Human Factors in Cybersecurity, Vol. 53, 2022, 58–65
https://doi.org/10.54941/ahfe1002202

Cyber Defense Adaptive Training Based on the Analysis of Operators' Cognitive State

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

[1]Université de Bretagne Occidentale, Lab-STICC UMR 6285, Brest, France
[2]Université de Bretagne Sud, Lab-STICC UMR 6285, Lorient, France

ABSTRACT

To address the increasing number and the variety of cyber attacks, the training and adaptation of cyber defense operators are critical elements that need to be managed throughout their careers. Thus, it is necessary to develop adaptive training methods that can detect operators' weaknesses quickly and provide a strategy to strengthen their skills on these points. This paper presents a cognitive model intended to guide the development of adaptive training software. To this end, the paper reviews several elements that have contributed to the development of the model.

Keywords: Adaptive training, Cyber defense, Human factors, Decision making model, Physiologically based adaptive training

INTRODUCTION

Cyber attacks are continuously increasing in variety and number, which requires constant adaptation from operators who must react to each attack quickly and efficiently. To be able to respond to these changes, cyber operators need regular training. This training aims to 1) maintain the cyber operators' knowledge up to date, 2) train the cyber operators to use new tools, and 3) allow the cyber operators to react to new attacks appropriately.

In this regard, adaptive training software supports the training of cyber defense operators in order to improve their performance in real conditions. To design adaptive training software, several requirements need to be met (Jones et al., 2019; Trifonov et al., 2020) such as an ecological environment, a system to adapt the training scenario autonomously, and a method to assess the difficulties experienced by the trainees. 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 construction of a cognitive model that could support the design of software for adaptive training in the cyber defense field. Such a model may enable us to understand the different cognitive processes used by operators to perform tasks and to identify the factors that could contribute to performance decrement. This model could then guide the selection of appropriate physiological and behavioural indicators to measure which parts of the tasks cause difficulty to the operators.

The organisation of this paper is as follows. First, existing models and the different tasks performed by cyber defense operators in the course of their daily activities are presented in the "Related work" section. The section "Model for adaptive training software" presents our model, which fulfils all the requirements for an adaptive training model. The final 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 detect the human reliability of operators when performing cyber tasks (Henshel et al., 2016; Klein et al., 2011; Sawyer et al., 2016) in particular by considering response times (e.g., for detection, for threat solving) and classifying attacks or threats. Others have also investigated and demonstrated the effect of visual load or fatigue on the increased error rate of cyber operators in detection tasks (Klein et al., 2011; Paul & Dykstra, 2017). However, these studies have focused on performance metrics only. These metrics may help detect some errors in the cyber tasks, but they 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 operators may come from.

The following section presents a brief literature review on some cognitive models applied to the domain of cyber defense operations. Some models are mainly inspired by the Naturalistic Decision-Making framework, with a focus on 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: perceiving the elements in the environment, comprehending the situation, and predicting future states of the situation (Endsley, 1995). The process of creating this SA is defined 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 develops as a cyclical situation analysis. Another process aiming to enhance the SA is sensemaking (Klein et al., 2006a, 2006b), which represents the process of understanding an unusual situation. It focuses on the inference of a frame that matches with the perceived data based on some pertinent points.

Various studies have analysed and modelled how SA is built in the cyber defense operations (D'Amico et al., 2005; Endsley & Connors, 2014; Franke

& Brynielsson, 2014). In particular, the work of d'Amico et al. (2005) provides a detailed model of the progression through three stages of cyber situation awareness throughout the operators' task. It also introduces the notion of a decision point during this process. The first stage is the detection stage, which involves analysing the primary sensor data and processing these data to transform them into information. The second stage is named the situation assessment stage and involves including more data sources and processing all the information to finally obtain knowledge. The last stage is called threat assessment and involves analysing the incident, adding intelligence data, and finally processing the information into knowledge and predictions.

This model provides a precise description of the successive technical activities needed to build operators' situation awareness. Although this model describes the specific 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 refine the SA using the actions performed by the operators. Decision making is a process that is heavily dependent on SA. This is particularly true in the cyber domain where it is highly related to the cyber SA (Endsley & Connors, 2014). The operators' task is to recognise a threat and to apply the relevant procedure. Hence, the main skills operators need to develop during training is their ability to correctly assess the situation and follow procedures.

System Analysis and Workflow in Cyber Defense

Some studies investigate the workflow of cyber operators (Curnutt & Sikes, 2021; Franklin et al., 2017; Gutzwiller et al., 2016; Trent et al., 2019). Such studies provide a finely detailed model of operators' technical activity. Trent et al. (2019), in particular, bring to light four distinct phases in the cyber operators' task. The first phase involves planning and logistics to define the activities that can be performed by cyber operators. The second phase involves monitoring and collecting data on the network's flow. These data are analysed in the third phase to identify and characterise the elements of interest. The last phase involves reporting the findings and defining a solution process. The two intermediate phases (i.e., monitoring / collecting and analysing) support the process of continuous sensemaking about the state of the network. The studies also emphasize the precise allocation of tasks among the team members (Trent et al., 2019). Each operator's task includes complying with the report procedure that enables other elements of the team to continuously develop and adapt the procedures. These studies provide a very precise description of the theoretical workflow of operators in a well organised team. Such precise details about the workflow have led to the development of several metrics such as the time needed to apply procedures or other metrics based on the implementation of the procedures (Willett, 2016). However, not all teams are well organised, and the operators do not always follow precisely the established protocols.

Finally, this type of models focuses only on the best way to perform the task without considering human or organisational failure. In order to take these points into account, it is necessary to look to naturalistic decision-making models in cyber defense that highlight the cognitive process implied in the different parts of the task described in technical models.

Towards a Naturalistic Decision-Making Model for Cyber Defense

The models presented above suffer from insufficient attention to the decision process itself as they focus only 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 explain how the team can influence the decision, or how the operators' expertise and their familiarity with the situation may impact upon the performance of the cognitive processes. These considerations are close to those of the naturalistic decision-making (NDM) approach (Zsambok & Klein, 2014). The NDM framework seeks to model the decision-making process closer to reality. To do so, based on the decision-making process used by experts, the recognition-primed decision (RPD) theory (Zsambok & Klein, 2014) proposes a model whereby subjects make a decision based on their recognition of the situation. This model can be adapted in three variations depending on the situation.

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

To model the decision-making process in the cyber defense operations, the RPD model could usefully be taken into consideration, 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 ensure a global model of cognitive activity, there is a need for a model that synthesises all the cognitive operations involved in the decision-making process, from the situation assessment and sensemaking to the decision itself and its team dimension. The proposal presented in the next section is based on RPD theory, with a few adaptations that take this issue into account.

MODEL FOR ADAPTIVE TRAINING SOFTWARE

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

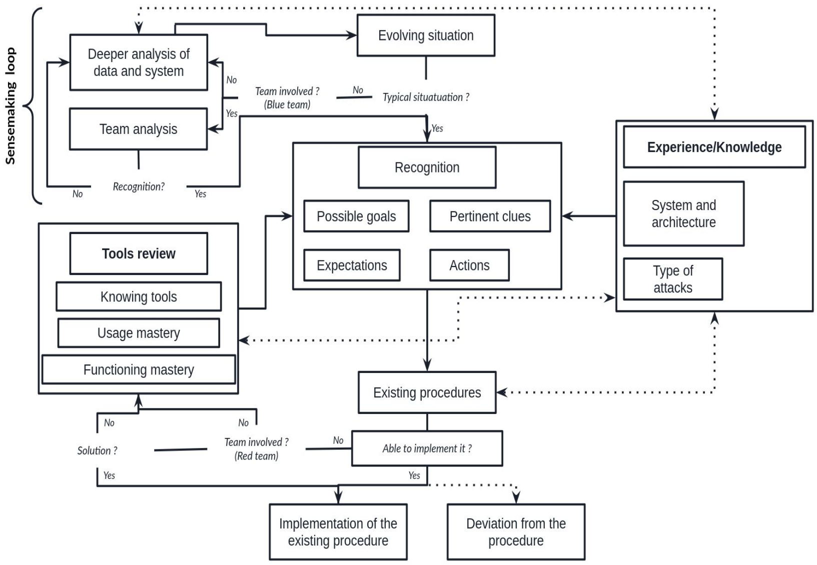

Figure 1: Model of the cognitive and social processes involved during the task.

and experience acquired by the cyber operators during the different phases of the model.

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

However, if the situation is not immediately recognized, the cyber operators seek 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 operators may use two different means. First, they use the team's resources, namely their colleagues' experience, 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 do so. Conversely, if they do not know how to implement the procedure, due to lack of knowledge or experience, the operators have to find another solution to restore the safety of the system.

At this point, there are two ways of finding the best solution to mitigate the attacks. First, they can ask for help from the team and follow a report procedure. According to their experience, the team members may propose a solution to the cyber operators who may then deploy it. Second, the cyber operators may find a solution to mitigate the cyber attacks on their own, 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, all accumulated knowledge is stored and reused for future training (see Figure 1. **Experience / Knowledge**) in order to curb the need to request assistance from the team, which can be time consuming. In order to have a fast and accurate response, the cyber operators are expected to understand the situation correctly and to perform the best actions to prevent the cyber attack. The experience and knowledge block shown in Figure 1 represents the operators' database that enables them to recognise the situation. It is also implied in the construction of the SA because the cyber operators use this database to infer their 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, thereby generating new scenarios for the adaptive training programmes.

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

Although specific to the activity of operators, this model represents the cognitive functions achieved in cyber defense operations, including the tasks that operators have to perform. It is sufficiently abstract and avoids adding too much detail on the tasks in order to retain high modularity. A specificity of our model is also its ability to leverage team experience for better understanding the situation or improving the selection of the required response to a threat. Moreover, the model highlights the link between the operators' decision-making process and their previous knowledge and experience.

CONCLUSION

Designing a physiologically based adaptive training model depends on physiological indicators that measure the difficulties encountered by the operators. Using these indicators, the existing models propose a decision-making process that is based on the situation awareness of the cyber operators. However, these models suffer from poor usability in a context of adaptive training because 1) they do not show cyber operators' interactions 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 regarding these issues needs 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 precision with a cognitive approach of the operations. Moreover, the two loops emphasised in the paper open new perspectives to assess the difficulties experienced by cyber operators. The instantiation of these two loops could be assessed with traditional performance metrics (e.g., temporal indicators or threat categorization accuracy), but we may also 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 designing adaptive training software and determining automatically which type of training programme is suitable for cyber operators, using a pedagogical strategy that is needed 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.