





# Exploring the Affordances of Multimodal Data to Improve Cybersecurity Training with Cyber Range Environments

Mariano Albaladejo-González , Sofia Strukova , José A. Ruipérez-Valiente , Félix Gómez Mármol   
 Department of Information and Communications Engineering, University of Murcia  
 Calle Campus Universitario, 30100 Murcia (Spain)  
 {mariano.albaladejog, strukovas, jruiperez, felixgm}@um.es

**Abstract**—During the last years, the constant cybersecurity breaches being reported are remarking the necessity of raising the number of cybersecurity experts that can tackle such threats. In this sense, educational technology environments can help to generate more immersive and realistic environments, and within this context, cyber range systems are one of the foremost solutions. However, these systems might not provide rich and detailed feedback to instructors and students regarding the performance in each cyberexercise. In this paper we discuss the potential of multimodal data, including clickstream, console commands, biometrics, and other sensor data, to improve the feedback and evaluation process in cyber range environments. We present the affordances that these techniques can bring to cybersecurity training as well as a preliminary architecture to implement them. We argue that these technologies can become a new generation of high-quality, realistic, and adaptive cybersecurity training that can have a dual (civil and military) impact on our society.

**Index Terms**—Cyber range, cybersecurity training, multimodal learning analytics, educational technology.

**Tipo de contribución:** *Investigación en desarrollo*

## I. INTRODUCTION

The last decade has made exceptionally clear the upmost necessity of growing the number and quality of cybersecurity experts that can design secure systems and respond to potential threats. Every week we hear of new security breaches and scandals, that jeopardize entire companies and the privacy of their users. The respondents of the ISACA's State of Cybersecurity of 2020 indicated that 53% of them were expecting a cyberattack within 12 months. Moreover, Cybersecy Ventures predicted that cybercrime will produce damages totaling \$6 million USD globally in 2021, a prediction which is based on recent year-over-year growth [1]. To face this problem, there is an overall agreement on the need to increase the quality of the training that these specialists receive [2]. However, a research report that interviewed over 300 cybersecurity professionals indicated that only 38% of them are happy with the level of training that they are receiving [3].

In this sense, educational technology training tools can play a pivotal role in the training quality that professionals can receive. Within this context, we are especially focused on cyber ranges, which are well-defined virtualized environments where trainees can develop practical hands-on-activities that resemble much better real cybersecurity operations. There are a good number of prominent cyber range examples in the literature [4], [5], [6]. These can represent realistic cybersecurity scenarios in safe sandbox environments where the

trainees can attempt to attack a network system (red team) or defend a system against an adversary attack (blue team). These cyberexercises resemble much better the real world situations that these professionals will need to face when an actual threat emerges.

However, one of the handicaps that the current state of the art of these environments shows is a low emphasis on performing effective automatic evaluations and feedback provision based on the trainee performance in the cyberexercise. For example, a recent literature review on cyber range environments that inspected all the existing ones until today, only mentioned that the evaluation can be either done manually (with human intervention) or automatically (based on an algorithm and key variables of the cyberexercise) [7]. The majority of cyber ranges provide very limited feedback on the process that the trainee followed to solve or fail the cyberexercise. For example, a capture-the-flag cyberexercise where an attacker needs to gain admin privileges and access a hidden code [8], might provide as only feedback to the instructor that the trainee knows said hidden code. Therefore, instructors cannot provide detailed and adapted feedback, nor perform a rich evaluation of the trainee taking into account diverse factors and actions that happened during the learning process.

To face this ambitious challenge, in this paper we argue on the potential of using multimodal data to improve such evaluation within the context of cyber ranges. To do so, we collect data from multiple sources, including clickstream data, console commands, biometrics and other sensor data. Then, we apply multimodal learning analytics conducting signal processing and artificial intelligence to transform the raw multimodal data into rich information [9]. In the paper at hand, we present our current advances regarding how these multimodal data can be used to improve the evaluation and feedback of trainees in cyber range environments. More specifically, we have the following two objectives:

- To present the affordances of multimodal data to improve the training process in cyber range environments.
- To propose a preliminary architecture adapted to this specific scenario to accomplish such goal.

The remainder of this paper is organized as follows: In Section II we present an overview of the affordances of multimodal data in cyber range environments, while in Section III we discuss our preliminary architecture. We finalize the paper in Section IV with conclusions and future research lines.

## II. MULTIMODAL DATA IN CYBER RANGE ENVIRONMENTS

The essential feature of a cyber range is the development of isolated and safe environments. For this reason, the core of a cyber range is virtualization, simulation and/or containerization technologies that support these environments. In addition to these technologies, a cyber range might also include front-end technologies to provide easy access to such environments. Their architecture isolates the users' computers and external networks from the environments that are running malware [10]. We find that in cyber range platforms, it is rare to find the presence of front-end dashboards that can monitor the results of the cyberexercises. The few cyber ranges that offer a dashboard show shallow information, measuring whether the user has completed the exercise successfully and the time required to do so. Our system aims to expand this state of the art with new measures of user skills and performance when interacting with cyber ranges.

The system requires data that can come from different sources to generate these news measures. For example, the cyber range can generate data related to the users' solution, along with the number of attempts, the typed commands, the proportion of unnecessary commands, and the quality of the solutions. Furthermore, it is easy to collect data related to user's telemetry adding keyboard and mouse monitoring tools in the front-end technologies, this is a common practice in websites and apps for real-time and asynchronous tracking [11]. These telemetry data can provide the following information:

- **Keyboard patterns.** These data are generated when the user writes commands. It includes the typing speed and the keystroke duration.
- **Clickstream.** It represents how the user interacts with the graphic interface of the environment. The clickstream includes the clicked elements, the click frequency, the click duration, and the mouse movement speed.

Our system aims to go further, including data collected by sensors and devices external to the cyber range. A camera and/or a kinetic device can get many interesting measures such as eye-tracking, the users' pose, position, and expression [12], [13]. Furthermore, we can add microphones to record the communication between the users [14].

In addition, we propose to measure physiological signals to get richer information about the users' state during the cyberexercises. Depending on the original context for which they are used, there are three types of devices to measure physiological signals: the devices used in the medical field for diagnosis purposes, the devices used for research purposes, and the commercial devices focused on the daily use of end users. Additionally, these devices can be placed in different parts of the body: for example, we can have wristbands, chest straps, and brain-computer interfaces (BCIs) that are placed as a helmet. BCIs measure the electrical activity of the brain and can estimate the emotions and moods of the users during the cyberexercises. The wristbands and chest straps can have different types of sensors to measure the heart rate, the blood pressure, the skin temperature, the oxygen saturation, the electrodermal activity (the measurement of the electrical activity of the skin), and the movement of the user measured

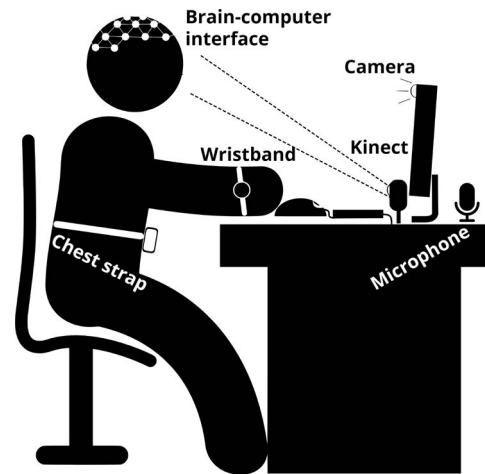


Fig. 1. Potential devices used to monitor the user during the cyberexercises.

through the accelerometers and gyroscopes, among others.

Figure 1 represents different devices collecting data throughout the cyberexercises. The system uses all the collected data to calculate additional user performance metrics and skills. The users' emotions during the cyberexercises can be estimated and classified depending on the valence and arousal degrees [15]. The valence represents the level of positive or negative affectivity and arousal, the calming or excitement level. Thereby, we could infer states like anger, joy, sadness, and pleasure.

In addition to the user emotions, the system could measure more advanced skills closely related to the necessities of cybersecurity professionals. In real-world environments, cybersecurity professionals can be under much pressure due to the impact of their decisions; for example, failing to detect sniffers on an online shop can end up causing a data breach of 40 million card numbers and 70 million personal records stolen [16]. For this reason, it is interesting to evaluate the capacity to work under pressure, for example, through user stress or the attention level [17]. Moreover, cyberattacks and their consequences can take place over an extended period of time [18]; for this reason, it is also interesting to measure the user fatigue [19]. Teamwork skills are critical for cybersecurity professionals as they will often be part of a larger and multidisciplinary team. The proposed multimodal system can be used to evaluate teamwork skills and how teamwork affects each user. All of these metrics aim to empower instructors with additional information to provide a more nuanced feedback and assessment to the cybersecurity students. The final goal is to improve the readiness of the cybersecurity professionals to detect and resolve cybersecurity breaches.

To implement the proposed system is essential to consider how invasive the devices are and whether they can be used for extended periods of time. Devices that are too invasive might endanger data recollection by reducing user freedom of movement and making the cyber range experience more uncomfortable. Furthermore, it is important to consider the devices' cost because since some of them are quite expensive, and can be used only by a single user at a time. Microphones, cameras, kinetics, and wearables are affordable solutions with

potential to measure useful constructs.

Finally, all the aforementioned types of data generated by trainees while using cyber range environments hold the potential for being used to adjust the cyberexercises to the current status of each specific trainee. This process, which is known as *adaptive learning*, has the goal of addressing the unique needs of each user [20]. In our case, we aim to dynamically adapt current cyberexercises to the knowledge of the trainee. Commands and clickstream data along with the biometric signals of trainees will allow us to analyze and compare the results of the different simulations to progressively improve subsequent training sessions and, therefore, maintain the optimal balance between the trainees' knowledge and the difficulty of each exercise.

### III. PRELIMINARY ARCHITECTURE

#### A. Description of the training process

Our system is used by: 1) the trainees, who interact with the learning contents and generate the raw data, and 2) the instructors, who are experienced teachers in the cybersecurity field responsible for keeping track of how the trainees are progressing and providing them with relevant feedback. Accordingly, the instructor first provides the trainees with the cyberexercises they must solve and afterward reviews the results represented in the dashboard in an easy and understandable way. This helps to build the feedback that the trainees will receive and choose the most suitable cyberexercises for the future users with similar knowledge.

The training process starts when the instructor distributes the cyberexercises across the trainees. While the latter are solving the tasks, our system collects various data types described in the previous section. Then, these data are processed and analyzed in order to visualize the dashboard with all the information about the cybersecurity development of each trainee.

#### B. Overview of the Architecture

Figure 2 presents the overview of the architecture of the cyber range environment with the multimodal learning analytics, and how the following components are connected within the system:

- **Cyber range.** The cyber range system is the origin of the learning process. When trainees interact in their cyber range environment, a large amount of raw multimodal data is generated, issued, collected, and stored in the webserver. We implement the event emission process using experience API schema (xAPI <sup>1</sup>) to make the rest of parts of the architecture agnostic of the specific cyber range system implemented.
- **Data collection.** The data collected within the cyber range include a wide variety of trainee actions, as well as the external sensors and devices. We use REpresentational State Transfer API (RESTful API) endpoints to send these data to the web server. There are several challenges regarding the ethical and security considerations of obtaining that data from the trainees. Thus, the collected personal data is encrypted and protected by applying appropriate technical and organizational measures

according to the General Data Protection Regulation (GDPR).

- **Data processing and analytics.** This step aims to measure and evaluate the development of the trainees regarding their cybersecurity skills. An Extract, Transform, and Load (ETL) procedure is employed in order to extract the needed data from the database, transform them into a proper storage structure for querying and analysis, and finally load them into a final database. Due to its large size, the processing cannot be performed in real-time. Therefore, we make use of *cron jobs* to launch the data processing scripts at scheduled times.
- **Visualization dashboard.** The last step consists in providing useful and effective visualizations to both the trainees and the instructors. This is done through the dashboard that represents an activity and performance measurement interface. Specifically, we can see general statistics presenting the overall progress across the cyberexercises, or active time, to name some examples. We can also see more complex measurements such as the capacity to work under pressure and concentration level. Trainees can access only their own data, while instructors can access the information of each trainee individually or see the aggregation of the entire class. At the same time, we also develop models that can evaluate trainees' competencies based on which cyberexercises they have been able to complete.

### IV. CONCLUSIONS AND FUTURE WORK

Raising a new generation of cybersecurity professionals during the 21st century is vital to have a secure digitized world and economy. However, the specialized training of these professionals is a challenging task. Cyber range environments represent a great asset that complements more traditional cybersecurity training in order to practice hands-on cyberexercises that can resemble real scenarios where trainees need to attack and/or defend a system in real time. However, the current feedback that cyber ranges provide to instructors regarding the performance of their trainees is quite scarce. In some cases we find that the instructors do not know more than whether the cyberexercise was completed or not, with no information about the process at all. This approach is definitely not sufficient to provide a just-in-time support and feedback to the students in order to improve the learning process, specially when we want to scale cyber range case studies with entire classes getting trained simultaneously.

In this paper we have argued on the potential that multimodal data can have to improve the training process when using cyber ranges. We can collect different data in various modalities like clickstream, console commands, biometrics or audiovisual data, apply signal processing and artificial intelligence techniques, and produce measures to assess ideal solution pathways, capacity to work under pressure, or concentration, which are key capacities to become a successful cybersecurity professional. Moreover, these techniques can have a dual impact on our society. First, on the civil side, we can use them to improve the academic training of students under-taking degrees related to cybersecurity and also on professional programs training cybersecurity professionals. Second, on the military side, we can use the same approach

<sup>1</sup><https://xapi.com/>

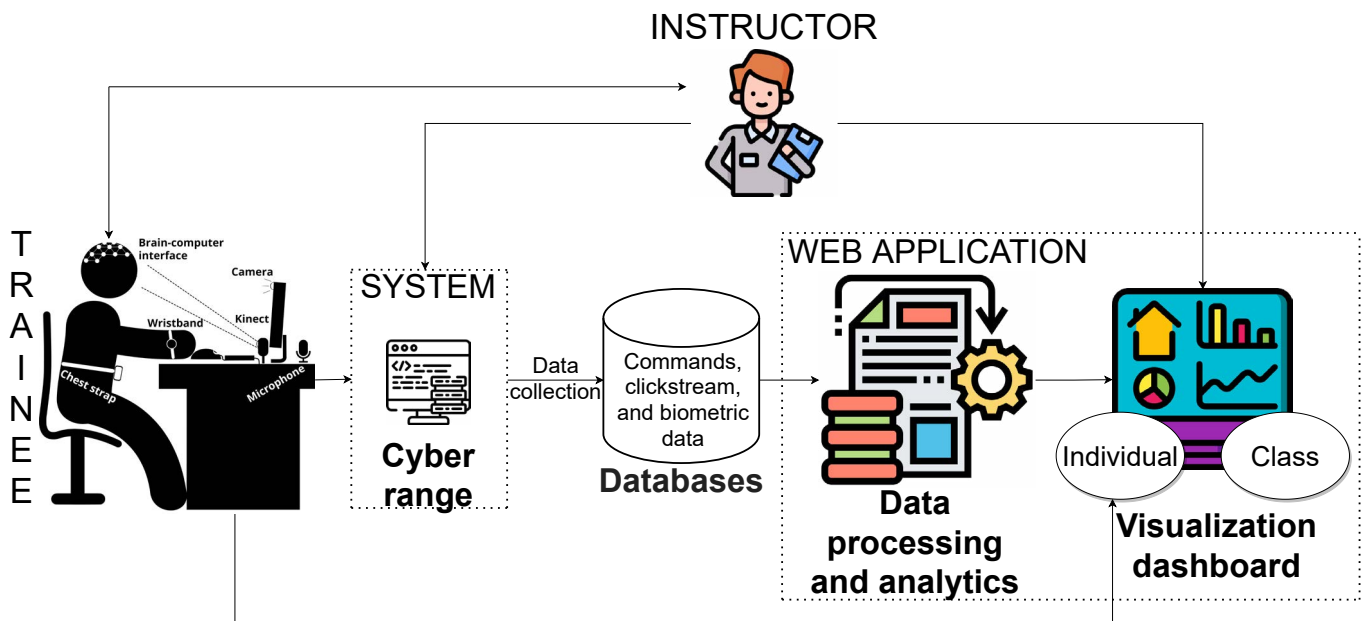


Fig. 2. Preliminary architecture of the cyber range environment with the multimodal learning analytics web application.

to improve the cyberdefence capabilities that a state may have to protect the cyberspace. Depending on the critical nature of the position of each professional getting trained, more or less invasive data collection approaches can be applied.

The future steps that we envision are multifaceted. First, we are working on developing this architecture as generic as possible, using different data sources and sensors. Then, we are planning to deploy several cyber ranges on controlled premises and make this architecture as inter-operable as possible. Then, we will conduct case studies with students undertaking security classes and with cybersecurity professionals in order to collect data and prove the viability of the architecture. Finally, we will validate that this approach is improving the overall training process.

#### ACKNOWLEDGMENTS

This work has been partially funded by project COBRA (10032/20/0035/00), awarded by the Spanish Ministry of Defense, as well as the fellowships FJCI-2017-34926 and RYC-2015-18210, awarded by the Govern of Spain and co-funded by European Social Funds.

#### REFERENCES

- [1] P. Morgan, "Cybercrime facts and statistics. 2021 Report: Cyberwarfare in the C-Suite," Cybersecurity Ventures, Tech. Rep., 2021.
- [2] B. E. Endicott-Popovsky and V. M. Popovsky, "Application of pedagogical fundamentals for the holistic development of cybersecurity professionals," *ACM Inroads*, vol. 5, no. 1, pp. 57–68, 2014.
- [3] J. Oltsik, C. Alexander, and C. CISM, "The life and times of cybersecurity professionals," *ESG and ISSA: Research Report*, 2017.
- [4] J. Vykopal, M. Vizváry, R. Oslejsek, P. Celeda, and D. Tovarnak, "Lessons learned from complex hands-on defence exercises in a cyber range," in *2017 IEEE Frontiers in Education Conference (FIE)*. IEEE, 2017, pp. 1–8.
- [5] C. Pham, D. Tang, K.-i. Chinen, and R. Beuran, "Cyris: a cyber range instantiation system for facilitating security training," in *Proceedings of the Seventh Symposium on Information and Communication Technology*, 2016, pp. 251–258.
- [6] M. Rosenstein and F. Corvese, "A secure architecture for the range-level command and control system of a national cyber range testbed," in *Proceedings of the 5th USENIX conference on Cyber Security Experimentation and Test*, 2012, pp. 1–1.
- [7] E. Ukwandu, M. A. B. Farah, H. Hindy, D. Brosset, D. Kavallieros, R. Atkinson, C. Tachtatzis, M. Bures, I. Andonovic, and X. Bellekens, "A review of cyber-ranges and test-beds: current and future trends," *Sensors*, vol. 20, no. 24, p. 7148, 2020.
- [8] K. Leune and S. J. Petrilli Jr, "Using capture-the-flag to enhance the effectiveness of cybersecurity education," in *Proceedings of the 18th Annual Conference on Information Technology Education*, 2017, pp. 47–52.
- [9] X. Ochoa and M. Worsley, "Augmenting learning analytics with multimodal sensory data," *Journal of Learning Analytics*, vol. 3, no. 2, pp. 213–219, 2016.
- [10] E. Ukwandu, M. A. B. Farah, H. Hindy, D. Brosset, D. Kavallieros, R. Atkinson, C. Tachtatzis, M. Bures, I. Andonovic, and X. Bellekens, "A review of cyber-ranges and test-beds: Current and future trends," *Sensors*, vol. 20, no. 24, 2020.
- [11] Whatpulse. Accessed: 2021-03-21. [Online]. Available: <https://whatpulse.org>
- [12] P. Joshi, *OpenCV by example : enhance your understanding of computer vision and image processing by developing real-world projects in OpenCV 3*. Birmingham: Packt Publishing, 2016.
- [13] J. St. Jean, *Kinect hacks*, 1st ed., ser. Hacks. Beijing ; Sebastopol, CA: O'Reilly, 2012, oCLC: ocn764382938.
- [14] D. Yu and L. Deng, *Automatic Speech Recognition*. Springer London, 2015.
- [15] L. Santamaria-Granados, M. Munoz-Organero, G. Ramirez-González, E. Abdulhay, and N. Arunkumar, "Using deep convolutional neural network for emotion detection on a physiological signals dataset (amigos)," *IEEE Access*, vol. 7, pp. 57–67, 2019.
- [16] X. Shu, K. Tian, A. Ciabrone, and D. Yao, "Breaking the target: An analysis of target data breach and lessons learned," *CoRR*, vol. abs/1701.04940, 2017.
- [17] S. Sriramprakash, V. D. Prasanna, and O. R. Murthy, "Stress detection in working people," *Procedia Computer Science*, vol. 115, pp. 359–366, 2017, 7th International Conference on Advances in Computing & Communications, ICACC-2017, 22-24 August 2017, Cochin, India.
- [18] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and R. Buyya, "Ddos attacks in cloud computing: Issues, taxonomy, and future directions," *Computer Communications*, vol. 107, pp. 30–48, 2017.
- [19] S. Huang, J. Li, P. Zhang, and W. Zhang, "Detection of mental fatigue state with wearable ecg devices," *International Journal of Medical Informatics*, vol. 119, pp. 39–46, 2018.
- [20] M. Liu, E. McKelroy, S. B. Corliss, and J. Carrigan, "Investigating the effect of an adaptive learning intervention on students' learning," *Educational technology research and development*, vol. 65, no. 6, pp. 1605–1625, 2017.