2024 IEEE 25th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM) | 979-8-3503-9466-5/24/$31.00 ©2024 IEEE | DOI: 10.1109/WoWMoM60985.2024.00016

Enhancing Cybersecurity Training Efficacy: A Comprehensive Analysis of Gamified Learning, Behavioral Strategies and Digital Twins

Yagmur Yigit
School of Computing
Edinburgh Napier University
Edinburgh, UK
yagmur.yigit@napier.ac.uk

Kitty Kioskli
trustilio B.V.
Amsterdam, Netherlands
kitty.kioskli@trustilio.com

Laura Bishop
Airbus Limited
Newport, UK
laura.l.bishop@airbus.com

Nestoras Chouliaras
School of Engineering
University of West Attica
Athens, Greece
nchouliaras@uniwa.gr

Leandros Maglaras
School of Computing
Edinburgh Napier University
Edinburgh, UK
l.maglaras@napier.ac.uk

Helge Janicke
Scool of Science
Edith Cowan University
Perth, Australia
h.janicke@ecu.edu.au

***Abstract*—This paper delves into enhancing cybersecurity training efficacy through an in-depth examination of gamified learning, behavioural strategies, and the deployment of digital twins. It identifies the critical role of behavioural strategies in bolstering cybersecurity defences by influencing human behaviour. The study explores the benefits of gamified learning in engaging participants and improving knowledge acquisition, alongside applying digital twins and cyber ranges in offering practical, hands-on experience. By analysing these methodologies, the paper aims to bridge the gap between theoretical knowledge and real-world application, encouraging the researchers to work on a forward-looking approach to cybersecurity training using these innovative methodologies that are both effective and engaging. Our findings suggest that by creating an immersive, interactive learning environment, it is possible to enhance the cybersecurity competencies of individuals, making them better prepared to navigate the complexities of the digital age. This paper contributes to cybersecurity training by offering insights using innovative approaches for effective training programs that are both engaging and informative, ultimately aiming to bolster organisations' cybersecurity posture.**

***Index Terms*—Cybersecurity, Training, Gamified Learning, Behavioral Strategies, Digital Twins, Cyber Ranges.**

I. Introduction

The widespread adoption of digital technology in modern society has made cybersecurity a critical problem in many industries. The boundaries between the digital and physical worlds are becoming more hazy due to the growth of Industry 4.0, autonomous cars, and the Internet of Things (IoT), which increases the potential consequences of cyber attacks beyond only data integrity and confidentiality. It demands more sophisticated cybersecurity education. Since cyber risks are becoming more sophisticated and can vary from data breaches to cyber addiction, effective cybersecurity training is more crucial than ever.

The primary obstacles to improving the effectiveness of cybersecurity training are keeping the curriculum current with the ever-evolving nature of cyber threats, involving students in meaningful experiences, especially through practical application, and making sure that the material is appropriate for and relevant to all technical skill levels. Measuring the impact of training programs on enhancing cybersecurity practices and behaviours inside enterprises and their efficacy also poses a significant problem. The use of gamification, digital twins, and adaptive learning technologies, as well as a dedication to continual development and alignment with current cybersecurity trends and threats, are some of the creative ways to train design that are needed to address these difficulties.

The use of digital twins in conjunction with gamification and virtual reality (VR) to improve training and learning is examined in [1]. It emphasizes the need for effective ways to manage complicated digital twins by proposing a gamified and VR-enhanced training environment. In addition to outlining the challenges with design and implementation, the research offers a plan for enhancing the efficiency and user engagement of digital twin learning. Creating a shared learning experience repository, providing adaptive and tailored feedback, and designing cooperative and individualized learning environments are all crucial elements. This innovative approach intends to revolutionize the use of digital twins in training and education by bridging the theoretical and practical implementation gaps.

In the context of Industrial Control Systems (ICS), particularly for systems that employ Programmable Logic Controllers (PLC), Tharota *et al.* suggested a training framework to enhance cybersecurity understanding [2]. Recognizing that traditional networked production systems are vulnerable to cyberattacks, the concept offers an interactive, game-based learning environment inside an industrial training setting.

979-8-3503-9466-5/24/$31.00 ©2024 IEEE
DOI 10.1109/WoWMoM60985.2024.00016

Through the integration of attack and defensive strategies in the curriculum, participants get a complete understanding of cybersecurity measures pertinent to industrial systems. Emulation cards, actual PLCs, and simulation tools are used to put this concept into reality, creating a more hands-on learning experience than typical classroom settings. According to participant comments, theoretical knowledge is clearly preferred over practical learning, and suggestions for improved simulation tool support and a more structured educational sequence were suggested.

Digital twins have played a key role in supporting advanced cyber defence training in several international cybersecurity exercises, such as the NATO Locked Shields [3]. The twin provides a unique combination of scalability, configurability, and usefulness through its deployment, whether dispersed for training exercises or centralized for development. Chandrashekar *et al.* presents an innovative solution to enhance cybersecurity awareness and preparedness within critical infrastructure sectors, focusing specifically on a wastewater treatment facility [4]. Through utilising VR and IoT, the research presents a full digital twin system that replicates real-world cybersecurity risks and intrusion detection techniques in an immersive setting. This comprehensive testbed, called SmartWater, aims to give staff members, researchers, and students practical training by enabling them to watch over, manage, and react to fictitious cyberattacks instantly. The effort seeks to improve the cybersecurity competencies of individuals who maintain these vital systems by bridging the knowledge gap between the digital threats that wastewater treatment facilities confront and their physical operations. Through this immersive and interactive platform, the paper demonstrates a novel approach to cybersecurity education, emphasizing the importance of practical, experiential learning in defending against the increasing prevalence and complexity of cyberattacks on critical infrastructure.

This paper analyses behavioural strategies, gamified learning, testbeds and cyber ranges, and digital twins to enhance cybersecurity training efficacy by addressing the above-mentioned critical needs. The remainder of the paper is organized as follows: Section II delves into the behavioural strategies employed in cybersecurity training, emphasizing the importance of influencing human behaviour to strengthen cybersecurity defences. Section III explores the benefits and methodologies of gamified learning in engaging learners and enhancing knowledge acquisition in cybersecurity. Section IV discusses the application of testbeds and cyber ranges in providing hands-on experience and practical skills essential for combating cyber threats. Section V focuses on the transformative role of digital twins in cybersecurity training, highlighting their scalability, customizability, and potential to bridge the gap between theoretical knowledge and practical application. Finally, Section VI concludes the paper.

II. Behavioral stategies

In the contemporary landscape of cybersecurity, the human element remains a critical factor in safeguarding digital assets against evolving threats. While technological advancements continue to bolster defensive capabilities, the effectiveness of cybersecurity measures ultimately hinges on the behaviours and decisions of individuals within organizations. Thus, there is a growing recognition of the importance of behavioural strategies in enhancing cybersecurity training efficacy. Fig. **??** illustrates the skills gap in cybersecurity training efficacy. It highlights the transition needed from current cybersecurity skills to the required future skills to address deficiencies and effectively counter emerging threats.

Behavioural strategies encompass a diverse array of techniques aimed at influencing human behaviour towards desired security outcomes. These strategies often draw from principles of behavioural psychology and organizational behaviour to encourage security-conscious habits and decision-making among individuals. For instance, Adams *et al.* highlight the efficacy of personalized feedback, social norms, and incentives in promoting adherence to security policies and procedures within organizations [5]. By addressing the cognitive biases and social dynamics that influence behaviour, behavioural strategies can effectively complement technical controls in mitigating cybersecurity risks. Similarly, Herath and Rao developed a framework based on protection motivation theory to enhance security policy compliance through the manipulation of perceived threat severity, vulnerability, and self-efficacy [6]. These studies highlight the potential of behavioural strategies to influence human behaviour and strengthen cybersecurity defences.

Several theoretical models underpin the design and implementation of behavioural strategies in cybersecurity training. One prominent model is the Protection Motivation Theory (PMT), which posits that individuals are motivated to engage in protective behaviours when they perceive a threat to their security and believe that they are capable of effectively mitigating that threat [7]. PMT has been widely applied in the development of cybersecurity training interventions aimed at increasing threat awareness and promoting proactive security behaviours [6]. Additionally, the Extended Parallel Process Model (EPPM) offers insights into the interplay between threat severity, efficacy, and message framing in shaping individuals' responses to security messages [8]. By leveraging these theoretical frameworks, cybersecurity trainers can design targeted interventions that resonate with learners and facilitate behavioural change.

Effective implementation of behavioural strategies in cybersecurity training requires careful consideration of best practices gleaned from empirical research and industry experience. Some key best practices include:

- Personalization: Tailoring training materials and interventions to individual learners' preferences, knowledge levels, and learning styles can enhance engagement and motivation [5].
- Social Norms: Leveraging social influence mechanisms, such as peer pressure and social comparison, can encourage adherence to security policies and foster a culture of shared responsibility [6].

TABLE I
CYBERSECURITY TRAINING EFFICACY SKILLS GAP

Cybersecurity Skill Area	Current Proficiency Level	Desired Proficiency Level	Gap Description
Threat Detection	Medium	High	Needs improvement in advanced threat detection techniques and tools
Incident Response	High	High	Adequate current levels, but continuous training is necessary to keep up with evolving threats
Secure Coding	Loa	High	Significant gap in secure coding practices and understanding of security by design principles
Network Security	Medium	High	Requires enhancement in network defense mechanisms and threat monitoring
Risk Assessment	Low	High	Lacks comprehensive risk evaluation methods and mitigation strategies

- Incentives and Rewards: Providing tangible rewards or recognition for demonstrating security-conscious behaviours can reinforce desired actions and motivate sustained compliance [5].
- Ongoing Evaluation: Regular assessment of training effectiveness through metrics such as knowledge retention, behaviour change, and security incident rates enables trainers to identify areas for improvement and refine training interventions accordingly [9].

By integrating evidence-based behavioural strategies, leveraging theoretical models, and adhering to best practices, cybersecurity training programs can effectively engage learners, promote security awareness, and foster behavioural change to enhance organizational resilience against cyber threats.

The recognition of human factors in cybersecurity has prompted a paradigm shift towards a more human-centric approach to security. Gerber *et al.* argue that while technological solutions are essential, they must be complemented by efforts to understand and influence human behaviour effectively [10]. Without the active engagement and cooperation of individuals, even the most robust technical controls may prove insufficient in thwarting sophisticated cyber threats. Thus, cybersecurity training programs must prioritize behavioural change initiatives to cultivate a security-aware culture and empower employees to become proactive defenders against cyber attacks.

Gamified learning represents a promising approach to cybersecurity training that leverages game design principles to motivate and engage learners. By integrating elements such as competition, rewards, and progression, gamified platforms encourage active participation and knowledge retention among trainees [11]. Xioa *et al.* conducted a systematic literature review highlighting the positive impact of gamification on cybersecurity education, including increased motivation, knowledge acquisition, and behaviour change [12]. Furthermore, gamified simulations enable learners to practice cybersecurity skills in a safe and controlled environment, facilitating the transfer of learning to real-world scenarios.

Digital twins offer a novel approach to behavioural analysis within cybersecurity training environments. By creating virtual replicas of individuals or organizational processes, digital twins enable trainers to observe and analyze human behaviour in response to simulated cyber threats [13]. This iterative feedback loop allows for targeted interventions and personalized coaching to address behavioural weaknesses and reinforce desired security behaviours. Furthermore, digital twins facilitate the exploration of complex cyber scenarios and the assessment of trainees' decision-making skills in a risk-free setting, ultimately enhancing the effectiveness of cybersecurity training programs.

To maximize the impact of cybersecurity training, organizations must adopt a holistic approach that integrates behavioural strategies into comprehensive training frameworks. Von Solms and Van Niekerk advocate for multifaceted training programs that cater to diverse learning styles and preferences [9]. By combining gamified learning, digital twins, simulations, and other interactive modalities, organizations can create immersive learning experiences that foster a culture of security awareness and compliance. Moreover, ongoing assessment and reinforcement mechanisms are essential to sustain behavioural change and ensure the long-term effectiveness of cybersecurity training initiatives.

III. GAMIFIED LEARNING

Over recent years, there has been an increased focus within research on the benefits of applying game architecture and mechanics to non-gaming contexts such as learning, with largely positive results [14]. The key objective of gamified learning is to increase engagement with and participation in pedagogical content, to help motivate learners and improve learning outcomes. Research suggests that the benefits of gamified learning reach far further than the intervention itself, improving general attitudes towards a given subject as well as helping users understand how to confidently apply the skill within their own environment [15]. The gamified learning approach is of particular interest within domains such as cybersecurity, where knowledge is often technical or complex as well as dynamic due to continual adaptations to the technologies, processes and techniques utilised by cybercriminals. It is the potential gamified learning has in motivating users to continuously engage with exigent knowledge that makes its application so suitable to cybersecurity.

Human behaviour is believed to be determined by the level of psychological motivation assigned to a particular act [16]. For example, should motivation to complete a course of

training be low, it is unlikely an employee will independently allocate the effort required to ensure the action is undertaken. Motivation can be defined as energy or urge towards completing a specified goal and can be experienced along a continuum from amotivation, through extrinsic motivation to intrinsic motivation [17] [18]. Amotivation is defined as an absence of drive to complete an action, extrinsic motivation is where the drive is determined through fundamental reasoning, and intrinsic motivation whereby an action is completed due to genuine interest or pleasure. Intrinsic motivation is believed to be the most superior form of motivation due to its self-determined nature and is particularly influential within education and learning [19] [18]. Despite its supremacy, there are some tasks humans are expected to undertake that are unlikely to naturally elicit interest or pleasure and, therefore, evoke intrinsic motivation. This includes cybersecurity education, training and awareness programmes that many organisations request their employees undertake to help reduce the probability of attack.

Self-determination theory [18] considers this challenge by addressing how extrinsic motivation can become more self-governed in the absence of intrinsic motivation. Generally speaking, extrinsic motivation can be determined in two ways - either externally via the use of rewards or punishments or internally whereby employees are educated about the true value of conducting a behaviour. Whilst rewards are useful in driving behaviour, it is the internalisation of an action's genuine importance that is more likely to result in an employee independently opting to engage with training despite a lack of interest in its content [20]. Self-determination theory posits three antecedents as key to encouraging self-governed motivation: competence, autonomy and relatedness [18]. These prerequisites suggest that in order for employees to engage with training, they must feel it enables them to achieve personal growth, feel they are trusted to set their own goals in relation to this growth and that the intervention opens doors to further social connection [17] [18]. Any cybersecurity education, training and awareness programme deployed must, therefore, seek to provide employees with the tools required to target these constructs directly. Serious games and gamification, two complementary aspects of gamified learning, have been found to improve motivation and increase competency by providing a fun and engaging learning experience that directly targets self-determined motivation.

Games are ordinarily defined as structured forms of play undertaken by humans for the purpose of fun, e.g., in the form of physical sports such as football or board games such as Chess. In particular, the online gaming industry is a prolific market, with around 40% of the total world population online gamers and 88% of young adults immersed in the online gaming world [21]. Games are, however, now being utilised for more than just pleasure, with their structure and mechanics applied to non-gaming contexts in attempts to evoke similar pleasurable game-like experiences in learning (Hew & Du, 2024). A number of examples include Anti phishing Phil – a mobile application used to educate on the identification of malicious links, CyberCEIGE - training within a 3D virtual world, and Control – Alt- Hack a puzzle card and board game, targeting both end-users and security specialists [22].

Serious games are defined as the use of game architecture in learning to increase player skill in areas such as cybersecurity training, including educational instructions, observation, strategy planning and response simulation [23]. The application of a game-like structure aims to help users consolidate the many elements of cybersecurity behaviours in one space, allowing them to achieve skill mastery through experimentation, often at a much faster pace [24] [25]. Serious games can support self-determined motivation by providing a pleasurable experience that can help increase perceptions of competency and autonomy, e.g., freely practising skills such as the identification of phishing emails under the intervention conditions until the desired behaviours become automatic. Augmented reality has been found to further increase the benefits of serious games as an intervention by fully immersing participants in the learning experience by combining both real and computer-generated worlds [24]. It is, however, important to note that such additions will be a cost to organisations, perhaps making it difficult for small to medium-sized enterprises to deploy.

A compatible yet different concept is gamification, whereby game mechanics are applied to the architecture of a serious game to help improve engagement and productivity and increase motivation to interact [26] [27]. A common example of gamification is seen within the mobile application Duolingo©, where mechanics such as badges, levels, leaderboards, awards, progress bars and challenges are used to support engagement in language education. The use of gamification to support cybersecurity awareness interventions has been found to increase self-determination by providing users with the feedback required to improve perceived competence, an array of options that increase the perception of autonomy, alongside the offer of an online community that helps foster shared learning and competition [28]. For example, user self-efficacy in relation to password generation can be increased by providing progress bars to encourage self-referenced ability and leaderboards to support other-referenced ability [26]. By providing employees with a platform to undertake dynamic cybersecurity exercises via gamified learning, users will be encouraged to continue to engage with content that supports the prerequisites for improved motivation and skill development, driving successful behaviour change.

IV. Testbeds and Cyber-ranges

One of the most critical assets of a company or a system lies in the experience and expertise of the individual users who interact with or control the system. These individuals can be either administrators of the systems, members of staff who interact or who have a certain level of control over several applications on a daily basis or external users or partners. Many recent reports state the lack of properly trained cybersecurity experts who could play a vital role in securing those systems. Except for this scarcity of professionals, a noticeable shortage of essential cybersecurity skills that are

related to their specific roles exists among digital system users [29]. Having identified these needs, Europe has developed the European cybersecurity skills framework that provides a practical tool to support the identification of the skills that are needed for each cybersecurity role [30].

Some years ago, the majority of educational programs within the cybersecurity sector had been awareness campaigns that included lectures or presentations with the main purpose of delivering content to a wide audience without offering tailored training to specific audiences. These campaigns were focused on delivering a lot of information in a short period of time, failing to transfer specialized knowledge. Even if training had achieved an immediate increase in understanding, it had been demonstrated that it did not reflect the long-term understanding of the audience [31]. It was correctly identified that the issue was not the content of the cyber awareness program but the nature of the delivery [32]. It was found that serious games were more engaging and effective than presentations, and thus, many educational programs engaged such activities in their learning programs. One of the major tools to support the enhancement of these skills is the use of hands-on exercises either within an academic environment or through academies, agencies and professional training.

Cybersecurity exercises have become one of the most impactful and efficient methods for instilling essential skills and expertise within the cybersecurity domain, especially when simulating high-stress cyberattack scenarios. These exercises can be tailored to specific domains like energy, transport or aviation and can focus on the technical [33] or business level [34] also covering the NIS_2 requirement for corporate accountability [35]. According to [36]–[38], Cyber Range Exercises (CRXs) play a pivotal role in addressing the cybersecurity workforce gap for organizations. Their findings emphasize how CRXs effectively enhance professionals' skills to combat evolving cyber threats, strengthening overall organizational resilience and security measures. Organized within cyber ranges, these exercises empower organizations to train their personnel to respond effectively during cybersecurity incidents that jeopardize their assets or the entire organizational framework.

A cyber range can be implemented using various technologies spanning from Local Network Virtualization to cloud-based solutions and contained-based platforms. Local network virtualization is ideal for producing customizable environments regarding the network and can be used to offer specialized labs for onsite trainees. Virtualization technologies such as VMware and VirtualBox allow for isolated environments on local machines [39], providing a controlled setting for training. Implementing such ranges requires a large initial financial investment while simultaneously comes with limited scalability. For better scalability, accessibility and efficiency, cloud-based platforms like AWS or Azure are used for many academic institutions and companies [40]. Many scholars use open-source platforms like OpenStack, which offer flexibility and customization capabilities. These platforms can be easily tailored to specific sector scenario requirements [41]. Finally, container-based platforms like Docker can offer lightweight [33] and Kubernetes [42] can offer lightweight, portable solutions. Each platform choice carries implications regarding resource utilization, scalability, ease of use, and security, choosing each one as a cost-benefit exercise that includes available resources and training needs.

V. Digital Twins

With the advent and integration of digital twin technologies, cybersecurity training is experiencing a radical transformation. Digital twins are highly developed virtual models replicating real-world systems, networks, or processes [43]. A basic digital twin configuration consists of a physical object and its virtual equivalent connected via a bidirectional data transfer. Understanding the relationships through intensive data gathering and analysis is the core of digital twin technology. When data is transferred from the physical to the digital realm, it is raw and needs to be cleaned up to provide insights that can be used [44]. Digital twins need the integration of many critical technologies, each ranked according to its degree of development and sophistication. This includes the Internet of Things (IoT) from a networking and Information Technology (IT) perspective, the Cyber-Physical System (CPS) approach from a system engineering and controls viewpoint, and the digital twin concept from a computational modelling perspective, incorporating ML and AI methodologies [45].See Table 1 on digital twins technologies.

Digital twins are becoming essential in cybersecurity education and training beyond their original industrial use. This innovative method uses simulation to provide an immersive learning environment that gives cybersecurity experts a dynamic platform to develop their abilities against constantly changing cyber threats [46]. In cybersecurity training, digital twins represent the fusion of theory and practice by allowing learners to interact with and react to simulated cyber threats in a virtual setting that mirrors their real-world IT and network systems. This methodological innovation makes possible the practical experience necessary to understand the nuances of cyberattacks and the complexity of security procedures [47]. In a safe and virtual environment, trainees are put in actual situations and given the responsibility of navigating the complexities of cyber events, from detection and analysis to containment and remediation. Along with honing technical abilities, this creates a thorough awareness of the cause-and-effect relationships that are fundamental to cybersecurity.

Among the most noteworthy features of digital twins are their scalability and intrinsic customisation. This flexibility allows training programs to be carefully tailored to meet the specific security architecture and threat landscape that apply to a given organization or learner. Digital twins may be scaled and adjusted to fulfil various training purposes, whether it's a simulation of a small business's network or an intricate digital architecture of a significant firm. By enhancing training efficacy and operational preparation, this degree of personalization guarantees that the training is not only pertinent but

TABLE II
CONDENSED OVERVIEW OF DIGITAL TWINS TECHNOLOGIES

Technology Type	Applications	Key Features	Benefits	Challenges
Manufacturing Digital Twins	Production lines, machinery, and product lifecycle management	Real-time monitoring, predictive maintenance, and process optimization	Increased efficiency, reduced downtime, and enhanced product quality	High initial setup costs, complexity of integration
Healthcare Digital Twins	Patient monitoring, personalized treatment plans, and medical device design	Simulations for treatment outcomes, virtual patient monitoring, and device testing	Improved patient outcomes, personalized treatments, and accelerated device development	Data privacy concerns, accuracy of virtual models
Urban Planning Digital Twins	City infrastructure planning, traffic management, and environmental monitoring	Dynamic simulations of urban environments, resource management, and disaster planning	Optimized city planning, reduced environmental impact, and improved emergency response	Scalability, data collection and management challenges
Energy Sector Digital Twins	Power generation, distribution networks, and renewable energy systems	Optimization of energy production, predictive maintenance, and grid management	Enhanced energy efficiency, grid reliability, and integration of renewable resources	Complexity of energy systems, data security concerns
Automotive Digital Twins	Vehicle design, manufacturing, and performance testing	Prototyping, safety testing, and lifecycle management	Reduced time to market, enhanced vehicle performance, and safety improvements	Integration with existing workflows, high computational demands

also in line with the dangers and vulnerabilities that learners are likely to encounter in the real world.

Cyber ranges are advanced, secure virtual environments essential to cybersecurity education because they provide a hands-on method for people, such as cybersecurity professionals, to gain practical skills [48]. ML techniques are being progressively integrated into these virtual training grounds to better address the developing risks within 5G networks, especially in mission-critical scenarios. Under the Horizon 2020 framework, the SPIDER project provides a specialized cyber range to give cybersecurity specialists in the telecoms industry thorough training across a range of 5G network cybersecurity scenarios using digital twins [49]. The SPIDER program focuses on developing people's capabilities and providing them with training similar to ethical hackers. An optional red team may also be charged with finding vulnerabilities and carrying out attacks, while the blue team's job is to identify threats and protect the network during an ordinary SPIDER cyber range training session. In an alternative scenario, automated assault simulations might assume the role of the red team and offer a training sequence of actual attack occurrences. By creating the SPIDER cyber range with digital twins, Rebecchi *et al.* offered a novel solution to the severe lack of highly qualified cybersecurity specialists, especially for 5G networks [50]. It is possible to conduct cyber exercises that provide interactive communication, information exchange, and real-time feedback from network equipment by simulating a personalized 5G network environment. The ultimate objective is to improve cybersecurity professionals' capacity to anticipate and manage vulnerabilities, sophisticated attacks, and security events. To meet real-world learning objectives, this paper describes the architecture of the SPIDER cyber range, highlighting its dependence on sophisticated network management, data processing pipelines, and machine learning. Use scenarios that illustrate the platform's validation and highlight how drastically it might alter cybersecurity readiness and training in 5G.

The development of a sophisticated reconfigurable digital twin aimed at advancing cybersecurity in industrial control systems is presented [51]. Initially conceived as a personal project on the SWaT water treatment plant at iTrust, SUTD, this digital twin was operational and has since developed to assist training, teaching, and research. During cyber exercises like NATO's Locked Shields, it stands out for its ability to quickly replicate different industrial areas and overcome the restrictions of physical testbeds. The design of the digital twin makes it possible to reconfigure seamlessly between domains, improving knowledge of the effects of cyberattacks and the efficacy of defensive programs. The importance of flexible digital twins in safeguarding vital infrastructure is highlighted by this breakthrough, which also opens the door for in-depth cybersecurity research and functions as a critical educational tool.

University production-based engineering courses are the subject of the investigation into the integration of digital twins into academic frameworks [52]. It highlights the role that context awareness plays in improving learning and highlights the ways in which digital twin experiences align with cognitivism, behaviourism, and humanism, three well-known theories of learning. The conceptual design of a pedagogical digital twin, as demonstrated by the research, allows digital twins to accommodate different learning theories and styles. In doing so, it makes the case that digital twins live up to their potential as a valuable educational resource by offering a flexible teaching aid that might enhance students' understanding of and engagement with intricate engineering systems. Digital twins have several educational advantages when used in cybersecurity education. Digital twins provide an effective and interesting interactive learning environment that aligns with modern educational ideals, with a focus on problem-solving, critical thinking, and active learning. To successfully navigate through simulated cybersecurity difficulties, trainees must apply their knowledge and abilities as active participants rather than just as information consumers. This method facilitates the gradual acquisition and retention of knowledge by encouraging a deeper comprehension of

cybersecurity principles and practices.

Moreover, digital twins' integrated instantaneous feedback mechanism functions as an effective learning aid since it reflects each decision and activity in the system with a corresponding response [53]. Trainees may immediately observe the fruits of their labour, understand the implications of various approaches, and adjust their strategies as needed. This real-time feedback loop helps ensure that students understand concepts and grow in their capacity to apply them in real-world contexts. Digital twins are essential to cybersecurity education because they facilitate the development of soft skills such as leadership, teamwork, communication, and technical proficiency in trainees. Digital twins replicate the collaborative aspect of cybersecurity work, which sometimes necessitates collaboration across multiple teams and departments, by enabling trainees to work together when responding to cyber disasters. Trainees gain from this collaborative learning environment by sharpening their technical abilities and developing the multidisciplinary teamwork required to successfully manage the complexities of real-world cybersecurity operations.

A forward-thinking approach to preparing cybersecurity professionals for the needs of the modern digital environment is to incorporate digital twin technology into cybersecurity training. Digital twins offer a dynamic, realistic, and immersive learning environment that has the potential to change cybersecurity education drastically. Training programs maintain program efficacy by staying up to date with the rapidly evolving cybersecurity requirements, ensuring that learners are ready to confront emerging cyber dangers. One of the best ways that cutting-edge technology can transform education and training while setting new standards for cybersecurity readiness and resilience is through the use of digital twins.

VI. Discussion & Conclusion

This research investigated the various approaches—such as gamified learning, behavioural strategies, and inventive usage of digital twins—that can enhance the efficacy of cybersecurity training. Our research suggests that these tactics could significantly boost cybersecurity postures for firms and increase the efficacy of cybersecurity training initiatives. The usage of behavioural techniques in cybersecurity training has brought attention to the significance of human behaviour in the ecosystem. These strategies mould people's decisions and behaviours in a security-conscious way by utilizing principles from behavioural psychology and organizational behaviour. Our research indicates that when training programs are created to address the cognitive biases and social dynamics influencing behaviour, cybersecurity risks may be significantly reduced.

Gamified learning has emerged as a powerful method for enhancing cybersecurity knowledge acquisition and motivating pupils. The integration of game design features into educational settings promotes engagement, motivation, and the application of knowledge to practical situations. Our research validates the idea that gamified learning environments, with their dynamic and competitive nature, can greatly enhance students' engagement and retention of complex cybersecurity ideas. One important step in closing the knowledge gap between theory and practice in cybersecurity training is the use of digital twins and cyber ranges. Digital twins give students a controlled environment in which they can research and respond to cyber threats through simulated, real-world encounters. This interactive learning environment fosters a deeper comprehension of the cybersecurity situation while also improving technical abilities. Our research indicates that digital twins are a priceless resource for creating customized training programs that faithfully represent the wide range of danger scenarios that businesses may encounter. They provide unmatched scalability and adaptability.

In conclusion, gamified learning, digital twins, and behavioural techniques in cybersecurity training programs provide a comprehensive way to train people about the subtleties of the digital era. By demonstrating how these cutting-edge methods could strengthen cybersecurity skills and promote proactive, security-aware cultures, this study advances the discipline. It is crucial that training programs change to give employees the knowledge and abilities they need to protect against these ever-evolving risks in an era of increasingly sophisticated cyberattacks. We strongly advocate for the execution of further research to delve into the long-term effects of these strategies on the cybersecurity fortitude of organizations. It is essential to explore innovative methodologies for augmenting cybersecurity training, aiming to identify groundbreaking techniques that significantly improve resilience against cyber threats. This future research should focus on assessing the sustainability of current practices and their adaptability to evolving cyber threats, ensuring that businesses can maintain a robust defense mechanism in the digital age.

Acknowledgment

The authors would like to acknowledge the financial support provided for the following projects: 'Collaborative, Multimodal and Agile Professional Cybersecurity Training Program for a Skilled Workforce In the European Digital Single Market and Industries' (CyberSecPro) project, which has received funding from the European Union's Digital Europe Programme (DEP) programme under grant agreement No 101083594. The 'Human-centered Trustworthiness Optimisation in Hybrid Decision Support' (THEMIS 5.0) project, which has received funding from the European Union's Horizon Programme under grant agreement No 101121042. The 'advaNced cybErsecurity awaReness ecOsystem for SMEs' (NERO) project, which has received funding from the European Union's DEP programme under grant agreement No 101127411. And 'Fostering Artificial Intelligence Trust for Humans towards the optimization of trustworthiness through large-scale pilots in critical domains' (FAITH) project, which has received funding from the European Union's Horizon Programme under grant agreement No 101135932. The views expressed in this paper represent only the views of the authors and not of the European Commission or the partners in the above mentioned projects.

REFERENCES

[1] A. Bucchiarone, "Gamification and virtual reality for digital twin learning and training: architecture and challenges," *Virtual Reality & Intelligent Hardware*, vol. 4, no. 6, pp. 471–486, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2096579622000675

[2] K. Tharot, Q. B. Duong, A. Riel, and J.-M. Thiriet, "A cybersecurity training concept for cyber-physical manufacturing systems," *Procedia CIRP*, vol. 120, pp. 1375–1380, 2023, 56th CIRP International Conference on Manufacturing Systems 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2212827123009113

[3] C. T. N. C. C. D. C. of Excellence. Locked Shields. [Online]. Available: https://ccdcoe.org/exercises/locked-shields/, Accessed Jan 15, 2024.

[4] N. D. Chandrashekar, K. King, D. Gračanin, and M. Azab, "Design & development of virtual reality empowered cyber-security training testbed for iot systems," in *2023 3rd Intelligent Cybersecurity Conference (ICSC)*, 2023, pp. 86–94.

[5] C. Adams, T. Coughlan, and M. Johnson, "Behavioral strategies for improving cybersecurity awareness and education," *Computers & Security*, vol. 96, p. 101905, 2020.

[6] T. Herath and H. R. Rao, "Protection motivation and deterrence: a framework for security policy compliance in organisations," *European Journal of Information Systems*, vol. 18, no. 2, pp. 106–125, 2009.

[7] R. W. Rogers, "A protection motivation theory of fear appeals and attitude change1," *The Journal of Psychology*, vol. 91, no. 1, pp. 93–114, 1975, pMID: 28136248. [Online]. Available: https://doi.org/10.1080/00223980.1975.9915803

[8] K. Witte, "Putting the fear back into fear appeals: The extended parallel process model," *Communication Monographs*, vol. 59, no. 4, pp. 329–349, 1992.

[9] R. von Solms and J. van Niekerk, "From information security to cyber security," *Computers & Security*, vol. 38, pp. 97–102, 2013, cybercrime in the Digital Economy.

[10] N. Gerber, P. Gerber, and M. Volkamer, "Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior," *Computers & Security*, vol. 77, pp. 226–261, 2018.

[11] S. Deterding, D. Dixon, R. Khaled, and L. Nacke, "From game design elements to gamefulness: defining "gamification"," in *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments*, ser. MindTrek '11. New York, NY, USA: Association for Computing Machinery, 2011, p. 9–15. [Online]. Available: https://doi.org/10.1145/2181037.2181040

[12] Xiao, Hanyu, Wei, Hao, Liao, Qichen, Ye, Qiongwei, Cao, Changlin, and Zhong, Yawen, "Exploring the gamification of cybersecurity education in higher education institutions: An analytical study," *SHS Web of Conf.*, vol. 166, p. 01036, 2023.

[13] M. Grieves, "Digital twin: manufacturing excellence through virtual factory replication," *White paper*, vol. 1, no. 2014, pp. 1–7, 2014.

[14] I. Zadeja and J. Bushati, "Gamification and serious games methodologies in education," in *International Symposium on Graphic Engineering and Design*, 2022, pp. 599–605.

[15] T. van Steen and J. R. Deeleman, "Successful gamification of cybersecurity training," *Cyberpsychology, Behavior, and Social Networking*, vol. 24, no. 9, pp. 593–598, 2021.

[16] M. Touré-Tillery and A. Fishbach, "How to measure motivation: A guide for the experimental social psychologist," *Social and Personality Psychology Compass*, vol. 8, no. 7, pp. 328–341, 2014.

[17] F. Guay, R. J. Vallerand, and C. Blanchard, "On the assessment of situational intrinsic and extrinsic motivation: The situational motivation scale (sims)," *Motivation and emotion*, vol. 24, pp. 175–213, 2000.

[18] R. M. Ryan and E. L. Deci, "Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being." *American psychologist*, vol. 55, no. 1, p. 68, 2000.

[19] R. Martens, J. Gulikers, and T. Bastiaens, "The impact of intrinsic motivation on e-learning in authentic computer tasks," *Journal of computer assisted learning*, vol. 20, no. 5, pp. 368–376, 2004.

[20] E. L. Deci, A. H. Olafsen, and R. M. Ryan, "Self-determination theory in work organizations: The state of a science," *Annual review of organizational psychology and organizational behavior*, vol. 4, pp. 19–43, 2017.

[21] USwitch. (2023) Online Gaming Satistics 2023 kernel description. [Online]. Available: https://www.uswitch.com/broadband/studies/online-gaming-statistics/

[22] M. Hendrix, A. Al-Sherbaz, and B. Victoria, "Game based cyber security training: are serious games suitable for cyber security training?" *International Journal of Serious Games*, vol. 3, no. 1, pp. 53–61, 2016.

[23] S. Kulshrestha, S. Agrawal, D. Gaurav, M. Chaturvedi, S. Sharma, and R. Bose, "Development and validation of serious games for teaching cybersecurity," in *Serious Games: Joint International Conference, JCSG 2021, Virtual Event, January 12–13, 2022, Proceedings 7*. Springer, 2021, pp. 247–262.

[24] M. Salazar, J. Gaviria, C. Laorden, and P. G. Bringas, "Enhancing cybersecurity learning through an augmented reality-based serious game," in *2013 IEEE global engineering education conference (EDUCON)*. IEEE, 2013, pp. 602–607.

[25] S. Hart, A. Margheri, F. Paci, and V. Sassone, "Riskio: A serious game for cyber security awareness and education," *Computers & Security*, vol. 95, p. 101827, 2020.

[26] S. Scholefield and L. A. Shepherd, "Gamification techniques for raising cyber security awareness," in *HCI for Cybersecurity, Privacy and Trust: First International Conference, HCI-CPT 2019, Held as Part of the 21st HCI International Conference, HCII 2019, Orlando, FL, USA, July 26–31, 2019, Proceedings 21*. Springer, 2019, pp. 191–203.

[27] M. S. Castellano, I. Contreras-McKay, A. Neyem, E. Farfán, O. Inzunza, N. E. Ottone, M. Del Sol, C. Alario-Hoyos, M. S. Alvarado, and R. S. Tubbs, "Empowering human anatomy education through gamification and artificial intelligence: An innovative approach to knowledge appropriation," *Clinical Anatomy*, vol. 37, no. 1, pp. 12–24, 2024.

[28] L. Li, K. F. Hew, and J. Du, "Gamification enhances student intrinsic motivation, perceptions of autonomy and relatedness, but minimal impact on competency: a meta-analysis and systematic review," *Educational technology research and development*, pp. 1–32, 2024.

[29] B. J. Blažič, "The cybersecurity labour shortage in europe: Moving to a new concept for education and training," *Technology in Society*, vol. 67, p. 101769, 2021.

[30] J. Hajny, M. Sikora, A. V. Grammatopoulos, and F. Di Franco, "Adding european cybersecurity skills framework into curricula designer," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 2022, pp. 1–6.

[31] J. Blythe, "Using behavioural insights to improve the public's use of cyber security best practices," *Government office for science*, 2014.

[32] D. Crookall, "Serious games, debriefing, and simulation/gaming as a discipline," *Simulation & gaming*, vol. 41, no. 6, pp. 898–920, 2010.

[33] N. Chouliaras, I. Kantzavelou, L. Maglaras, G. Pantziou, and M. A. Ferrag, "A novel autonomous container-based platform for cybersecurity training and research," *PeerJ Computer Science*, vol. 9, p. e1574, 2023.

[34] S. O'Connor, S. Hasshu, J. Bielby, S. Colreavy-Donnelly, S. Kuhn, F. Caraffini, and R. Smith, "Scips: A serious game using a guidance mechanic to scaffold effective training for cyber security," *Information Sciences*, vol. 580, pp. 524–540, 2021.

[35] T. Sievers, "Proposal for a nis directive 2.0: companies covered by the extended scope of application and their obligations," *International Cybersecurity Law Review*, vol. 2, no. 2, pp. 223–231, 2021.

[36] M. Glas, F. Böhm, F. Schönteich, and G. Pernul, "Cyber range exercises: Potentials and open challenges for organizations," in *International Symposium on Human Aspects of Information Security and Assurance*. Springer, 2023, pp. 24–35.

[37] N. Chouliaras, G. Kittes, I. Kantzavelou, L. Maglaras, G. Pantziou, and M. A. Ferrag, "Cyber ranges and testbeds for education, training, and research," *Applied Sciences*, vol. 11, no. 4, p. 1809, 2021.

[38] J. Gomez, E. F. Kfoury, J. Crichigno, and G. Srivastava, "A survey on network simulators, emulators, and testbeds used for research and education," *Computer Networks*, vol. 237, p. 110054, 2023.

[39] M. Thompson and C. E. Irvine, "Labtainers cyber exercises: Building and deploying fully provisioned cyber labs that run on a laptop." in *SIGCSE*, 2021, p. 1353.

[40] O. Darwish, C. M. Stone, O. Karajeh, and B. Alsinglawi, "Survey of educational cyber ranges," in *Web, Artificial Intelligence and Network Applications: Proceedings of the Workshops of the 34th International Conference on Advanced Information Networking and Applications (WAINA-2020)*. Springer, 2020, pp. 1037–1045.

[41] S. Zhou, J. He, T. Li, X. Lan, Y. Wang, H. Zhao, and Y. Li, "Automating the Deployment of Cyber Range with OpenStack," *The Computer Journal*, p. bxad024, 04 2023. [Online]. Available: https://doi.org/10.1093/comjnl/bxad024

[42] J. de Salle, A. Legay, and B. Duhoux. Clustering Hybrid Cyber Ranges for Cybersecurity Education Purposes. [Online]. Available: https://dial.uclouvain.be/, Accessed Jan 15, 2024.
[43] Y. Yigit, L. D. Nguyen, M. Ozdem, O. K. Kinaci, T. Hoang, B. Canberk, and T. Q. Duong, "TwinPort: 5G Drone-assisted Data Collection with Digital Twin for Smart Seaports," *Scientific Reports*, vol. 13, p. 12310, 2023.
[44] Y. Yigit, K. Huseynov, H. Ahmadi, and B. Canberk, "Ya-da: Yang-based data model for fine-grained iiot air quality monitoring," in *2022 IEEE Globecom Workshops (GC Wkshps)*, 2022, pp. 438–443.
[45] Y. Yigit, O. K. Kinaci, T. Q. Duong, and B. Canberk, "Twinpot: Digital twin-assisted honeypot for cyber-secure smart seaports," in *2023 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2023, pp. 740–745.
[46] Y. Yigit, B. Bal, A. Karameseoglu, T. Q. Duong, and B. Canberk, "Digital twin-enabled intelligent ddos detection mechanism for autonomous core networks," *IEEE Communications Standards Magazine*, vol. 6, no. 3, pp. 38–44, 2022.
[47] Y. Yigit, C. Chrysoulas, G. Yurdakul, L. Maglaras, and B. Canberk, "Digital Twin-Empowered Smart Attack Detection System for 6G Edge of Things Networks," in *2023 IEEE Globecom Workshops (GC Wkshps)*, 2023, pp. 178–183.
[48] S. Vakaruk, A. Mozo, A. Pastor, and D. R. López, "A digital twin network for security training in 5g industrial environments," in *2021 IEEE 1st International Conference on Digital Twins and Parallel Intelligence (DTPI)*, 2021, pp. 395–398.
[49] C. Xenakis, A. Angelogianni, E. Veroni, E. Karapistoli, M. Ghering, N. Gerosavva, V. Machamint, P. Polvanesi, A. Brignone, J. N. Mendoza, and A. Pastor, "The spider concept: A cyber range as a service platform," in *EUROPEAN CONFERENCE ON NETWORKS AND COMMUNICATIONS (EUCNC2020), VIRTUAL*. Zenodo, 2020.
[50] F. Rebecchi, A. Pastor, A. Mozo, C. Lombardo, R. Bruschi, I. Aliferis, R. Doriguzzi-Corin, P. Gouvas, A. Alvarez Romero, A. Angelogianni, I. Politis, and C. Xenakis, "A digital twin for the 5g era: the spider cyber range," in *2022 IEEE 23rd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2022, pp. 567–572.
[51] A. P. Mathur, "Reconfigurable digital twin to support research, education, and training in the defense of critical infrastructure," *IEEE Security & Privacy*, vol. 21, no. 4, pp. 51–60, 2023.
[52] J. David, A. Lobov, and M. Lanz, "Learning experiences involving digital twins," in *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, 2018, pp. 3681–3686.
[53] Y. Yigit, I. Panitsas, L. Maglaras, L. Tassiulas, and B. Canberk, "Cybertwin: Digital twin-boosted autonomous attack detection for vehicular ad-hoc networks," 2024.