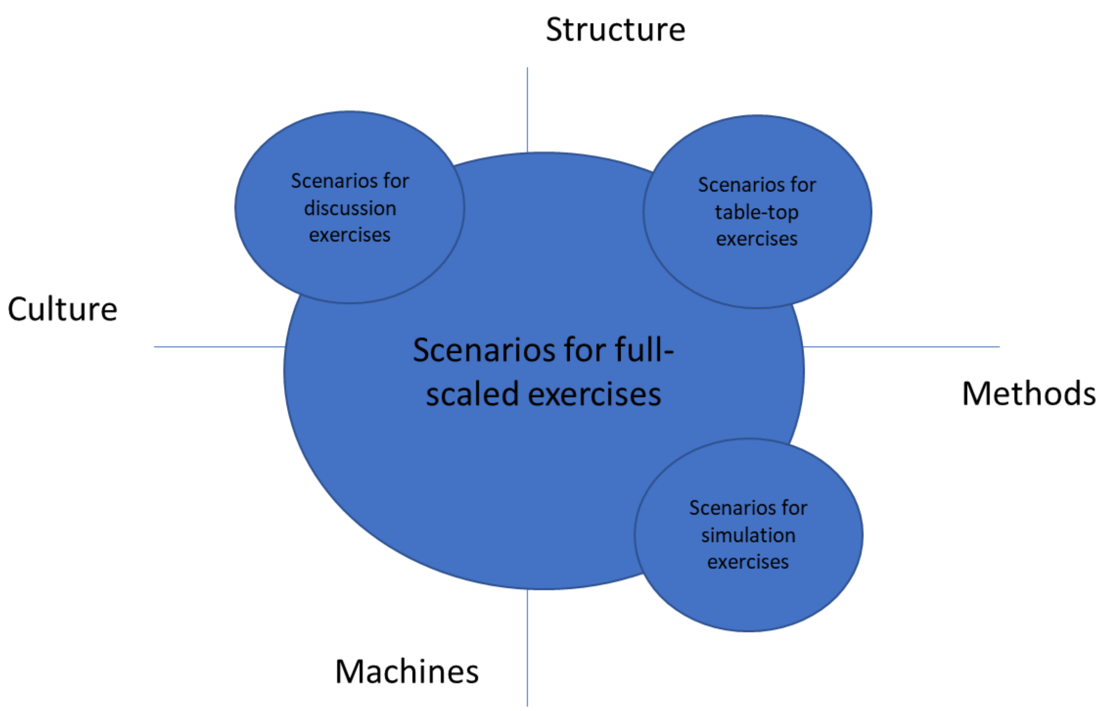

Figure 2: Surface artifact, placing different scenarios for exercises in a social-technical context

By having performed a root cause analysis and thus determined the underlying “reality” – that is major reasons for the cyber-attack, building an appropriate scenario for exercise could prove more accurate learning and give higher quality of the learning. 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 the middle of the model, but the strategic part of the exercise would be placed in the upper left part of the model.

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 describes 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 an organizational issue, we considered this as relevant in designing especially for discussion exercises, and table-top exercises.

The Security by Consensus model (SBC), is a model that attempt to capture the static and dynamic characteristics of ICT systems security (Kowalski, 1994). We chose this model since it has been used to analyze organization security. The model starts off with an abstract categorization of a socio-technical systems observable and measurable components of culture, structure, methods and machines. Then suggests that security vulnerabilities or inconsistencies in one component can bring about systemic insecurity.

In the Norwegian Cyber Range project, we also plan to run full-scaled exercises in Norway. Cassano-Piche, Vicente and Jamieson Socio-technical systems analysis of the BSE Epidemic in the UK using the Rasmussen framework. 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. Consequently, we believe it can be used to design scenarios for large scale cyber security incidents and evets in Norway.

4 RELEVANT LITERATURE

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

Most organizations are not prepared to handle 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 a 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).

Our hypothesis is that by analyzing actual events with socio-technical models, we can make scenarios that will improve the learning in exercises.

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 (Gallager, 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…" (Gallager, 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 (Gallager, 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, Guarnieri, & Gallagher, 2014), the APT kill-chain was as follows:

- Recon; 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 Linked In.
- 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.

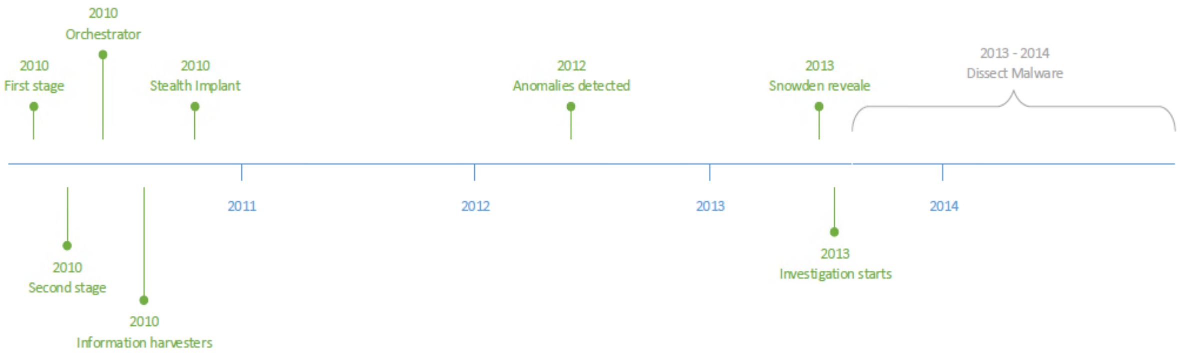

Figure 3: Quantum Insert escalation and period of detection, investigation and dissection

5.2 Example

One of the models we analyzed was the BSE Structural Hierarchy model based on Rasmussen structural hierarchy model (Cassano-Piché, Vicente, & Jamieson, 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. Analyzing Operation Socialist by using this model present the possibilities of making scenarios for every layer in both the organization and the society affected. When using this model, we analyzed that it can be used for making scenarios for full-scaled exercises and can divide into other kind of exercises for the organization and societal responsibilities.

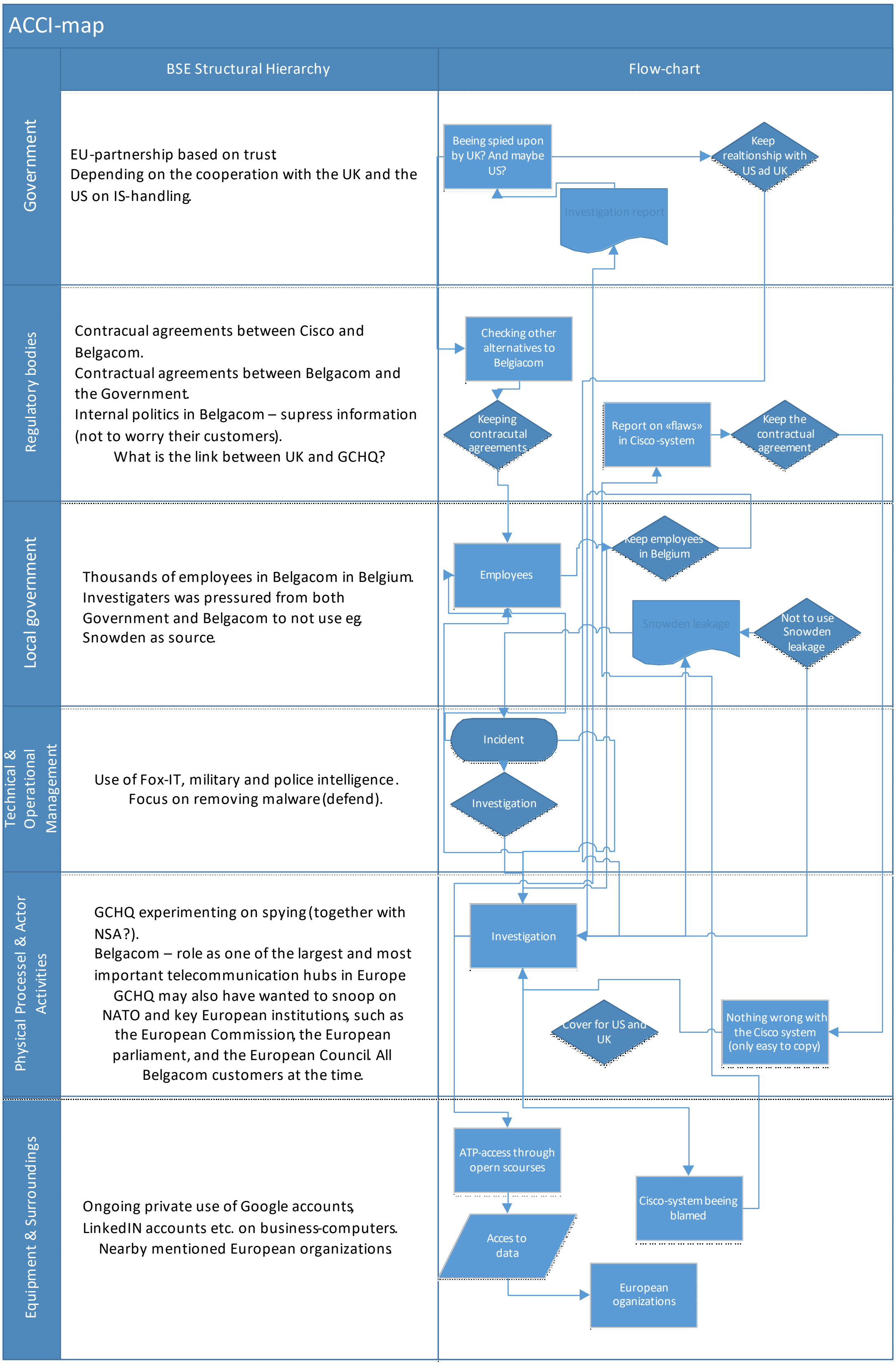

Figure 4: BSE Structural Hierarchy model analysis of Operation socialist

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 function exercise in regard to apply the Belgacom incident since it helps to indicate what functional area of the organization were the organization is vulnerable. By using the SBS 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 found it difficult to be detailed using this model; Therefore, 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 modelling a scenario for exercise, by using this model, you therefore 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 criterias-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.

Socio-technical model	Withford	SBC-model	Kowalski	BCE-model
Scenario	Operation Socialist	Operation Socialist	Operation Socialist	Operation Socialist
Apropriate for exercise	Discussion Exercise	Function Exercise	Discussion Exercise Table top exercise National Level	Full Scale Exercise

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

In figure 5 we map the different models into a cartesian grid to attempt to visualize the strength and weakness of different models. We may also 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 cartesian grid a socio-technical system design framework for cyber security training exercises (STSD-CSTE).

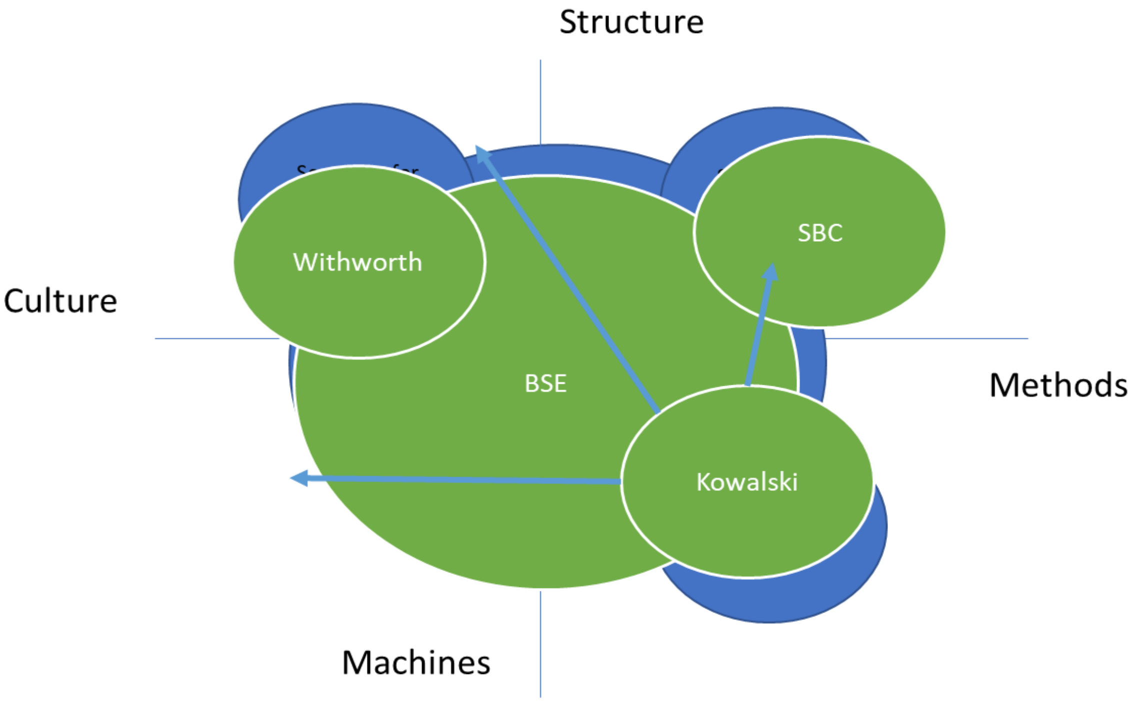

Figure 5: Framework for building relevant scenarios for exercises, based on socio-technical models to analyze real life incidents (STSD-CSTE)

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 Norwegian Cyber Range (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.

To ensure the best possible effect in the cyber-range arena in Norway, current existing information systems tools used in the community will be emulated. 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.

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, as a consequence 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. (n.d.). *A SOCIOTECHNICAL SYSTEMS ANALYSIS OF THE BSE EPIDEMIC IN THE UK THROUGH CASE STUDY*.

Chalmers, A. F. (Alan F. (1999). *What is this thing called science?* Hackett Pub.

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).

Doggett, M. (2004). *Solving problems : a statistical comparison of three root cause analysis tools*. Retrieved from https://www.researchgate.net/publication/34256585

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/

Gallager, R. (2014, December 13). Operation Socialist The Inside Story of How British Spies Hacked Belgium's Largest Telco. *The Intercept_*. Retrieved from https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/

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/

Greenwood, R. E. (1993). The Case Study Approach. *Business Communication Quarterly*. https://doi.org/10.1177/108056999305600409

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

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/

Peterson, G. D., Cumming, G. S., & Carpenter, S. R. (2003). Scenario planning: A tool for conservation in an uncertain world. *Conservation Biology*. https://doi.org/10.1046/j.1523-1739.2003.01491.x

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

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