Human Factors in Cybersecurity, Vol. 91, 2023, 101–110
https://doi.org/10.54941/ahfe1003724

C.S. Technopoly: A Megagame for Teaching and Learning Cybersecurity

Stewart Kowalski[1], Eduard von Seth[2], and Erjon Zoto[1]

[1]Norwegian University of Science and Technology, Norway
[2]Stockholm University, Stockholm, Sweden

ABSTRACT

In this paper we present our ongoing research where we are attempting to integrate sustainable development issues into a megagame designed to teach cybersecurity. There are several serious games that have been developed to teach and inform individuals about sustainability issues but none that deal specifically with both cybersecurity and sustainability issues. A Megagame is a multiplayer game with between 30–40 players who play in teams of 3–5 players that take on specific roles in dealing with complex problems that cover subject matters ranging from science fiction and heroic fantasy to political, economic, historical, and even cyber conflicts. We have built and tested a megagame entitled CS -Technopoly using the socio-technical framework of sustainability proposed by Geels and integrated it further with the Security by Consensus Model proposed by Kowalski. The intended learning objectives of the game, such as teaching adversarial and sustainable systems thinking by exposing the students to cyber threat intelligence reports and cyber security investments decision making, were tested by performing semi-structured interviews of a stratified sample of the participants. Preliminary results from 11 interviews from the two first trials of CS Technopoly indicate that the participating security experts found that C.S. Technopoly would be a useful tool for team building and improving collaboration between security departments and upper strategic management.

Keywords: Serious games, Cybersecurity education, Sustainable systems, Megagames

INTRODUCTION

Serious games have been shown to be an effective method of teaching and discussing complex issues. given their ability to engage more of the participants' senses and human-focused design which nudges players to want to learn and understand more. Many games have been focused on raising awareness and teaching about technical risks and countermeasures. This, however, misses the fact that risks are not just of a technical nature, nor social, but a combination of the two socio-technical root-causes which have shown to underline most of the cybercrime issues (Zoto et al., 2019). There are also several serious games that have been developed to teach and inform individuals about sustainability issues. Katsaliak (2015) found in a systematic literature review 35 publications on sustainability developmental games that range from simple board games for 4–5 players to complex pervasive games. The Games4Sustainability site lists over 100 games and simulations arranged

according to the 17 United National sustainability goals (Game4Sustainablity 2022). However, to the authors' knowledge, only two Megagames have been run that tackle the problem of sustainable development, *The Climate Change Game,* (2020) and an adaptation of the *Alliance megagame* (Alliance 2019, Megagame 2019). These two Megagames did not however include cybersecurity game mechanics.

The increase of cyber threats and attacks has garnered much scrutiny from media, the public and scholars in the last decade. As more and more devices are connected to the internet, this intertwining of information and ICT with everyday life has resulted in a cyber-physical society. The search for solutions involves new and effective cyber security policies and regulations, the development of security software, and secure software and development practices. These new solutions can act as a double-edged sword. As new technologies are added to the technical stacks of different systems and services, new threats keep on arising. Multiple instances across different industrial segments have raised the need to educate more information security professionals to meet this challenge. The reported global shortage ranges from 2.7-3.4 million professionals according to (ISC)2, 2022. In order to adequately face this challenge, new ways of educating and training people on how to secure information systems are needed.

Socio-technical systems analysis is the analysis of the problems and their potential solutions that arise with the adoption and integration of cyber and information technologies in society (Kowalski, 1994). In this paper we have sought to explore how a form of serious game called megagames could be used to raise awareness on socio-technical systems analysis, cyber security investments, and threat intelligence in an adversarial environment. This research contributes to the growing body of knowledge on serious games and cyber security training.

The paper is divided into 6 parts. Following this introduction in the next part we discuss the research goals and methodology used in our ongoing research. In the third part the theoretical background to the game design is discussed. In the fourth part we outline a more detailed description of the game mechanics and design. The fifth part outlines preliminary results from interviews of the participants of the two trial runs of the game. The paper then concludes with a summary and outline of the current development plans for future testing and validation of the C.S. Technopoly megagame.

RESEARCH GOALS AND METHODOLOGY

The purpose of this research is two-fold. The first is to continue the research of Dewar (2018) and investigate if there are alternative ways one can teach cyber security policy. The second is to investigate how one can teach adversarial and sustainable systems thinking and awareness by exposing players to investment decisions' scenarios concerning allocation of funds for transitioning towards sustainable production and socio-technical cyber security protection efforts. The aim is to model and build a serious game using the socio-technical framework that teaches adversarial and sustainable systems thinking.

The problem is that much of today's education is based on a faulty mental model of security. Most certificates and university programs focus on the confidentiality, integrity, and availability (CIA) triad. The attacker's perspective is not present. The Security By Consensus (SBC) mode shows both the static and dynamic properties of security (Kowalski, 1994). It divides the socio-technical systems into observable categories of structure, culture, social factors like new regulations, change in societal culture, norms, ethics, and new methods and procedures that can all affect the security posture of any organization today.

Considered all the above assumptions, the main research goal for the work behind this paper would be the following:

> "To develop a cyber security serious game that would help in reducing the required manpower and monetary resources when creating cross-disciplinary team exercises and training".

In order to achieve this, the authors decided to adopt a Design Science (DS) strategy, together with the DS sub-activities and processes. Furthermore, 9 requirements were identified based on a socio-technical systems analysis. The requirements then served as the foundation for the design and development of the serious game C.S. Technopoly.

Design Science Overview

Design science is about the methodical generation of knowledge through design of the artificial (Baskerville, 2008). In other words, new knowledge is discovered by creating artifacts that solve real problems. The objective here is to create and use artifacts that can advance the lives of individuals, organizations and the society as a whole (Bider, Johannesson and Perjons, 2013). Design science is built on the principle that the creation and application of artifacts, such as a software model, can produce knowledge and understanding of a problem and its corresponding solution (Bider, Johannesson and Perjons, 2013). Artifacts are abstractions of general solutions to a particular set of problems (Baskerville, RL, Pries-Heje, Venable 2009). These sets of problems, otherwise known as generic problems, can be found either as individual problems derived from a real-life situation or through the identification of the problem from previous research then assessed as part of a more general class of problems (Bider, Johannesson and Perjons, 2013).

However, DSR was not the only methodology considered for this research project. Much like DSR, Action Research (AR) strives towards solving real, practical problems in a real-world setting by interventional means on top of generating new knowledge (Johannesson & Perjons 2014). Action research was deemed unsuitable for this project as it risks becoming resource-intensive when the researcher is tasked with iterating and finding a solution to the problem until the problem is solved. As this research project is time bound, it would risk not producing a solution that solves the problem nor contributes to the existing body of scientific knowledge. The more artifact- (solution-)centered methodology was found to guarantee that even if the game is found not to adequately meet the current research goal, at least the discovered knowledge base would be relevant.

BACKGROUND

The Design Science Research (DSR) model of the workflow describes five main activities: Explicating problem, Eliciting requirements, Design and Develop artifact, Demonstrate artifact, and Evaluate artifact (Johannesson & Perjons 2014). To produce an artifact, inputs are transformed by the activities into outputs, thereby producing an artifact that solves the problem. These activities contain sub-activities which are executed upon iteratively and in a particular order, forming stages or cycles in order to reflect the "changing environment, shifting stakeholders' interests, and unclear problem situations" (Bider, Johannesson and Perjons, 2020).

As an example, during the Design and Develop artifact, the initial idea was to build a game that would expose cyber security practitioners, training program participants and specifically C-level executives to systems thinking, adversarial thinking and the socio-technical nature of cyberspace through a serious game. After conducting a literature review on cyber security serious games, a gap was found in the area of games that could perform deeper conceptual transfers and that fell within the scope and resources available to

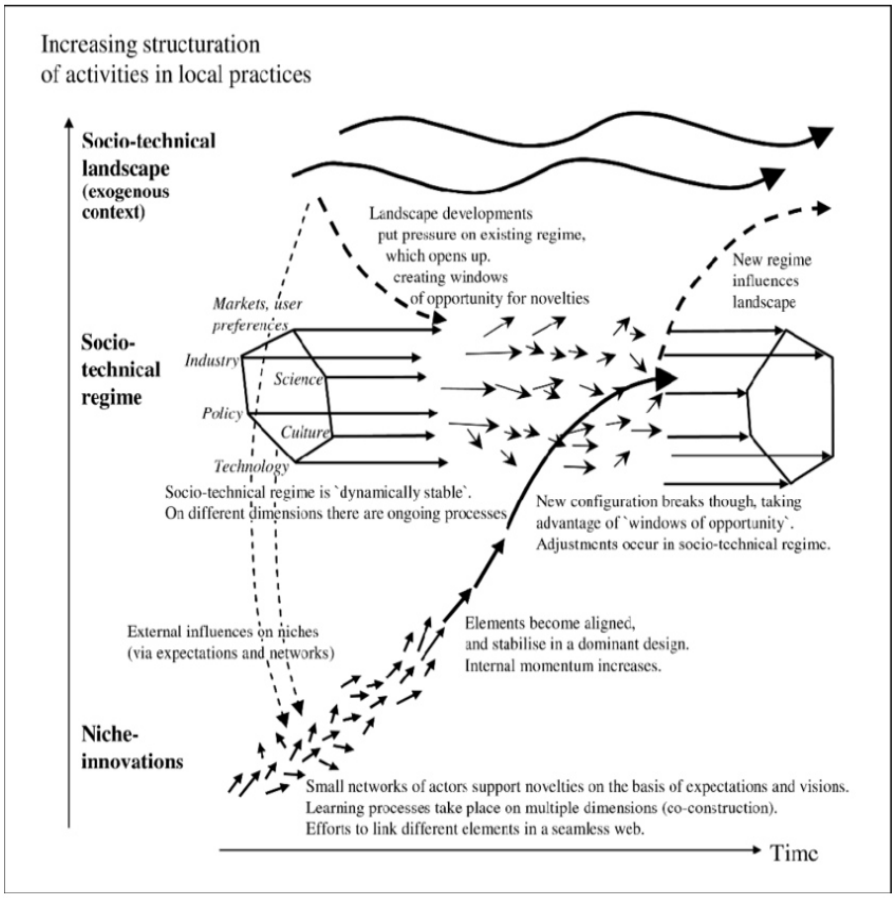

Figure 1: The multi-level perspective by Geels and Schot (2007:401).

this study. The choice quickly fell on a strategy game. The question arose on which model to use that could adequately simulate the socio-technical nature of the world as it is and as its systems constantly transition. Having identified Geele's model of socio-technical transitions Geels, F. (2019), as a suitable model, the question moved on to how to express it in a serious game.

The authors have experienced how mega games can simulate political, economic and military systems. The question then arose if it would be possible to apply Geele's socio-technical transitions model to current geo-political situations in a mega game scenario. Existing cyber security games either lack depth or have high costs attached to them. The authors have experienced the game and seen the potential for adapting cyber security serious games to the flexible, cost-effective, immersive and fun structure of mega games. As mega games consist of multiple concurrent sub-games going on, the authors saw the synergic effect of combining existing serious games into an emerging narrative scenario-based serious strategy game.

GAME MECHANICS AND DESIGN

C.S. Technopoly is a combination of a live-action role playing game and a tabletop board game, otherwise known as a megagame. Megagames usually last 6 hours, but this megagame has been shortened down to 3 hours.

Intended Learning Outcomes

The intended learning outcomes refer to the question of whether the game solves the awareness problem and to what degree. This includes understanding about cyber security investments and risk management. In addition to that, participants of the game should feel that they have learned about:

- Sustainable Systems thinking and how to navigate and change the system
- Adversarial thinking
- Negotiation and estimating risk with technological changes
- Understanding threat intelligence
- Hype curve for security technology
- Cooperation and when it is useful
- Antitrust and its effects

Domain Requirements

Role playing games are forms of simulations. Underlying every simulation is an abstract model of the world it is supposed to imitate (Johanesson & Perjons 2018). One requirement that should be achieved is that of having an adequate model of cyber security policy to aid with developing the role-playing game. Other requirements include the following:

- **Offensive capabilities should be present in the game.**
- **Players should face the same uncertainty over attribution in the game.**
- **Nation-states should be represented in the game.** They should be able to affect regulation and invest in technologies.
- **Companies should be represented in the game.** They should not have offensive capabilities.

- **Threat and Attack frameworks should be represented in the game.**
- **Security technology solutions should be represented in the game.** There should be an aspect of cyber security investments Hype cycle.
- **Security value chain security controls should be represented.**
- **Players should have to manage the need for profit and keeping their organization secure.**

Game Description

Players are called to use not only their cyber security knowledge to interpret the threat intelligence reports that are given throughout the game, but also their understanding of diplomacy to build or destroy alliances, in addition to basic business and risk analysis to make cybersecurity purchases or investment. Their decisions along with some luck will decide if they manage to mitigate and even prosper from the different cyber events throughout the game.

Players are divided into different teams. The three playable teams are Nation-states, Businesses, and security technology startups. The teams exist in a semi-fictional world where the aim of businesses is to achieve technological domination, the aim of startups is to develop and sell their security innovations in the hope of becoming part of the dominant regime, and nations want to extract as much taxes as possible from their companies. Amongst them is the established and accepted dominant regime called Military Industrial Cyber Complex (MICC). MICC performs information sharing, recommends solutions and can financially support any given team at a time. MICC is not a playable character, but they are essentially in control. Incidentally, the game is facilitated by a team of 2–3 people, also known as control or incident masters.

The story narrative of C.S. Technopoly is driven forward by threat intelligence briefs. These intelligence briefs have a technical and political component. Sometimes the intel briefs detail a breach. Sometimes they detail incidents where it has not been established that a breach has occurred, only that relevant actors should be wary. The attacks are orchestrated by cybercrime groups and Advanced Persistent Threat (APT) groups that are native to the different playable countries, but that can attack anywhere and multiple targets simultaneously. The teams have to protect themselves against the attacks by investing in the right security controls. To their aid is the security value chain team sheet where they place their investments (chips) together with the chosen security control cards.

The security control cards are divided into the four types of security controls: Detect, Protect, Respond and Recovery. The Deter security control category was omitted during the playtesting phase as initial feedback from the focus group was that it would be confusing even to information security specialists. These security controls are in turn divided into social and technical controls. The idea being that e.g., deploying an incident response (IR) team that lacks experience with regular incident exercises shouldn't be as effective as deploying an experienced IR team. Teams don't just have to

be concerned with making security control investment, they also must ensure that their ability to produce is maintained.

The game is divided into rounds. Before the first round begins a test attack round is run by one of the Control/incident masters with the purpose of showing how to use the die, how the attack mechanics work and how cyber defense technology and production investments are done.

Once an attack is announced, the teams might win or lose their money depending on the die roll and type of technology they chose to invest (Fig. 3).

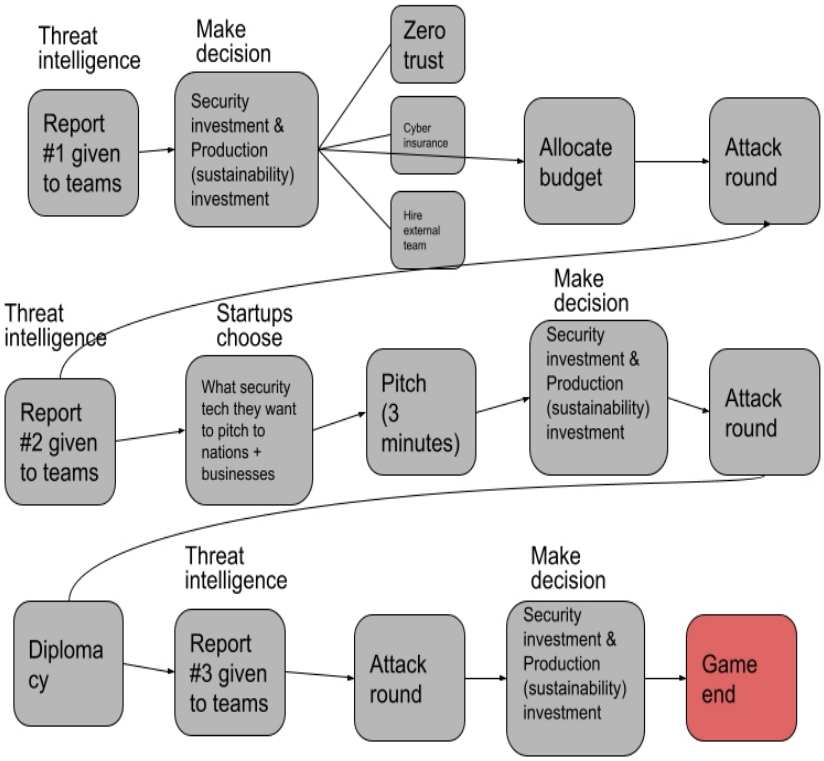

Figure 2: Flow chart of C.S. Technopoly game sequence.

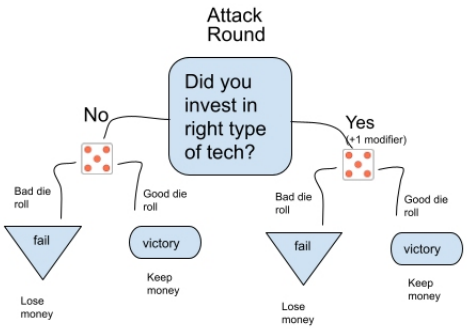

Figure 3: Flow chart of attack rounds.

RESULTS

An expert evaluation was conducted using stratified sampling with cyber security experts, educators and general public groups. The primary data collection method was post-session semi-structured interviews in which the participants reflected on their experiences. 18 people played the game and 11 people responded to the interview request. Participants found overall the game to be engaging, even fun. They also appreciated being exposed to threat intelligence and cyber security investments in a realistic semi-fictional narrative. Soft skills like collaboration within teams and with entities were recurring themes. Constructive criticism related to a large degree to reducing complexity, making the game longer than the offered 3 hours, and providing pre-game materials for them to be better prepared. Two main themes were identified during the thematic analysis: improving the clarity of game mechanics and learning outcomes.

Semi-Structured Interviews

Improve clarity of game mechanics

One common theme was a reported struggle to grasp the rules of the game. The comment below is exemplary:

> "So, I think if you had said something a little more like, "ok people, what matters is not what you answer but what aspects you think, in what phases, and what you invest. And so with the dice, the outcome of the defence you set works. And that Had given us a kind of, "aha". Because what you brought was relevant in preparation for a live situation. But we didn't understand that the choice of technology didn't matter."

In addition, participants suggest pre-game text or a video presentation showing gameplay narrated by a knowledgeable person.

Learning outcomes

A common theme when analyzing learning outcomes was a deeper understanding of context, as exemplified by the following comment.

> "I like workshops like that. So, anything that makes people put things in the right context. Because it's a context, isn't it? That learning was through group work in the form of telling a story[...] our organization can be attacked, but what we are most afraid of is that our customers will be attacked and especially that the attacks will come through us. And this play helps us understand the context to the customers. And we have many large customers. Real customers. Equinor, Statnet, the defence, the tax authority, so we definitely have customers who are attacked all the time."

Individual Survey

All 11 participants were asked to answer a short questionnaire. As a whole, the responses from the survey complement the interviews. The game experience frameworks of PLEXQ, Boberg, M. *et al.* (2015), UGALCO Peixoto et al. (2015), and EGameFlow (Fu et al., 2009) were selected to measure the participants' game experience. The survey allows the validation of the

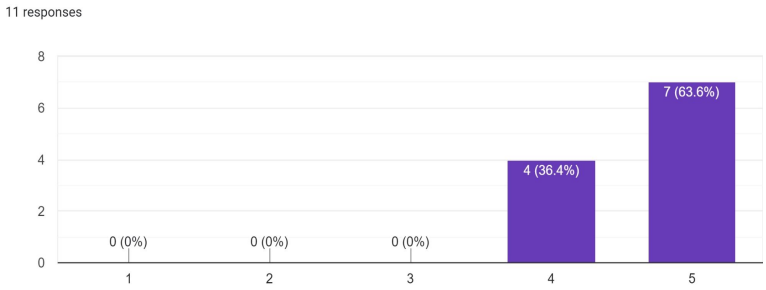

Figure 4: Did you have fun during the game play?

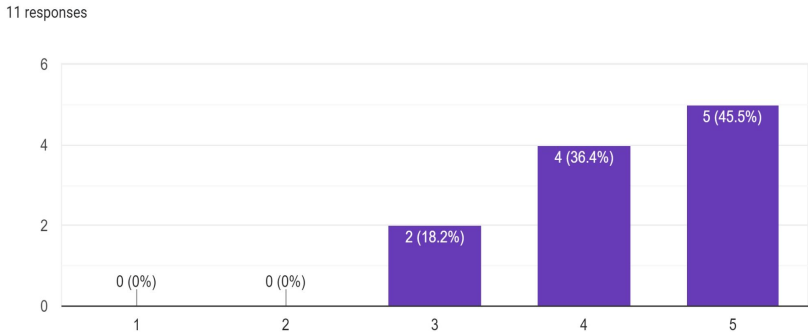

Figure 5: "Did you learn new information security concepts?" (1-5).

interviews. Meaningful conclusions, however, are not possible because of the limited sample size. Some results are shown in Fig. 4 and 5.

To conclude, one of the expressed requirements from one of the subject matter experts is for the game to act as the foundation for further development of Cyber Defence Exercises and tabletop exercises in a cyber range platform of training exercises. However, the game is not limited to local practices as it is conceivable that the game could be used for organizational capability assessment which would involve different stakeholders.

CONCLUSION

In this paper, the authors have succeeded into showcasing the current research gap when designing cybersecurity serious games dealing with sustainability issues. The gap can be addressed by designing megagames and using them for training different target groups spanning across all industrial segments. Preliminary results show that such megagames can help improve teamworking skills and increase collaboration between the security (IT) teams and upper management. Future work will help customize the process towards the intended audience, as well as integrate better sustainability aspects with ongoing security events and related strategies.

REFERENCES

Alliance 2019, https://mymegagame.weebly.com/, Access 2022-12-23.

Baskerville, R. (2008). What design science is not. *Eur J Inf Syst* 17, 441–443 (2008). https://doi.org/10.1057/ejis.2008.45

Bider, I., Johannesson, P. and Perjons, E. (2012) "Design Science Research as movement between individual and generic situation-problem–solution spaces," *Designing Organizational Systems*, pp. 35–61. Available at: https://doi.org/10.1007/978-3-642-33371-2_3.

Boberg, M. *et al.* (2015) "PLEXQ: Towards a Playful Experiences Questionnaire," *Proceedings of the 2015 Annual Symposium on Computer-Human Interaction in Play* [Preprint]. Available at: https://doi.org/10.1145/2793107.2793124.

CS Technopoly 2022, https://cstechnopoly.wordpress.com/ Accessed 2022-11-30.

Dewar, R. (2018). Cyber Defense Report: Cyber Security and Cyber Defense Exercises, September 2018, Center for Security Studies (CSS), ETH Zürich.

Fu, F.-L., Su, R.-C. and Yu, S.-C. (2009) "EGameFlow: A scale to measure learners' enjoyment of e-learning games," *Computers & Education*, 52(1), pp. 101–112. Available at: https://doi.org/10.1016/j.compedu.2008.07.004.

Geels, F (2019), Socio-technical transitions to sustainability: a review of criticisms and elaborations of the Multi-Level Perspective, Current Opinion in Environmental Sustainability, Volume 39, 2019, https://doi.org/10.1016/j.cosust.2019.06.009

Geels, F. W. and Schot, J. (2007) "Typology of sociotechnical transition pathways," *Research Policy*, 36(3), pp. 399–417. Available at: https://doi.org/10.1016/j.respol.2007.01.003.

(ISC)2, 2022, *CYBERSECURITY WORKFORCE STUDY 2022*. rep. (ISC) [2]. Available at: https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx (Accessed: January 30, 2023).

Johannesson, P. & Perjons, E. 2014. *An Introduction to Design Science*. 1. Springer Cham.

Katsaliaki, K., & Mustafee, N. (2015). Edutainment for Sustainable Development: A Survey of Games in the Field. *Simulation & Gaming*, *46*(6), 647–672. https://doi.org/10.1177/1046878114552166

Kowalski, S. (1994). *IT Insecurity: A Multi-disciplinary Inquiry*. Stockholm University

Megagame 2019, https://greatglory.org.sg/megagame-2019/, Accessed 2022-12-22.

Peixoto, D. C., Resende, R. F. and Padua, C. I. (2015) "Evaluating software engineering simulation games: The UGALCO framework," *2014 IEEE Frontiers in Education Conference (FIE) Proceedings* [Preprint]. Available at: https://doi.org/10.1109/fie.2014.7044204

Seay J., (2022), Active Learning Immersive Scenario Games in Teaching & Learning: Megagames, https://libguides.library.cofc.edu/c.php?g=929135&p=6693758

Slupska, J. *et al.* (2021) "Participatory threat modelling," *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems* [Preprint]. Available at: https://doi.org/10.1145/3411763.3451731.

Zoto E., M. Kianpour, S. J. Kowalski, and E. A. Lopez-Rojas, 2019 "A Socio-technical Systems Approach to Design and Support Systems Thinking in Cybersecurity and Risk Management Education," Complex Systems Informatics and Modelling Quarterly, CSIMQ, no. 18, pp. 65–75, 2019. Available https://doi.org/10.7250/csimq.2019-18.04