Human Factors in Cybersecurity, Vol. 127, 2024, 157–166
https://doi.org/10.54941/ahfe1004775

Cracking the Code: A Cyber Security Escape Room as an Innovative Training and Learning Approach

Tash Buckley[1] **and Oliver Buckley**[2]

[1]Royal Holloway University of London, Egham, UK
[2]Loughborough University, Loughborough, UK

ABSTRACT

This project explores the unique potential of physical escape rooms to foster embodied learning of cyber hygiene practices for the general public, addressing the challenges of traditional methods in engaging learners. It begins with a comprehensive review of existing training methodologies, highlighting their limitations, and underlines the necessity for more interactive learning experiences due to the increasing complexity of cyber threats. The core idea revolves around using escape rooms as educational and training tools, combining immersive, interactive elements with key cybersecurity principles to foster engagement and enhance retention. The paper includes a framework for integrating cybersecurity into escape room scenarios, discussing aspects like storyline development, puzzle design, and the inclusion of real-world cybersecurity challenges, while maintaining a balance between learning and gameplay. The conclusion presents initial findings on the effectiveness of escape rooms in cybersecurity education and training, showing positive impacts on engagement and behaviour, and suggests further research to refine this method.

Keywords: Escape rooms, Cyber security education, Positive cyber security behaviours, Applied games, Game based learning

INTRODUCTION

There has been a rapid evolution of cyber threats, both in terms of their sophistication and ubiquity, with around 97 victims of cybercrime per hour in 2024, compared to 6 per hour in 2001 (AAG, 2024). This has created a need for effective cyber security education. Often the most common causes of cyber incidents are directly attributable to basic security hygiene (DSIT, 2023), and cyber security issues are no longer the preserve of IT professionals alone. The growing importance of cyber security across all facets of our daily lives highlights the requirement for methods to increase engagement and understanding.

Cyber security presents a dynamic environment characterised by significant challenges in education and awareness of current best practice. The growing complexity of cyber threats, coupled with the pivotal role of human behaviours in cyber security have provided the motivation for this work. A considerable number of data breaches and cyber incidents are ultimately attributable to human behaviour, or a lack of awareness, resulting in the need for effective and engaging education methods. Traditionally, cyber security education has placed the emphasis on passive learning approaches, which often struggle to maintain engagement and to effectively instill robust and sustained behaviour change (Bada et al., 2019). These training approaches, such as e-learning modules, often fail to engage participants fully, leading to suboptimal retention and application of cybersecurity principles. One of the core aims of the *Cyber Escape Room* is to deliver accessible and engaging cyber security education to bolster overall awareness.

This paper proposes a novel, interactive and immersive learning environment, drawing from the popular entertainment concept of a traditional escape room. The *Cyber Escape Room* concept (Williams & El-Gayar, 2021) offers an engaging experience that enables participants to fully immerse themselves with hands-on cyber security challenges, based on real-life incidents and threats. This methodology aims to leverage the intrinsic appeal and growing public awareness of escape rooms to create a challenging, educational and, most importantly, enjoyable experience.

The remainder of this paper is structured as follows, the next section provides an overview of the related work in both cyber security education and the use of escape rooms as an educational tool. Following this we provide an overview of the design and development of the *Cyber Escape Room* to date, and finally we reflect on the conclusions of our current work and highlight future directions and challenges.

RELATED WORK

The importance of positive security behaviours in the workplace cannot be understated, as they play a crucial role in safeguarding organisational assets, data, and the overall integrity of IT infrastructure. Organisations with strong security cultures and positive security behaviours have been shown to experience fewer security breaches. Additionally, there are financial benefits, the 2020 Cost of a Data Breach Report (IBM, 2020) highlights that companies with an extensive employee training program save an average of $200,000 in the costs associated with a data breach. These findings underscore the critical importance of cultivating positive security behaviours in the workplace. They not only contribute to a more secure operational environment but also offer significant financial, regulatory, and reputational benefits.

Academic studies into effective means of promoting and training staff in positive security behaviours often focus on awareness campaigns, but the findings of these studies draw similar conclusions to that of Bada et al. (2019) who note that exposing employees to information and knowledge, although a prerequisite to learning, does not result in behaviour change. Steen et al. (2020) explored large scale security awareness campaigns delivered by a number of governments and found that several campaigns were unsuccessful when measured against behaviour change metrics. Improvements suggested were a more tailored approach to building awareness in security behaviours that considered demographics more specifically, training should be delivered to smaller groups of participants and the success of the campaigns should be measured against evidence-based success measures. Ertan et al. (2020) go further and emphasise the importance of needs-based training in positive security and security culture building.

Research into cybersecurity training and awareness frequently engages with psychological paradigms, applying behaviour change techniques defined in the behaviour change wheel by Michie, Atkins, and West (2014), as demonstrated in studies by Alshaikh et al. (2019) and Steen et al. (2020), or employing behavioural nudging as explored by Branley-Bell, Coventry, and Sillence (2021). The influence of personality traits, particularly those within the 'dark triad', on security behaviours and risk tolerance has also been examined by Moustafa, Bello, and Maurushat (2021), who recommend a suite of psychological assessments. The extensive corpus of research in this domain underscores the viability of a psychological approach to evaluating training methodologies. Nevertheless, the unique physical and gamified nature of the cyber escape room concept discussed in this paper suggests an alternative pedagogical perspective is warranted, specifically that of game-based learning for behaviour change.

Before exploring the merits of game-based learning (GBL), this review will look at key definitions to establish a foundation for subsequent discussion. GBL will be used to mean "the achievement of defined learning outcomes through game content and play and enhancing learning by involving problem-solving spaces and challenges" as defined by Qian and Clark (2016), referenced in Krath, Schürmann, and Von Korflesch (2021). This term is distinct from 'gamification', which is characterised by the integration of computer game elements into non-game contexts to enhance engagement (Passalacqua, 2020). The efficacy of GBL in effecting behavioural change is well-documented across various domains, from modifying children's dietary habits (Chow et al., 2020) to influencing environmental sustainability practices (Janakiraman, Watson & Watson, 2018). Although discussing e-learning more generally, Skinner at al. (2018) note relevantly to this project that "educational gamification […] shows it can increase understanding of cyber security threats in a more engaging manner, to better help implement behaviour change". Although often examples of game based learning and gamification elements are used within an educational setting (Liu, Shaikh and Gazizova, 2020), Passalacqua et al. (2020) used gamification elements, such as added competition and a leader board, within a warehouse setting to increase engagement and motivation for staff. It is worth noting that within the warehouse environment and reviewed in the literature by Krath, Schürmann, and Von Korflesch (2021) a limitation of current studies shows that behaviour change is only demonstrated in the short term and more research would be needed into the efficacy of game based learning on longitudinal behaviour change, an area that can be considered for future work for this project. Another aspect of game based learning that should be considered when developing the Cyber Escape Room project is the gamification technique of competition, which if used in excess can crowd out an intrinsic motivation to engage (Krath, Schürmann, and Von Korflesch, 2021), however team based competitions in a local environment mitigate this concern.

The popularity of the ‘escape room’ as a form of entertainment has seen a marked increase in recent years, which has led to its emerging application in the domain of cybersecurity education. In their work, Williams and El-Gayar (2022) outline a conceptual map for a virtual escape room aimed at imparting cybersecurity principles. Although promising, this initiative remains in its formative stages, having not yet undergone empirical validation through pilot testing.

In contrast, the project by Pirta-Dreimane et al. (2023) presents a hybrid learning environment that combines a virtual escape room with tabletop exercises. This innovative pedagogical tool aims to educate undergraduate students on both the technical and socio-technical facets of cybersecurity. Nevertheless, findings from this initiative indicate a disparity in learning outcomes, with a pronounced bias towards socio-technical competencies at the expense of more technical skills. This underscores the escape room concept’s potential to predominantly enhance understanding of cybersecurity behaviours rather than technical acumen.

Further contributions to this field include DeCusatis et al. (2022), who developed a virtual escape room as a computer game, leveraging the Octalysis gamification framework to increase user engagement. Of particular note to the current project is the work of Löffler et al. (2021), who, utilising the EscapED conceptual framework, crafted a virtual escape room to provide cybersecurity awareness training tailored to the needs of small and medium-sized enterprises.

Collectively, the body of research above predominantly explores the integration of escape room concepts within virtual spaces for educational purposes. The Cyber Escape Room project intends to contribute to this body of literature by investigating the efficacy of a physical escape room environment in fostering effective learning and engagement with positive cybersecurity behaviours, initially engaging with the general public for a pilot study but with future work to engage with industry for cyber security training purposes. This project will be grounded in the theoretical constructs of game-based learning (GBL), offering a novel perspective on this emergent educational phenomenon. The immersive nature of escape rooms, coupled with their competitive and collaborative elements, aligns strongly with game-based learning principles shown to enhance motivation and knowledge retention (Chow et al., 2020). Specifically, our room’s “phishing email” puzzle requires participants to analyse real-world examples, fostering a deeper understanding of this common threa.

The work within the Cyber Escape Room project builds on the previously mentioned conceptual framework, EscapeED, created by Clarke et al. (2017) as part of the Game Changers initiative set up by the Disruptive Media Learning Lab at Coventry University. The framework is designed “to promote a return to inclusive, human-centred interaction and play within GBL” using an escape room concept. The choice to adopt this framework was motivated by its solid grounding in the theoretical principles of GBL and its emphasis on collaborative, constructivist learning experiences that are mediated through in-person interaction and the collective resolution of games and puzzles. More in-depth detail on the use of the framework with the Cyber Escape Room project can be found later in this paper in relation to the methodological approaches employed.

DESIGN AND DEVELOPMENT

One of the key considerations when designing the initial prototype of the Cyber Escape Room was to identify the threats the elements within the room would address. The UK government's Department of Science, Innovation and Technology (DSIT) recently carried out their Cyber Security Breach Survey (DSIT, 2023), which highlighted a number of interesting issues. While more than 70% of organisations involved cited cyber security as a high priority, this is still a decrease on last year's figure of more than 80% (DSIT, 2022).

The UK's National Cyber Security Centre (NCSC, 2023) suggests that poor cyber hygiene is responsible for a significant amount of incidents. Cyber hygiene is generally viewed as something that can be improved, and by extension improving the security of an organisation, through a 'security-centric mindset' (Kaspersky, 2023).

Inspired by the immersive and collaborative aspects of escape rooms, our approach places learners in a realistic environment. This fosters active problem-solving and deepens understanding of cyber security threats, as supported by constructivist learning theory (Clarke et al., 2017).

This provides the backdrop for our initial design of the Cyber Security Escape Room, with a focus on incidents that would typically be associated with cyber hygiene. The survey by DSIT (2023), identified that a number of good practices in regards to cyber hygiene have seen a decline from previous years. For instance, in 2021 approximately 79% of businesses surveyed had a password policy in place, compared to only 70% in 2023.

Based on this analysis, we derived a prioritised list of cyber hygiene issues that commonly lead to breaches. This list informed the development of our escape room's challenges, ensuring that each activity directly addressed a key area of concern. By focusing on these specific issues, our escape room aims to enhance participants' knowledge and skills in practical ways that can significantly mitigate the risk of common cyber security incidents.

Our work builds on that of Buckley et al. (2014), and their taxonomy of accidental insider threat incidents, which identifies a range of issues directly related to that of cyber hygiene (see Figure 1). Through the use of contemporary industry white papers, data breach reports and government surveys ((Deloitte, 2023), (Trowers & Hamlins, 2023), (Splunk, 2023)) the list of core threats has been updated to include:

- Password policies including password sharing, reuse and choice.
- Email issues, including phishing, as this is an area identified to be increasing in commonality but something organisations are paying less attention to (DSIT, 2023).
- Data leakage
- Social engineering
- Network firewalls, this is a technology that has seen a decline between 2021 (78%) and 2023 (66%) (DSIT, 2023).

This methodology grounded our escape room's design in real-world data and ensured that the educational content was highly relevant and targeted towards making a meaningful impact on participants' cyber security practices. Through engaging with our escape room, participants are exposed to critical cyber hygiene issues, fostering a deeper understanding and commitment to implementing best practices in their daily digital interaction

ESCAPED FRAMEWORK

Our study utilised the EscapED framework, as seen in Figure 2, to develop a cyber security-themed educational escape room, aimed at improving participants' cyber hygiene practices and awareness. This framework guided the integration of game-based learning with specific educational content, ensuring an engaging and instructional experience. The framework suggests six elements to include in the design of an escape room for learning; participants, learning objectives, theme, puzzles, equipment and finally evaluation.

The process began with identifying our target audience, with a focus on the general public with no specific technical knowledge, which was essential for tailoring the escape room's difficulty and content to effectively meet participants' learning needs.

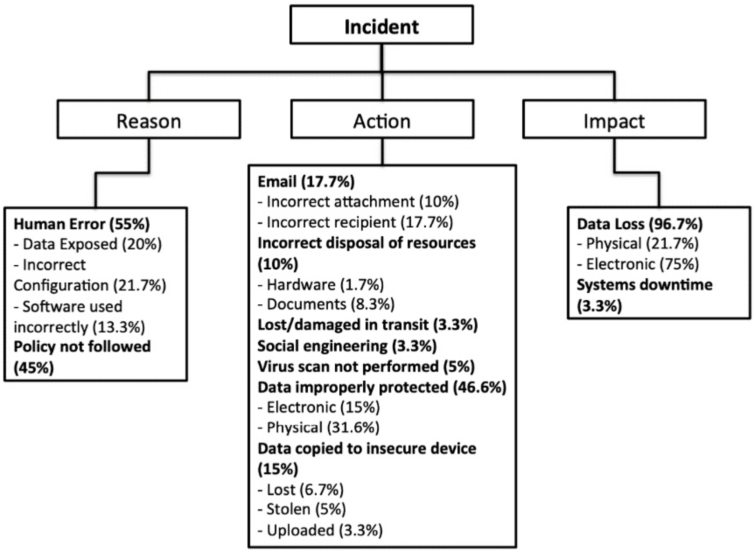
Incident
Reason
Action
Impact
Human Error (55%)
- Data Exposed (20%)
- Incorrect Configuration (21.7%)
- Software used incorrectly (13.3%)
Policy not followed (45%)
Email (17.7%)
- Incorrect attachment (10%)
- Incorrect recipient (17.7%)
Incorrect disposal of resources (10%)
- Hardware (1.7%)
- Documents (8.3%)
Lost/damaged in transit (3.3%)
Social engineering (3.3%)
Virus scan not performed (5%)
Data improperly protected (46.6%)
- Electronic (15%)
- Physical (31.6%)
Data copied to insecure device (15%)
- Lost (6.7%)
- Stolen (5%)
- Uploaded (3.3%)
Data Loss (96.7%)
- Physical (21.7%)
- Electronic (75%)
Systems downtime (3.3%)

Figure 1: Reasons, actions and impacts of accidental insider threats (Buckley et al., 2014).

The educational goals of the escape room were established based on these learning needs, with objectives such as understanding phishing attacks and creating strong passwords. These objectives informed the thematic and puzzle design, embedding the educational purpose within an engaging narrative. Puzzles and challenges were crafted to directly contribute to these goals, varying in complexity to cater to different learning styles and promote critical thinking in cyber security.

An immersive theme was selected to provide a relevant and compelling context, enhanced by the careful selection of both physical and digital props to add realism. The narrative guided participants through the experience, with each solved puzzle unveiling parts of the story. The *Cyber Escape Room* was delivered in a competitive, time tracked environment, with teams working together to solve the escape room. Additional hints were available to participants to differentiate and support learning.

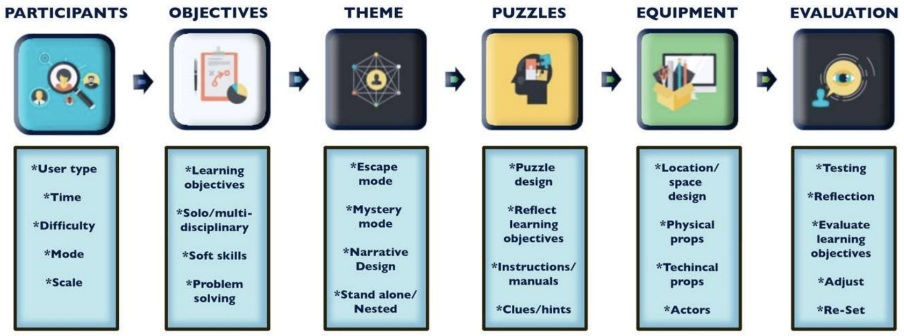

Figure 2: The EscapEd framework (Clarke et al., 2017).

DISCUSSION

A prototype of the *Cyber Escape Room* was tested during a pilot study at the British Science Festival in Exeter in 2023. This interactive session was open to the public, with small groups participating in a set time slot to solve puzzles and complete the escape room challenges collaboratively. Subsequent to the experience, attendees were invited to evaluate their experience using a five-point Likert scale survey. Findings from the survey indicated that 41% of the participants reported an increased awareness of cybersecurity threats following the escape room activity. This outcome echoes the assertions of Bada et al. (2019), reinforcing the premise that awareness alone is not sufficient for behaviour change although there is no measure of prior awareness so this cannot be verified. However, the survey also revealed that 71% of participants felt a renewed inspiration and motivation towards cybersecurity, with 100% reporting engagement and enjoyment during the activity, suggesting that interactive and collaborative learning environments can significantly enhance engagement with cybersecurity.

A common critique of employing escape rooms for educational purposes, as noted by Veldkamp et al. (2020) and Fotaris and Mastoras (2019), is the lack of rigorous pre- and post-learning assessments, which impairs the ability to measure actual knowledge acquisition. This critique also applies to the present pilot study and will be a focal point for refinement in subsequent research. Additionally, the reliability of self-reported data on engagement levels warrants a more objective evaluation mechanism in future iterations of the Cyber Escape Room.

This paper outlines the preliminary findings from a pilot study, and to advance this research, several steps are proposed. Firstly, the development of a bespoke framework, drawing from and expanding upon the EscapEd framework. This will involve crafting an updated taxonomy, building on Buckley et al. (2014), to ensure that future Cyber Escape Room iterations are current with the latest cyber hygiene threats and include emerging issues such as engagement in the workplace with large language models and artificial intelligence technologies. Lastly, there is a need to design and implement a companion web application that will facilitate the tracking of learning behaviours and enable a more rigorous evaluation of learning outcomes before and after the Cyber Escape Room experience.

REFERENCES

AAG (February 1, 2024) The Latest 2024 Cyber Crime Statistics. AAG Website: https://aag-it.com/the-latest-cyber-crime-statistics/.

Alshaikh, M., Naseer, H., Ahmad, A. and Maynard, S. B., 2019. Toward sustainable behaviour change: an approach for cyber security education training and awareness.

Bada, M., Sasse, A. M. and Nurse, J. R., 2019. Cyber security awareness campaigns: Why do they fail to change behaviour?. arXiv preprint arXiv:1901.02672.

Branley-Bell, D., Coventry, L. and Sillence, E., 2021, June. Promoting cybersecurity culture change in healthcare. In The 14th PErvasive Technologies Related to Assistive Environments Conference (pp. 544–549).

Buckley, O., Nurse, J. R., Legg, P. A., Goldsmith, M. and Creese, S., 2014, July. Reflecting on the ability of enterprise security policy to address accidental insider threat. In 2014 Workshop on Socio-Technical Aspects in Security and Trust (pp. 8–15). IEEE.

Chow, C. Y., Riantiningtyas, R. R., Kanstrup, M. B., Papavasileiou, M., Liem, G. D. and Olsen, A., 2020. Can games change children's eating behaviour? A review of gamification and serious games. Food Quality and Preference, 80, p. 103823.

Clarke, S., Peel, D., Arnab, S., Morini, L. and Wood, O., 2017. EscapED: A framework for creating educational escape rooms and interactive games for higher/further education. International Journal of Serious Games, 4(3), pp. 73–86.

DeCusatis, C., Gormanly, B., Alvarico, E., Dirahoui, O., McDonough, J., Sprague, B., Maloney, M., Avitable, D. and Mah, B., 2022, January. A cybersecurity awareness escape room using gamification design principles. In 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0765–0770). IEEE.

Deloitte (2023) 2023 Global Future of Cyber Security. Deloitte Website: https://www.deloitte.com/content/dam/assets-shared/legacy/docs/gx-deloitte_future_of_cyber_2023.pdf

DSIT. (July 11, 2022) Cyber Security Breaches Survey 2022. UK Government Website: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022

DSIT. (April 19, 2023) Cyber Security Breaches Survey 2023. UK Government Website: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/

Ertan, A., Crossland, G., Heath, C., Denny, D. and Jensen, R., 2020. Cyber security behaviour in organisations. arXiv preprint arXiv:2004.11768.

Fotaris, P. and Mastoras, T., 2019, October. Escape rooms for learning: A systematic review. In Proceedings of the European Conference on Games Based Learning (pp. 235–243).

IBM (2020) Cost of a Data Breach Report. IBM Website: https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf.

Janakiraman, S., Watson, S. L. and Watson, W. R., 2018. Using game-based learning to facilitate attitude change for environmental sustainability. Journal of Education for Sustainable Development, 12(2), pp. 176–185.

Kaspersky (2023) Top Tips for Cyber Hygiene to Keep Yourself Safe Online. Kaspersky Website: https://www.kaspersky.com/resource-center/preemptive-safety/cyber-hygiene-habits

Krath, J., Schürmann, L. and Von Korflesch, H. F., 2021. Revealing the theoretical basis of gamification: A systematic review and analysis of theory in research on gamification, serious games and game-based learning. Computers in Human Behavior, 125, p. 106963.

Liu, Z. Y., Shaikh, Z. and Gazizova, F., 2020. Using the concept of game-based learning in education. International Journal of Emerging Technologies in Learning (iJET), 15(14), pp. 53–64.

Löffler, E., Schneider, B., Zanwar, T. and Asprion, P. M., 2021. Cysecescape 2.0—a virtual escape room to raise cybersecurity awareness. International Journal of Serious Games, 8(1), pp. 59–70.

Michie, S., Atkins, L. and West, R., 2014. The behaviour change wheel. A guide to designing interventions. 1st ed. Great Britain: Silverback Publishing, 1003, p. 1010.

Moustafa, A. A., Bello, A. and Maurushat, A., 2021. The role of user behaviour in improving cyber security management. Frontiers in Psychology, 12, p. 561011.

NCSC (2023) Cyber security: Practical Tips for Protecting Your Organisation Online. NCSC Website: https://www.ncsc.gov.uk/files/NCSC_SME%20Cards.pdf

Passalacqua, M., Léger, P. M., Nacke, L. E., Fredette, M., Labonté-Lemoyne, É., Lin, X., Caprioli, T. and Sénécal, S., 2020. Playing in the backstore: interface gamification increases warehousing workforce engagement. Industrial Management & Data Systems, 120(7), pp. 1309–1330.

Perryer, C., Celestine, N. A., Scott-Ladd, B. and Leighton, C., 2016. Enhancing workplace motivation through gamification: Transferrable lessons from pedagogy. The International Journal of Management Education, 14(3), pp. 327–335.

Pirta-Dreimane, R., Brilingaitė, A., Roponena, E., Parish, K., Grabis, J., Lugo, R. G. and Bonders, M., 2023, July. CyberEscape approach to advancing hard and soft skills in cybersecurity education. In International Conference on Human-Computer Interaction (pp. 441–459). Cham: Springer Nature Switzerland.

Skinner, T., Taylor, J., Dale, J. and McAlaney, J., 2018, April. The development of intervention e-learning materials and implementation techniques for cyber-security behaviour change. ACM SIG CHI.

Splunk (2023) The State of Security 2023. Splunk Website: https://www.splunk.com/en_us/pdfs/gated/ebooks/state-of-security-2023.pdf

Trowers & Hamlins (2023) Cyber Security Breaches Survey 2023. Trowers & Hamlins Website: https://www.trowers.com/-/media/files/thought-leadership/cyber-security-breaches-survey.pdf

Van Steen, T., Norris, E., Atha, K. and Joinson, A., 2020. What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use?. Journal of Cybersecurity, 6(1), p. tyaa019.

Veldkamp, A., van de Grint, L., Knippels, M. C. P. and van Joolingen, W. R., 2020. Escape education: A systematic review on escape rooms in education. Educational Research Review, 31, p. 100364.

Williams, T. and El-Gayar, O., 2022. Design of a Virtual Cybersecurity Escape Room. In National Cyber Summit (NCS) Research Track 2021 (pp. 60–73). Springer International Publishing.