Inference of a Weighting Scheme for Cybersecurity Emergency Simulations

JMC Sturlese and Edgar Weippl

University of Vienna
Faculty of Computer Science
Doctoral School Computer Science
Vienna, Austria
jenny@sturlese.com

University of Vienna
Faculty of Computer Science
Vienna, Austria
edgar.weippl@univie.ac.at

Abstract. We develop a weighting scheme that enables an automated threat agent in cybersecurity emergency simulations to make realistic decisions about which attacks to launch as its next move. In the first part of the paper, we introduce core economic concepts and argue for viewing cyberattacks as traded services on dark-web markets, analogous to legal commodities. In the second part, we build upon the fundamental theories of the supply function, utility function, and choice probability to propose a Likelihood Score and provide inference on the theoretical derivations. The contribution of this approach lies in the empirical value of neoclassical economic theorems in the context of dark-web markets. Finally, we discuss avenues for applying the results of the weighting scheme to cybersecurity emergency simulations.

Keywords: Dark-web markets, neoclassical economics, emergency simulation, cybersecurity, weighting scheme

1 Introduction

The effect of simulations on emergency management is a well-studied area [1–5]. However, most of these cases consider only physical emergencies. A rapidly accelerating tidal wave of digital emergencies arrives with the rise of crimes that occur in cyberspace and affecting people offline [6, 7]. Still, we believe that the emergency management cycle [8] remains a relevant framework. However, new approaches to preparation, training, mitigation, detection, response, and recovery must be formalized.

A persistent challenge in emergency response is threat-rigidity [9], whereby decision-making in crises is limited to previously learned responses. In most organizations, cybersecurity is assigned to people with technical expertise. Yet today, cybersecurity is omnipresent, and anyone with internet access can become a target of cyberattacks. In particular, executive managers face heightened vulnerability: their role requires leading through crises, but without prior experience, they are especially prone to threat-rigidity. This makes it all the more critical to provide cybersecurity education to those without deep technical

backgrounds. Here, the strength of emergency simulations comes in handy with scenarios that closely mirror reality and enable learning without requiring actual crisis experience [10, 11]. To date, however, no simulation framework has been designed specifically for people without technical expertise to help them develop cybersecurity awareness and decision-making skills.

The scope of this article is to contribute to emergency management by addressing the stage of preparedness [8, p.297], with the goal of designing a centerpiece of any emergency simulation, a threat agent, that can subsequently be integrated into the training phase [8, p.297]. Our target user-group are executive managers who lack technical expertise but must lead during cyberattacks. While our preceding article examined *cyber espionage* as a suitable use-case for modeling a cybersecurity emergency simulation [12], the present article takes a applied mathematical perspective. It aims to serve as a reference point for researchers and emergency trainers in developing cybersecurity-focused emergency simulations with the greater goal of reducing disaster risk [13] related to cyberattacks. To the best of our knowledge, no existing emergency simulation has explicitly modeled cyberattacks as threats.

Thus, our contribution lies in ensuring that threatening cyberattacks are represented both realistically and empirically. We therefore pose the following research question: *How can an automated threat agent reflect realistic cyberattacks in emergency simulations that aim to enhance preparedness in line with emergency management?* To address this question, we begin by examining the digital epicenter of cyberattacks: dark-web markets. We continue by showing how the prices of cyberattack services traded in these marketplaces can serve as a basis for weighting an automated threat agent's choices in emergency simulations. Our findings introduce a Likelihood Score that integrates empirically valid estimations with mathematically derived inference. Finally, we discuss the implementation of this approach and outline its envisioned applications.

2 Dark-web Market Economics

Dark-web markets are online platforms that operate on anonymous networks, enabling the trade of illegal goods and services while concealing the identities of both buyers and sellers [14, 15]. Access to these platforms requires specialized software to bypass standard search engines and ensure anonymity [15]. In fact, they function similarly to conventional e-commerce sites but specialize in illegal offerings, including drugs [16], weapons [17], and cyberattacks including stolen data [18], distributed denial-of-service attacks [19], ransomware-as-a-service [20], credential theft [21], phishing kits [22], all potentially contributing to cyber espionage operations [12].

From an economic perspective, cyberattacks can be viewed as a service, provided by criminal agents with the objective of inflicting harm on organizations in the real world [23]. Such services may either be directly executed by the criminal agents themselves or purchased through dark-web markets. *Servitization* is as a trend equally relevant to illegal economies as it is to the legal sphere [24].

Dark-web markets conform to the key assumptions associated with perfect market competition, including (1) price-taking behavior (2) product homogeneity, (3) barrier-free market entry and exit and (4) perfect market transparency [25].

First, the market consists of a large number of suppliers, each holding only a small share of the market [25]. On dark-web markets, suppliers cannot set their own prices independently because demand quickly shifts toward cheaper alternatives [26]. Since suppliers hold only a small fraction of the total market supply, they must accept the market-set prices or risk losing buyers to competitors [27].

Second, the goods and services offered by different suppliers are perfectly substitutable because of their homogeneous nature [25]. Offerings by different suppliers on dark-web markets, including counterfeit documents, malware, and drugs, tend to be largely interchangeable [28]. As a result, any attempt by a supplier to raise its price would immediately lead to a loss of buyers to competitors [27].

Third, no significant barriers exist to enter or exit the market, which allows buyers to switch suppliers easily across markets [25]. On dark-web markets, both suppliers and buyers can simply join or leave with the use of pseudonymous identities and encrypted communication [29].

Fourth, all market participants possess complete information about relevant factors which enables perfectly informed decisions by all parties [25]. In dark-web markets, discourse on forums is of significant value especially for buyers [30]. This almost perfect access to information allows for buyers to make choices with complete information.

To further develop this economic perspective, it is necessary to introduce the idea of substitute and complementary services. A substitute service offers a comparable function and allows buyers to switch without losing utility [31]. In legal markets, examples include competing streaming platforms [32]. In dark-web markets, substitutes may include phishing services. Complementary services, by contrast, are those that are typically purchased in conjunction with one another, as the utility of one service enhances the other [31]. An example would be the joint purchase of a car lease and a corresponding insurance policy [33]. In dark-web markets, complementary services include the purchase of an initial network access service alongside malware deployment services that together increase the probability of a successful cyberattack.

3 Theoretical Derivation of Neoclassical Theorems

We take a deductive approach that is rooted in neoclassical economic methodology [34]. We make use of theoretical derivations of supply and utility functions along with choice probability theory [35]. This theoretical derivation provides a robust foundation for application in previously unexplored areas. In this article, we extend it to the context of dark-web market economics, examining the behavior of the aforementioned functions in this setting and deriving insights relevant to modeling an automated threat agent for emergency simulations.

For conceptualizing the weighting scheme of the decisions of our automated threat agent in emergency simulations in the context of cybersecurity, we follow three core functions inherently central to the field of economics, useful to apply to computer science (in specific for automated decision logic [36,37]): The supply function [38,39], the utility function [40–42], choice probability [43–46]. We take a deductive approach to derive from the supply function a corresponding utility function which can then be placed into the choice probability equation. While the mathematical derivations draw directly from the foundational contributions [38–46], the application to cyberattacks as a traded service on the dark-web is a novel application. The result is a formula on discrete choice which can be used for automated threat agents to take decisions as an attacker within emergency simulations. The goal is that its decisions are rooted in economic theorems and have empirical relevance as the variables can be estimated with realistic observations that can be made on dark-web markets.

In a given cybersecurity emergency simulation, the human plays the defendant, while an automated threat agent chooses from a set of cyberattacks over multiple rounds, each involving one decision per agent. This is a common logic that many video-games have adopted in Tower-Defense games [47–50]. In fact, one of the classical methods for cybersecurity training is through game simulations, particularly modeled after Tower-Defense games, where players must defend their territory against successive waves of attacks [47–50]. To ensure the educational relevance of such simulations, we argue that integrating empirical aspects of cyberattacks is essential. In the simulation process, analogous to chess, the automated threat agent chooses its next move based on rules and probabilities [51]. However, as chess is a fully theoretic game [52], it does not serve optimally as a blueprint for a cybersecurity emergency simulation. The core difference is that in cybersecurity, there is an empirically-valid demand and supply pattern available [53, 54]. Ignoring this and postulating random choice logic would significantly shrink learning opportunities for the human agents. Therefore, we seek to establish a weighting scheme that incorporates dark-web market patterns into the decision logic of an automated threat agent in every round. Prior studies have incorporated empirical data to model their simulations in like manner [55–57].

4 Inference to the Weighting Scheme

The results are visually presented in Fig. 1. The weighting scheme yields a Likelihood Score that drives the automated threat agent's attacks decision logic. An overview of our findings is presented in Table 1. What follows is inference to the Likelihood Score.

4.1 The Supply Function

We stipulate the supply function Q^s for each attack j as

$$Q_j^s = f(P_j, R_j, C_j, T_j) + \varepsilon_j$$

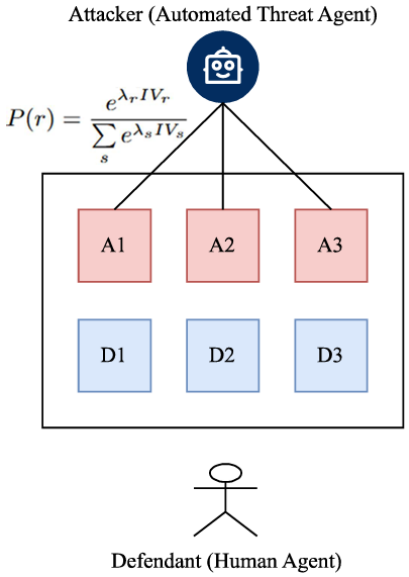

Fig. 1. Likelihood Score in Automated Decision Logic

Theorem	**Proposition**
I. Supply Function	
Supply Function	$Q_j^s = f(P_j, R_j, C_j, T_j) + \varepsilon_j$
II. Utility Functions	
Deterministic Utility	$V_{jr} = \alpha_j + \psi_1 P_j + \psi_2 R_j + \psi_3 C_j + \psi_4 T_j$
Total Utility	$U_{jr} = V_{jr} + \varepsilon_{jr}$
III. Controlling for Substitutes & Complements	
Inclusive Value	$IV_r = \ln\left(\sum_{j \in J_r} e^{V_{jr}/\lambda_r}\right)$
IV. Choice Probabilities	
Within-Round	$P(j \mid r) = \frac{e^{V_{jr}/\lambda_r}}{\sum_{j \in r} e^{V_{jr}/\lambda_r}}$
Across-Round	$P(r) = \frac{e^{\lambda_r IV_r}}{\sum_s e^{\lambda_s IV_s}}$
Likelihood Score	$P(j, r) = P(j \mid r) \cdot P(r)$

Table 1. Inference to the Weighting Scheme

with exogenous variable `price` P and endogenous synthetic variables `risk` R, `cost` C, and `technical level` T. Moreover, ε_j stipulates unobserved factors, known as error term. Variable `price` P constitutes an exogenous variable in

the function because we intend to integrate empirical values for this variable available in dark-web markets. An exogenous variable is one that is determined outside the model and is imposed upon it, meaning any change in such a variable is considered an exogenous change [58]. In contrast, an endogenous variable is one whose value is determined within the model itself [58]. In our case, those are also our synthetic variables variables `risk` R, `cost` C, and `technical level` T. To estimate the values of those, we work with MITRE ATT&CK ICS Matrix[1]. We propose standardizing the variables into ordinal scales ranging from low, medium, and high; numerically

$$R_j, C_j, T_j \in \{0.3, 0.6, 0.9\}$$

4.2 The Utility Function

When deriving the choice probability of an economic agent influenced by the market supply function, the utility of the agent, assuming rational behavior, serves as the intermediary linking the two. This approach is widely utilized in behavioral economics [59–62].

We define the utility that the automated threat agent gains from choosing attack j in round r as

$$U_{jr} = V_{jr} + \varepsilon_{jr} \tag{1}$$

Here, V_{jr} is the deterministic component of utility which is observable and can be modeled while ε_{jr} is the stochastic component that captures unobserved effects. We assume that ε_{jr} follows a Gumbel distribution, which leads to closed-form expressions in logit models [63–65]. Thus, the deterministic utility V_{jr} is derived as a linear function from our supply function Q^s.

$$V_{jr} = \alpha_j + \psi_1 P_j + \psi_2 R_j + \psi_3 C_j + \psi_4 T_j \tag{2}$$

The term α_j represents a fixed effect associated with attack j that stems from unobserved factors. Meawhile, the coefficients $\psi_1, \psi_2, \psi_3, \psi_4$ are the marginal utility coefficients associated with the various variables of the attack, derived from the supply function Q_j^s. In detail, ψ_1 reflects the utility sensitivity to price, which is typically expected to be negative, indicating that a higher cost diminishes attractiveness. ψ_2 captures the negative utility of risk, which is generally negative unless risk-taking is preferred in certain contexts. ψ_3 represents the impact of costs required to execute the attack. Lastly, ψ_4 measures sensitivity to technical difficulty, with higher values likely deterring lower-skill actors and thus reducing utility.

[1] https://attack.mitre.org/matrices/ics/;this database is a curated repository maintained by cybersecurity practitioners and researchers. It serves as a semantic ontology by systematically classifying cyberattacks, thereby functioning as a widely adopted knowledge base in the cybersecurity community.

4.3 The Choice Probabilities

Building on the utility function outlined above, we now convert the automated threat agent's utility into probabilistic choice behavior. We use a discrete choice model that determines the choice probability each attack option based on its utility. We use with a standard Multinomial Logit model [65,66], which describes how an automated threat agent chooses from a range of attack options in a given round r. Let J_r represent the set of three attack options in round r, and V_{jr} the deterministic utility of option j. The probability of choosing option j within round r is given by

$$P(j \mid r) = \frac{e^{V_{jr}}}{\sum\limits_{j \in J_r} e^{V_{jr}}} \tag{3}$$

The proposition captures two important ideas, options with higher utility are more likely to be chosen and the relative likelihood of choosing one attack over another depends on their respective utilities.

4.4 Controlling for Substitutes and Complements

As outlined in Section 2, attack services may exhibit relationships of substitution or complementarity. These inter-dependencies are critical for accurately representing the decision logic of an attacker. We argue that it is vital to incorporate these relationships when designing the weighting scheme in order to be empirically realistic. Substitution occurs when the automated threat agent must make a choice between mutually exclusive options, which is typically the case within a single round. This within-round substitution is captured using the Multinomial Logit model. This ensures that the likelihood of choosing an attack is based on its relative utility in comparison to the other available options within the same round. Given a set of attacks $j \in r$ in round r, the probability of choosing attack j is:

$$P(j \mid r) = \frac{e^{V_{jr}/\lambda_r}}{\sum\limits_{j \in r} e^{V_{jr}/\lambda_r}} \tag{4}$$

Here, V_{jr} is the utility of attack j in round r, and λ_r is a scale parameter that governs the degree of substitution, i.e. a smaller λ_r implies stronger substitution and denotes within-round decision probability.

Complementarity, on the other hand, occurs across rounds, where executing a particular attack in one round can increase the value of related attacks in future rounds s; to model this, we use the Inclusive Value, an aggregated measure of expected utility that combines the utilities of all attacks within round r, called across-round probability.

$$IV_r = \ln\left(\sum_{j \in J_r} e^{V_{jr}/\lambda_r}\right) \tag{5}$$

Thus, it reflects the combined value of the current attack's utility and its potential for complementarity with future decisions. As the simulation progresses, the probability of continuing to each sequential round is determined by the Inclusive Value, which is influenced by previous choices and the anticipated benefits of future actions.

$$P(r) = \frac{e^{\lambda_r IV_r}}{\sum_s e^{\lambda_s IV_s}} \tag{6}$$

4.5 The Likelihood Score

As the simulation progresses, each round's likelihood will be determined not only by the current attack options but also by how the automated threat agent perceives future opportunities. Combining the within-round decision probability and the across-round weighting yields the total likelihood of choosing attack j in round r:

$$P(j,r) = P(r) \cdot P(j \mid r) = \left(\frac{e^{\lambda_r IV_r}}{\sum_s e^{\lambda_s IV_s}} \right) \cdot \left(\frac{e^{V_{jr}/\lambda_r}}{\sum_{j \in J_r} e^{V_{jr}/\lambda_r}} \right) \tag{7}$$

This is ultimately the Likelihood Score which shall be integrated in the automated decision logic so that its decisions are weighted by empirical values, the actual price of cyberattack services traded on dark-web markets along with estimated factors including risk, cost, and technical expertise level.

5 Integrating the Weighting Scheme for an Automated Threat Agent within an Emergency Simulation

In the Sections before, we explained the theoretical derivations of the decision logic for the automated threat agent within a cybersecurity emergency simulation. In this Section, we discuss the further steps taking this into action.

Next up, we will employ a web scraper that will collect price information on several active dark-web marketplaces for 15 distinct cyberattacks identified in preceding papers (see [12, 67] for details). As elaborated in Section 4.1, the variable price is the only exogenous variable in the function and we will integrate empirical values for this. That is the next step. The step after that is to assess our synthetic variables risk, cost, and technical level with the use of the aforementioned MITRE ATT&CK ICS Matrix (see footnote 1 for details) for the same 15 cyberattacks. Once all variables will be fed with realistic empirical values, the weights will be ready to be integrated into the algorithm of the automated decision logic. The result will be that the automated threat agent launches cyberattacks in a realistic manner, backed by empirical values that stem from to-date relevant dark-web market indices.

For developing the simulation, we are using *Godot*[2] which is an open source game engine (MIT licensed), known for its flexibility and ease of use, especially for creating 2D simulations. Our proposed Likelihood Score is integrated as weighting scheme within the automated threat agent's decision logic on calculating which attack should be launched each round [67].

Testing will be conducted to ensure that the Likelihood Score accurately reflects realistic cyberattacks. With iterative experiments, we will then adjust the parameters (marginal utility coefficients) to assess how the simulation aligns with empirical expectations.

The results must be seen in light of some limitations. A major limitation relates to the exogenous nature of the price P. In many dark-web markets, price is not entirely exogenously determined but rather shaped by the market dynamics of supply and demand. Consequently, price may respond to unobserved demand shocks, which introduces bias into the estimation of its effect on attacker choices or supplier behavior. If this endogeneity of demand is not properly addressed, conventional estimation methods can produce biased and inconsistent parameter estimates. In particular, we may incorrectly attribute variation in outcomes (here, attack choice) to price effects when they are actually driven by omitted or latent variables influencing demand of a specific dark-web market. To deal with this issue, we propose to include an Instrumental Variables approach to isolate the part of price variation that is exogenous, i.e. not driven by changes in demand.

6 Conclusion

In the present article, we ask ourselves how the choices of an automated threat agent can be weighted to reflect realistic cyberattacks observable on dark-web market behavior. Adhering to the four key assumptions of perfect market competition, we argue that cyberattacks can be viewed as a service traded on dark-web markets. Moreover, the subject of cybersecurity is by nature bound to be very fitting for simulations, as there is an existing large body of literature dealing with gaming approaches to cybersecurity training. In order to leverage learning of our target user group of executive managers without deep technical expertise, we argue that the decisions of an automated threat agent shall reflect empirically-valid decision logic to mirror real dark-web cyberattacks in line with increasing their preparedness through experience by emergency simulations. For our weighting scheme, we made use of classical economic theorems, the supply function, the utility function, and choice probability, to derive our proposed Likelihood Score. While the variable price is of exogenous nature, directly taken from dark-web marketplaces, the other variables risk, cost, and technical level are synthetics and endogenous, standardized estimations. The utility function is a direct derivation and is used to stipulate the choice probabilities. For this, we distinguish between

[2]https://godotengine.org

within-round and across-round probabilities, controlling for substitute and complementary choices. Finally, our Likelihood Score is a multiplication of these two that can be integrated into the decision logic of an automated threat agent in cybersecurity emergency simulations. With the result of a weighting scheme for an automated threat agent, what naturally would follow is the development of a mid-fidelity prototype using an open source game engine and then to test on the empirical value of the automated attack choices.

Acknowledgments

This work is supported by SBA Research (SBA-K1 NGC), a COMET Center within the COMET – Competence Centers for Excellent Technologies Programme and funded by BMIMI, BMWET, and the federal state of Vienna. The COMET Programme is managed by FFG.

References

1. Franck Taillandier and Carole Adam. Games ready to use: A serious game for teaching natural risk management. *Simulation & Gaming*, 49(4):441–470, 2018.
2. Luca Chittaro and Riccardo Sioni. Serious games for emergency preparedness: Evaluation of an interactive vs. a non-interactive simulation of a terror attack. *Computers in Human Behavior*, 50:508–519, 2015.
3. Ilona Heldal. Simulation and serious games in emergency management: Experiences from two case studies. In *2016 22nd International Conference on Virtual System & Multimedia (VSMM)*, pages 1–9. IEEE, 2016.
4. David Alexander. Scenario methodology for teaching principles of emergency management. *Disaster Prevention and Management: An International Journal*, 9(2):89–97, 2000.
5. Felix Baumann, Lennart Landsberg, Thomas Säger, and Ompe Aimé Mudimu. Tabletop exercises as a potential to improve" preparedness for society in health crises and disasters". *Procedia Computer Science*, 256:101–105, 2025.
6. Jonathan Lusthaus and Federico Varese. Offline and local: The hidden face of cybercrime. *Policing: A Journal of Policy and Practice*, 15(1):4–14, 2021.
7. David Buil-Gil, Fernando Miró-Llinares, Asier Moneva, Steven Kemp, and Nacho Díaz-Castaño. Cybercrime and shifts in opportunities during covid-19: a preliminary analysis in the uk. *European Societies*, 23(S1):S47–S59, 2021.
8. Bartel Van de Walle and Murray Turoff. Decision support for emergency situations. *Information Systems and E-Business Management*, 6(3):295–316, 2008.
9. Barry M Staw, Lance E Sandelands, and Jane E Dutton. Threat rigidity effects in organizational behavior: A multilevel analysis. *Administrative science quarterly*, pages 501–524, 1981.
10. Jacqueline J Arnold, LeAnn M Johnson, Sharon J Tucker, James F Malec, Sarah E Henrickson, and William F Dunn. Evaluation tools in simulation learning: performance and self-efficacy in emergency response. *Clinical Simulation in Nursing*, 5(1):e35–e43, 2009.
11. Lei Zhou, Xianhua Wu, Zeshui Xu, and Hamido Fujita. Emergency decision making for natural disasters: An overview. *International journal of disaster risk reduction*, 27:567–576, 2018.

12. Jennifer-Marieclaire Sturlese and Ronald Hochreiter. Modeling the case of cyber espionage for executive game simulations. In *International Conference on Information Technology in Disaster Risk Reduction*, pages 66–81. Springer, 2024.
13. Terje Gjøsæter, Jaziar Radianti, and Yuko Murayama. *Information Technology in Disaster Risk Reduction*. Springer, 2023.
14. Piotr Siuda, Mikko Aaltonen, Ari Haasio, Angus Bancroft, Juha Nurmi, Haitao Shi, and J Tuomas Harviainen. Digital drug trading ecologies in context: Technological, geographic, and linguistic variation across darknet platforms. *International Journal of Drug Policy*, 2025.
15. Mohammad J Obaidat, Ibrahim A Al-Syouf, Yahea F Awawdeh, Anas E Masa'deh, and Qasem Abu Al-Haija. Darknet threats and detection strategies: A concise overview. In *2025 16th International Conference on Information and Communication Systems (ICICS)*, pages 1–6. IEEE, 2025.
16. Matthew C Nali, Zhuoran Li, Vidya Purushothaman, Meng Zhen Larsen, Raphael E Cuomo, Joshua S Yang, and Tim K Mackey. Identification of cannabis product characteristics and pricing on dark web markets. *Journal of Psychoactive Drugs*, pages 1–9, 2025.
17. Edwin Xorsenyo Amenu and Sridaran Rajagopal. Dark web complications: Policing and surveillance–challenges and implications. In *2025 International Conference on Engineering, Technology & Management (ICETM)*, pages 1–9. IEEE, 2025.
18. Tayyba Jabeen, Yasir Mehmood, Hamayun Khan, Muhammad Fawad Nasim, and Syed Asad Ali Naqvi. Identity theft and data breaches how stolen data circulates on the dark web: A systematic approach. *Spectrum of engineering sciences*, 3(1):143–161, 2025.
19. Victor Obojo, Richard A Ikuesan, AbdulKabir Adekanye, and Elias Iortom. The importance of dark web access in cyber threat intelligence. In *2025 13th International Symposium on Digital Forensics and Security (ISDFS)*, pages 1–6. IEEE, 2025.
20. Luqman Hafiz, Taufik Hidayat, et al. Unveiling the cybercrime ecosystem: Impact of ransomware-as-a-service (raas) in indonesia. *International Journal of Science Education and Cultural Studies*, 4(1):11–21, 2025.
21. George Pantelis, Petros Petrou, Sophia Karagiorgou, and Dimitrios Alexandrou. On strengthening smes and mes threat intelligence and awareness by identifying data breaches, stolen credentials and illegal activities on the dark web. In *Proceedings of the 16th international conference on availability, reliability and security*, pages 1–7, 2021.
22. Adam Oest, Yeganeh Safei, Adam Doupé, Gail-Joon Ahn, Brad Wardman, and Gary Warner. Inside a phisher's mind: Understanding the anti-phishing ecosystem through phishing kit analysis. In *2018 APWG Symposium on Electronic Crime Research (eCrime)*, pages 1–12. IEEE, 2018.
23. Mehdi Kadivar. Cyber-attack attributes. *Technology Innovation Management Review*, 4(11), 2014.
24. Thomas Friis Søgaard and Mike Salinas. Competing through service: Entrepreneurial bricolage and the servitization of local drug markets. *The British Journal of Criminology*, page azaf021, 2025.
25. George J Stigler. Perfect competition, historically contemplated. *Journal of political economy*, 65(1):1–17, 1957.
26. Dimitrios Georgoulias, Ricardo Yaben, and Emmanouil Vasilomanolakis. Cheaper than you thought? a dive into the darkweb market of cyber-crime products. In *Proceedings of the 18th International Conference on Availability, Reliability and Security*, pages 1–10, 2023.

27. Paul J McNulty. A note on the history of perfect competition. *Journal of Political Economy*, 75(4, Part 1):395–399, 1967.
28. Andres Baravalle, Mauro Sanchez Lopez, and Sin Wee Lee. Mining the dark web: drugs and fake ids. In *2016 IEEE 16th international conference on data mining workshops (ICDMW)*, pages 350–356. IEEE, 2016.
29. Javeriah Saleem, Rafiqul Islam, and Muhammad Ashad Kabir. The anonymity of the dark web: A survey. *Ieee Access*, 10:33628–33660, 2022.
30. Othmane Cherqi, Ghita Mezzour, Mounir Ghogho, and Mohammed El Koutbi. Analysis of hacking related trade in the darkweb. In *2018 IEEE international conference on intelligence and security informatics (ISI)*, pages 79–84. IEEE, 2018.
31. Paul Anthony Samuelson, Paul Anthony Samuelson, Paul Anthony Samuelson, Etats-Unis Economiste, and Paul Anthony Samuelson. *Foundations of economic analysis*, volume 197. Harvard University Press Cambridge, MA, 1983.
32. James H Richardson. The spotify paradox: How the creation of a compulsory license scheme for streaming on-demand music platforms can save the music industry. *UCLA Ent. L. Rev.*, 22:45, 2014.
33. Taneli Vaskelainen, Karla Münzel, Wouter Boon, and Koen Frenken. Servitisation on consumer markets: entry and strategy in dutch private lease markets. *Innovation*, 24(1):231–250, 2022.
34. Mark Blaug. *The methodology of economics: Or, how economists explain*. Cambridge University Press, 1992.
35. John R Hicks. Léon walras. *Econometrica: Journal of the Econometrica Society*, pages 338–348, 1934.
36. Cristian A Díaz, José Villar, Fco Alberto Campos, and M Ángel Rodríguez. A new algorithm to compute conjectured supply function equilibrium in electricity markets. *Electric Power Systems Research*, 81(2):384–392, 2011.
37. Mario J Miranda and Paul L Fackler. *Applied computational economics and finance*. MIT press, 2004.
38. Paul D Klemperer and Margaret A Meyer. Supply function equilibria in oligopoly under uncertainty. *Econometrica: Journal of the Econometric Society*, pages 1243–1277, 1989.
39. Richard J Green and David M Newbery. Competition in the british electricity spot market. *Journal of political economy*, 100(5):929–953, 1992.
40. John Von Neumann and Oskar Morgenstern. Theory of games and economic behavior: 60th anniversary commemorative edition. In *Theory of games and economic behavior*. Princeton university press, 2007.
41. Gerard Debreu. *Theory of value: An axiomatic analysis of economic equilibrium*, volume 17. Yale University Press, 1959.
42. Kenneth J Arrow. *Social choice and individual values*, volume 12. Yale university press, 2012.
43. Drazen Prelec. The probability weighting function. *Econometrica*, pages 497–527, 1998.
44. R Duncan Luce et al. *Individual choice behavior*, volume 4. Wiley New York, 1959.
45. Daniel McFadden. Conditional logit analysis of qualitative choice behavior. 1972.
46. Moshe E Ben-Akiva and Steven R Lerman. *Discrete choice analysis: theory and application to travel demand*, volume 9. MIT press, 1985.
47. Vid Kraner, Iztok Fister Jr, and Lucija Brezočnik. Procedural content generation of custom tower defense game using genetic algorithms. In *International Conference "New Technologies, Development and Applications"*, pages 493–503. Springer, 2021.

48. Aura Hernández-Sabaté, Meritxell Joanpere, Núria Gorgorió, and Lluís Albarracín. Mathematics learning opportunities when playing a tower defense game. *International Journal of Serious Games*, 2(4), 2015.
49. Gabriel Teixeira Galam, Tiago P Remedio, and Mauricio A Dias. Viral infection genetic algorithm with dynamic infectability for pathfinding in a tower defense game. In *2019 18th Brazilian Symposium on Computer Games and Digital Entertainment (SBGames)*, pages 198–207. IEEE, 2019.
50. Julia Brich, Katja Rogers, Julian Frommel, Martin Weidhaas, Adrian Bruckner, Sarah Mirabile, Tamara Dorn, Valentin Riemer, Claudia Schrader, and Michael Weber. Liverdefense: using a tower defense game as a customisable research tool. In *2015 7th International Conference on Games and Virtual Worlds for Serious Applications (VS-Games)*, pages 1–8. IEEE, 2015.
51. Shiva Maharaj, Nick Polson, and Alex Turk. Chess ai: competing paradigms for machine intelligence. *Entropy*, 24(4):550, 2022.
52. Omid E David, H Jaap van den Herik, Moshe Koppel, and Nathan S Netanyahu. Genetic algorithms for evolving computer chess programs. *IEEE transactions on evolutionary computation*, 18(5):779–789, 2013.
53. Scott Borg. Economically complex cyberattacks. *IEEE security & privacy*, 3(6):64–67, 2005.
54. Stephen Adams, Bryan Carter, Cody Fleming, and Peter A Beling. Selecting system specific cybersecurity attack patterns using topic modeling. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pages 490–497. IEEE, 2018.
55. John F Affisco and Michael N Chanin. An empirical investigation of integrated multicriteria group decision models in a simulation/gaming context. *Simulation & Gaming*, 21(1):27–47, 1990.
56. Enrique Areyan Viqueira and Cyrus Cousins. Learning simulation-based games from data. In *Proceeding AAMAS'19 Proceedings of the 18th International Conference on Autonomous Agents and MultiAgent Systems*, volume 2019, 2019.
57. Michael Wunder, Siddharth Suri, and Duncan J Watts. Empirical agent based models of cooperation in public goods games. In *Proceedings of the fourteenth ACM conference on Electronic commerce*, pages 891–908, 2013.
58. Manfred Deistler and Wolfgang Scherrer. Models with exogenous variables. In *Time Series Models*, pages 155–166. Springer, 2022.
59. Daniel Kahneman. Maps of bounded rationality: Psychology for behavioral economics. *American economic review*, 93(5):1449–1475, 2003.
60. Paul JH Schoemaker. The expected utility model: Its variants, purposes, evidence and limitations. *Journal of economic literature*, pages 529–563, 1982.
61. David Schmeidler. Subjective probability and expected utility without additivity. *Econometrica: Journal of the Econometric Society*, pages 571–587, 1989.
62. Richard H Thaler. Behavioral economics: Past, present, and future. *American economic review*, 106(7):1577–1600, 2016.
63. Enrique Castillo, José María Menéndez, Pilar Jiménez, and Ana Rivas. Closed form expressions for choice probabilities in the weibull case. *Transportation Research Part B: Methodological*, 42(4):373–380, 2008.
64. Frank S Koppelman. Closed form discrete choice models. In *Handbook of transport modelling*, volume 1, pages 257–277. Emerald Group Publishing Limited, 2007.
65. Baibing Li. The multinomial logit model revisited: A semi-parametric approach in discrete choice analysis. *Transportation Research Part B: Methodological*, 45(3):461–473, 2011.

66. Jerry Hausman and Daniel McFadden. Specification tests for the multinomial logit model. *Econometrica: Journal of the econometric society*, pages 1219–1240, 1984.
67. JMC Sturlese and Peter Purgathofer. Optimizing algorithmic decisions in executive game simulations. In *2025 4th International Conference on Computational Modelling, Simulation and Optimization (ICCMSO)*, pages 238–242. IEEE, 2025.