Advancing Human Performance in Cybersecurity, ADVANCES

Ginta Majore[1,*,†], Linas Bukauskas[2,†], Stefan Sütterlin[3,†] and Agnė Brilingaitė[2,‡]

[1]*Vidzeme University of Applied Sciences, Tērbatas str. 10, Valmiera, 4201, Latvia*
[2]*Institute of Computer Science, Vilnius University, Didlaukio str. 47, Vilnius, 08303, Lithuania*
[3]*Østfold University College, B.R.A. Veien 4, Halden 1757, Norway*

Abstract

Cybersecurity as a domain is essential for all complex digitalized environments within the public and private sectors. It incorporates technical requirements, workforce skills, and human aspects for system development, deployment, and support for business continuity. The technological advancement of cyber attacks and social engineering solutions of the adversary raise the demand for a competent cybersecurity workforce. The upskilling process has to go hand in hand with abilities to work in complex environments and even under crises. Project Advancing Human Performance in Cybersecurity (ADVANCES) contributes to research regarding the role of human factors and limitations in cybersecurity. Domain-specific engineering enables the development of a comprehensive framework as an ecosystem for future workforce development.

The three Baltic countries, Lithuania, Latvia, and Estonia, and their partners from Norway and Liechtenstein investigate human behavior in cybersecurity by combining research areas of computer science, psychology, and human genomics. The project aims to develop a comprehensive, science-based interdisciplinary framework to develop and assess generic and subject-related competences of the current and future cybersecurity workforce. The team is developing an environment that supports testing behavioral patterns, attitudes toward cyber hygiene, and specific technical skills. Educational components integrating behavior change are tested in the student environment, while multidisciplinary research requires inviting participants using public announcements. Statistical and data mining tools are used to interpret multilayered data and to find correlations among genetic, behavioral, and technical skills.

Keywords

Domain-Specific Engineering, Multidisciplinary Approach, Cybersecurity Training, Human Performance

RPE@CAiSE'23: Research Projects Exhibition at the International Conference on Advanced Information Systems Engineering, June 12–16, 2023, Zaragoza, Spain

*Corresponding author. Representative of the ADVANCES team and presenter at the CAiSE'23 event.
†These authors contributed equally.
‡The ADVANCES project leader contributed to the work equally.
ginta.majore@va.lv (G. Majore); linas.bukauskas@mif.vu.lt (L. Bukauskas); stefan.sutterlin@hiof.no (S. Sütterlin); agne.brilingaite@mif.vu.lt (A. Brilingaitė)
0000-0002-9514-7229 (G. Majore); 0000-0002-9781-9690 (L. Bukauskas); 0000-0002-4337-1296 (S. Sütterlin); 0000-0001-9768-4258 (A. Brilingaitė)

© 2023 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).
CEUR Workshop Proceedings (CEUR-WS.org)

CEUR-WS.org/Vol-3413/paper11.pdf

Iceland Liechtenstein Norway grants

The Advancing Human Performance in Cybersecurity, ADVANCES, benefits from nearly €1 million grant from Iceland, Liechtenstein and Norway through the EEA Grants under the Baltic Research Programme. The aim of the programme is to consolidate research potential of Baltic States, Iceland, Liechtenstein and Norway, strengthen regional cooperation in research relevant to the countries of the region, and fill the gap between the national research funding and the European Union Structural Assistance.
The aim of the project is to advance the performance of cybersecurity specialists by personalizing the competence development path and risk assessment. Project contract with the Research Council of Lithuania (LMTLT) No is S-BMT-21-6 (LT08-2-LMT-K-01-051).

1. Project Information

The project *A*dvancing Human Performance in Cybersecurity (in short ADVANCES) [1] started on January 1^{st}, 2021, and it will end on December 31^{st}, 2023. Eight partners from five countries implement the project. Lithuania, Latvia, and Estonia are beneficiary countries, while higher education institutions from Norway and Liechtenstein represent donor states:

1. Vilnius University (Institute of Computer Science and Institute of Biomedical Sciences), Lithuania — project promoter
2. The General Jonas Žemaitis Military Academy of Lithuania, Lithuania
3. Riga Technical University (Institute of Information Technology), Latvia
4. Vidzeme University of Applied Sciences (Socio-Technical Systems Engineering Institute), Latvia
5. Tallinn University of Technology (School of Information Technology), Estonia
6. Norwegian University for Technology and Science (Department of Information Security and Communication Technology), Norway
7. Østfold University College (Faculty of Health, Welfare and Organisation), Norway
8. University of Liechtenstein (Institute of Information Systems), Liechtenstein

The main **project objective** is to develop the domain-specific infrastructure that enables advancing the performance of the cybersecurity specialist considering possible improvements from three different perspectives: by regarding the human as a biological entity, by analyzing the behavioral patterns of the person, and by addressing the necessary technical knowledge and skills of the cybersecurity specialist. A team of more than 25 IT and cybersecurity specialists, educators, psychologists, and human geneticists joined to apply the multidisciplinary approach when searching for a solution to the project-defined problem.

The project relies on the **assumption** that it is possible to map cyber competences required to investigate digital crime, defend infrastructure, or be resilient to cyber abuse and afterward

to develop a rational competence improvement path for a CS specialist. When dealing with critical infrastructures or handling life mission-critical support systems, tools that assess human traits or inherent risks are nonexistent, or research components must be validated scientifically.

The project's **expected outcomes** consist of methodologies and tools, including specific software components to gather and analyze data, self-report tools to collect factual data on socio-behavioral patterns, risk assessment methods based on cooperative interdisciplinary data, and recommendations to ensure a personalized skill development path. The designed comprehensive framework for developing and assessing generic and subject-specific competences would serve as a tool for the international research and professional community to understand human capabilities and challenges regarding the phases of the cyber-kill-chain and to build the future cybersecurity workforce.

The **envisioned research results** include a) identification of key performance indicators in individual/team level training/exercises to develop an evidence base for a comprehensive assessment of cyber competences, b) analysis and development of methods to assess and predict the performance of a human in individual tasks and collaborative decision-making environments in cyberspace, c) development of research-proven specific tools to advance the performance of a human in learning to cope with challenges during stressful situations that require technological knowledge, and d) prototype implementation and testing to illustrate the developed framework's applicability to support a complex ecosystem for future workforce development.

2. State of the Art

The project's ambitious goal to develop a multi-discipline-based infrastructure requires ensuring the engineering processes of gathering the requirements, performing analysis of the domain from different perspectives, designing the architecture components, and implementing the prototype of Technology Readiness Level 3–4 to build a characteristic proof of the concept with possible validation in the lab setting.

The project already has nine associated papers published or accepted for publication [2, 3, 4, 5, 6, 7, 8, 9, 10] in international journals and scientific conferences.

2.1. Project Results

Most cyber incidents occur to human error. Therefore, risk assessment strategies should consider digital assets and challenges that lead to risks due to individual human characteristics under certain conditions, e.g., in stressful situations during crises. The initial project's paper [2] presented a theoretical ontology-based model as a basis for a human trait semantic network. The built proof-of-the-concept prototype combined artificial intelligence algorithms and psychological questionnaires to demonstrate existing human trait links to cyber hygiene. Another paper [3] presents a holistic architecture to assess human traits and explains the links between the natural human and digital-self using the impulsivity trait example. Also, we deconstructed the stress factor understandable in an everyday setting of the cybersecurity specialist to emphasize the need for personalized training to build resilience against stress as genetics influences reaction to the environment's triggers [4]. Therefore, in a project, the competence model of the trainee (see Figure 1) considers the trainee's performance (behavior and results) under certain conditions

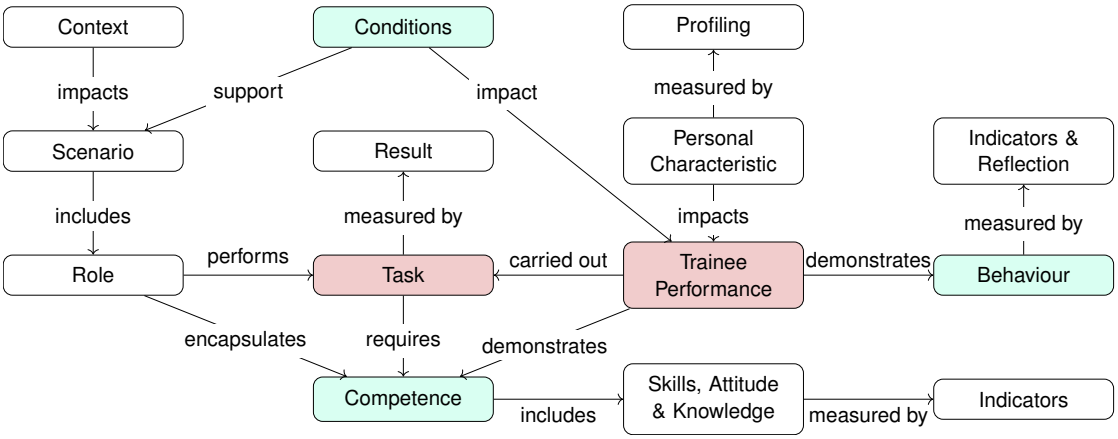

Figure 1: General competence model [5]

with an impact of personal characteristics during a particular scenario that requires one to play a professional role and apply related competences [5]. The ADVANCES intervention mapping methodology [5, 6] supports the designed competence model. The methodology consists of three building blocks—competence model, course design process, and training environment [6].

The multidimensional approach that combines soft and hard skills, behavior, and cognitive aspects requires redesigning training methods and scenarios to involve trainees and stimulate their interest in cybersecurity [7, 8, 10]. For example, we demonstrated that a penetration testing course for military cadets with no prior technical skills could increase their interest in a cybersecurity career [7] if it was designed using the experiential learning paradigm, thus, making an additional professional development path. The developed CyberEscape approach [8] is based on the hybrid training environment with physical elements and virtual infrastructure to simulate the Computer Security Incident Response Team (CSIRT) tasks. The execution results showed the approach's value in increasing self-efficacy and engagement, stimulating critical thinking, and fostering collaboration and communication skills.

The project research scope involves an educational environment and professional training, i.e., cyber defense exercises. Thus, the ontology was developed to overcome the knowledge management gap [9]. Finally, we introduce the multidimensional approach for a cyber defense exercise based on the event cycle, stakeholders' goals, and necessary social, emotional, and cognitive aspects [10]. The approach ensures psychological safety, motivation, and other event ingredients to achieve training goals.

2.2. Intermediate Results

Figure 2 shows the overall architecture of the project system. The user at the focus is a cybersecurity specialist willing to understand the personal strongest side and learn about possible future risks. In identifying recommendations, field professionals are involved: psychologists for behavioral analysis, health medical professionals for health risk assessment, and cybersecurity professionals for cybersecurity, engineering, and IT competence indication and assessment.

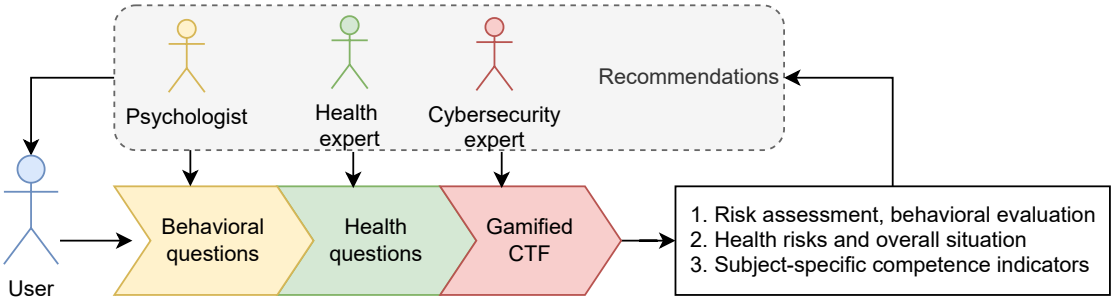

Figure 2: The general architecture of the ADVANCES ecosystem

The cybersecurity specialist has to go through all three steps of scenarios in order to get some feedback recommendations and possible risks assessed.

For the project team in order to be able to observe, experiment, and gather medical data of a subject, Vilnius University received approval from the Bioethics committee to perform a multidisciplinary experiment, including gathering and analyzing genetic data (No. 2022/4-1417-895, 12/04/2022). All ethical principles are assured, and written consent is received as voluntarily expressed declarations. All participants can leave and stop interviews at any time. Gathered data are managed according to the data management plan approved by the Research Council of Lithuania.

3. Advanced Information Systems Engineering

The team has built an advanced information system as a prototype to demonstrate a proof of concept of the complex system that relies on a multidisciplinary approach for the educational process of cybersecurity specialists. The prototype corresponds to Technology Readiness Level 4. The prototype as a domain-specific system contains several components. The main three components are the questionnaire subsystem of self-assessment tools, the health data gathering module that maps health and genome data, and an interactive exercise platform to check cybersecurity skills. Due to the sensitive genetic data, anonymization is ensured in the infrastructure. The system has a link between genetic data and other parts via specific identifiers, and additional precautions are taken to guarantee data privacy. All the digitally sequenced genetic data stays on the limited-access network. Thus, only predefined views and aggregates are imported into analytical modules. Immediate experiment results are delivered to the participant regarding behavior, health, and cybersecurity skill assessment to ensure participant attention and satisfaction. This requirement arose due to the experimentation location and game duration.

The complex system is a web-based solution involving several air-gaped components switched on or included on a need basis. One of the components is a Capture The Flag (CTF) module reflecting typical cybersecurity training platforms and providing a platform for cyber skill assessment. CTF is a gamified, hint-based three-level knowledge and skill testing platform with dynamically opened branches of problems to be solved according to the participant's level. The

platform keeps track of user parameters such as the number of guesses, number of hints, time used to submit an answer, and the time taken to complete overall CTF. The control group solves cyber hygiene questions but also can try more complex challenges of the target group. The CTF implementation and execution reflect the competence model design presented in Figure 1.

Another component includes several psychological questionnaires for self-assessment. The self-assessment tools applied in this project are scientifically validated and have been constructed under considerations of behavioral science standards, ensuring quality criteria such as construct validity, predictive validity, reliability, and objectivity. Both personality traits, cognitive styles, and the capacity for cognitive, emotional, and behavioral regulation have been assessed. The theoretical base of this selection of assessment tools draws from research on the impact of personality, situational context, and work stress on decision-making under pressure. Inspired by behavioral-cognitive models such as the critical path mode, our methodological approach leading to the self-assessment toolbox incorporates several risk factors that are potential markers for human failure, errors and other factors beyond momentarily apparent behavior. This also includes risk factors for lacking personal integrity and deviant behavior (e.g., insider threats), individual vulnerabilities to social engineering-based attack vectors, and performance-related traits such as conscientiousness.

The established self-assessment toolbox assesses information that is predictive for decision-making, risk assessment/taking within IT networks, the choice of strategies within cyber operations and how to handle ambiguous threats under pressure. To capture the whole picture and consider changing situational contexts, we go beyond pure personality factors and tap into behavioral patterns resembling the interaction of personality and environmental factors. With this approach of quantifying individual traits that are stable across situations and over time, we do not only measure momentary risk factors or potentials, but actually also a proxy for the individual's overall susceptibility. In sum, this comprehensive approach addresses the behavioral science part of the project aims and identifies statistically valid and relevant predictors of cognitive performance and behavioral control in cyber operations.

While building on previous research of project partners on communication and decision-making in socio-technical systems and cyber operations in particular, we use essential predictors for human performance that find their neural substrates in prefrontal cortical functions responsible for executive planning and execution and the control of emotional impulses and cognitive regulation.

Currently, the project team is in the experimentation phase with research participants. Preliminary correlation results of behavior, health, and cybersecurity skills with recommendations are expected at the end of June 2023. The project team expects to share with the research community results as scientific publications.

References

[1] EEA Grants, Advancing human performance in cybersecurity, 2021. URL: https://www.eeagrants.lt/en/programmes/projects/program/26/id/92/advancing_human_performance_in_cybersecurity.

[2] A. Jurevičienė, A. Brilingaitė, L. Bukauskas, Digital human in cybersecurity risk assessment,

in: Augmented Cognition - 15th International Conference, AC, Held as Part of the 23rd HCI International Conference, HCII, Proceedings, volume 12776 of *Lecture Notes in Computer Science*, Springer, 2021, pp. 418–432. doi:10.1007/978-3-030-78114-9_29.

[3] L. Ambrozaitytė, A. Brilingaitė, L. Bukauskas, I. Domarkienė, T. Rančelis, Human characteristics and genomic factors as behavioural aspects for cybersecurity, in: Augmented Cognition - 15th International Conference, AC, Held as Part of the 23rd HCI International Conference, HCII, Proceedings, volume 12776 of *Lecture Notes in Computer Science*, Springer, 2021, pp. 333–350. doi:10.1007/978-3-030-78114-9_23.

[4] I. Domarkienė, L. Ambrozaitytė, L. Bukauskas, T. Rančelis, S. Sütterlin, B. J. Knox, K. Maennel, O. Maennel, K. Parish, R. G. Lugo, A. Brilingaitė, Cybergenomics: Application of behavioral genetics in cybersecurity, Behavioral Sciences 11 (2021) p. 15. doi:10.3390/bs11110152.

[5] R. Pirta-Dreimane, A. Brilingaitė, G. Majore, B. J. Knox, K. Lapin, K. Parish, S. Sütterlin, R. G. Lugo, Application of intervention mapping in cybersecurity education design, Frontiers in Education 7 (2022) p. 12. doi:10.3389/feduc.2022.998335.

[6] R. Pirta-Dreimane, A. Brilingaitė, E. Roponena, K. Parish, Multi-dimensional cybersecurity education design: A case study, in: IEEE Intl. Conf. on Dependable, Autonomic and Secure Computing, Intl. Conf. on Pervasive Intelligence and Computing, Intl. Conf. on Cloud and Big Data Computing, Intl. Conf. on Cyber Science and Technology Congress, DASC/PiCom/CBDCom/CyberSciTech, IEEE, 2022, pp. 1–8. doi:10.1109/DASC/PiCom/CBDCom/Cy55231.2022.9927931.

[7] A. Melnikovas, R. G. Lugo, K. Maennel, A. Brilingaitė, S. Sütterlin, A. Juozapavičius, Teaching pentesting to social sciences students using experiential learning techniques to improve attitudes towards possible cybersecurity careers, in: Proc. of the 22nd European Conference on Cyber Warfare and Security, 2023, p. 10. To appear.

[8] R. Pirta-Dreimane, A. Brilingaitė, E. Roponena, K. Parish, J. Grabis, R. G. Lugo, M. Bonders, CyberEscape approach to advancing hard and soft skills in cybersecurity education, in: Proc. of the 25th HCI International Conference, July 2023 (LNCS series), Springer, 2023, p. 19. URL: https://hdl.handle.net/11250/3051549, To appear. URL is provided to the accepted version.

[9] G. Babayeva, K. Maennel, O. M. Maennel, Building an ontology for cyber defence exercises, in: IEEE European Symposium on Security and Privacy, EuroS&P, IEEE, 2022, pp. 423–432. doi:10.1109/EuroSPW55150.2022.00050.

[10] K. Maennel, A. Brilingaitė, L. Bukauskas, A. Juozapavičius, B. J. Knox, R. G. Lugo, O. Maennel, G. Majore, S. Sütterlin, A multidimensional cyber defense exercise: Emphasis on emotional, social, and cognitive aspects, SAGE Open 13 (2023) p. 12. doi:10.1177/21582440231156367.