RESCAPE Project: Tool for cyberdefense adaptive training based on the classification of operator cognitive state.

Yvan Burguin, Philippe Rauffet, David Espes, Christine Chauvin, Philippe Le Parc

Chapter XX

Cyberdefense Adaptive Training Based on the Classification of Operator Cognitive State

Yvan Burguin[1], Philippe Rauffet[1], David Espes[2], Christine Chauvin[1], Philippe Le Parc[2]

[1] Université de Bretagne Sud, Lab-STICC UMR 6285

Lorient, FRANCE

[2] Université de Bretagne Occidentale, Lab-STICC UMR 6285

Brest, FRANCE

ABSTRACT

To face the increasing number and the variety of cyberattacks, training and adaptation of cyberdefense operators become critical and should be managed all along their careers. Thus, it is necessary to develop adaptive training methods that are able to quickly detect operators' weaknesses and to propose a strategy to reinforce their skills on these points. This paper presents the choice of a cognitive model in order to guide the development of an adaptive training software. In this regard, the paper proposes a review of several elements that contributed to the development of the model.

Keywords: Adaptive Training, Cyberdefense, Human Factors, Decision Making Model, Physiologically Based Adaptive Training

INTRODUCTION

Cyberattacks are continuously increasing in variety and number, and therefore require a constant adaptation from the operator who must react to each attack with rapidity and efficiency. To face these changes, cyber operators must be trained regularly.

This training aims to: 1) maintain knowledge of cyber operators up to date, 2) train cyber operators to use new tools and 3) allow cyber operators to appropriately react to new attacks.

In this regard, adaptive training softwares support the training of cyberdefense operators in order to improve their performance in real conditions. To propose an adaptive training software, there are several requirements to satisfy (Jones et al., 2019; Trifonov et al., 2020) such as an ecological environment, a system to adapt the training scenario autonomously and a way to assess the difficulties experienced by the trainee. To support this dynamic and customised adaptation of the training scenario, it is important to detect or predict when errors may occur. For this purpose, behavioural and physiological data can be used to assess the variations in performance and mental workload that can lead to an error (Dykstra & Paul, 2018; Sawyer et al., 2014).

This paper deals with the choice of a cognitive model that could support the design of a software for adaptive training in the cyberdefense field. Such a model would allow us to understand the different cognitive processes used by the operator to perform tasks, and to identify the factors that could contribute to performance decrement. This model can then orient the selection of appropriate physiological and behavioural indicators to measure what parts of the task cause difficulty to the operator.

The organisation of this paper is as follows. First, existing models and the different tasks performed by a cyberdefense operator during its daily activities are presented in the Related Work section. The section “model for an adaptive training” presents our model that fulfils all the requirements for an adaptive training model. The conclusion section concludes this paper.

RELATED WORK

Different approaches have been developed to identify the problems occurring in the cognitive activities of cyber operators. Several studies have focused on the definition of metrics that help to detect the human reliability of operators during the cyber tasks (Henshel et al., 2016; G. Klein et al., 2011; Sawyer et al., 2016), by especially considering response times (e.g., for detection, for threat solving) as well as categorization of attacks or threats. Some others have also investigated and demonstrated an effect of visual load or fatigue on an increased error rate of cyber

operators in detection tasks (G. Klein et al., 2011; Paul & Dykstra, 2017). Nevertheless, these studies only focused on the performance metrics. If they can help for detecting some errors in the cyber tasks, these metrics do not provide insights on the root causes of the errors. It is therefore necessary to open the black box of the cognitive activities carried out by operators, to understand where the error or the difficulty experienced by the cyber operator can come from.

The following section will present a brief literature review on some cognitive models applied to the domain of cyberdefense operations. Some models are mainly inspired by the Natural Decision Making framework, with a focus on the situation awareness, while others are more focused on the planning and the organisation of the different cognitive tasks within structured workflows.

Situation Awareness Model in Cyber Activities

Endsley introduces the situation awareness (SA) concept as the combination of three levels: perception of the elements in the environment, the comprehension of the situation and the projection of future states of the situation (Endsley, 1995). She defines the process of creating this SA as the situation assessment. An important point of the situation assessment process is that it is highly dependent on the actual SA. Based on this knowledge, the situation assessment process is performed as a cycle that analyses the situation. Another process aiming to enhance the SA is sensemaking (G. Klein et al., 2006a, 2006b). This process tends to represent the understanding process of an unusual situation. It focuses on the inference of a frame that matches with the perceived data based on some pertinent points.

Various studies already attempt to analyse and model how the SA is built in the cyberdefense operations (D'Amico et al., 2005; Endsley & Connors, 2014; Franke & Brynielsson, 2014). Especially, the work of d'Amico et al. (2005) brings a well detailed model of the progression through three stages of cyber situation awareness during the whole task of the operator. Moreover it also introduces the decision point during this process. The first stage is the detection stage, which consists in an analysis of the primary sensor data and processing of these data to transform them into information. The second stage is named the situation assessment stage and consists of including more data sources and processing all the information to finally obtain knowledge. Then the last stage is called threat assessment, which consists in the analysis of the incident, adding intelligence data, and finally in processing the information into knowledge and predictions.

This model brings a precise description of the successive technical activities to build operator's situation awareness. Although this model describes precise actions to be taken, it does not detail the cognitive process involved to achieve the task. To build the SA, decision points are introduced in the model. They help to refine the SA based on the actions that are done by the operator. Indeed, decision making is a process that highly depends on the SA. It is particularly true in the cyber domain where it is highly related to the cyber SA (Endsley & Connors, 2014). The task of the operator is to recognise the threat and to apply the established procedure. Then the main skills to

develop for the operator during the training should be its ability to correctly assess the situation and to correctly adhere to procedures.

System Analysis and Workflow in Cyber

Some studies lead to further investigation into the workflow of the operators (Curnutt & Sikes, 2021; Franklin et al., 2017; Gutzwiller et al., 2016; Trent et al., 2019). Such studies bring a finely detailed model of the technical activity of the operators. The paper of Trent, Hoffman, Merritt and Smith especially, highlights four distinct phases in the cyber operator task (Trent et al., 2019). These four phases consist in a first step of planning and logistics to define the activities that can be done by the cyber operator. The second phase consists in the monitoring and the collection of data on the network's flow. Then these data are analysed in the third phase to identify and characterise the elements of interest. Finally a last phase consists in reporting the findings and defining a solution process. The two intermediate phases (i.e., monitoring and collection, and analysis) support the continuous sensemaking about the state of the network. Another main point highlighted by all these studies is the precise repartition of the task among the team (Trent et al., 2019). Indeed, the task of the operator includes the respect of the report procedure that allows for other parts of the team to continuously develop and adapt the procedures. This kind of study brings a very precise description of the theoretical workflow of the operator in a well organised organisation. Such precise details about the workflow have led to the development of several metrics like time needed to apply procedures or other metrics based on the procedure implementation (Willett, 2016). But, not all the organisations are well organised and the operators do not always follow precisely the established protocols.

Finally, this type of models only focus on the best way to realise the task without considering human or organisational failure. In order to take into account these points, there is a need to look forward to natural decision making model in cyberdefense, trying to highlight the cognitive process implied in the different parts of the task described in technical models.

Towards a Naturalistic Decision Making Model for Cyberdefense

The previous models presented above suffer from a lack of comprehension about the decision process itself and only focus on the elements that support the decision process, such as the building of the SA, or the organisation of the activity. Moreover they do not really explain how the team can influence the decision, or how the operators' expertise as well as their familiarity with the situation impact on the performance of the cognitive processes. These considerations are close to those of naturalistic decision making (NDM) approach (Zsambok & Klein, 2014). Indeed, the NDM attempts to model the decision making closer to reality. To do so, based on the decision making process used by experts, the recognition primed decision theory

(RPD) (Zsambok & Klein, 2014) proposes a model where the subject makes a decision based on a recognition of the situation. This model can be adapted in three variants depending on the situation.

The first variant is the simple match decision, and it is used when the operators immediately perceive the situation as typical. This straightforward recognition of the characteristics of the situation allows them to immediately implement the appropriate actions. The second variant corresponds to the situations where the operators do not recognize the situation as typical, and implement several mechanisms to further investigate it. Such mechanisms are also involved in case of anomaly detection after the first recognition of the situation to correct the diagnosis. Finally the last variant consists in the evaluation of the projected outcomes of the decision. In such a case the operators add a step of mental simulation before implementing the decision and if the projected results are not perceived as satisfying, they will try either to adapt the decision or to reconsider the situation if needed.

To model the decision making process in the cyberdefense operations, it could be useful to consider this model, along with the question of interactions with the rest of the team. Cybersecurity operations are rarely the burden of one single operator and have to be considered as a team activity, with collective decision making. Thus, to dispose of a global model of cognitive activity, there is a need for a model that synthesises all the cognitive operations involved in the decision making, from the situation assessment and sensemaking to the decision itself and its team dimension. The proposal presented in the next section will be based on RPD, with a few adaptations to take into account this question.

MODEL FOR AN ADAPTIVE TRAINING SOFTWARE

In order to propose a global model of the cognitive activity involved during the different cyberdefense tasks, we propose to add specific elements to a basic RPD scheme, related to the building of SA of cyber operators, the potential team interactions, the relationships between the decision quality and the technical skills of the operators, and finally the link between the benefits of training and experience acquired by the cyber operators during the different phases of the model.

As mentioned by Klein (1993), when experts are confronted to highly dynamic situations with strong time pressure, they implement a process of recognition (see Figure 1. **Recognition**) of the situation which allows them to make a reactive decision based on their past experience.

However, if the situation is not immediately recognized, the cyber operators try to increase their comprehension of the anomaly i.e., they act to increase their SA (see Figure 1. **Sensemaking loop**). In such a case, the cyber operator can act by following two different ways. First, they use the team's resources which basically consist of the experience of their colleagues to recognize the anomaly. Second, they carry out a deeper analysis of the system in order to increase their SA. This process can be iterated several times until the anomaly is correctly identified.

Once the anomaly is recognized, the operators have to apply the established procedure (see Figure 1. **Existing procedures**). If they are able to implement the procedure, they will do it. Conversely, if they do not know how to implement the procedure, due to a lack of knowledge or experience, the operators have to find another solution to restore the safety of the system.

At this step, there are two ways to find the best solution to mitigate the attacks. First, they can ask for help from the team and follow a report procedure. According to their experiences, they can propose a solution to the cyber operators that can deploy it. Second, the cyber operators can find themselves a solution to mitigate the cyber attacks, by adapting and slightly changing an established procedure. Usually, an analytical strategy is used to decide the course of action. The cyber operators look for all the possible ways they have at their disposal to prevent the cyber attacks. They select the one with which they are the most familiar (see Figure 1. **Tool review**).

For future events and to increase the experience of cyber operators, the previous accumulated knowledge has to be stored and reused for future training (see Figure 1. **Experience / Knowledge**). The aim is to limit the need to request assistance from the team that can be time consuming. In order to have a fast and accurate response, the cyber operators should be able to correctly understand the situation and to perform the best actions to prevent the cyber attack. The experience and knowledge block represents the database of the operators that allows them to recognise the situation. It is also implied in the construction of the SA because the cyber operators infer from this database the knowledge of the network architecture and their understanding of the cyber attack. Finally, this block is the main component for the training of cyber operators. The knowledge that it contains can be used for the mental simulation of the cyber operators and so to generate new scenarios for the adaptive training of cyber operators.

Unlike other existing models that only focus on a part required by adaptive training models, such as situation awareness or operator errors, our proposed model integrates all these components and describes how they interact between them. Our model is based on a decision block that is at the centre of the model. As in other models, the situation assessment corresponds to a loop that helps to recognize the situation. The novelty of our model resides in the use of a second loop that represents the process undertaken by the operator in reaction to the perceived situation. Moreover, this second loop admits potential deviations with existing procedures.

This model, although specific to the activity of the operators, represents the cognitive functions achieved in cyberdefense operations without forgetting the tasks that he has to perform. It is sufficiently abstracted and avoids adding too much details on the tasks in order to keep a high modularity. A specificity of our model is also its ability to leverage team experience for a better understanding of the situation or improving the

choice of the response that has to be done. Moreover the model highlights the link between the operators' process and their previous knowledge and experience.

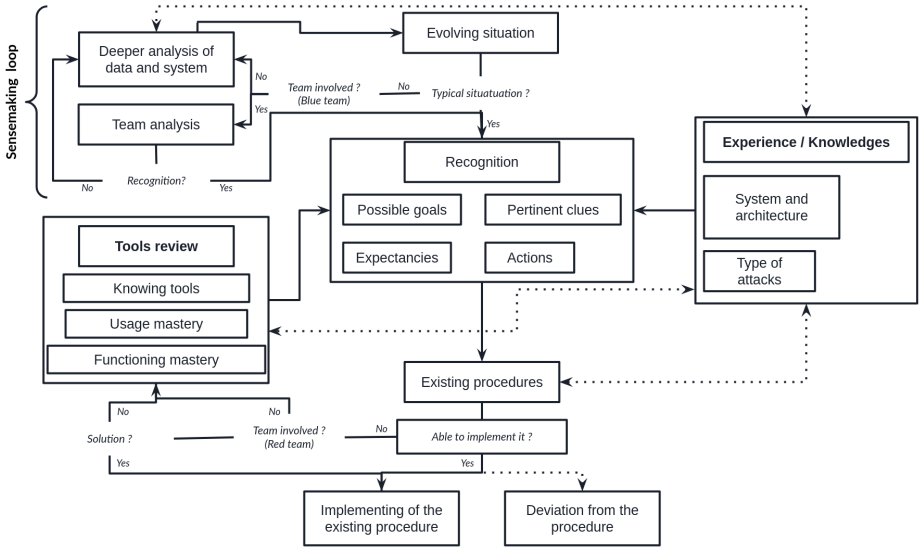

Figure 1. Model of the cognitive and social process involved during the task

CONCLUSION

The design of a physiologically based adaptive training model depends on physiological indicators that measure the difficulties encountered by the operator. Using these indicators, the existing models propose a decision process that relies on the situation awareness of the cyber operator. However, these models suffer from a lack of usability in a context of adaptive training because 1) cyber operators do not interact sufficiently with other members of the team and 2) they do not take into account the errors that cyber operators can make. The contribution of our model on these points would gain to be reinforced through experimental validation.

Unlike other existing models, our proposed model is sufficiently flexible to support cyber operators during their training in an autonomous way. To reach this goal, we compensate for the loss of technical precisions with a cognitive approach of the operations. Moreover, the two loops emphasised in the paper open new perspectives to assess the difficulty experienced by cyber operators. The instantiation of these two loops could be assessed with traditional performance metrics (like temporal indicators or threat categorization accuracy), but we could also imagine to use physiological and behavioural indicators to measure the mental effort exerted by cyber operators to implement these loops, and to determine the causes of these difficulties. Our model is the cornerstone to design adaptive training software to automatically determine which type of training is suitable for the cyber operator in order to follow a pedagogical strategy that is necessary to respond appropriately to new threats in cybersecurity.

REFERENCES

Curnutt, A. J., & Sikes, S. R. (2021). *KNOWLEDGE MANAGEMENT APPLICATION TO CYBER PROTECTION TEAM DEFENSE OPERATIONS* [PhD Thesis]. Monterey, CA; Naval Postgraduate School.

D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., & Roth, E. (2005). Achieving cyber defense situational awareness : A cognitive task analysis of information assurance analysts. *Proceedings of the human factors and ergonomics society annual meeting*, *49*(3), 229-233.

Dykstra, J., & Paul, C. L. (2018). Cyber Operations Stress Survey: Studying fatigue, frustration, and cognitive workload in cybersecurity operations. *11th USENIX Workshop on Cyber Security Experimentation and Test (CSET 18)*.

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human factors*, *37*(1), 32-64.

Endsley, M. R., & Connors, E. S. (2014). Foundation and challenges. In *Cyber defense and situational awareness* (p. 7-27). Springer.

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness–a systematic review of the literature. *Computers & security*, *46*, 18-31.

Franklin, L., Pirrung, M., Blaha, L., Dowling, M., & Feng, M. (2017). Toward a visualization-supported workflow for cyber alert management using threat models and human-centered design. *2017 IEEE Symposium on Visualization for Cyber Security (VizSec)*, 1-8.

Gutzwiller, R. S., Hunt, S. M., & Lange, D. S. (2016). A task analysis toward characterizing cyber-cognitive situation awareness (CCSA) in cyber defense analysts. *2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, 14-20.

Henshel, D. S., Deckard, G. M., Lufkin, B., Buchler, N., Hoffman, B., Rajivan, P., & Collman, S. (2016). Predicting proficiency in cyber defense team exercises. *MILCOM 2016-2016 IEEE Military Communications Conference*, 776-781.

Jones, R. M., O'Grady, R., Maymi, F., & Nickels, A. (2019). Cognitive Agents for Adaptive Training in Cyber Operations. *International Conference on Human-Computer Interaction*, 505-520.

Klein, G. A. (1993). A recognition-primed decision (RPD) model of rapid decision making. *Decision making in action: Models and methods*, *5*(4), 138-147.

Klein, G., Moon, B., & Hoffman, R. R. (2006a). Making sense of sensemaking 1 : Alternative perspectives. *IEEE intelligent systems*, *21*(4), 70-73.

Klein, G., Moon, B., & Hoffman, R. R. (2006b). Making sense of sensemaking 2 : A macrocognitive model. *IEEE Intelligent systems*, *21*(5), 88-92.

Klein, G., Tölle, J., & Martini, P. (2011). From detection to reaction-A holistic approach to cyber defense. *2011 Defense Science Research Conference and Expo (DSR)*, 1-4.

Paul, C., & Dykstra, J. (2017). Understanding operator fatigue, frustration, and cognitive workload in tactical cybersecurity operations. *Journal of*

Information Warfare, *16*(2), 1-11.

Sawyer, B. D., Finomore, V. S., Funke, G. J., Mancuso, V. F., Funke, M. E., Matthews, G., & Warm, J. S. (2014). Cyber vigilance : Effects of signal probability and event rate. *Proceedings of the human factors and ergonomics society annual meeting*, *58*(1), 1771-1775.

Sawyer, B. D., Finomore, V. S., Funke, G. J., Matthews, G., Mancuso, V., Funke, M., Warm, J. S., & Hancock, P. A. (2016). *Cyber vigilance : The human factor*. Air Force Research Lab Wright-Patterson AFB OH Human Performance Wing (711th ….

Trent, S., Hoffman, R. R., Merritt, D., & Smith, S. (2019). Modelling the cognitive work of cyber protection teams. *The Cyber Defense Review*, *4*(1), 125-136.

Trifonov, R., Nakov, O., Manolov, S., Tsochev, G., & Pavlova, G. (2020). Possibilities for Improving the Quality of Cyber Security Education through Application of Artificial Intelligence Methods. *2020 International Conference Automatics and Informatics (ICAI)*, 1-4.

Willett, K. D. (2016). *Cybersecurity Decision Patterns as Adaptive Knowledge Encoding in Cybersecurity Operations* [PhD Thesis]. Stevens Institute of Technology.

Zsambok, C. E., & Klein, G. (2014). Current and future applications of naturalistic decision making in aviation. In *Naturalistic decision making* (p. 101-110). Psychology Press.