Leveraging Gamification for Cyber Threat Intelligence for Resilience in Satellite Cyber Supply Chains

Mona Kriesten, Mamello Thinyane and David Ormrod
University of South Australia, Adelaide, Australia

mona.kriesten@mymail.unisa.edu.au
mamello.thinyane@unisa.edu.au
dave.ormrod@unisa.edu.au

Abstract: Cyber Threat Intelligence (CTI) is collected threat information put in context to enhance decision-making before, during and after an attack. The application of CTI is widely limited to the reactive field of cybersecurity. The evolving cyber threat landscape requires a shift to an anticipatory and adaptable approach that addresses the complex and changing cybersecurity environment. CTI has the potential to support this shift to proactive threat handling towards a more resilient cybersecurity posture. This research is part of a project that aims to enhance the use of CTI for satellite cyber supply chain resilience through gamification. Cybersecurity games are established tools to raise security awareness and train security staff in red and blue team exercises. However, there is a lack of research on how gamification and serious games can be used to improve the application of CTI and enable training for security staff, even though existing literature points out the beneficial effects of gamification. Building on the gamification approach in cybersecurity, the research focuses on creating a gamified experience that simulates a cyber-attack derived from real-world examples and the utilisation of CTI to handle the simulated cyber-attack. The scenario addresses the need for informed decision-making throughout a cyber-attack by focusing on the utilisation of CTI in the context of satellite cyber supply chain security as the domain of application. This paper takes stock of the recent developments in CTI towards improving cyber resilience and presents gamification for cybersecurity and CTI to highlight the benefits of the approach. Further, it discusses the potential of gamification as an effective tool for CTI and describes the approach that is used to build a gamification solution inspired by real-world events. This paper contributes to the nascent research on gamification of CTI to strengthen cyber resilience in the context of increasingly frequent and sophisticated cyber threats, especially against space systems.

Keywords: Cyber Threat Intelligence, Gamification, Cyber Resilience, Satellite Supply Chain Security, Cybersecurity

1. Introduction

Global reliance on space systems has increased in recent years, providing numerous services including positioning, navigation, and timing (PNT), communications and earth observation. This increased reliance has occurred across civilian and defence contexts. In the civilian context, space systems are an integral part of critical societal infrastructure; and in the defence context, space systems have become a domain of ongoing militarisation and geopolitical contestation (Falco 2018; Pavur and Martinovic 2022). The increasing complexity of the space ecosystem, the growing satellite cyber supply chain (SCSC) attack surface, and several prominent attacks against satellite systems, including the Viasat KA-SAT cyber-attack linked to the Ukraine conflict (Viasat, Inc. 2022) and the non-malicious demonstrator hack of the Moonlighter satellite at DEFCON 31 in 2023 (Vasquez 2023), have highlighted the vulnerability of these systems and heightened the need for adaptable and proactive approaches towards strengthening the cyber resilience (CR) of space systems (Manulis et al, 2021).

Cyber threat intelligence (CTI) has shown the potential to improve cybersecurity and the handling of cyber-attacks, by facilitating informed decision-making and creating an adaptable environment for the vastly evolving threat landscape (Yeboah-Ofori et al, 2021). While CTI is currently predominantly used in reactive contexts, this research is oriented towards enhancing the proactive use of CTI for SCSC resilience (Samtani et al, 2017). The specific approach explored in this research towards this goal is gamification, which has effectively been used in different areas to improve cybersecurity outcomes.

The primary line of inquiry and the key question addressed in this paper is “How can gamification enhance the use of CTI towards CR in general and resilient SCSC in particular?” To address this question, the paper first explores the current literature across four focus areas in this project: (1) satellite supply chain security (SSCS), (2) CR, (3) CTI, and (4) gamification. This is followed by a mapping of the role of CTI across the CR phases to highlight the associated affordances and opportunities. Next, the development approach and scenario that form the basis for the gamification solution implemented in this project are presented. The paper concludes by discussing the significance of gamification, as a user-centred approach, to amplify the performance of human defenders towards the resilience of the complex SCSC socio-technical systems.

2. Literature Review

This research is undertaken at the intersection of space systems security, CR, CTI, and gamification. Prior research in these domains is presented and synthesized as the basis for the solutions developed in this research and presented in the paper.

2.1 Satellite Supply Chain Security

Space systems are vulnerable to many types of cyber threats targeting elements within the ground, space, or user segments. One of the vectors that is exploited in satellite attacks which is the focus of this research, is the SCSC – the set of entities, resources, and processes supported by digital technologies to establish an effective value chain in the production and delivery of space system (Kim and Im 2014). This has become an important vector for space systems security due to the increased commercialisation of the space industry, the popularity of commercial-of-the-shelf (COTS) components, and the growing number of third-party service providers involved in the industry (Falco 2018). Further, as evidenced in recent high-profile supply chain incidents, cyber supply chains can increase the risk exposure and degrade the cybersecurity posture of organisations and their systems (Linton, Boyson and Aje 2014).

Satellite supply chain security builds on the body of work on supply chain security and applies it to the space systems domain. The SSCS cuts across the ground, space and user segment and the extension of supporting units including software, hardware manufacturing, tools and cloud infrastructure (Burch 2020; Manulis et al, 2021). The research in the field identifies the following five categories of measures to address threats to the SCSC: network management, identification and authentication, system management, general security and incident prevention and response (Fleming, Reith and Henry 2023). While these are formulated from the cybersecurity perspective, there is an evolution in perspectives towards strengthening the CR of space systems.

2.2 Cyber Resilience

Cyber Resilience is a system's ability to prepare (or anticipate), absorb (or withstand), recover and adapt (or evolve) amid adverse cyber incidents (Bodeau and Graubart 2011; Kott and Linkov 2019). In contrast to the goal of operating fail-safe systems, the goal of CR is to operate systems that are safe to fail, and that can maintain critical functioning in the face of cyber-attacks. There are frameworks and models that operationalize the CR goals, such as the Cyber Resiliency Engineering Framework by Bodeau and Graubart (2011) or the CR model by the U.S. Department of Defense (2011). These provide guidance on how to engineer resilient environments across many domains such as industrial network supply chains and the space industry (Burch 2020; Gajek, Lees and Jansen 2021). Beyond the traditional technocentric notions of CR, there is an increasing recognition of the need for a socio-technical systems perspective towards resilience. The socio-technical perspective includes human and organisational factors that contribute to the overall CR posture. Human defenders play a critical role across the CR phases, leveraging CTI to inform decisions and responses to cyber threats. A mapping of the role of CTI across the CR phases has been developed and is presented later in the paper.

2.3 Cyber Threat Intelligence

CTI originates from the military notion of Threat Intelligence (TI). In the military, TI is used to warn of threats and indicate adversary action. CTI applies this military perspective to cyberspace; it provides analysed and correlated data about past, present, and emerging threats to inform decision-making and action. The three types of CTI; strategic, operational and tactical; can assist different organisational levels, from management to system administration, to improve their cybersecurity practice (Ainslie et al, 2023). CTI can be used both from a reactive and a proactive perspective, with the former representing efforts to respond to cyber-attacks and the latter representing an anticipatory action before the onset of the cyber threats. Research suggests that proactive approaches have a higher potential to increase a system's resilience (Samtani et al, 2017). However, despite this potential, the main challenges in the CTI field are handling the large amount of threat data that must be analysed, correlated, and structured; establishing sharing standards to overcome interoperability challenges between platforms; and defining consistent quality measures. Apart from the challenges with the management of CTI, developments in cyber-attacks and the shift to more evasive methods on the attacker side, affect the life-span and validity of CTI (Sahrom Abu et al, 2018).

Efforts have been made to define ontologies as a basis for a uniform understanding of CTI and to derive quality dimensions and metrics for CTI (Schlette et al, 2021; Yeboah-Ofori and Islam 2019). Recommendations have

been provided on how to effectively implement CTI, such as considering a knowledge base with a threat repository, applying detection models including AI approaches and utilising visualisation tools for monitoring and measurement purposes (Saeed et al, 2023). There are knowledge databases shared across the industry, such as MITRE ATT&CK (The MITRE Cooperation 2024). However, much of the research on CTI focuses on the technology-driven perspective like sharing standards and technical implementation approaches, whereas the benefit of CTI is to support better-informed decision-making. This research focuses on the need for user-centric and proactive approaches that enable defenders to use CTI to inform and improve their decision-making and response in dealing with cyber threats. Gamification is proposed as a user-centred approach towards enhancing the use of CTI to improve the CR of SCSC.

2.4 Gamification

Gamification is the process of using game elements in non-game contexts (Deterding et al, 2011) to improve learning, increase motivation and influence a positive outcome in users (Abdul Rahman et al, 2018), and to simplify real-world problems and make problem-solving more approachable (Schell 2019). Gamification approaches are employed within serious games, which are defined as games developed for purposes that go beyond entertainment (eds Ritterfeld, Cody and Vorderer 2009). While gamification and serious games are predominately linked to educational and training purposes, serious games analytics focuses on the analytical side to measure and assess performance through gamification (Loh, Sheng and Ifenthaler 2015).

One of the major benefits of gamification for cybersecurity is the creation of a safe environment that simulates real-world conditions to practice, train and test certain operations (Wolfenden 2019). Common examples of gamification approaches in cybersecurity include red teaming and blue teaming exercises and Capture The Flag (CTF) challenges. Research has been undertaken to test the benefits of gamification for cybersecurity. For example, tabletop exercises were used to identify skill gaps in the field and to find solutions to close the skills gaps using gamified experiences (McClaskey 2022). Further, cybersecurity games in the category of serious games were designed to investigate the differences in effectiveness between common video games and cybersecurity games with a focus on behavioural elements (van Steen and Deeleman 2021). In general game-based learning has been found to be most effective for the engagement of humans (Thompson et al, 2022). In the context of research on first responder's cybersecurity training, positive effects and learning outcomes were noted from introducing a gamified solution (Coull et al, 2017).

While existing research points to the broad effectiveness of gamification within the cybersecurity domain, there is a dearth of research on the gamification of CTI specifically for SCSC resilience. This gap is addressed in this research by mapping the possibilities of CTI for SCSC and by demonstrating an approach to gamify SSCS.

3. Mapping the Role of CTI Across Cyber Resilience Phases

CTI provides knowledge and insights about cyber threats and threat actors to security roles across organisations for better decision-making and practice at many levels from the technical to the strategic (Ainslie et al, 2023). Due to the versatility of CTI, it has emerged as a critical component in organisations' cybersecurity arsenal (Kant 2022). The resilience-creating ability originates from the CTI process of obtaining, processing, analysing, and distributing threat information and risk assessment that affects an organisation's cybersecurity. Organisations are able to employ risk and threat information to proactively decide on measures to mitigate risk and be better prepared against cyber threats. Protection, detection and response functions can be improved through the enrichment of CTI towards improved CR (Saeed et al, 2023).

Cyber resilience is enacted across different phases in the attack lifecycle. The order and number of phases vary depending on the model referenced, for example, Burch (2020) uses a modified model from the U.S. Department of Defense (2011) that defines the resilience phases as avoidance, robustness, reconstitution, and recovery. Whereas a publication from the MITRE Corporation defines resilience goals as anticipate, withstand, recover and evolve (Bodeau and Graubart 2011). For this research, the CR lifecycle that builds on the presented approaches was developed. It combines the approaches and defines the resilience phases as Anticipation, Avoidance, Robustness, Recovery, Reconstitution, and Evolution – as in Figure 1.

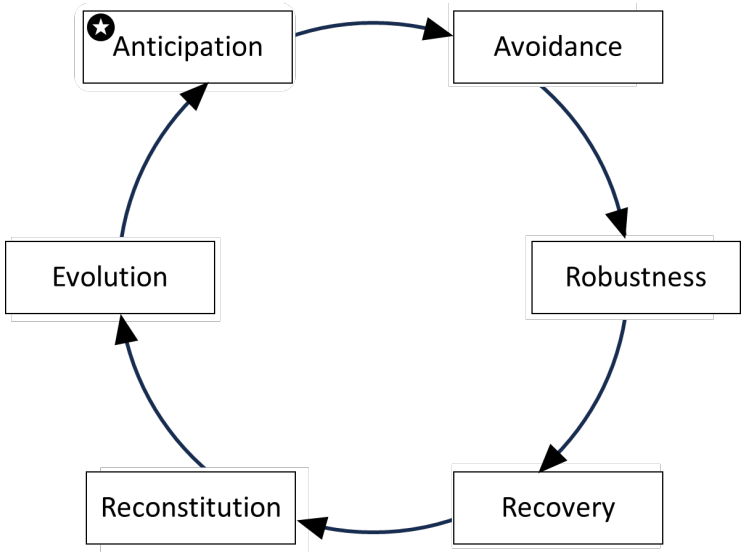

Figure 1: Cyber Resilience Lifecycle

Based on the literature on CR and CTI, a mapping of the role of CTI for each of the CR phases has been developed, starting with the *Anticipation* phase – as illustrated in Figure 1*:*

- *Anticipation* has the purpose of maintaining a state of informed readiness to prevent the impairment of functions through evolving threats (Bodeau and Graubart 2011). CTI is used for proactive situational awareness without any indication of an intrusion. In this context, CTI data must be continuously collected, updated, and analysed to predict threats and help security staff develop countermeasures against potential threats.
- *Avoidance* refers to the ability to evade and reduce risk. Accordingly, *Avoidance* includes the prevention and preparation for a cyber-attack (Burch 2020). As with Anticipation, CTI information must be collected continuously. However, at this stage, there is already a suspicion or a threat has been identified, for which information is collected in a targeted manner.
- *Robustness* describes the situation when a cyber-attack is detected, and the attacked infrastructure must be defended. It allows a system to withstand an attack by continuing mission-critical operations and constraining the attack's impact (U.S. Department of Defense 2011). Here, CTI provides information about adversarial tactics, techniques, and procedures (TTPs), reducing the effectiveness of the cyber-attack and increasing the probability of detection.
- *Recovery* aims to stop the attack, provide damage assessments and restore functions and capabilities to an acceptable level of operation (Burch 2020). In this phase, CTI enhances the prevention of lateral movement by isolating the threat and blocking attack vectors, enabling a return to mission-critical operation.
- *Reconstitution*, which occurs after a successful defence against and isolation of the threat, re-establishes the full operation of capabilities and functions. The objective is to get back to the status quo of operation (Burch 2020). CTI information enables threat hunting which eliminates persistence, identifies backdoors, and evicts the adversary. At this stage, the attack was successfully stopped, and attack residues were removed.
- *Evolve* contains the steps of transforming and re-architecting the infrastructure. It represents the lessons learned stage of the lifecycle (Bodeau and Graubart 2011). CTI supports the response to environmental change and the evolving threat landscape, including updates to the threat model and changes to TTPs. Gathered attack information can be incorporated and analysed to improve the security posture. Finally, further hardening activities of the infrastructure and continuous CTI updates should be undertaken.

From this mapping, it is apparent that CTI plays an important role towards CR. The critical element of this process is that high-quality CTI should be used, which among others means CTI that is timely, specific, and actionable. Assessing the quality of CTI is a key component of the gamification solution in this project, but this is beyond the scope of this paper.

4. Gamifying Cyber Threat Intelligence for Satellite Cyber Supply Chain Resilience

CTI has been identified as another potential area where gamification has beneficial effects from a training as well as an analytical perspective. Due to the dearth of prior work on the gamification of CTI in the SCSC contexts, a relevant approach and methodology to tackle the problem had to be developed. This was synthesized from existing gamification approaches in cybersecurity, and iterative and human-centred design methodologies. An output of this process along with the SCSC attack scenario are presented hereafter.

4.1 Gamification Design Approach

The overall approach for the development of the gamification solution is based on the design science methodology. This methodology employs three cycles. The relevance cycle connects the design process to the SCSC security context. The design cycle is outworked through an iterative build and evaluate cycle. The rigour cycle grounds the work in relevant domain expertise including cybersecurity frameworks and models (see Figure 2). Inspirations for this approach include iterative build and evaluate cycles aligned to the Rapid Application Development processes and the framing of the design in terms of the Mechanics, Dynamics and Aesthetics (MDA) components from gamification methods (Hevner 2007). The approach features influence from participatory design (PD) and User-Centred Design (UCD). By collecting feedback from experts who are potential users of the product, features of the game can be tested while they are developed to improve the user experience (Lowdermilk 2013).

The specific method to engage users in this process is primarily through Delphi. In Delphi, expert's opinions are collected to generate common sense during a decision-making process to find consensus and receive controlled feedback (Dietz 1987). Traditionally, Delphi covers three decision rounds. Each round builds on the previous one and a new iteration is updated based on the received feedback (Brady 2015). For the game development, the traditional process was virtualised allowing for a regular cadence of engagement with experts framed around identifying requirements (within the relevance cycle), evaluating and receiving feedback on key game artifacts such as the MDA components and the CTI (within the design cycle), and lastly leveraging their experience and expertise (within the rigour cycle) – see Figure 2. The expertise of the recruited participants ranges across cybersecurity, CTI, space systems engineering and game design domains. The variety of expertise and experience allows for a broad coverage of topics relevant to the game. Thus, not only MDA components are considered, but more importantly for this research, the SCSC attack scenario and the associated CTI are also evaluated.

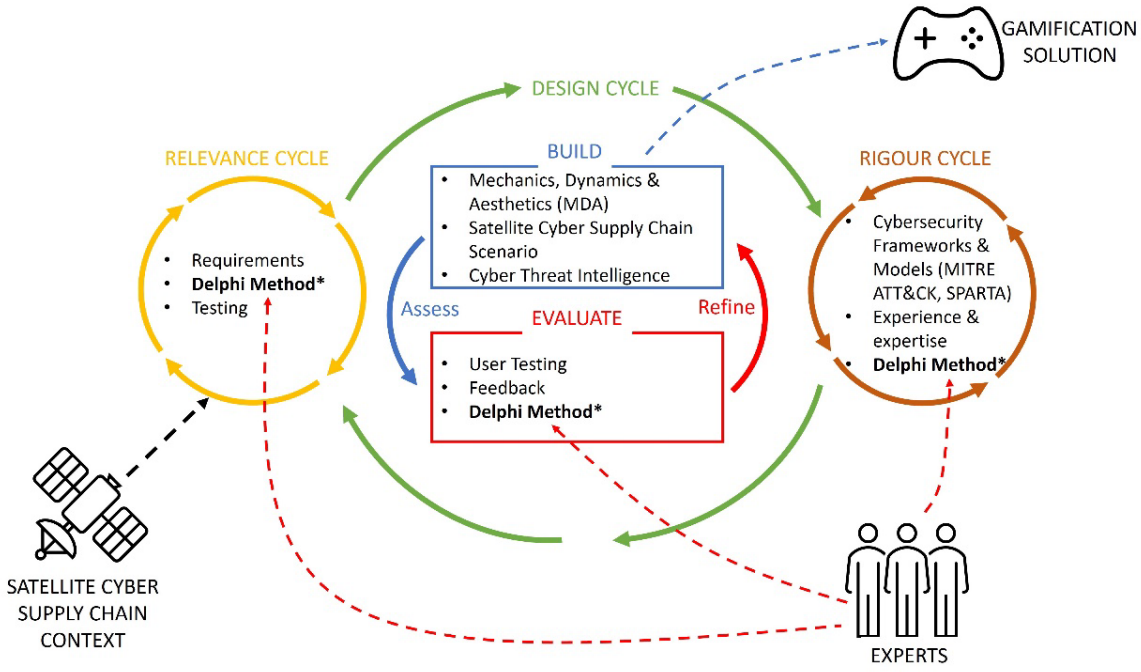

Figure 2: Game Development Process aligned to Delphi

4.2 Satellite Cyber Supply Chain Attack Scenario

A hypothetical SCSC cyber-attack scenario has been constructed to capture the core elements and key decision points as the attack unfolds (see Figure 3). References from real-world examples were used that covered a cyber supply chain attack and one targeting a satellite service provider. The SolarWinds attack from 2020 was used as the inspiration for the supply chain elements in the scenario (Willett 2021). This was combined with elements of the ViaSat KA-SAT cyber-attack from 2022 where attackers were able to access satellite modems and interrupt the satellite communication causing multiple service disruptions (Viasat, Inc. 2022).

Figure 3: Hypothetical Satellite Cyber Supply Chain Attack

The phases of the attack were divided into the different SCSC components (which are marked by different colours). The proposed cyber-attack was then reviewed and refined through the participant's feedback. After the attack drafting, the attack steps were used to assign CTI to enable the simulation of the decision-making process based on CTI information. The CTI information is synthesised from real-world examples and based on knowledge databases like MITRE ATT&CK (The MITRE Cooperation 2024) and SPARTA. SPARTA, similar to MITRE ATT&CK, is a TTP database specifically for space system TTPs (The Aerospace Corporation 2022). The collected CTI data was then divided into strategic, operational, and tactical intelligence to enable a differentiated analysis of the player's decision-making process. Based on the underlying goal of improving SCSC resilience, the generated CTI is also considered in terms of the mapping to CR phases as presented in Section 3.

The development of this SCSC attack scenario and the associated CTI has benefited from the iterative build and evaluate (i.e., feedback) cycle discussed in the approach above. The initial game prototypes were also developed to test the MDA components and feedback from the participants was collected to improve the design iteratively.

5. Discussion and Conclusion

There is an opportunity to enhance SCSC resilience by leveraging gamification to improve the use of CTI in these contexts. The research presented in this paper shows that CTI can be beneficial across each CR phase and can be shaped to inform decisions and response action along each step of the SCSC cyber-attack scenario. The suggested gamification solution that encapsulates real-life inspired SCSC scenarios and that has been developed with input from domain experts can help to better analyse and improve decision-making processes as well as the use of CTI to support these decisions. This can have an impact on the effectiveness of dealing with actual SCSC attacks. The approach involves the end user in the development phase, enabling feedback and adjustments to be made at an early stage of development. A game has the potential to test different scenarios, enables

adjustments to analyse the human decision-making processes, and can be adapted into an educational or training version.

This paper has presented three key elements from the research: an analysis of the benefits of CTI for improving cyber resilience, a CTI gamification approach, and a SCSC scenario that forms the basis of the gamification solution. The synthesis of a CR lifecycle, from existing CR models, and the mapping of the role that CTI can play for CR demonstrates the utility of CTI and has provided a foundation for the gamification solution. These benefits include additional information during each CR lifecycle phase to better inform sense-making and decision-making about the cyber-attack. The SCSC scenario is an example of how real cyberattacks can be incorporated and used for hypothetical simulations. Further, the gamification approach provides the use case for such a simulation that can be leveraged for analysis, educational or training purposes. Finally, the gamification of CTI provides a platform for further research on human-centred cybersecurity scenarios. The developed scenario and associated CTI provide a refined (i.e., by domain experts) and rigorously developed knowledge base of ideal decision-making and action towards addressing SCSC attacks.

There are, however, a few limitations and constraints to consider. First, the involvement of experts with different backgrounds does not eliminate personal bias. Hence, the need for broader testing and validation of the SCSC scenario, the CTI, and the game MDAs is necessary. Second, the scope of the scenario is informed by a small set of real-world cases and has a narrowly defined focus. A broader context could be reached by creating multiple cyber-attack versions which can be considered in future versions and further research in this field.

Future activities in this project will focus on the quality of CTI to integrate other metrics, such as trustworthiness, reliability, and timeliness, into the game design. In addition, different difficulty levels, associated with the complexity of the decision-making process, will be generated. Further, the CTI information will be presented to have a balanced distribution of information across the CR lifecycle. This will enable observations of how CTI can be used to enhance CR in the SCSC context.

In summary, this research presents an interactive approach to tackle the challenges of applying CTI to enhance CR and create resilient SCSC. The gamification approach enables the integration of the human factor and the possibility of adapting scenarios depending on the research focus for future use cases. Multi-player versions and different cyber-attack examples can extend on the given example.

References

Abu, M.S., Selamat, S.R., Ariffin, A. and Yusof, R. (2018), "Cyber Threat Intelligence – Issue and Challenges", *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 10, No. 1, p 371. Available at: https// 10.11591/ijeecs.v10.i1.pp371-379.

Ainslie, S., Thompson, D., Maynard, S. and Ahmad, A. (2023), "Cyber-threat intelligence for security decision-making: A review and research agenda for practice", *Computers & Security*, Vol. 132, p 103352. Available at: https://10.1016/j.cose.2023.103352.

Bodeau, D.J. and Graubart, R. (2011), "Cyber Resiliency Engineering Framework, MTR110237", [online], September, The MITRE Corporation, Bedford, Massachusetts, www.mitre.org/sites/default/files/pdf/11_4436.pdf, [Accessed 13.10.2022].

Brady, S.R. (2015), "Utilizing and Adapting the Delphi Method for Use in Qualitative Research", *International Journal of Qualitative Methods*, Vol. 14, No. 5, p 160940691562138. Available at: https://10.1177/1609406915621381.

Burch, R.W. (2020), Resilient space systems design: an introduction, CRC Press, Boca Raton.

Coull, N., Donald, I., Ferguson, I., Keane, E., Mitchell, T., Smith, O.V., Stevenson, E., Tomkins, P. (2017), "The Gamification of Cybersecurity Training", in F. Tian, C. Gatzidis, A. El Rhalibi, W. Tang and F. Charles (eds), *E-Learning and Games*, Vol. 10345, Springer International Publishing, Cham, pp 108–111.

Deterding, S., Sicart, M., Nacke, L., O'Hara, K. and Dixon, D. (2011), "Gamification. using game-design elements in non-gaming contexts", in *CHI EA'11 Proceedings of the 2011 annual conference extended abstracts on Human factors in computing systems*, p 2425-2428. Available at: https://10.1145/1979742.1979575.

Dietz, T. (1987), "Methods for analyzing data from Delphi panels: Some evidence from a forecasting study", *Technological Forecasting and Social Change*, Vol. 31, No. 1, pp 79–85. Available at: https: 10.1016/0040-1625(87)90024-2.

Falco, G. (2018), "The Vacuum of Space Cyber Security", in *2018 AIAA SPACE and Astronautics Forum and Exposition*, p 5275. Available at: https://10.2514/6.2018-5275.

Fleming, C., Reith, M. and Henry, W. (2023), "Securing Commercial Satellites for Military Operations: A Cybersecurity Supply Chain Framework", *International Conference on Cyber Warfare and Security*, Vol. 18, No. 1, pp 85–92. Available at: https:// 10.34190/iccws.18.1.1062.

Gajek, S., Lees, M. and Jansen, C. (2021), "IIoT and cyber-resilience: Could blockchain have thwarted the Stuxnet attack?", *AI & SOCIETY*, Vol. 36, No. 3, pp 725–735. Available at: https://10.1007/s00146-020-01023-w.

Hevner, A. (2007), "A Three Cycle View of Design Science Research", *Scandinavian Journal of Information Systems*, Vol. 19, No. 2, pp 87–92.

Kant, N. (2022), "How Cyber Threat Intelligence (CTI) Ensures Cyber Resilience Using Artificial Intelligence and Machine Learning", in J. Om Prakash, H.L. Gururaj, M.R. Pooja and S.P. Pavan Kumar (eds), *Advances in Information Security, Privacy, and Ethics*, IGI Global, pp 65–96.

Kim, K.-C. and Im, I. (2014), "Research letter: Issues of cyber supply chain security in Korea", *Technovation*, Vol. 34, No. 7, pp 387–388. Available at: https:// 10.1016/j.technovation.2014.01.003.

Kott, A. and Linkov, I (2019), "Fundamental Concepts of Cyber Resilience: Introduction and Overview" in A. Kott and I. Linkov (eds), *Cyber Resilience of Systems and Networks*, Springer International Publishing, Cham.

Linton, J.D., Boyson, S. and Aje, J. (2014), "The challenge of cyber supply chain security to research and practice – An introduction", *Technovation*, Vol. 34, No. 7, pp 339–341. Available at: https:// 10.1016/j.technovation.2014.05.001.

Loh, C.S., Sheng, Y. and Ifenthaler, D. (2015), "Serious Games Analytics: Theoretical Framework", in C.S. Loh, Y. Sheng and D. Ifenthaler (eds), *Serious Games Analytics*, Springer International Publishing, Cham, pp 3–29.

Lowdermilk, T. (2013), *User-centered design: a developer's guide to building user-friendly applications*, First edition, O'Reilly, Beijing.

Manulis, M., Bridges, C.P., Harrison, R., Sekar, V. and Davis, A. (2021), "Cyber security in New Space: Analysis of threats, key enabling technologies and challenges", *International Journal of Information Security*, Vol. 20, No. 3, pp 287–311. Available at: https:// 10.1007/s10207-020-00503-w.

McClaskey, T.M. (2022), "Tabletop Exercises: Gamification in Cybersecurity", [online], Master Thesis, Utica University, www.proquest.com/docview/2665552356/74B62B4D8B3F402FPQ/1?accountid=14649, [Accessed 17.04.2023].

Pavur, J. and Martinovic, I. (2022), "Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight", *Journal of Cybersecurity*, Vol. 8, No. 1, p tyac008. Available at: https:// 10.1093/cybsec/tyac008.

Rahman, M.H.A., Yusuf Panessai, I., Noor, A.Z.M. and Salleh, N.S.M. (2018), "Gamification Elements and their Impacts on Teaching and Learning - A Review", *The International Journal of Multimedia & Its Applications*, Vol. 10, No. 06, pp 37–46. Available at: https:// 10.5121/ijma.2018.10604.

Ritterfeld, U., Cody, M.J. and Vorderer, P. (eds) (2009), *Serious games: mechanisms and effects*, Routledge, New York.

Saeed, S., Suayyid, S.A., Al-Ghamdi, M.S., Al-Muhaisen, H. and Almuhaideb, A.M. (2023), "A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience", *Sensors*, Vol. 23, No. 16, p 7273. Available at: https:// 10.3390/s23167273.

Samtani, S., Chinn, R., Chen, H. and Nunamaker, J.F. (2017), "Exploring Emerging Hacker Assets and Key Hackers for Proactive Cyber Threat Intelligence", *Journal of Management Information Systems*, Vol. 34, No. 4, pp 1023–1053. Available at: https:// 10.1080/07421222.2017.1394049.

Schell, J. (2019), *The art of game design: a book of lenses*, Third edition, Taylor & Francis, CRC Press, Boca Raton.

Schlette, D., Böhm, F., Caselli, M. and Pernul, G. (2021), "Measuring and visualizing cyber threat intelligence quality", *International Journal of Information Security*, Vol. 20, No. 1, pp 21–38. Available at: https:// 10.1007/s10207-020-00490-y.

The Aerospace Corporation (2022), "Space Attack Research & Tactic Analysis (SPARTA)", [online], *SPARTA*, www.sparta.aerospace.org, [Accessed 04.11.2022].

The MITRE Cooperation (2024), "MITRE ATT&CK", [online], *ATT&CK Matrix for Enterprise*, www.attack.mitre.org, [Accessed 25.10.2022].

Thompson, L., Melendez, N., Hempson-Jones, J. and Salvi, F. (2022), "Gamification in Cybersecurity Education: The RAD-SIM Framework for Effective Learning", *European Conference on Games Based Learning*, Vol. 16, No. 1, pp 562–569. Available at: https:// 10.34190/ecgbl.16.1.504.

U.S. Department of Defense (2011), *FACT SHEET: Resilience of Space Capabilities*, www.dod.defense.gov/Portals/1/features/2011/0111_nsss/docs/DoD%20Fact%20Sheet%20-%20Resilience.pdf, [Accessed 19.01.2024].

van Steen, T. and Deeleman, J.R.A. (2021), "Successful Gamification of Cybersecurity Training", *Cyberpsychology, Behavior, and Social Networking*, Vol. 24, No. 9, pp 593–598. Available at: https:// 10.1089/cyber.2020.0526.

Vasquez, C. (2023), "First in space: SpaceX and NASA launch satellite that hackers will attempt to infiltrate during DEF CON", [online], *Cyberscoop*, www.cyberscoop.com/moonlighter-hack-a-sat-defcon, [Accessed 19.12.2023].

Viasat, Inc. (2022), "KA-SAT Network cyber attack overview", [online], *Viasat News*, www.news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview, [Accessed 19.12.2023].

Willett, M. (2021), "Lessons of the SolarWinds Hack", *Survival*, Vol. 63, No. 2, pp 7–25. Available at: https:// 10.1080/00396338.2021.1906001.

Wolfenden, B. (2019), "Gamification as a winning cyber security strategy", *Computer Fraud & Security*, Vol. 2019, No. 5, pp 9–12. Available at: https:// 10.1016/S1361-3723(19)30052-1.

Yeboah-Ofori, A. and Islam, S. (2019), "Cyber Security Threat Modeling for Supply Chain Organizational Environments", *Future Internet*, Vol. 11, No. 3, p 63. Available at: https:// 10.3390/fi11030063.

Yeboah-Ofori, A., Ismail, U.M., Swidurski, T. and Opoku-Boateng, F. (2021), "Cyberattack Ontology: A Knowledge Representation for Cyber Supply Chain Security", in *2021 International Conference on Computing, Computational Modelling and Applications (ICCMA)*, IEEE, Brest, France, pp 65–70. Available at: https:// 10.1109/ICCMA53594.2021.00019.