STAP
Smart Technologies Academic Press

Journal of Cyber Security and Risk Auditing

https://www.jcsra.thestap.com/

Check for updates

The Role of Simulating Digital Threats through Interactive Theater Performances

Hayder Jaafar Aldaghlawy[1], Mahmood A. Al-Shareeda[2]

[1]*Department of Art Education, College of Fine Arts, University of Basrah, Basra, Iraq.*
[2] Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, Basra, Iraq.

ARTICLE INFO

Article History

Received: 17-05-2025
Revised: 30-07-2025
Accepted: 23-08-2025

Vol.2025, No.4

DOI:
https://doi.org/10.63180/jcsra.thestap.2025.4.7

***Corresponding author.**
Email:
mahmood.alshareedah@stu.edu.iq

Orcid:
https://orcid.org/0000-0002-2358-3785

ABSTRACT

Amid increasingly sophisticated cyber threats embedded in everyday digital life, the public's understanding and interest in these dangers remain limited. Existing cybersecurity education pedagogies lack effective, ethics-based reflection, leaving significant blind spots in comprehending both the digital and ethical landscape. This paper explores the potential of interactive theater to constructively simulate digital threats—such as surveillance, phishing, and data breaches—for experiential learning and ethical reflection. Using a qualitative case study research method, data were gathered from documentation, audiences with auto-ethnographical reflection, post-performance surveys, and interviews. The results suggest that politically informed theatrical simulations provide an effective means of translating arcane digital concepts into embodied encounters that resonate emotionally, provoke ethical reflection, and, in some cases, inspire action. Through the lenses of performance theory, simulation theory, and critical digital studies, this study argues that interactive theater is not only a pedagogical mediation but also a critical cultural intervention in the age of surveillance capitalism. The study contributes to both cybersecurity education and performance studies by advancing a hybrid framework for public engagement in the affective and ethical dimensions of digital security.

Keywords: Interactive Theater; Cybersecurity Education; Digital Threat Simulation; Surveillance Capitalism; Participatory Performance; Critical Digital Pedagogy.

How to cite the article
Aldaghlawy, H. J., & Al-Shareeda, M. A. (2025). The Role of Simulating Digital Threats through Interactive Theater Performances. Journal of Cyber Security and Risk Auditing, 2025(4), 276–286.

1. Introduction

In a time when digital systems touch virtually all aspects of society, from social life to political structures and transactions, the security of information systems is essential for both personal and societal well-being [1, 2]. But the discussion around cybersecurity threats is still fragmented, abstract, and often disconnected from ethical considerations [3–5]. Despite growing numbers of technical solutions—from two-factor authentication to AI-generated threat analysis—the day-to-day human side of security, encompassing awareness, responsibility, and conduct, remains a significant point of weakness [6, 7]. As a result, there is a pressing struggle for popular, emotionally compelling, and ethically reflexive models of public cybersecurity education [8–10]. This work considers interactive theatre performances as a platform to stage digital threats – data breaches, phishing scams, surveillance – and prompt audience reflection upon their digital lives. Using theories from performance [11, 12], simulation, and digital ethics [13, 14], the research explores how theatre can take on abstract digital concepts, stir ethical dissonance, and incite shifts in behavior and attitude towards privacy and online safety.

Although past research has shown the educational benefits of simulation in training [15] and the potential of theater as a forum for societal critique [16–18], there is scarce empirical work on immersive, live performance in connection with cybersecurity pedagogy. Our paper aims to contribute to fill this gap by covering a case study of a participatory theater production that was developed to simulate digital threat cases. The production combined live audience voting, moral quandaries, and fan-out environments that recreated the emotional and informational environments of actual cybersecurity deluges [19–21].

Similarly, Kim et al. [22] performed a multi-study to evaluate the effect of gamification on cybersecurity learning, and they concluded that gamification can improve learners' motivation and understanding of the concepts of security. While drawing on live examples, how VR platforms performed live theatre during the COVID-19 situation was discussed in Baia et al. [23]. It identifies experimental productions and suggests a conceptual framework based on ethnography and arts-based research for understanding new forms of performance, both virtual and live/live-streamed. Adejumo et al. [24] underline that the financial sector is increasingly protected by cybersecurity. It specifically addresses the key challenges of ransomware and phishing and how they might be met. Meanwhile, it advocates proactive, cooperative ways of gaining credibility, resiliency, and trust in the grounds of digital financial territory. The focus of this study is to explore how simulating digital risk through interactive theater can help improve public perceptions of cybersecurity and encourage ethical and behavioral interplay. More precisely, it answers the following questions:

• How do members of the audience physically encounter and interpret simulated digital threats in a 'live', participatory performance context?
• What kind of emotional, cognitive, and moral experiences do such simulations generate?
• How do they affect post-performance reflections or the digital?

This work has an impact on a number of fields. In the context of cybersecurity teaching, it presents a pedagogical model that integrates storytelling, simulation, and embodiment to maximize engagement. For durational and live art, it also pushes interactive theater's limits of digital ethics and technological critique. Lastly, societal implications of the work include new methods to foster critical digital citizenship, which empower individuals to make their own way through and push back against the coercive architectures of surveillance capitalism. This research contributes to:

• Performance Studies by describing the interactive theater as a site for digital simulation, and ethical connection.
• Cybersecurity Education by providing an embodied, affective counterpoint to the purely technical models.
• Critical Media Studies by examining theatre's resistance to datafication and surveillance by means of cultural critique.

2. Theoretical Framework

Situated within an interdisciplinary framework that encompasses performance studies, simulation theory, and critical digital theory, we explore the social and pedagogical implications of simulating digital threats through interactive theatre. The framework offers an intellectual footing for examining the ways in which theatrical simulations shape audience comprehension, ethical involvement, and affective engagement with cybersecurity concerns. Figure 1 provides a heuristic mindmap of the theory guiding this study. They map four key theoretical lineages - Performance as Social Practice, Simulation and Hyperreality, Critical Digital Theory, and Participatory Spectatorship and Ethical Reflexivity - each framed by a set of critical discussions encapsulated by the readers' six visual essays.

2.1 Performing as social practice

Applying Richard Schechner's concept of "restored behavior" (1985) [25], this study foregrounds interactive theater as a model of social performance to act out and interrogate multifaceted realities. Schechner argues that performance does not occur solely in theatres; it is a part of everyday life, ritual, and drama including theatre. Performance can also be taken as a method of constructing reality, a tactic of simulation and abstraction. Digital threats fora One way to help the public to make sense of the fast-moving world of digital threats is through interactive theater in which the public is exposed to simulations of cyber-attacks, allowing audiences to so that abstract risks become personal experiences.

2.2 Simulacrum and Hyper reality

Jean Baudrillard's (1983) [26] simulation theory provides a theoretical framework to reflect on the simulation of digital acts of threat within performance-based spaces. Simulations, for Baudrillard, could supplant the real, leading to what he called "hyper reality," where signs and symbols lose their connection to the things they were meant to represent. Amid a fictitious scenario of hacking, surveillance, or data theft, the audience is confronted with artificially created realities that could indeed evoke equal, real-to-life reactions to the above-described digital encounters. This model permits the study to evaluate the cognitive and affective realism of simulated cyber environments for training.

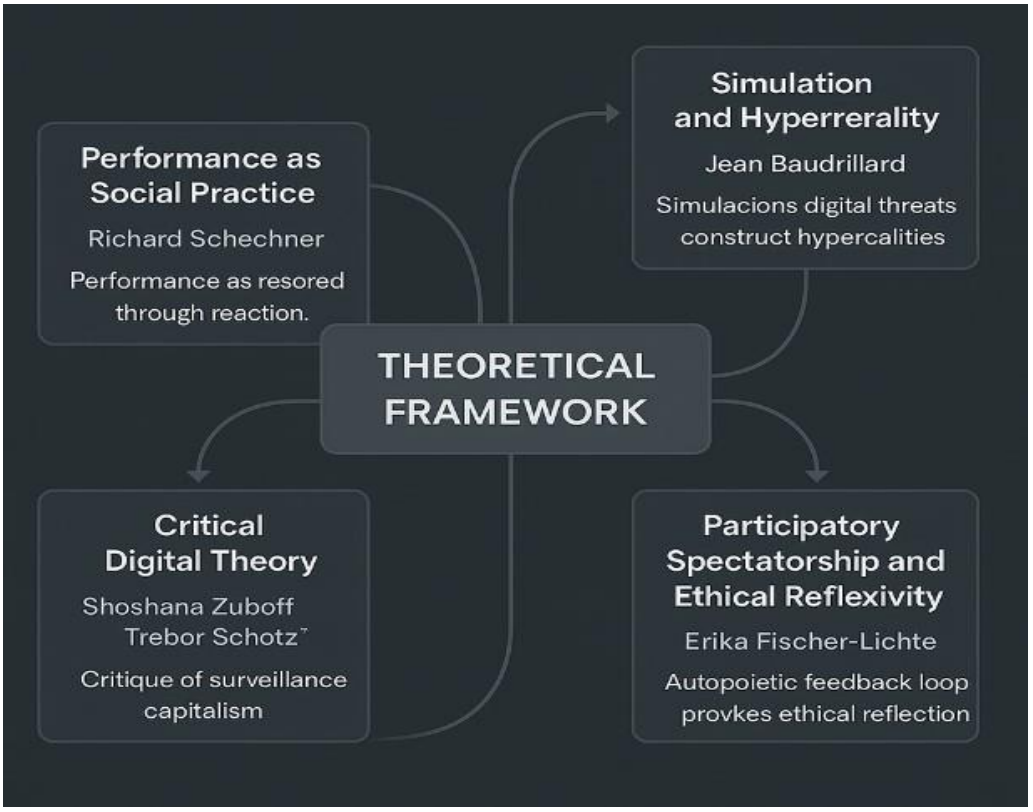

Figure. 1 Theoretical Framework

2.3 Critical Digital Theory

And to situate digital threats within socio-political dimensions, the research draws on critical digital theorists like Zuboff (2023) [27] and Trebor Scholz (2016) [28], who reflect on the logic of surveillance capitalism and the exploitation of digital labor. Zuboff's framing of "instrumentarian power" recognizes the power and power asymmetry of algorithmic systems

over users' behavior. The staged performance of these power structures permits their aesthetic dismantling and examination, cultivating a crowdsourced critique of present-day digital governance systems.

2.4 Participatory Spectatorship and Ethical Reflexivity

As Burnett's annotation suggests, one of the approaches through which fans come to understand such details and these courting practices more broadly is through "closeup," participatory, spectatorship. The research also employs Erika Fischer-Lichte's [29] concept of the autopoietic feedback loop when thinking about the interplay of performer and audience behaviours in live performances. In the responsive theater that is interactive theater, the audience is no longer a receptacle but a producer of meaning whose participation weaves the narrative and moral destiny of the simulation. It also allows insights into ethical reflexivity: how participants decide, experience, and grapple with their own digital fragility in the simulation.

3. Methodology

The research conducted through this work is a qualitative case study exploring how interactive theater performances can represent digital threats and act as catalysts for audience reflections about cybersecurity, surveillance, and digital ethics. The methodology seeks to document not only the creative making of such performances but also the process of engaging spectators and the responses of spectators. Figure 2 depicts the methodology used in this study, which clusters components such as research design, data collection, data analysis, and ethical issues in the following. It emphasizes the use of a single-case study design to examine an interactive theater play of exposure to digital threats, partnering with qualitative methods such as observation, semi-structured interviews, and thematic analysis. The diagram highlights the study's adherence to ethical and methodological rigor in pursuing an investigation of audience engagement with cybersecurity themes – using performative simulation as the tool.

3.1 Research Design

A case study-based strategy has been adopted, featuring a single interactive theater production, which simulates a digital threat scenario (e.g., a data breach, phishing attack, algorithmic profiling). This design enables detailed situational analysis of how the performative process of meaning-making of cybersecurity is achieved through a performance design, interactivity, and narrative immersion. The research is grounded in interpretive epistemology, which assumes that knowledge is co-constructed through meaning-making and lived experience (Denzin & Lincoln, 2011) [30]. This epistemology is not unsuited to interactive theatre, which invites participants to actively construct meaning.

3.2 Data Collection Methods

- Performance Documentation: The video recordings, scripts, audience cues, and stenographic material will be analyzed to consider the shaping and enactment of the digital danger. These are the materials we use for tracing narrative, symbolic, and technological decisions.
- Audience Observation: Field notes will be collected during the performance to capture real-time audience response (behavior, interaction, and decision) in reaction to the simulated digital threat. Data will concentrate on engagement, affect, and moral dilemmas.

- Semi-Structured Interviews: 10-15 audience members will be invited for a semi structured interview after the performance. Questions will question their comprehension of the computer-based threat, emotional response, realism appraisal, and thoughts regarding technology-related behavior and ethics.
- Expert Interviews: Interviews will be held with performance makers (playwrights/directors/designers) to assess their intentions, design processes, and to elicit any opinions on the simulation's efficiency.
- Surveys: General audience reaction will be captured using Until These Dreams of death's post-performance survey (Likert-scale and open-ended questions): what kind of feedback the piece has elicited from the public. Engagement and clarity; Realism of threat simulation; Emotional impact; Intentions or Outcomes of the Behavior being Learned.

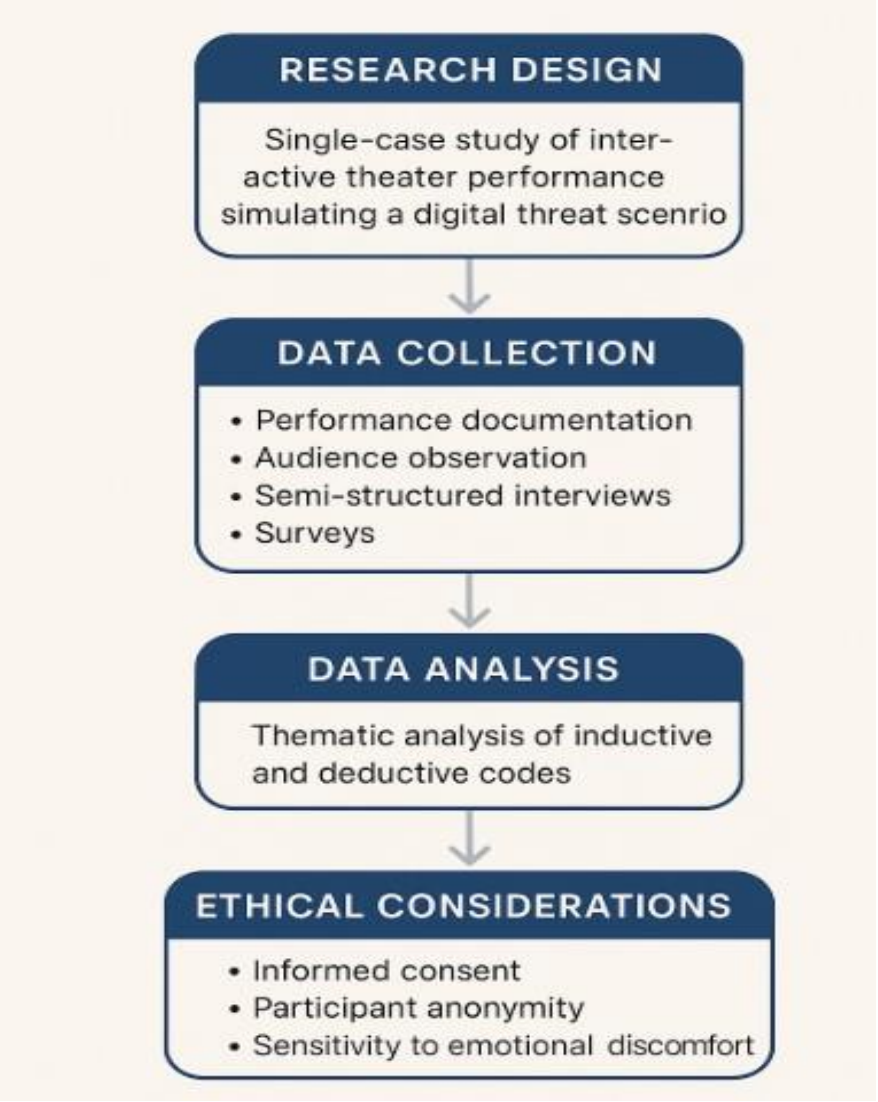

Figure 2. The methodology steps

3.3 Data Analysis

Data will be analyzed using thematic analysis (Braun & Clarke, 2006) [31], through a process that involves six steps: Familiarization with data; Generation of initial codes; Searching for themes; reviewing themes; Defining and naming themes; producing the final report. Codes will be generated inductively from participant responses and deductively from theoretical concepts (e.g., embodiment, simulation, ethical engagement). Data coding and visualization will be done using NVivo software.

3.4 Trustworthiness and Rigor

The study will employ the four criteria proposed by Lincoln and Guba (1985) [32] to ensure methodological rigor:

- Validity: Member check, Triangulation of data sources (interviews, observation, and document).

- Transferability: Description of context and setting of the performance.
- Reliability: Utilization of Audit trail and reflective research journals.
- Confirmability: Reflexive analysis in the effort to avoid researcher bias.

3.5 Ethical Considerations

• Informed consent will be obtained from all of the participants, who have the right to withdraw at any time.

- Real names will be disguised, and pseudonyms will be used throughout all records. • Appropriate consideration will be given to feelings of emotional distress before, during, and after participation in performance.
- Institutional review board approval will be obtained.

4. Analysis and Findings

In this section, the thematic analysis extracted the qualitative data from the live interactive theater performance of Digital Danger and the post-performance. Data consisted of performance recordings and audience observation, respondent interviews, and post-show surveys. As listed in Table 1, four integrated themes were identified, all of which reveal how the theatrical simulation of digital threats influenced audience sensemaking, affective engagement, and ethical deliberation.

4.1 Embodying the Abstract

The hands-on participants were united in their comments about the way in which the performance took complex, not always visible, digital threats and transformed them into real and bodily experiences–from phishing and metadata extraction to facial recognition. One scene, for example, enacted a phishing attack with actors posing as familiar faces and summoning spectators on stage to "authorize" live data transfers.

Table 1. Summary of Emergent Themes

Theme	Description	Evidence Source
Embodying the Abstract	Translating digital threats into lived, theatrical form	Observation, Interviews
Ethical Dissonance	Provoking Moral Engagement through Real-time Decision making	Surveys, Dialogue Analysis
Simulation as Safe Experimentation	Risk-free rehearsal of cyber threat scenarios	Audience Feedback
Reflexive Engagement with Future Tech	Shaping post-performance behavior and attitudes	Follow-up Interviews

Many participants indicated that this "brought home the danger", demonstrating how the connection to the material enhanced understanding. *"I've read about phishing but never felt personally tricked—this performance gave me that moment of doubt and guilt."* (Audience Member A03)

4.2 Communion and Ethical Dissonance

Interaction invites the audience to engage with ethical conflicts that are part of the digital environment. In one notable vignette, participants faced a decision whether they should provide anonymized data for the good of society or block access

in the interest of their own privacy. Observational reports described reluctance, furtive arguments, and discomfort while the simulation was being run, and the simulation appeared to have evoked a moral dilemma. Interviews confirmed this: *"It's not easy when you have to make a choice in front of others, especially when it's about surveillance and safety. It felt like a real ethical situation."* (Audience Member B07)

4.3 Simulation as Safe Experimentation

Speaking of experimentation, yet another point that one may argue is that simulation enables safe experimentation. Somehow, the tumbler of the stage created a space in which people could try out cyber-risk without being touched by concrete risk. Unlike informational campaigns or policy forums, the show permitted trial and error, emotional reaction, and real-time consideration. This is also in line with the notions of simulation as Baudrillard [26], pedagogic devices in which one constructs hyperreal events that audiences perceive as "true" in the sense of being emotionally authentic. *"I knew it wasn't real, but I still panicked when I thought my data was being sold. It hit harder than any workshop I've attended."* (Audience Member C12)

4.4 Pre-Congress on Digital Futures

Lumiere's post-show talks and interviews showed a very significant change in how audiences felt about digital futures. Several participants described becoming more skeptical of platforms, more interested in privacy tools, and more conscious of data capitalism. The event galvanized the reflexive positioning of emerging technologies, not just as consumers but as moral agents.
"After the show, I actually deleted three apps and checked my data permissions. I didn't expect the theater to do that." (Audience Member D04)

5. Discussion

The results from this work provide valuable information about the way interactive theater can serve as a transformative medium for rehearsing digital threats and promoting critical reflection around cybersecurity content. In the sections that follow, we will analyses these sets of findings using the theoretical frameworks introduced above with an emphasis on four key areas: embodiment and cognition, ethical reflexivity, pedagogy, and cultural critique.

Table 2. Summary of Key Discussion Themes.

Dimension	Theoretical Insight	Empirical Findings
Embodiment and Cognition	Schechner's concept of "restored behavior" and embodied learning in performance	Audiences felt digital threats as lived experiences; increased emotional comprehension
Ethical Reflexivity	Fischer Licht e's autopoietic feedback loop and Freirean pedagogy	Participants confronted real-time ethical dilemmas and reflected on personal responsibility
Simulation and Hyperreality	Baudrillard's theory of simulation and hyperreal experience	Fictional threats elicited real emotional responses; theater functioned as a cultural sandbox
Pedagogical Impact	Concepts of Critical Digital Citizenship and transformative learning	Reported Behavior Change (e.g., increased privacy awareness, app deletions)
Cultural Critique	Zuboff's "instrumentation power" and surveillance capitalism	Performance exposed and critiqued the hidden structures of digital control

5.1 Theatre comprises an embodied epistemology

The concretization of abstract, digital processes—like data tracking, phishing, and algorithmic profiling—as tangible, performative acts reaffirms Schechner's [25] notion that theater is a type of "restored behavior" in which social rituals and problems may be relived and repositioned. The audience's powerful affective and cognitive responses to, for instance, scenes in which consent is given for data, or privacy is breached, are indicative of the epistemological force of ES. Theater, in this sense, was not simply a representation of digital risk, but a performance of digital risk by enabling participants to "live through" the effects of virtual hazards.

5.2 Ethical Reflexivity and Participatory Agonism

The evidence massively favors Fischer-Lichte's [29] argument of the autopoietic feedback loop: interactivity delivered dynamic, unpredictable replies that altered the trajectory of the performance and intensified ethical investment. Audience members weren't just watching dilemmas; they were ethically complicit. It also created instances of moral high dissonance, in line with Freirean pedagogy, in which learning occurs as an experiential contradiction and reflection.

5.3 Simulation as a Cultural Sandbox

Resonating with the idea of simulation as understood by Baudrillard [26], the event constituted a hyperreal setting, wherein players responded in earnest to imaginary circumstances. This testifies to the disruptive potential of the theatrical simulation in comparison to conventional pedagogical models, as it endows subjects with a virtual terrain to try out choices through an act, with no fear of incision. In the way of "cultural sandboxing," the experience is like a cybersecurity training ground — but with aesthetic, not technical interfaces. It creates a site for emotional practice, it capitalizes on the opportunity for people to make lessons their own in ways that traditional instruction cannot.

5.4 Teaching, Conduct and Digital Literacy

The recorded post-performance learning behaviors, such as deleting apps and deploying privacy settings, suggest that the pedagogy around performance and its role in stimulating digital agency is promising. Digital citizen sugar baby –The performance acted as a spark that entices critical digital citizenship, an act that challenges users to not only interact with technologies but to question and ethically respond to them Zuboff, [27]. The contextualization within the theater allowed for a cognitive-affective fusion to ignite reflection and facilitate action that was different from the traditional form of cybersecurity education.

5.5 Cultural Critique and the Spectacle of Surveillance

Finally, the performance is a cultural critique of digital capitalism, resonating with Zuboff's [27] alarms of 'instrumentation power' and the asymmetries of control implicated within digital platforms. By dramatizing the unseen dynamics of data commodification and algorithmic profiling, the theater performance aestheticizes resistance, not just giving people awareness, but symbolic tools with which to criticize and envision alternatives. The performance, therefore, mediates imagination and intention, catalyzing new cultural genres through which digital power might be challenged.

5.6 Open Issues

As this study demonstrates, there are many open questions in the field of interactive theater for cybersecurity education.

- Scalability and Generalization: From a case study standpoint, the results may be less than generalizable. The bigger question is whether the same results would be found in different educational settings, areas of culture, and/or among distinct groups of people. To validate and extend the method of interactive play as described, further research in sociocultural settings will be required.

- Long-Term Impact: Despite immediate post-performance changes in user behavior (e.g., deletions of apps and resetting privacy parameters), the absence of longitudinal data leaves questions about continuity. Research should explore how long-lasting changes initiated by such performances are meant to be—and can be—sustained.
- Technological Integration and Accessibility: The incorporation of advanced technologies such as AI (artificial intelligence) and VR (virtual reality) into interactive drama provides opportunities for improving the reality of simulation or experience by audience participants. However, problems of access and digital competence may impede participation. Research should explore how high-tech theatrical tools can be fairly adopted in different places.
- Ethical and Psychological Risks: The intensity of emotions and moral quandaries presented in such performances may trouble or distress participants. More structured ethical frameworks and supportive mechanisms are needed to ensure audience well-being, especially with productions dealing with invasive or traumatic digital threats.
- Assessment Frameworks: Currently, evaluation is dominated by qualitative feedback. The construction of standardized mixed-method assessment instruments would not only strengthen quantitative assessment of cognitive, emotional, and behavioral impacts but also facilitate more rigorous academic and teaching validation.
- Integration with Formal Curricula: The study demonstrates the potential for the theater to be an informal educational tool, although its integration into formal education systems has not been studied extensively. Further research could examine what institutional pathways exist and how curriculum design methods might be adapted to bring interactive performance into the field of security studies and digital ethics.

6. Conclusion and Future work

This report reveals the potential of interactive theater to simulate digital security problems; indeed, it is compelling as an alternative to traditional cyber education methods. Take phishing, data breaches, or electronic surveillance as examples. Our qualitative case study shows that participatory theater performances can bring them to life in a very direct way for readers. From the theory of drama, simulation and critical pedagogy—in a digital world. We come to see that the theatre can serve not only as an educational tool but also a font of cultural criticism. Our research indicates that interactive theater can lead to stronger interest in cybersecurity, ethical reflection and increased attention to issues of digital responsibility. Furthermore the combination of both physical and affective learning modalities employed by theatrical simulations provides a framework for a more general approach to critical digital citizenship. This gives us an opportunity to change the habitual patterns which influence consumer behavior in cyberspace. Nevertheless, the research also identified a number of areas requiring further investigation. Future projects need to verify whether these findings apply across different social contexts in order to test their portability and scalability. Longitudinal studies will be needed to confirm whether or not the influence of performances on audience members lives over time is permanent. In addition, the introduction of more advanced technologies such as virtual reality or AI simulation ought not only to improve accuracy but also calls for attention on issues like accessibility and ethics. Bringing this research method into educational settings and developing standardized evaluation metrics for it will also help to establish this innovative approach. In conclusion, with the continuing development of digital threats so must the strategies for educating and empowering people. This book opens yet another frontier in theater as a public service committed to cybersecurity education: interactive public education.

Corresponding author

Mahmood A. Al-Shareeda
mahmood.alshareedah@stu.edu.iq

Acknowledgements
NA.

Funding
No funding.

Contributions
HJA; MAA; Conceptualization, HJA; MAA; Investigation, HJA; MAA; Writing (Original Draft), HJA; MAA; Writing (Review and Editing) Supervision, HJA; MAA; Project Administration.

Ethics declarations
This article does not contain any studies with human participants or animals performed by any of the authors.

Consent for publication
Not applicable.

Competing interests
All authors declare no competing interests.

References

[1] Dahlan, M. M. (2025). *Navigating the digital frontier: Understanding technology's impact on society*. Universiti Poly-Tech Malaysia.
[2] Kalema, N. L. (2024). The 'digital transformation for development' anti-politics machine: A case study on global digital development governance and public-sector digital transformation in Uganda. *Policy & Internet, 16*(4), 750–763.
[3] Umoga, U. J., Sodiya, E. O., Amoo, O. O., & Atadoga, A. (2024). A critical review of emerging cybersecurity threats in financial technologies. *International Journal of Science and Research Archive, 11*(1), 1810–1817.
[4] Aldaghlawy, H. J. (2024). A proposed system for using augmented reality technology in actor training. *Basrah Arts Journal, (28)*, 133–142.
[5] Rahim, M. J., Rahim, M. I. I., Afroz, A., & Akinola, O. (2024). Cybersecurity threats in healthcare IT: Challenges, risks, and mitigation strategies. *Journal of Artificial Intelligence General Science (JAIGS), 6*(1), 438–462.
[6] Ibrahim, I. M. (2024). The aesthetic and educational use of music and sound effects in the structure of school theater performances. *Al-Academy, (112)*, 125–140.
[7] Al-Salihi, B. S. A. (2024). Design objectives of the mask in children's theater performances. *Al-Academy, (112)*, 141–156.
[8] Crabb, J., Hundhausen, C., & Gebremedhin, A. (2024). A critical review of cybersecurity education in the United States. In *Proceedings of the 55th ACM Technical Symposium on Computer Science Education* (Vol. 1, pp. 241–247).
[9] Aldaghlawy, H. (2024). Visual rhythm in the Iraqi theatrical performance. *Journal of Arts and Cultural Studies, 3*(1), 1–9.
[10] Santa Barletta, V., Caruso, F., Di Mascio, T., Greco, F., Islam, T., Rossano, V., & Xiao, H. (2024). Cybersecurity education for industry and academia. In *17th International Conference on Advanced Visual Interfaces (AVI2024, pp. 1–4)*. ACM.
[11] Marshall, J. D., Aguinis, H., & Beltran, J. R. (2024). Theories of performance: A review and integration. *Academy of Management Annals, 18*(2), 600–625.
[12] Abbas, M. A. A., et al. (2022). Intellectual implications of the duality of mother and child in the social perspective. *Journal of Education and Teaching Trends (JETT), 13*(4), 233–241.
[13] Neethirajan, S. (2023). The significance and ethics of digital livestock farming. *AgriEngineering, 5*(1), 488–505.
[14] Aldaghlawy, H. J. (2024). The aesthetics of forming acting performance in children's theater performances. *Al-Academy, (112)*, 209–222.
[15] Mukherjee, M., Le, N. T., Chow, Y.-W., & Susilo, W. (2024). Strategic approaches to cybersecurity learning: A study of educational models and outcomes. *Information, 15*(2), 117.
[16] Puvaneyshwaran, D., Liang, P., & Lee, J. (2025). The impacts of forum theatre in social work practice: A scoping review. *The British Journal of Social Work, 55*.
[17] Al-Shareeda, M. A., Gaber, T., Alqarni, M. A., Alkinani, M. H., Almazroey, A. A., & Almazroi, A. A. (2025). Chebyshev polynomial based emergency conditions with authentication scheme for 5G-assisted vehicular fog computing. *IEEE Transactions on Dependable and Secure Computing*.
[18] Gulkhara, A., & Farzaliyeva, E. (2025). Theatre as a reflection of social change: How dramatic arts capture cultural shifts and historical transformations. *Acta Globalis Humanitatis et Linguarum, 2*(1), 254–261.
[19] Al-Shareeda, M. A., Ali, A. M., Hammoud, M. A., Kazem, Z. H. M., & Hussein, M. A. (2025). Secure IoT-based real-time water level monitoring system using ESP32 for critical infrastructure. *Journal of Cyber Security and Risk Auditing, 2*, 43–52.
[20] Aldaghlawy, H. J. (2013). Human rights & directing treatments in the Iraqi theatrical performance. *University of Basrah*. https://doi.org/10.5281/zenodo.7779863
[21] Al-Shareeda, M. A., Obaid, A. A., & Almajid, A. A. H. (2025). The role of artificial intelligence in bodybuilding: A systematic review of applications, challenges, and future prospects. *Jordanian Journal of Informatics and Computing, 2025*(1), 16–26.
[22] Kim, J. B., Zhong, C., Liu, H., et al. (2025). The impact of gamification on cybersecurity learning: Multi-study analysis. *Communications of the Association for Information Systems, 56*(1), 6.
[23] Baía Reis, A., & Ashmore, M. (2022). From video streaming to virtual reality worlds: An academic, reflective, and creative study on live theatre and performance in the metaverse. *International Journal of Performance Arts and Digital Media, 18*(1), 7–28.

[24] Adejumo, A., & Ogburie, C. (2025). The role of cybersecurity in safeguarding finance in a digital era. *World Journal of Advanced Research and Reviews, 25*(3), 1542–1556.
[25] Schechner, R. (1985). *Between theater & anthropology*. University of Pennsylvania Press.
[26] Baudrillard, J., Foss, P., Patton, P., & Beitchman, P. (1983). *Simulations*. Semiotext(e).
[27] Zuboff, S. (2023). The age of surveillance capitalism. In *Social Theory Re-wired* (pp. 203–213). Routledge.
[28] Scholz, T. (2016). *Platform cooperativism: Challenging the corporate sharing economy*. Rosa Luxemburg Stiftung.
[29] Fischer-Lichte, E., & Jain, S. (2008). *The transformative power of performance: A new aesthetics*. Routledge.
[30] Denzin, N. K., & Lincoln, Y. S. (2011). *The Sage handbook of qualitative research*. Sage.
[31] Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101.
[32] Lincoln, Y. S. (1985). *Naturalistic inquiry* (Vol. 75). Sage.