Board Games As A Behavioural Collection Method

Tatjana Sidorenko*, Dr. Duncan Hodges*, and Dr. Oliver Buckley†
*Centre for Electronic Warfare, Information and Cyber
Cranfield University
Defence Academy of the United Kingdom, Swindon, SN6 8LA, UK
Email: tatjana.sidorenko@cranfield.ac.uk, d.hodges@cranfield.ac.uk
†Department of Computer Science
University of East Anglia, Norwich, UK
Email: o.buckley@uea.ac.uk

***Abstract*—Traditionally, games have been viewed as a form of entertainment. Yet, given how engaging games can be their effects can be beneficial in many domains. This paper explores the use of games as a methodology of exploring the decision-making processes demonstrated by a group of information security specialists when role-playing as malicious actors.**

To achieve this a board game has been designed which enables players to impersonate different types of attackers each with different motivations and goals. Each player is given a set of tools, techniques and procedures (TTPs) in form of cards and a set of end goals which need to be achieved in order to 'win' the game. By interacting with the facilitator, who is also representing the defending organisation or location, they voice out their intended actions and decisions and play a TTP card of their choice.

By adopting a persona in an engaging fictional setting players are freed from concerns associated with self-image maintenance and concerns about reputational damage and ultimately, are better able to construct creative and malicious attacks. The game methodology also provides a less limited framework for the data gathering, and with suitable facilitation allows the capture of a very diverse set of attacks.

By using this methodology, it is possible to gather a more diverse set of both decision-making behaviour and attacks, improving our understanding of offensive actors. This understanding will then be used to influence the creation of an agent-based simulation of these actors and scenarios.

I. Introduction

Today, our lives are becoming increasingly digital, with day-to day activities, such as paying bills, shopping, socialising with friends and family and engaging with government services all being performed digitally and mediated by the Internet. This digitisation is not limited to individuals and our home lives -— organisations and governments also are increasingly transferring business data and processes to a digital format with the aim of working 'better' [1]. This digitisation is not only focused on information assets such as data and business processes, but we are increasingly digitising our physical world and creating Cyber-Physical systems (systems that are comprised from physical and computational components in a seamless integration [2]), this includes both critical national infrastructure and our wider national infrastructure.

This digital world enables a new variety of threats that may seek to compromise the security of these systems. Different adversaries that have a varying level of expertise and a variety of different motivations to attack are, on a daily basis, trying to compromise our information systems and gain some real-world outcome. For some actors it will be financial gain, for some it will be tied to national strategic goals and for others it will be simply a feeling of achievement. To reduce the cyber-associated risk it is important to understand both the actors involved in these attacks and their individual approaches to compromising information systems.

Even with recent improvements in machine learning and artificial intelligence it is challenging to replicate complex human decision-making such as is observed during cyber attacks, this is particularly true with advanced persistent threats (APTs) who exhibit complex naturalistic decision-making. The closest we can get to understanding a thought process of an adversary is surveys and interviews, such as work of Thackray et al. [3]. Even with interviews, there are a number of challenges: firstly, engaging with genuine adversaries is a problem, as not all actors would disclose their Tools, Techniques and Procedures (TTPs). Secondly, offensive cyber activity requires complex naturalistic decision-making which is typically difficult to access [ref] and participants may not be able to accurately describe their decision-making processes. An alternative approach to surveys or interviews might be lab-based observation where attackers are asked to perform an attack using a heavily metricated platform, with follow-up interviews to attempt to capture the decision-making process. This is a very costly process (in terms of time) and ultimately not flexible enough as the environment will need to be reconfigured for each different target environment. In this paper an alternative solution is proposed — using board games to replicate certain decisions taken by an adversary.

Board games have traditionally been used as a method of entertainment, and have a high engagement level, often involving different mechanics or a fictional setting. The fact that games are so engaging has led to various creative uses of board games. For example Atys of Lydia has used board games to help his people survive hunger for 18 years after a severe drought [4]. Since games were so addictive and entertaining people have managed to stay away from gastronomy-related thoughts and were able to survive by only eating every other day. Alternative applications of board games will be explored in Section II. As the application of board games has shown promising results in other fields, they have been used for the

approach that is outlined in this paper.

Section II sets out the background behind the study by considering past work in the field. Section III outlines the methodology by which the study has been carried out, whilst section IV describes the subsequent use of the outputs from the games as well as validation strategies. Finally, section V contains concluding remarks.

II. Background

The first step to understanding adversaries is to recognise that there are different types of adversaries with different motivations, i.e. different 'goals' or measures of success for their attack. Some are driven by money [5], some by revenge [6], some are merely thrill-seekers [7]. Meyers et al. [8] have defined four key factors associated with attacker motivation — *revenge, financial, curiosity* and *notoriety*. Seebruck [9] builds upon this model and defines a fifth motivation of ideology, resulting in the following five: *prestige, recreation, ideology, profit* and *revenge*. This is shown in Table I.

TABLE I
THE HIGH-LEVEL MOTIVATIONS FOR NON-STATE MALICIOUS ACTORS

Meyers et al. [8]	Seebruck [9]
Revenge	Revenge
Financial	Profit
Curiosity	Recreation
Notoriety	Prestige
	Ideology

As the base motivations have now been identified, it is also important to understand how these drive the variety of attackers and the Tools, Techniques and Procedures they use, attacks are likely to vary in their level of complexity merely from the type of an individual (or a group) executing them and the motivation of the said individual or a group.

To achieve this classification of malicious actors a taxonomy of attackers was synthesised from the literature. The taxonomy of adversaries used in this study is listed below:

Script kiddies Meyers et al. [8] define script kiddies as novices in the field, that are motivated by boredom and thrill-seeking. Historically these are the least sophisticated category that rely on pre-written tools which are not reconfigured or tailored to the task. They are also the least creative and unable, or unwilling, to adapt attack methodologies should an attack fail. Seebruck [9] writes that they are motivated by curiosity whilst Coleman [10] defines script kiddies as *'a derogatory term for a technologist lacking real skills'*. Barber [11] describes them as school-aged, typically male. And while they do not know the specifics of how internet works, they do know enough to cause damage.

Hacktivists Meyers et al. [8] acknowledge hacktivists being motivated by a political cause. They attack primarily using DoS and defacements, although can also use other forms of attacks. Usually they are targeting organisations, yet their attacks can have more widespread negative consequences. Barber [11] describes hacktivism existing *'to cause damage to make an ecological, political or ethical reason'*.

Counter-culture A combination of thrill and fame seeking, these adversaries are interested in having fun from illegally accessing a target. Meyers et al. [8] defines them as 'cyber punks' that are seeking 'attention and prestige'. They typically are more experienced than script kiddies and can write their own simple tools, and typically are not politically or ideologically motivated, unlike hacktivists. Typically, they pick high-profile targets, that causes them to be featured in the news. In the work of Sailio et al. [12] they are denoted as 'thrill-seekers' and are defined as *'a person, who attacks computer systems merely to prove himself, in order to learn or experiment.'*

State-affiliated This term refers to both hostile nation-state actors, such as state intelligence or military actors. In addition we include proxies who are sponsored, acting in support of the state or part of a state/crime nexus [13]. Activity is commonly part of a geographic strategic goal, and can vary from simple destructive payloads [14], large scale financial theft [15] through to operationally preparing the environment within Critical National Infrastructure [16].

Cyber criminal A cyber criminal is a definite subset of a black hat [8], and their two objectives are: to extract value (money or valuable data) and to avoid legal consequences [12]. Historically they have acted alone or within small 'gangs' although increasingly operate within a 'marketplace' framework that allows (and rewards) specialism and can result in very sophisticated attacks [17].

Insider Cappelli et al. [18] define insider threat as *'a current or former employee, contractor, or business partner who has or had authorised access to an organisation's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.'*. The scope of this paper is external cyber threats therefore insiders will not be considered at this stage, however it is possible to create insider roles using the same methodology discussed in this paper and indeed some external attacks are likely to involve the manipulation of unintentional insider threats [19].

Above is the list of common adversaries that might be observed in cyberspace, and the goals or motivations we could attribute to them. However, this understanding must be supplemented with knowledge of the Tools, Techniques and Procedures (TTPs) observed by the actors. It is these TTPs that generate observable artefacts within cyberspace, before and during an offensive cyber operation. Attempts have previously been made to identify and classify common TTPs [20]–[22]. Yet such taxonomies are problematic to keep up to date, as new proof-of-concepts and new vulnerabilities are released very often, for example Common Vulnerabilities and Exposures

(CVE) list is updated daily [23], which opens a possibility for new attacks that exploit these disclosed vulnerabilities, and indeed we see both criminals and sophisticated actors such as Turla and The DUKES/ APT 29 weaponizing vulnerabilities at a very high tempo. Rather than build yet another taxonomy of TTPs we chose to use the MITRE ATT&CK Framework [24] to capture the tools, techniques and procedures associated with our adversaries. This taxonomy, in our view, provides the most up-to-date structured understanding of observed TTPs [25].

An extensive list of adversaries and TTPs provides an understanding of the 'pieces' or entities we might need to understand to be able to model cyber attacks. The next stage is to consider how a given adversary builds and then executes their attack using these constructs. Previous attempts have been made to better understand the process by which attacks shape in the mind of an adversary and become tangible, the literature generally supports three methods: interviews, observations, and role-play.

A. Interview

In the interview approach, individuals are asked a variety of questions on their experiences. Lusthaus [26] has conducted an extensive study with 238 interviews in various locations over a seven-year period. The interviewees included current and former law enforcement officials, IT professionals and cybercriminals and other individuals who could provide a useful insight. Other notable work is of Thackray et al. [3], who employed a combination of virtual observation on private 'hacking' forums to study and observe social norms on these forums and a survey hosted on Reddit, a social networking platform that focuses on communities and topics.

Interviews allow a broad insight into certain topic or a situation, as it is possible to interact with the interviewee in real time and ask them to elaborate on any chosen aspect [27]. However, interviews are restricted by self-presentation of the individual being interviewed, as anything they say can potentially be taken out of context, hence an answer to any question has to be passed through a rigorous self-filter [28]. In case of online surveys, there is an entirely different issue. Online surveys provide a diverse sample of responses, which can have both beneficial and detrimental consequences. One of the benefits is that it is possible for anyone who has a link to contribute and have their opinions considered. The wider the reach of the survey, the greater the sample of the target audience. In case of cyber adversaries this would be information security professionals, security enthusiasts, potentially former cyber adversaries themselves. Yet, with the diversity and openness of a study, there will always be individuals who do not take it seriously, or those who would claim to be security specialists, when in reality, they are not. There is no reliable way to verify every single respondent and whether they are telling the truth or not [29].

B. Observations

Within the context of this study observations would involve creating a controlled environment where it would be possible to witness various individuals at work. Such emulation is required to get the conditions as close to an adversary's conditions as possible. The existence of a controlled environment ensures the overall experiment is reproducible. This observational research method would allow the artefacts from the decision-making process to be observed, even if the participant cannot express their decision-making process [30]. On the other hand, setting up such an environment is a time-consuming process and provides little flexibility in terms of alternative scenarios and context. In addition there is the observer effect caused by the participant knowing they are observed and tailoring or controlling their behaviour [31].

C. Role-play

Another method is observation of individuals adopting and role-playing a chosen persona. An example of this technique is the work of Bolland [32], where experienced role-players were selected to impersonate world leaders. This method attempts to capture a perspective on actions or decisions that are usually inaccessible individuals (due to their business, social status, language barriers, location or similar reasons) and obtain an approximate understanding of their world view and what decisions would they take. This approach also has its flaws, for example if a persona that an individual has to act out has a vastly different world view from the individual who has adopted it, there might lead to a possibility where certain decisions that a persona would take would contradict the world view possessed by an individual impersonating it. This can arise, for example due to differences in morals, which can impede an accurate representation. This can be mitigated by making sure the individual themselves pick the persona they would be comfortable portraying.

An emerging approach that has also shown promising results when used in other applications is the use of games [33], [34]. In the field of cyber security there have been several attempts in the industry, including PwC [35] with a game that is aimed at educating the board of executives on the impact of cyber adversaries. Another example is Infosec D&D [36] where players representing the defending side (SoC, incident response and similar) are walked through a cyber attack taking place. Engaging with fictional scenarios and having a well-thought out game mechanic to tie everything together allows the participants to 'experience' a cyber attack themselves, hence realising the impact and consequences of having a poor defensive posture.

The use of games can be considered an augmentation of role-play, with the addition of a framework of game mechanics. The introduction of game mechanics ensures there is a structure to play by guiding the players through the game yet the game unfolds with an element of chance, represented by elements such as die rolls and unpredictable human behaviours.

In this paper, a methodology is proposed, where instead of representing the defending side participants are role-playing as attackers, framing the defensive mission as an attacker-orientated exercise.

III. Method

The intended players of the game will be cyber security specialists and those with basic cyber security knowledge as there will be a degree of familiarity with common Tools, Techniques and Procedures. Bearing the target audience in mind the next step is to create some design criteria for the game. The objective is to design a game with the following characteristics in mind:

1) Be engaging
2) Be reproducible with a rigorous scientific, evidence-based underpinning
3) Be easy to play and run
4) Have a way to easily capture the gameplay to generate actionable intelligence

Initially existing tabletop games were considered as a framework: tabletop role-playing game platforms such as Dungeons and Dragons (D&D) [37] and FATE [38]. Typically in games of this type, there is a Dungeon Master (DM) or a Games Master (GM) that chairs the game and ensures that players do not break the rules as well as setting a scene or a scenario. Both of these frameworks rely heavily on collaboration between players, yet the game that is being designed should provide some options for collaboration, yet interactions *between the players* should not be the key driving force. Instead, the focus would be on the interaction of a player and the system they are attacking, with collaboration being transient and mutually beneficial (as it is in a contested cyberspace). An alternative paradigm in the field of tabletop adventure games is titles such as Android Netrunner [39], which is a cards-only board game that uses cards as the key driving mechanism for progressing the gameplay.

Both types of a tabletop adventure game mentioned above are engaging, but with the approach fully focused on player interactions it is easy to lose the structure of the game. Whilst this lack of structure allows an entertaining and enjoyable experience for the participants maintaining a repeatable study which could be used to gather actionable intelligence is challenging.

Meanwhile, with the cards-only approach, it might be very difficult for novice players to pick up the rules, since card interactions might can become very complex. As 'ease of use' was one of the primary targets, the game needs to be complex enough to convey the scenario and generate realistic interactions, yet simple enough to be picked up by a complete novice. This will be achieved by using a combined approach — game cards to provide structure and Games Master (GM) to support the players and ensure the gameplay is focused within the scenario. A GM will be able to guide players and get support weaker players, yet there will also be a help-sheet with quick, bite-sized actions of what each player can do on their turn. By tailoring to different board game familiarity levels it would be possible to achieve initial engagement, and with rules and interactions that are simple enough – preserve this level of engagement.

The presence of game cards and clear instructions guarantees that the process of playing the game is consistent, which ensures reproducibility between games. Furthermore, the game resources have been designed following the principle of minimalism — only the essential information is printed on the cards, and only decks that are essential for the game are used. With this principle, it is possible to see essential information at a glance. Visually coherent cards coupled with clear instructions make the game easy to use.

The game itself consists of a role-scenario pack and four additional decks: techniques, counter-techniques, information and opportunity. These decks are summarised below:

Role-scenario pack consists of a cyber attack scenario and adversarial roles outlined in Section II. These role cards have goals and motivations specifically tailored to the scenario. Completing goals allows a player to 'win' the game — goals can range from 'getting access' to 'publishing stolen data online'. These goals are designed to be related to the motivation of a given role — for example, given a script-kiddie and a nation-state are likely to have different motivations for attacking the organisation, they in turn have different goals and hence a different 'win' condition. The scenario is used to provide context and to ensure the game setting is as close to a 'real-world' conditions as possible.

Techniques deck contains of commonly used TTPs and is designed for use by the players. These techniques were selected using MITRE ATT&CK and then distributed in a survey among information security professionals and enthusiasts so that they could provide more information. An example of the information provided was the pre-requisites needed for a technique to succeed.

Counter-techniques deck contains common counter-techniques or 'mitigations' as they are listed under in the MITRE ATT&CK framework. This deck is designed for use by the Games Master in response to techniques that players themselves use.

Opportunity deck is an amalgamation of various enabling strategies for an adversary to exploit. For example, one of the opportunities enables the player to tailgate an employee into a building. These opportunities are designed to be handed out by the GM if they see that a player is struggling or to steer the scenario into a particular direction. These are sourced from case studies and in parts from the survey, as when survey respondents have listed pre-requisites for an attack, some of these pre-requisites were fit for an opportunity card.

Info deck is a deck of assets to capture, that may later evolve into pre-requisites to carry out a particular attack. They are handed out to each of the players as the players acquire them. Info cards are also sourced from case studies and the survey using the same logic as the Opportunity cards.

It is important that the game resources are developed with scientific rigour, hence all decks have been generated using

existing literature and experts' opinion via a survey that resulted in 141 responses. A visual representation of information sources for all cards and scenarios is shown in Figure 1.

The foundation for the game mechanics has been developed using the NCSC kill chain [40]. It considers four stages: survey, delivery, breach and affect as it's foundation. Techniques from the MITRE ATT&CK framework have been classified into these four categories to provide structure to their use and ensure the game generates realistic attacks.

Initially, players start with a set number that is called the 'risk appetite', which defines a specific role's susceptibility to use high-risk high-reward techniques. Choosing to use different techniques in the game costs risk-appetite points, these get restored when a chosen technique succeeds and at a much lower rate than they are spent. In a real-world scenario, this would represent the tendency to take more risks if previous techniques have succeeded, or vice versa — trying to be more careful if previous techniques have failed. This concept can be roughly translated to the concept of 'health' in other games.

There is a concept of 'luck' in games that is represented by a six-sided die roll. Each technique has a minimum roll number — a minimum number that needs to be rolled for a technique to succeed. Equation 1 shows how it is calculated, $factor$ represents the impact or recon factors — these have been determined by survey respondents. This metric determines how much information a technique can disclose about the target (recon factor) or how severe the consequences would be from a cyber attack when translated to real-world (impact factor), e.g. power outage. $category$ is NCSC kill chain mappings explained above — techniques that are classified as being related to the preparation of an attack, i.e. survey or delivery will, in general, involve less interaction with an adversary than those relating to later stages of the kill-chain, i.e. belonging to breach and affect. This, in turn makes them less costly in terms of risk points, as during the early stages if a technique fails, the consequences are likely to be less severe. The entire sum is divided by two to map the values to a six-sided die.

$$min\ roll = \left\lceil \frac{factor + category}{2} \right\rceil \tag{1}$$

Lastly, one of the initial objectives was to have a way to easily capture the gameplay. A system has been developed to quickly record game moves, that is similar to the 'algebraic notation' in chess [41], see Figure 2. Each card within the deck of cards has been unambiguously identified in the format **LDD**, where 'L' stands for 'letter' and 'D' stands for 'digit'. The first symbol is the deck that a card belongs to, it can be one of the following:

- T = Technique
- O = Opportunity
- I = Information
- C = Counter-technique
- R = Role

The double-digit at the end represents the card number in the deck and is designed to tell cards apart from each other.

The Games Master can optionally react with a counter-technique, which is represented by **GM CDD**, where 'GM' stands for Games Master, 'C' stands for Counter-technique and 'DD' is the number of the card.

Finally, techniques succeeding or failing is represented by **S** or **F** respectively. If a player rolls less than the minimum roll outlined in Equation 1 a technique fails. When a technique fails, a consequence is applied to a player. This is represented by **cs D**, where 'D' is a single digit corresponding to which consequence of three (light, medium or severe) has been applied.

Using such notation will allow the efficient capturing of the decisions during the game and will allow reconstructing the game just from the move set, similarly to chess.

IV. Simulations and Validations

The objective of the game is to capture the decisions that are made as individuals play as a variety of different attackers, and the processes by which they go about reaching their desired goal. Ideally, we would like to be able to run many iterations of this game and explore the non-linear interaction effects between offensive actors. However, running these games is time-consuming and resource intensive, whilst this is still less than an lab-based observation study it can still become prohibitive. To expand the application of the data gathered from the game-based studies we can look to construct a computational simulation of the game allowing us to 'play-out' many different scenarios. Ultimately, the goal is to run computational simulations and physical-world games in parallel, examining and comparing outputs from the two. This section will explain how the simulation would be used to augment what has been achieved with the game.

Over the course of a number of games there are multiple people playing the same scenario with one role (attacker persona), this samples from the wide-range of possible approaches to playing that role. While the in-person games are restricted by how many people can play the game at once, a simulation does not have these restrictions. For example, it would be possible to explore the range of outcomes if there is a single attacker of a given persona and compare this with a large number of attackers of that persona. Effectively exploring the aggregated threat from a very large number of attackers who have a low-level of success. This flexibility in the composition of those participating in a scenario allows us to provide a rich understanding of the likelihood of success associated with each role/scenario pairing.

In a scenario-specific case it is possible to see what roles and in which amounts work better in a certain context. But what happens when the roles are taken out of a scenario-specific context? The details of the goal change, yet the nature of it does not [42]. In case of a hacktivist, they would want to get their message across. On one hand, the nature of the message might change depending on the scenario: political, environmental, ethical. On the other, the goal of 'get the message across' would not. Each role has a limited set of goals driven by the intrinsic motivations that they would follow

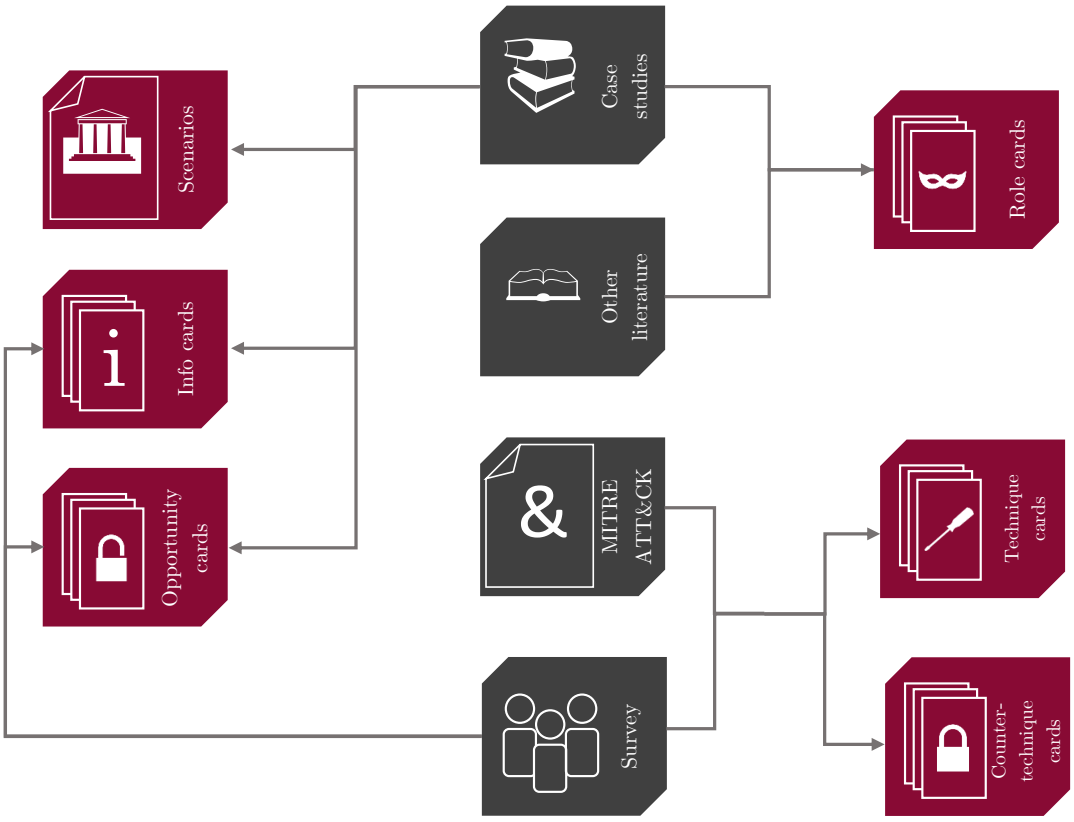

Fig. 1. *Information sources*. **Scenarios** come from the news stories and use-cases. **Role cards** come from attacker taxonomies outlined in Section II and motivations for these roles come from case studies. **Info** and **Opportunity** cards will also depend on the scenario, although some have been identified in the survey. **Technique** and **Counter-technique** card titles and descriptions are sourced from MITRE ATT&CK with other game mechanics-dependent information comes from the survey, and the number of cards in the counter-technique deck is dependent on the Techniques deck.

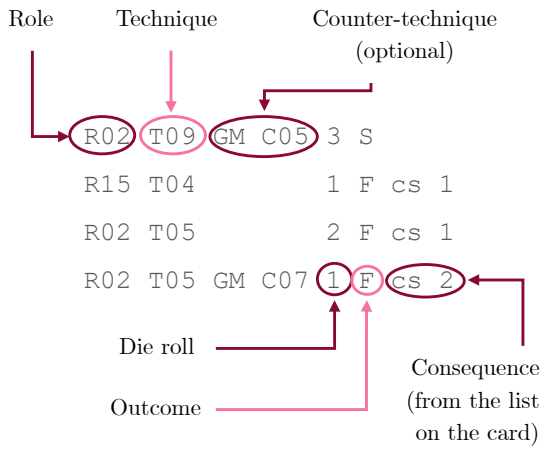

Fig. 2. *An example transcription of a move set using custom notation.*

to get involved in an adversarial attack. While the intrinsic motivation of an adversary is out of scope of this paper, the goals they use to fulfil it are not.

If the fundamental goal stays the same, we could hypothesise that it should also be possible to transfer certain decisions from one scenario to another. For example, in most businesses with a digitised infrastructure there will be a database that will store employees' personnel records. In every e-commerce platform there will be a products database. There is almost guaranteed to be some kind of public-facing website or an internal file store. Decisions involving these key information assets may be transferable between scenarios.

With the ability to vary the composition of the set of attackers within the simulation and the potential to transfer decision to new scenarios it will be possible to support the defensive posture of an organisation or mission. Effectively allowing the enumeration of the techniques which are more likely to lead to successful security compromises, rather than the techniques that are simply observed most often.

V. Conclusion

Games provide a unique mechanism to explore adversaries and can allow those with basic cyber expertise to role-play as a variety of adversaries within a structured framework. This arrangement requires significantly less setup than a controlled lab environment and can be repeated as many times as required. Use of a fictional scenario built upon real-life case-studies allows players to step away from their real-life selves to adopt a fictional persona, which enables a more 'free' and unconstrained set of decisions.

To ensure the decisions made in the game were as realistic as possible, a combination of literature (case-studies, attacker taxonomies and TTP frameworks) and experts' opinions have been used to synthesise resources that replicate real-world scenarios, attacker motivations and TTPs as closely as possible. The game was required to be easy to use, reproducible and engaging, as well as providing a way to capture the gameplay for later analysis. This was achieved by ensuring that the game mechanics were intuitive yet functional, with the game resources ensuring good reproducibility, whilst the role-playing aspects have been inspired by existing recreational tabletop games to maximise engagement. Use of a shorthand notation allows capturing the gameplay as the game occurs.

Using a computational simulation in parallel with serious games enables the aggregation of attack-patterns and an assessment of the threat caused by varying adversary role types compositions. A computational simulation driven by the diversity of attacks generated by a diverse range of participants creates a set of decisions that have a solid grounding in literature as well as being backed up by creative, dynamic and emerging effects from the real-world players. This evidence-based approach to defensive posture permits a mission-centric view of cyber defence, enabling the most efficient **mission** assurance.

VI. Acknowledgements

The research covered in this paper is funded by Defence Science and Technology Laboratory under the project 'Agent Based Modelling of Offensive Actors in Cyberspace' Military Cyber Systems PhD Studentship.

References

[1] GOV.UK, "GDS communications strategy: 2018 to 2019," 2018, accessed: 2020-10-19. [Online]. Available: https://www.gov.uk/government/organisations/government-digital-service/about

[2] National Science Foundation, "Cyber-physical systems (CPS)," p. 2, 2020, accessed: 2020-10-19. [Online]. Available: https://www.nsf.gov/pubs/2020/nsf20563/nsf20563.pdf

[3] H. Thackray, C. Richardson, H. Dogan, J. Taylor, and J. Mcalaney, "Surveying the Hackers: The Challenges of Data Collection from a Secluded Community," Bournemouth University, Tech. Rep., 2017. [Online]. Available: https://www.researchgate.net/publication/322342449_Surveying_the_Hackers_The_Challenges_of_Data_Collection_from_a_Secluded_Community

[4] F. N. David, *Games, gods and gambling: The origins and history of probability and statistical ideas from the earliest times to the Newtonian era*. Hafner Publishing Company, 1962, p. 6, iSBN: 978-0486400235.

[5] S. Coble, "Two new carding bots threaten e-commerce sites," 2019, accessed: 2020-10-24. [Online]. Available: https://www.infosecurity-magazine.com/news/two-new-carding-bots-threaten/

[6] B. Sussman, "Revenge hack against a security researcher," 2020, accessed: 2020-10-24. [Online]. Available: https://www.secureworldexpo.com/industry-news/revenge-hack-vinny-troia

[7] J. Cowan, "Majority of hackers do it for the thrill, believe they won't be caught: Survey," 2014, accessed: 2020-10-24. [Online]. Available: https://www.sitepronews.com/2014/08/14/majority-hackers-thrill-believe-wont-caught-survey/

[8] C. Meyers, S. Powers, and D. Faissol, "Taxonomies of cyber adversaries and attacks: a survey of incidents and approaches," Lawrence Livermore National Lab.(LLNL), Livermore, CA (United States), Tech. Rep., 2009. [Online]. Available: https://www.osti.gov/biblio/967712

[9] R. Seebruck, "A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model," *Digital Investigation*, vol. 14, pp. 36–45, 2015. DOI:10.1016/j.diin.2015.07.002

[10] Gabriella Coleman, *Hacker, Hoaxer, Whistleblower, Spy The Many Faces of Anonymous*. Verso, 2014, iSBN: 9781781685839.

[11] R. Barber, "Hackers Profiled — Who Are They and What Are Their Motivations?" *Computer Fraud & Security*, vol. 2001, no. 2, pp. 14–17, 2001. DOI:10.1016/S1361-3723(01)02017-6

[12] M. Sailio, O.-M. Latvala, and A. Szanto, "Cyber Threat Actors for the Factory of the Future," *Applied Sciences*, vol. 10, no. 12, p. 4334, Jun 2020. DOI:10.3390/app10124334

[13] T. Maurer, "Cyber proxies and their implications for liberal democracies," *The Washington Quarterly*, vol. 41, no. 2, pp. 171–188, 2018. DOI:10.1080/0163660X.2018.1485332

[14] BBC News, "Shamoon virus targets energy sector infrastructure," 2012, accessed: 2020-10-24. [Online]. Available: https://www.bbc.co.uk/news/technology-19293797

[15] Novetta, "Operation Blockbuster: Unraveling the Long Thread of the Sony Attack," Novetta, Tech. Rep., 2016. [Online]. Available: https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf

[16] Cylance, "Operation Cleaver Report," Cylance, Tech. Rep., 2014. [Online]. Available: https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

[17] K. Huang, M. Siegel, and S. Madnick, "Systematically understanding the cyber attack business: A survey," *ACM Comput. Surv.*, vol. 51, no. 4, Jul. 2018. DOI:10.1145/3199674

[18] D. M. Cappelli, A. P. Moore, and R. F. Trzeciak, *The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (Theft, Sabotage, Fraud)*. Addison-Wesley, 2012.

[19] F. L. Greitzer, J. Strozer, S. Cohen, J. Bergey, J. Cowley, A. Moore, and D. Mundie, "Unintentional insider threat: Contributing factors, observables, and mitigation strategies," in *2014 47th Hawaii International Conference on System Sciences*, 2014, pp. 2025–2034. [Online]. Available: https://ieeexplore.ieee.org/document/6758854

[20] U. Lindqvist and E. Jonsson, "How to systematically classify computer security intrusions," in *Proceedings. 1997 IEEE Symposium on Security and Privacy*, 1997, pp. 154–163.

[21] C. Simmons, C. Ellis, S. Shiva, D. Dasgupta, and Q. Wu, "AVOIDIT: A cyber attack taxonomy," *9th Annual Symposium on Information Assurance*, pp. 12–22, 2014. [Online]. Available: https://www.albany.edu/iasymposium/proceedings/2014/ASIA14Proceedings.pdf#page=12

[22] M. A. Douad and Y. Dahmani, "ARTT taxonomy and cyber-attack Framewok," *NTIC 2015 - 2015 1st International Conference on New Technologies of Information and Communication, Proceeding*, 2015. DOI:10.1109/NTIC.2015.7368742

[23] The Cassandra Tool, "CVE changelog: today," 2020, accessed: 2020-10-20. [Online]. Available: https://cassandra.cerias.purdue.edu/CVE_changes/today.html

[24] Mitre, "Mitre ATT&CK," 2020, accessed: 2020-10-17. [Online]. Available: https://attack.mitre.org/

[25] J. Work, "In wolf's clothing: Complications of threat emulation in contemporary cyber intelligence practice," in *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 2019, pp. 1–8. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8885269

[26] J. Lusthaus, *Industry of anonymity: Inside the business of cybercrime*. Harvard University Press, 2018, iSBN: 9780674979413.

[27] S. Kvale, *InterViews: An Introduction to Qualitative Research Interviewing*. Sage, 1996, iSBN: 080395820X.

[28] Y.-J. Lee and W.-M. Roth, "Making a scientist: Discursive "doing" of identity and self-presentation during research interviews," *Forum: Qualitative Social Research*, vol. 5, no. 1, 2004. DOI:10.17169/fqs-5.1.655

[29] J. F. Gubrium and J. A. Holstein, *Handbook of interview research: Context and method*. Sage Publications, 2001. [Online]. Available: https://dx.doi.org/10.4135/9781412973588

[30] J. Sanger, *The compleat observer?: A field research guide to observation*. Psychology Press, 1996, no. 2, iSBN: 978-0750705516.

[31] A. E. Kazdin, "Observer effects: Reactivity of direct observation." *New Directions for Methodology of Social & Behavioral Science*, 1982. [Online]. Available: https://psycnet.apa.org/record/1983-22374-001

[32] B. Bolland, "Re-thinking Coercion," *The RUSI Journal*, vol. 151, no. 4, pp. 42–46, Aug 2006. DOI:10.1080/03071840609442034

[33] L. von Ahn, "Games with a purpose," *Computer*, vol. 39, no. 6, pp. 92–94, 2006. DOI:10.1109/MC.2006.196

[34] A. Lieberoth, "Shallow Gamification," *Games and Culture*, vol. 10, no. 3, pp. 229–248, May 2015. DOI:10.1177/1555412014559978
[35] PwC, "Game of threats," 2020, accessed: 2020-10-17. [Online]. Available: https://www.pwc.co.uk/issues/cyber-security-services/game-of-threats.html
[36] Purple Squad Security, "Episode 15 – Infosec Tabletop D&D with Brakeing Down Security," 2017, accessed: 2020-10-21. [Online]. Available: https://purplesquadsec.com/episode/d1cc212c63164e6b/episode-15-infosec-tabletop-d-d-with-brakeing-down-security
[37] Wikipedia, "Dungeons & dragons - wikipedia," 2018, accessed: 2020-10-23. [Online]. Available: https://en.wikipedia.org/wiki/Dungeons_%26_Dragons
[38] B. E. Leonard Balsera, "Fate core," 2013, accessed: 2020-10-23. [Online]. Available: https://www.evilhat.com/home/fate-core/
[39] BoardGameGeek, "Android: Netrunner — board game — boardgamegeek," 2020, accessed: 2020-10-23. [Online]. Available: https://www.boardgamegeek.com/boardgame/124742/android-netrunner
[40] N. C. S. Centre, "How cyber attacks work," 2016, accessed: 2020-10-23. [Online]. Available: https://www.ncsc.gov.uk/articles/how-cyber-attacks-work
[41] International Chess Federation, "Appendix c - fide handbook," 2018, accessed: 2020-10-23. [Online]. Available: https://handbook.fide.com/chapter/E012018
[42] O. Kenneth, "Motivation And Demotivation Of Hackers In The Selection Of A Hacking Task – A Contextual Approach," Ph.D. dissertation, McMaster University, Hamilton, Ontario, Mar 2016. [Online]. Available: http://hdl.handle.net/11375/19114