Computer Standards & Interfaces 95 (2026) 104030

Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

Human-centered interface design for a dynamic cyber-risk group-based training game

Tony Delvecchio [a,*], Sander Zeijlemaker [b], Giancarlo De Bernardis [a], Michael Siegel [b]

[a] Cybersecurity Laboratory, BV TECH S.p.A., Milan, 20123, Italy
[b] Cybersecurity at MIT Sloan, Sloan School of Management, Massachusetts Institute of Technology, Cambridge, MA, USA

ARTICLE INFO

Keywords:
Human-centered interface design
Dynamic cyber-risk training
Gamification
Team/Group-based training

ABSTRACT

This study presents the benefits of employing a gesture-based natural user interface (NUI) for a scientifically grounded cyber-risk management collaborative game. Such a human-centered interface facilitates group-based training and enables board members to achieve better results collectively compared to operating individually. The main contribution of this tool is to enhance the group training leveraging on collective intelligence. To show that, the results and learning paths of single users and groups acquired from this game are compared. Moreover, the collaborative game provides executives and business leaders with insight into cyber-risk management issues, thereby improving their results through deeper learning. This work demonstrates that the interface is the key factor in the success of group cooperation. The idea, the design, and the improvement of the NUI are critical to make it possible to achieve these results.

Contents

* Corresponding author.
E-mail address: tony.delvecchio@bvtech.com (T. Delvecchio).

https://doi.org/10.1016/j.csi.2025.104030
Received 15 April 2024; Received in revised form 8 April 2025; Accepted 1 June 2025
Available online 21 June 2025

1. Introduction

Most cyber-risk management research has primarily focused on individuals [1] and groups under stress [2]. However, due to international and regulatory developments, such as Cyber Security Rules of the Security Exchange Committee, Network and Information Security directive, and Cyber Resilience Act in Europe, bringing cyber-risk to the forefront in boardrooms [2–5], new approach paradigms are required. Consequently, cyber-risk management decisions are now made in groups [6]; however, not everyone in the group has a solid background in IT or cybersecurity [7]. In addition, the group's strategic dialog focuses on the financial, operational, and business context of cyber-risk [2,5]. Considering that collective intelligence differs from individual intelligence because it depends on collaboration and diversity among decision-makers, as demonstrated by Woolley et al. [8], Kendon [9], and Malone [10], we investigated the potential benefits of collaborating in cyber risk management investment decision-making in [11]. It has become increasingly apparent that human–machine interaction strengthens collaboration and decision-making [12], and metaphors appear to assist business practitioners in acquiring a particular management skill [13] required in business training settings. Therefore, to harness groups' collective intelligence, we designed and implemented a gesture-based natural user interface (NUI) based on the results obtained by Jalali et al. [1]. In this game, single players manage their investments in Preventive, Detective, Responsive cybersecurity measures by using a dashboard interface. Starting from this game perspective, we used the Rapid Iterative Testing and Evaluation (RITE) method to identify the most appropriate metaphor for our collective approach. Finally, we refined this metaphor using the Mechanics, Dynamics, and Aesthetics (MDA) framework. The results of this study revealed that the game enabled users to overcome the difficulty of managing cybersecurity [14] and addressed decision-makers' tendencies toward misperceiving security levels [1], excessive reliance on off-the-shelf solutions, underestimation of cyber threats [1] and their repercussions [15], as well as prioritization of other business activities [16]. Furthermore, it provides an accessible and non-technical explanation of cyber-risk management, recognizing the varying roles and levels of understanding and awareness among board members and executives. Section 2 describes the literature to which we refer. Subsequently, in Section 3, we delineate the steps that enable us to design, develop, and refine the human-centered interface to its final form. A description of our experiment is provided in Section 4 where, we had users engage in individual simulation training with a predetermined attack scenario to establish a reference baseline of performance. Subsequently, the same scenario is presented to a team or group of users, allowing us to identify the effects of diversity and collaboration. Section 5 elaborates on our research insights in greater detail.

2. Literature

This study bridges two different research areas. One area explores the complexity of cybersecurity and the necessity for simulations and training. Furthermore, the other area considers how a NUI could leverage the collective intelligence of decision-makers, enabling them to approach cybersecurity issues more freely without being constrained by system interfaces. The most relevant works we used as the baseline for this research, with the aim of narrowing the gap between these two areas of research and discovering where they intersect, are presented in this section.

2.1. Complexity of cybersecurity and decision support tool usage in cybersecurity decision-making

Members of the decision-making team should understand the impact of their budget allocation decision on cybersecurity risk; however, nowadays, they are usually not aware concerning the topics at hand. The changing internal (including, people, processes, technology, suppliers, and priorities) and external (including, adversarial evolution, emerging attacks, and remediation of cyber incidents) [14] environments serve as indicators of the complex nature of cybersecurity [1,2,17]. Decision-support tools that enable access to and management of cyber-risk can assist decision-makers in overcoming this complexity and pressure to act. Such tools can provide reports on adherence to security frameworks (such as National Institute of Standards and Technology [NIST] and Cybersecurity Capability Maturity Model [C2M2]) or facilitate comparison with positioning benchmarks, legislative compliance, and breach response plans [18]. While near real-time dashboards offer a significant improvement, they may fail to alleviate the myopic bias of prioritizing short-term gains over long-term effects (as highlighted out by Sterman [19]). This underscores the importance of exploration and training in the decision-making process for cybersecurity budget allocation.

2.2. Need for exploration and training

Simulation-aided serious games translate systems science and simulation modeling into learning experiences [20,21]. They capture human behavior and contribute to knowledge retention, behavioral change, and soft skill development. In the field of simulation-aided serious games, a set of games that focus on training decision-makers to cope with the complex nature of the cyber-risk landscape is already available. For instance, consider the following examples:

- Jalali et al. [1] focus on the individual training of investing in security measures while running a fictional company;
- Zeijlemaker et al. [2] focus on the collective management of an organization by allocating resources and surviving cyberattacks. The game is played competitively (and, therefore, under pressure);
- Armenia et al. [17] focus on performing cyber-risk management for small-medium entities.

All of the aforementioned games recognize the importance of improving decision-making but fail to consider the significance of decision support tool interface design in a collaborative setting involving decision-makers who have no ties to technology or cybersecurity. This highlights the critical role of user interfaces design in strengthening the understanding and awareness of decision-makers, as well as fostering collaboration in the decision-making process [22].

2.3. Criticality of a successful interface design

In this context, the ability to effectively interact with machines plays a fundamental role in decision-making [23]. Most modern interfaces convey communication through verbal and, above all, gestural channels, allowing interaction with digital devices to be more natural even for people with different types of motorial or intellectual disabilities. The same was demonstrated by Gong et al. [24], Braun et al. [25], and Francisco-Martínez et al. [26]. By operating with such tools in

an almost unconscious manner, without consciously considering how to interact to achieve the expected result/behavior from the device being used, the human brain manages to focus on the issues it is dealing with. As demonstrated by Pietriková and Sobota [27], this phenomenon becomes even more evident when interactive methods are structured according to a game-based approach that leverages a supporting metaphor capable of conveying semantic information to users. In this way, learning is unconsciously facilitated, much like in the case of video games.

2.3.1. Natural human–machine interfacing

From its initial conception [28] and subsequent redefinitions [29], the NUI has been regarded as the most effective means of bridging the communication gap between humans and computers. It enhances the capabilities of expert users while simultaneously enabling inexperienced users to become proficient and efficient in a short amount of time. In addition, according to Wigdor and Wixon [28], an NUI must be designed and built basing on some key principles. The first principle, upon which the intuitiveness of an interface is based, is the concept of *affordance* [30]. Gibson defines affordance as the property of the environment or the context to "suggest" and support an action by someone, and simultaneously, that action, being the right one to do, should be performed in such a manner. This action, of course, should produce the expected effect. In addition, to perfectly respect the property of affordance, the environment should also "suggest" the correct subsequent action that must be performed by the user. *Scaffolding* is the second principle. It is a principle emerging in psychology, which can aid developers in achieving natural interaction. It fosters autonomous learning by employing actions that encourage users to develop their cognitive, emotional, and psychomotor skills. This concept was initially introduced in the field of language learning by Jerome Bruner in the 1950s, and given its current definition in 1986 [31]. A more comprehensive definition was provided by Lajoie [32], who adopted a classical approach: "A scaffold is, by definition, a temporary entity that is used to reach one's potential and then is removed when learners demonstrate their learning". It may be applied to different contexts, including human–computer interaction. The cornerstone of this principle is to break down the learning process into small steps, focusing on solving manageable problems that can be addressed with suggestions or guidance. Through solving such problems, users acquire the know-how to progress along the learning journey, propelled by small successes and fueled by curiosity for active exploration. The third and fourth principles are closely related to each other. The third principle is the concept of *seamlessness*, which originated in a context entirely detached from the IT realm [33]. It is also very pertinent in the creation of natural interfaces. The goal of such interfaces is to immerse the user in a state of mental excitement, thereby enhancing receptivity through enthusiasm. In this mindset, users can effortlessly and pleasantly learn from the system itself in real-time, resulting in a seamless experience. Such an experience generates what is known as the suspension of disbelief effect, wherein what was previously considered merely imaginary suddenly becomes tangible. Consciousness accepts something as true or sufficiently realistic, even if it acknowledges that certain things cannot happen or exist in the real world (such as the possibility of zooming in on a cell phone image, which is not possible with a real image). Approaches that extend interactions with interface elements beyond what is physically natural are based on super-realism [34]. *Super-realism* is, therefore, an intuitive extension of reality achieved through dynamics that facilitate fluid, natural experiences by imitating physical interactions of the real world and extending them beyond what is possible within it. Although conceptualized in different historical periods and contexts, this principle is not necessarily confined to information technology, Wigdor and Wixon [28] identify the aforementioned principles as the basis for realizing natural interaction. Through these principles and expedients, an incremental experience can be created wherein the user is led to familiarize themselves with the environment and engage in basic interactions while being stimulated to explore what is reproduced in the real world. A natural interface must replicate users' capabilities, respond to their needs and preferences, leverage what they already know how to do, and provide them with an easy method to do it. It must consider users, their behavior and attitudes, and their sensations during the usage experience. Consequently, it must result from an organic process in which the technological potential is suitably and rigorously organized to reflect human capabilities and comprehensively satisfy their interactive needs.

2.3.2. Gesture language

The use of gestures in human–machine interaction is a diverse and multisectoral subject of study. Research on languages, gesture, and non-verbal communication, intended as functional tools for human activities and social interactions, has been conducted in the fields of anthropology and psychology [9,35–37]. Additionally, it has been demonstrated that constructive cooperation is accompanied by non-verbal communications. In the IT field as well, numerous studies have focused on gestural interaction. Since 1980 [38] on multimodal interfaces), research has been ongoing in both theoretical approaches [39–45] and specific uses of gestural-based interfaces [37,46–49]. Given these considerations, it is not surprising that many studies in the 2000s focused on the use of gestures to reduce the communication gap between humans and electronic equipment [50–53]. In building the NUI proposed in this paper, gestural languages are a crucial point because, as demonstrated by Soro et al. [54], multitouch systems that allow the exploitation of gestures in a collaborative environment are more efficient than traditional interfaces.

2.3.3. Metaphors, methods, and frameworks

One of the fundamental characteristics of an NUI is the need to ensure that the user is guided through a rapid learning process to create a funny and stimulating experience with movements and interactions that appear "natural" to users. To fulfill the requirement of naturalness, it is essential to base the interactions and the entire graphical interface on a strong metaphor, which is also considered a cornerstone by Bruce "Tog" Tognazzini [55]. A specially tailored method for the design and development of natural interfaces is RITE [56–58], through which interactions can be perfected while simultaneously guaranteeing rapid progression of the designs. In addition to the fields of video games and academic education, the RITE method is also used in more concrete-application fields such as the creation of the NUI for Microsoft Surface [59] or, recently, in the development of human–machine interfaces to support mode awareness in different automated driving modes [60,61]. Once the most appropriate metaphor has been identified, different and more advanced versions should be developed. In order to effectively refine the chosen metaphor, a framework called MDA has been adopted. Ideated by Hunicke in 2004 [62], it is now a widely used tool in gamification models for education [63–67].

2.4. Contribution to the literature

The benefits and costs of investing in cybersecurity are well understood by those with adequate training in the matter and, above all, who hold responsibility roles in this domain. However, these professionals cannot operate independently from their colleagues because the decision-making process regarding cybersecurity investments is only a part of the overall corporate strategic investment decision process, which is a collaborative effort. Not all members of such group have specific skills in the field of cybersecurity; indeed, they often possess very different backgrounds and expertise. In such a scenario, investing money on cybersecurity may be perceived merely as a cost by some of them. Those with technical skills in the cybersecurity field, on the other hand, tend to emphasize that this assumption is fundamentally flawed and that such expenditures must be regarded as investments. The gamification process of the system proposed by Delvecchio et al. [11]

is described in detail here, focusing specifically on how the human-centered cybersecurity interface has been designed and developed. The game aims to provide a tool tailored to operate in a critical domain (such as a board briefing). Thus, it is capable of supporting board members, business leaders, and executives in promoting the understanding of benefits (or risks) that stem from investment (or lack thereof) in cybersecurity, even for individuals with education and technical skills in fields remotely far from cybersecurity. Such tool comprises a collaborative system with natural interaction that can free the decision-making process from the need to learn how to operate the system itself. Consequently, this system guarantees a rapid learning curve through simple, automatic, unconscious, and above all, engaging interaction. In emotionally charged situations, users are guided to focus on the work topic and learn, through game dynamics, the notions that the tool aims to convey. The process unfolds rapidly and captivates users, inviting the "players" to improve the obtained results by starting another game, thus generating an unconscious learning mechanism on the subject at hand.

3. Research design

In the previous section, we explained the critical role of interface design in strengthening collaboration and decision-making. Regarding our research design, we repurposed a well-regarded executive training simulation [1] with a new user interface to bolster collaboration within the decision-making process. Additionally, we devised a tool (called Risk-Profit Matrix) to evaluate this collaboration. Moreover, we provide a detailed account of the entire process that led us to consider the selected interface and its refinement.

3.1. Explaining the executive training simulation

We utilized a version of the cybersecurity game by Jalali et al. [1], which is scientifically grounded in system dynamics and control theory. This game mimics the strategic decision-making environment for investing in cybersecurity. Decision-makers must aim to maximize business performance while strengthening the security posture of the organization to withstand cyberattacks. Decision-makers can allocate their yearly budgets (in %) to Prevention, Detection, and Response, with allocations ranging from 0% to 5% of the total information technology budget. The game spans five virtual years, during which company profits are generated every month, and cyber-attacks that may impact the company's revenues could be occur. The winner of the game is the participant with the highest accumulated profits over the five-year period, i.e., whoever minimizes the overall total cost for the company (sum of cybersecurity investments and revenue losses caused by cyber-attacks). We repurposed this game and redesigned its interface to create a collaborative setting for decision-makers with limited knowledge of technology and cybersecurity.

3.2. Detailed metaphor design and finalization

The entire process of designing the metaphor and finalizing it is described step by step in this section.

3.2.1. Choosing the reference metaphor through RITE method

Among the basic characteristics of an NUI, there is the need to guarantee that the user is led to guided and rapid learning through a funny and stimulating experience, and, above all, through movements and interactions that seem "natural" to those who use them. Creating an appropriate metaphor involves two steps. First, it must be understood whether the system design elements effectively communicate the metaphor to the user. Second, it is necessary to ascertain whether the chosen metaphor makes sense for the user, i.e., whether it aids in their learning process, while respecting the need for learning to be progressive and fun. The RITE method, specifically tailored for designing and developing gestural interfaces, facilitates the perfection of interactions while ensuring rapid design progression. Based on the definition of a metaphor, the method allows it to convey the underlying metaphor more effectively. In particular, it aids in metaphor selection and, simultaneously, allows the user to focus on the feedback and previews necessary for effectively communicating such metaphor. In scaffolding, RITE precisely enables us to address the needs of designers. It supports users and guides them toward successfully completing small learning tasks. The prototype of the system undergoes an iterative testing process, allowing designers to understand whether the metaphor communicates or not. By refining certain details and continually presenting the new prototype to users, it becomes easier to understand and more enjoyable to use each time. Through this process, we can also quickly identify the problems that users are facing and make appropriate improvements. Gradually, the design elements of the metaphor are refined, enhancing its the communicativeness. Simultaneously, the second key point, ascertain whether the chosen metaphor makes sense for the user, becomes preponderant, shifting the focus to understanding whether and to what extent the metaphor facilitates the user's learning process, helping them become experts while maintaining a high level of enjoyability. To pursue this aim, the RITE method involves expanding the range of communication by creating and proposing multiple metaphors in parallel. Once these metaphors have been submitted to the sample users, the results can be compared, and ultimately, the best-performing one is selected. The recursive application of RITE allows, for example, the identification of various problems and to find a suitable solutions for them. This, consequently, improves the task performance. Simultaneously, it helps remove elements that can create confusion and increases the number of elements supporting the interface. Finally, comparing the performances of different metaphors reveals the different strengths and weaknesses of each one. The RITE method can be summarized in the following three steps:

- Define different metaphors;
- Submit these metaphors to a set of standard users;
- Choose the one that will prove to be the most congenial.

Four metaphors were primarily identified and tested for this work. Two of them have proven to be more suitable for single users, while the other two are more suitable for multi-users:

1. **Classic sliders**. Three sliders corresponding to the input parameters of the game by Jalali et al. [1] (Prevention, Detection and Response), which fully align with the basic model (a web-based interface currently implemented on Forio, https://forio.com), are presented to the user. Additionally, the interface includes a graph displaying the outcome of the simulation (with the final value of the accumulated profit);
2. **TV knobs**. The user sees an old-fashioned television with three knobs, each representing one of the three input parameters of the model (Prevention, Detection and Response). By turning these knobs on the TV, the image gradually becomes clearer. The clearer the image on television, the greater the accumulated profit;
3. **Potions**. Three colored bottles represent the three input parameters (Prevention, Detection and Response) of the game by Jalali et al. [1]. By mixing different doses of the three potions in a cauldron, one must attempt to obtain a target color that represents the best possible performance;
4. **Inverse Roulette**. Users are given the opportunity to "bet" on what the best cybersecurity measures might be. Such measures affect the European roulette gaming table on which the attacker bets. Attackers' bets are removed (Response measure), blocked (Detection measure), or prevented (Preventions measure) at each measure chosen by the defender. After each session, an index of the effectiveness of the combination of choices is provided through the metaphor of the roulette game.

Fig. 1. Desktop metaphor with Classic sliders. Rational and immediate visualization that is not very cooperative and too desktop-oriented.

For each one of these metaphors the RITE method has been applied in order to understand:

- Does the metaphor convey the message correctly?
- Does the metaphor make sense to the user?
- Does feedback analysis show that the simple learning tasks have been comprehended?

The interface for solution 1 was previously implemented in a study conducted by Jalali et al. (2019) (see Fig. 1). This and the other three solutions created in a minimal version, were compared with each other. The comparison revealed that the first solution is direct and functional but is more oriented toward classic device and interfaces types, such as those used for desktop PCs. The second solution, resembling a television interface, was decidedly more game-based and allowed for quicker learning of the interactive methods Fig. 2. Applying the RITE method to this interface it immediately showed some issues. First of all, it was not easy to understand how much to turn the knobs in order to translate this movement to investment in the three measures of intervention. So the SLTs were not well achieved. Moreover, there was not an idea of what to represent on the television monitor. The interface was then improved by letting the knobs to turn and reach only five positions in order to better align the use of a knob to the amount of cybersecurity investment (ranging from 1 to 5%). That improves the comprehension of the SLTs but there was still the poor relevance of the image represented on the television (Fig. 3). So, in order to better express the meaning of the metaphor it was proposed another improvement by showing the writing "Clean" on the TV and trying to make it as readable as possible Fig. 4. But the feedback analysis showed yet less relevance. Moreover the players tend to not interact much with each other since each knob could be touched by a single player each time. Thus, akin to the first solution, it seemed to be oriented toward a single-user environment. So the RITE method tell that this solution assure a quite good SLT learning and is easily understandable, but the metaphor has little relevance with the topic and group interactive skills are not emphasized. Solutions 3 and 4, on the other hand, immediately demonstrated greater aptitude in multiplayer environments and were thus excellent for teamwork. In the former, users poured the contents of a flask into a cauldron, observing the color change after each interaction Fig. 5.

This interface offers players a solution that enhances superrealism and, probably for this reason, none of the players hesitated to use one of the three flasks to pour its contents into the cauldron so as to be able to see the exciting effect of the smoke produced and the color change into the cauldron Fig. 6. However, although exciting, this solution did not guarantee the ability to fully understand the relevance of "pouring" one of the components of the potion because it was difficult to associate this action with an investment in Prevention, Detection or Response. Furthermore, even how much to invest, or in this case pouring by using a single flask, became difficult to understand. The next version circumvented this last problem by allowing discrete quantities of the components to be poured: each flask was in fact equipped with five graduated levels. However, once the contents of the flask were poured into the cauldron, this action remained irreversible. The subsequent iterative tests carried out on this interface concerned the color that could be obtained as the final product. But the only solution found, aiming for the "pure" white, was difficult to obtain due to the small difference in the different shades forcing designers to find further measures for differentiation (more or less high smoke) Fig. 7. Finally, once again, the metaphorical relevance to cybersecurity was not high. In conclusion, the RITE established that, despite a good learning capacity of the SLT, a high interactive capacity and a highly attractive component, this metaphor was not ideal to support the concept of investments in cybersecurity. The last interface aimed to provide a metaphor with greater relevance to economic issues. The initial version submitted to RITE only presented a screen with a classic roulette table on the left and a table with the intervention measures that could be adopted to reduce the possibility of a potential attacker betting (Fig. 8). Learning the SLT was simple but the correspondence with categories of intervention measures (Prevention, Detection and Response) was poor and this, evidently, also affected the players' ability to interact with each other. In the second iteration, we therefore focused on differentiating the defenders' betting areas, improving this aspect above all and obtaining a stronger correspondence with the intervention measures in cybersecurity (cybersecurity parameters) and in the third iteration, chips of different colors were also adopted (Fig. 9). With these measures, we obtained easy learning of the SLT, better understanding of the context, improved group interactive capacity and above all, the ability of the underlying metaphor to perfectly communicate the message.

Although this solution of the cauldron was the most congenial for achieving the effect of suspension of disbelief, its relevance to the topic and the poor control of "how much to invest" and a poor attendance with economic meaning made it less of a priority compared to the roulette one. In fact, by utilizing roulette chips, not only did the mutual

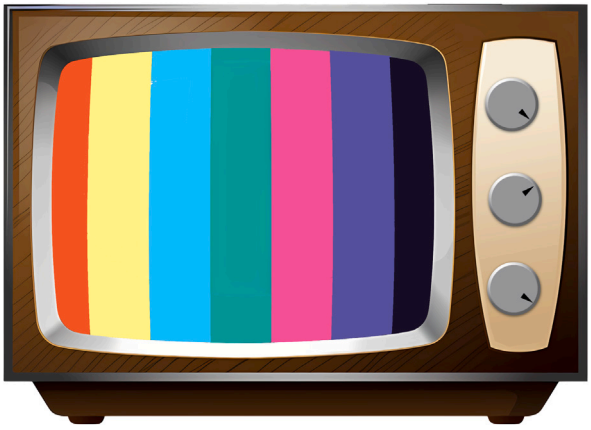


Fig. 2. Television metaphor. The starting point, each knob is associated with a kind of interventions in cybersecurity (parameters).

Fig. 3. Television metaphor. Each knob can be rotated in five defined positions.

interaction between the participants in the game increase but it was also possible to revert to the choices made (by moving the chips to another cybersecurity measure and, in doing so, altering the kind of investment/measure based on the bet). Finally, there was also a better metaphorical correspondence between the final result (the victory of the roulette game) and its relative significance (accumulated profit compared to the compromised and at-risk resources resulting from the original game model [1]. All these factors make the "Inverse Roulette" metaphor more congenial than the others. Therefore, this metaphor was selected for refinement (Fig. 10).

3.2.2. Refinement of the metaphor using the MDA framework

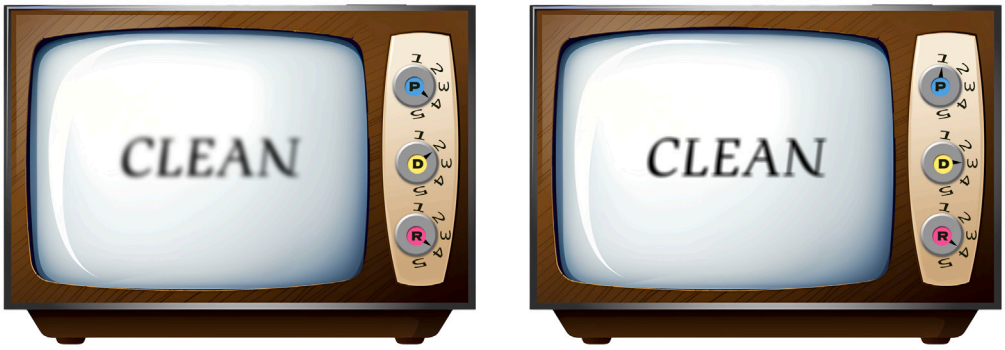
Once the most appropriate metaphor is identified, the refinement process commenced. To create a natural game-based interface, an established framework from the field of the videogame industry, is adopted: **MDA**. This framework does not provide guidelines but serves as a powerful support tool for design, as it helps in independently focusing on these three elements. They are closely intertwined yet distinct, allowing for separate examination while maintaining the overall vision. **Mechanics** of software encompass its functions, outlining the actions users can perform and the objectives achievable through these functions. **Dynamics**, on the other hand, define the rules of human–machine interaction and, therefore, determine the actions and behavior through which the user can operate with the machine to exploit the functions made accessible by the mechanics. Thus, they possess a predictable character (i.e., the rules cannot be bypassed) that simultaneously, cannot be completely determined (i.e., the methods of use can vary from user to user). While talking about interfaces, it is relevant to identify the "object", that are the elements the interface is composed of. Such "objects" can be distinguished as *primary* and *secondary* and are directly and unequivocally associated with these two elements. The former are linked to mechanics and represent what the user understands as the domain of the application and its ultimate purpose. The latter encompasses the control tools through which the user can operate, so are related to the dynamics. The final cornerstone of the MDA model is **Aesthetics**. Through this, it is possible to focus on the set of sensations that a user experience evokes in human beings, ensuring that it is exciting, compelling, and comfortable. Above all, the fact that users do not want to stop using the game, and that they desire to repeat the usage experience as soon and for as long as possible, is crucial. The objective, therefore, is to transmit domain knowledge and knowledge of the tools so that the users are guided through a direct, active, and engaging learning path step-by-step. They will learn both the context and the dynamics of the interface by being instructed on what can and cannot be done in an even more efficient way compared to real experience. The user first learns the domain (Mechanics) through basic functions and is then gradually accompanied by active and proactive discovery of the other functions (Dynamics), proceeding with small steps, recording "successes" on increasingly complex tasks. At the same time, we must ensure that the users are always satisfied with the experience they are having (Aesthetics). By applying the MDA framework to the Inverse roulette metaphor, the functionality (i.e. betting) can be easily identified. This includes the *mechanics* of the interface and the primary objects of the metaphor: *the chips*. The rules according to which the interface works, the *dynamics* – i.e., what regulates the user's actions and behavior – are represented by how and where to move the chips, therefore, identifying the secondary "objects": *the betting areas*. Finally, *aesthetics* are represented by the objective of the game, i.e., reaching the final state of the system (placing bets, effects of the defenders' bets on the roulette table, starting the simulation, and obtaining the result) through *captivating graphic techniques*. *These techniques should be immediately clear and understandable, pushing the user to want to play again* to achieve a better result. An essential component for natural interface rendering is the ability of the metaphor to exploit properties such as *scaffolding* and *affordance*. The gestural language created for the interface involves moving chips from the collection area to the betting areas. To facilitate user learning, graphic devices will be implemented to help users understand both how to accumulate chips for a bet and how to move the chips to bet on one of the intervention measures. Correspondingly, the effect of the bet will then be displayed in the central area of the screen (roulette carpet). Utilizing the MDA model, has facilitated the design and refinement of the NUI focusing on enabling users to:

- understand the domain (related to primary objects/mechanics);
- acquire knowledge of available tools (secondary objects/dynamics);
- have an experience so pleasant that you willing to repeat it as soon as possible.

The whole process from the adoption of the RITE method to the refinement process through the MDA framework is represented in Fig. 11.

3.2.3. Brief description of the game interface and intervention measure identification

The screen resembles a modified roulette table appropriately named "Inverse Roulette" because the bets allowed to users are not the classic ones of the roulette game but operate inversely. Although the classic roulette carpet of European roulette is represented with numbers from 0 to 36, the actual interactive areas – where users can operate – are defined by the colored regions surrounding the roulette carpet on three sides. Users will be prevented from betting on numbers from 0



(a) Television Metaphor. Approaching to "Clean" (b) Television Metaphor. Best "Clean"

Fig. 4. Television Metaphor. Locking for the best combination.

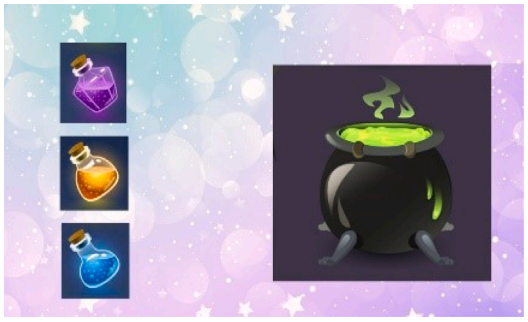


Fig. 5. Potion metaphor. Starting point: each potion represents a kind of interventions in cybersecurity (parameters). (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

Fig. 6. Potion metaphor. Smoke produced after pouring a potion and color change into the cauldron. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

to 36, as this area is intended solely to represent attacks (potential and actual) and to demonstrate the effects of the investments that the defenders (the company) choose to adopt through investments in cybersecurity. Betting is possible only within the colored areas surrounding the roulette carpet represented by 15 colored regions, each corresponding to a field of intervention in cybersecurity where the company can invest to mitigate threats. In order to understand what these areas represent and why they have been chosen, it is necessary to refer to the NIST cybersecurity framework, where five different functions (identify, protect, detect, respond, and recover) are defined. The simulation game [1], which forms the core of the system, simplifies this classification by grouping them into three categories. The first category, achieved by merging the "identify" and "protect" functions, combines all actions that can help protect computer systems from cyberattacks and is called "Prevention" (P). Likewise, all capabilities that help mitigate attack damage and fall under "respond" and "recover" function, are grouped as "Response" (R). The "Detection"(D) function is not combined with any other action and represents the measures used to detect systems that are at risk of or currently under attack. In the original game a parameter for each function (P, D and R) is used. With the "Inverse Roulette" it was deemed necessary to provide users with as many choices as possible because utilizing only three parameters would have resulted in a drastic reduction in their ability to interact with the roulette game plan. In addition, it was necessary to ensure that these decisions could be traced back to P, R and D parameters and that for each category the same number of measure can be selected. To address this requirement, it was decided to examine each category of the NIST framework to understand how to group those belonging to the same function while adhering to the grouping required by the model. Fig. 12 illustrates how some of the NIST subcategories have been grouped in order to identify 15 intervention measures, or parameters, divided into the three families (5 parameters for each category) corresponding to the Prevention, Detection and Response measures. The table in Fig. 12 summarize the intervention measure name and the NIST category IDs which the measure refers to. On the Inverse Roulette table, the name of the parameter is indicated in each area surrounding the carpet and colored in Blu (Prevention), Yellow (Detection) and Violet (Response). When the relevant area is "activated" (when a user is about to place a bet on it by moving chips), a *tooltip* appears with a more precise indication of the type of intervention is about to be selected. Since the betting areas surrounding the Inverse Roulette game table precisely correspond to these parameters, the actions of players directly relate to the risk management steps outlined in NIST for specific application areas. The reference model offers a choice among the three families of possible cybersecurity interventions, allocating a value between 0% and 5% of available resources to each. To accurately map the operators' choices onto the reference model, *the bets must be traceable back to three percentage values, ranging from 0 to 5, for each P, R and D category*. In the roulette metaphor, it was decided to assign to each chip a value of half a percentage point, therefore, to provide the player with 10 chips

(a) Potion metaphor. White graduation 1 (b) Potion metaphor. White graduation 2

Fig. 7. Potion metaphor. Different graduations of white smoke. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

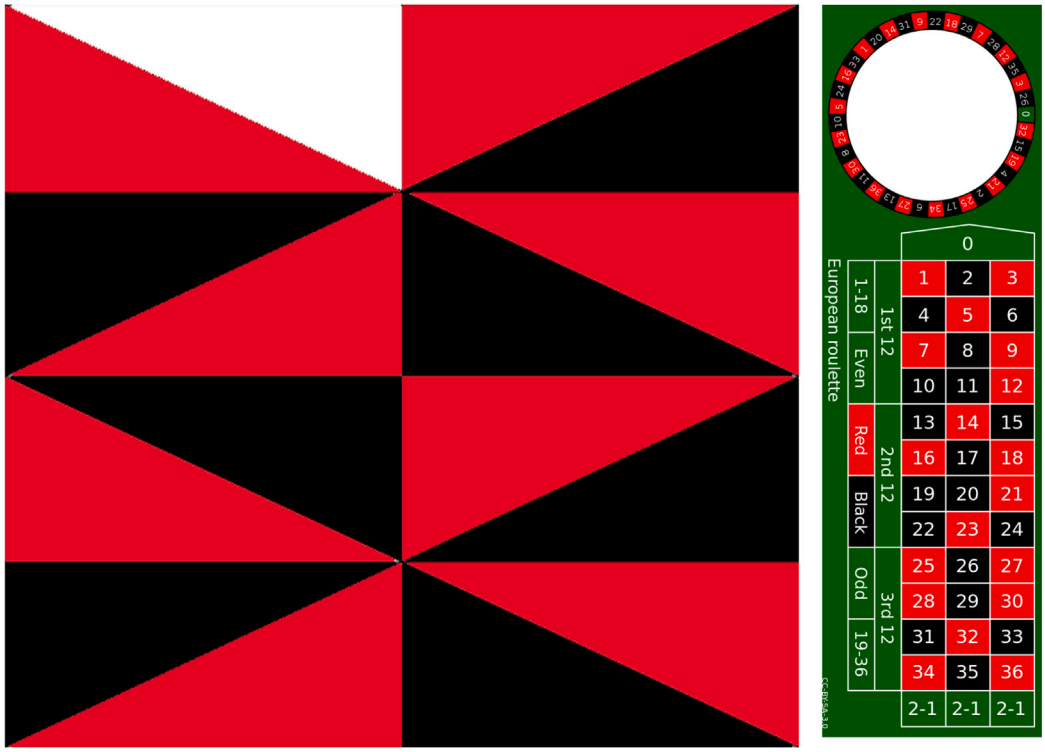


Fig. 8. Roulette metaphor. First basic representation. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

for each category (family). The chips are not all identical: although, in total, the player has 30 chips at each game run (i.e., every year of simulation), a maximum of 10 chips can be spent for each family in a run, consequently obtaining an investment equal to 5% for that family). Thus, an overall maximum investment of 15% of resources can be spent in each run. Users will, therefore, have three groups of 10 chips at their disposal, and each group can only be spent on the five areas of measures within that group. To make the association immediate, the three groups of chips and their related areas of intervention fields were colored in the same way. The light blue chips can only be spent in the five light blue areas corresponding to the category of Prevention measures, the yellow ones for Detection, and the purple ones for Response.

3.2.4. Starting situation and effect of investments on the "Inverse Roulette" table

The system assumes the role of the attackers, while users will only reduce the likelihood of a successful attack through actions that correspond to budget allocation in specific areas. At the onset of each simulation step (which corresponds to the beginning of a new business year), a hypothetical starting situation is displayed on the roulette table (numbers from 1 to 36), representing the known or unknown vulnerabilities of the company's IT systems (highlighted in transparent, non-covering purple or transparent, non-covering yellow, respectively). Users can start playing by moving chips onto the intervention areas surrounding the "Inverse Roulette" table. Once the intervention fields

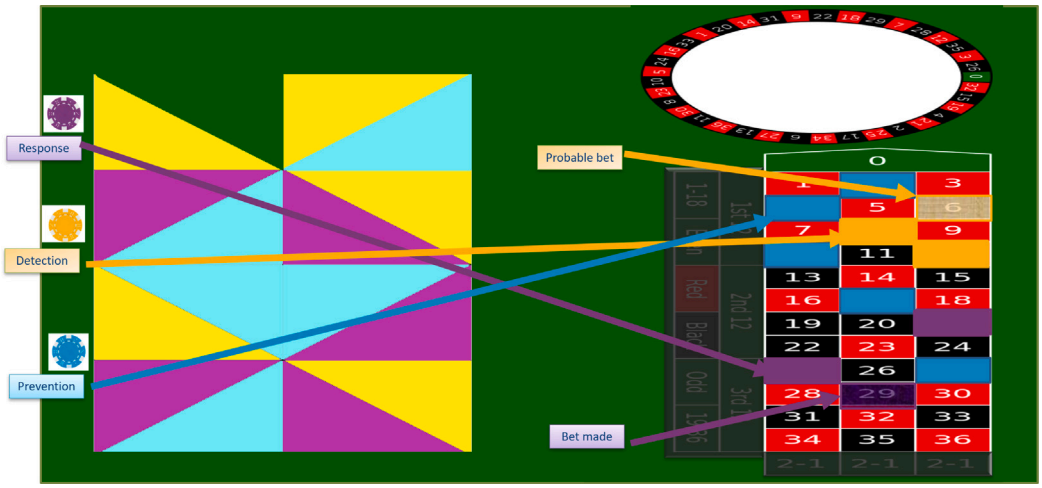


Fig. 9. Roulette metaphor. Different color introduction. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

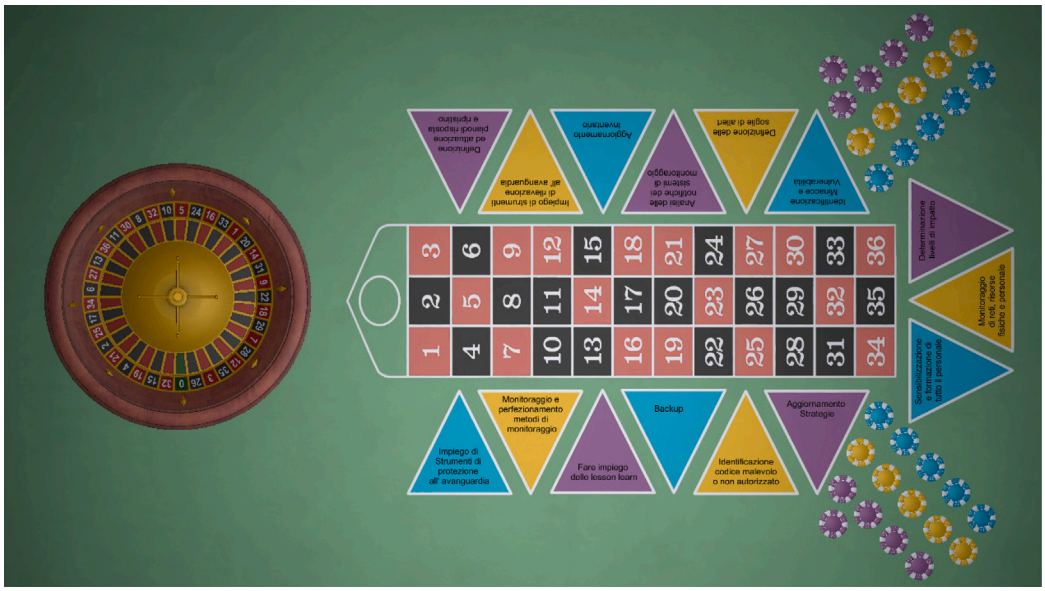


Fig. 10. Final version of Inverse Roulette metaphor. Betting areas representing cybersecurity parameters with corresponding colored chips. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

are selected and chips are placed on them, the obtained effect is displayed on the roulette carpet. This effect will vary depending on the category to which the intervention field belongs. The metaphor of the "Inverse Roulette" translates Prevention action onto the gaming table by concealing part of the board from the attackers' view, thus preventing them from betting on certain numbers. The adversary is effectively prevented from exploiting certain system vulnerabilities. Each number that is "protected" by a preventive measure is concealed by a light blue box covering it, means that the attacker cannot bet on it due to the protection measure related to the proper budget allocation (bet of the player). Detection consists of adopting constant monitoring measures for resources subject to risk and implementing increasingly refined procedures to effectively obtain a picture of their cyber-health state. This concept is translated into the metaphor of "Inverse Roulette", representing the possibility of being aware of the bets that are the object of the attacker's interest and intercepting them before they materialize. The starting situation will include indicating certain numbers that have the greatest possibility of being bet on by the attacker, and, through the adoption of detection measures, their quantity can be reduced (reducing the attacker's available bets, i.e. the attack surface, in cybersecurity terminology). When a run session begins, a certain number of attacker targets are highlighted in veiled, non-covering yellow. Through the Detection actions, i.e., by placing the yellow chips on the corresponding areas on the left side of the interface, some of these "Inverse Roulette" numbers will be entirely covered in yellow. When this occurs, it indicates that the attackers' bet has been intercepted and will not result in a win. In other words, defenders observe where the opponent intends to bet and prevent that bet from being successful. Response measures intervene after the event has occurred; therefore, they respond to attacks rather than threats. Consequently, these are not measures that can take place a priori but intervene once the threat has materialized. In the real world, the effect of these measures is to eliminate or contain the effects of a successful attack. To make this concept usable through the metaphor of the "Inverse Roulette", on the gaming table not only the bets with the greatest probability of being made are represented, but also the hypothetical situation of already made bets. The numbers on the board representing the subject to such attacks will be highlighted with a non-covering purple veil. Through Response actions, which involve placing purple chips on the respective areas, users will see the effect of removing the possibility to make certain bets by the attacker on the "Inverse

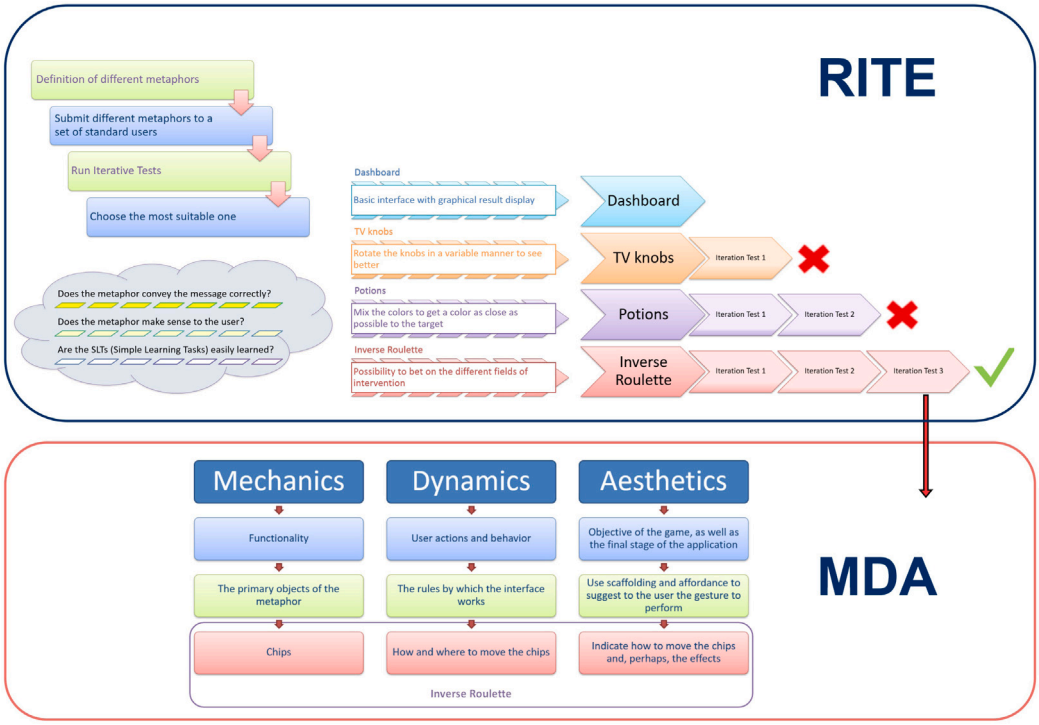


Fig. 11. RITE method and MDA framework graphical relation.

NIST Subcategory	Family	Parameter
ID.AM-1 E 2	Prevention	Inventory update
ID.RA-1,2 e 3		Identification of threats and vulnerabilities
PR.AT-1,2 e 4		Raising awareness and training of all staff
PR.IP-4		Backups
PR.PT-4		Use of cutting-edge protection tools
DE.CM-4	Detection	Use of cutting-edge detection tools
DE.AE-5		Definition of alteration thresholds
DE.CM-1,2 E 3		Monitoring of networks, physical assets and personnel
DE.CM-4 e 5		Identification of malicious or unauthorized code
DE.DP-3 e 5		Monitoring and improvement of monitoring processes
RS.MI-1 E 2	Response	Definition and implementation of response and recovery plan
RS.AN-1		Analysis of monitoring system notifications
RS.AN-2		Determination of impact level
RC.IM-2		Strategies update
RS.IM-1, RC.IM-1		Use of lessons lern

Fig. 12. NIST category vs Intervention measures (Parameters) relation. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

Roulette" gaming table. This signifies that the chosen investment takes the form of an intervention that tends to counteract the opponent's advantage from a previously placed bet, effectively eliminating such bet. The numbers on the gaming table, thus safeguarded, will be those entirely covered in purple.

3.2.5. *Maximum carpet coverage*

The greater the resources invested, the greater the numbers that can be covered by P, R and D measures. To determine the maximum portion of the carpet that can be protected with prevention, detection, or response measures, visual representation were decided to be favored

over mathematical proportion. In fact, an investment of 5% of the total resources invested by a company in one category (e.g., Prevention) within a year should translate into the probability of preventing an attack on less than two numbers out of 37 (ranging from 0 to 36) on the table. To favor the game-based approach, it was instead decided to make two chips (therefore, one percentage point) correspond to the concealment of a single number subject to betting. Therefore, with 10 chips available to invest in one of the three kinds of measures, users will be able to hide a maximum of five numbers on the board from the attacker's view for each category. Ultimately, using 5% in each category corresponds to preventing a winning bet on 15 numbers on the board, or almost half. This "coverage" of cybersecurity threats *is far from being achieved in reality*. However, the decision, as expressed, is dictated by factors of representation and metaphorical relevance. This choice can be considered admissible due to the super-realism that natural interfaces allow to achieve. Nonetheless, it is important to understand that not taking any measures will leave the attacker free to bet on any number. On the other hand, taking measures to prevent all bets would be too expensive. Therefore, balancing behavior should guide the choices of investments.

3.2.6. Evolution process for the metaphoric representation of the game result

Once the fields of intervention have been selected, a simulation run is started. Similar to a real roulette, when the croupier announces "Rien ne vas plus" and throws the ball, the betting phase stops, and the roulette wheel is spun. When the ball stops, it signifies that a business year has ended, and the results of investments in cybersecurity must be evaluated. The "Inverse Roulette" metaphor involves displaying a result consistent with it, i.e., a number between 0 and 36. In the *first version* of the metaphor created, the result was normalized on a scale compatible with this range. However, the value of the winning number had *no correlation with the roulette game*. In other words, obtaining a value closer to 36 (which is the maximum) absolutely did not correspond to the attacker's bets being unsuccessful. Therefore, in the *second version*, it was decided to display the value of an index normalized between 0 and 100. Although this representation was not entirely consistent with the roulette metaphor, it was easy understandable and offered an index that could be used both in comparison to the performance of another player and to the performance of the same player in relation to a new exercise. Above all, it allowed users to receive feedback on their work during the individual simulation, enabling comparisons with past exercises and thus promoting the learning through gaming. However, *the break in the game paradigm proved to be significant and was perceived as forcing the underlying metaphor by the users*. The recursive application of the RITE method and the targeted refinement of aesthetics required by the application of the MDA framework made it possible to obtain a hybrid solution, which has been implemented. In the *final version*, akin to the roulette game, a number is presented, which will determine whether it is a win (favorable for the opponent) or a loss (beneficial for the user). To understand if the run was a winning one or not for the user, it has been necessary to link the output of the simulation to the interface. We utilize the outputs of the cybersecurity game by Jalali et al. [1] to obtain a performance index. Further, we compare this performance index to a prefixed threshold. If the performance index is lower than the threshold, a number on which the attacker had bet and has not been covered by player's bet is displayed on the roulette disc. On the other hand, when the performance index is higher than the threshold, a covered number is shown on the roulette disc. Therefore, both indicators, the winning number and the performance index, can be displayed. The former is displayed as the result of the roulette game, just as the winning number on the roulette dial indicates in a real roulette game. This ensures metaphorical correspondence for the game. Similarly, the performance index is also displayed, particularly in the internal area of the disc. However, the representation is structured in such a way that it conveys the significant semantic meaning underlying it. Specifically, the internal area of the disk is, in fact, divided in four sectors whose meaning will be illustrated in Section 3.2.8, representing the performance index achieved by the player in that simulation round. The game spans five "launches" of the ball, corresponding to five years of operation. Additionally, the performance index keeps track of the cumulative results of previous launches (years) with each subsequent launch. Thus, the real performance index of the entire simulation achieved by the players reflects the results after the fifth launch (marking the end of the fifth year of activity).

3.2.7. Performance index determination

A detailed analysis has led us to define the performance index as the ratio between the accumulated profit and the sum of the systems compromised by attacks and at risk. These parameters are derived from the cybersecurity game by Jalali et al. [1]. The basic underlying assumption is that a lack of security investments puts systems at risk regardless of whether they are attacked or not. Such index also takes into account the company's increasing risk exposure over time. Additionally, such an index is relevant from an educational perspective. In practice, department managers may decide not to implement or enforce strict security policies. This decision usually involves reducing costs or realizing benefits that will be reflected in their team budget or personal business targets, while the company's increased risk exposure is typically managed at a higher-level business unit or at the corporate level. This higher risk exposure becomes visible only later when discussed with corporate risk, corporate audit, or after ethical hacking or pen testing. This can also be noticed by the fact that the performance index at the beginning of the game (in the early years of a game run) is consistently high. Part of this phenomenon is attributed to the game's model: the performance index tends to be higher at the beginning because the impacts of uncontrolled risks escalate over time. Another contributing factor is the nature of the performance index, as it accumulates year by year, reflecting the outcomes of all preceding years (see Section 4).

3.2.8. Risk-profit matrix

As elucidated in Section 3.2.6, since the game metaphor must provide players with feedback on whether they are winning or losing, we display the winning number of the roulette game run by run using the performance index/threshold method. Although this feedback is suitable for the game, it lacks meaning from the perspective of cybersecurity education. Therefore, another powerful feedback mechanism with semantic content is introduced. The final performance index is represented within a 2×2 matrix (see Fig. 13), termed as the Risk–Profit Matrix. This matrix is constructed by plotting the accumulated profit (the original game output) on the x-axis and the total compromised and at-risk systems (also the original game model outputs) on the y-axis. The Risk–Profit Matrix defines four quadrants in which the final performance index can "fall". If the performance index is within the Defense Gap Area (violet), it indicates that the organization is significantly impacted by adversarial behavior. If it lay within the Risky Defense Posture Area (blue), it was understood that the attacker could exploit some vulnerabilities but has not yet exploited this opportunity to impact the organization. When the performance index is inside the Security Burden Area (red), the organization is overinvesting in cybersecurity. Finally, if it is in the Balanced Behavior area (green), it signifies that cyber-risk management aligns with business needs. It is possible to ascertain the appropriate cyber-risk management action needed to improve the company's cybersecurity posture based on the position of the performance index. For example, understanding the offense-defense gap provides the space where the adversary can exploit vulnerabilities and be successful. Improving security after suffering from a materialized threat (reactive approach) is costly, because the organization must pay for to remediate the effects of the attack and for subsequent security improvements. Conversely, reactive learning may lead to overspending on cybersecurity measures. Achieving a balance

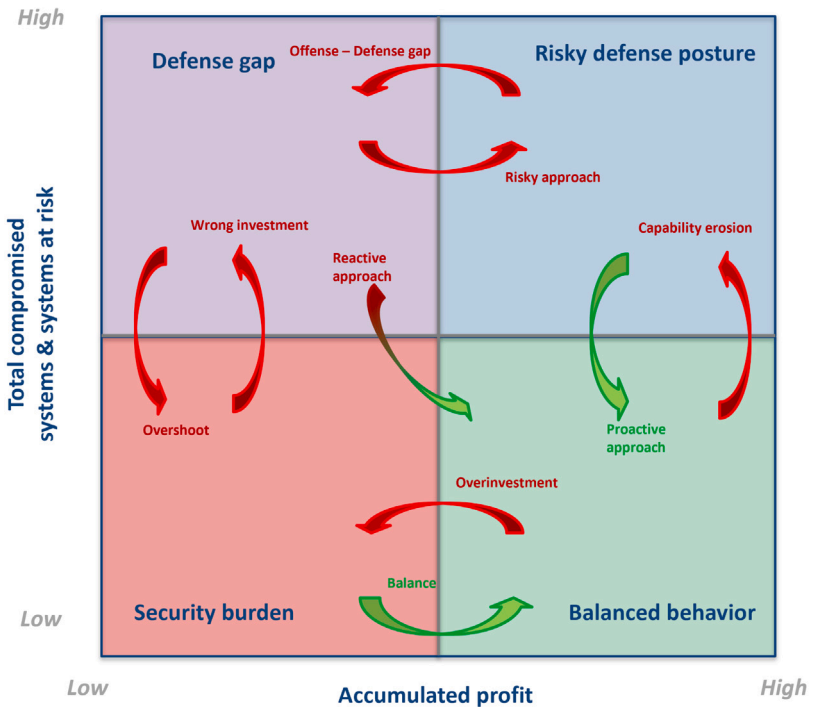
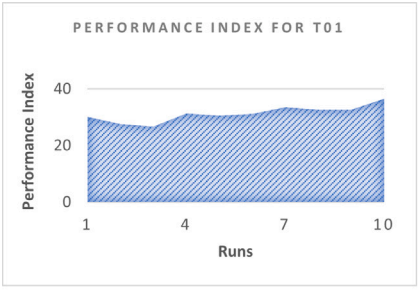
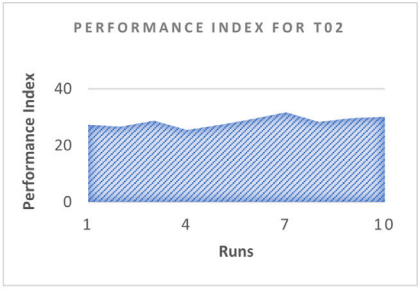


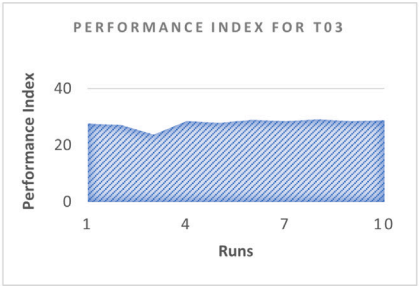
Fig. 13. Two-by-two Risk Profit Matrix.



(a) Test Session 01 (Single Player)



(b) Test Session 02 (Single Player)



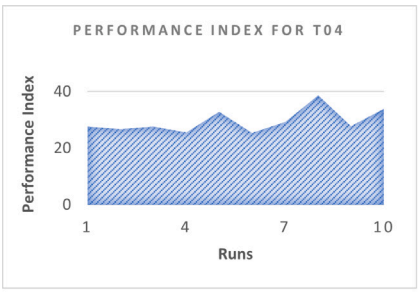
(c) Test Session 03 (Single Player)

Fig. 14. Performance Index obtained in the Single Players sessions (01-03)

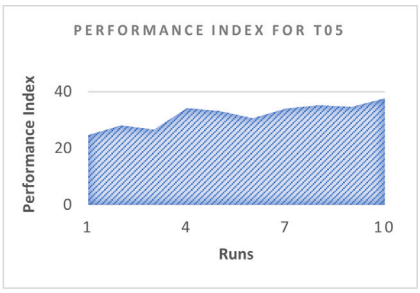
between profitability and robust system security ensures that cyber-risk measures align effectively with business requirements. Proactive learning occurs when the security posture of the organization improves, the level of profitability remains high, and the adversary has limited success in their endeavors. It requires a thorough understanding of the threat landscape. Capability erosion occurs when maintaining system security becomes challenging, potentially leading to inadvertent and unintended control lapses that could be exploited by attackers over time. This semantic representation can be invaluable not only for learning about the effects of cybersecurity risk and its management but also as a strategic tool for a company's cybersecurity posture assessment and investment planning.

3.3. Research approach

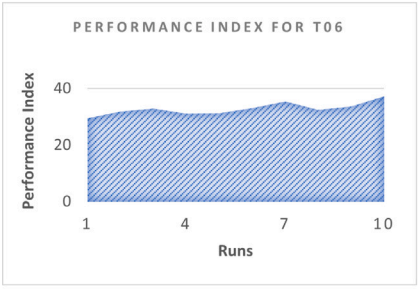
This study aims to verify whether the introduction of a collaborative, natural interaction game-based system brings learning benefits and improves performance. For this purpose, as mentioned, the dynamic model presented in [1] was used as the "core" of the system. This dynamic system is able to operate in two distinct modes. In real life,



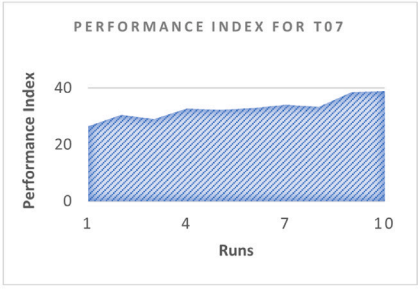
(a) Test Session 04 (Group)



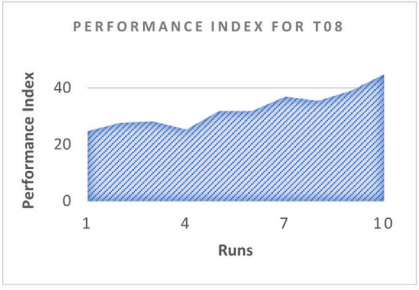
(b) Test Session 05 (Group)



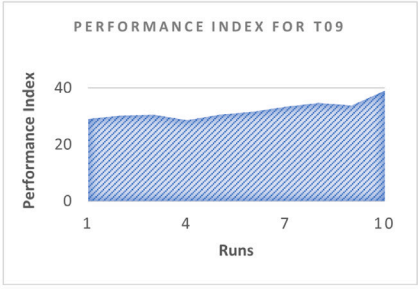
(c) Test Session 06 (Group)



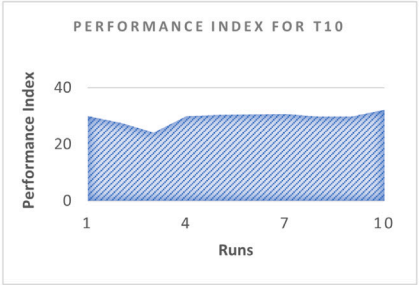
(d) Test Session 07 (Group)



(e) Test Session 08 (Group)



(f) Test Session 09 (Group)



(g) Test Session (Group)

Fig. 15. Performance Index obtained in the Groups sessions (04-10)

obviously, the opponent's behavior is not predictable, consequently, the model can operate by presenting the player with a random attack scenario, that is, replicating a climate of absolute uncertainty identical to the real one. However, in order to compare the performances of individual players with those operating in a group, it was necessary for all participants in the test to be subjected to the same risk conditions and simulated events. In that way it is possible to evaluate how each of them responded to the same crisis and how, over time, they became able to cope with it. To do this, the second operating mode of the system [1] can be used. In fact, it can also operate in a deterministic way by canceling the random component and presenting, from time to time, a five-year situation identical to itself, with attacks that occur at the same time and with the same magnitude at each repetition of the game. Thanks to this common scenario, shared among all groups and always consistent with itself, it is possible to compare the learning capacity of individual players and groups that undergo the game because each group or individual player will be subjected to the same scenario ten times. Overall, this study comprises two phases, both employing the same deterministic attack scenario. First, the game is played by individual users, separately. Subsequently, it is played by a heterogeneous group of users with varying technical backgrounds. To prevent group members to leverage from experience gathered by playing alone, they are excluded from group exercise. The results of the two phases, obtained by operating in the same deterministic scenario, is compared using the final performance indexes. In the first phase, several players played individually the game a given number of times. At the end of each game session (simulating a time span of five business years), the player was notified the resulting performance index, according to the graphic representation shown in Fig. 13. All single player performance data (user choices and results obtained) are recorded in order to determine not only the best or worst performance but also whether there was improvement in performance as the player

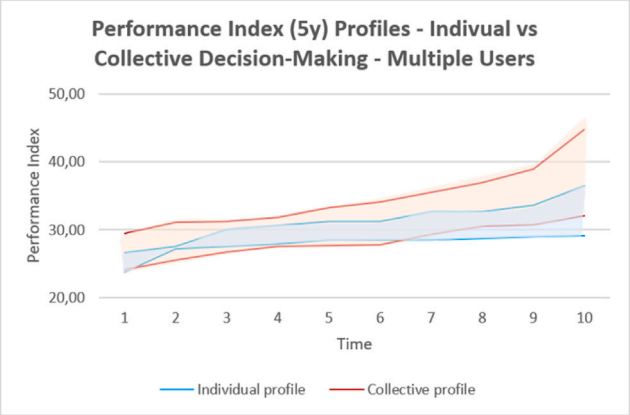


Fig. 16. Trend of Performance Index per User Group and Run.

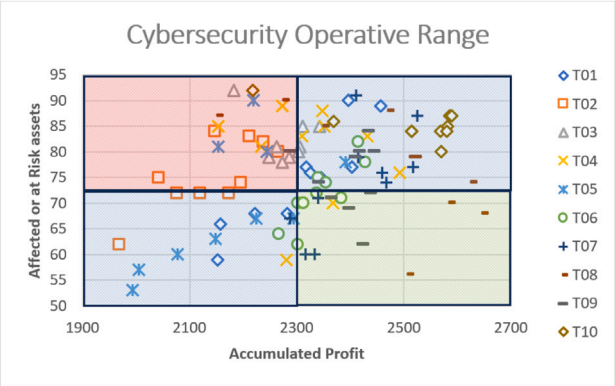


Fig. 17. Learning behavior per team across the Risk-Profit Matrix.

repeated their experience. The same was done in the second phase, with the only difference being that players played in groups. The results of the two test sessions is compared to check whether the collaborative (group) approach provides or not benefits in terms of final result.

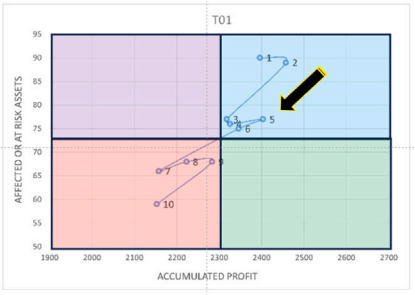
4. Research results

On a total of ten test sessions, three were executed by single players, and seven were conducted by teams of three players each with diverse backgrounds and understanding of cyber-risk management. One hundred employees of the same company participated in the experiment. Each participant was tasked with performing the test either as a single player or as a member of a three persons team. They possessed various roles and functions within the company, and had different skills and experiences. In such a heterogeneous climate, it is easy to imagine that not all of these individuals had the same familiarity with video games. At the same time, the experience gained in the more strictly technical field from the point of view of cybersecurity is also different. The age of the subjects varies from 24 to 60 years and their cultural background is mainly IT, economic, administrative. Such a varied audience represents the ideal audience to evaluate whether, in fact, a Natural User Interface like the one proposed can make people of different ages and experience competent in cybersecurity, in a short time, with little effort and through an engaging group experience. Test sessions (single or multiplayer) consisted of 10 runs each, and a five-year scenario was completed for each run. Year by year, players investments allocation in cybersecurity measures (divided into prevention, detection, and response measures) is recorded by the system. At the same time, accumulated profit and the number of compromised and assets at-risk are collected at the end of each year. By comparing these two types of data, we obtained the performance index that represents the effectiveness of resources allocation made by a player or a team the specific year of the scenario (see Section 3.2). Every year, players are presented with performance indexes within the Risk–Profit Matrix (shown in Fig. 13). By looking at their own performance, they can evaluate it and, therefore, decide their allocation investment budget for the next year. Performance indexes do not only consider the performance of the last year but also that of previous years. Consequently, the performance index obtained at the end of the fifth year represents the entire scenario run. Each of the ten runs, has the same game scenario. By playing the scenario run by run, players gain experience in determining which allocation is most effective within a given run and how to adjust it accordingly. This allows them to experiment with different strategies to improve their performance. Furthermore, due to the deterministic nature of the scenario, it is possible to compare the performance of the players (singles or groups).

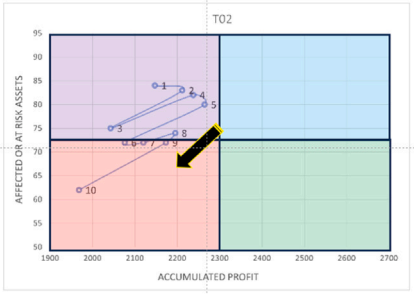
Fig. 14 depicts a graphic representation of the performance trends obtained from individuals during their respective test session of ten runs. These test sessions are labeled T01 to T03. Fig. 15 shows equivalent data compared to Fig. 14 withe the difference that Fig. 15 resulted from the game performance of teams that consisted of three players. These test session are labeled T04 to T10. While some performances show greater improvement than others, overall the trends indicate positive growth. This improvement in performance across the ten test sessions runs within the same scenario is "translated" into how fast the participants understand the topic of the exercise (cybersecurity investment optimization). These learning trends stem from two key factors. First, the model is specifically designed to encourage understanding key element about cybersecurity issues [23]. The second and equally important reason is the use of an NUI. By emphasizing principles such as affordance, scaffolding, superrealism, and suspension of disbelief, this platform fosters interaction and encourages exploration. Game interfaces can adapt to users' capabilities, leverage their real-world experience, and simplify their tasks.

4.1. Single vs. multiplayer performance

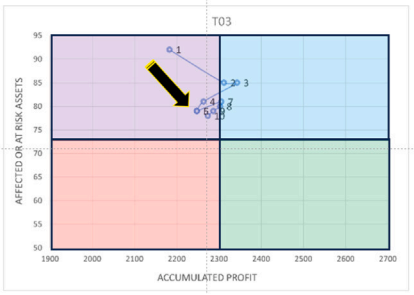
Observable differences exist between single decision-making (Fig. 14) and group decision-making (Fig. 15) based on financial performance and risk result. A t-test [68] to compare the performance index score at the end of the game has been used. Comparing the total runs of the 10 test sessions (8 degrees of freedom), a right-tailed P value of 0.029 was observed. Additionally, a significant P value of 0.0017 is observed at the level of the individual test comparison (98 degrees of freedom). In both cases, a significant difference is evident. Moreover, regression analysis [68] demonstrated an association between performance index, compromised systems, and accumulated profit ($F = 52$ and adj-$R2 = 0.51$). Specifically, for every 1-point increase in the performance index, accumulated profit increases by 0.01, and number of compromised systems decrease by 0.34%. These relationships are highly significant because the P value is below 0.001. By comparing the results achieved for the two groups, it is also possible to determine whether and how the adoption of a natural interface on a collaborative decision-making system can lead to notable results. With the exception of two cases, the groups demonstrated superior results in terms of performance and learning curve. Teams T04 (Fig. 15(a)) and T10 (Fig. 15(g)), however, obtained worse results compared to those in test session T01 (single-player session, Fig. 14(a)). However, these two groups remain significantly more successful compared to the other two single players' runs (T02, Fig. 14(b) and T03, Fig. 14(c)). T01's performance appears to have exceeded expectations. The graphic representation displayed in Fig. 16 provides further evidence supporting this assertion. It displays multiplayer and single-session performance



(a) Learning Path for T01 (Single Player)



(b) Learning Path for T02 (Single Player)



(c) Learning Path for T03 (Single Player)

Fig. 18. Groups learning paths for Single Players (T01–T03)

indexes in an aggregated profile view. In the area generated from the collective profile, performance levels are notably higher. Only one of the single players has achieved a performance index exceeding 35. This occurred only once, at the end of his/her game. The results of test sessions T02 and T03 (respectively Fig. 14(b) and Fig. 14(c)) indicate a performance index below 30. Furthermore, teams consistently exhibit a quicker learning curve compared to individuals. Therefore, the referenced literature studies are corroborated, and the initial hypothesis is assumed to be true: a NUI collaborative game-based system provides a dual advantage: enhancing the learning curve at a faster rate and improving overall performance.

4.2. Risk-profit matrix areas and learning path

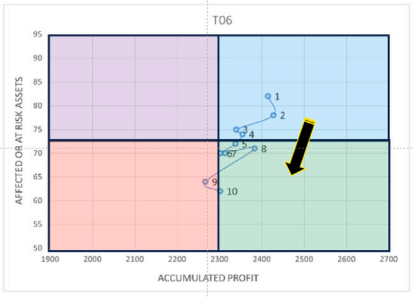
In the previous sections it has been reported that it is possible to track the quality of a team's learning process by representing the performance index obtained at the end of a single run within the Risk–Profit Matrix. The significant contribution to the learning process of that representation has been described in Section 4. Furthermore, this representation can support a new relevant interpretation of results when all the obtained performance indexes are depicted in the Risk–Profit Matrix. These results are displayed in Fig. 17. The first consideration is that teams with better growth in their performance index (see Fig. 17) are also those that tend to "move" toward the Balanced Behavior area (where there is a balance between business need and cyber-risk). In Fig. 17, there is no indication of the full 0% and full 5% allocations. This is because within it, there exists only the true operative range, and such allocations are, of course, far from entering that range. Additionally, there is no benchmark representation because no benchmark can be defined for the simulation game. To gain a clearer understanding, Fig. 18 and Fig. 19 show each session run results plotted in sequence. The difference is that Fig. 18 relates to the individual performance (T01 to T03) and Fig. 19 related to the team performance (T04 to T10). Each plot can be seen as the "learning path", i.e., how, within 10 runs, each user/group changes the approach to improve their own performance by modifying their own budget allocation decisions. On the basis of these plots, it is evident that every test session seems to follow a counterclockwise direction. However, at each starting point, the path followed, and the arrival point are markedly distinct from each other. This representation enables us to also draw an additional important conclusion. It appears that the quadrant representing the Risky Defense Posture (blue quadrant) emerges as significant factor in the learning process. Accordingly, this suggests that learning experience is enriched by being exposed to material threats, which are essential for learning to take place. The curves represent the learning path that each individual/group took to arrive at the final result of their last run. Fig. 18 (individuals) and Fig. 19 (groups) demonstrates how all paths progressively improve their positions from the starting point, indicating a deepening in cybersecurity investments understanding since the start point. Furthermore, it is possible to confirm that the best performances were achieved during the group test sessions (T04–T10), particularly with T06–T09 (from Fig. 19(c) to Fig. 19(f)). Consequently, although T01 exhibits a very good performance index (Fig. 14(a)), it has not yet attained a business need/cybersecurity risk balance point (Fig. 18(a)). Instead, it has transitioned from a risk defense posture to a state of security burden, indicating an overinvestment in this area. Conversely, the most effective performance occurs when the balance behavior area is reached, leading to the best results. Thus, it is interesting to note how this goal has been achieved by the T06 (Fig. 19(c)) and T07 (Fig. 19(d)) groups, and particularly by the T09 (Fig. 19(f)) and T08 groups (Fig. 19(e)), the most successful ones, as those two groups did not overshoot the target at any point. Generally, there is a clockwise learning path along the Risk–Profit Matrix, starting with a high risk with low profit, then progressing to high risk with high profit, and eventually ending culminating in low risk with high profit.

5. Discussion and recommendations for future research

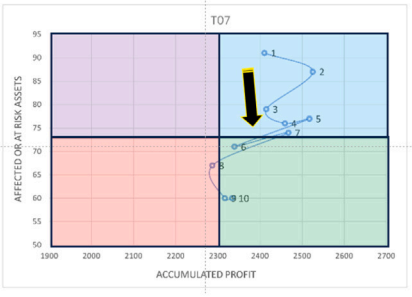
By employing the example of a high-level decision-making process, this study aims to demonstrate how introducing a cooperative NUI can positively impact cybersecurity budget allocation versus cyber-risk performance. First, a significant difference between the two types of test sessions (single vs. group) was observed at the statistical level. Furthermore, single-session and group-session results were compared and the latter always performed better. Moreover, the results of the study indicated that not only group performance is better than single

(a) Learning Path for T04 (Group)

(b) Learning Path for T05 (Group)



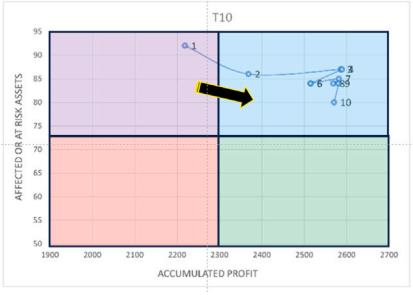
(c) Learning Path for T06 (Group)



(d) Learning Path for T07 (Group)

(e) Learning Path for T08 (Group)

(f) Learning Path for T09 (Group)



(g) Learning Path for T10 (Group)

Fig. 19. Groups learning paths for T04–T10.

users one, but that it speeds up the learning process as well. Therefore, such a tool can be very beneficial to help to bridging the gap between skilled and unskilled users and foster collaborative decision-making processes when strategically managing cyber-risks to reduce the impact of cyber-attacks. Through the proposed gaming interface, individuals with a variety of skill levels were able to quickly learn how to use the system and became more confident in allocating costs against risks. By analyzing the Risk–Profit Matrix graphical representation in further detail, additional elements that support the conclusion that group sessions perform significantly better than individual sessions can be identified. Such representation illustrates the learning path evolution within the cybersecurity operative range, providing information about how players (single or in groups) alter their approach step-by-step. This study underscores the critical importance of understanding the business and financial consequences of cyber-risks. This is because these learning paths lead from high risk with low profits (higher overall security + impacts costs) to a high risk with high profits (lower overall security + impacts costs) and finally to low risk with high profits, moving clockwise through the quadrants. This study was conducted with employees of different skills and roles to collect the results. Although such results are statistically accurate, the authors are aware that their value may be considered relative due to the relatively low number of users in the sample. Consequently, the experiment need to be repeated with a larger number of participants in the sample before proceeding to future steps. In fact, the objective of this study was to gain a first understanding on the effectiveness of such an approach to improve the learning process among a heterogeneous group of individuals. However, the final objective of the game is to position itself as a powerful tool for

raising cybersecurity awareness in high-level decision-making contexts where not all participants have a clear understanding of the issue (executive leaders such as CEOs, CFOs, CTOs, and CIOs). Therefore, it can assist CISOs to promote the importance of proper resources allocation on cybersecurity not as just a cost, but a wise investment decision, improving the overall company's business performance. Another interesting research area which can benefit from the proposed gaming approach is the study of the effect of "bias", such as company culture, on the result. Such research area could provide insight into whether and how company culture affects outcomes. The better group decision-making performance obtained in this study may be attributed to the specific company culture of the sample organization (which might foster encourages cooperation). What could occur in another company with a different culture? Might the results vary? Finally, to conduct this study effectively, it was essential to utilize a scenario that was shared among all the groups, and the scenario should have been consistent each time. Utilizing a model that operates in a deterministic manner ensures this. Since such a model can also operate randomly, another significant result regarding the learning process and the contribution of the NUI may also emerge from this scenario.

6. Conclusions

International and regulatory developments have pushed cybersecurity into the boardroom, making cyber-risk management a cooperative decision-making process. While not all members of the board possess solid backgrounds in information technology or cybersecurity. Furthermore, the group process should consider the business, operational, and financial context of cyber-risks. Unfortunately, there is no comprehensive approach that considers all these aspects together. Yet, only through a collective approach it is possible to emphasize the multidisciplinary skills of the group members. Our research showed that their achieved results were much better than those that the members could achieve individually. This confirm the aim of our research, that was to reuse a scientifically grounded cyber-risk management dashboard serious game, revolutionizing the interface by employing NUI design theory, to leverage on the collective intelligence of the members of a group. This fosters a collaborative and understandable environment in which people can manage and educate themselves on the risks associated with cyber-security. As depicted in this article, collaborative and collective decision-making can lead to significant improvements in financial performance and substantial reductions in the risk profile compared to individual decision-making. Additionally, through the collaborative game, executives and business leaders can gain a deeper understanding of cyber-risk management issues through in-depth insights into their own learning paths, thereby improving their performance. In the context of cyber-risk management, our results have significant practical implications because they demonstrate that the design of a cyber-risk management dashboard and the formulation of a collaborative natural human-centered interface game are critical for a successful approach. In addition, this work is an example of the application of a new type of collective intelligence that involves an interconnected group of people and computers performing intelligent tasks [69], in this case, reducing the impact cyber-risks.

CRediT authorship contribution statement

Tony Delvecchio: Writing – review & editing, Writing – original draft, Visualization, Validation, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Sander Zeijlemaker:** Writing – review & editing, Writing – original draft, Validation, Software, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Giancarlo De Bernardis:** Supervision, Conceptualization. **Michael Siegel:** Writing – review & editing, Validation, Supervision, Methodology, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work was supported in part by the Fondo Europeo di Sviluppo Regionale Puglia Programma Operativo Regionale (POR) Puglia 2014-2020-Axis I-Specific Objective 1a-Action 1.1 (Research and Development) Project Titled: CyberSecurity and Security Operation Center (SOC) Product Suite by BV TECH S.p.A., under grant CUP/CIG B93G18000040007.

Data availability

Data will be made available on request.

References

[1] M.S. Jalali, M. Siegel, S. Madnick, Decision-making and biases in cyber-security capability development: Evidence from a simulation game experiment, J. Strat. Inf. Syst. 28 (1) (2019) 66–82, http://dx.doi.org/10.1016/j.jsis.2018.09.003.

[2] S. Zeijlemaker, E.A.J.A. Rouwette, G. Cunico, S. Armenia, M. von Kutzschenbach, Decision-makers' understanding of cyber-security's systemic and dynamic complexity: Insights from a board game for bank managers, Systems 10(2),49 (2022) http://dx.doi.org/10.3390/systems10020049.

[3] EuropeanCommission, Cyber resilience act - factsheet, European commission newsroom, in: European Commission Newsroom, 2022, ec.europa.eu/newsroom/dae/redirection/document/89528.

[4] EuropeanCommission, Revised directive on security of network and information systems (NIS2) – factsheet, in: European Commission Newsroom, ec.europa.eu/newsroom/dae/redirection/document/72155.

[5] K. Pearlson, C. Hetner, Is your board prepared for new cybersecurity regulations? in: IT Security Management, Harvard Business Review., 2022, http://bit.ly/40Jql8v.

[6] P.J. Bezemer, G. Nicholson, A. Pugliese, Inside the boardroom: Exploring board member interactions, Qual. Res. Account. Manag. 11 (3) (2014) 238–259, http://dx.doi.org/10.1108/QRAM-02-2013-0005.

[7] I. Bongiovanni, M. Gale, S. Slapnicar, Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead, Comput. Secur. 121 (4) (2022) 102840, http://dx.doi.org/10.1016/j.cose.2022.102840.

[8] A.W. Woolley, C.F. Chabris, A. Pentland, N. Hashmi, T.W. Malone, Evidence for a collective intelligence factor in the performance of human groups, Science 330 (2010) 686–688, http://dx.doi.org/10.1126/science.1193147.

[9] A. Kendon, Gesture: Visible action as utterance, Cambridge University Press, 2004, http://dx.doi.org/10.1017/CBO9780511807572.

[10] T.W. Malone, Superminds: The surprising power of people and computers thinking together, Little, Brown Spark, 2018, 978-0316349130.

[11] T. Delvecchio, S. Zeijlemaker, G. De Bernardis, M. Siegel, Revolutionizing board cyber-risk management using collaborative gaming, in: Proceedings of the 10th International Conference on Information Systems Security and Privacy, 2024, pp. 112–119, http://dx.doi.org/10.5220/0012349400003648.

[12] G.A. Boy, The handbook of human-machine interaction: a human-centered design approach, 2017, pp. 211–218, http://dx.doi.org/10.1201/9781315557380,

[13] H. Skorczynska, Metaphor and education: Reaching business training goals through multimodal metaphor, Procedia- Soc. Behav. Sci. 116 (2014) 2344–2351, http://dx.doi.org/10.1016/j.sbspro.2014.01.570.

[14] S. Zeijlemaker, M. Siegel, Capturing the dynamic nature of cyber risk: Evidence from an explorative case study, in: Proceedings of the 56th Hawaii International Conference on System Sciences, vol. 10, 2023, hdl.handle.net/10125/103372.

[15] G. De Smidt, W. Botzen, Perceptions of corporate cyber risks and insurance decision-making, in: The Geneva Papers on Risk and Insurance-Issues and Practice, vol. 43, 2018, pp. 239–274, http://dx.doi.org/10.1057/s41288-018-0082-7.

[16] R. Anderson, Why information security is hard - an economic perspective, in: Seventeenth Annual Computer Security Applications Conference, 2001, pp. 358–365, http://dx.doi.org/10.1109/ACSAC.2001.991552.

[17] S. Armenia, M. Angelini, F. Nonino, G. Palombi, M.F. Schlitzer, A dynamic simulation approach to support the evaluation of cyber-risks and security investments in SMEs, Decis. Support Syst. 147 (2021) 113580, http://dx.doi.org/10.1016/j.dss.2021.113580.

[18] T.W. Moore, S.B.C. Dynes, F. Chang, D. Deason, Identifying how firms manage security investment, in: Workshop on the Economics of Information Security, WEIS, 2016, api.semanticscholar.org/CorpusID:8135043.

[19] J.D. Sterman, System dynamics modeling: Tools for learning in a complex world, Calif. Manag. Rev. 43 (2001) 8–25, http://dx.doi.org/10.2307/41166098.

[20] J.N. Rooney-Varga, F. Kapmeier, J.D. Sterman, A.P. Jones, M. Putko, K. Rath, The climate action simulation, Simul. Gaming 51 (2) (2020) 114–140, http://dx.doi.org/10.1177/1046878119890643.

[21] S.S. Tseng, T.-Y. Yang, Y.J. Wang, A.-C. Lu, Designing a cyber-security board game based on design thinking approach, in: International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing Advances in Intelligent Systems and Computing, 2019, pp. 642–650, http://dx.doi.org/10.1007/978-3-319-93554-663.

[22] K. Wisiecka, Y. Konishi, K. Krejtz, M. Zolfaghari, B. Kopainsky, I. Krejtz, H. Koike, M. Fjeld, Supporting complex decision-making: Evidence from an eye tracking study on in-person and remote collaboration, ACM Trans. Comput.-Hum. Interact. 30 (5) (2023) 1–27, http://dx.doi.org/10.1145/3581787.

[23] Y. Jin, M. Ma, Y. Zhu, A comparison of natural user interface and graphical user interface for narrative in HMD-based augmented reality, Multimedia Tools Appl. 81 (3) (2022) 5795–5826, http://dx.doi.org/10.1007/s11042-021-11723-0.

[24] W. Gong, L. Xiao, X. Wang, C.H. Lee, Dots - an inclusive natural user interfaces (NUI) for spatial computing, in: MobileHCI '20: 22nd International Conference on Human-Computer Interaction with Mobile Devices and Services, 2020, pp. 1–4, http://dx.doi.org/10.1145/3406324.3410715.

[25] M. Braun, M. Wölfel, G. Renner, C. Menschik, Accessibility of different natural user interfaces for people with intellectual disabilities, in: 2020 International Conference on Cyberworlds, CW, 2020, http://dx.doi.org/10.1109/CW49994.2020.00041.

[26] C. Francisco-Martínez, K.S. Morales-Soto, J. Prado-Olivarez, J. Díaz-Carmona, J.A. Padilla-Medina, A.I. Barranco-Gutiérrez, C.A. Herrera-Ramírez, A. Espinosa-Calderón, Quantitative upper limb assessment with natural user interface in children with hemiparesis, IEEE Access 11 (2023) 35080–35088, http://dx.doi.org/10.1109/ACCESS.2023.3264599.

[27] E. Pietriková, B. Sobota, Game development and testing in education. Game theory—From idea to practice, IntechOpern (2022) http://dx.doi.org/10.5772/intechopen.108529.

[28] D. Wigdor, D. Wixon, Brave NUI world: Designing natural user interfaces for touch and gesture, Morgan Kaufmann Publishers Inc, 2011, 978-0-12-382231-4.

[29] L.P. Fu, J. Landay, M. Nebeling, Y. Xu, C. Zhao, Redefining natural user interface, in: Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems, 2018, pp. 1–3, http://dx.doi.org/10.1145/3170427.3190649.

[30] J.J. Gibson, The theory of affordances, in: Perceiving Acting and Knowing. Lawrence Earlbaum, 1977.

[31] J.S. Bruner, Actual minds, possible worlds, Harvard University Press, 1986, 9780674003668.

[32] S. Lajoie, Extending the scaffolding metaphor, Instr. Sci. 33 (2008) 541–557, http://dx.doi.org/10.1007/s11251-005-1279-2.

[33] E. Herrigel, Zen in the art of archery, in: Pantheon Books, 1953.

[34] R.J. Jacob, A. Girouard, L.M. Hirshfield, M.S. Horn, O. Shaer, E.T. Solovey, J. Zigelbaum, Reality-based interaction: a framework for post-WIMP interfaces, in: CHI '08: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2008, pp. 201–2010, http://dx.doi.org/10.1145/1357054.1357089.

[35] S.W. Cook, Z. Mitchell, S. Goldin-Meadow, Gesturing makes learning last, Cognition 106 (2) (2008) 1047–1058, http://dx.doi.org/10.1016/j.cognition.2007.04.010.

[36] D. Kirsh, P. Maglio, On distinguishing epistemic from pragmatic action, Cogn. Sci. 18 (1994) 513–549, http://dx.doi.org/10.1207/s15516709cog18041.

[37] A. Morrison, G. Jacucci, P. Peltonen, CityWall: Limitations of a multitouch environment, in: PPD 2008: Workshop on designing multi - touch interaction techniques for coupled public and private display, 2008.

[38] R.A. Bolt, "Put-that-there": Voice and gesture at the graphics interface, in: In Proc. Of SIGGRAPH '80: The 7th Annual Conference on Computer Graphics and Interactive Techniques, vol. 14, 1980, pp. 262–270, http://dx.doi.org/10.1007/978-1-4020-5820-2.

[39] G. Castellano, L. Kessous, G. Caridakis, Emotion recognition through multiple modalities: Face, body gesture, speech, in: Affect and Emotion in Human-Computer Interaction: From Theory to Applications, 2008, pp. 92–103, http://dx.doi.org/10.1007/978-3-540-85099-18.

[40] P. Bruegger, B. Hirsbrunner, Kinetic user interface: Interaction through motion for pervasive computing systems, in: Proceeding of the 5th International Conference on Universal Access in Human-Computer Interaction, UAHCI, 2009, pp. 297–306, http://dx.doi.org/10.1007/978-3-642-02710-9.

[41] U. Hinrichs, S. Carpendale, Gestures in the wild: Studying multitouch gesture—Sequences on interactive tabletop exhibits, in: CHI '11: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, vol. 2011, pp. 3023–3032, http://dx.doi.org/10.1145/1978942.1979391.

[42] S.H. Khandkar, F. Maurer, A domain specific language to define gestures for multitouch applications, in: DSM '10: Proceedings of the 10th Workshop on Domain-Specific Modeling, 2010, pp. 1–6, http://dx.doi.org/10.1145/2060329.2060339.

[43] K. Kin, B. Hartmann, T. DeRose, M. Agrawala, Proton: Multitouch gestures as regular expressions, in: CHI '12: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2012, pp. 2885–2894, http://dx.doi.org/10.1145/2207676.2208694.

[44] V. Pavlovic, R. Sharma, T. Huang, Visual interpretation of hand gestures for human-computer interaction: A review, IEEE Trans. Pattern Anal. Mach. Intell. 19 (7) (1997) 677–695, http://dx.doi.org/10.1109/34.598226.

[45] Y. Wu, T.S. Huang, Vision-based gesture recognition: A review, in: Gesture-Based Communication in Human-Computer Interaction: International Gesture Workshop, GW'99, Gif-sur-Yvette, France, March 1999. Proceedings, 1999, pp. 103–115, http://dx.doi.org/10.1007/3-540-46616-910.

[46] U. Hinrichs, H. Schmidt, S. Carpendale, Emdialog: Bringing information visualization into the museum, IEEE TVCG 14 (6) (2008) 1181–1188, http://dx.doi.org/10.1109/TVCG.2008.127.

[47] E. Hornecker, I don't understand it but it is cool": Visitor interactions with a multitouch table in a museum, in: CHI '11: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2008, pp. 121–128.

[48] P. Peltonen, E. Kurvinen, A. Salovaara, G. Jacucci, T. Ilmonen, J. Evans, A. Oulasvirta, P. Saarikko, "It's mine, don't touch!": Interactions at a large multitouch display in a city centre, in: CHI '08: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2008, http://dx.doi.org/10.1145/1357054.1357255.

[49] H. Schmidt, U. Hinrichs, A. Dunning, S. Carpendale, Memory [en]code—Building a collective memory within a tabletop installation, Comput. Aesthet. Graph. Vis. Imaging (2007) 135–142, http://dx.doi.org/10.2312/COMPAESTH/COMPAESTH07/135-142.

[50] N. Ahmed, H. Kharoub, S.M. Medjden, A. Alsaafin, A natural user interface for 3D animation using kinect, Int. J. Technol. Hum. Interact. 16 (4) (2020) 35–54, http://dx.doi.org/10.4018/IJTHI.2020100103.

[51] S.K.T. Bailey, D.E. Whitmer, B.L. Schroeder, V.K. Sims, Development of gesture-based commands for natural user interfaces, in: Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 61, (1) 2017, pp. 1466–1467, http://dx.doi.org/10.1177/1541931213601851.

[52] M. Hancock, S. Carpendale, A. Cockburn, Hallow-depth 3d interaction: Design and evaluation of one-, two- and three-touch techniques, in: Proceeding CHI, 2007, pp. 1147–1156, http://dx.doi.org/10.1145/1240624.1240798.

[53] A.D. Wilson, S. Izadi, O. Hilliges, A. Garcia-Mendoza, D. Kirk, Bringing physics to the surface, in: UIST '08: Proceedings of the 21st annual ACM symposium on User interface software and technology, 2008, pp. 67–76, http://dx.doi.org/10.1145/1449715.1449728.

[54] A. Soro, S.A. Iacolina, R. Scateni, S. Uras, Evaluation of user gestures in multi-touch interaction: a case study in pair-programming, in: ICMI '11: Proceedings of the 13th international conference on multimodal interfaces, 2011, pp. 161–168, http://dx.doi.org/10.1145/2070481.2070508.

[55] B. Tognazzini, First principles of interaction design (revised expanded), 2014, https://asktog.com/atc/principles-of-interaction-design/.

[56] M.C. Medlock, The rapid Iterative Test and evaluation method (RITE), Oxford-Press, 2018, pp. 203–216, http://dx.doi.org/10.1093/oso/9780198794844.003.0013.

[57] M.C. Medlock, D. Wixon, M. Terrano, R.L. Romero, B. Fulton, Using the RITE method to improve products: A definition and case study, Usability Professional Association, 2002.

[58] M.C. Medlock, D. Wixon, M. McGee, D. Welsh, 17 chapter - the rapid iterative test and evaluation method: Better products in less time, in: Cost-Justifying Usability, second ed., 2005, pp. 489–517, http://dx.doi.org/10.1016/B978-012095811-5/50017-1.

[59] K. Hofmeester, D. Wixon, Using metaphors to create a natural user interface for microsoft surface, in: CHI EA '10: CHI '10 Extended Abstracts on Human Factors in Computing Systems, 2010, pp. 4629–4644, http://dx.doi.org/10.1145/1753846.1754204.

[60] A.M. Tinga, D. Cleij, R.J. Jansen, S. van der Kint, N. van Nes, Human machine interface design for continuous support of mode awareness during automated driving: An online simulation, Transp. Res. Part F: Traffic Psychol. Behav. 87 (6) (2022) 102–119, http://dx.doi.org/10.1016/j.trf.2022.03.020.

[61] A.M. Tinga, I.M. van Zeumeren, M. Christoph, E. van Grondelle, D. Cleij, A. Aldea, N. van Nes, Development and evaluation of a human machine interface to support mode awareness in different automated driving modes, Transp. Res. Part F: Traffic Psychol. Behav. 92 (1) (2023) 238–254, http://dx.doi.org/10.1016/j.trf.2022.10.023.

[62] R. Hunicke, M.G. Leblanc, R. Zubek, MDA: A formal approach to game design and game research, in: Proceedings of the AAAI Workshop on Challenges in Game AI, vol. 4, (1) 2004, api.semanticscholar.org/CorpusID:6056852.

[63] G.P. Kusuma, E.K. Wigati, Y. Utomo, L.K. Putera Suryapranata, Analysis of gamification models in education using MDA framework, Procedia Comput. Sci. 135 (2018) 385–392, http://dx.doi.org/10.1016/j.procs.2018.08.187.

[64] F. Angelia, Suharjito, Improving english learning through game using 6–11 MDA framework, in: 12th International Conference on Information Communication Technology and System, ICTS, 2019, pp. 21–26, http://dx.doi.org/10.1109/ICTS.2019.8850951.

[65] S.D. Putra, V. Yasin, MDA framework approach for gamification based elementary mathematics learning design, Int. J. Eng. Sci. Inf. Technol. 1 (3) (2021) 35–39, http://dx.doi.org/10.52088/ijesty.v1i2.83.
[66] R. Junior, F. Silva, Redefining the MDA framework—The pursuit of a game design ontology, Information 12 (10) (2021) 395, http://dx.doi.org/10.3390/info12100395.
[67] Z. Mohammadzadeh, H.R. Saeidnia, M. Kozak, A. Ghorbi, MDA framework for FAIR principles, Stud. Health Technol. Inform. 289 (2022) 178–179, http://dx.doi.org/10.3233/SHTI210888.
[68] J. Hair, W. Black, B. Babin, R. Anderson, R. Tatham, Multivariate data analysis, sixth ed., Pearson Prentice Hall, Upper Saddle River, 2006.
[69] T.W. Malone, M.S. Bernstein, Handbook of collective intelligence, MIT Press, 2022, 9780262545846.