Mizar. Costellazione di pensieri

Rivista del Dipartimento di Studi Umanistici
Unisalento

Using Games for Cybersecurity Training

Antonio Balestra[1],

[1] *Assegnista di Ricerca – Dipartimento di Ingegneria - Unisalento*

Abstract: The use of "game" as a didactic strategy is always more widespread in training contexts, even in university education. Research and advances in ICT and educational technologies have allowed students to "learn by playing" even in asynchronous and distance learning contexts. Based on this approach, this paper described how simulation games and online games have been designed to promote learning of topics related to cyber security in the context of the European project called "EuSecure".

Keywords: learning by playing, didactic strategies, Eusecure Project.

Riassunto: L'uso dei "game" come strategia didattica è sempre più diffuso nei contesti formativi, anche nell'istruzione universitaria. La ricerca e i progressi delle TIC e delle tecnologie educative hanno permesso agli studenti di "imparare giocando" anche in contesti di apprendimento asincrono e a distanza. Sulla base di questo approccio, il presente lavoro descrive come i giochi di simulazione e i giochi online siano stati progettati per promuovere l'apprendimento di argomenti legati alla sicurezza informatica nel contesto del progetto europeo denominato "EuSecure".

Parole Chiave: imparare giocando, strategie didattiche, Progetto Eusecure.

1. Introduction

The great challenge for Higher Education Institutions (HEI) is to be able to foresee what the society of the future will be like, to design learning pathways capable of providing the next generation of citizens and policy makers with the necessary skills to respond to the changes in economic macro-scenarios, social structures, and the world of work. HEIs will need to know "what" to teach but, above all, "how" to teach in order to encourage students to move from “knowing” to “knowing how to do”, from “knowing how to do” to “knowing how to act in contexts” (Le Boterf, 2008). The complexity of this challenge is to promote a plurality of competencies, teaching students to know how to "be in change" and to possess the tools of "simplexity" (Berthoz, 2012).

The "what to teach" seems to be tied to aspects of security, resilience, and sustainability, to the risks that need to be addressed and prevented. The "how to teach" must consider the characteristics of generations Y and Z, the learning environments, synchronous and asynchronous teaching in presence and distance learning.

The Erasmus+ funded project "EUSecure: Interdisciplinary Training on EU Security, Resilience and Sustainability" (KA203 - Strategic Partnerships for higher education) addresses these aspects at HEI (Higher Education Institution) level from an interdisciplinary point of view. In this article, it will be addressed how cybersecurity

aspects have been designed and how they will be implemented in the EUSecure project.

2. Activity Types

Nowadays, the design of training activities mixes and matches traditional training methodologies and online learning tools to promote innovative methodologies: this is possible thanks to the number of digital tools available. This innovation supports new forms of teaching, made available thanks to the spread of, among others, virtual simulation platforms, virtual classrooms, mobile applications, and the like.

In this scenario, one approach emerges from the background: the production of open educational resources (OER) and Massive Open Online Courses. According to the Organization for Economic Co-operation and Development (OECD), OER should be defined as "teaching, learning and research materials that make use of appropriate tools, such as open licensing, to permit their free reuse, continuous improvement and repurposing by others for educational purposes" (OECD, 2015).

Given these premises, the innovative element of the SimMOOC of the EUSECURE Project is based on the realisation of online training-simulation activities, the aim of which is to structure learning experiences that arise from the encounter between doing and acting, in which digital tools are used and managed in an educational key to the boast of the quality of students' learning (Paparella, 2012).

Practical activity (learning by doing) favours the development of an adequate critical approach on the part of the students: the activities can be carried out in both virtual and face-to-face modes and are all aimed at placing the student at the centre of the learning process, giving him or her the opportunity to solve concrete problems even if they are virtual (Paparella, 2007).

In EuSecure, the design of the practical activities was developed considering three dimensions: 1) solo/group activity; 2) synchronous/asynchronous activity; 3) face-to-face/distance (digital) activity (Zappatore, Longo, Balestra, 2022), as highlighted in Figure 1.

Mizar. Costellazione di pensieri, n. 18 - Gennaio-Giugno 2023 ISSN 24995835 DOI 10.1285/i24995835v2023n18p.217

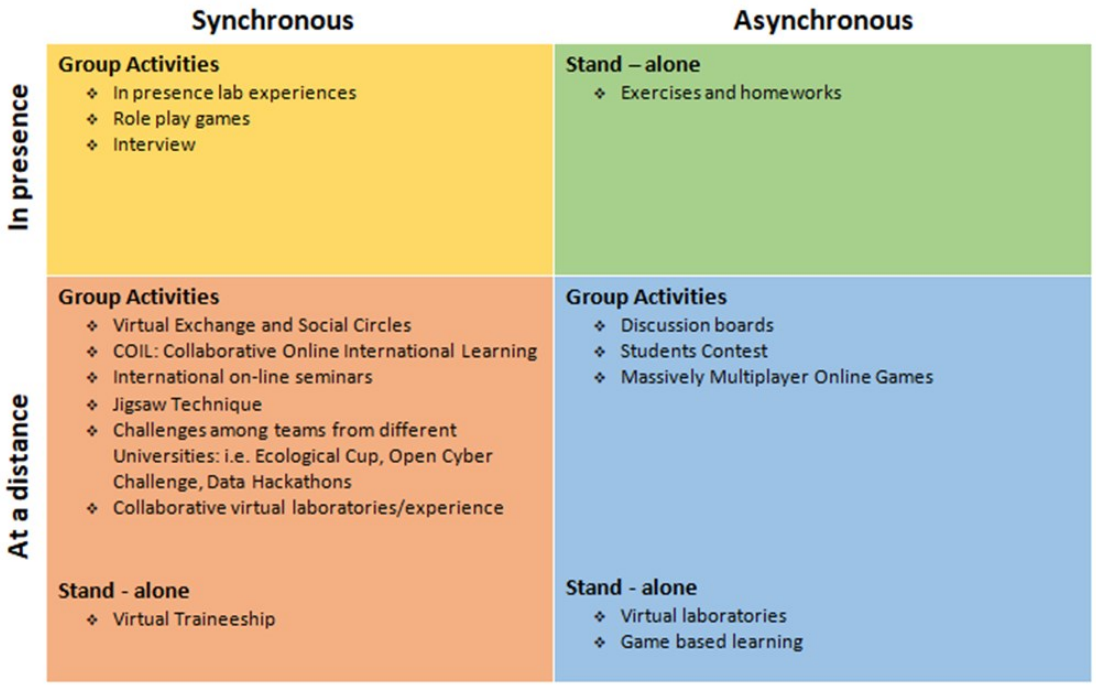

Figure 1.The three dimensions of practical activities.

In the course design phase, the lecturer will identify the practical activities taking into consideration not only the aspects characterising the module in terms of content but also what is represented in Figure 1.

Distance education separates both the teacher from the learner and the learner from the learning group, by means of digital communication technologies: virtual rooms, video calls, using the numerous tools implemented in bulk after the pandemic has started. On the contrary, “In presence” learning subsumes all the members of a class to be physically present at the same place. Blended learning combines the approaches explained and represents their synthesis. A synthesis that is not a simple distinction between presence and distance, between the physical and the practical, between the linear and the creative, but which follows an innovative pairing logic, to create a "generative environment of meaningful learning" (Maggi, 2020).

3. The EUSecure Project

The project “EuSecure SimMOOC: Interdisciplinary training on European Union security, resilience and sustainability” is a project funded by the European Union Erasmus+ Strategic Partnership in Higher Education Programme. The main objective is to contribute to European cooperation on issues related to security, resilience and

sustainability through education, offering students, professors, researchers but also professionals and the interested public, an international and multidisciplinary course. Through video lectures, asynchronous individual (game-based learning) and group activities (student contest, massive multiplayer online games), synchronous online group activities (international online seminars, collaborative virtual experience) it is intended to develop knowledge and skills on complex and interdisciplinary issues on the major challenges faced by Europe in the field of Security, Resilience and Sustainability. In order to achieve the above objectives, taking advantage of the synergies created by the complementarity of the partners involved, it is intended to create incrementally a series of real transdisciplinary modules in Security, Sustainability and Resilience Studies (SSRS) in order to develop them further and gradually, in a vertical modular system and possibly in joint degree courses at a later stage. The international partnership involves five universities (from Hungary, Greece, Italy, Portugal and Romania) and this allows to exploit their respective research areas of excellence, specific geographical collocations and featuring historical backgrounds in order to enrich the project's significance further.

The EUSEcure SimMOOC is characterized by the following 15 topics: 1) EU power (strategic autonomy) in a multipolar world; 2) Megatrends; 3) International Governance: Institutions, norms, multilateral regimes; 4) Maritime security; 5) Migration; 6) Cyber security and AI (Artificial Intelligence) risks; 7) Water security and water geopolitics; 8) Social media issues and fake news; 9) Sustainability, Resilience and Development; 10) Climate security; 11) Public health and pandemic management; 12) International development cooperation; 13) Humanitarian aid, Food security; 14) Critical infrastructure resilience; 15) Qualitative research methodologies.

The Objectives of the project are:

- developing an interdisciplinary course on EU security, resilience, and sustainability.
- designing a SimMOOC - a simulation-oriented massive open online course supported by practical and laboratory activities on EU security, resilience, and sustainability.
- launching the EuSecure course on EU security, resilience, and sustainability at the project partner universities, with a mixed form of training (based on SimMOOC), interactive international teaching elements, an international faculty, and international student groups working on common activities.
- creating a course for secondary school students on EU security, resilience, and sustainability.
- disseminating the relevance and results of the project to make it a widely available educational resource.

The main activities of the project, therefore, are addressed at developing an academic curriculum, training materials, teaching methodologies, and online platforms; designing transnational teaching/training/learning activities; designing an in-person summer and winter edition; and conducting events to disseminate the project.

The SimMooc of the EUSecure project will be delivered on the Moodle platform starting from the first semester of 2022-2023 academic year, as an activity of choice, in the 5 partner universities of the project. The attendance of the course will allow students to obtain a minimum of 2 to a maximum of 6 ECTS. The target audience is male and female students of bachelor's and master's degrees.

Module Structure

Each of the 15 didactic modules that characterize the EUSecure SimMOOC have been developed by working groups of at least 2 partner universities of the project, according to the structure described below.

1. Preparatory activities, testing and self-assessment of learning. The module dedicated to preparatory activities will allow the student to learn the basic constructs and appropriate terminology to study the topics covered in each module.
2. Video lectures, testing and self-assessment of learning. Each module includes 5 video lectures with a duration varying between 10 and 20 minutes. In the video lessons will be addressed in detail the topics that characterize each module.
3. Podcasts/videos, testing and self-assessment of learning. Each module features podcast or video resources in a maximum number of 3 and with a maximum duration of 20 minutes. These resources are selected from the web and provide insights into the topics covered in the video lessons. Also, in this phase there are tests to assess learning.
4. Practical activities, testing and self-assessment of learning. This phase includes interdisciplinary simulation activities specifically designed or customized ad hoc. The idea is to involve all students enrolled in EUSecure modules and beyond, to involve at least 100 students per institution. To provide them with real-life experience to use and deepen their knowledge and skills. The activities will be asynchronous individual (game-based learning) and group (student contests, massive multiplayer online games), synchronous online group (international online seminars, collaborative virtual experiences).
5. Required in-depth readings: Mandatory in-depth readings may be excerpts from

Mizar. Costellazione di pensieri, n. 18 - Gennaio-Giugno 2023 ISSN 24995835 DOI 10.1285/i24995835v2023n18p.217

official EU documents, scientific articles, essays, or in-depth studies created ad hoc.

6. Suggested in-depth readings: Suggested in-depth readings can be official documents of the European Union in whole or in part, scientific articles, essays, books. These readings allow the student to deepen in an autonomous way, both for personal culture and for professional objectives, the topics covered.

7. Final test of the module. The final module test will verify the learning of the topics covered and the activities carried out in every EUSecure SimMOOC module.

8. Final Course Evaluation Activities. The simulation game will be discussed in Section

4. The manual "Interdisciplinary training

The manual "Interdisciplinary training on EU security, resilience and sustainability" is the reference textbook of the course. It is one of the intellectual outputs of the project, written by all partner universities.

4. Module Overview: Cybersecurity and the Risk of AI

As described above, the learning modules have been designed according to a specific structure to outline the cognitive content of the module into subtopics to address and hands-on activities to practice. The learning objectives of the module "Cybersecurity and the Risk of AI" are:

- Provide students with the basics of the new type of threats and challenges of the information society.
- Introduce the topic of cyber-attacks: information-based attacks and attack methods.
- Present the complexity of cybersecurity and the risks associated with AI.
- Provide students with knowledge related to European cybersecurity strategies.

The different sub-topics covered by the module concern the challenges to security in the information society, the main actors and players in cyberspace, the classification of cyber threats and the short- and medium-term risks of AI-based societies.

The prerequisites and skills required of students are basic digital skills and a B2 level knowledge of the English language.

Due to the importance of the cognitive content covered and its implications in everyday life, Problem Based Learning, a student-centred approach to learning that fosters collaborative and cooperative learning, role-playing and online games were used to make learning more effective.

Based on the structure described in section 2.1, we detail the content and hands-on activities that will be developed in the module.

Mizar. Costellazione di pensieri, n. 18 - Gennaio-Giugno 2023 ISSN 24995835 DOI 10.1285/i24995835v2023n18p.217

1. Preparatory activities, testing and self-assessment of learning. Each pre-reading exercise will engage the student for an estimated 10 minutes of reading time. Topics covered will be cyberspace terminology with a focus on basic information society terms, overview of what and how many actors there are in cyberspace, cyber threats with a focus on the most common ones and core risk of artificial intelligence. Once the study phase is over, the student will be able to assess their learning by taking a multiple-choice test with feedback (formative assessment).
2. Video lectures, testing and self-assessment of learning. The module will feature 5 video lessons that will average 10 minutes in length. Each video lesson will be accompanied by some slides to help the student fix the concepts. The topics of the video lessons will be information society and security challenges, actors of cyberspace, cyberthreats with a focus on cybercrime, cyberwarfare, hacktivism/cyberterrorism and cyber espionage, threats of the near future, the risk of AI A multiple-choice test with feedback concludes this phase of the module.
3. Podcasts/videos, testing and self-assessment of learning. Two video products have been selected for this section: "The life of a hacker" a series divided into 12 episodes with an approximate duration of 5 minutes, created by NUPS CyberSec; some short videos starring Kevin Mitnick, selected from the YouTube channel of Cybercrime Magazine and produced by Cybersecurity Ventures. In this part of the module, testing and self-assessment of learning activities are provided as well.
4. Practical activities, testing and self-assessment of learning. SimMOOC participants will experience online, and in-person hands-on activities designed to enable inquiry-based learning, problem-based learning and design thinking. The tools will enable the implementation of simulations as well as enable inter-peer communications and knowledge sharing opportunities. The hands-on activities for the "Cybersecurity and the Risk of AI" module will be: Capture The Flag (CTF), an online collaborative role-playing game, customized considering the basic skills of the module participants; [d0x3d!] a cooperative board game; a synchronous role-playing game, based on the document "ERNCIP training for professionals in Critical Infrastructure Protection: from risk management to resilience" (Lazari, 2017).
5. Compulsory and suggested in-depth readings. Some official documents from the European Union have been identified for this part of the module to allow participants to perceive the international dimension of cybersecurity challenges in a much more structured way. Documents that refer to the EU's approach to AI (European

Commission 2020), (European Commission 2021), and how to improve trust in AI (Bahrke, Manoury, 2020) will be considered.

6. Final test of the module. The final module test will include a series of multiple-choice questions to assess achievement of the learning objectives.
7. Using games for Cybersecurity Training.

Learning through play has been an approach that has crossed the boundaries of childhood for several years. Play is used in school and university settings but also in adult education settings (e.g., corporate training). There are several pedagogical approaches, methods and tools that use play to foster learning.

Described below are the game methods used for the "Cybersecurity and the risk of AI" module and the simulation game designed for the final evaluation of the whole EUSecure project course.

Capture The Flag (CTF)

Capture the Flag (CTF) is an online game mode, typically used to develop skills related to cybersecurity. It is a hacking game, in which the objective is to find the flag. In a predefined time, players must solve problems of varying complexity from manipulating data traffic, to techniques of obtaining administrative privileges of a system or remote and unauthorized access (version of the game called Jeopardy). In the version called Attack/Defence, in addition to breaking into someone else's computer system, you must also defend your own system from the attack of your opponents (Vykopal, Švábenský, Chang, 2020) The game is inspired by and takes its name from the traditional children's game called Capture the Flag.

The version currently being developed for SimMOOC will offer simplified challenges related to User and Password security, security of sensitive digital document data, and use of Caesar's encryption. The addition of a base64 URL decoding challenge, which is a more advanced CTF game type, is currently under evaluation, as it might be less appropriate for the potentially variegated skills of the course participants, since EUSecure SimMOOC is open to all students of different degree programs.

[d0x3d!]

[d0x3d!] is a cooperative board game. The name comes from the hacker jargon used to describe the public online dissemination of personal and private information about a person, usually with malicious intent.

Mizar. Costellazione di pensieri, n. 18 - Gennaio-Giugno 2023 ISSN 24995835 DOI 10.1285/i24995835v2023n18p.217

In [d0x3d!] players take on the role of a hacker and attempt to infiltrate a network to recover some digital assets. The digital assets to be recovered are personally identifiable information, authentication credentials, some financial data, and intellectual property assets. The goal is to recover the data without being caught, evading the oversight of network administrators. From a learning point of view, the game is very interesting because the team of hackers plays together against the game. This means that the group of players collaborate for a common purpose, adopting problem solving skills and using common strategies. The game was chosen because the goal of the developers is to introduce students to network security terminology, attack and defense mechanisms, and basic computer security concepts.

Simulation Games

A simulation is a form of role-playing, structured in scenarios that are more complex and closer to real-life settings. Students can take on a role or play themselves. In simulation games, decisions are based, often, on formal game rules drawn from real life. The effectiveness of a simulation game allows scenarios to be structured for even very complex topics. The student takes on a particularly active role in which he or she must consider different strategies for intervening in a critical situation.

The simulation game designed for the module "Cybersecurity and the risk of AI" is based on a real event and draws from the document "ERNCIP training for professionals in Critical Infrastructure Protection: from risk management to resilience" (Lazari, 2017). In 2016, the BlackEnergy malware, a Malware for Cyber-Physical Attacks hit some power transmission companies in Europe by exploiting some specific Windows-related vulnerabilities. The attack caused cascading service disruptions in many regions of the EU, with more than 100 million citizens from five EU countries losing access to electricity and gas. In addition, the pattern of outages was random in the affected countries, making it even more difficult to identify the systems that were affected first.

Starting from the Black Energy scenario, students, guided by a series of questions, will have to discuss some issues related to aspects of decision making (Crisis Management, Information Sharing, Consequences).

Based on this scenario, some students of the Bachelor of Arts, Music and Performing Arts and some students of the Bachelor of Information Engineering of the University of Salento, will develop a multiplayer videogame (mimicking Minecraft or Fortnite) that will simulate an attack on a power plant in a city, with a consequential blackout. Players

Mizar. Costellazione di pensieri, n. 18 - Gennaio-Giugno 2023 ISSN 24995835 DOI 10.1285/i24995835v2023n18p.217

will have to restore electricity by following real-world protocols, making decisions, and using collaborative strategies.

The final assessment activity of the course will be a simulation game. This activity also aims to replicate reality, based on the reproduction of certain roles and having as reference rules and norms existing in the real world.

This simulation game will deal with the theme of the European Health Union and will last 8 hours.

The simulation activity developed for the EUSecure project features two forms of simulation: a classroom simulation and a simulation of European councils, including two COREPER (Committee of the Permanent Representatives) meetings, which are recommended for the final joint simulation. The topic will be related to pandemic and health care and the time allotted for the simulation will depend on the universities, but the activity will have a deadline. Each partner university in the EUSecure project will develop the national position of several EU member states on the EUSecure topic. The developers of the simulation will produce a manual on how it should be organized, along with guidelines for developing national positions. In the simulation, the role of chair will be played by the mentor. Also, since only 15 students are participating in the simulation but there are 27 EU member states, the choice of countries and country positions will be left to the tutor. At the end of the game, students will stop "acting" their roles and discuss the situations that occurred.

The two simulations were tested during the project's Summer School and Winter School, which took place in Lecce and Athens respectively, with the participation of lecturers and 50 students from all partner universities.

5. Conclusion

Preparing the next generation to face the future is the great challenge for institutions of higher education. A challenge that cannot be failed. Learning by playing can be an approach to teach even complex and structured topics such as those related to cybersecurity. If the "what to teach" is important, the "how to teach" is fundamental, using methodologies and tools useful to encourage the development of strategic thinking, problem solving, creative thinking and collaborative work.

Cyberspace is a fundamental concept in the modern world and will be increasingly so in the future. A hotbed of growing power conflicts between the nations of the world but also a favorite crime scene that now poses an equally dramatic threat to members of

society. A world that is unfolding before our eyes, but in many ways still unknown.

References

Bahrke J., & Manoury C. (2021). Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence. European Commission - Press Release, 2021. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682.

Berthoz, A., & Weiss, G. (2012). Simplexity: Simplifying Principles for a Complex World. Yale University Press. Retrieved 28 Apr. 2022, from https://yale.universitypressscholarship.com/view/10.12987/yale/9780300169348.001.0001/upso-978030016934

European Commission. (2020) WHITE PAPER On Artificial Intelligence - A European Approach to Excellence and Trust. Brussels, Belgium, 2020.

European Commission. (2021). Fostering a European approach to Artificial Intelligence. Brussels, Belgium.

Lazari, A. (2017). ERNCIP training for professionals in Critical Infrastructure Protection: from risk management to resilience. EUR 28657 EN. Luxembourg (Luxembourg): Publications Office of the European Union; 2017. JRC105204. DOI 10.2760/88009

Le Boterf G., (2008). Costruire le competenze individuali e collettive. Napoli, Alfredo Guida Editore.

Maggi D. (2016). Allenatore, atleta, ambiente: il modello delle 3A. Progettare ambienti di apprendimento. FORMAZIONE & INSEGNAMENTO. Rivista internazionale di Scienze dell'educazione e della formazione, vol. 14, no. 3, pp. 157–166.

Paparella N., (2007). Ontologie, Simulazioni, Competenze. Amaltea Edizioni.

Paparella N., (2012). L'agire didattico. Napoli, Alfredo Guida Editore.

Vykopal J., Švábenský V., & Chang E. (2020). Benefits and Pitfalls of Using Capture the Flag Games in University Courses. Proceedings of the 51st ACM Technical Symposium on Computer Science Education. Association for Computing Machinery, New York, NY, USA, 752–758. https://doi.org/10.1145/3328778.3366893

Zappatore M., Longo A., Balestra A. (2022). Designing a University SimMOOC for Security, Resilience and Sustainability in Europe: the EUSecure Project. IEEE Learning with MOOCS (LWMOOCS), Antigua Guatemala, Guatemala, 2022, pp. 56-60, doi: 10.1109/LWMOOCS53067.2022.9928004.