CRANFIELD UNIVERSITY

TATJANA SIDORENKO

AGENT-BASED MODELLING OF OFFENSIVE ACTORS IN CYBERSPACE

SCHOOL OF DEFENCE AND SECURITY

PhD
Academic Year: 2018–2021

Supervisors: Dr D. Hodges, Dr O. Buckley
December 2021

CRANFIELD UNIVERSITY

SCHOOL OF DEFENCE AND SECURITY

PhD

Academic Year: 2018–2021

TATJANA SIDORENKO

Agent-Based Modelling of Offensive Actors in Cyberspace

Supervisors: Dr D. Hodges, Dr O. Buckley
December 2021

Abstract

With the rise of the Information Age, there has also been a growing rate of attacks targeting information. In order to better defend against these attacks being able to understand attackers and simulate their behaviour is of utmost importance. A recent approach of using serious games provides an avenue to explore offensive cyber attacks in a safe and fun environment. There exists a wide range of cyber attackers, with varying levels of expertise whose motivations are different. This project provides a novel contribution in using games to allow people to role play as malicious attackers and then using these games as inputs into the simulation.

A board game has been designed that emulates a cyber environment, where players represent offensive actors, with seven roles - Cyber Mercenary (low and high capability), State-backed (low and high capability), Script Kiddy, Hacktivist and Counter-culture (not motivated by finances or ideology). The facilitator or the Games Master (GM) represents the organisation under attack, and players use the Technique cards to perform attacks on the organisation, all cards are sourced from existing Tools, Techniques and Procedures (TTPs). Along with the game, players also provided responses to a questionnaire, that encapsulated three individual differences: Sneider's self-report, DOSPERT and Barratt's Impulsiveness scale. There was a total of 15 players participating in 13 games, and three key groups of individual differences players. No correlation was identified with the individual Technique card pick rate and role. However, the complexity of the attack patterns (Technique card chains) was modulated by roles, and the players' individual differences.

A proof-of-concept simulation has been made using an Agent-Based Modelling framework that re-plays the actions of a player. One of the aspects of future work is

the exploitation of the game data to be used as a learning model to create intelligent standalone agents.

Contents

List of Figures

List of Tables

Acknowledgements

First and foremost I would like to thank my incredible supervisor, Dr. Duncan Hodges for going above and beyond for making this work possible, always providing excellent advice and helping me on my research journey, for always finding the time for discussions, and for making sure the drafts always find me just in time. Truly, thank you for all your help.

Thank you to my wonderful colleagues, Dr. Katie Paxton-Fear, who was and still remains an inspiration to me to this day, always offering support in the hardest of times. And a special thank you goes to Shabarish Sriraman for his fresh perspective on many aspects of the project and looking after me while I look after my project.

Also I would like to thank Dr. Natalie Clewley, Dr. Adam Zagorecki and Dr. Rob Black, your advice has been invaluable for my work and has definitely helped me to think like a researcher. Natalie, whose eagle eye was able to spot a discussion point, Adam, whose experience in modelling and simulations has been extremely valuable, and Rob, whose support and insight into relevant research has greatly helped me with the completion of my thesis.

And a thank you each goes to my fellow research students and colleagues - Damien Lancereau, Marlene Vetter, Sam Westlake, Alix Leroy, Akhil Kallepalli, Joe Luery, Amélie Grenier, Ruben Moya Torres, Jacopo Bonifacio and Marco DiFraia. Another thank you goes to the wonderful DFU team - Dr. Sarah Morris and Melissa Hagkiss. A special thank you goes to Dr. Vicky Smy for the wonderful tea! I would also like to thank Nikki Williams for sharing her experiences on making educational games.

I would also like to thank DSTL for sponsoring my project, and especially Faye Parker-Jeffery for always providing helpful and insightful comments that have guided me in certain parts of my project and Oliver Lanning for always providing avenues for development, and Sarah Johnson for making sure the project runs smoothly.

Thank you to Cranfield University for providing me with all the necessary resources, and a wonderful office to stay in throughout my journey, lovingly called 'The Lair'. And to the very reliable ThinkPad laptop that the university has provided, for serving me well and never failing me (computers should also get the credit). And thank you to the wonderful staff – Mandy Smith for the best library training sessions, the rest of the library team for always responding to any queries that I had, and making sure that I find the correct resources, Annie Maddison Warren for her sense of humour and Bea Kingdon for always being a ray of sunshine.

A special thank you to my parents, Ludmila and Andrey, I will forever be grateful for all the unconditional love, care and support that they have given me. Without them none of this would be possible. A thank you also goes to my brother Alexander,

for supporting me with whatever I do.

List of Abbreviations

ANOVA	ANalysis Of VAriance
APT	Advanced Persistent Threat
DES	Discrete Event Simulation
MFA	Multi-Factor Authentication
SME	Small-to-Medium-sized Enterprise
SMB	Small-to-Medium-sized Business
SSW	Sum of Squares Within
TTPs	Tools, Techniques and Procedures
VAPT	Vulnerability Assessment and Penetration Testing

Chapter 1

Introduction

> Hackers are breaking the systems for profit. Before, it was about intellectual curiosity and pursuit of knowledge and thrill, and now hacking is big business.
>
> Kevin Mitnick

This chapter will begin by examining the effect of malicious cyber attacks and the impact on society from their attacks. This will be followed by having a closer look at some of the modern cyber defence methods. Within this context the aims and objectives of this research will be developed. This chapter will be wrapped up by highlighting how this research is novel and contributes to the literature.

1.1 The Evolution of Malicious Cyber Attacks

Every year organisations suffer from cyber attacks, and every year the problem only keeps getting bigger. According to the annual IC3 report released by the Federal Bureau of Investigation, there has been a total of $4.2 billion loss (Federal Bureau of Investigation, 2021) due to cybercrime in 2020 compared to $3.5 billion loss in 2019. Around 43% (Нефёдова, 2021) of these losses were attributed to Business Email Compromise (BEC) and regular Email Account Compromise (EAC). BEC attacks happen when an employee falls victim to phishing, spear-phishing and email

scams (Bakarich & Baranek, 2019), implying that either companies do not train their personnel enough or the attackers are getting more and more proficient with crafting sophisticated phishing campaigns that are capable to fool even the most vigilant security researcher just because the timing was right or the phishing content was relevant to the target (Doctorow, 2010; Heaton, 2019; Grobmeier, 2016). 59% of consumers would likely avoid doing business with an organisation that had experienced a cyberattack (Arcserve, 2020). Not only would an organisation experience loss from the cyber attack on its own (as the data was leaked), but also now the clients would begin leaving, as in their eyes this organisation is no longer secure. This would mean that organisations have to try harder to avoid becoming a victim of cyber attacks, otherwise they risk losing clients. Recently, the General Data Protection Regulation (GDPR) has been introduced, adding further measures for companies to comply with. Now, the organisation must report a data breach within just 72 hours of becoming aware (Information Comissioner's Office, 2021). So far, thousands of companies have already been fined for not complying with the regulations (CMS, 2021), with maximum possible fine to be £17.5 million or 4% of annual global turnover in the UK (whichever is greater) and €20 million or 4% of annual global turnover in the EU (whichever is greater)(IT Governance, 2021). With the COVID-19 pandemic still ongoing at the time of writing of this thesis, many attackers have used panic and collective anxiety to construct COVID-19 related scams (Microsoft, 2020b), which also implies that malicious attackers would be prepared to capitalise on world's tragedies and major events.

1.1.1 Dawn of the Hacking Era

Let us examine how it came to this state and where has it all begun.

Ever since personal computers have become commonplace it has become easier and far more space-efficient to keep track of various documentation. Compared to manually updating the records before and storing them away in thick and heavy binders now it was possible for all information to be fit into compact data carriers. When the problem of keeping records up to date was solved the next step has been

to centralise records.

In parallel with global digitalisation there has always been a group of curious individuals that wanted to push those systems to their limit. At first, that curiosity carried the nature of mischief, yet over time it has become more and more elaborate, turning into a fully-fledged illegal activity. The process described here is, of course, hacking. Originally, the word 'hacker' has been used to mean someone who wanted to know everything about how a computer system would work (often spreading beyond computers to other devices, such as radio and telephone) (Raymond, 2003).

If at the dawn of personal computers hacking was mostly done to test the capability of a system, presently the noun 'hacker' has sadly gained another meaning, the one analogous to the word 'cracker' - someone who attempts unauthorized access to a system, often with a malicious intent (Malkin & Parker, 2008). With this, accessing systems illegally has dramatically developed over the past 20 years and is now an entire industry directed at extracting valuable information.

Cyber attacks themselves have also evolved. At first, people would write small and benign code designed to prank the user (such as Elk Cloner (Levy & Crandall, 2020)) that would only affect local machines and devices. As more and more day-to-day operations have begun to be carried out online, the number of malicious cyber operations has also increased. With offensive actors continuing to adapt to the defences put out by the organisations the complexity of these attacks also continues to rise (Sophos, 2019).

1.1.2 State Attacks

In parallel with evolving cyber attacks that are executed by criminals and targeted at the general public there has been another vector in which malicious cyber operations developed - offensive cyber activity. Often covert, these operations allow countries to gather intelligence, target critical infrastructure or influence public opinion (Maurer, 2018). It has become very convenient for countries to engage in cyber activity, as the cost of operations is usually significantly lower than involving ground, marine or airforce (Maurer, 2018). Other reasons for engaging in this activity can include

"disrupting elections, spreading fake news, stealing sensitive data, sabotaging defence facilities" (Geenens, 2020) as well as stealing intellectual property.

The first mentions of nation-state actors and cyber espionage date as far as the end of the previous century (Maurer, 2018; Warner, 2012; Kindlund et al., 2014). Recent examples involve setting up spoofed news websites in Asia (Volexity, 2020), the SolarWinds attack (CIS, 2021), and targeting business network infrastructures (FireEye, 2020), all three done by different groups.

With cyber attacks being their full-time job nation-state actors have the time and resources to persist in networks for longer, as well as having a longer duration for their operations, making their detection progressively more difficult (Microsoft, 2020b). Another recent observation is that nation-state APT groups have started to pay more attention to public organisations, such as ones involved in public policy and geopolitics, Microsoft (2020b) reports that 90% of their nation-state notifications relate to non-critical infrastructure. This could indicate that even organisations that are not directly involved with the government would also be at risk from the nation-state actors. For example, IoT device attacks have become far more common, especially last year, as the organisations have been shifting to remote work (Trend Micro, 2021). Misconfigured IoT devices can be turned into bots for greater scale attacks, and nation-state actors have the capability to breach the security of IoT devices (Garner Jr, 2017). With services such as Shodan (2021), a search engine for IoT devices, one does not have to target a specific organisation, it is enough to merely find a vulnerable device. In 2020 alone there was a 35% increase in IoT attacks compared to 2019 (Microsoft, 2020b).

Although many organisations can become the victim of a nation-state attack due to being in the supply chain to the target organisation (Geenens, 2020), profit still remains to be the number one goal for breaching into the organisations (Nathan & Scobell, 2020).

1.1.3 The Advent of Cybercrime

With the Internet becoming widely available for the general public in the 1990s the laws around it were still unclear and required some time to be properly formalised (Sterling, 1998), especially in the UK (Walton, 2006). Before the Internet the UK had a system with similar functionality called Prestel, but due to it being very expensive to the general public it never took off quite as expected (Lean, 2016). Although it was not as popular, it did root itself firmly in history as the first ever 'hack' happened through Prestel. Two journalists have managed to illegally access Prince Philip's Prestel account, which has lead to the development of the Computer Misuse Act, UK's first computer hacking law (Leyden, 2015).

However in addition to breaching security there came to be another way to illegally profit from the emerging technology. Laws on email marketing were not as refined, and a lot of websites operated referral schemes, that allowed for the profit to be made from new visits via a clicked link (Rhysider, 2020; Cheek et al., 2001; Goodman, 2005). These schemes have lead to a group of people wanting to make a profit from referring other people to visit websites that had those referral schemes in place. In order to do this, this group of people (who later got known as spammers) has regularly scraped email addresses from chat clients and sent them unsolicited messages via these scraped addresses, so that they could profit from the clicks and sign-ups that came from the people clicking on the links in the unsolicited message. This is how spam was born. These spam campaigns have been very successful, generating spammers around $1,000 per week (Rhysider, 2020). When the laws about unsolicited email have become more regulated with the CAN SPAM act (Kigerl, 2016) spammers have found a way to legalise this activity (Rhysider, 2020).

Presently, phishing and social engineering attacks, born from that very same tactic are still widely in use (Sophos, 2019; Nathan and Scobell, 2020). Microsoft (2020b) reports "over 13 billion malicious and suspicious mails" some of which were set up to launch a phishing attack. The reason for these attacks surviving the test of time is that they are simple, require little expertise and they still have small chances

of success.

The online dark market has also been evolving. It has been described as a 'thriving marketplace' (Trend Micro, 2021), where a variety of malware, illegal databases and other services are being sold, giving adversaries easier access and the ability to find what they need. One of such services is APT as a crime, these are highly skilled and sophisticated groups without a state affiliation. These also continue to be increasingly popular. One recent non-state APT group is Deceptikons (Muncaster, 2020).

According to the latest Sophos (2019) report, public-facing services are getting targeted by automated attacks, that have become increasingly more sophisticated. This means that organisations need to pay attention to how their public-facing services are configured in order to avoid becoming a target of these automated attacks.

To conclude this section, cyber attacks are detrimental to an organisation, as they greatly undermine the trust that its clients have, leading to decreasing customer base. Also, if a company has any intellectual property, it might get stolen (Andrijcic & Horowitz, 2006). Moreover, if a company does not have a backup strategy, it might lose all of its data, in case it ever gets attacked by ransomware. A company might also have its data leaked as part of a cyber attack, exposing employees and clients to cyber criminals who would find ways to misuse this data. Furthermore, we have seen that any organisation is at risk from a cyber attack, as many attacks are automated and a small misconfiguration in any of the internet-facing services can result in an organisation being compromised. In addition to this, even if a company invests in cybersecurity awareness training - its employees can still become victims of phishing and social engineering as they are taking only minimal measures of protection (Zwilling et al., 2020). If a company has any way to influence the public opinion, and, of course, if it is working with the government - there is an increased risk of a nation state attack. Finally, an attacker does not need to be highly skilled to be able to operate advanced tools that do most of the work, thanks to the underground marketplaces offering a variety of services. All around, the risks of attacks are significant and a lot is at stake. If an organisation does little to protect

itself and does not invest in sufficient preventative measures, then it is only a matter of time before an attack will happen.

1.2 Methods of Improving the Defensive Posture

With malicious cyber activity being on the rise, companies are more willing to dedicate more resources to securing their information. In this section we will examine the options available to an organisation to improve and validate its security against cyber threats.

1.2.1 Establishing a defensive posture

The first step to understanding how to improve the cybersecurity of one organisation is to devise a plan that would cover all stages of a cyber intrusion attack. An organisation needs a way to keep the situation under control before, during and after an attack occurs. National Institute of Standards and Technology (NIST) (2018) framework provides guidance on how to approach it. The framework itself was designed to "foster risk and cybersecurity management communications" and is "based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk" (National Institute of Standards and Technology (NIST), 2018). The key benefit of this framework is that it can be integrated with existing cybersecurity practices that the organisation already has (NIST, 2016).

The framework itself identifies five functions that represent different levels of an attack. These five functions are: Identify, Protect, Detect, Respond and Recover.

The 'Identify' stage is involved in deducing what part of the organisation forms the attack surface. The 'Protect' stage is concerned with securing this potential attack surface. These two contribute to the passive aspect of defending the organisation. Next, the 'Detect' stage is concerned with methods and ways to recognise the fact that an attack is taking place in time. The 'Respond' stage deals with steps involved during and after a security incident. Lastly, the 'Recover' stage helps the organisation to work out what needs to be done for the organisation to restore

normal course of operation as soon as possible (NIST, 2018). Yu (2019) gives some examples over how this framework can be applied and even used with the Lockheed Martin Cyber Kill Chain (Hutchins et al., 2011).

1.2.2 Establishing a defensive posture in the SMEs and SMBs

Small-to-Medium-sized Enterprises/Businesses (SMEs/SMBs) often struggle to allocate enough time to ensuring their defensive posture is sufficient due to the resource shortage (Paulsen, 2016). Managers of such businesses often lack the necessary knowledge and awareness to sufficiently address the problem (Watad et al., 2018), sometimes falsely believing that they are not vulnerable to cybersecurity threats due to the size of their business (Barlette et al., 2017).

Because of this, SMEs/SMBs can be assisted in establishing a defensive posture. One way to assist them is by raising awareness of potential cyber security risks (Gundu, 2019). This can be done by hosting seminars or providing personal consultations to SMEs (Bada & Nurse, 2019). It is also important to note that advice alone is insufficient when addressing SMEs/SMBs to make them change their behaviour (Bada et al., 2019). Another way in which an SME/SMB can receive help and advice is by informing themselves with free online courses, such as the one from The National Archives/Cabinet Office (NA) (2017), as resources of an SME/SMB can be scarce. Being supported by government initiatives can also be helpful, as this way the gaps in defensive posture can be addressed systematically (Bada & Nurse, 2019).

Compared to SMEs/SMBs, larger organisations have an allocated cybersecurity department, as well as affording to set aside a larger budget for reinforcing their defensive posture, as well as having more systematic measures for educating their workforce.

Once an organisation has a way of managing its own defence practices it is time to analyse what defensive practices are available out there, as well as evaluate them.

1.2.3 Verification methods for defensive tactics

There are a number of measures that an organisation can put in place. Most of these methods rely on being constantly updated and monitored, otherwise the detection of an attack will not happen. Another example from this class of methods are intrusion detection, penetration testing or red teaming, these are methods that also focus on prevention. Some of the methods listed in this section are not constantly present in the system and are more related to the surrounding factors, such as case studies.

Compliance and Auditing

Regularly revising cybersecurity practices established in Section 1.2.1 and ensuring they are validated by an external body helps with keeping up to date on the latest cybersecurity practices.

Compliance checks ensure organisations have a rigorous set of cybersecurity enforcement procedures they can follow, and protect the internal assets of the company (Islam et al., 2018). Having a standard set of requirements helps to establish a set of criteria against which the safety of a company can be assessed. Regular compliance checks help a company to keep certain practices enforced and make sure it is prepared for any upcoming security incidents. Examples of these standards include PCI Security Standards Council (2021), ISO 27001 (ISO, 2021b), Def Stan 05-138 (GOV.UK, 2017).

However, following the latest standards and having regular checks does not on its own ensure complete protection against cyber threats (Veksler et al., 2018). For example, standards might not be all relevant if an organisation is at the cross-section of two fields - compliance practices might be different between industries and sometimes even contradictory (Magd & Curry, 2003). Often organisations use a combination of different frameworks (Dimensional Research, 2016), which further increases the difficulty. All of the different systems require management, constant updates and a regular examination on how to better integrate them together. Secondly, cyber attacks also evolve quickly, therefore standards need to be changed and updated open to accommodate these changes. A situation may arise that although a company has

certain defensive measures in place they can be out of date or misconfigured, or the attack can be specifically crafted to bypass them. Hence compliance and auditing should be used as part of a more reinforced cybersecurity posture.

Automated technical solutions

Existing tech solutions on the market include those dedicated to systematic detection of cyber attacks, such as anti-virus systems or intrusion detection systems. However, installing these without having an idea what an attacker might be after in a system will not maximise the value from the use of these systems, as without correct filter configuration these systems will only catch out the most basic attacks, as off-the-shelf these programs come with default settings . More sophisticated attackers can craft solutions that are bespoke to the target (Stuttard & Pinto, 2011, p. 33), which makes signature-based techniques poor. Additionally, these systems rely heavily on being monitored and analysed. If they are configured without being monitored or managed - they will bring very little use to control and contain a security incident (A. Jones & Colwill, 2008).

Case studies

Among the qualitative methods in cybersecurity, case studies are the second most popular method of research (Fujs et al., 2019). Case studies are used to understand a specific process while using a specific organisation or process as an example, such as in the works of Zainudin and Molok (2018) and Colicchia et al. (2019).

One way to understand what an attacker might need from a particular company or a network is to look at similar cases in the past that have taken place with different organisations. Analysing these past cases will help the organisation with understanding cause and effect between various incidents and the attacks that they lead to.

Having said that, each such case is different. For example, an attack on a government organisation will be different from an attack on a power station. Even if the two organisations - the company that wants to increase its defensive posture and the company in a case study are similar, they might operate at radically different scales.

One of them could be large-scale, whilst the other one is just a small business. Such differences would indicate that the budget these companies can spend on improving their cyber defensive posture would also be very different. Their differences would not end there - networks can have different structures, internal management chain can be different, that would indicate that internal reporting would also be different and there are more similar factors that indicate that despite the field, no two companies are the same.

It would be highly undesired for a company to just wait until they get attacked so that they can gather the logs and the attack data to analyse what can be improved. Of course, this is not to say that past attacks, if the organisation was unfortunate enough, should not be analysed. Quite the opposite - every such occasion must be analysed to prevent it from happening again. But waiting for a cyber attack as *the only* opportunity to improve defensive posture is a flawed approach.

Penetration testing

Alternatively, to better understand what specific places does a company need to focus on is to conduct a penetration test. A penetration test considered to be the *"primary method used to ensure that vlunerrabilities... are known about and can be addressed before they are exploited in a real attack"* (Tang, 2014, p. 8), providing a *"cost-effective and assured assessment tool to analyse the status of current security posture of an organisation"* (S. Shah & Mehtre, 2014, p. 48). A penetration test outlines the evidence of any weaknesses that could potentially be exploited by malicious cyber attackers. The test also provides the potential impact caused to the company. A reason why a company would want to use a penetration test over a vulnerability assessment is to identify the vulnerabilities that are bespoke to the system, or not known by famous vulnerability scanning tools (Tang, 2014, p. 9). Even if the regular penetration tests are mandatory, they should always be approached fundamentally, as this will help prevent monetary losses in the long run. Yeo (2013, p. 20) defines the ultimate goal of the penetration tester as identifying *"gaps in security posture"* and using *"exploits to get in to the target network and gain access to sensitive data"*. For a test to be successful, it is vital to correctly define a scope. Gaining access is

not always straightforward, so a sequence of steps is followed to achieve the desired goal, often chaining weaknesses together (Yeo, 2013, p. 20).

From the legal perspective, under the Computer Misuse Act 1990, a penetration test is acceptable, provided a permission has been obtained from the target company (Dautlich, 2004, p. 41), when the minimum number of employees know about a penetration test, an authorisation from the target client is needed. However, if the company has any third-party services, a client must clarify if they, or the penetration tester have the right to carry out penetration tests on the service providers' equipment (Dautlich, 2004, p. 42), and the penetration testers should perform the due diligence to know which systems are owned by the client, and which ones are owned by a third-party. Under the Data Protection Act 1998, the penetration testers need to know whether there would be any access to the personal data involved, and to have clear definitions of who is the data controller, and who is the data processor (ibid.).

Vulnerability Assessment and Penetration Testing (VAPT) is *"proactive in nature"* (S. Shah & Mehtre, 2014, p. 48), which means that the organisations can determine where and when they want the test to occur to be able to take the required mitigations before the real attack takes place.

Attempts have been made to use the potential of the Artificial Intelligence (AI) in the field of penetration testing. At the moment, scalability remains an issue, which has a potential of being addressed in future research (McKinnel et al., 2019, p. 187). Another finding was when general exploits have been applied, only surface-level vulnerabilities are detected (ibid).

Simulations

Another way for a company to assess and review defensive practices is to walk through most likely and unlikely scenarios with the use of a simulation. There are multiple ways in which this can be done, and it can help to understand cyber attackers, defenders or users (Veksler et al., 2018). Simulations can also help derive aggregate trends, which in normal, simulation-free circumstances would have involved a long time to gather, analyse and investigate.

There are multiple approaches to simulations. The primary focus of the simulation can be either on the interactions between the people who are using the system (or attacking it), or the events that are occurring. Doing such simulations is a lot more cost-effective than creating a hardware network replica (Veksler et al., 2018).

However, both types of simulations have their shortfalls. Human reasoning is very inconsistent and therefore there will be inaccuracies when using very consistent behavioural models (Veksler et al., 2018). One way this factor can be accounted for is to ensure that multiple characteristics are taken into account when gathering data. This will help to build a surface-level image of a participant, as well as how likely is that participant to be consistent or inconsistent.

Network and process simulations also need to account for various factors. For example, if the model in question involves Wi-Fi connection, factors such as radio signal strength need to be accounted for and it is difficult to factor in with existing network simulations (Veksler et al., 2018). If a network is to be modelled, then the simulation outputs in regards to data travel speeds should only be considered as estimations as opposed to being absolute truths.

If a simulation is made, it is always designed with attacks that are already known in mind. If there is a new type of attack that suddenly becomes popular, a simulation will not account for this. This in turn implies that simulations are bounded in creativity - they can only model the attacks that are known to the simulation makers in the attack patterns and routes that have been accounted for by the simulation designers. Another aspect is the limitation in parameters. A simulation usually requires a set of parameters to function, and the decision is often left to the simulation designer as to which parameters need to be considered. The inclusion of additional parameters also increases the overall complexity of the model. To ensure that the simulation conforms to the needs of the organisation it is important to work closely with the stakeholders and facilitate communication to extract the most important features that are to be simulated.

Finally, having a good information source in order to create models and simulations is paramount, regardless of the type of simulation made. The accuracy and overall usefulness of a model will depend on the information supplied, hence this

information needs to be gathered reliably and updated frequently. In the field of cybersecurity one of the possible ways information can be gathered for the simulation of malicious cyber activity is by collecting data from penetration testers and red teamers. This allows combining the human aspect of specially-trained individuals impersonating attackers with the convenience and cost-effectiveness of a simulation.

1.3 Aims and Objectives

Let us focus specifically on the incorporation of the human decision elements into a simulation. We have already established that simulations rely on accurate and up-to-date information provided. Extracting decisions from a group of individuals with some interest in cybersecurity could become such an information source. Presenting participants with a fictional scenario that is specifically crafted to explore relevant bits of the system that is being tested and relevant situations can serve as a framework for this data collection. A fictional scenario needs structure to ensure the entire attack surface of an organisation is covered, and elements of the game mechanics can serve as a scaffolding for information collection and decision extraction. This will be covered in more detail in later sections.

1.3.1 Aim

This research project aims to provide an answer to the following question:

Can specifically tailored games (also known as 'serious games') be used for informing computer simulations?

For this we need to break the project down into several parts in order to be able to generate research objectives.

There are three essential components in order to answer this research question. The first component is designing a game with a specific purpose in mind, and that purpose is to generate a set of decisions that players make as they play the game. The second is to come up with a way to effectively extract these decisions. The final part is the creation of a simulation that is using these decisions.

1.3.2 Objectives

Since the research question has been defined, the next step is to break it down into a set of steps that can be taken in order to answer the research question. For convenience, they have been split in accordance with the core elements of the project.

The first set of objectives relates to the game development. The key idea is to balance the 'fun' element of game mechanics with obtaining the desired results. Therefore, attention must be paid from the early game development stage to correctly balance the game, and to plan the number of features that constitute it. The objectives are:

1. *To build a realistic game based on rigorous evidence*
2. *To ensure that the game enables players to make decisions that reflect their true intention*

The second set of objectives ensures the decisions from the game are translatable to the simulation and that the semantics are preserved as much as possible.

3. *To devise an efficient approach to the recording of the game decisions*
4. *To ensure the events within a game can be restored from the recording, with semantics preserved*

The final objective ensures the created simulation is able to accommodate the game to simulation translation.

5. *To ingest the game decisions into a simulation.*

Thesis structure

The thesis will continue with Chapter 2 will provide a thorough review of relevant literature and Chapter 3 will explain the methodology employed in this research project. In Chapter 4 the game will be discussed in greater detail, while Chapter 5 will explore the simulation. Chapter 6 will present the results that have been obtained throughout the project and Chapter 7 will discuss them. Finally, Chapter 8 will contain concluding remarks, as well as the contributions.

Chapter 2

Literature Review

> Truth is often a multiplicity of perspectives, and sometimes the more viewpoints and versions of events there are, the closer the reader gets to an overarching truth.
>
> Susan Barker

This chapter will examine current advancements in the field. The chapter will begin by studying how current industry practices validate their defensive posture. This will be followed by considering how malicious cyber attackers are currently modelled, followed by general simulation approaches. A more detailed outlook at penetration testing will be next. The last section will focus on high-engagement data gathering approaches such as role-playing and serious games.

2.1 Methods of validation

Let us now examine other methods that help companies validate if their strategy to defend the organisation is effective and what other measures can a company take to ensure it is consistent with the best industry practices.

2.1.1 Standards

There exist a number of security standards, such as ISO 28000 (ISO, 2007) or ISO 31000 (ISO, 2018) that organisations need to comply with to ensure that risks are correctly managed and that the products that the organisation provides or services that it handles are up to the correct quality standard. Yet, data security has been poorly covered by these standards to this date (Verdugo & Rodrìguez, 2019). Additionally, accessing these standards are not free (ISO, 2021a), hence to comply with them there is an initial cost.

One of the purposes of such standards is to ensure that risks are accounted for in a systematic process Palmer et al. (2001) states that it is important to perform a risk assessment to balance business assets being exposed with costs associated with securing said valuable information. This relationship is illustrated in Figure 2.1.

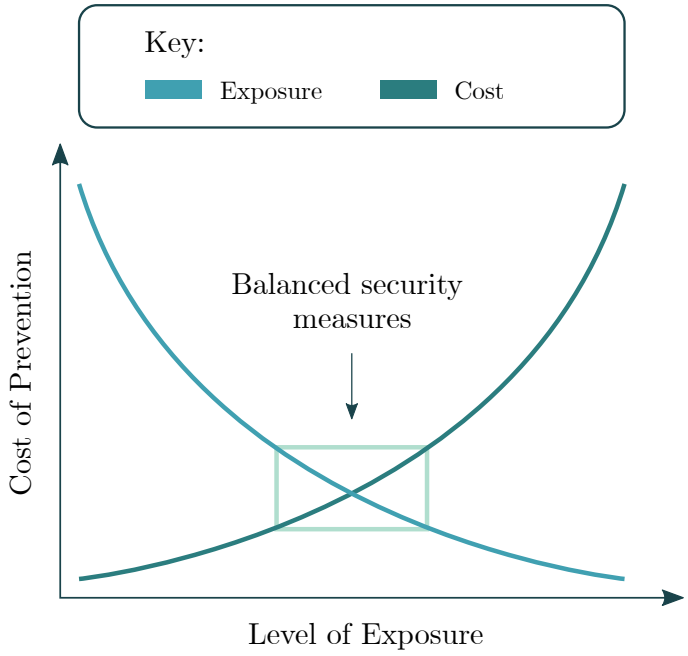


Figure 2.1: Balancing Cost of Risk Prevention Versus Exposure (Palmer et al., 2001)

In addition to risk management, the paper further proposes to adopt a hierarchical policy structure, with procedures being linked to parent standards. These standards in turn link to the policy with which they are associated, allowing procedures to be traced all the way back to the business objectives (Palmer et al., 2001).

An illustration of this can be seen in Figure 2.2.

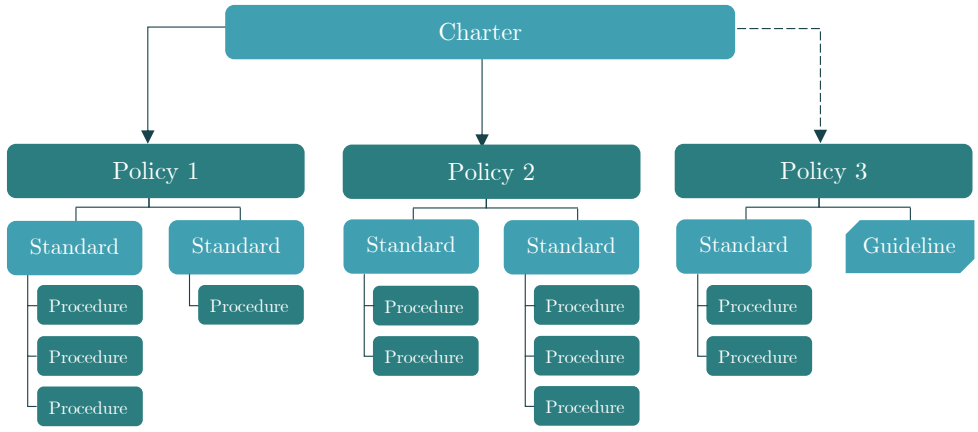


Figure 2.2: A modified diagram, reproduced from Palmer et al. (2001). A Traceable, Hierarchical Set of Policy Guidance Documents. In this example Policy 3 is still being developed. Guidelines are there to provide recommendations as a new standard is being developed.

The next stages are defining guidelines, Palmer et al. (2001) define a guideline as *"a standard in waiting"*. This stage is followed by addressing threats and vulnerabilities at a policy level. The final concept introduced is the application of existing policies to new Information Technology and Information Security topics. According to the authors, adopting these steps ensures that traceability to risk management and business objectives is preserved, and the organisation can have a measure of completeness at the policy and standard level (Palmer et al., 2001), which permits the organisation to easily validate and review their practices.

2.1.2 Compliance

Standards not only need to be set, but they also need to be enforced. In some sectors, regulating bodies have a way to punish companies for non-compliance in the best case providing recommendations, and in the worst case — withdrawing the business license (Duncan & Whittington, 2014).

Beautement et al. (2008) identify two reasons for employee non-compliance. The first reason is that the employees see the security procedures as an additional barrier to their day-to-day tasks. The second reason is that they do not see how what

they do helps the organisation. Firstly, to ensure the employees do not see security procedures as an additional barrier, it is important to ensure that it is easy for the employees to follow these practices, set it up in a way that does not take away significant time from their day-to-day tasks. For example, instead of using a password substituting it with a graphical password (Stobert & Biddle, 2013), however these are prone to shoulder surfing. Other methods include using a fingerprint reader (Jakobsson et al., 2012) as an easier and a more secure alternative, however there is a risk that a fingerprint may be cloned (Paul & Irvine, 2016). YubiKeys (yubico, 2021) are another emerging method, they allow to authenticate by plugging in a USB pen drive, or to use it as a form of Multi-Factor Authentication (MFA). Their cost and compatibility (some are USB-c and some are regular USB) can be a limiting factor to their popularity.

Alternative authentication methods allow the employees to change passwords less frequently and there is no need to write them down, helping to achieve a sufficient level of security and allowing the employees to carry on with their day-to-day duties. Returning to the subject of MFA, there has been a rise of more than one stages of authentication, as an alternative solution to password fatigue. With the average user accessing about 20 accounts per day (Y. Shah et al., 2015) this comes as no surprise. However, this approach still need to be refined in the underlying implementation as it is vulnerable to some attacks, such as Man-in-the-Mobile (Sinigaglia et al., 2020).

A full discussion of behavioural non-compliance is beyond the scope of this literature review, however Herath and Rao (2009) in their work point out that there are three categories of effects that can impact behaviour of the employees. The effect can be positive, negative and significantly amplified in either direction. The types of factors that have a positive effect on the employee compliance are perceptions about the severity of the situation, the individual impact of their actions (response efficacy) and how comfortable they are in following instructions (self-efficacy). The negative effects are introduced by the response cost. The factors that can significantly affect the employee compliance are social influence and resource availability.

Secondly, for the employees to understand the role of compliance and the effect it has on the organisation, compliance and company values need to be enforced on the

level of the company culture (von Solms & von Solms, 2004), although this can often be difficult as the senior management often does not communicate these intentions in an effective way (Ashenden & Sasse, 2013). Beautement et al. (2008) acknowledge that the problem of compliance lies not only on the employees themselves but also on the senior management. This study outlines that the issue of non-compliance also arises from the miscommunication of the employees and the senior management.

So, does this mean that if an organisation diligently follows standards, and employees understand well their role in the organisation and comply with these standards, regularly passing all the necessary checks that an organisation is completely secure? Not necessarily. For example, if an organisation hires contractors and temporary workers, their understanding of compliance procedures and their loyalty to the organisation will not be the same as one of the full-time regular employees (Sharma & Warkentin, 2019). It is also possible even for the most loyal employee to become a victim of a well-planned spear phishing or phishing or a supply chain attack even if they meant no malice (Greitzer et al., 2014b). It is also important to not forget external attacks. The cybersecurity landscape is ever-changing, standards take some time to get approved and updated, furthermore the company may be using some third-party tools that themselves have unpatched vulnerabilities - zero-day attacks still occur even on the most well-maintained products (NIST, 2019; Microsoft, 2020a; NIST, 2020).

2.1.3 Risk-based approach

Previously, information security has been viewed as a purely technical concept and lacked the attention of the top management (Posthumus & von Solms, 2004). Today, this is no longer the case, as 80% of directors, trustees and other senior managers see cybersecurity as a high priority (GOV.UK, 2020). To ensure the cybersecurity budget of the company is rationally distributed, it is worth assessing what information is the most valuable in the company, as well as what the external threats are.

The idea of a risk-based approach is to address the most vulnerable parts of the

system first (Griffiths, 2016, p. 5). This allows a company to focus on the areas that need the most attention first, and then to address areas of lesser risk. While this may seem like a company will improve its security in the shortest possible timespan this is not necessarily true, as the priority is on minimising risk, which may take different amounts of time depending on the area of the business that is currently being addressed. For example some changes need to be integrated on the level of company culture and would require senior management influence it (Cuganesan et al., 2017).

To better understand what would constitute an organisational risk, it is essential to get a proper definition of risk. In his book, Griffiths (2016, p. 17) lists two definitions of risk, the first one by the Economist Intelligence Unit, that defines it as follows:

> *The threat that an action or event will adversely affect an organisation's ability to achieve its objectives and execute its strategies successfully.*

He also argues, that it is important to note that risk might not always have negative connotations, and lists the alternative definition by the Australia and New Zealand risk standard:

> *The chance of something happening that will have an effect on business objectives.*

These two definitions adopt different perspectives, we can relate one of them to a more risk-averse mindset, and another to risk-embracing one. Furthermore, Kimball (1993) defines the types of risks to be ***loss-aggravating*** or ***loss-ameliorating***, the former can worsen with a small monetary loss, while the latter can improve with a small monetary loss. If we apply these concepts to the field of information security, paying a ransom in ransomware would be an example of a loss-aggravating risk, while paying a subscription fee to the intrusion detection service, or paying for the audit would be an example of a loss-ameliorating risk, as the risk of a cyber intrusion (greater potential monetary losses) is now mitigated with an active protection system.

In addition to all of the above, a risk-based approach needs to operate in tandem with the existing Governance, Risk and Compliance (GRC) procedures of an organisation. Al-ahmad and Mohammad (2013) claim that they *"should always be viewed as a continuum of interrelated functions"*, suggesting a more holistic approach to the organisational defensive posture.

2.2 Modelling approaches

So far, we have examined only one side of the validation approaches — documentation and compliance, the risk-based approach and management. All of these approaches require substantial changes in the organisation to follow standards or to protect valuable assets. However, what if, before making substantial changes, we would want to see what needs to be prioritised, or what would be the worst-case scenario before committing to a specific risk-management strategy? This is where models and simulations are very helpful, as they allow seeing potential consequences of cyber attacks before committing to a specific defensive solution.

In cybersecurity there are numerous approaches that are aimed at modelling cyber attacks. It is possible to model cyber intrusions in terms of network graphs, profiling attackers or building behavioural models.

Before understanding the behavioural patterns of an attacker there have been some previous attempts to understand different kinds of attackers and what their motivation might be when they are targeting a system.

2.2.1 Profiling attackers

In the past, there has been work that strives to build a taxonomy-agnostic collection of identifiers, such as biographic information or usernames for various online accounts and the likelihood of them belonging to the same individual (Hodges et al., 2012). Apart from curating sets of data, there have also been various historical cases (such as the ones outlined in Zhang et al. (2011)) that had lead to certain types of attacks forming. Bolgan (2018, p. 12) performs an extensive analysis on the kinds

of individual differences, skills and aptitudes and motivations that are shared by different attackers.

Different taxonomies outline different types of external adversaries, therefore authors have taken a liberty to group similar types of motivations into a single entry.

Before listing all the external archetypes it is important to make a short intermezzo to cover internal threats. Insider threat is an example of an internal threat, it is defined 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"* (Cappelli et al., 2012). It is also important to note, that sometimes organisations fall prey to the unintentional insiders, who wish them no harm, but whose actions can end up being an important component of an external attack succeeding, such as unknowingly clicking on a phishing email link (Greitzer et al., 2014a). Insider threats are outside the scope of this research, yet there is no reason that the methodology listed in this thesis cannot be applied to insider threats.

The first group of external attackers is the most inexperienced one, representatives of this group are characterised by the name ***script kiddies***. These individuals are described as *"generally 14-16 years old and still at school"*, *"usually male"* and *"prefer to spend their free time working on computers"* (Barber, 2001). Having said that, they are described as having *"little knowledge of the mechanics of the Internet, such as routing and switching"* and would just use ready-made powerful tools with enough success to cause damage (Barber, 2001). Meyers et al. (2009) believes that the term 'script kiddie' is synonymous to novice, and describes them as *"often young and eager for acceptance from the hacker subculture"* but having a low overall *"maliciousness level"* as they do not know enough and are not skilled enough yet.

For the next archetype we have chosen the name ***counter-culture***. This type denotes skilled individuals that do *not* have financial or ideological motivation (Sidorenko et al., 2020). Following the weighted arc circumplex model of Seebruck (2015), these attackers would be motivated by recreation or prestige, such as

Jonathan James (Emma, 2017). It is also important to note that curiosity is also a valid motivation for this group, such as in BBC (2008), where the main objective was to find the evidence for the existence of aliens or free energy sources. Counter-culture attackers are more skilled than script kiddies, being very comfortable with various hacking techniques, but unlike white hats (bug bounty hunters, red teamers or penetration testers, see Sen et al. (2020) or Caldwell (2011)) their methods may sometimes be questionable.

The next cyber adversary category that can be slightly more impactful than the counter-culture group is ***hacktivists***. Seebruck (2015) describe them as being motivated by an ideology, which can be politics, religion or chauvinism. Barber (2001) describes their purpose to make an ecological, political or ethical cause or to simply *"cause damage"*. An example of a hacktivist group would be the Anonymous (Gabriella Coleman, 2014), or an organisation deriving from it - LulzSec (Schurman, 2012), many members of which were in disagreement with the Anonymous, hence left to form their own group.

Perhaps, one of the most common categories is the one of ***cyber mercenaries***. The key motivation for that group is profit. This goal can manifest itself in many ways, starting from selling crimeware (*"software that performs illegal actions unanticipated by a user running the software; these actions are intended to yield financial benefits to the distributor of the software"* (Jakobsson & Ramzan, 2008)) and finishing with offering APT-like services for hire (Constantin, 2020). Underground marketplaces offer a variety of services and tools that will suit any purpose or budget (Trend Micro, 2021).

Finally, the most sophisticated and impactful category of them is the ***state-backed*** group. Typically individuals or groups that belong to this category are hostile nation-state-affiliated and perform intelligence or military activities on their target (Sidorenko et al., 2020). The nature of the activities carried out is a *"part of a geographic strategic goal"* and vary in complexity and scale of operations, be it gathering intelligence/surveillance (Kaspersky, 2015), attack on critical infrastructure (Sky News, 2018), watering hole attacks on major news websites (Volexity, 2020) or financial operations (INTSIGHTS, 2017).

All types of external attackers listed above are summarised in table 2.1.

Title	Skill level	Motivation	Threat level
Script Kiddie	Low	Get accepted by the community	Low
Counter-culture	High	Not finance or ideology	Moderate
Hacktivist	High	Ideology	High
Cyber mercenary	High	Finance	High
State-backed	High	Intelligence, sabotage	High

Table 2.1: A synthesis of cyber adversary types, their relative skill levels and high-level motivation overview.

2.2.2 Behavioural models

As is evident from the previous section, there exists a multitude of attackers with different motivations. This section will examine what methods would be the most optimal should we want to model the behaviours of the attackers mentioned in the previous section. There exist numerous theories, each of which can be used as a protocol for adversarial behaviour modelling.

The *Beliefs-Desires-Intent (BDI) model* has been first introduced by Bratman (1999). The BDI model shows the process of thoughts turning into actions. One of the key concepts is the one of *pro-attitudes*, which are states that determine the actions of an individual. Intentions and desires are examples of pro-attitudes. Bratman also defines boundaries, an example of such would be defining at what point does a desire become the intention. When translated to a computational model, it allows an agent to reason about an action before committing to it. This is possible due to the agent having informational, motivational and deliberative states (Rao & Georgeff, 1995).

Schmidt (2002) argues that in order to model sophisticated social systems just belief, desire and intent would not be enough and proposes an alternative model - ***P****hysical conditions,* ***E****motional state,* ***C****ognitive Capabilities and Social* ***S****tatus (PECS)*. It is intended to be a replacement for the BDI model and introduces more dimensions to behavioural modelling.

Despite being quite dated, these behavioural models have been widely applied

to the existing agent-based models. They provide a framework for how an agent should behave, which can be beneficial in terms of structuring agent mechanics on a temporal scale, i.e. what is the logic behind a particular agent's action, as well as the reason why was this logic employed in making this decision.

When it comes to the domain of cybersecurity and previous efforts to model adversarial behaviour, a notable example is the *SKRAM model* (Parker & Parker, 1998). According to the SKRAM model, to perform a malicious cyber attack, an adversary would consider the following factors:

Skills The competency of the attacker to execute the intrusion

Knowledge Attacker's familiarity with the tools and the target network

Resources Whether an attacker has access to time, financial resources, hardware and/or software facilities and similar factors

Authority This parameter acknowledges whether the attacker has access to facilities or information systems (Maimon et al., 2017)

Motivations The underlying reasons for the attack

The SKRAM model has been developed when cybersecurity was a young field, thus studies were only beginning to explore factors behind the motivations that drove cyber adversaries to commit malicious cyber activities. It provides only a few aspects of the knowledge and reasoning of an adversary, hence there is a risk of oversimplification. Maimon et al. (2017) propose a revision to the SKRAM model. They argue that those five factors are not sufficient to describe motivations and that the following additional two factors need to be considered: attacker's demographic and goals, turning the acronym into *DSK-RAMG* (Demographic, Skills, Knowledge, Resources, Authority, Motivations and Goals):

Demographic This accounts for the background of the attacker — their gender, race, social status, intellect, religion, personality and age

Situational motivation and Goals More on the concept below

The concept of *Situational motivation* is described by Cornish and Clarke (2003). In their paper, five generic situations are described relating to when a criminal may see an opportunity to commit a crime. The first situation is when malicious actors need to apply a low amount of effort for initiating crime, such as the absence of a password on a computer. The second situation is when the risk of punishment is low, such as when an individual is alone in the room and there are no security cameras around. The third situation is when the potential reward is very appealing to the criminal, such as the newest specification computer when they are trying to break into an electronics shop. The fourth situation is when an individual is affected by an emotional factor, for example after a dispute. The final situation is when an individual can justify themselves committing the crime, such as throwing rubbish on the floor when there are no bins around in a public place. Those situations can be applied in the domain of cybercrime. If a website is poorly secured, an adversary may justify their intrusion by using poor website security as an excuse.

2.2.3 Cognitive architectures

The definition of cognitive science is "the study of thought, learning, and mental organization, which draws on aspects of psychology, linguistics, philosophy, and computer modelling" (Lieto, 2021). One of the core missions of cognitive architectures is to "enable the realisation of artificial systems able to exhibit intelligent behaviour in a general setting through a detailed analogy with the constitutive and developmental functioning and mechanisms underlying human condition" (Lieto et al., 2018). This field has yielded several cognitive architectures, the most famous ones being ACT-R (Anderson & Lebiere, 1998) and SOAR (Laird & Newell, 1983).

ACT-R is a behavioural modelling framework that has multiple revisions, publications for which are available at Carnegie Mellon University (2013b). One of the important distinguishing factors of ACT-R is that it permits researchers to collect quantitative measures that can be compared with similar measures obtained from human participants (Carnegie Mellon University, 2013a).

SOAR Stands for State, Operator and Result (Laird & Newell, 1983), and has

initially been developed for AI systems. The goal of SOAR is "support all the capabilities required of a general intelligent agent" (SOAR, 2021). The framework was based on the work of (Newell, 1990), who has defined the Problem Space Hypothesis. This hypothesis states that all goal-oriented behaviour can be described as a set of states (or a problem space). Its focus is more on the field of AI, while ACT-R focuses more on cognitive modelling. Unlike ACT-R, SOAR makes it possible for multiple rules to fire at once, while ACT-R 6.0 has a "cognitive bottleneck" that only allows one production rule instantiation to match at a time, even if multiple rules are matched (R. M. Jones et al., 2007).

Another well-developed cognitive model is the PSI model (Dörner, 1999), which gets its name from the Greek letter ψ, which has also traditionally been used to represent psychology (Dörner & Güss, 2013). The PSI model covers 14 of 22 major areas of cognitive functioning defined by DARPA (2005) (Bach, 2009). These areas include memory, learning, sociality and emotion, logic and reasoning and others (Bach, 2009). It is more advanced than ACT-R and SOAR, as both of these models do not incorporate motivation (Dörner & Güss, 2013). Its four core processes are motivation, perception, cognition and action (Dörner, 1999).

Other notable frameworks include CLARION (Sun, 2006), LIDA (Franklin et al., 2014) and Sigma (Rosenbloom et al., 2016).

Cognitive architectures could represent the reasoning process of a cyber adversary, which requires the knowledge of the obstacles an attacker will encounter to be able to account for them in the rulesets. A big amount of rule sets can significantly increase the complexity of the model, which can lead to an increased computational requirement.

2.2.4 Simulations

We have explored the transition of human reasoning and decision-making process to a computerised approach and examined current methods. This section discusses more generic simulation approaches that allow modelling processes and interactions, and to create a simulation it is necessary to explore how external stimuli affect the

subject that is being modelled.

Discrete event simulation

In Discrete Event Systems (DES) simulation method state changes are recorded at concrete points in time (Nance, 1996). The useful analogy to have in mind is the one of a calendar. There may be days when there are multiple events occurring, while there may also be days when no events are occurring. DES focuses only on the days with 'events' Campbell (2018). In other words, the simulation transitions between states upon an occurrence of an event (Fujimoto, 1990). The first DES programming language, GSP (General Simulation Program), has been credited to K.D. Tocher and D.G. Owen in 1960s, followed by Gordon simulator 1960 by Geoffrey Gordon, later renamed as GPSS (General Purpose System Simulator) (Nance, 1996).

DES has not been chosen for this project due to its focus on the environment and events that happen in that environment, which would be an optimal approach if the requirement was to model the attack from a defensive point of view, as the key information that is visible throughout the course of the attack are the changes to the target system — a login attempt, accessed files and similar. These little 'islands' of information are discrete. However, if we want to model the attack from an attacker's point of view, we need to focus on an attacker's actions and decision-making processes, and DES cannot provide a rich description of this.

System Dynamics

System dynamics uses differential equations to monitor variables being observed over time (Parunak et al., 1998), unlike discrete event simulation, which focuses on distinct points in time. The availability of specialist software does not require mathematical training in order to create those simulations (Sterman, 2001).

The core notion in System Dynamics is the presence of feedback loops, which can be of two types. Positive loops reinforce or amplify the events in the system, such as a product generating good reviews, which causes more people to buy it to generate even more good reviews. Negative loops are the balancing loops — they counteract the change. If a city is attractive — more people will move in to live

there, which will cause the rise in population density (that will raise house prices) and a shortage of jobs in that area, which will eventually make this city average again (Sterman, 2001). Those feedback loops govern the simulation.

Compared to DES, System Dynamics provides a continuous view of the attack process. At first glance, it would have made this method more suitable than the previously mentioned discrete-event simulation. Having said that, system dynamics is better suited to representing aggregate patterns — if our simulation had represented a theoretical network, system dynamics would have provided a good overview of what parts of the network are overloaded the most during the attack and how does that change throughout the course of an attack. Alternatively, we could model how the priorities of an attacker change throughout the course of an attack, but that would have required to define discrete goals, perhaps mapped to a kill chain and observe how the priorities shift between the stages. However, this would have required producing differential equations that model the transition of priorities of an attacker. Due to its limitations of having clear focus points as attacker priorities, it does not provide enough flexibility to model an attacker's decision-making process to the required level.

Monte Carlo

This approach has been named after a casino in Monaco, as the Monte Carlo solution involves the element of randomness (Nance, 1996). The Monte Carlo approach can be summarised as follows: if there exists a difficult problem, a solution to it can be approximated by using random values (Morgenthaler, 1961). In certain cases, this ends up being a faster approach as opposed to a traditional solution method.

The primary drawbacks of Monte Carlo simulations are significant computational time and excessive memory demand (Martin, 2012), which prevent it from becoming the most popular and ubiquitous approach to solving various problems that involve simulations. Solutions combining Monte Carlo with other methods (Bugert, 2019; Lumbroso and Davison, 2018) use Monte Carlo for part of the problem, such as sampling (Figueira & Almada-Lobo, 2014) as opposed to implementing the solution entirely using Monte Carlo, which helps with offsetting performance costs.

Some of the applications of the Monte Carlo simulation method in the field of cybersecurity include simulating a variety of cybersecurity incidents to create a framework for analysing these incidents (Gai et al., 2016), simulating the impact of cyber attacks on microgrid systems (Liu et al., 2017), and creating a model for cybersecurity resource allocation using Monte Carlo approach to minimise disparities caused by uncertainties (Fagade et al., 2017).

Agent-based modelling

Unlike DES, which focuses on the events, agent-based modelling (ABM) is constructing a model is in terms of the agents. An agent is a person or an object encoded within a model that has properties and behaviours (Wilensky & Rand, 2015a). In this context, behaviours are defined as sets of actions that an agent performs based on the current knowledge of its environment (Crooks & Heppenstall, 2011). Behaviours of agents can be encoded using simple rules (Wilensky & Rand, 2015a), unlike the system dynamics approach that does not have an explicit representation of behaviours (Parunak et al., 1998). There is a common misconception that ABM is used for predicting events or behaviours of the subject groups that are being modelled (Epstein, 2012, p. 38), instead, this modelling approach is used to explore emergent trends and to understand the issue (Helbing, 2012).

Having said that, Agent-based models can be very challenging to validate (Levy et al., 2016). This happens due to a number of reasons. Firstly, the nature of complex systems implies that they are designed to be unpredictable (Batty & Torrens, 2005), which implies that it is very difficult to anticipate all of the expected outputs. Secondly, as agent-based models behave very differently in different conditions, they tend to heavily rely on initial conditions (Crooks & Heppenstall, 2011, p. 99), which means that a small change can result in a drastically different output.

So, how are ABMs validated? One such method of validation is described by Ngo and See (2011), illustrated in Figure 2.3. Another approach to validation is to have models mimic existing models as closely as possible so that a pre-existing method of validation can be applied (Levy et al., 2016).

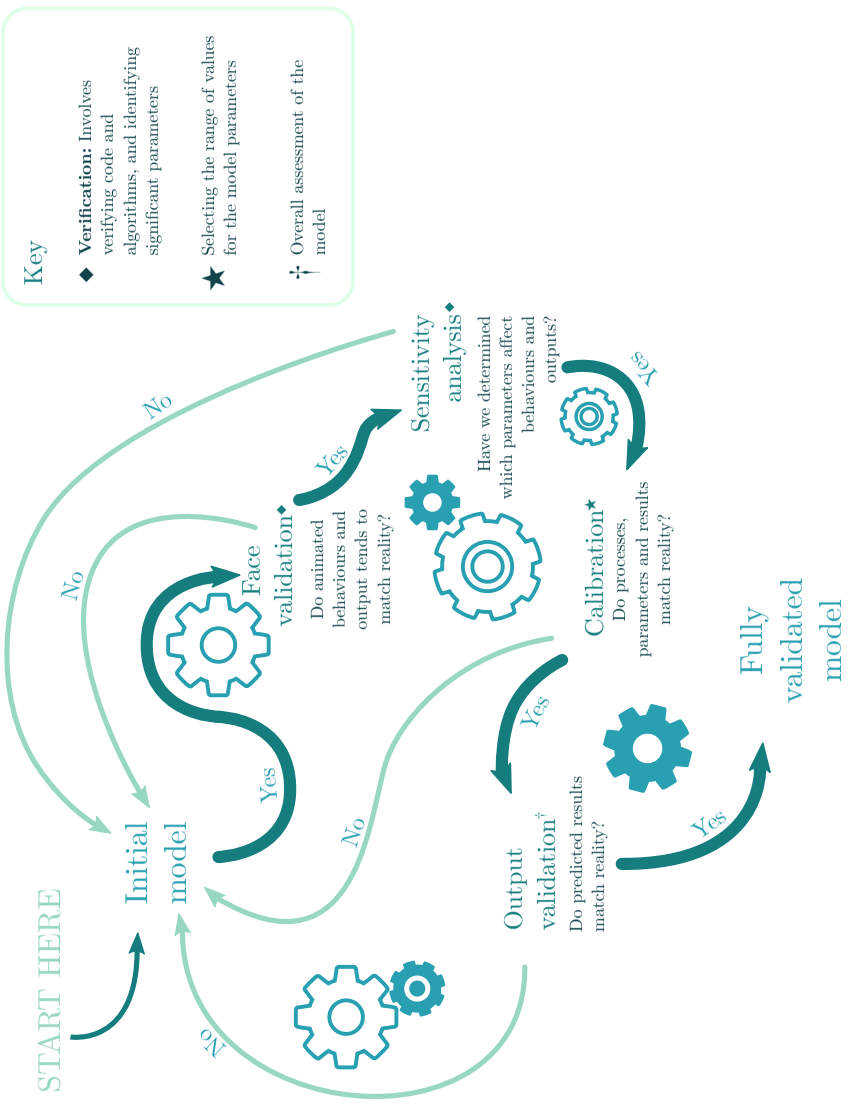


Figure 2.3: Agent-based model validation process as described by Ngo and See (2011).

ABM can be combined with other methods, such as Monte Carlo simulations. Lumbroso and Davison (2018) use a hybrid approach to simulate floods in residential areas. The model has a few possible types of agents: people, buildings, vehicles and similar. People-agents have three possible states: unaware, aware-stationary and aware-evacuating. During the evacuation, the height and weight of a person play a crucial role, as those characteristics affect their probability to be injured in the flood. A Monte Carlo approach was used to estimate the critical depths and velocities at which an individual has a potential for injury or drowning. This was done due to there not being enough studies on the topic (Lumbroso & Davison, 2018). The generated data was then used to construct a model. Viana et al. (2018) have used ABM together with DES to analyse overdue pregnancies.

Recent studies related to agent-based modelling have shown that it can be used with inverse reinforcement learning (IRL) to assist with the extraction of behavioural rules. Markov Decision Processes (MDPs) are used for this task. An MDP encompasses states, actions, transition probabilities rewards and reward discount factors. The expected cumulative reward function is broken down into reward features and weights based on the MDP without rewards (Lee et al., 2017).

Several attempts have been made to use deep learning in combination with agent-based modelling. For example, van der Hoog (2016) proposed to use deep learning to make agents imitate other agents, as well as running multiple parallel simulations.

The first one describes a model of botnets, where a simulation has been developed from scratch including the network (Kotenko et al., 2010). Although botnets are the consequence of criminal activity, they are not themselves human entities, which does not necessarily tell us anything about the motivations of their owners.

Another area is examined by Malleson et al. (2010) who attempt to model the motivations for committing a burglary with two key driving factors - money and sleep using the PECS model as a base.

Punzo (2016) create an agent-based model of imitating criminal behaviour. In this model, there are opportunities for crime and agents - potential criminals who can choose whether to commit a crime or not. This is determined by whether they consider this approach as successful or if everyone else around them is committing

a crime.

2.3 Penetration testing

There exists a different way of modelling the attackers, which involves simulating the attack by having specially-trained individuals participate in a security breach of the company that wants to improve its defensive posture. The scope of the security breach is agreed upon in advance. This way of modelling and simulation takes place on a different level — as opposed to it being a computer simulation, the attack happens in the real world. However, it is still not an actual cyber attack with malicious attackers. Hence it can be considered an attack simulation, albeit more costly and resource-intensive.

Penetration testing has been considered as the most common security practice (McKinnel et al., 2019). To obtain the best results from this method, a company hires information security specialists and gives them a scope to test the security. Penetration testers should not be confused with red teamers, who usually carry out an assessment on a much broader scale, assessing an entire network and employing the TTPs of real adversaries (Applebaum et al., 2016; Knowles et al., 2016), with social engineering among their arsenal (DeMarco, 2018).

Penetration testing is beneficial for the companies that choose this as a method, as they can get the expertise of qualified professionals that would employ methods that are similar or identical to a cyber adversary, while maintaining a degree of control over what gets attacked, allowing normal business operations to continue even during a test (Xynos et al., 2010). However, this approach is not without its challenges and limitations. Firstly, as companies control the scope of the test, it is very simple for them to overlook important areas that might be more vulnerable at the time the test takes place, but in a different area that is outside the scope (Netragard, 2020). Secondly, the attack surface of the organisation would change frequently, every time there is a major update, a new product or a new integration with an external or internal service (EC-COUNCIL, 2011, p. 15). This would imply that a penetration test needs to be carried out every time this happens. An ad-

versary may attack in between these penetration tests (NCSC, 2021), meaning that despite the organisation performing regular penetration tests there is still a chance that they might get attacked in between the tests. Lastly, the cost of the average penetration test can vary anywhere between £3,000 - £14,000 (RSI Security, 2020; Bulletproof, 2021), hindering the ability of a small business to afford a penetration test often, which makes the goal to secure the company more challenging. The cost of a penetration test can vary, depending on numerous factors, such as the size of the company, scope of test or expertise level of the tester (RSI Security, 2020). Although small start-ups may not have such a large scope of testing, their budget is also a lot tighter as a company is still young (Liao et al., 2008).

A typical network penetration testing process is depicted in Figure 2.4. As most of the systems are currently web-based, the procedure might be slightly different (Security Audit Systems, 2021).

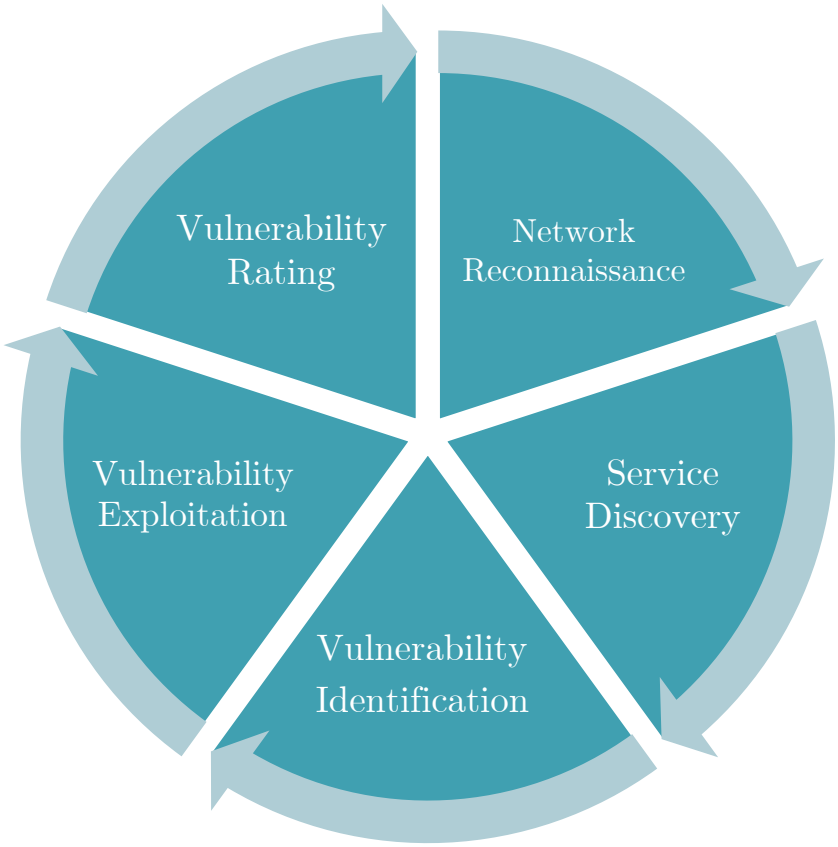


Figure 2.4: Network penetration testing cycle. Reproduced from Hussain et al. (2017).

2.4 High-engagement data gathering approaches

This section covers somewhat non-traditional approaches to data gathering, such as role-playing and serious games. As will become evident from this section, these approaches offer a number of advantages compared to the more conservative data collection approaches, which makes them suitable to be used in the field of cybersecurity research.

2.4.1 Role-playing

Crooltall et al. (1987) define role-playing activity as a simulation, but without the simulation necessarily involving role-playing. This way, role-playing becomes a subset of simulations. Crooltall et al. (1987) also define role-playing as *"a social or human activity in which participants 'take on' and 'act out' specified 'roles', often within a predefined social framework or situational blueprint."* It is important to note that authors use *'situational blueprint'* synonymously with *'scenario'*.

Engaging in role-playing activity allows participants to play a character different from their own nature, allowing the participant to express their character without the fear of being judged, or without the need to conform to social norms or perceived expectations (Mauriras-Bousquet, 1984; Daniau, 2016). Having said that, during role-playing the participant always maintains the connection to the real world (Harviainen, 2009), thus there is a risk that parts of the participant's personality will propagate to the role that they are impersonating. This is defined as ***'bleed'*** in role-playing game terminology (Bowman, 2015).

Due to its immersive nature, role-playing has been used in education, for example, to teach empathy in school children (Fischer, Jan; and Vander Laan, 2002) or to help nursing course students with various work-related scenarios (Soares et al., 2015). It has also been observed to be used for validation of jury behaviour studies (Kerr et al., 1979). Due to their simplicity and accessibility, role-playing has been used in the study done by Bolland (2006), where the participants have impersonated world leaders and their response to a variety of sanctions to stop them from propagating hostility.

2.4.2 Educational games

Schell (2008, p. 37) defines the game as *"a problem-solving activity, approached with a playful attitude"*, while Aarseth (2014) defines games as *"facilitators that structure player behavior, and whose main purpose is enjoyment"*. Game players can be defined as *participants* in the events of the game (Avedon, 1981) as *adversaries*, or *eammates* (Klabbers, 2009) or as *decision-makers* (Clark, 1970). There is a sub-type of games that is focused on providing a learning goal in addition to the fun element (Prensky, 2003). This type of games is known as educational games, or 'serious games', originally defined by Abt (1987) and later updated by Zyda (2005). An educational game, should have the following elements (Whitton, 2010, p. 31; Barnard-Wills and Ashenden, 2013):

- the goal to achieve an outcome that is superior to others *(competition)*;
- tasks that require effort and are non-trivial *(challenge)*;
- a context-sensitive environment that can be investigated *(exploration)*;
- the existence of a make-believe environment, characters or narrative *(fantasy)*;
- measurable results from game play *(scoring)*;
- explicit aims and objectives *(goals)*;
- action in game that changes the state of play and generates feedback *(interaction)*;

Robinson and Bellotti (2013) have created a taxonomy of various game features to rank levels of player commitment from various game attributes. Some of the most commitment-hungry features are virtual currencies and virtual abilities, whilst the features that require the least amount of commitment from the player are attributes such as game rules and high score boards.

The format of educational games can range from CTF-style challenges (or any challenges which accept no solution as an answer, or accept an answer past the deadline (Gondree et al., 2016) to table-top adventure games (Denning et al., 2013).

Despite achieving their intended learning objectives very few make it past the evaluation stage to be available to the general public (Roepke & Schroeder, 2019).

Purple Squad Security (2017a) have created a game where the objective is to defend the organisation against internal and external threats by combining role-playing and elements of game mechanics, such as the use of 20-sided dice. This game intends to persuade organisations to ensure appropriate cybersecurity measures are taken and to illustrate the consequences of not implementing a certain security measure. The game uses a selection of existing cybersecurity-themed tabletop scenarios (badthingsdaily, 2017), that have been adapted from real-life events (Purple Squad Security, 2017b). Steiger (2016) has designed a deck-building board game that uses MITRE (2021a) ATT&CK framework and Lockheed Martin kill chain (Hutchins et al., 2011). The game has both the attacker and the defender, the attacker aims to complete the kill chain, while the defender aims to stop the attacker or to make the attacker repeat kill chain stages by taking defensive measures. Both parties build their decks, and it is possible to strategically build a deck against the other players.

Figure 2.5: Lockheed Martin Cyber Kill chain (Hutchins et al., 2011)

Denning et al. (2013) have created a game that is aimed at 18-30-year-old individuals in STEM and Computer Science fields. The aim of the game is to inspire them to pursue an information security career (Tamara Denning & Kohno, 2014). The game has been validated by carrying out an evaluation survey.

To design an educational game or a serious game there exist a number of frameworks. They range from including the various game elements to defining the processes that should happen throughout the course of the game.

A framework that captures both the learning mechanics and game mechanics is the ***Learning Mechanics-Game Mechanics (LM-GM) model*** by Arnab et al. (2014), shown in Figure 2.6. This framework allows to balance learning and game elements to create and validate an optimal serious game.

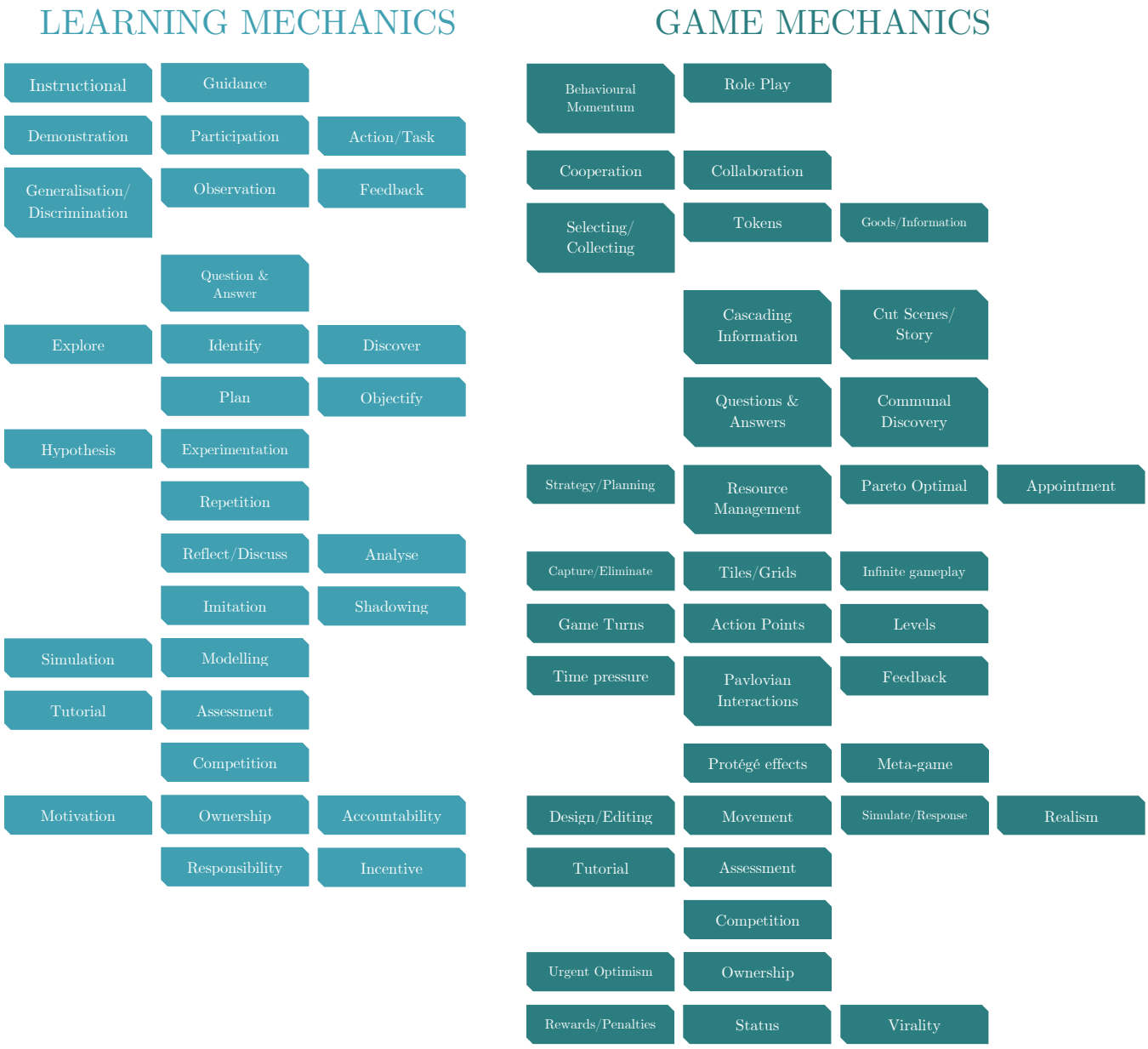


Figure 2.6: Learning Mechanics-Game Mechanics (LM-GM) model. Reproduced from Arnab et al. (2014).

Work of Marczewski (2017) illustrated in Figure 2.7 describes a variety of factors that relate together to create a well-balanced serious game. While the LM-GM framework above is focused on balancing the learning elements and game elements, the framework by Marczewski (2017) The outer layer is the ***discovery*** layer. The discovery layer includes three fundamental aspects that define the serious game, these are *problem*, *people* and *success*. Defining the problem is about constantly coming back to the requirements and asking what the client requires. The next aspect is to define the people that are going to be playing the game, and this group might have a different idea of how the game needs to function, or what is important in any given case. Lastly, defining success deals with the problem of how success will look to the players and the client, and what records of success are going to be required.

The outer square on Figure 2.7 is the ***design*** stage. At this stage, there are four aspects – *Behaviours*, *Motivations*, *Emotions* and *Mechanics*.

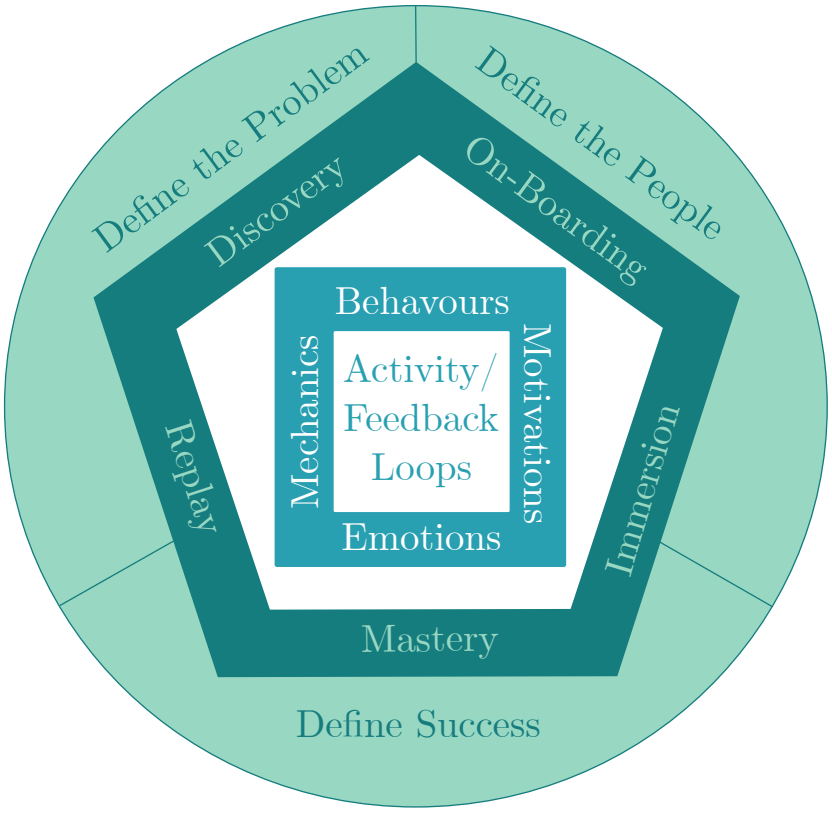


Figure 2.7: A Revised Gamification Design Framework by Marczewski (2017).

Behaviours are concerned with the intended actions of users – what do they need to achieve as they are playing the game. Motivations are initially defined in the discovery stage, in this case it is concerned with refining the target end users – future game players, by, for example, applying a framework, such as RAMP (Marczewski, 2021), which stands for *Relatedness, Autonomy, Mastery* and *Purpose*. The next category is Emotions, this category explores how the players feel and what is the intended feeling they would be experiencing. Final category is Mechanics, and some gamification techniques and elements are outlined in Figure 2.8. The table is broken down into activity categories targeted to a particular type of players. Examples include Disruptor, Philanthropist or Socialiser. There are also miscellaneous categories that can be applied to games in general, such as Reward Schedule. Each of these categories are colour coded, and contain more than one game attribute, such as Quests or Narrative. All of these elements are present to keep the players engaged with the game.

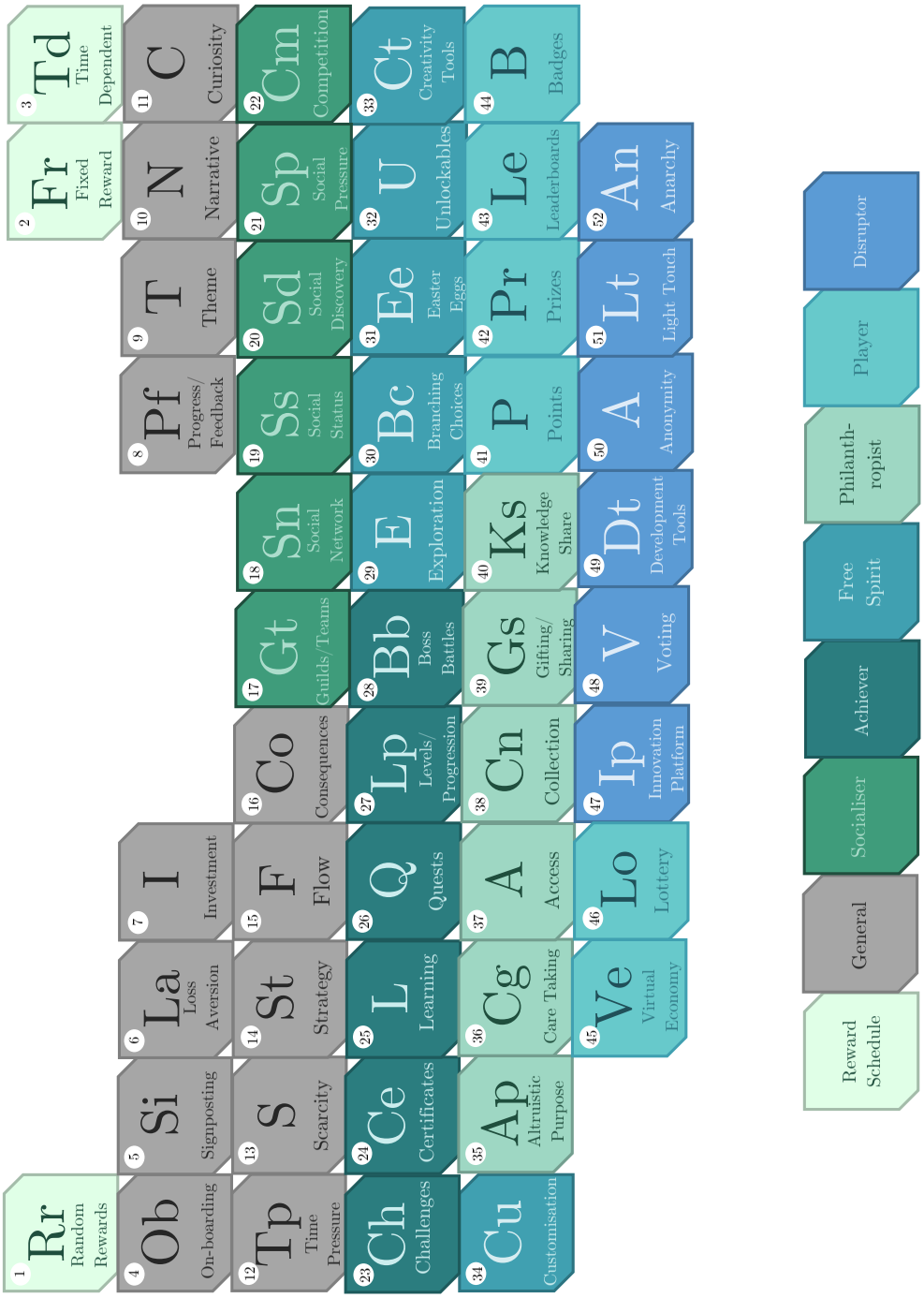


Figure 2.8: The Periodic Table of Gamification Elements by Marczewski (2017).

Summary

In this chapter, we have examined current methods that organisations use to validate their defensive posture. Next, we have discussed current modelling and simulation methods as an alternative means to validate and analyse the defensive posture. As part of this discussion, we have touched on how cyber adversaries are currently profiled and what alternative modelling methods exist to represent human decision-making. As simulations would heavily rely on pre-existing data, in the final third of this chapter we have reviewed the high-engagement data gathering approaches as a means to collecting this information, as well as some of the validation strategies. These high-engagement data gathering approaches will inform these simulations. This project aims to bridge the gap between the high-engagement data collection methods and simulations by developing a methodology that will allow using the data from a serious game by capturing decisions of game players to inform a computational simulation.

Chapter 3

Methodology

This chapter will focus on the research methodology that underpins this project as well as examining the reasons for choosing the methods used for conducting the research.

We will begin by examining different research philosophies that will drive this research project, moving on to research approaches and methods that have been chosen for this research project. This section will conclude by examining assumptions that have been made during this project, the constraints, and the validity of the methods chosen.

3.1 Research Philosophy

Research philosophy determines the underlying set of beliefs that define the research that is to be conducted. Adopting a philosophical stance will help us pick the correct research approach later. By deciding on our ontology (how we view the world and the elements that it contains (Silverman, 2017, p. 309)) we can decide on our epistemology (how we should investigate what proportion of our knowledge is valid (Gray, 2004, p. 398)).

Quantitative approaches align best with *positivism*, while qualitative approaches are more prominent in the *interpretivistic* research philosophy. As there is such a distribution of methods employed in this research, rather than confining ourselves to either end of the philosophical spectrum we could take the *pragmatic* approach

instead, which will be the final research philosophy discussed in this section.

3.1.1 Positivism

Positivism was the dominant philosophy during 1930s-1960s (Gray, 2004, p. 18; Williams, 2016, p. 161). Historically, many methods that are in use in modern-day social science have originated from natural sciences (Williams, 2016, p. 162). Gray (2004, p. 18) summarises the following assumptions of positivism:

- *Reality consists of what is available to the senses - that is, what can be seen, smelt, touched, etc.*
- *Inquiry should be based on scientific observation (as opposed to philosophical speculation), and therefore on empirical inquiry.*
- *The natural and human sciences share common logical and methodological principles, dealing with facts and not with values.*

As can be seen from these three points, positivism does not take into account theoretical sciences, where most of the discoveries are hypothesised about as opposed to observing them (Gray, 2004, p. 18). The same applies to certain fields of astronomy (ibid.), where personally observing the phenomena such as black holes is not possible with current technology. This implies that there are perfectly reasonable cases where a starting theory is necessary, permitting observations to be mapped onto it, as opposed to forming a theory based on the observations alone.

Reflecting back to our first objective:

1. *To build a realistic game based on rigorous evidence*

Building a game implies that we will require both numeric data and descriptive data. For factual information in the game, we will require descriptive data, while the game mechanics will require numeric data. For numeric data, quantitative approaches would be more fitting. However, for the descriptive data, it would be best to use

qualitative approaches.

The second objective will also require a stringent framework that will ensure a common ground for decisions the players make in the game, no matter how diverse these decisions are:

> *2. To ensure that the game enables players to make decisions that reflect their true intention*

Taking this diversity into account, it would be better to devise a set of criteria that will serve as constant points of reference for the decisions made by the players, bringing them to a common reference point and allowing them to be compared to each other.

> *3. To devise an efficient approach to the recording of the game decisions*

Decisions made in the game will not always follow the same pattern. Sometimes there will be circumstances where the standard game turn description notation will not be sufficient or there will be cases that will happen less commonly. Key decisions will be recorded in a computer-processing-ready format. Hence, some information will be sacrificed, but the decisions will be recorded unambiguously. This unambiguous manner of recording almost certainly belongs with the positivistic philosophy.

Yet, many aspects of this research are focused on descriptive elements and subjective interpretation, as will become evident from the subsequent chapters. This implies that following a pure form of positivism is not possible in the context of the research project.

3.1.2 Interpretivism

Unlike positivism, which insists on objectivity and the application of identical methods both for natural and social sciences, interpretivism *"asserts that natural reality (and the laws of science) are different and therefore require different kinds of methods"* (Gray, 2004, p. 20). Crotty (1998) specifies that interpretivism is searching for *"culturally derived... interpretations of social life-world"*. As such, it makes interpretivism perfect for qualitative approaches and measuring individual differ-

ences. Interpretivism does not come without its challenges - one such challenge is ensuring that the researcher does not simply propagate the misinterpretations of the situations through the prism of his or her research participants (Williams, 2016, p. 115).

To create a realistic game using rigorous evidence, the amount of misinterpretation must be minimised, and as mentioned before, for elements of the game, such as game mechanics it might be necessary to use quantitative data, which is not suitable for a purely interpretivist perspective.

By contrast, some of the research objectives employ interpretivistic methods. Let us examine them in greater detail.

> *4. To ensure the events within a game can be restored from the recording, with semantics preserved*

This objective would include a degree of interpretation, as the reasons that players make a certain decision can differ, and the in-game circumstances would also not be identical if we were to take two different players, who are playing the same game. Even if the game that they are playing is a game to the likes of chess when presented with the same situation, the outcome of the move will vary depending on the player, and their perception of the situation would be one of the deciding factors for choosing a move. For a researcher, it is important to capture these individual differences.

> *5. To ingest the game decisions into a simulation*

Due to the decisions being different depending on various circumstances, individual differences and luck (various aspects of the game mechanics) they will be recorded while being impacted by those differences, while the game is still fresh in mind. However, as time passes by, recalling certain events may become more challenging, hence some details might be lost in translation. To ensure this does not affect the game, major decisions will be recorded unambiguously, enabling them to be transferred into the game as they are.

Secondly, translating human decisions into computer input will almost certainly require adopting a certain interpretation and making several assumptions, hence

placing it in the interpretivism category seemed the most sensible.

The choice of approaches at each stage of the research project is summarised in Figure 3.1.

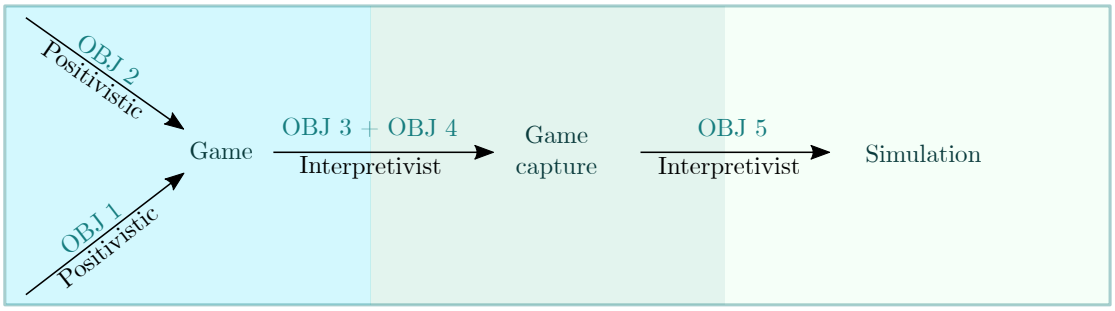


Figure 3.1: This diagram shows a summary of research objectives, outlined in the Introduction chapter. The numbers of the objectives correspond to the order that they have originally appeared in. The diagram illustrates the transition across all three stages of the research project together with the associated philosophies.

The next research philosophy perfectly encapsulates the requirements and the view that is required for this research project.

3.1.3 Pragmatism

Pragmatism *"offers a way of thinking about method choice, based on the demonstrated utility"* (Hoshmand, 2003, p. 42). This statement has majorly influenced the choice of research philosophy for this project. The primary differentiating characteristic of pragmatism is that it places greater importance on the effects that the phenomena generates, as opposed to any intrinsic properties that it has (Dennis, 2011, p. 464). Additionally, pragmatism assumes that there is no separation between a 'human' and a 'natural' world (Williams, 2016, p. 172). This research is not purely positivistic or interpretivistic, therefore if there is a single philosophy that describes the entire research project it would be pragmatism.

3.2 Research Approach

Once the philosophy has been decided, the next step is to allocate the research approach to the research objectives. A research approach would help us structure

the research in a manner that fits the project best. Notably, there are two key approaches - *deductive* and *inductive* that will be considered for this project.

A ***deductive approach*** is defined as an *"experimental approach that uses a priori questions or hypotheses that the research will test"* (Gray, 2004, p. 397). It starts with a specific hypothesis that develops into a broader theory. Snieder and Larner (2009) illustrates this process as:

$$Theory \rightarrow Hypothesis \rightarrow Observations \rightarrow Confirmation/Rejection \quad (3.1)$$

This transition from theory to observations makes this approach suitable for the following two objectives:

1. *To build a realistic game based on rigorous evidence*
2. *To ensure that the game enables players to make decisions that reflect their true intention*

When building the game we begin with past cases, which help us formulate certain expectations on how an offensive actor should behave. We can re-formulate our theory once we observe whether the players are behaving the way we want.

A similar remark can be made about objective number two. We would have certain assumptions about how would the players make the decisions that reflect what they truly want to do, but our expectations can differ from what truly benefits the players. For example, we might assume that players will make the best decisions when they are not made the centre of attention, but there may be players that do not mind being the centre of attention and their decision-making process will be unaffected.

An ***inductive approach*** is the *"establishment of facts on which theories or concepts are later built, moving from specifics to generalizations"* (Gray, 2004, p. 400). Contrary to the *deductive* approach, an *inductive approach* starts with a broad theory and focuses on the details later. Reflecting on the final research objectives:

3. *To devise an efficient approach to the recording of the game decisions*
4. *To ensure the events within a game can be restored from the recording, with semantics preserved*
5. *To ingest the game decisions into a simulation*

For our third objective, we establish what needs to be captured first, by observing factual events and validating the events with the game rules and various aspects of game mechanics. Then, we can make a list of the actions to be captured and consider how best is it to capture it. Effectively, this is our transition:

> *observing items to capture (factual information)→ arranging and compiling them into requirements (theory) → devising notation (new concept)*

For objective number four, to understand what information will need preserving, and what information will be lost we need a certain amount of factual information - an existing game, perhaps obtained from an early playtest. This way we would be able to compile a list of requirements that would allow us to devise a new way to represent the game captures. This transition from game captures to a theory about how best to capture the game, to a completely new notation, a new way that allows representing future and existing games makes it suitable for an inductive approach.

As we get more and more games that are completed we would get more potential directions that the game could take, sometimes shifting from the pre-determined route prescribed by the game mechanics, yet still valid as far as the game rules go. These situations, which do not occur commonly but are still valid according to the game rules may not conform to the pre-selected notation, making them more difficult to be represented accurately.

Finally, for our objective number five we begin with some factual data again, this time it is a set of the game captures. This way, based on the data that we begin with we can formulate theories and conclude with new concepts, which aligns with an inductive approach.

Since for all three of these objectives we begin with information that is quite specific, we also move on to generalisations at a later stage. This is another common trait of an inductive approach, as mentioned above by Gray (2004, p. 400), who pointed out that inductive reasoning moves from specifics to generalisations.

3.3 Research Strategy

Our research objectives have now been mapped onto their corresponding research philosophies and approaches. In this section, we will examine the research methods that have been selected for this research project.

3.3.1 Case studies

Yin (2009) defines a case study as *"an empirical enquiry that investigates a phenomenon in depth and within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident."* Case studies are often adopted after the event has occurred, which adds on to the misconception that case studies are atheoretical (Lune & Berg, 2017, p. 171). Some of the critiques of case studies include them being prone to "selection bias" (Geddes, 1990), which can lead to a truncated sample among the dependent variable being selected (Collier & Mahoney, 1996).

For this project, as will be explored in Section 3.6, existing scenarios or case studies have been chosen due to their availability. Having said that, it is important to acknowledge that several assumptions are being made specifically relating to case studies specific to the project, the past cyber incidents, which are summarised below:

1. *News reports capture true events without omitting important details that could transform the outcome of an event.* For example, if a news story mentions penetration testers who got arrested for breaking into a building, it does not miss out the fact that they have been doing this as part of their job and not because they have suddenly turned rogue and are acting out of their own desire to break into a building. If this detail (arrest during their job) would have

been omitted then the story would be an inaccurate record of the event. In the first case, it merely seems that penetration testers have accidentally made a mistake on their job to allow themselves to be detected, but their intentions have still been benevolent. In the second case, it is evident that the police has done the right thing and stopped a pair of criminals who were abusing the skills they have gained as part of their job.

2. *Events that have happened in news stories in the past may occur again in the future* The criteria for selecting such stories is the context in which they have occurred. If there are no old technologies that feature in the story, or the events can be applied to more modern technologies - it is a story that will be deemed relevant. An example here would be the "password on a post-it note". This practice has been observed since the beginning of passwords, yet the assumption is it would still be in use today in some form.

Additionally, only news stories that were available in open-source literature were considered for this research for pragmatic reasons. If a news story is unusual enough, it will be available online. As the research is a proof of concept, it has been decided that a valid sample of past news cases can be obtained without examining physical news archives.

The following method has been used to source the news stories. First, the following search queries have been input into the search engine DuckDuckGo: ***famous hacking cases*** and ***famous social engineering cases***, as well as the following list from Wikipedia (20021). It is important to note that these have been used as starting points, user-generated timelines that help to learn about the fact that the event has occurred, and subsequent research on a specific event followed afterwards. Noteworthy events were selected if they concerned an individual or a group (to help generate Role cards), if they explicitly mentioned using a certain tool or acquiring access to it in the course of the attack (to help generate Information cards), if there were any rare and unusual circumstances that helped the attack take place, for example an employee forgetting their laptop on the train and the attacker using this opportunity to carry out their attack. These types of news stories have been used

for the generation of Opportunity cards. With Information and Opportunity cards, another important aspect is the fact that there is a link between Information and Opportunity cards, and the Opportunity card must enable the Information card. An example of this is in the case where the laptop has been forgotten on the train, the Information card outcome is "CEO's physical laptop access". To keep the Opportunity cards more relevant, a lot of information has been sourced from social media, such as the term "rabbit hole" and other small details, such as "#BugBountyTips". This has been achieved by following a number of penetration testers and bug bounty hunters, until recurring trends have been spotted.

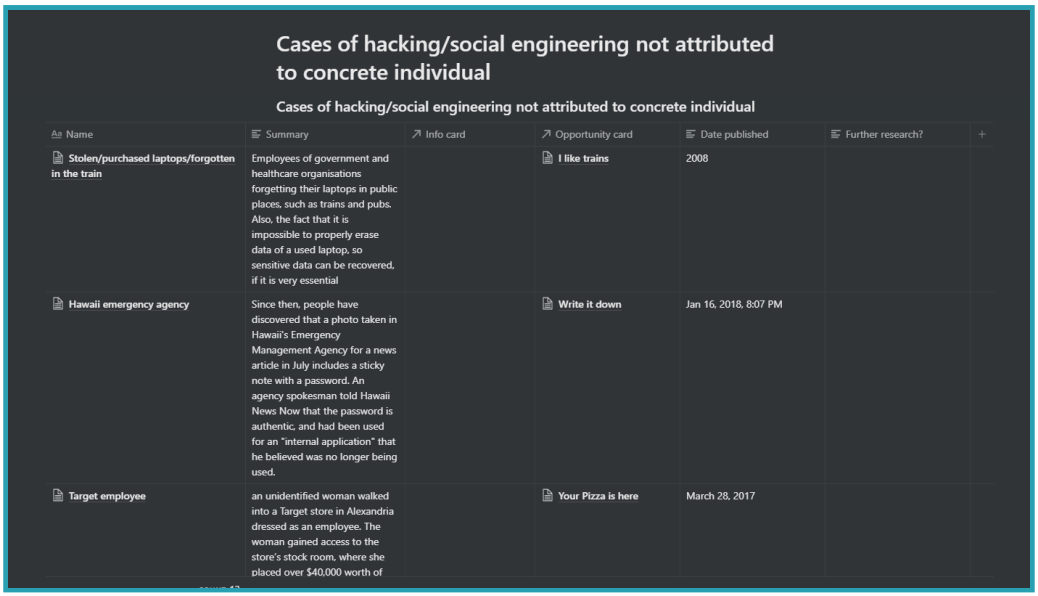


Figure 3.2: Saving cases of data breaches/cyber attacks into a table to build Opportunity cards

Figure 3.2 shows a table of curated news stories, where a table has been created for a number of instances. This table depicts isolated hacking incidents and data breaches that have inspired some of the Opportunity cards or the assets obtained as the data breach happened.

The next table has been dedicated to individuals or entities. These have been curated to subsequently produce role cards. An example of how the statements from these news stories have been used are shown in Figure 3.3. In this case, the role is Counter-culture and by using a number of statements from different counter-culture individuals that have operated alone it is possible to build a Role card inspired by

the real-life events.

Another noteworthy remark, specifically relevant to the APT Role cards – there is a low-capability APT Role card, and a high-capability APT Role card. Own judgement has been used to map the capability level to these Role cards. This decision was made due to the news stories or security reports about APT groups not making this distinction clear – whether an APT group was high or low capability. Besides, different organisations have different styles of reporting and no universal scale that maps the relative capability has been identified during the course of the investigation.

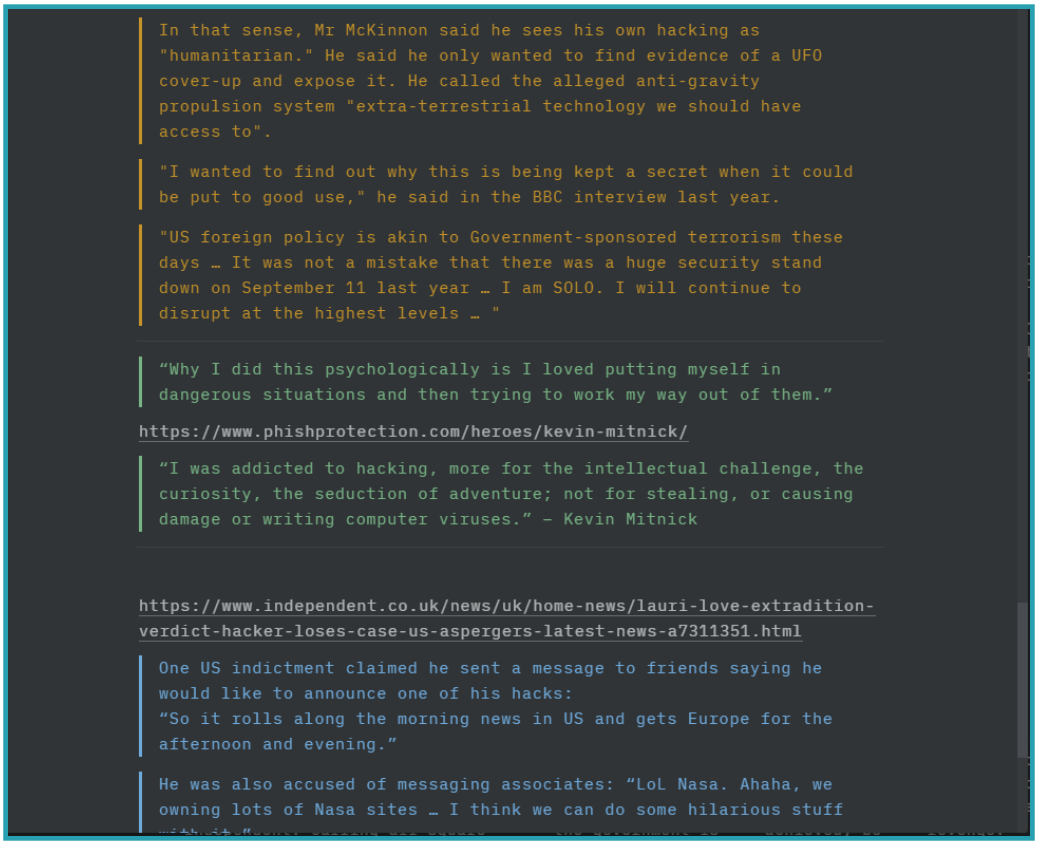


Figure 3.3: Extracting statements from news stories to build a Counter-Culture role card. Different colours denote different sources.

3.3.2 Surveys

As Gray (2004, p. 188) points out, surveys/questionnaires are very popular, as they provide a low-cost method that can provide a quick inflow of data, where

respondents' anonymity can be assured. The analysis is also simple, provided the questions are not free text fields. There is also a lack of interviewer bias.

That said, the response rate becomes negatively affected if the questionnaire or a survey is too long. Answers can also be inaccurate and misleading with no opportunity to ask for clarification. Additionally, it is important to acknowledge that surveys may be prone to selection bias.

In the context of this research project, the participants for the provision of game information were selected using Twitter and other social networks, with a combination of convenience and snowball sampling. This implies that a true variety of experiences and opinions will not be achievable in practice, as the sample will be limited to individuals who regularly use social networks and are either direct acquaintances of the authors, or acquaintances of acquaintances. To minimise selection bias, a wider amount of social media platforms have been utilised, so that the participants are not restricted to a single platform.

Gray (2004, p. 188) also notes that questionnaires inherently reflect the designer's view of the world, from individual questions to the broader world picture. In order to minimise the impact of misinterpretation, the questions need to be formed unambiguously and account for the survey designer's prism of view. In the case of this research, an example of such a view can be that any TTP can be used to impact the target organisation or for finding out more information about it.

An example research pipeline involving a survey is shown in Figure 3.4.

3.3.3 Focus groups

Focus groups are considered to be a low-cost way to collect data, but they require participants to cooperate (Gray, 2004, p. 230). A typical focus group session consists of a small number of participants under the guidance of a facilitator (called the *'moderator'*) (Lune & Berg, 2017, p. 94). Authors also note that focus groups are treated as a unit of analysis, rather than individually collecting data from each participant (ibid.). For bigger focus groups recording the outcome may be problematic. Silverman (2017) suggests not to ask direct questions and instead recommends

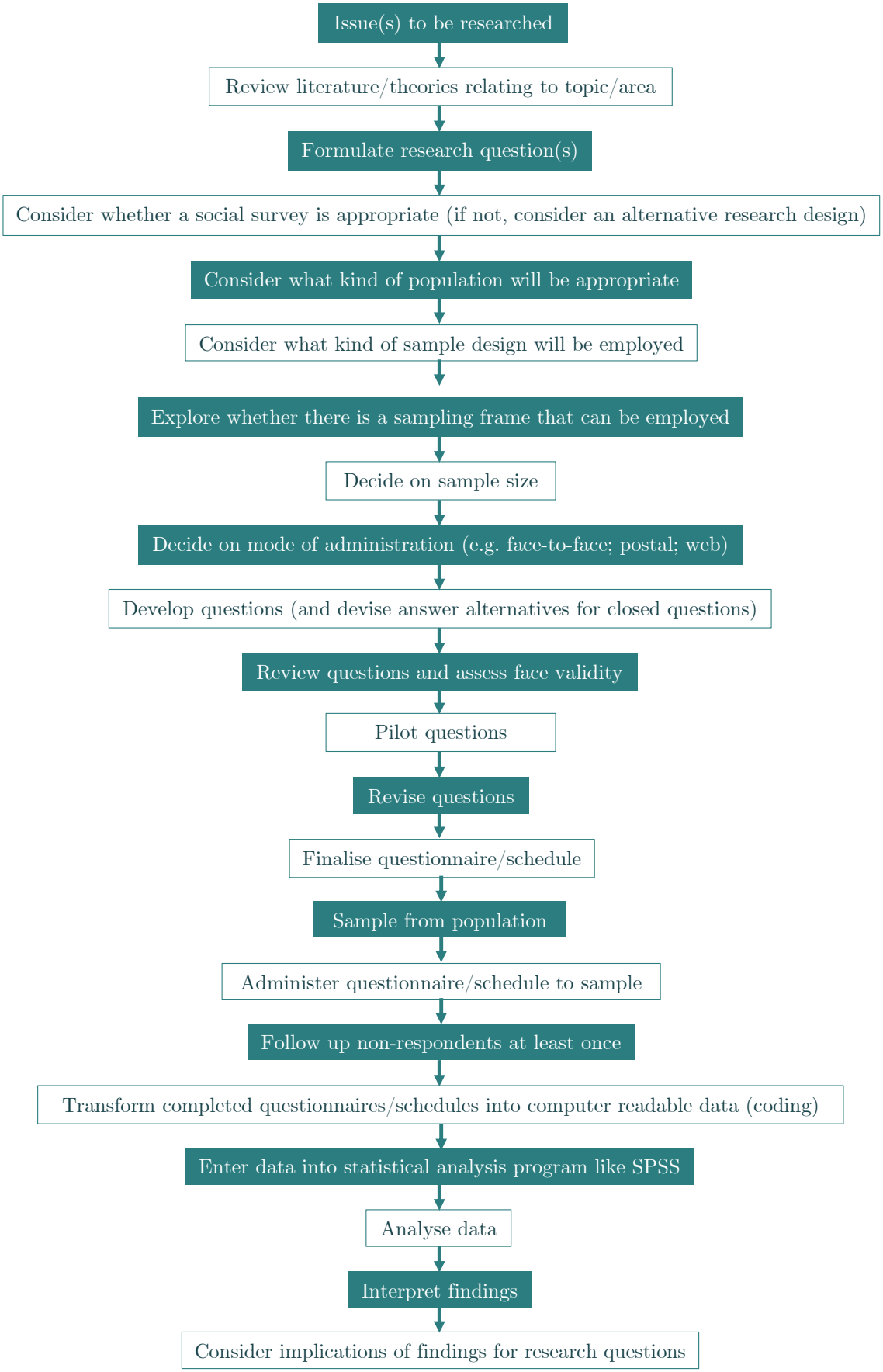


Figure 3.4: Steps in conducting a social survey, reproduced from (Bryman, 2012, p. 185).

offering a stimulus to focus group members. He also points out that the focus group leader is often considered an outsider.

Lune and Berg (2017, p. 95) provide the following elements of a focus group interview:

> 1. *A clearly defined objective and/or research problem*
> 2. *The nature of the group*
> 3. *Atmosphere/environment and rapport*
> 4. *An aware listening facilitator*
> 5. *A well-organised and prepared facilitator*
> 6. *Structure and direction but restrained contribution to the discussion*
> 7. *Research assistance*
> 8. *Systematic analysis*

From the above, to have a successful focus group it is important to have a clear discussion goal in mind, to have a facilitator that directs the conversation without affecting it, and a reliable way to process the outcome of the discussion.

3.4 Assumptions

Throughout this research project, some assumptions have been made to simplify the implementation. These assumptions are listed below.

> 1. *Attacker's risk appetite is only modified by the outcome of the tools or techniques that they are using*

If an attacker picks out a certain TTP for use if that technique succeeds - their risk appetite stays the same or slightly increases. If the technique fails - their risk appetite falls. This is the only modifier of the risk appetite. External circumstances,

such as game-wide modifiers (such as increasingly vigilant incident response teams serving as a risk-appetite lowering mechanic) and events (such as unexpected visitors to the attacker in the game world interrupting their activity — a friendly neighbour may visit the cyber attacker mid-way through an attack) are not considered by the game mechanics.

> *2. The organisation's defensive posture does not improve throughout the course of the attack.*

At the start of the game, a certain set of defensive techniques is chosen. As the player is playing the game (a direct parallel with an attacker performing an attack on the organisation) it is assumed that the organisation does not suddenly host a multitude of training sessions, install a new intrusion detection system, or similar. While in practice this can happen, for simplicity it has been decided that the defensive toolkit of an organisation does not change throughout the course of the attack.

> *3. A single attack is enough to bypass a defensive measure*

Another assumption has been made for the simplification of game mechanics. Each defensive measure that is in place in the organisation can only be used a single time. For example, after the attacker takes down a firewall, it no longer comes back up throughout the course of a game. The use of single-time defensive measures was an assumption that has been made to keep the game mechanics simple.

3.5 Constraints

This research project has a certain amount of limitations, the main one has been time. This, in turn, has mandated that some compromises are made in terms of the implementation. Here are some of the constraints that have been set as a result.

> *1. Each player can represent an entity, such as an APT group or a Hacktivist group. However, there is only one player for one entity, and the collaborations between players or entities are not explored.*

For simplicity, interactions within a malicious attacker group or groups forming alliances to attack a common target are not considered as part of this project.

> *2. This project does not focus on insiders and insider threat - it only considers external attacks and attackers*

Methodology and methods described in this project are applicable to insiders, however for simplicity and demonstration that this method works only external malicious actors have been considered.

> *3. An Agent-Based model does not feature agent-to-agent interactions*

The Agent-based model is a proof of concept and only demonstrates the outcome of the game output capture system. Agents do not modify each other's state or behaviours, partly because of constraint number 1 – the focus on individuals as opposed to interactions within or between groups. As no interactions have been considered for this project the ABM also does not feature any interactions.

3.6 Validity

In this section, various research methods will be compared and applied to the context of this research project. Consequentially, it will become evident which methods are more suitable for this research project along with the reasons why they are chosen.

Case studies have been chosen for obtaining relevant information on past incidents in order to construct scenarios in which the games can take place. The reason this approach has been chosen is due to its historical credibility since these are cases that have already occurred.

The reason that case studies were chosen over ***action research*** is due to ethical considerations. Performing breaches on a real target has to be agreed with the target and usually is confidential, hence obtaining approval would take a long time. Additionally, carrying out an intrusion without prior approval of the target organisation is illegal under the UK law. ***Observations*** of real penetration testers or red teamers is also very difficult for two reasons. The first reason is the targets. Penetration

testers usually sign a non-disclosure agreement to not expose their clients. Hence, approval would be necessary from both parties: the client and the penetration tester themselves. If we get the penetration tester to carry out a scan on a target that we have created (effectively replacing a real client with the lab environment), this is where the second reason becomes noticeable. Creating a lab environment that would replicate a real target would require a lot of insider information and time. An existing lab environment cannot be used, as penetration testers use it to practice their skills, hence there is a probability that they have already had some degree of exposure to it. Observing penetration testers would also impose a hidden complication in that a lot of penetration testers work in silence, hence some of their actions will not be entirely clear.

The idea of a custom lab environment or a honeypot has also been briefly mentioned in the above paragraph. The reason why ***system logs*** from a honeypot cannot serve as a data collection method is due to the limited number of actions that a system log can display. Examples of what can get displayed are successful operations or sometimes unsuccessful attempts, such as unsuccessful password attempts. What does not get captured are unsuccessful connection attempts, or the reasoning for picking a particular tool, which is equally as important for this research.

Diaries is another method that can be used to collect data about attacks. In this scenario, penetration testers will be asked to produce their own notes. This would essentially make penetration testers produce a report, similar to the one that they produce for their client. However, this places a big load on the participants. Also, the diary needs to be in a specific format to keep the notes consistent. This would be necessary, as different people have different formats for taking notes, and it may not always be evident from the notes, e.g. what stage they relate to.

Another method for collecting the data about decisions that offensive actors make is with the use of ***documentation***. Although it is a reputable unambiguous source of information, there are several issues with this method. Firstly, the documentation offers a generic outlook, as opposed to the ways that individual people use it. DEFCON is an example where the diversity of approaches is demonstrated.

This diversity has been used as an inspiration for this research. On many occasions, creativity and the search for new approaches have served as a basis for a new cyber attack or a way to exploit an existing program or feature. This creativity leads to individual approaches to be favoured over a more universal approach. Secondly, there is no one single source, a cyber attack manual that covers all possibilities of every single attack vector. Finding one that would be a reputable single point of reference would be problematic. Coming back to the example of DEFCON, even within the same area of cybersecurity, such as social engineering, there is more than one way to get to the desired outcome. At the Social Engineering CTF competition participants were required to get the call recipients to answer some questions to get the points for the said questions. Quite often participants had their unique ways to get the answer in the correct form.

The next two methods are quite similar – ***Concurrent Verbal Protocol (CVP)*** and ***Retrospective Verbal Protocol (RVP)***. In the first instance (CVP) it is getting participants to narrate what they are doing. In the case of our research, we can capture any actions that are usually not given very much attention in different walkthroughs, allowing us to get a full picture of what the participant is doing and what was the intention behind their actions. Although if the nature of things that require mentioning during the research study session is not discussed in advance, and the participant is narrating their actions without a certain list of items that require mentioning in mind, there is a risk that some aspects of the cyber intrusion will continue to get only a brief mention or a participant may get sidetracked by talking about a specific topic in depth. This method has been deemed suitable for this research as it allows for a better understanding of participants' intentions. The second method, RVP is getting participants to narrate their actions retrospectively. This method allows getting two different perspectives – as the participant carries out a specified task the researcher can build a specific understanding of what the participant is doing. During the retrospective narrative phase, the researcher can confirm or deny any assumptions or impressions that he or she has built during the participant observation process by getting the perspective of the participant, as they retrospectively narrate their actions. A significant drawback of this method

is that a significant load is placed on the participant as they have to first carry out the task specified, in our case - breach the security in a lab environment, then watch a recording of them doing it and narrate over it. This also brings additional complexity, as the participant might not recall all of the reasoning behind certain decisions. The strain placed on the participant was the primary deterring factor against using this method in this research project.

A method similar to RVP, but without an opportunity for the participant to re-watch the recording of themselves, is a ***retrospective interview***. The benefits of this method are the same as with RVP, but recall suffers even more, as with this method participants do not have the option to watch a recording of themselves performing the task. Having said that, there is also a reduced load on the participants as they do not have to re-watch the recording and record themselves narrating over it, the discussion is lead by the researcher. The element of reduced load on the participant coupled with the ability to gather different perspectives from a variety of participants were the key reasons why this method has been chosen to ask participants for feedback on sessions. Using it for feedback as opposed to a significant data gathering process prevents the drawbacks from affecting the research. This way, each participant gets to mention only the elements that are most important to them that have either impressed or disappointed them, along with anything that could be improved.

Another method that has not been chosen is ***experimentation***. This research is mostly qualitative, and experimentation is usually a method associated with quantitative research. Due to the nature of the research question, repeating the same experiment (and keeping conditions the same) would be difficult, as the participants would already be familiar with the target that they will be attacking during the repeats. Obtaining the data experimentally for the first two research objectives would be difficult, as gathering information for the game belongs to a completely different research paradigm and has a different goal (populate the game as opposed to finding an effect of one variable on another).

Furthermore, another method that has been chosen for this research is a ***survey***. Surveys provide an opportunity to reach out to many people and gather a large

volume of quantitative data. It is possible to also gather qualitative data, although the number of questions, especially mandatory free text fields has to be controlled for an optimal response rate. This method has been chosen due to its simplicity and availability - it is possible to reach out to a wide range of populations, without being restricted by the geographical location. All that is needed is an internet connection and a device to fill the survey out on. Having said that, its simplicity can also be the reason why the data might not always be of the highest quality, but this can be mitigated by reviewing responses and ensuring that they are of satisfactory quality before including them in the dataset. Applied to this research project, it will have several uses. Firstly, to help accomplish research objective number one - building a game. A survey allows to obtain the expertise of a number of cybersecurity experts and enthusiasts without allocating extra time to build a panel of experts, and obtaining information for the game is a task that fits well for this purpose. Secondly, to gather supplementary data for the game playing stage. In both cases, the surveys help enrich the data gathered by other methods without additional costs and without spending a lot of time on it.

The last method that has been considered and subsequently used is a ***focus group***. Focus groups are panels of experts that come up with a solution to a specific problem or answer questions. Since every member has a solid understanding of the subject area, a collective mind of such people can provide valuable opinions that will help with accomplishing research objectives. For example, a panel of experts in the defence industry can provide insight on any past cyber attacks and what areas have been targeted, as well as what methods have the defenders tried to protect themselves against malicious attackers. That said, a panel of experts in a single room can influence each other's opinion and gravitate towards a single point of view (also known as *group think* (Lune & Berg, 2017, p. 95)). This should not be a problem for the research as the focus group will be used to choose a high-impact scenario for the game premise, hence the research data will not be affected.

Table 3.1: A summary of all research methods, their application to the research project and justifications

Method	Implementation	Benefits	Drawbacks	Chosen?
Case studies	• Reviewing past news reports of cyber atttacks	• Provide context to attacks • Accurate, as these are real events that occurred in the past	• Might not be up-to-date • Might not be most relevant	✓

Table 3.1: A summary of all research methods, their application to the research project and justifications

Method	Implementation	Benefits	Drawbacks	Chosen?
Surveys	• Gathering information about the attack techniques • Gathering an understanding of players' individual differences	• Accesses a wide range of participants • With sufficient skills data processing can be automated	• With a lot of mandatory free text boxes the completion rate drops • Due to its availability not all responses will be of high quality	✓

Table 3.1: A summary of all research methods, their application to the research project and justifications

Method	Implementation	Benefits	Drawbacks	Chosen?
Focus group	• Employing a panel of experts to agree on which type of an organisation should be the target in a fictional game world	• Subject-matter experts can provide a relevant and credible opinion	• Experts may become affected by group think, which can be both beneficial and detrimental	✓(elements)

Table 3.1: A summary of all research methods, their application to the research project and justifications

Method	Implementation	Benefits	Drawbacks	Chosen?
Concurrent Verbal Protocol (CVP)	• Participants carry out a task (breach security of a selected target, or emulate this process) as they narrate what they are doing	• Augments the actions with the participant's perspective on them	• Without a framework a lot of details can be lost	✓

Table 3.1: A summary of all research methods, their application to the research project and justifications

Method	Implementation	Benefits	Drawbacks	Chosen?
Action research	• Breaking into companies myself • Hiring penetration testers to do this	• Research data will be as recent, relevant and accurate as possible	• Expensive if hiring penetration testers • Illegal if no prior agreement • Agreement might take a long time to get processed	×

Table 3.1: A summary of all research methods, their application to the research project and justifications

Method	Implementation	Benefits	Drawbacks	Chosen?
Observations				×
	• Observing penetration testers at their job	• Realistic and recent, as real targets are involved • Accurate in terms of TTPs and timescales	• Not all clients will agree for an external observer to be present • Observer effect might be a problem • A lot of actions are tacit, hence may not be captured by the observing researcher • Takes a long time to observe and process the outputs of the observation	

Table 3.1: A summary of all research methods, their application to the research project and justifications

Method	Implementation	Benefits	Drawbacks	Chosen?
System logs	• Set up a honeypot and get information security enthusiasts to break into it	• Controlled environment • Recording of actions is done automatically	• Pre-existing honeypots are widely available, there is a chance that participants are already familiar with it • Creating a honeypot would take a long time • Not all information about the target will be openly available, if we want to replicate how a port or a defence prime operates this information might not be openly available	×

Table 3.1: A summary of all research methods, their application to the research project and justifications

Method	Implementation	Benefits	Drawbacks	Chosen?
Diaries	• Get penetration testers to produce their own notes about the target • Target could be a honeypot	• Quite descriptive, participants can determine what is worth noting	• Places a big load on the participants • Note taking style is not uniform, might need a template for it	×

Table 3.1: A summary of all research methods, their application to the research project and justifications

Method	Implementation	Benefits	Drawbacks	Chosen?
Documentation	• Find a reputable manual that describes correct course of action in different situations	• Provides a reliable step-by-step guide on what to do and how to act in a certain scenario, walks through the process of selecting the correct TTP.	• A manual is a set of recommended actions, which does not always correspond to the set of actions that are carried out in practice • Restricts creativity — no different approaches • Finding a reputable, up-to-date manual that contains all modern TTPs is very problematic	×

Table 3.1: A summary of all research methods, their application to the research project and justifications

Method	Implementation	Benefits	Drawbacks	Chosen?
Experimentation	• Experiment cannot be designed for game design phase • Reproducing the experiment for gathering decisions phase would be tricky, as participants will already be familiar with the target	• Reliable way to find relationships between factors • Gives a clear set of instructions to be repeated by others	• Not applicable to this research project	×

Table 3.1: A summary of all research methods, their application to the research project and justifications

Method	Implementation	Benefits	Drawbacks	Chosen?
Retrospective verbal protocol (RVP)	• Participants re-watch their attempt to breach security in a lab setting and record their thoughts over the footage	• Allows to get two perspectives on the task - the outside perspective (researcher observing the participant) and the inside perspective (participant's thoughts at the time of doing the task)	• Participant might not remember everything as they are narrating • It puts a significant load on the participant, as they need to do double the amount of work - to carry out the task and record their thoughts after the task is finished	×

Table 3.1: A summary of all research methods, their application to the research project and justifications

Method	Implementation	Benefits	Drawbacks	Chosen?
Retrospective interview	• This method is being used for obtaining feedback on sessions	• Allows to gather different perspectives • Less load on the participant compared to RVP	• Participants may not remember all the details	✓(elements)

3.7 Ethics

Cranfield Research Ethics Policy has been followed during this research. The policy outlines the following practices:

- *Maintain professional standards which comply with ethical, legal and professional frameworks*
- *Properly document results*
- *Evaluate critically results whilst maintaining integrity*
- *Attribute honestly the contributions of others*
- *Wherever possible report all results openly, . . . bearing in mind the University's commercial considerations, sponsors' needs for confidentiality or other good reasons*
- *Ensure all research studies gain ethical approval through the Cranfield University Research Ethics System (CURES) prior to commencement of data collection*
- *Handle potential instances of research misconduct in an appropriate manner, including reporting to the appropriate person*

There were two data gathering stages in the project that involved external participants. The first stage has been gathering information about attack techniques. The exact paperwork that the participants had to fill is included in Appendix D. The second stage is the survey and the gameplay process, which is summarised in Appendix E.

Ethics has been paramount when designing the surveys and practical sessions, and the rest of this section will examine how ethics has been considered during information gathering stages, and how the gathered information was handled.

During the data-gathering stage, the core principle that has been followed is gathering only the strictly necessary information. In both studies, participants were

not required to disclose their backgrounds or any sensitive information about themselves, or their past or present work. One of the decisions that has been taken is not to gather the demographic information about the participants, as in the first study this was not the aim of the activity and in the second case the activity has been role-playing, therefore the demographic information is not critical. Although every care has been taken to spread the information about the studies only in the Discord and Twitter channels frequented by information security specialists and enthusiasts, these communities are open to the public, which means a person with any background can join them. This has been mitigated by not asking the participants about any experiences that may be considered sensitive. Due to the nature of the activity, which is role-playing, this has been a simple task, as most of the discussions focus on the adopted roles and the events that happen as part of the game. As part of this study, dark web forums were not considered as a destination for data gathering due to the demographic that frequents these forums, instead choosing safer alternatives. At the beginning of both studies, participants have been informed about how their data is stored, as well as how can they withdraw from the study if they wish to do so.

All studies have been designed in a way so that the users would only disclose the information that they are comfortable with disclosing. The questions were not requiring participants to share any sensitive information and the only personal data that was gathered were the email addresses.

Care has been taken when handling the information. AxCrypt (2021a) (free version) has been used to encrypt individual files. It uses AES-128 encryption(AxCrypt, 2021b). Data files have been shared in password-protected zip files to ensure secure transmission and storage.

For the first study, source files have been encrypted to prevent the disclosure of email addresses. The subsequent survey results were stripped of any identifying information and combined into single cohesive statements or paragraphs.

For the second study, all records have been anonymised by storing the associated names and numbers in a separate file. Individual differences have been gathered separately. All records have been given a unique participant number, which participants

were made aware of.

The role-playing world featured fictional countries, which avoided the potentially sensitive issue of country attribution. The role descriptions themselves did not involve any sensitive topics that could serve as potential triggers for some of the players, ensuring that the game experience is comfortable.

Summary

In this Chapter, we have explored the research philosophy and concluded that if a single philosophy had to be chosen to describe this research project, it would be *pragmatism*. Otherwise, the research objectives map to almost opposing philosophies - the game design aspect would map on to *positivism*, as precise data is important for producing a game in an academically rigorous manner. Another area of great importance that would benefit from positivism is establishing a framework that would allow the comparison of decisions from different individuals to each other. The rest of the objectives fit better with *interpretivism*, as recording the decisions will be done taking into account the participant's view of the TTPs and options in the game, and the researcher's interpretation of what the participant might intend with their course of actions. Translation of those decisions into the simulation will also be deeply affected by how the researcher perceives the decisions and the researcher will decide what needs to be included.

Next comes the research approach. We have examined *inductive* and *deductive* reasoning, and have established that the research once again splits into two halves with the game design being *deductive* due to us examining the evidence (past attack cases) and challenging the established expectations on how an attacker should behave, proving or disproving our hypotheses, while the game decisions translation to simulation would take an *inductive* approach, as we might not have a specific theory at the beginning, but by examining the data and finding patterns we can form a theory.

As far as the methods are concerned, the most notable ones are *surveys*, *case studies* and *focus groups*. *Case studies* have been chosen to populate certain parts

of the game. *Surveys* have been chosen to help with the game design and to gather additional personality data at a later stage of the project, with *focus groups* to help with choosing what scenario would become an adequate test scenario. The entire set of steps and methods is summarised in Figure 3.5.

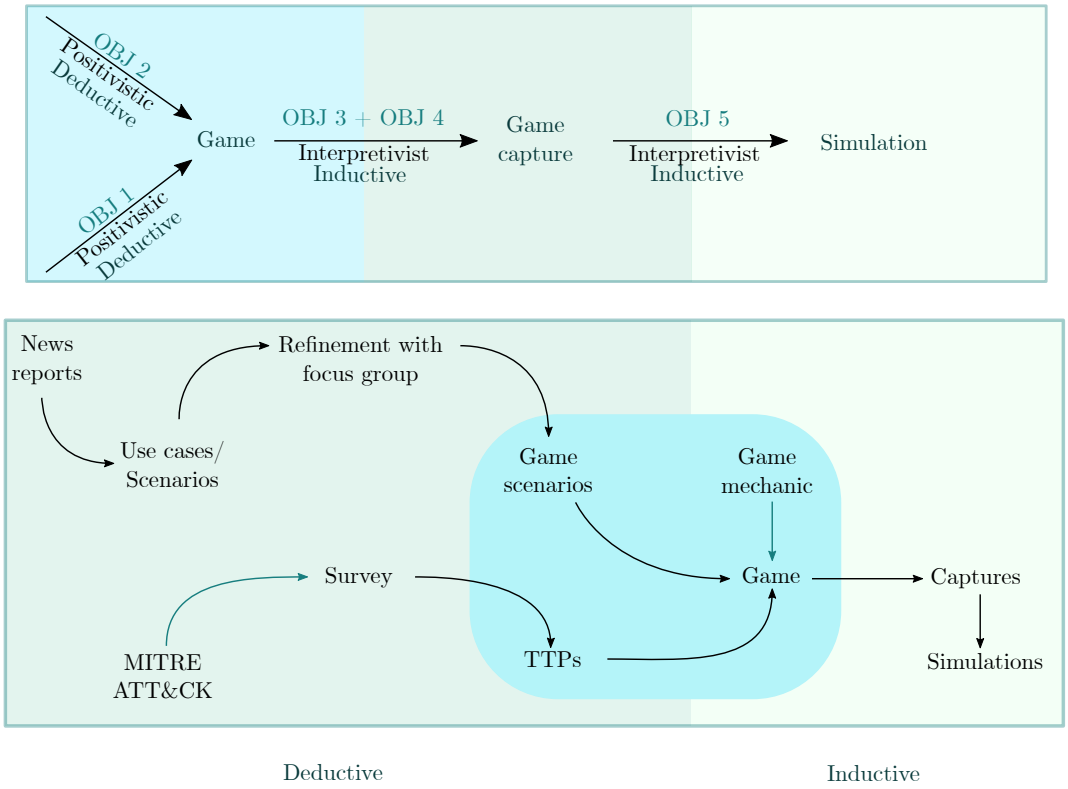


Figure 3.5: This diagram shows a summary of all research philosophies, approaches and methods employed in this project. The top half demonstrates what research philosophy and research approach does each one of the research objectives belong to, while the bottom half shows the transition of methods into game components and how do they all interact with each other.

Next, we have talked about assumptions, constraints and how will the project be validated at different stages, as well as why these specific methods were selected over other research methods, which is summarised in Table 3.1.

Finally, the last section has been dedicated to ethical considerations of the project, from adhering to Cranfield Research Ethics Policy to data encryption and ensuring participants are comfortable with the studies.

Chapter 4

Method: Board Game

> Playing a game is the voluntary attempt to overcome unnecessary obstacles.
>
> Bernard Suits

This chapter examines the process of designing a cyber attack board game. The chapter will open up by outlining the research objectives, followed by a discussion on deciding the optimal format the game should have. Next, the requirements for the game will be outlined and revisited again at the end of the chapter to demonstrate how they have been implemented. Following this, the three core aspects of the game will be explored in detail: the game mechanics, the game scenario, and the game cards. The next section will explore the mitigations that were in place due to the pandemic. This chapter will conclude with a summary, which maps the game implementation to the research objectives.

Research objectives

This chapter is dedicated to the fulfilment of the following research objectives:

1. *To build a realistic game based on rigorous evidence*

> 2. *To ensure that the game enables players to make decisions that reflect their true intention*

4.1 Game format

As mentioned above, this part of the project is dedicated to designing a game that allows decisions to be gathered in an engaging manner.

Initially, it was important to decide on the format the game should have. The possible options have been an online text-based adventure game or a board game. An open-world sandbox computer game would not be suitable for this task, as it would require developing the surrounding world, which would take a long time. Developing a visual novel instead would also require drawing the accompanying artwork, which would take time, hence a simpler online text-based adventure game has been considered instead. It also cannot be a shooter game, as it is a different game paradigm involving a different set of skills.

Using an ***online text-based adventure game*** would have allowed wider access to cybersecurity enthusiasts and experts, and the format of the online text-based adventure game would be appealing to command-line users, as it can be run from a terminal. That said, devising an online game would have inevitably led to a big portion of game logic being pre-determined, that is, the players would be limited in their choices, forced to choose from the available options rather than having the freedom to follow their own choices. The game cannot be entirely free-flowing, it still requires a certain structure to it. However, we are searching for a solution that would both provide this essential structure, but will also allow for more freedom than a set of pre-scripted choices. Plus, the research objective number two requires that the game enables players to make decisions that reflect their true intention. Therefore, it was decided that alternatives need to be sought instead.

The next game medium explored was a ***tabletop role-playing game (RPG)***. Tabletop RPGs are traditionally more open in the gameplay as they allow the games to be more free-flowing and no game is the same as any other game. An example of such games is Dungeons and Dragons (D&D), first published in 1974 and originally designed by Gary Gygax and Dave Arneson (Peterson, 2021). They involve

a moderator, who is called a ***Dungeon Master (DM)***. A DM plays the role of all non-playable characters and sets the state of the environment. Players in this game usually take one character that they play in a scenario set by the DM. Players and the DM roll special polyhedral dice that determine the outcome of a particular event. Since D&D, there have been variations of tabletop RPGs published, including the frameworks that allow designing custom tabletop RPGs with adjustable scenarios, such as FATE (Balsera & Engard, 2018). FATE focuses on the story and story building (Hicks, 2018), allowing players to collaborate and defeat enemies. In FATE, the Dungeon Master (DM) is called a ***Games Master (GM)*** instead. This abbreviation will be used subsequently to refer to the coordinator of the games. Frameworks such as FATE served as the inspiration behind the final version of the game that was designed in this project.

The use of the FATE framework was subsequently discarded, as in FATE players are required to collaborate and interact with each other. As mentioned in Section 3.5, this project does not focus on interactions between malicious cyber attackers, that is, the player can represent an entity, such as an APT group, but players will not interact with each other, and one role will be portrayed by a single player, as opposed to a team of players. In this scenario, hacking would be an activity that is usually done alone. Alternative game architectures have been sought using BoardGameGeek (2018b) as a resource to find games on. Another notable example that has been suggested by a colleague (and appeared in the BoardGameGeek list) is Android Netrunner (BoardGameGeek, 2018a). This game could be considered as an opposite of a tabletop role-playing game, as here the game mechanics are reliant on decks of special cards drawn by players instead of the GM taking all decisions. The game features two opposing sides, which are the big corporations and the entities known as '*netrunners*', who may transfer their consciousness into a virtual world. The goal of netrunners is to break into the network of large corporations, while the goal of the corporations is to defend themselves from those entities. The hacking aspect in the game is very abstracted, having very little resemblance to its real-world equivalent. On the contrary, the mechanics of the game has been well thought out, resulting in a set of complex rules and multiple decks, each serving their own purpose.

FATE and games similar to Android Netrunner provide the two opposite paradigms as FATE is controlled almost entirely by the GM, while Android Netrunner achieves the same with the use of game cards. Neither of the two ends of the spectrum have been deemed suitable for the game in this project. If the game is played without a set of cards or any other tokens, then the game is at risk of drifting away from the required objectives. Completely removing the GM from the game places a big load on the player to familiarise with the rules and mechanics of the game. If game sessions are to be kept short, it is better to make rules simpler so that the players can get from being introduced to the game to playing the game in the shortest possible time span. Moreover, the GM in the game adds to the element of unpredictability for the player, as no two sessions will be the same, just like no two cyber attacks are the same. Thus, the final approach has been to use a custom framework, that has the single-player element of Android Netrunner (it is completely possible to do a game between a single netrunner and a single corporation, as opposed to multiple netrunners attacking the same corporation, or multiple corporations being attacked by the same netrunner), but the GM and interactions of the FATE system. This approach will subsequently be referred to as the ***single-player*** (in terms of interaction) ***tabletop RPG***.

4.2 Setting requirements

In the light of some constraints for the game, now is a good time to formalise what key components of the game need to be in place, and to understand if additional requirements need to be formulated before moving on to the game implementation.

4.2.1 Educational game criteria

In Chapter 2 a set of criteria for educational games, first defined by Whitton (2010, p. 31) has been briefly mentioned. These criteria will be used to ensure that the game conforms to the standards of an educational game:

- the goal to achieve an outcome that is superior to others *(competition)*;

- tasks that require effort and are non-trivial *(challenge)*;
- a context-sensitive environment that can be investigated *(exploration)*;
- the existence of a make-believe environment, characters or narrative *(fantasy)*;
- measurable results from game play *(scoring)*;
- explicit aims and objectives *(goals)*;
- action in game that changes the state of play and generates feedback *(interaction)*;

As a reference, the framework by Arnab et al. (2014) (Figure 2.6 in Section 2.4.2) will be used to apply different learning and game mechanics to the finished game to see if the number of mechanics is an acceptable balance. A balance is deemed acceptable if the game is deemed fun by the participants, while achieving the intended outcome.

4.2.2 Game functionality essentials

To design a functional game we will need three core aspects. The first one is the game scenario, to provide players with motivations and create a setting that allows them to distance themselves from reality. The second aspect is game mechanics, which would determine how the game should be played. The last aspect is game resources - a medium that enables the game mechanics while incorporating elements from the game scenario.

In Section 4.1 we have explored how the high-level game format was decided. We will be using a game that uses both the GM mechanics and cards mechanics. Much like in Android Netrunner we will have two entities - the 'hackers' and the 'organisation' that the hackers will attack. The organisation will be a defending party, and the GM will represent the organisation. This decision was taken due to the organisation a priori having a lot more insight into the attack, such as what has been accessed. Consequently, this makes the organisation player more difficult to

learn. Furthermore, players from this category would not provide useful answers to the research question, as it is out of scope to study defensive actors.

The ***game mechanics*** choice should reflect this idea of the two sides, the player and the GM, a hacker and an organisation. The game would be turn-based, both sides need to have some means to interact with and modify the game state.

The ***game scenario*** should provide many different choices to the players so that the roles offered in the game are believable and motivations seem realistic. The scenario would put the game mechanics into context, contributing to the fun element of the game, making it more engaging.

In light of the decision that the game will require some pre-determined elements, a certain amount of game ***cards*** would be required. Cards were chosen for their relatively small size and ease of use, their ability to display necessary information in a note format. The decision on what decks needed to be used largely depended on the minimum elements of the game mechanics that were required to be present in the game.

4.3 Refining game mechanics

In Section 4.1 we have established that the game we are developing is a single-player tabletop RPG with an offensive and a defensive side. Offensive actors attempt to capture resources to advance their goals by using techniques, while defensive actors protect those resources and are trying to stop offensive actors by using counter-techniques or defensive measures.

4.3.1 First prototype

To work out what game mechanics elements would be required, the first prototype of the game has been developed on post-it notes. The use of post-it notes has helped to ensure that the focus is on the interactions between the cards, as opposed to their appearance. This process is illustrated in Figure 4.1.

Initially, the following decks have been defined:

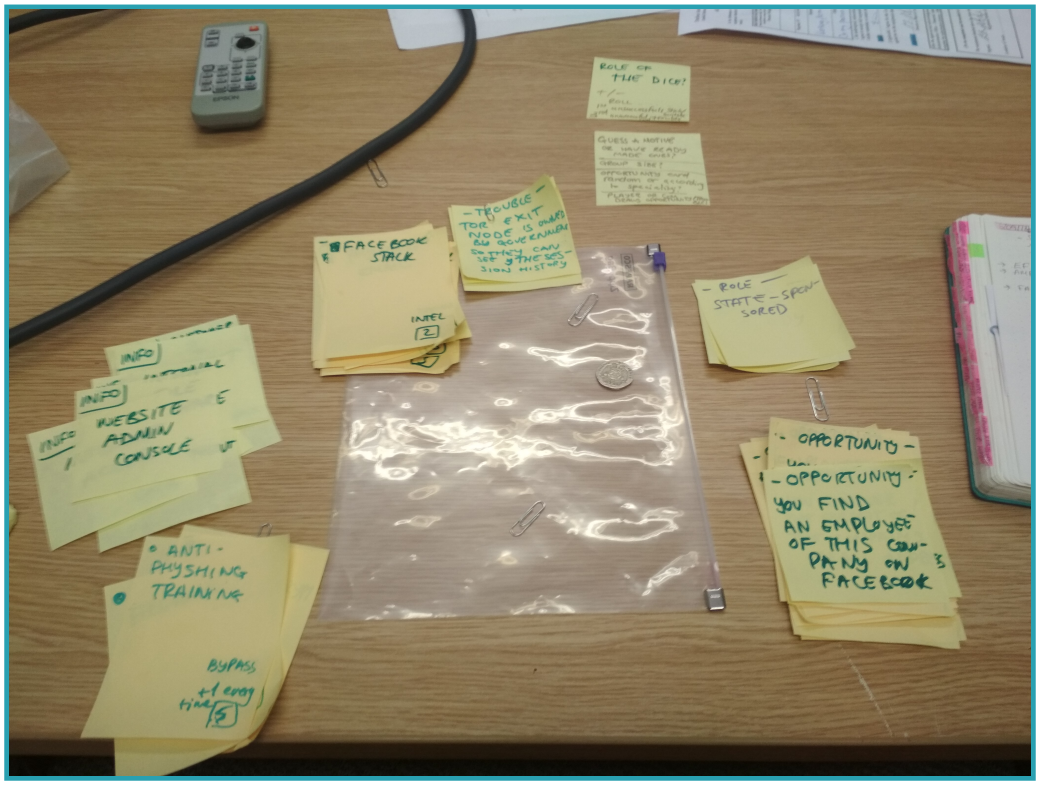


Figure 4.1: Early game prototype. On the photograph, from left to right, top to bottom: Info deck, Technique deck, Trouble deck, Role deck, Counter-technique deck and the Opportunity deck. A 20p coin can be seen next to the Trouble deck, that was intended to be used as a success determiner.

Role A role is assigned to each player at the beginning of the game. At this stage, it was decided to make it either a deck or a list, allowing the players to select a role. An example role is 'Script Kiddy'.

Motivation This was designed to be a standalone deck, although the possibility of it being a list was also considered. Each motivation has a list of roles it can be applied to since not all motivations apply to every role. Those cards can be used as a reference or an own motivation can be devised instead. During the first prototyping stage, the possibility of the GM guessing the motivation was being considered. The motivation determines what information or actions are needed to win the game. An example motivation would be 'Hired to take down the competitor' with an example list of suitable roles being 'Script Kiddy', 'State-backed', 'Cyber mercenary'.

Technique A list of TTPs, each technique made into a card with additional information. Each card can be played as many times as needed. An example Technique card may be 'SQL Injection' or 'A Phishing Email'.

Counter-technique This is an elaborate list of defensive or mitigating measures that counter malicious cyber activity on a target and are the ones that the defending company may use to protect itself from attackers or to mitigate the impact of an attack. An example Counter-technique card can be 'Anti-Phishing Training' or 'A Firewall'.

Opportunity The second most important deck after the 'Technique' deck. These can serve as hints or plot points and can be used to increase or decrease the pace of the game, as well as guiding less-experienced players. An example Opportunity card can be enabling physical access to the building as a consequence of a player discovering a dropped access key card.

Info Pieces of information uncovered during the course of the game. Example Info cards may be 'Directory Structure' or 'Company Intellectual Property'.

Action Initially, it was planned that a player would take a card out of the 'Action' deck and act according to what was written on that card, but there was

already a similar mechanic in place for the 'Opportunity' cards. Ultimately, this element has been discarded.

Trouble After a number of unsuccessful coin flips a player may earn a 'Trouble' card. Trouble cards can be replaced by 'Consequences' and represent technique or the whole hacking session going wrong. An example text on a Trouble card can be *"You forget to connect to a VPN while leaving your IP exposed"*. An example condition could be *"Your IP is exposed in the intrusion detection system logs. Expect law authorities at your door."*

In addition to the decks, two other elements helped with the flow of the game and/or added a useful contribution to the lore of the game.

Company fact file An information sheet presented in form of a Wikipedia printout that provides players with some initial information about the company they will be attacking.

A coin An element of randomness, which is often a die or a pair of dice. A coin produces a binary outcome - heads or tails. The coin is used when a player decides to use a Technique card and determines whether the technique succeeds or fails, depending on which side will the coin land on.

4.3.2 Second prototype

Since the first concept the elements of the game mechanics, as well as the decks have been slightly modified. In the next revision, the cards have become fully playable, some decks have also been discarded or merged with other decks for simplicity. The second prototype can be seen on Figure 4.2.

In this revision the following changes have been made:

Role Role cards are now tied to the scenario, with each role goal being related to the target person, organisation or infrastructure. This allows switching scenarios and roles to fit a specific use case.

Motivation This deck has been integrated into the Role cards as role-specific goals.

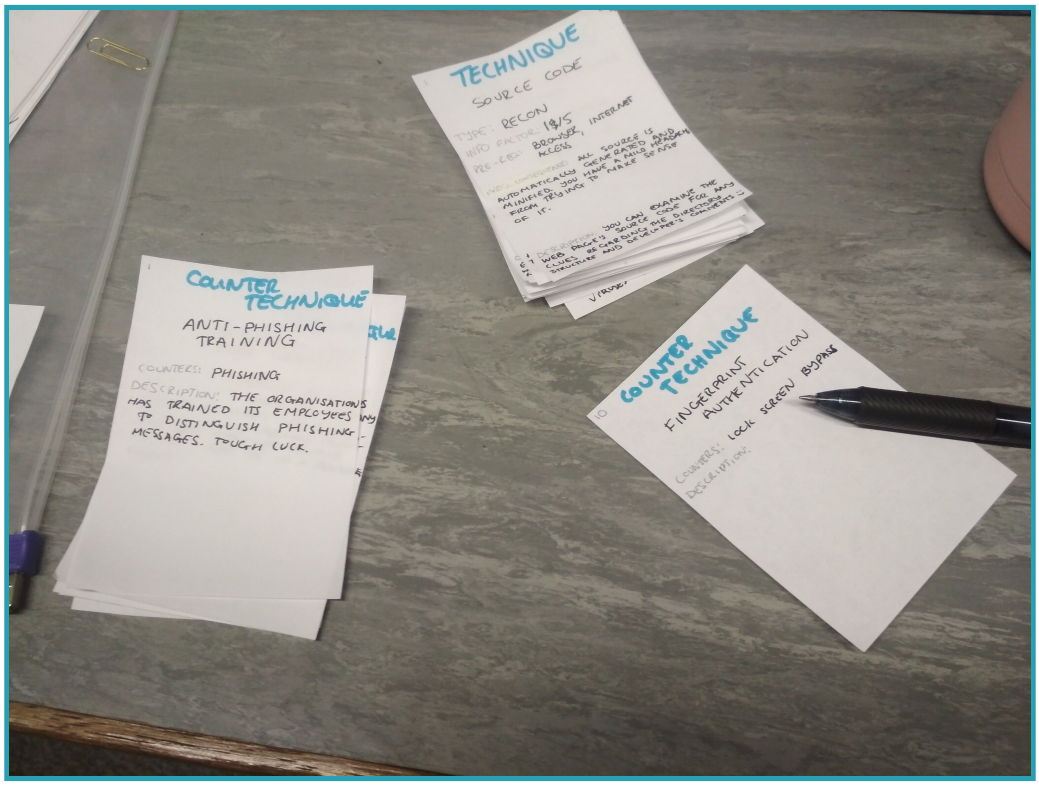


Figure 4.2: Second game prototype. Compared to the first prototype, this version included more cards, the objective was to make this version playable. The first version did not contain enough cards, thus it was just a concept.

Trouble This deck has been integrated into the Technique cards themselves as a negative consequence if the technique fails.

In addition, a coin has been replaced with a standard six-sided die to allow more complex success/failure scaling. This will be explained in the game cards section.

Role decks are now tied to a specific scenario, making them part of a ***role-scenario pack***.

4.3.3 Final version

The mechanics established in the second prototype have served as a base for the final game version. From that stage, only the scenario, the appearance of the cards and sometimes certain fields on the card have been changed. For example, the 'Counter-technique' deck got renamed into 'Countertechnique', and the 'Info' deck has become the 'Information' deck.

Another important change since the second prototype has been related to Opportunity cards, namely that now they have one or more Information cards that the player gets together with the Opportunity card. It is now a mechanic that allows players to get free Information cards.

4.3.4 Impact and Recon factors

Each Technique card gets two special numbers assigned to it that are used as essential components for calculating several elements of the game mechanics.

The first element, the ***Impact Factor***, refers to consequences caused by the technique in the physical world as opposed to virtual. It is difficult to translate the damage from a cyber attack into a tangible equivalent, therefore a relative metric was used instead. The higher the Impact Factor, the greater is the tangible effect of a specific technique.

The second element, the ***Recon Factor***, is used to indicate how much useful information this technique provides to its user.

Both values are measured on a scale of five, as each of these values were adapted from survey questions with a Likert scale (No impact, Little impact, Some impact, Significant impact, Critical impact).

These definitions for Impact Factor and Recon Factor will be used in subsequent sections.

4.3.5 Cyber Kill Chain stages

First introduced in Section 2.4.2, the Cyber Kill chain has been used to classify different techniques into categories. The exact version of the Kill Chain that has been used has been the NCSC (2016) Kill Chain, as opposed to the Lockheed Martin Kill Chain, which consists of seven stages, the NCSC version consists of just four - ***Survey***, ***Delivery***, ***Breach*** and ***Affect***. These stages have been used as an indication of how impactful the technique is, as well as how many Risk points need to be assigned to it.

4.3.6 Risk Appetite

Not all roles are created equal in this game. The game assumes that a Script Kiddy would not possess the same capabilities that a State-backed actor has. To distinguish the roles from one another they are given a different amount of ***Risk Appetite***, a consumable resource, which acts as 'health' in the game, i.e. spending the entirety of this resource would equate to losing the game. Each player starts with an initial Risk Appetite number that diminishes should a Technique they decide to use fail.

Each Technique card has a cost associated with execution, hence a higher Risk Appetite means more freedom to use more costly or effective TTPs, while a lesser Risk Appetite would restrict the player with the techniques they can have in their arsenal. In case the technique succeeds, they gain one Risk point back (provided that their Risk point balance is not greater than their initial Risk Appetite, which is printed on the Role card), cascading successful attempts will get two points back instead. In case a technique is unsuccessful - a player will lose the number of points printed on the card.

First of all, let us explore how the risk points have been assigned to each Technique card. There are two key values present on each Technique card - $factor$ and *category*. The combination of these two is mostly unique[1] for Technique cards. Here, $factor$ refers to Impact or Recon factor (if both are present, they are averaged), and has been explored in Section 4.3.4. This value is coupled with *category*, which represents the simplified Kill Chain stage of a technique. Each Kill Chain category has been assigned a weighting based on the potential effect that it can have on the target, the greater the effect - the greater is the weighting. The exact weights are shown in the conversion table (Figure 4.1).

The product of $factor$ and *category*, P, takes into account how far down the attack chain the technique is, as well as how effective (and risky) it is to execute it. This product (see equation 4.1) can be used to classify the techniques into the following risk brackets: no risk (green), low risk (yellow), medium risk (orange) and

[1]Duplicate values are possible for techniques in the same stage of the Kill Chain with similar Impact or Recon factors, but these cases are expected to be a rare occurrence and will still provide a value suitable for the purpose described.

category	**Numeric Value**
Survey	1
Delivery	2
Breach	3
Affect	4

Table 4.1: Category to number conversion. Represents the increasing cost as a player goes down the Kill Chain.

high risk (red).

The matrix is available in Table 4.2.

$$P = factor \times category \tag{4.1}$$

	factor				
category	1	2	3	4	5
1 (Survey)	1	2	3	4	5
2 (Delivery)	2	4	6	8	10
3 (Breach)	3	6	9	12	15
4 (Affect)	4	8	12	16	20

Table 4.2: An even-subset risk matrix. There are four colour categories - green, yellow, orange and red. Each colour category represents the risk severity, with green being least 'risky' or severe, and red being the most severe. Every colour subset has an even amount of elements inside.

Thus, a Technique card gets its risk number according to its Kill Chain stage and its Impact/Recon Factors. Further down the kill chain steps become more critical, as an unsuccessful attempt might mean a lost connection and the necessity to try again. Additionally, there is a potential to get discovered, as the attack is happening over the target's network. The target organisation may have intrusion detection systems that will generate the alerts, or there might be incident response teams that will be able to detect the intrusion. Hence, the risk is greater in the later stages of the kill chain.

The second step is to decide on the exact number of Risk points for each role. For this, a two-stage process has been carried out. The objective of the first step is to estimate the baseline number of points, the minimum amount that would be necessary in case of a successful outcome to complete the game. To do this, we first

arrange the techniques in order of their Cyber Kill Chain stage and make sure some important statistics are also visible. This is summarised in Table 4.3.

Kill chain stage	Name	Roll number	Risk points	Probability of failure	Average points lost per kill chain stage
Survey	Credentials from Web Browsers	3	2	1/3	
Survey	Man in the Browser	2	1	1/6	0.33
Survey	Steal Web Session Cookie	2	1	1/6	
Delivery	Drive-by Compromise	3	2	1/3	
Delivery	Exploit Public-Facing Application	2	2	1/6	
Delivery	Spearphishing Link	3	2	1/3	
Delivery	Spearphishing via Service	3	2	1/3	0.50
Delivery	Trusted Relationship	3	2	1/3	
Breach	Browser Extensions	3	2	1/3	1.08
Breach	Web Shell	4	3	1/2	
Affect	Domain Fronting	3	4	1/3	
Affect	Exfiltration Over Alternative Protocol	4	4	1/2	1.78
Affect	Exploitation for Client Execution	4	4	1/2	
				Total average:	**3.69**

Table 4.3: Each Technique card split into a Kill Chain stage with a probability of failure calculated. The number of lost points is calculated by summing up the probabilities of failure

The 'Risk points' column is self-explanatory, but to understand the subsequent stages, it is worth explaining how the ***probability of failure*** and the ***average number of points lost*** are calculated. First, let us examine the probability of failure. Each Technique card has a Risk number. In addition to the Risk number, a Technique card also has a Roll number, which is the minimum number that needs

to be rolled on a six-sided die for a technique to succeed. The reasoning and steps to generate the Roll number will be explained later. Therefore, if the Roll number of a specific Technique card is *3*, if a die lands a *1* or *2*, the Technique will fail, and if the die lands on a *3* or above - the Technique will succeed. To summarise, the probability of success is $\frac{4}{6}$, while the probability of failure is $\frac{2}{6} = \frac{1}{3}$. If we multiply this probability with the number of Risk points of each technique and sum them up, we will get the average number of points lost, which is the last column in Table 4.3. A sample calculation is given below:

T1 Risk: 2, Probability of failure: $\frac{1}{3}$, T1 Average points lost:

$$2 \times \frac{1}{3} = \frac{2}{3}$$

Following the same procedure we calculate the same for T2 and T3.

T2 Average points lost: $1 \times \frac{1}{6} = \frac{1}{6}$

T3 Average points lost: $1 \times \frac{1}{6} = \frac{1}{6}$

$$\frac{\frac{2}{3} + \frac{1}{6} + \frac{1}{6}}{3} = \frac{1}{3} \approx 0.3\dot{3}$$

Next, a CDF graph (Figure 4.3) has been plotted using the probabilities calculated in this table. The graph was created using NCSC Kill Chain as a guide, i.e. it was assumed that completing a Kill Chain stage would be equivalent to completing the game, and to complete a single stage of the Kill Chain, e.g the Survey stage, only one successful technique would be enough. Random games were then generated by randomly sampling a technique from the relevant stage of the Kill Chain and attempting to succeed at the technique (succeeding at the technique means a simulated die roll outcome would be greater or equal to the Roll number of the technique). If the roll is successful, the simulation moves to the next Kill Chain stage, if the technique is not successful the simulation randomly selects another technique in that stage. This continues until a technique has been successful in each stage of the Kill Chain. To summarise, this CDF graph represents a player randomly choosing Technique cards rather than a well-planned out and structured attack, but provides

an estimate of the probability of success for a given number of Risk points. These estimates can then be used to allocate the starting Risk points for each role.

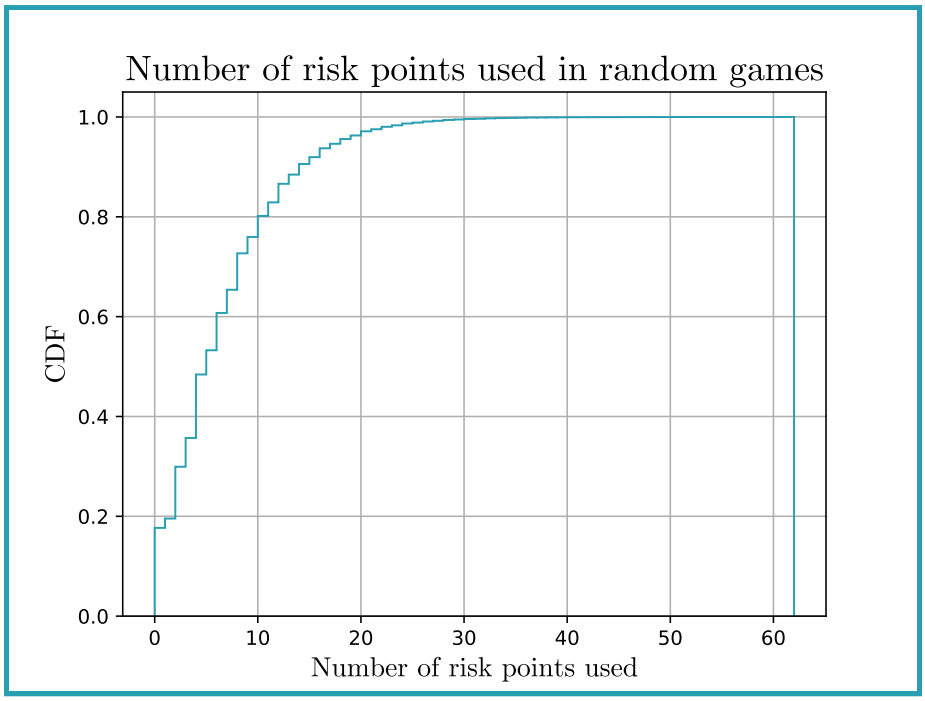


Figure 4.3: Optimal points number CDF graph.

The second stage of deciding an optimal number of Risk points for every Role card has been to vary the number of Risk points for every single role to make it unique, using **10** as a baseline number of points (as the success rate reaches 80% after 10 points with randomly picked techniques for each stage, as shown on the graph in Figure 4.3). We want to minimise the chance of success if the techniques are picked at random, and make it so that it is only possible to win the game by carefully considering Technique cards and strategising. Below ten points the probability of winning the game by using a set of random techniques drops significantly, hence this number of points is suitable for our purpose. Next, Risk Appetite points are allocated to roles in order of their capability.

The idea of different roles having differences in their Risk Appetite has been alluded to in previous paragraphs. Coming back to the earlier example: if we would rank a Script Kiddie and a State-Backed actor, a Script Kiddie would have fewer Risk points. This is due to a couple of factors. First of all, not only their capability is not that of a State-Backed actor, but also there are more consequences

to an individual if they are discovered by law enforcement forces, as opposed to this individual being a part of a Nation-State group. Since it is a Nation-State group, there is a possibility that the group will be protected by the State, kept secret, or identities of individuals within the group will not get disclosed, and the attribution by external experts would be more generic (as they will be focusing on attributing to a country or a nation, as opposed to the individuals within).

4.3.7 Minimum Roll number

As mentioned above, the primary reason for replacing a coin (binary outcome) with a six-sided die was to allow for a more accurate representation of attack techniques further down the Kill Chain. To be more specific, techniques that are in later stages of the Kill Chain have a smaller chance of success due to them being high-risk. To reflect this in the game, an additional metric has been introduced to every Technique card - a minimum number needed to roll for a particular technique to succeed. Impact and Recon numbers also play a part in the Roll number.

Firstly, the *factor* and *category* are also present here, and just like the Risk number calculation, the *factor* is the average of the Impact and Recon factors, and *category* is the Cyber Kill Chain stage translated into a number. The sum of these two factors is the overall weighting of the technique, i.e. how significant is this particular technique at this stage of the Kill Chain. The sum is modulated to ensure the result does not exceed *6*, so that a six-sided die can still be used.

$$min\ roll = \left\lceil \frac{factor + category}{2} \right\rceil \tag{4.2}$$

Let us look at a sample application of this formula. Taking a technique with an Impact of 3 and Recon of 3 in the Affect stage (4) we would get the following Roll number:

$$ave_{impact \cup recon} = \frac{3+3}{2} = 3$$

$$min\ roll = \frac{3+4}{2} = 3.5 \approx 4$$

It is worth noting that any non-integers get rounded up to the nearest whole number, like in the example above.

4.4 Creating the scenario

Creating a fictional setting plays an integral part in board game design. The human brain is able to distinguish fiction from the truth, as there are different parts of the brain responsible for recalling truth and fictional events (Abraham et al., 2008). Thus, when put into a fictional context a player can disassociate themselves from reality. Having this fictional world can also prevent any sensitive topics such as politics and religion from being brought up.

An initial prototype of the fictional world, together with a game map, nations and motivations has been created with FATE game mechanics in mind, shown in Figure 4.4.

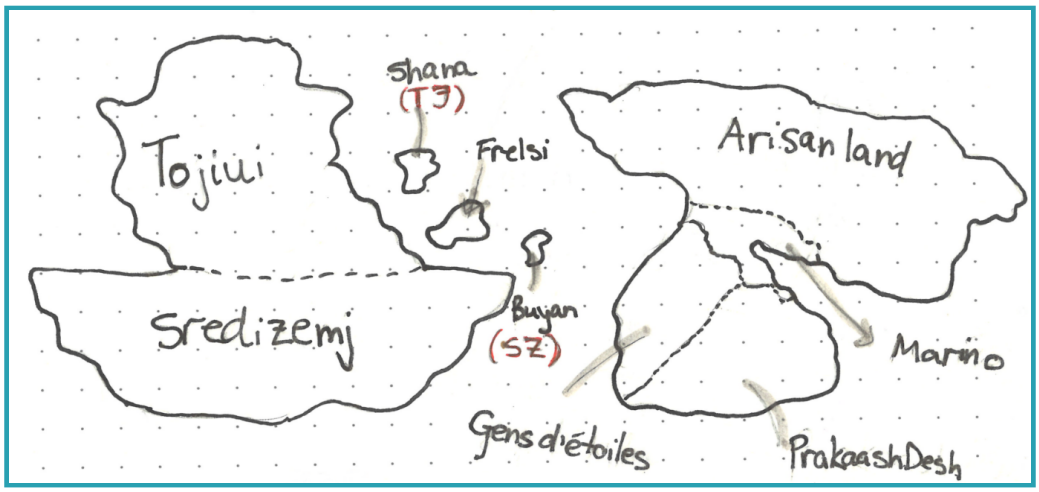


Figure 4.4: A discarded concept of the fictional world. It included countries with various governments to allow a broad range of malicious actors to emerge from all types of backgrounds. It was developed for FATE, which later turned out to be infeasible for the project.

As mentioned in Section 4.1, the use of FATE has been discarded later, making space for a more simple tabletop RPG version. To model nation-states there was a need in:

- A hostile country
- A small neighbouring country

The rest was improvised. The final map is shown in Figure 4.5. Full scenario is available in Appendix F.2.

Figure 4.5: The updated game map. This map contains just four countries - Circle-Land, Rectangle Country, Hexagon Republic and Triangle Overseas Territory (TOT). The organisation that the players are attacking is located in Rectangle Country. A bigger version of this map is available in Appendix F.2.

4.5 Creating game cards

As the objective is to create the game in an academically rigorous manner, the accuracy of the supplied information is paramount. While the information for the other decks can be tailored to fit particular scenarios, the deck of tools techniques and procedures has two potential routes of development - the 'wildcards' approach and the 'all techniques' approach.

The *'wildcards'* approach is when players are supplied with blank cards, which allows them to write the technique name and its characteristics on the blank card

to be able to use it one or more times during the game. This approach allows the freedom to use any technology, including ad-hoc scripts. Additionally, it allows players to make cards, as opposed to making cards for the players.

However, the fact that players themselves create those cards also implies that the abstraction level of the techniques will vary, making recording the gameplay harder. Furthermore, scenarios where two players define the same attack technique but to different abstraction levels also need to be considered. It is also important to define what should happen to the cards once players are finished with them, and there are two options: re-using the cards for future games and requiring players to make new cards with every new game. If the re-use will happen, strategies for de-duplicating techniques and maintaining a constant level of abstraction need to be outlined and specified. Another issue that may potentially arise from this is the fact that the GM may not be familiar with a technique proposed by a player. The players, in turn, may go a step further and devise imaginary techniques with imaginary characteristics to achieve the win conditions quicker and 'cheat' the game. The Games Master has to be able to verify the information supplied by the players, potentially extending the game duration and placing a further load on the GM. Lastly, less experienced players may be challenged by the need to create their cards.

An alternative approach is the ***'all techniques'*** approach, which involves players being given an extensive list of Technique cards in which they can search and select the technique that applies best to the current situation. This approach allows less experienced players to use an attack technique that they know as opposed to coming up with a technique, which may prove to be a far more challenging task. This approach also ensures that the techniques use the same abstraction level, as well as giving the Games Master a chance to familiarise themselves with a technique before the game.

This approach does not come without problems. For example, there is a need to obtain the techniques from a reputable source, however by the time the cards will get printed the source may update again due to a high volume of security breaches occurring every year. The need for the TTPs to stay current would imply that the Technique cards would need a regular update - expansion packs, which would

make searching through them even more difficult. Some players may also find it challenging to use the techniques provided, as they may be used to different names of this technique or they may be using their custom scripts, which will not be present in the master list of techniques.

It has been decided that the 'all techniques' approach would be chosen for the game implementation, as it allows the techniques to have the same abstraction level, as well as letting players with less cybersecurity experience to participate. Having a fixed list will help the GM to familiarise themselves with the toolkit, which in turn will help in providing players with guidance. Additionally, it will ensure that games follow a fixed structure, yet providing enough variety for different scenarios and different playstyles. Rather than having various game completion routes pre-coded it will allow different game scenarios to develop, while still being structured. Having such a structure in place aids the conversion of recorded gameplay into the simulation.

4.5.1 Deck population strategies

Previously, we have established that the game is going to have the following decks:

Role Outlines the roles that apply to this specific scenario.

Technique Effective TTPs that can be used to achieve player's goals

Countertechnique Mitigation/defence measures that the targeted organisation can use to defend itself

Information Tokens that players unlock during the game. Examples include passwords, system information, access to servers.

Opportunity A tool for the GM to advance the game when a player is stuck or confused. Contains non-standard methods to obtain Information cards, such as abusing the trust of the target, social engineering, exploiting the human factor.

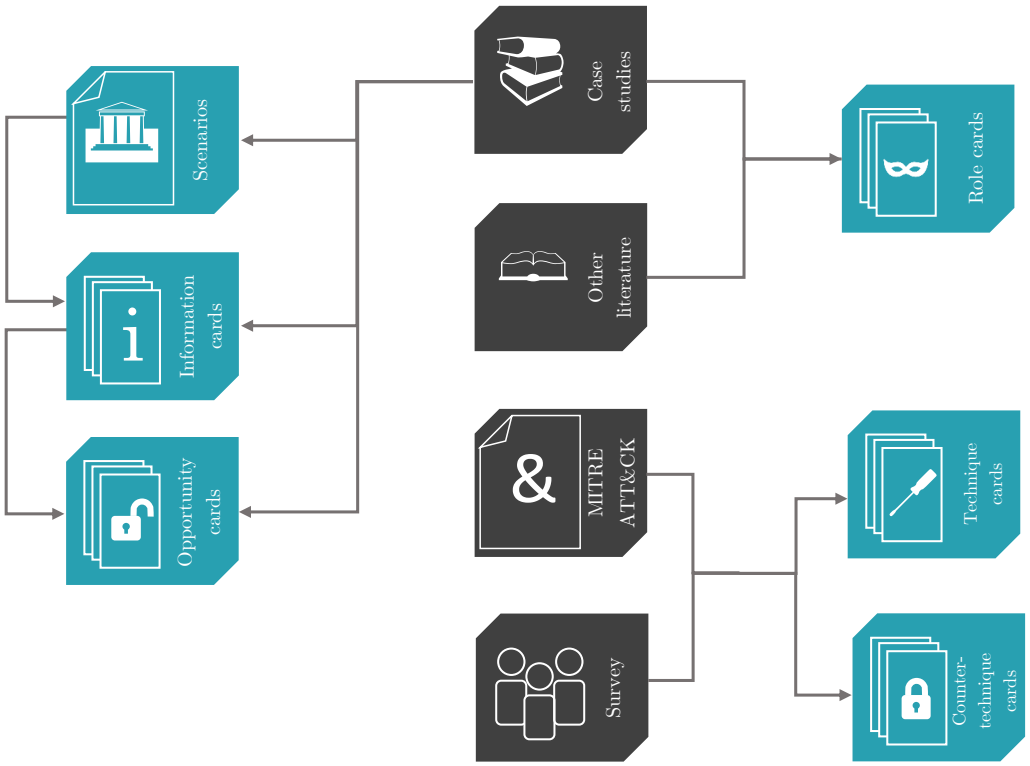


Figure 4.6: Information sources diagram. Past news stories are used to inform Opportunity cards, Information cards and inspire the Scenarios. Roles are sourced from the literature and news stories. Technique and Countertechnique cards are sourced from the survey and MITRE ATT&CK taxonomy.

Figure 4.6 shows the information sources for all of the card decks. For the ***Role*** deck, attacker types were sourced from Section 2.2.1 of the Literature Review chapter. All of the archetypes are listed below:

- Counter-culture
- Hacktivist
- Script Kiddy
- State-backed
- Cyber Mercenary

Individual player goals along with the role descriptions were sourced directly from the game scenario.

Before we proceed any further, let us explore two of these information sources in greater detail. The first of the two sources is MITRE (2021a) ***ATT&CK Taxonomy*** (Figure 4.7). ATT&CK stands for ***A***dversarial ***T***actics, ***T***echniques, and(***&***) ***C***ommon ***K***nowledge. It is an attack taxonomy that gets renewed bi-annually. It was initially developed in 2013 to track common Tools, Techniques and Procedures (TTPs). Initially used internally the framework went public in May 2015. The purpose of the creation of this framework is similar to the current project - documenting adversary behaviours. Mitre had several key issues that needed to be addressed (Strom, 2019):

1. *Detecting behaviours, as digital footprints, such as IP addresses and file hashes did not accurately represent how adversaries interact with systems*
2. *Existing adversary lifecycles and Kill Chains were too high level*
3. *TTPs needed to be based on real incidents to show the framework is applicable to real environments*

4. *TTPs need to be compatible across different groups using the same terminology*

Figure 4.7: Mitre ATT&CK taxonomy. Each table cell represents an attack technique, each column corresponds to a category, such as 'Defence Evasion'.

The ATT&CK taxonomy was chosen for a number of reasons. The first reason is that it is one of the only attack technique frameworks available at the time of writing. The second reason is its frequent updates, allowing the list of TTPs to always stay current. The third reason is a generous procedure examples list, so it is possible to trace every single TTP to when it was first observed to be used by attackers, and what kinds of attackers usually use it. Lastly, this list is coming from a reputable organisation.

The second on that information sources list that needs to be addressed is the ***survey***. As the Mitre ATT&CK framework did not provide enough information to complete the Technique cards deck, it has been decided to source the missing parts of the card, such as the Impact factor and Recon factor, explained in Section 4.3.4, as well as the consequences – what would happen to the user if the technique goes wrong, and pre-requisites – what items or conditions need to be in place for the technique to run.

A Delphi approach (Rodney L. Custer, 1999) was initially chosen as a method to populate the cards. Here is an example application of Delphi used for formulating an agreed definition:

1. A group of experts is gathered (this may be done anonymously)
2. Each of the experts is presented with an initial definition or a question that they need to answer relating to the topic
3. Experts write their definitions
4. In the next round those definitions are gathered and a common theme is extracted
5. Experts are presented with the common theme and an opportunity to change their answer
6. Experts may amend their answer
7. Last three steps can be repeated as many times as needed
8. A definition is extracted

The Delphi study has been designed and launched, but the response rate was very low (only two responses). Due to the lack of responses, it has been decided to discard this approach and substitute it with a single pass survey instead, as well as to open it up to a larger group of participants, as the Delphi study has only been open to academics with an interest in cybersecurity research.

The survey is available in Appendix G. Once the administrative part of the survey is filled out, participants are presented with categories that they are the most familiar with. Techniques inside these categories can overlap with each other, but this way participants are not overwhelmed with all of the techniques at once. Once a participant selects a specific category, they are presented with techniques that apply to this category. For each applicable technique that participants select, they need to answer four questions for the four technique characteristics mentioned above. A remark that needs to be made is that for brevity, the "Per technique I" block repeats for every technique in every question category (e.g. Web, Code execution, Privilege escalation, etc.), but is identical to the block included in the survey.

Survey participants were chosen by snowball sampling (Gray, 2004, p. 325). A tweet with the survey link was posted, as well as posting it (with permission) on various information-security themed Discord servers. Discord was chosen as it allows the creation of focused communities (servers) and multiple cybersecurity communities have a presence there.

Participants were optionally entered into a prize draw with two categories of winnable prizes - the first category had Amazon vouchers on offer, while the second category had a more tailored set of prizes - 1 month of PentesterLab (2021) and 1 month of HackTheBox (2021), both are services that provide virtual labs and help enthusiasts and professionals to strengthen their knowledge. A paid subscription to these services provides significant benefits to novices or professionals alike. Figure 4.8 shows the distribution across the communities.

Service	URL/Joining link	Reward offered
Twitter	https://twitter.com/tasidonya/s	£50/£30 Amazon Voucher
Discord	N/A	£50/£30 Amazon Voucher
Discord	https://discord.gg/hRXnCFA	£50/£30 Amazon Voucher
Discord	https://discord.gg/trustedsec	£50/£30 Amazon Voucher
Discord	https://discord.com/invite/32Z	1 Month PentesterLab sub/1
Discord	https://discord.gg/V8EXEkr	1 Month PentesterLab sub/1
Discord	https://discord.gg/REfpPJB	1 Month PentesterLab sub/1
Discord	https://discord.gg/Kgtnfw4	1 Month PentesterLab sub/1
Discord	https://discord.com/invite/ewq	1 Month PentesterLab sub/1
Discord	(link is not publicly accessible)	1 Month PentesterLab sub/1
Discord	https://discordapp.com/invite/	1 Month PentesterLab sub/1

Figure 4.8: List of Discord servers and a Twitter page

Surveys with different reward categories were kept separate to avoid this difference in prize categories affecting the data. The survey has run for about a month to two months (both versions). Short Python scripts were created to process survey data. The first file has extracted just the information relevant to the game, while the

second file put the information into a more readable data format. Dataset matching and removal of malformed responses were done manually. Figure 4.9 shows the entire process.

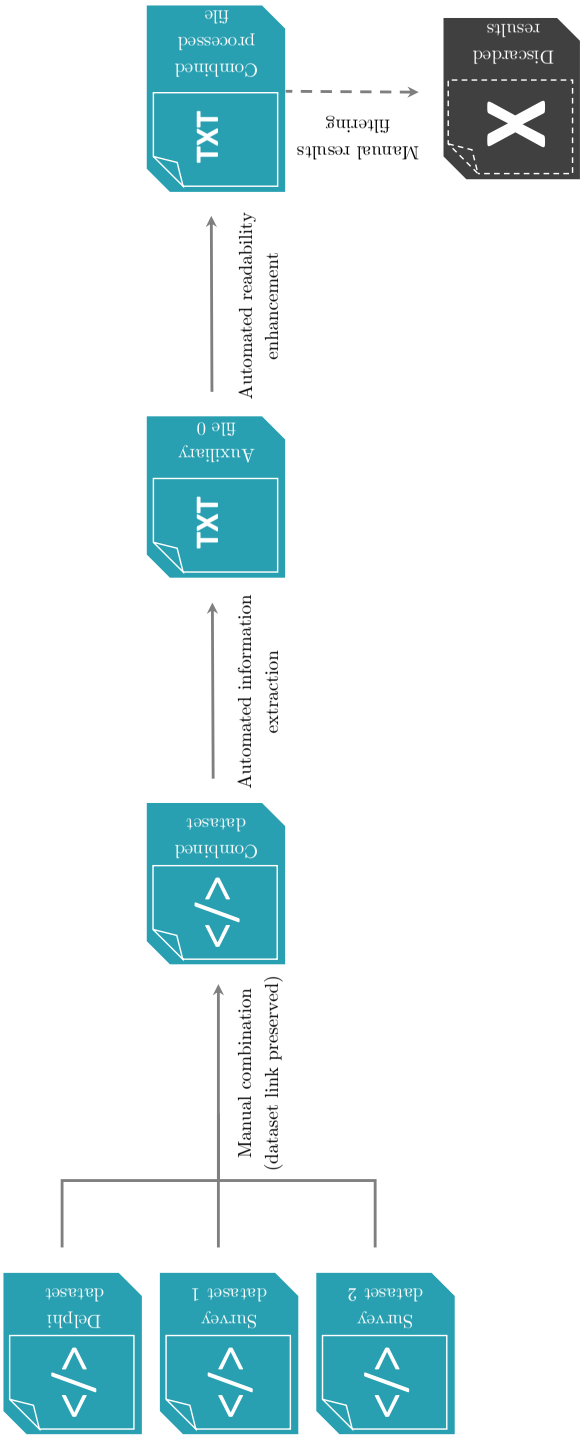


Figure 4.9: Dataset processing strategy

The responses were then split into two types of data - numeric and textual. Numeric data consisted of the Likert scale Impact and Recon factors, while textual data involved pre-requisites and consequences. All Impact and Recon factor survey question responses were gathered into a single spreadsheet, where statistics such as mean, median and standard deviation were calculated. This analysis is shown in Figure 4.10. The decision was to use the median of each TTP as the final value that would go on the card, as it was less affected by outliers than the mean. Any non-integer value is rounded up, which would imply that the techniques may end up having greater Impact or Recon factor than they would otherwise have.

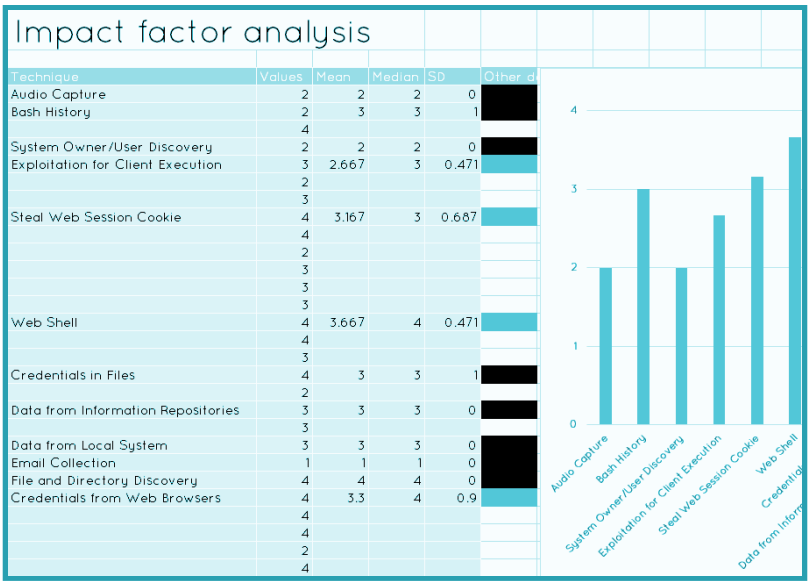


Figure 4.10: Impact factor analysis

For the textual analysis, the method was slightly different. The chosen method was Braun and Clarke's Six Phases of Thematic Analysis (Clarke & Braun, 2014):

1. Read the data and any extract patterns that are occurring.
2. Document patterns – derive initial codes and their meaning
3. Combine codes into themes, describing exactly what each theme means, plus add in any missing themes at this stage.
4. Check if the generated themes support the data, if they do not – repeat

the previous steps and fill in any missing themes.

5. Define each theme, what it captures and why is this theme noteworthy.

6. When generating a report, choose a couple of meaningful themes for it. At this stage, verify if the themes describe the data accurately again.

The process of labelling responses is illustrated in Figure 4.11. Each answer was examined for common themes and assigned a category. Those categories have become the early version of pre-requisites and the final version of consequences on Technique cards.

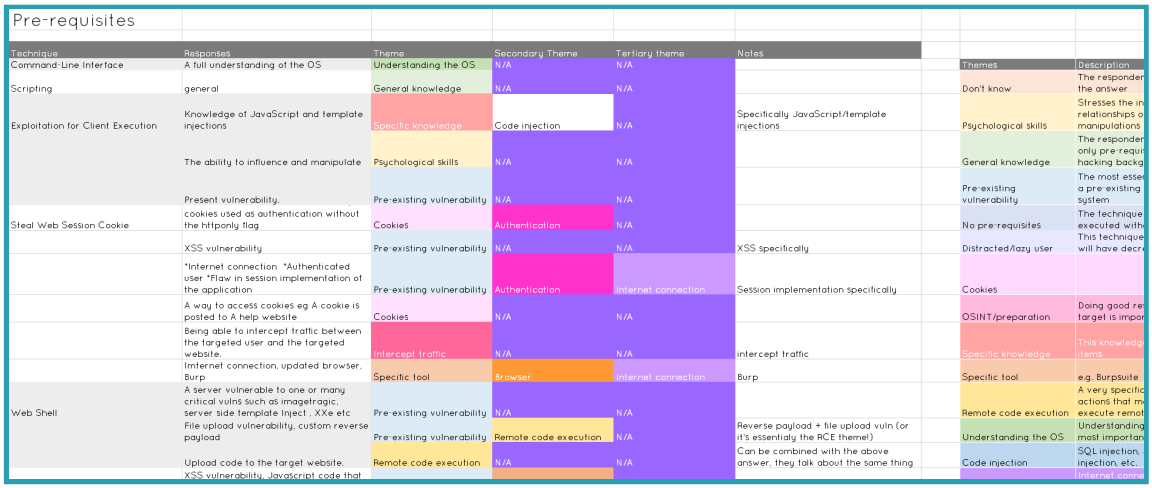


Figure 4.11: Thematic analysis

It was originally planned to source ***Information*** and ***Opportunity*** cards from pre-requisites of the TTPs. However, throughout the study, it has become apparent that pre-requisites were very subjective. Sometimes they were a part of the technique itself, for example in the case of 'Steal Web Session Cookie' the pre-requisites were 'Intercept traffic' and 'Authentication'. Such pre-requisites are more likely to be a part of the technique itself rather than a separate pre-requisite. Other pre-requisites were considered very general, such as 'Knowledge of the system'. It has therefore been decided that the Information cards would now be sourced from the mix of scenario-specific contexts, for example, from the internal network (Figure 4.12) of the fictional company that appears in the scenario. This network has been designed using a number of reference architectures and modern practices as inspiration.

Technique cards were sourced using a two-stage process. First, Mitre

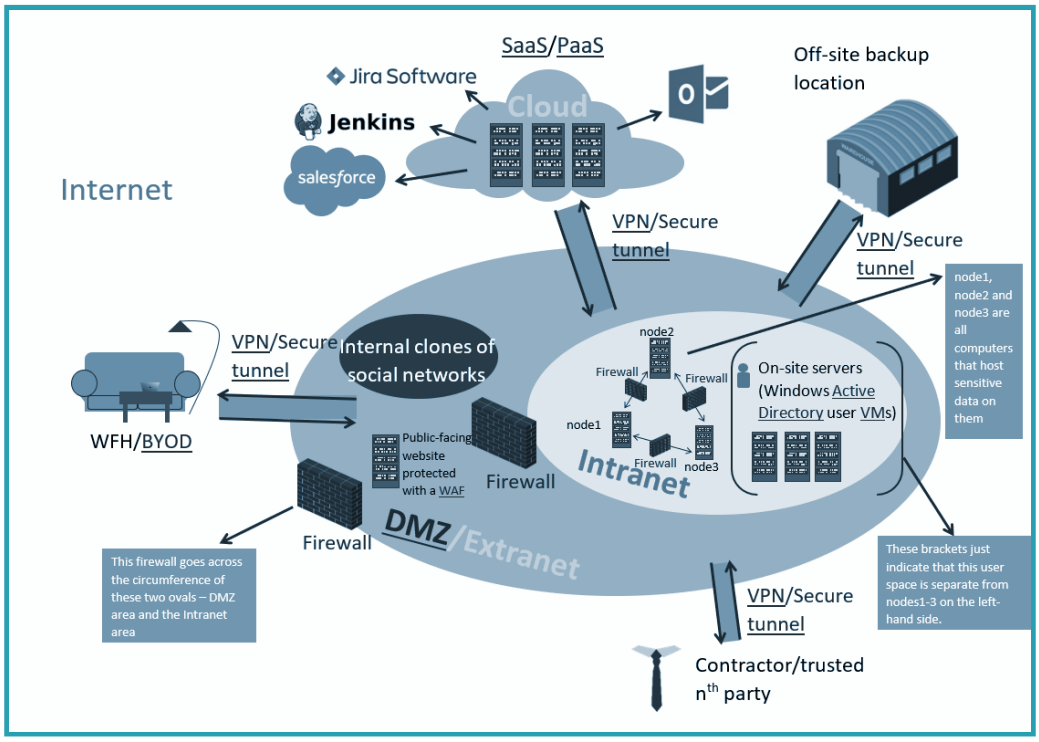


Figure 4.12: A reference network diagram that has been used by the GM to provide guidance to the players.

ATT&CK Taxonomy was used to obtain a list of titles of those techniques. The second stage has involved running the survey that has just been described. The *Countertechnique* deck was populated using the information on the MITRE ATT&CK framework website - almost every single TTP that was listed there had a 'Mitigations' section that listed some of the known mitigations or defensive measures that could help to stop or mitigate the impact of this specific technique.

4.6 Playing around COVID-19

The game was originally planned as an in-person tabletop game, so certain aspects had to be adapted to make it suitable for playing online.

Firstly, as instead of paper cards players will now view the information on the screen, it was necessary to re-think how the player experience would differ. Most of the players who will participate in the game sessions have not seen it before, which would imply that we must ensure that new players are comfortable navigating the game and can understand the rules quickly. For this, instead of the finished

Technique card PDF document (Figure 4.13), players were provided with a table of techniques, which was considerably easier to scroll.

Figure 4.13: The final Technique card PDF document. Considerably less information can be visible on the screen at once with regular viewing. The document needs to be scrolled, especially for a first-time user, who does not yet know what Techniques are available and what they need to be search for.

The next adjustment has been the use of the online platform, Discord in this case. Using a platform like this has significantly simplified communication between players and the GM, despite participating parties being based in different locations. Scheduling the games has also become simpler, as players would be able to schedule a game session in between their regular daily commitments. Doodle (2021) has been used to organise sessions, and a text channel on the Discord server has been dedicated to announcing when the next Doodle poll becomes available.

Lastly, players no longer can come to a physical location where all the resources necessary for playing the game are already provided. Thus, it is necessary to ensure that when the games happen online, players do not need to bring anything to the playing session. Discord provides a system of bots - automated scripts that can display useful statistics. One such bot automates die rolls, so the players no longer need to bring a physical die with them. An example use of this bot is shown in Figure 4.15. If a virtual die would not have been provided by the Discord bot system, a die-rolling script would have been created or downloaded from another location.

Deck number	Name	Recon	Impact	Playful description	Serious description	Pre-requisites	Consequences	Min roll	Risk
T 01	Exploitation for Client Execution	3	3	"All it took was a torpedo to a thermal exhaust port to explode a Death Star."	Adversaries can take advantage of certain vulnerabilities through targeted exploitation for the purpose of arbitrary code execution.	Psychological skills, Pre-existing vulnerability	1. Technique not executed 2. Technique not executed 3. Being discovered	4	4
T 02	Steal Web Session Cookie	4	3	"No cookies for you!"	An adversary may steal web application or service session cookies and use them to gain access web applications or Internet services as an authenticated user without needing credentials.	Pre-existing vulnerability	1. Technique not executed 2. Technique not executed 3. Being discovered	2	1
T 03	Web Shell	4	4	"I will take my shell with me anywhere on the web. Everything I have I carry with me after all!"	Web shells may serve as Redundant Access or as a persistence mechanism in case an adversary's primary access methods are detected and removed.	Pre-existing vulnerability	1. Technique not executed 2. Technique not executed 3. Being discovered	4	3
T 04	Credentials from Web Browsers	4	4	"Browser wars - now in your file system!"	Adversaries may acquire credentials from web browsers by reading files specific to the target browser.	Pre-existing vulnerability, Distracted/lazy user, Resource compromised, Exfiltration channel, OSINT/Preparation	1. Being locked out of the system 2. Being discovered 3. Countermeasures taken by target	3	1

Figure 4.14: A screenshot of the draft Technique cards table. This version was preferred over the finished Technique cards PDF document, as it is more optimised to be viewed on screen and makes finding the right information quicker than scrolling through every single card.

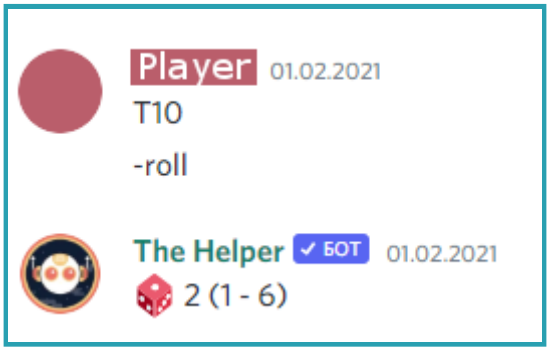


Figure 4.15: An example of using the virtual die.

4.7 Mapping requirements to implementation

4.7.1 Criteria for educational games

We have initially set out a list of requirements for our game, that was inspired by a general list of requirements for an educational game, referenced in Section 4.2.1. Let us map the various aspects to the implemented board game.

> *the goal to achieve an outcome that is superior to others (competition)*

Although there is no direct competition involved in the game mechanics, the game takes place with different players taking turns. A side-effect of that is that players would want to finish the game before other players.

> *tasks that require effort and are non-trivial (challenge)*

At the start of the game, a player is presented with a list of different techniques. A player then needs to work out how to use those techniques to achieve the winning conditions, which often are not trivial and require chaining attack techniques to complete them.

> *a context-sensitive environment that can be investigated (exploration)*

Players have an opportunity to ask GM questions about the organisation that they are attacking, as well as if they have access to directory scanning or other features, the interactive element with the GM provides a means to explore the environment.

> *the existence of a make-believe environment, characters or narrative (fantasy)*

The game includes a scenario that is inspired by past events with a realistic target, and a realistic geopolitical landscape, but the countries are not the same as in the real world. This small difference from the real world makes the scenario believable, but also reminds the players that they are playing a game.

> *measurable results from game play (scoring)*

Each player is allocated a role that has a different amount of a consumable resource (risk appetite). This resource gets used when the player decides to use a certain technique and it does not succeed, the resource, in turn, replenishes when a player repeatedly succeeds at using a specific technique. Depending on the number of points remaining, players get access to different techniques, and running out of risk appetite points is equivalent to losing the game.

> *explicit aims and objectives (goals)*

Each role has a clearly defined list of goals that the player needs to accomplish to end the game. These goals are the *'win conditions'*.

> *action in the game that changes the state of play and generates feedback (interaction)*

Players interact with the GM, who also represents the organisation that is being attacked. They roll dice to determine the outcome of a technique (success or failure) and the GM has the option to respond with a defensive measure to hinder the progress of a player. The player can get answers from the GM that reveal various information about the organisation, further reinforcing that feedback loop.

4.7.2 The LM-GM framework

Figure 4.16 shows the LM-GM framework applied to the final game. Overall, there are 10 learning mechanics and 11 game mechanics present, which overall makes it a balanced serious game.

Instructional and *Guidance* are used when the GM walks the players through the game. The GM guides the players at all times to make sure they know what needs to be done at every stage.

Participation is key in the game, as it relies on player-to-GM interactions.

Each player has a set of *Actions/Tasks* that they need to perform in order to complete the game.

At every stage of the game there is constant *Feedback* from the GM as to how are the players performing, as well as from the players to the GM if there is something in the game that does not make sense to them.

Question & Answer is used if a player wants to learn more about the world, boundaries of the game or their current status within the game.

Players are encouraged to *Explore* the game and the game world. This can be achieved by players asking questions and the GM providing answers.

Players also are required to *Plan* their actions, as they have a limited amount of resource (risk points) that they can spend. The notion of *Responsibility* is also manifested through planning how to spend the risk points and knowing that the game will be lost if the player responsibly manages their resources. This also intersects with *Strategy/Planning* section in the Game Mechanics section.

Motivations are given to players when they receive their respective role cards.

The game is built on *Role Play* as a core mechanic. *Selecting and collecting* is also a widely-used tactic in the game. Players select a Technique card that they will use for a given game turn, and players collect Information cards that allow them to use more techniques based on the information they have available.

Information cards act both as *Tokens* that players can use as a tangible measure of progress and as *Goods/Information* that players discover as they progress through the game. *Cascading Information* is a principle that accurately describes how the knowledge of the players evolves - first they learn about the organisation on a high level, as the game progresses they learn about the employees and the inner workings of the organisation in a given scenario.

Resource Management is one of the key game mechanics that are used to make the game challenging. Players are given a limited resource – risk appetite, and they are required to strategise how best to use it.

The game takes place with *Game Turns*, where players take turns, which are then responded to by the GM, one by one.

A degree of *Realism* has been utilised to ensure parallels can be made with the real world, such that the principles from the game would be relevant to the real world to a certain extent.

Rewards/Penalties are also actively used to create a challenging environment and to make the game engaging.

Players can find about their game *Status* by asking the Games Master or checking the bot messages in the text channel.

4.7.3 The revised gamification design framework

The game mechanics combines some of the elements shown in Figure 2.8 (Section 2.4.2). One of these examples is the game having a theme - cyber attacks and different cyber attacker types. Another gamification element used in the finished game is the Narrative - players are immersed into a scenario. There are also elements of Progress/Feedback – player is interacting with the GM, receiving constant status updates. The game also has a number of Unlockables and a variety of Easter Eggs, tailoring to the creative minds (denoted by the 'Free Sprit' player type). To cater to the 'Achiever' player type the game demonstrates Progression (element 27), which is exhibited when players unlock various Information cards.

Although the developed game does not cater to all of the player types, this framework does not mandate that all the elements need to be present, and since the target audience is cybersecurity enthusiasts and researchers, the game only needs to be targeted to these groups, tailoring the game to all other groups is an optional extra. This framework does not specify the optimal amount of elements that need to be present, but given there is a set of general elements that applies to general game features, and the fact that the majority of the elements in the developed board game are general makes the developed game fit to be called a serious game. The application of the LM-GM model has established that the game as a whole has both learning mechanics and game mechanics. The revised gamification design framework has specifically evaluated the game mechanics of the developed game to determine whether the game is engaging. With a sufficient amount of elements present the game can be considered engaging.

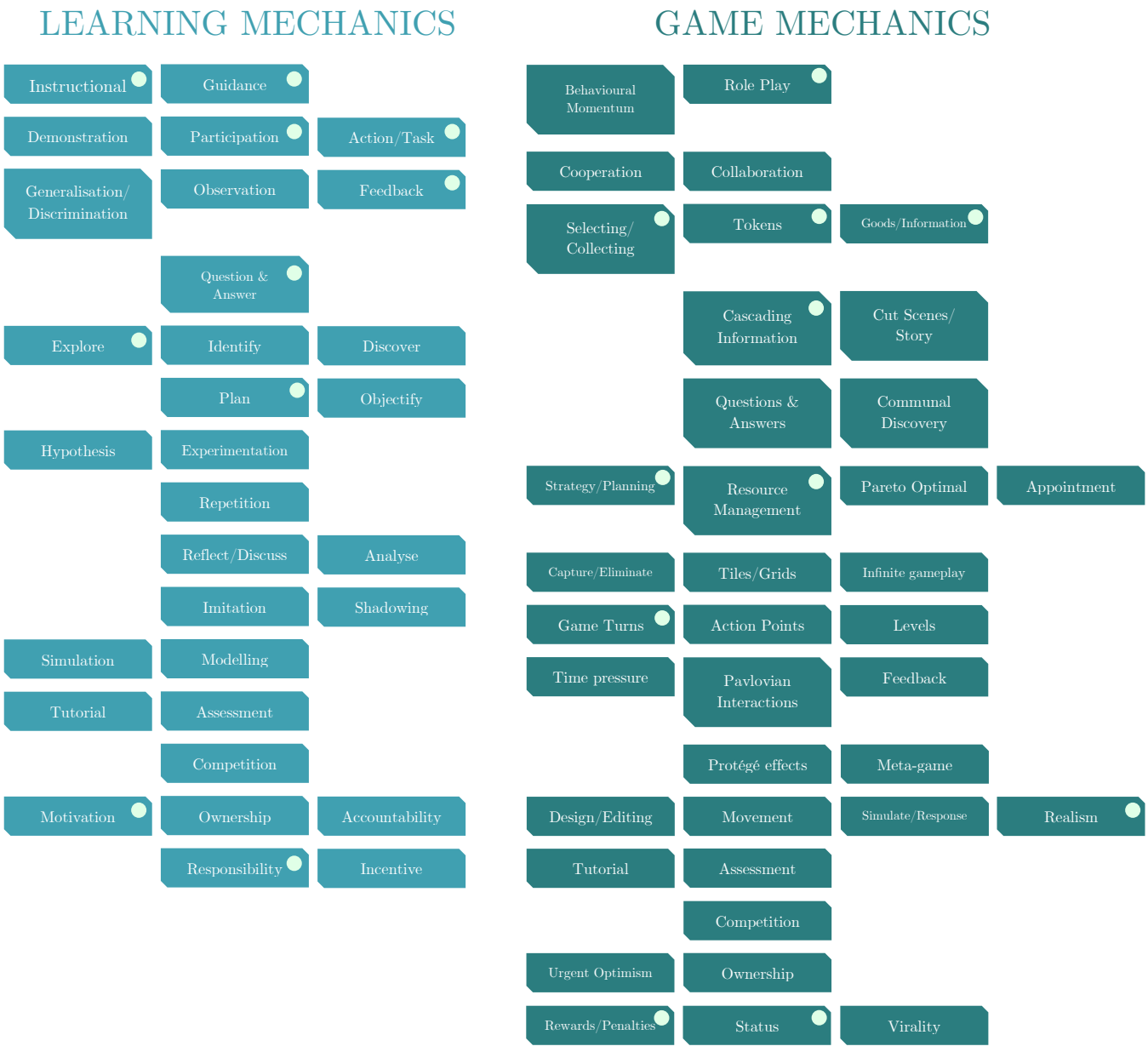


Figure 4.16: Learning Mechanics-Game Mechanics (LM-GM) model by Arnab et al. (2014) applied to the developed game. A circle indicates that this feature is relevant to the game.

4.7.4 Engagement and commitment

Using the preliminary taxonomy by Robinson and Bellotti (2013), first mentioned in Section 2.4.2, the highly demanding game features such as *"Ambiguous Path to Objective"* or *"Virtual abilities"* are sufficiently mitigated. In the first case, the path to objective is clearly mapped on the Role cards that players get at the start of the game. In the second case, players' virtual abilities are Technique cards. Each Technique card has an explanation and an outline of the effects it produces, ensuring the player understands what is required.

The game also includes some low-commitment gamification features, such as *"Choice architecture"*, where a player has a choice of what they can do next. With all options clearly explained a player is able to make a decision that most accurately reflects their intention.

Overall, the game is sufficiently balancing player commitment with the engagement levels, creating a comfortable gaming experience.

Summary

The game has been made into a card game with a number of decks that are: Role, Technique, Countertechnique, Information and Opportunity. The decks have been generated by using past news stories, Mitre ATT&CK framework and a specifically generated survey (Appendix G). A Games Master(GM) is representing the organisation that is to be attacked, while the player is representing the attacker, that can assume any of the seven roles provided: Script Kiddy, Counter-culture, Hacktivist, Cyber Mercenary(APT for hire), Cyber Mercenary(individual), State-backed(low capability) and State-backed(high capability). Each of these roles has different goals linked with the game scenario, that the player needs to complete to win the game. To complete these goals a player needs to gather Information cards that would help with getting access to certain areas (an example of an Information card can be a password or information about the existence of a specific server on the network). The Technique deck is a set of TTPs players can use to obtain Information cards. The GM (who is representing the organisation) can choose to respond with a pre-selected

Countertechnique card, but this can only be done once per set of techniques that this Countertechnique applies to. Players have an option to ask the GM questions that allow them to find out more about their current position in the game, their location and other helpful information. The Opportunity deck is a set of hints that unlock one or more Information cards. This deck is designed to be used in three possible situations: as a last resort for a player, if a player is deviating from the scenario, or if a player is stuck. The players have a consumable resource that they use in-game, Risk Appetite, which represents the attacker's desire to use potentially more rewarding techniques (which are more high-risk as the result). Running out of Risk points would make the player lose the game. It is possible to restore Risk points, but they cannot be restored past a Role-specific maximum. A more detailed set of rules is available in Appendix F.1.

As mentioned in Section 4, the following objectives have required to be fulfilled:

A realistic game based on rigorous evidence has been built, with the information sources coming from different equally reputable locations, such as MITRE ATT&CK frameworks or by surveying specialists in the field. The realism in the game has been achieved by taking past events as inspiration and modelling realistic inter-country relationships.

The game enables players to make decisions that reflect their true intention by allowing a degree of freedom for the players by using the GM to handle communication. The list of TTPs in use by the game is small, but it helps to cover any TTPs that are not in that list by communicating with the GM. The GM, who is more familiar with the games can also help the player formulate their decision in terms of the game logic and artefacts.

Chapter 5

Method: Simulation

> All models are wrong; some models are useful.
>
> George E. P. Box

This chapter is dedicated to devising efficient notation for capturing in-game decisions, as well as showing how they can be ingested into a simulation. Additionally, the topic of individual differences is considered for a better understanding of players of the game. Next, the design process for the simulation will be discussed. Lastly, we will map the existing proof-of-concept simulation to an ABM validation framework.

Research objectives

This chapter is dedicated to the fulfilment of the following research objectives:

3. *To devise an efficient approach to the recording of the game decisions*
4. *To ensure the events within a game can be restored from the recording, with semantics preserved*
5. *To ingest the game decisions into a simulation*

5.1 ABM validation framework

As first mentioned in Section 2.2.4 (Figure 2.3), the following example framework will be used to validate the ABM. Although the approach here is a proof-of-concept, mapping it onto the validation strategy will indicate where the research fits in terms of the original contribution.

1. *Face validation: Do animated behaviours and output tends to match reality? This stage involves verifying code and algorithms and identifying significant parameters.*
2. *Sensitivity analysis: Have we determined which parameters affect behaviours and outputs? This stage involves verifying code and algorithms and identifying significant parameters.*
3. *Calibration: Do processes, parameters and results match reality? This stage involves selecting the range of values for the model parameters*
4. *Output validation: Do predicted results match reality? This stage involves the overall assessment of the model.*

The aim of this project is to provide a proof-of-concept simulation, therefore it would not undergo a full validation process. From the framework above, the work done in this research project corresponds to steps **1** and **2**.

5.2 Capturing gameplay

Capturing the output of a board game is challenging, especially if the game involves players interacting with the GM. To capture *all* of the interactions, the game session needs to be recorded and transcribed. Processing this output would take a long time, therefore a more refined approach would be required.

An ideal kind of game recording, from the perspective of the researcher, would be the one that captures most of the interactions but does not take a long time

to generate and also allow efficient ingestion into the simulation. Significantly, this approach would allow the actions, decisions and interactions to be recorded during the game. A further augmentation would be to get the players to record the decisions themselves, without making the process too difficult.

The shorthand notation presented here has been inspired by the algebraic notation in chess, first used by Philipp Stamma in his book "The Noble Game of Chess" (Du Toit, 2016, p. 37). In this notation, each chess figure has a letter that represents it, e.g. `B` for bishop. Each square of the chessboard also has a unique reference, e.g. `d8`. Each move can be recorded using this shorthand notation.

The first step to developing a similar notation for the cybersecurity board game is deciding how the turns would be presented. Each turn resides on a single line, displaying both the actions of the player and the GM. Any actions done by the GM are represented by preceding a move with the prefix '`GM`'. If there are any artefacts unlocked as a result of the player's or GM's actions, they will also be displayed on that same line.

The second step is to give each of the game decks a unique reference. The decision has been to label the decks with the first letter of their name as follows:

- `R` = Role
- `T` = Technique
- `C` = Countertechnique
- `I` = Information
- `O` = Opportunity

Each card in the deck is numbered, to help distinguish the cards that are located in the same deck.

The next step has been to find indicators of success or failure. For this, a binary notation has been chosen, with `S` representing Success, and `F` representing Failure. If a Technique card does not succeed, an additional notation is introduced to represent consequences to the player when the technique goes wrong. This is denoted by the

`cs [number]` notation, where `[number]` is the number of the consequence, from one to three.

Lastly, if a player completes the objective, this is written on the next line from their regular turn, and if this is the last objective that needs to be completed – this is indicated by the `[Role] WIN` in brackets, or if the current move leads to the player's loss – `[Role LOSS]` is indicated in brackets next to the losing move, like so:

```
R04 T10 F cs 3 (R04 LOSS)
```

The summary of the notation can be seen in Figure 5.1.

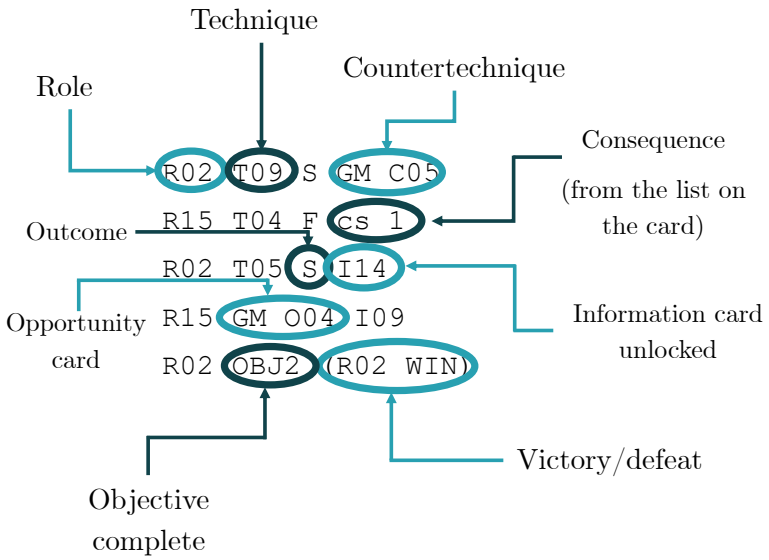


Figure 5.1: A diagram explaining the shorthand convention. Adapted from (Sidorenko et al., 2020, p. 6).

Notably, this notation is used when transcribing the games, that is, putting the game turns into a text file based on Discord chat logs. Due to the small sample size, turning games into text files has been done manually, condensing Discord chat logs into text files. With larger sample sizes a script that would automate text processing would have been used instead. During the game, players and the GM write their moves in a special channel, that is visible to only the player whose turn it is now, and the GM who is responding to the player moves. An example game in progress can be seen on Figure 5.2. After the game is complete, the game is put into the

notation specified in Figure 5.1 above. This way the game can be recorded during the session, and the minimum time is required to put it into a condensed notation.

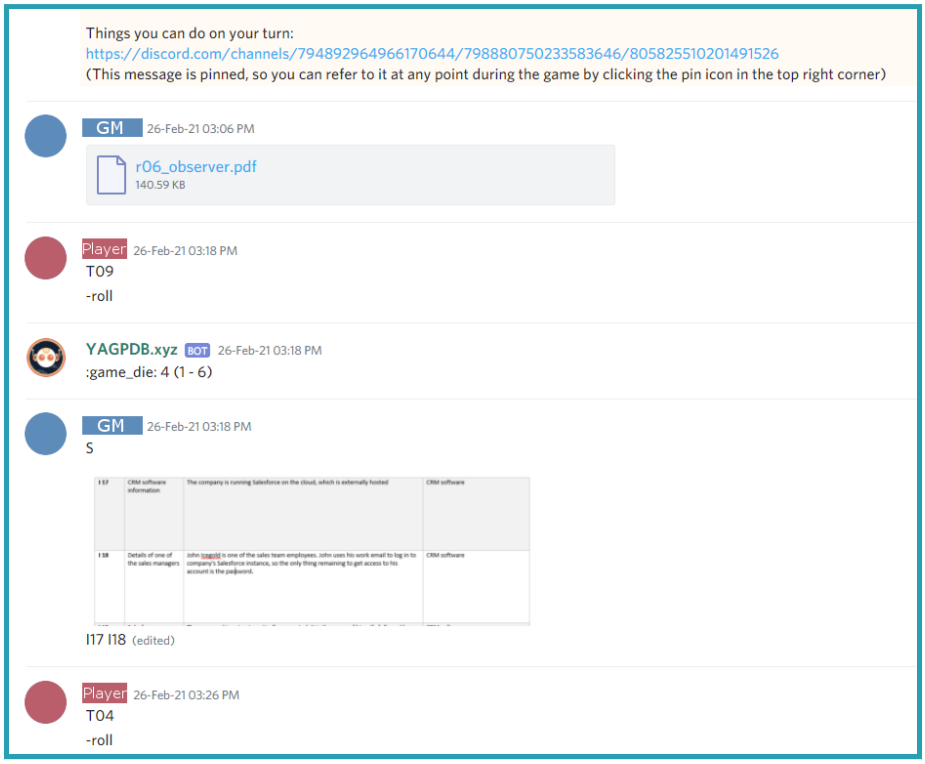


Figure 5.2: Discord screenshot of the chat log

5.3 Understanding players

So far, our discussions about the game have only mentioned the role-specific risk appetite. Yet, the game players all have different backgrounds, personalities and a range of characteristics that can affect the way they play a specific role. To investigate whether there is an effect on how accurately the participants portray a specified role and whether their individual differences play an important part in this they have filled out a short questionnaire, a copy of which is available in Appendix H.

No two individuals are the same due to their genetic composition and the environment these individuals were brought up in. These factors constitute individual differences ('Chapter 3 – Individual differences', 2021). These differences manifest into regular behavioural patterns that change infrequently.

For this short questionnaire, three different scales were used to investigate the

individual differences. Each prospective player was required to complete the questionnaire prior to participating in the game. The survey combines three different measures: Sneider's self-monitoring scale (Snyder, 1974), Domain-Specific Risk-Taking (DOSPERT) 30 scale (Blais & Weber, 2006) and Barratt's impulsiveness scale (Patton et al., 1995).

Sneider's self-monitoring scale, which the author defines as "self-observation and self-control guided by situational queues to social appropriateness"(Snyder, 1974, p. 1), investigates how accurately the emotions experienced are portrayed by the individuals, ultimately determining how well an individual can 'act out' a certain role, or, in our case, role-play.

The DOSPERT scale examines the attitudes towards risk, as well as the individual's perception of risk (Weber et al., 2002b). This scale was included in the questionnaire to determine if the individual's perceived risk would override the role-specific risk.

The Barrat's impulsiveness scale is designed to assess three different factors (Bari et al., 2016, p. 115):

1. *attentional impulsiveness, defined as the (in-)ability to concentrate or focus attention*
2. *motor impulsiveness, or the tendency to act without thinking*
3. *non-planning impulsiveness, or the lack of future planning and forethought*

The reason for choosing this scale is to assess whether these factors would affect the decisions taken by the players.

5.4 Simulation (Proof-of-concept)

The model for the simulation that is to be developed for this project aims to reflect the intentions of offensive actors. Hence, the design of the model must reflect their

mindset transition given the changing environment and different possibilities given the information available.

5.4.1 Spatial vs non-spatial

There were several concepts as to what the model should look like. The first important design decision has been whether the model is going to be spatial, i.e. will the space in the model play an important part, or it is going to be non-spatial and all attention will be dedicated to interactions of agents with the environment.

For the ***spatial*** prototype, it was decided that the environment in the model will represent a network, while the agents will be the attackers moving through that network information space. Various network locations can be connected with links, which makes this model similar to a graph. As the entire infrastructure is visible upfront, as well as the location of each one of the attackers, this simulation is assuming the defender's point of view. This concept is illustrated in Figure 5.3.

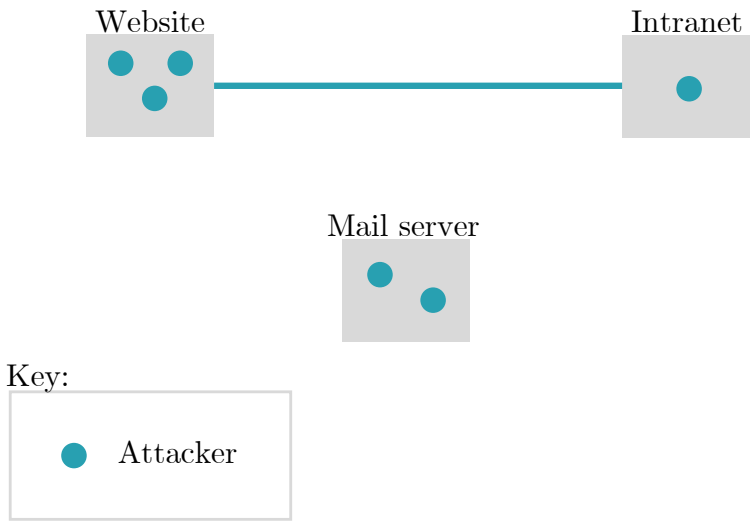


Figure 5.3: A spatial concept of the simulation. The location of each attacker is signified by an agent.

This idea has been discarded, as the aim is to understand the attacker from the attacker's perspective. Otherwise, this concept would have been used instead.

An alternative paradigm is the one of a ***non-spatial*** simulation, where the

physical space in the simulation represents a more abstract concept, and interactions between agents are the focus of the simulation. In the case of our simulation, space will represent the goal advancement, and the agents will still represent attackers. Further from the centre of the circle is the dot, further from the goal completion is the attacker. Reaching the centre of the circle represents achieving the specified goals. Figure 5.4 provides a visual demonstration.

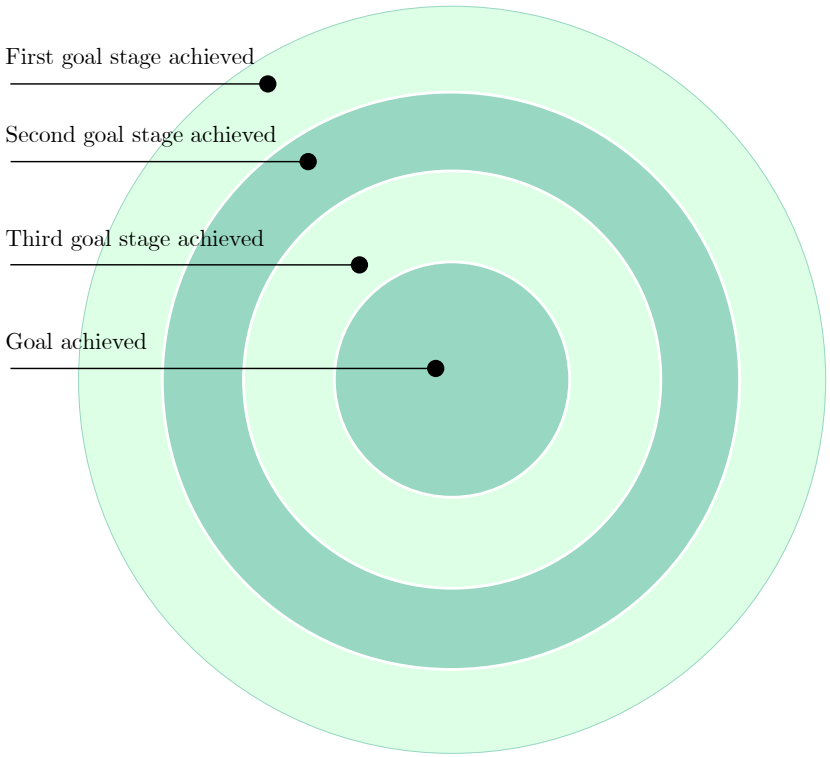


Figure 5.4: A non-spatial initial concept of the simulation. The circle is the representation of achieving the goal, with the goal being the centre of the circle. The layers represent percentage completion to achieve the specified goals.

The concept was further modified (Figure 5.5) so that now the agents are still representing attackers, but instead of moving the attackers, each attacker now has a progress indicator that would show how far they have moved. This subtle change incorporates the ability to show multiple progressions on the same line, for example, if an attacker has attempted to gain access to this target three times, on each simulation tick it would be possible to overlay the three attempts and see how far the attacker has been at this point of the simulation on their three attempts.

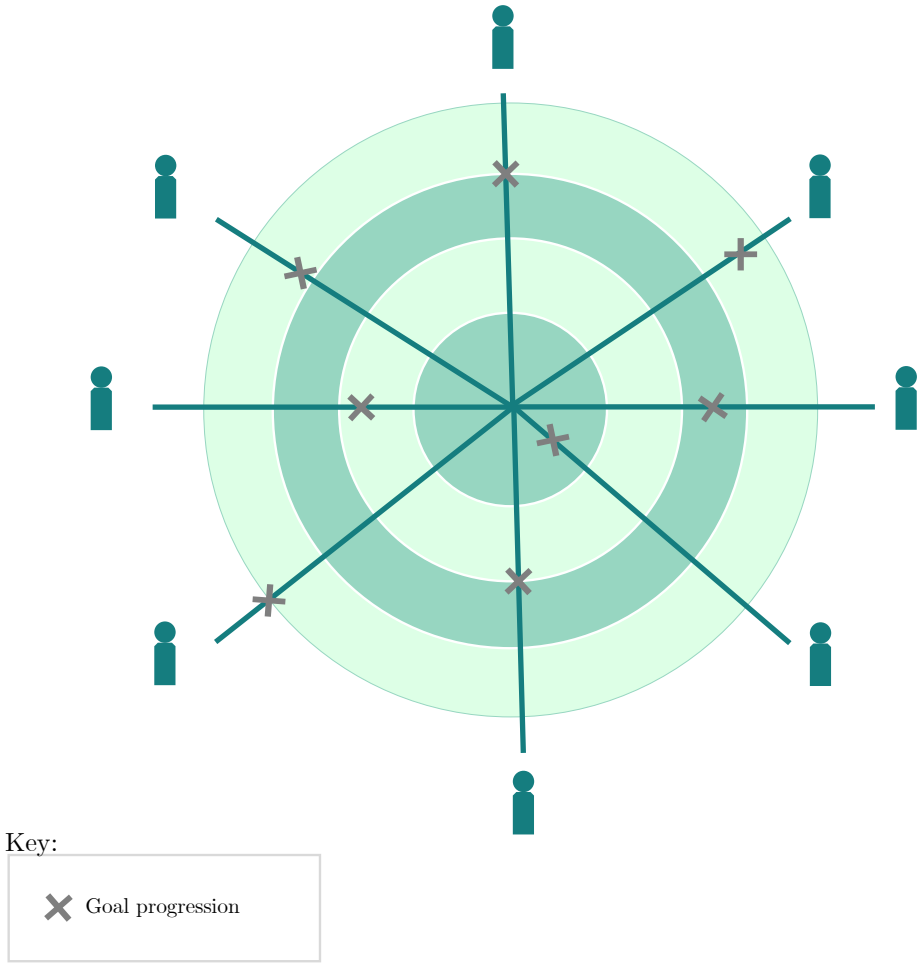


Figure 5.5: A combination of the goal progression and the initial circular model. Represents different cyber attackers at different stages of their respective goal completions.

5.4.2 Implementation

After the initial speculative design, work has begun on the implementation of the simulation. The first step has been to get the agents to align outside the circle. The types of an agent can be configured - each type has a sliding scale that allows creating a number of agents of that type. Each agent type has its unique colour to differentiate it from the other agent types. This is shown in Figure 5.6.

Wilensky and Rand (2015b), the creators of the modelling language NetLogo, define an agent as *"an autonomous individual element of a computer simulation. These individual elements have properties, states, and behaviours"*. Although this

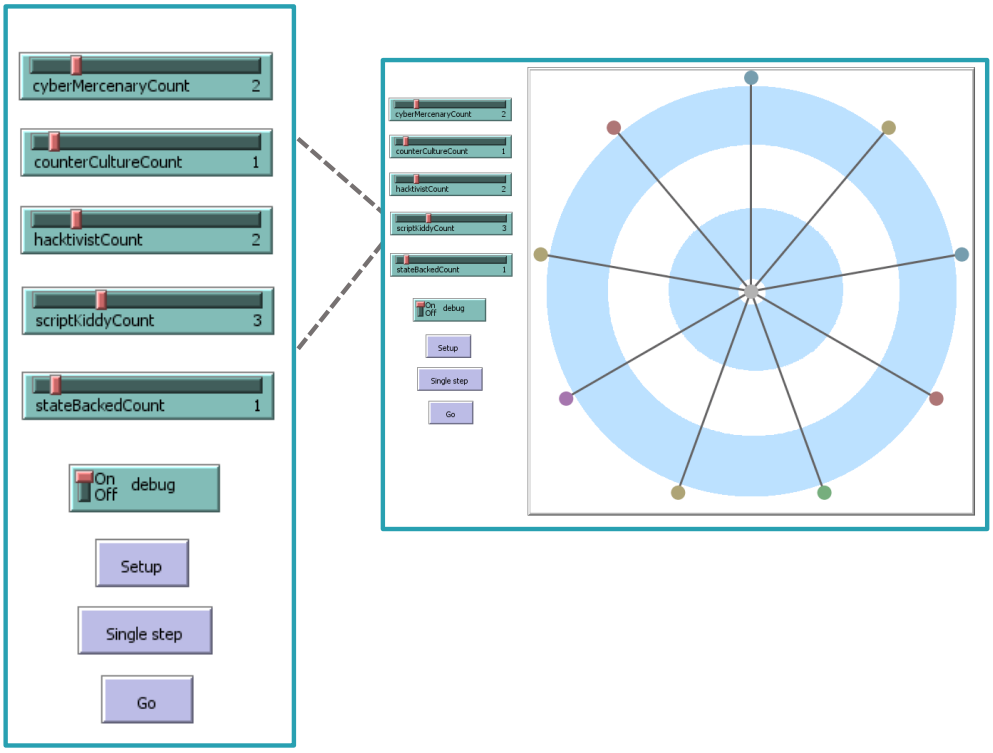


Figure 5.6: Initialising the simulation. The model allows freely selecting the required number of each agent type. The available types are: Cyber Mercenaries, Counter-culture, Hacktivist, Script Kiddy and State-backed. Each role has its own colour.

model is a proof-of-concept and does not implement the interactions between agents as such, certain aspects of the agent-based model have been implemented. An individual agent has properties, and a concept of behaviour, presented in form of a list of actions that it will do next. The properties of an agent can be summarised as follows:

hackerType A type can be 'Script Kiddy', 'Hacktivist', or similar. Set at the initialisation of the simulation.

riskPoints How many risk points does it have at any point of the game. Set at the initialisation of the simulation, then updated throughout.

infoPieces This would correspond to the Information cards unlocked in-game. Set and updated throughout the simulation.

nextSteps Its future moves. Set at the initialisation phase, then updated throughout the game.

This is further demonstrated in Figure 5.7. At the moment agents replay the actions of the players. That is, for each gathered player action there will be an agent that is generated. Each of the generated agents is to be matched with a player decisions file of the corresponded role, i.e. if a hacktivist is generated by the user operating the simulation, the future actions of the agent are sourced from a captured game output, with this player representing a hacktivist as well.

The mappings of the game files are as follows. If there is exactly ***the same*** number of generated agents as there are game files, as discussed, agents will get assigned to the matching game files. If there are ***more*** generated agents than there are game files, a game file that has a role matching the generated agent will be selected at random. Finally, if there are ***fewer*** generated agents than there are game files, then more than one generated agent will get a game output file assigned at random.

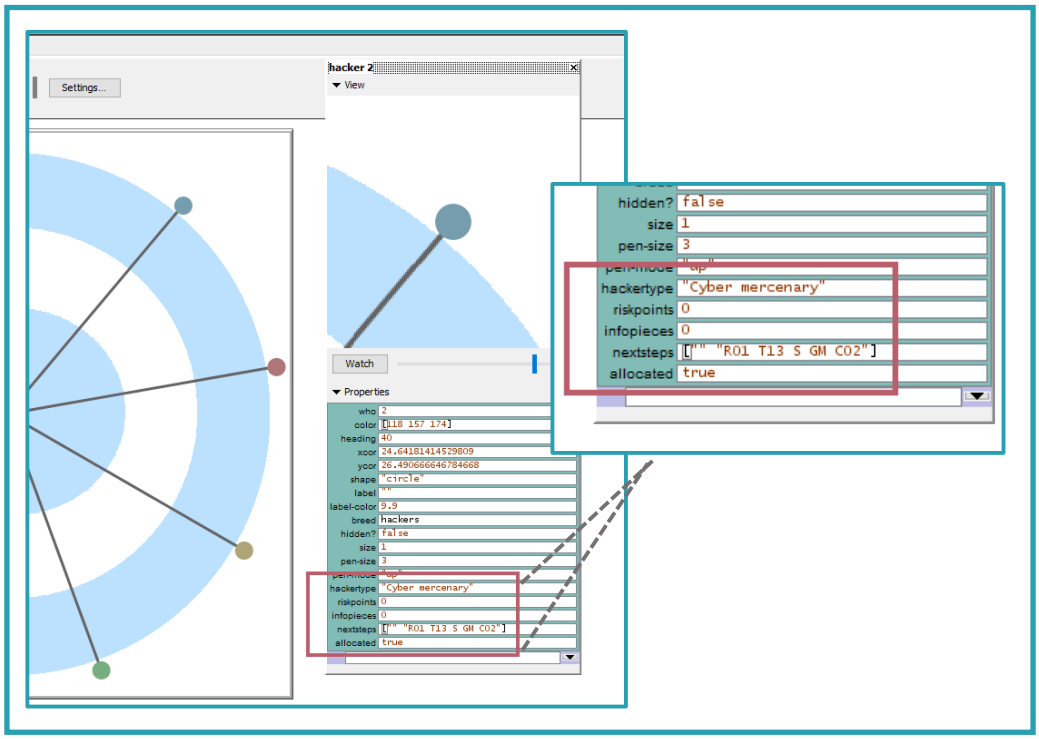


Figure 5.7: Examining an individual agent. In the red box, we can clearly see its type, number of risk points allocated, number of information pieces (Information cards) possessed, and lines of game transcription that will serve as its next steps.

5.5 Validation of the model

Let us come back to the framework that has been outlined in Section 5.1.

> *1. 'Face validation: Do animated behaviours and output tends to match reality? This stage involves verifying code and algorithms and identifying significant parameters.*

Upon initialisation, we generate the agents that correspond to the types specified in the simulation parameters. Our significant parameters for this simulation are types of attackers, role-specific risk appetite and the individual risk appetite. Each agent has a specified risk appetite, which corresponds to the roles in the game. Future actions of the agent are stored in each of the individual agent's memory. Any information agents unlock is stored in the memory of each individual agent, which would correspond to an attacker learning about confidential data their target possesses (e.g. orders database access, a username-password pair from the admin console, etc.).

To make it a truly realistic simulation, only the immediate next action could be stored in the memory of the agent, but currently it is replaying the game moves. If the agents were adaptive, i.e. they would keep the initial conditions, such as their risk appetite (which cannot be greater than the initially-specified value) and their role, but would have been able to change their next move according to the situation, this would have made a more dynamic simulation.

> *2. Sensitivity analysis: Have we determined which parameters affect behaviours and outputs? This stage involves verifying code and algorithms and identifying significant parameters.*

In the parts of the simulation that are currently implemented, parameters that affect the output and behaviours are the role-specific risk appetite (both how much is available initially, and how much is used throughout the simulation depending on the actions performed), and the set of actions that are stored in each agent.

Summary

In this chapter, we have explored and walked through the validation process for the proof-of-concept simulation, identifying that only the first two steps will apply to this model. We have then examined the notation that is used for recording the games. We have also acknowledged that it is important to consider not only the role-specific risk appetite, but also step back and examine the individual playing the game, and how their risk appetite and ability to role-play affects the decisions made in the game. Lastly, we have researched the two concepts of how the simulation should be laid out, comparing the two different paradigms - spatial and non-spatial models. Our model is non-spatial, representing the agent's individual proximity to the goal.

Let us now map the takeaways from this chapter to the research objectives[1]:

[1]Note, that the numbers correspond to the research objectives, and are not a continuation of the earlier model validation section.

> *3. To devise an efficient approach to the recording of the game decisions*

This notation allows to represent a game turn on a single line, and capture decisions during the game. The key events that take place every game turn can be restored from this notation alone.

> *4. To ensure the events within a game can be restored from the recording, with semantics preserved*

As mentioned above, the shorthand notation can restore a game from a text file. The notation captures what card has been used by what role, and what were the consequences of these actions.

> *5. To ingest the game decisions into a simulation*

The text files containing the recorded games are loaded into the agents and stored in each agent's memory so that every move is ready to be retrieved by the agent during the course of the simulation.

Chapter 6

Results and Findings

This chapter will summarise the outcomes of the games, as well as examining the player and the GM experience. It is important to note, that the sample size of participants was quite small, hence the results should be treated with caution.

Next, individual differences and Technique card usage patterns will be examined, with accompanying graphs and statistics. Lastly, we will take a brief look at the simulation and compare the results against the research objectives.

6.1 Descriptive information games

There were a total of ***13 games*** carried out, with ***15 participants***. Most of the games were organised one-to-one, i.e one player and one GM, but sometimes there were groups of 2-4 players. Out of 15 people, 3 people were returning players, more people have expressed interest but could not return due to scheduling. Notably, only one of these games has been lost, all of the other games have been successfully completed.

Each game session typically lasted from 50 minutes to one hour, with sessions taking longer if there were more players. Despite the small number of participants, the data generated was sufficiently rich as the games have lasted for many turns.

The participants were sourced from various social networks, as a result, there was a mixture of ages and experiences, and even players with less experience have picked the techniques that were effective and had a good vision of the goal.

6.1.1 Experience of the Games Master

During the first several games it was difficult to memorise the functionality of every card, as well as the number each card had. A player declares their intention, chooses a Technique card and rolls a die. To respond with a creative mini-scenario, that incorporates the Technique card, the outcome and fits with the overall scenario, there are some details that the GM needs to know. An example of a mini-response to a successful use of a Spearphishing Link Technique on the CEO of the target organisation can be of this format:

> *"The CEO is an avid golf player. You decide to craft a phishing email with a link to a very promising golf club membership discount voucher..."*

A mini-response like this requires knowing what Technique card a player used (as they would typically just name the number, and not the technique itself), how a technique works and if it appears in any of the Countertechnique cards so that it can be countered in a timely manner. One of the players was also a golf player and has confirmed that golf memberships can get expensive and that an email like this would definitely lower the guard of the CEO in the scenario. Most of the responses like these were improvised on the spot, with the help of a reference document (Appendix F.3), that contained examples of the Technique cards and past cases that involved the use of this TTP, as well as the short summary of what the technique does. Eventually, the list of TTPs used in the game was memorised, and some GM responses could be re-used, as it was a different set of players that were playing the game.

Some players required more guidance than others, almost exclusively these players had less experience and exposure to the technical aspect of cybersecurity. It was still possible for the less experienced players to complete the game, and Opportunity cards were very helpful in that instance. The players with less experience would take longer, but they would normally still take sensible decisions that would bring them closer to their goal.

More experienced players have expected the techniques to be less abstracted away, and have looked for TTPs that have provided the opportunity to do reconnaissance on the system. This is an example of a case, where the presence of the

GM has been helpful to players. Otherwise, there would not be any guidance on the course of action in the absence of the cards dedicated to enumeration.

All the players were very cooperative and understood instructions well. Even without any prior exposure to the game, they tended to understand the game mechanics during the introductory 20 minutes and play the rest of the game without any problems.

A special command was helpful in tracking how many risk points each player had. The command was a very simple textual script that echoed back a set amount of points with formatting. The output of this command is illustrated in Figure 6.1.

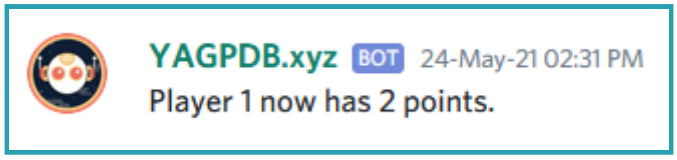


Figure 6.1: A simple command that displays how many points a player has

This command was helpful for the GM to keep track of how many points each player has due to how distinct the bot message looked.

6.1.2 Player feedback

Players seemed to enjoy the game, and the visual aspects (card designs and playful descriptions) were noted in the feedback the most frequently. There was one comment about the convenience - this player was very happy that no extra resources were necessary to play the game. Some players were given the option to choose a table of Technique cards or a PDF document with cards that matched the design of the rest of the decks. All of these players preferred a table over the PDF document with individual cards.

One player made an observation, that if a Technique card is used repeatedly and on several consecutive uses it fails, if on the next use it succeeds it needs a credible justification, a reason why did it succeed after so many unsuccessful attempts. Implementing this feature for the later games was not necessary, as this situation has never occurred, but it is nevertheless a useful observation.

As mentioned above, more experienced cybersecurity professionals and enthusiasts have initially been looking for cards that are dedicated to reconnaissance, cards that are on a different level of abstraction from the other techniques in the deck. When the game was developed, this was also a common trend among the survey respondents. Some respondents have provided parts for a successful technique as pre-requisites. The same was evident during the game sessions. As a workaround, any enumeration techniques have relied on the player and GM interaction, hence the level of abstraction has been adapted to fit these players.

Although these subtle differences were noted in the way the more experienced and less experienced players played the game, player demographic data was not collected, and there are several reasons for this decision. Firstly, the game itself is relatively high level, therefore elaborate knowledge of how every technique works is not required – the players can get more information from the Games Master if they do not fully understand a specific technique. All types of players have finished the game and did it achieving at least one of the specified objectives. Secondly, the reason why none of the black hat hackers have been asked to complete this game (and the information about their demographic collected) is due to there being a limited number of Technique cards. It has been decided in Section 4.5 that custom exploits and wildcards will not be part of the game due to the necessity to validate every custom technique. With this in mind, both white and black hats will be using the same toolkit to complete the objectives, and because this is a tabletop role playing game. Finally, everyone can assume the role of an attacker with the goals and objectives given without any consequences. Hence, the backgrounds of the attackers, assuming the current design of the game, would not be significant in the context of this research.

Two players have commented that they found the absence of tangible steps (that are more refined and detailed than the goals printed on the Technique card) difficult. They have described feeling uncertain about how to begin the game, or how to get closer to a certain goal. Notably, both of the players have completed the game, and have been guided by the GM with the use of hints that are acceptable by the game rules. Both of the players did not have penetration testing as their main job, they

tended to be either information security researchers or cybersecurity enthusiasts.

More experienced players have found that there was enough information to begin the game, and that Technique cards were realistic and understandable. They have also enjoyed the scenario and described it as 'realistic'.

Another important topic that recurred in the feedback was the multi-player element. A group of players would have liked to see this game as collaborative, and some of the players have pointed out that the current version of the game does not require groups of players, and is good enough to be carried out as a single-player game. Contrary to the initial theory, that players would prefer to play in groups of two, many of the players were perfectly comfortable in a one-to-one session.

6.2 Individual differences

As mentioned in the previous chapter (Section 5.3), there have been three kinds of individual differences scales that have been used in order to better understand the players.

The first measure that has been used is ***Snyder's self-monitoring scale*** (Snyder, 1974). The questionnaire is coded, listing the answers that allow achieving the highest possible score (25), which would indicate that the individual has an exceptionally high self-monitoring scale. A high self-monitoring would indicate better adaptability to social situations, while low self-monitoring would indicate that the behaviour of an individual stays consistent regardless of the social environment.

The resulting distribution is plotted in Figure 6.2. There appear to be two groups present - those with a slightly lower self-monitoring (a small peak around self-monitoring of 10) and those with an average self-monitoring (peak around 15). The mean self-monitoring was 14.5 with the highest score of 22, and the lowest of 8.

The second measure that has been included in the pre-game questionnaire that the participants had to complete was the ***DOSPERT 30*** (Blais & Weber, 2006) scale. The reason for using a DOSPERT 30 as opposed to the original DOSPERT 48 scale was to ensure a higher completion rate. It is also important to note that the internal consistency of the results in the original risk-taking scores ranged from

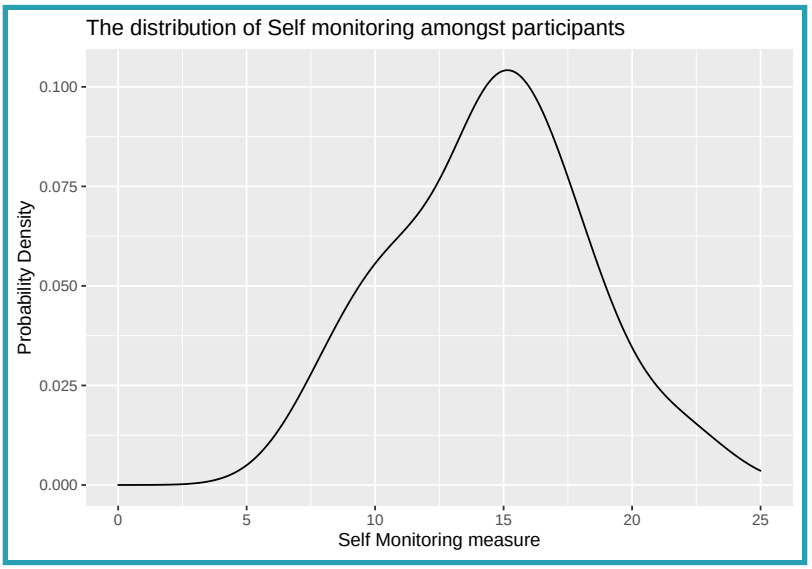


Figure 6.2: The probability distribution of Self-monitoring among the survey participants

$\alpha = 0.70$ to $\alpha = 0.84$ perception as reported by Weber et al. (2002a), meaning that alpha values below 0.8 are to be expected.

Each of the questions in the scale is labelled with a sub-scale it contributes to (*Ethical*, *Finiancial*, *Health/Safety*, *Recreational* and *Social*). All rating scores across the items of a given sub-scale are to be added to produce a total score for that sub-scale. The resulting graph can be seen on Figure 6.3.

Here, we can see the noticeable divide again. The graphs seem to be comprised of two parts, and in the case of Recreational and Social risk perception, they seem to have two distinct peaks.

For each of the sub-categories the scores are shown in Table 6.1.

Measure	High	Low	Mean
Ethical	36	22	29.6
Financial	35	20	28.8
HealthSafety	38	20	31.5
Recreational	35	15	24.1
Social	22	8	15.4

Table 6.1: Risk perception values from the respondents - high and low values.

Adding all the scores produces a general risk perception distribution, shown on Figure 6.4. As the result of the visible divide in all other sub-scores, as opposed

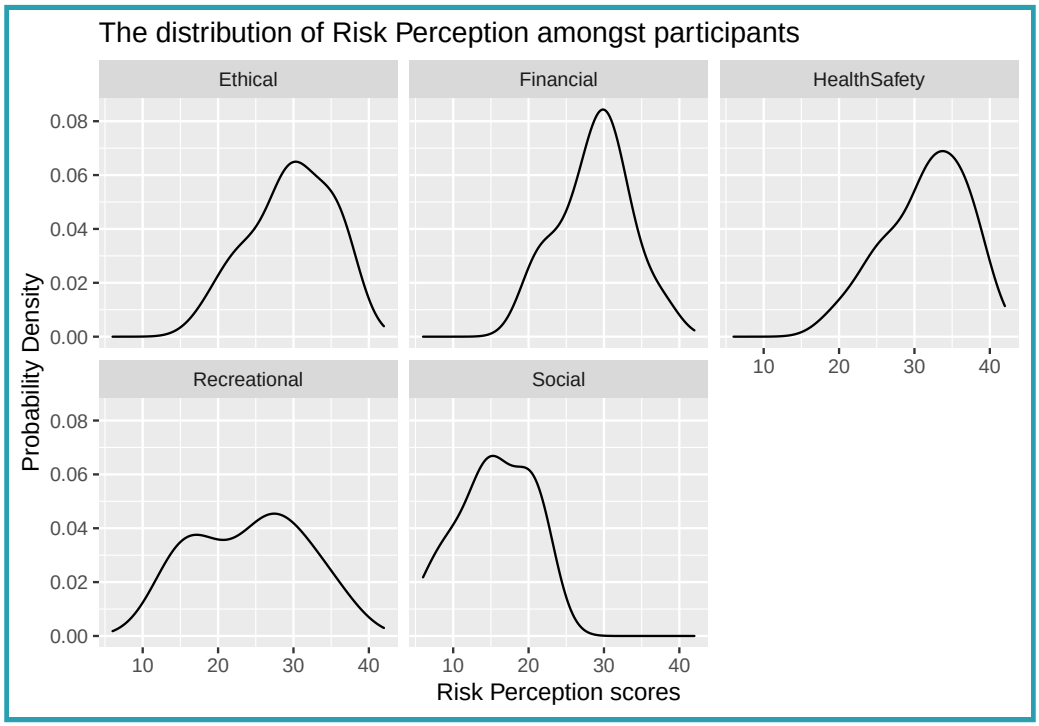


Figure 6.3: The distribution of risk perception by factors

to the perfect bell-shape we have a slightly asymmetric bell curve, indicating the presence of the sub-group that scores lower on risk perception. The mean general risk perception score was 129.5, with the lowest score of 89 and the highest score of 157.

The final questionnaire that was included into the set filled out by the participants is the ***Barratt's Impulsiveness Scale (BIS)*** (Patton et al., 1995). There are 30 questions, each of them has the following responses that are translated into numbers as follows: *Rarely/Never = 1*, *Occasionally = 2*, *Often = 3* and *Almost Always/Always = 4*.

The guide also recommends reporting at least the secondary score, as opposed to reporting a single overall score. The second-order factors are *Attentional*, *Motor* and *Nonplanning*. Each of the second-order factors has two first-order factors, which are: *Attention*, *Cognitive Instability* for *Attentional*; *Motor* and *Perseverance* for *Motor*; *Self-control* and *Cognitive complexity* for *Nonplanning*. Each of the first-order factors has questionnaire items that contribute to it. Some of the questions are reverse-keyed, indicating that a person with high impulsiveness would answer

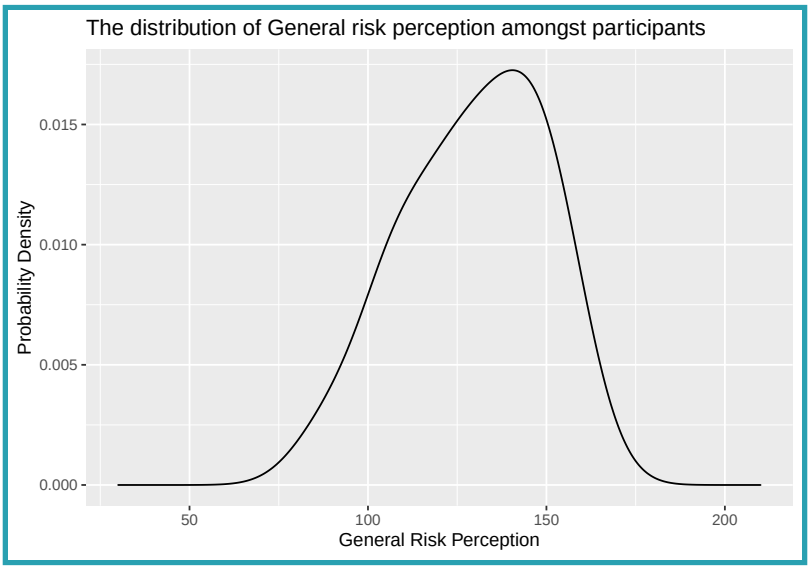


Figure 6.4: General risk perception distribution

negatively to them. The scores would then be added up for each of the first-order measures, and then the scores for the first-order measures would be added up to produce an overall score for the second-order measures. The summary of the scores is given in Table 6.2. The overall distribution is plotted in Figure 6.5.

Measure	High	Low	Mean
Attention	17	8	11.1
CognitiveComplexity	14	5	9.6
CognitiveInstability	12	5	8.1
Motor	24	9	16.2
Perseverence	10	5	7.5
SelfControl	19	7	12.5

Table 6.2: Impulsiveness - first-order factors summary

An overall summary of the second-order factors is given in Table 6.3. The distributions are plotted in Figure 6.6. Here, the two groups are very noticeable, with each of the second-order measures consisting of two parts.

Measure	High	Low	Mean
Attentional	27	13	19.2
Motor	32	16	23.8
NonPlanning	31	15	22.1

Table 6.3: Impulsiveness - second-order factors summary

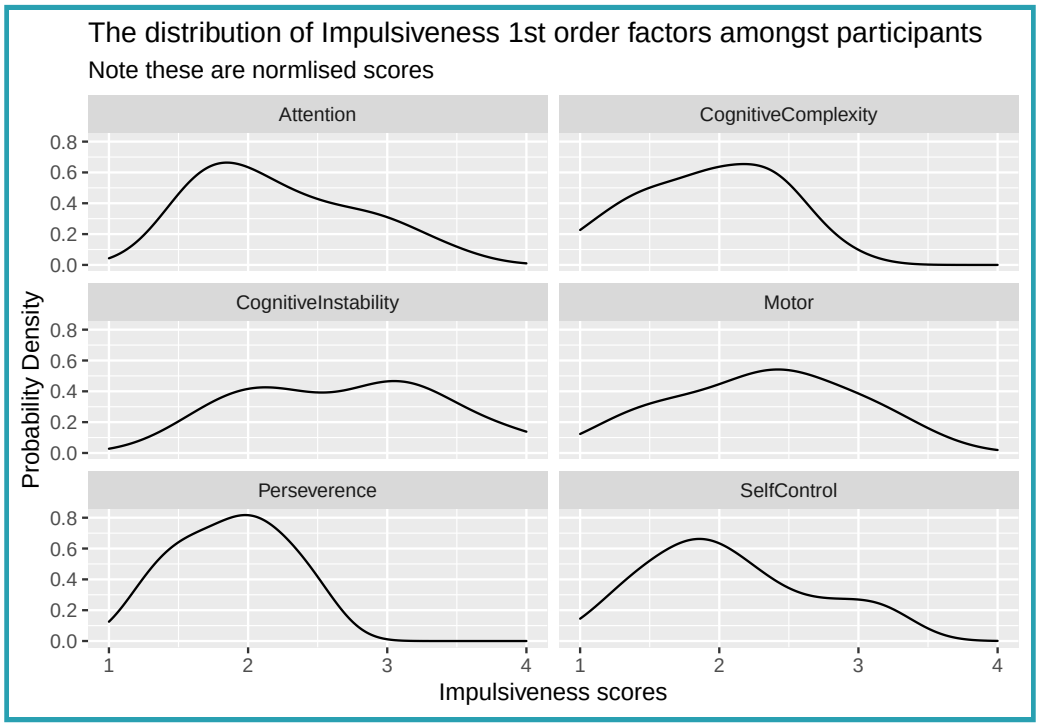


Figure 6.5: A breakdown of probability distributions by first-order factors of Impulsiveness

Let us look at the ***overall consistency*** of the measures, for which Cronbach's Alpha has been used. There are several assumptions to using Cronbach's Alpha. The first assumption is that there is no correlation between the error terms. We do not want a great variability due to error for each of the factors, we want each of the factors to be indicative. The second assumption is that the items are tau-equivalent, meaning that in this model all factor loadings are equivalent to each other. No one indicator is more important than the other, and their almost equal importance takes effect on their factor loading.

Figure 6.7 shows the alpha scores for all of the individual difference measures. Usually, the values of alpha scores of 0.8 or higher are considered good (indicated by the right-hand side, green line on the graph). For our analysis, only a handful of the measures are around that mark. Hence, a lower threshold value of 0.7 (indicated by the left-hand side, red line on the graph) has been considered the cut-off point instead, with the Impulsiveness (2 - Motor) being the last significant scale. The reason for including Impulsiveness (2 - Motor), even though it falls just below the threshold is because it allows us to have a complete set of second-order factors, while

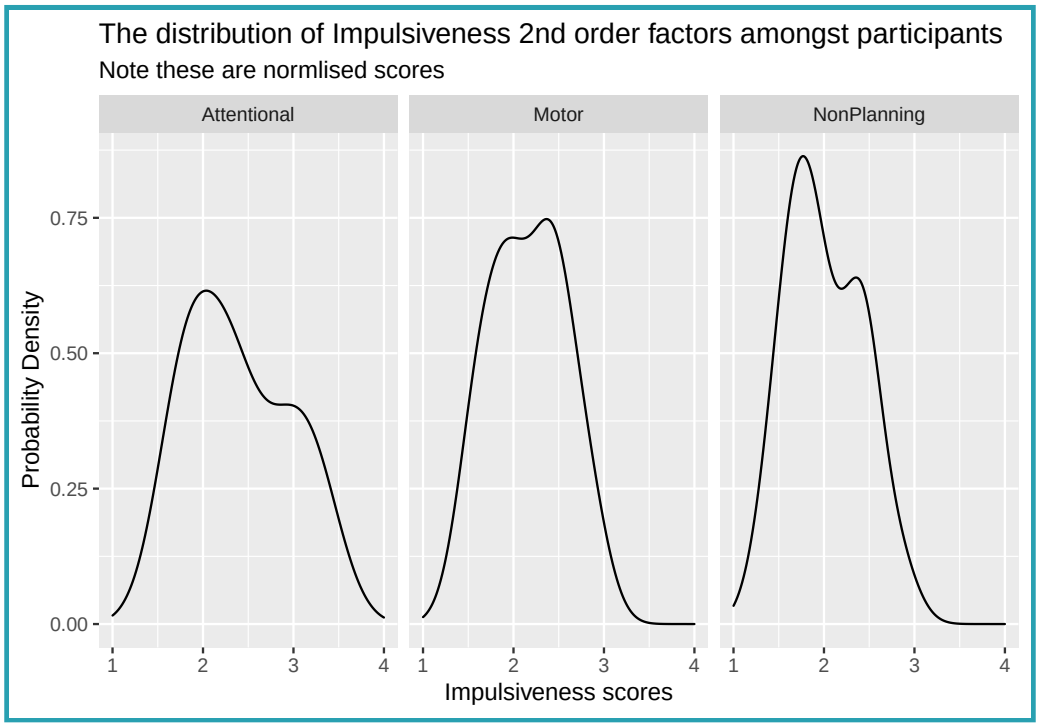


Figure 6.6: A breakdown of probability distributions by second-order factors of Impulsiveness

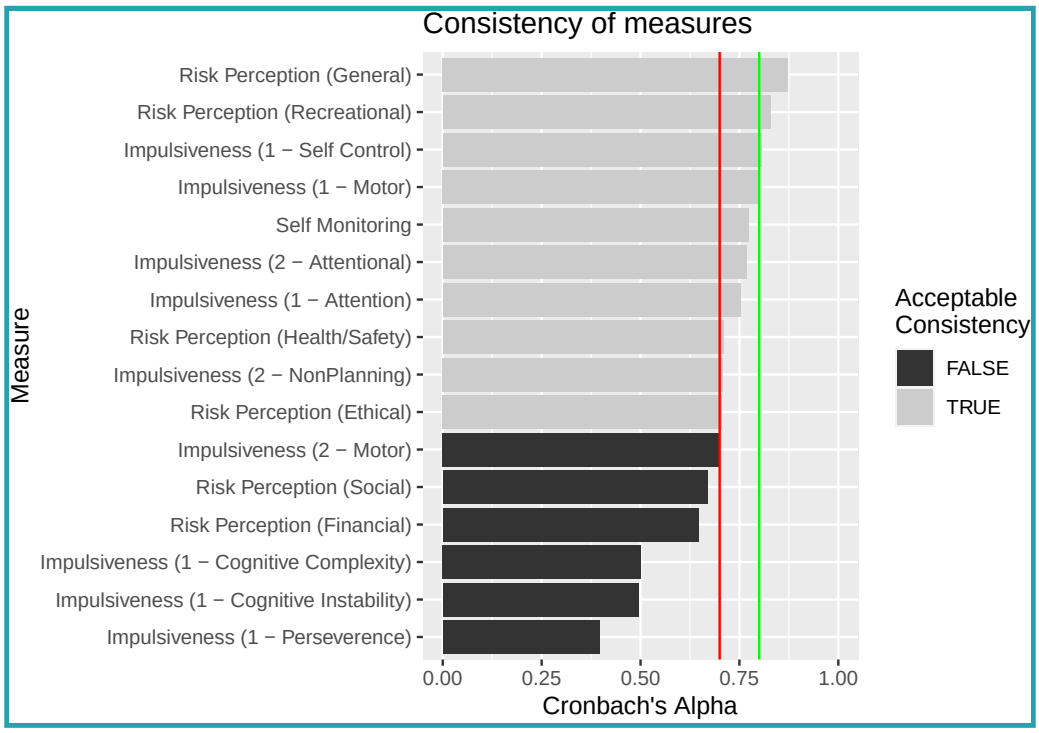


Figure 6.7: Consistency of measures (Cronbach's Alpha). As there were not enough of measures that were on or above 0.8 alpha score, a threshold of 0.7 has been used instead. The grey bars indicate measures with the acceptable consistency.

most of the first-order factors have fallen below the threshold, with the second-order only one of them is just about below the threshold, and not by a significant amount. The most consistent result is the general Risk perception (DOSPERT) value, with the least consistent being the first-order measure for Impulsiveness (Perseverance). The values that correspond to the chart are listed in Table 6.4.

Measure	**Alpha**
Risk Perception (General)	0.87268246878755
Risk Perception (Recreational)	0.828641713961188
Impulsiveness (1 - Self Control)	0.80540603458843
Impulsiveness (1 - Motor)	0.802024233614176
Self Monitoring	0.773089434892851
Impulsiveness (2 - Attentional)	0.767867840867397
Impulsiveness (1 - Attention)	0.75265707710202
Risk Perception (Health/Safety)	0.709764341835443
Impulsiveness (2 - NonPlanning)	0.708498940810586
Risk Perception (Ethical)	0.705453023264052
Impulsiveness (2 - Motor)	0.698453658607053
Risk Perception (Social)	0.668928462396073
Risk Perception (Financial)	0.646555016225431
Impulsiveness (1 - Cognitive Complexity)	0.500564499175556
Impulsiveness (1 - Cognitive Instability)	0.494971286307819
Impulsiveness (1 - Perseverence)	0.396839905582687

Table 6.4: Consistency scores for every measure, sorted with respect to Figure 6.7.

Figure 6.8: Each of the three questionnaires, all sub-orders in correlation to each other

The first-order measures from the Impulsiveness scale will not be considered, as there is not enough consistency in some of them (such as 1 - Perseverence, or 1 - Cognitive Instability). Instead, as mentioned above, the second-order measures have been chosen. With this in mind, there is a total of eight measures that have been deemed to be consistent enough to be used in our study. Let us now have a look if there are any correlations between the measures. The correlation graph is shown in Figure 6.8. There are no significant inter-scale correlations, apart from a link of Self-monitoring and Impulsiveness Non-planning. Intra scale correlations include various sub-levels of the Risk Perception scale, and, separately, there are some correlations between the different sub-orders of the Impulsiveness scale.

In our study, we had 15 participants, with the individual differences plotted across eight dimensions. Using a cluster analysis we can group individuals across all eight dimensions. The first task is to identify how many clusters exist within the

dataset. For this, we are going to use two methods: a Silhouette analysis and Sum of Squares Within (SSW).

We begin with ***Silhouette analysis***, which is used to measure the consistency of data clusters. Its objectives are to determine how similar is it to its own cluster compared to other clusters. A higher value would indicate that it is well-matched to its own cluster and poorly matched to the neighbouring ones.

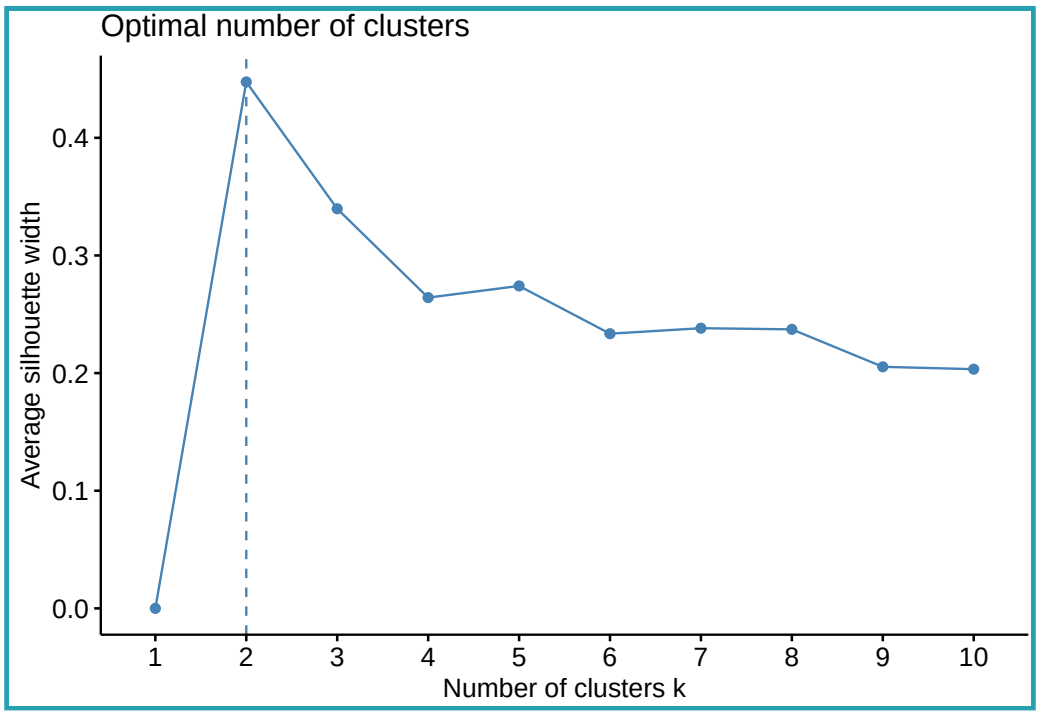


Figure 6.9: Determining an optimal number of clusters (Silhouette Analysis)

The Silhouette analysis is shown in Figure 6.9. In our case the highest width is two, indicating that two clusters would be optimal in this configuration.

The next analysis technique that we will use is the ***Sum of Squares Within (SSW)***. The aim of SSW is to find the balance between large and less accurate clusters, and smaller clusters with not many individual points in them. It does this by calculating the distance between the points and analysing how close are the points to each other. For this analysis we are trying to select a value that would be somewhere in the middle - not too high, but also not too low. SSW graphs tend to have an elbow shape.

The resulting graph is shown in Figure 6.10. The analysis is suggesting to have two or three clusters. Let us plot both of the arrangements on the graphs.

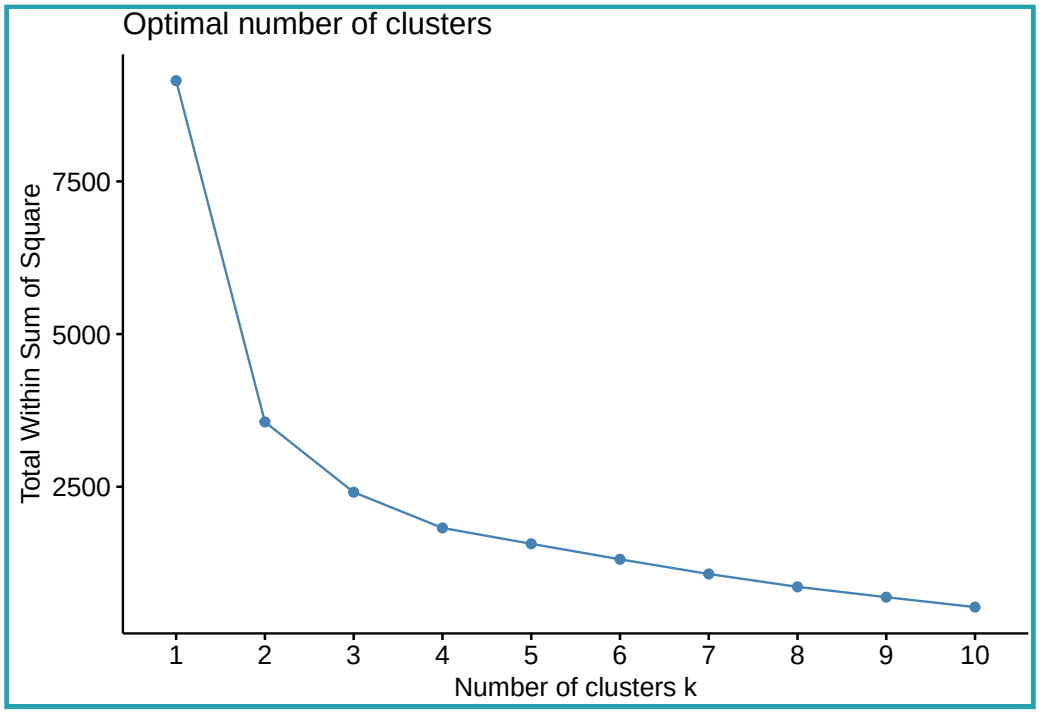


Figure 6.10: Determining an optimal number of clusters (Sum of Squares Within)

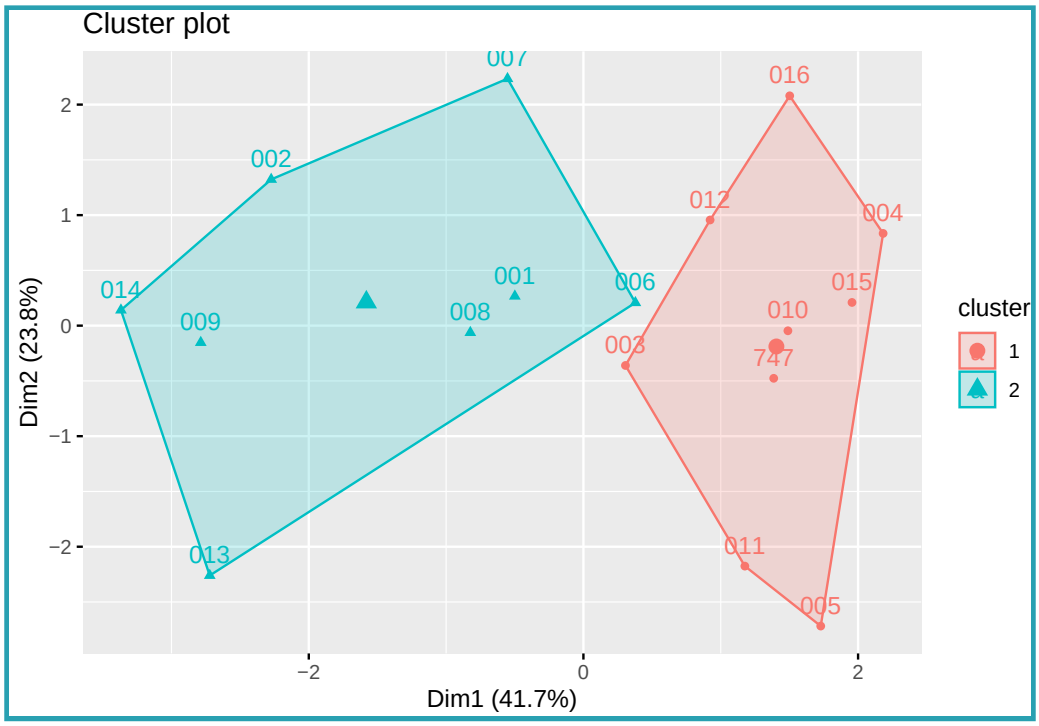


Figure 6.11: Cluster plot (survey responses grouped into two clusters)

The eight dimensions shown in Figure 6.8 have been flattened into just two using a process called principal components analysis. Each of the eight dimensions is compared with each other to spot the greatest difference. This way, the dimensions are not removed, but the information from them still contributes to the overall visualisation. The resulting representation can be seen in Figure 6.11. The first dimension (Dim1) has a variance of 41.7%, dimension two (Dim2) has a variance of 23.8%. The overall variance is a combination of two, yielding a total of 65.5% variance.

To split the results into three clusters instead of two, there were several steps that have been followed. First, the Euclidean distance between the points has been calculated, then hierarchical clustering has been applied. In our case, cluster one has been left untouched, while cluster two got separated into clusters two and three. The resulting visual representation of all three clusters can be seen in Figure 6.12.

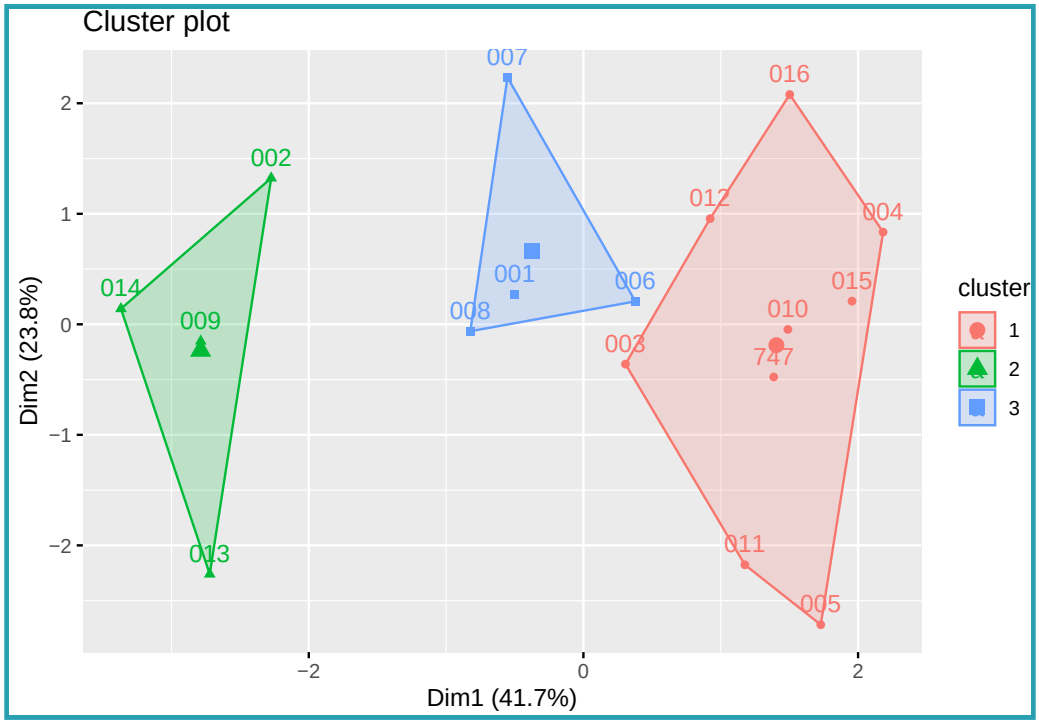


Figure 6.12: Cluster plot (survey responses grouped into three clusters)

6.3 Cards that were played

First of all, let us examine whether the Role card the participant played has any effect on the number of techniques used. For this, the game transcripts have been broken down to one role per file and all instances of technique cards have been counted. The resulting box plot is shown on Figure 6.13. State-backed (high capability) has the highest variance – people representing this role have used both a lower number of techniques and a higher number of techniques. The lowest variance is the Hacktivist role, the number of techniques used is between six and seven.

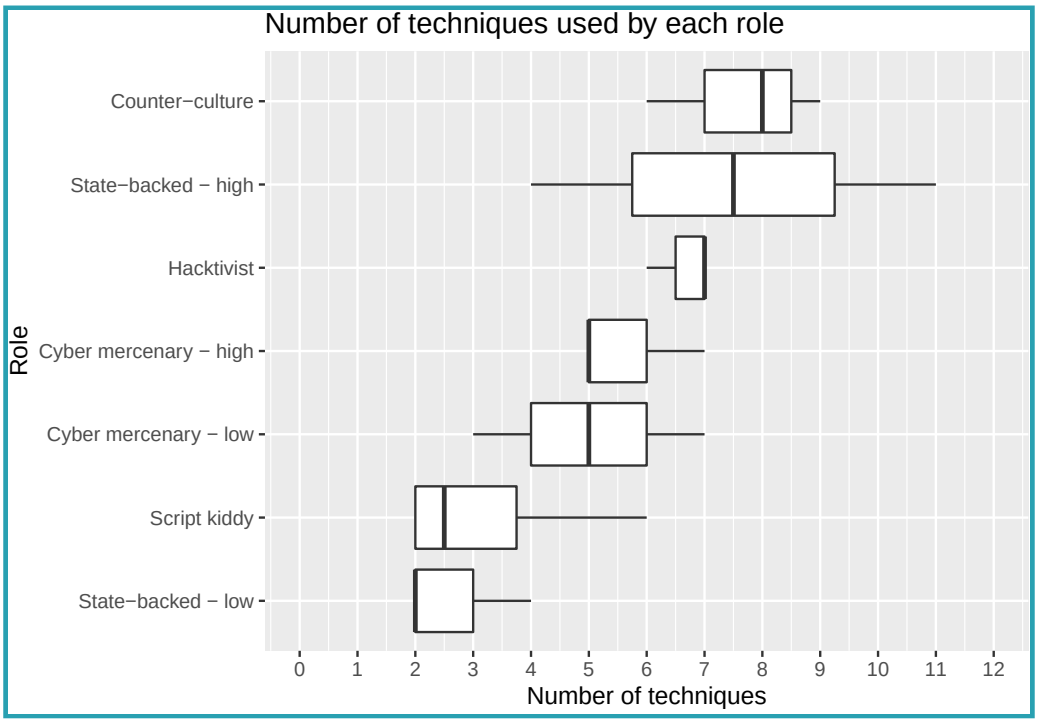


Figure 6.13: Technique numbers by roles

Now let us plot the frequencies of all cards. For this, all instances of all 13 techniques have been counted across all game files. The graph is available in Figure 6.14. `T09` (Spearphishing Link) has become the most used Technique card (26 times), followed by `T10` (Trusted relationship) at 19 times, followed by `T13` (Man in the Browser), at 12 times. The least used technique is `T01` (Exploitation for Client Execution), which has, interestingly, never been used in the conducted games, followed by `T06` (Exfiltration Over Alternative Protocol), used only twice.

Next, let us look at the probability of a certain technique being used by a specific

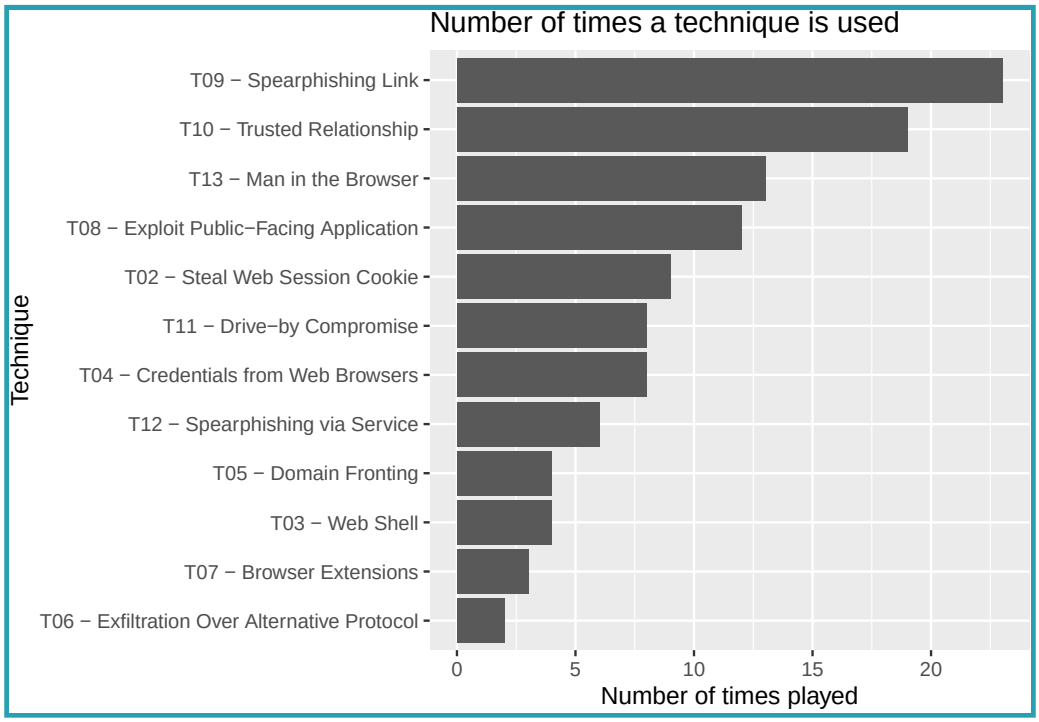


Figure 6.14: Overall Technique card frequency

role. The results have been normalised by dividing the number of times a particular technique has been played by the overall number of cards played by each role. As each role is not played the same number of times, this gives us an expected percentage of time that a given technique is used per role. The resulting graph is available in Figure 6.15. Counter-culture and Hacktivist have the greatest variability in Technique cards, while Cyber Mercenary (low capability) and State-backed (high capability) have the least breadth.

We want to determine whether players choose a specific card because of their role, or if there are any other factors that influence their choice, perhaps something about the card characteristics. Let us now investigate whether players choose the card based on any of its three properties:

- Impact Factor
- Recon Factor
- Risk number

For this, we will be using an analysis of variance (ANOVA), which measures the

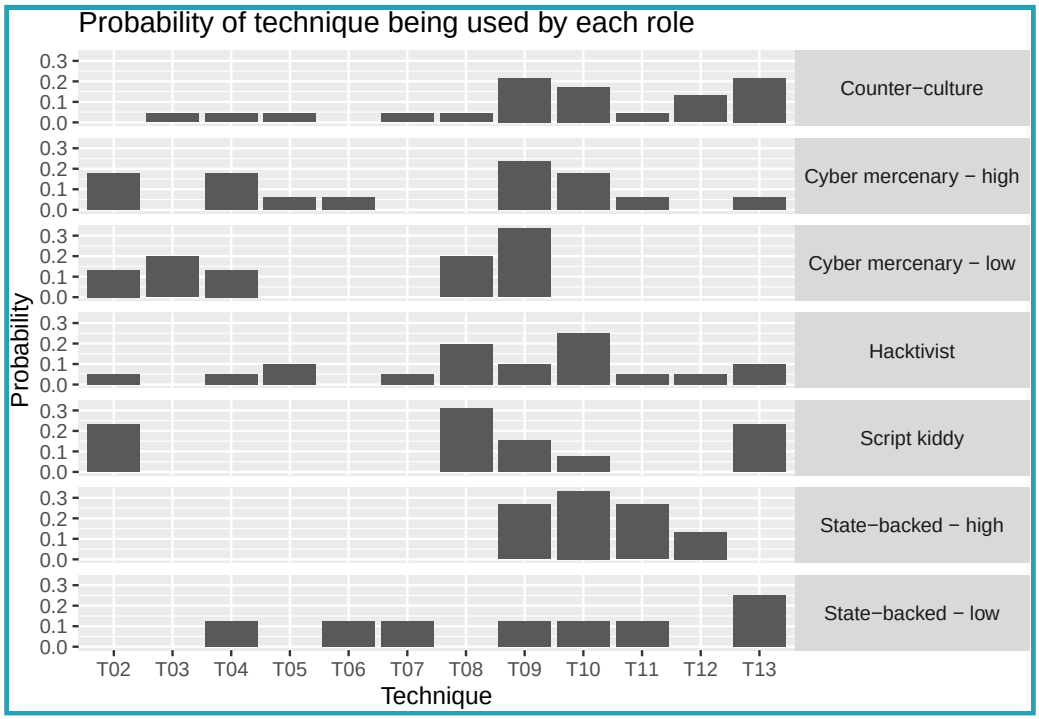


Figure 6.15: Technique card distribution by role

relationship of the dependent variables (in our case these are the card's individual statistics) on the independent variable (card pick rate in our case). The result is shown in Table 6.5.

	df	Sum Sq	Mean Sq	F value	Pr(>F)
Impact factor	1	0.56	0.562	0.0122	0.9148
Recon factor	1	2.15	2.148	0.0465	0.8346
Risk points	1	94.15	94.148	2.0390	0.1912
Residuals	8	369.39	46.174		

Table 6.5: Analysis of Variance Table. This table determines whether there is any effect of Impact/Recon factors or number of Risk points on the Technique card pick rate. df stands for degrees of freedom.

The p-value is very high for Impact and Recon factors and still remains above 5% for the Risk points. Some assumptions have been made for this analysis. The first assumption is that our participant pool is normally distributed. The second assumption is that the variances of the populations of the samples are equal. The final assumption that has been made in producing this table is that the observations within the groups are independent of each other and have been obtained from a random sample.

The next step is to determine whether there is any effect individual differences have on the roles. Can the results show us any correlations? Let us try to break down the specific individual differences clusters playing a specific role. The result is shown in Figure 6.16. There is not enough data to show any significant relationships with the current sample size. `R01` is one of the only diverse roles that has a spread of all three clusters playing different techniques, but there is not enough evidence to derive any significant patterns.

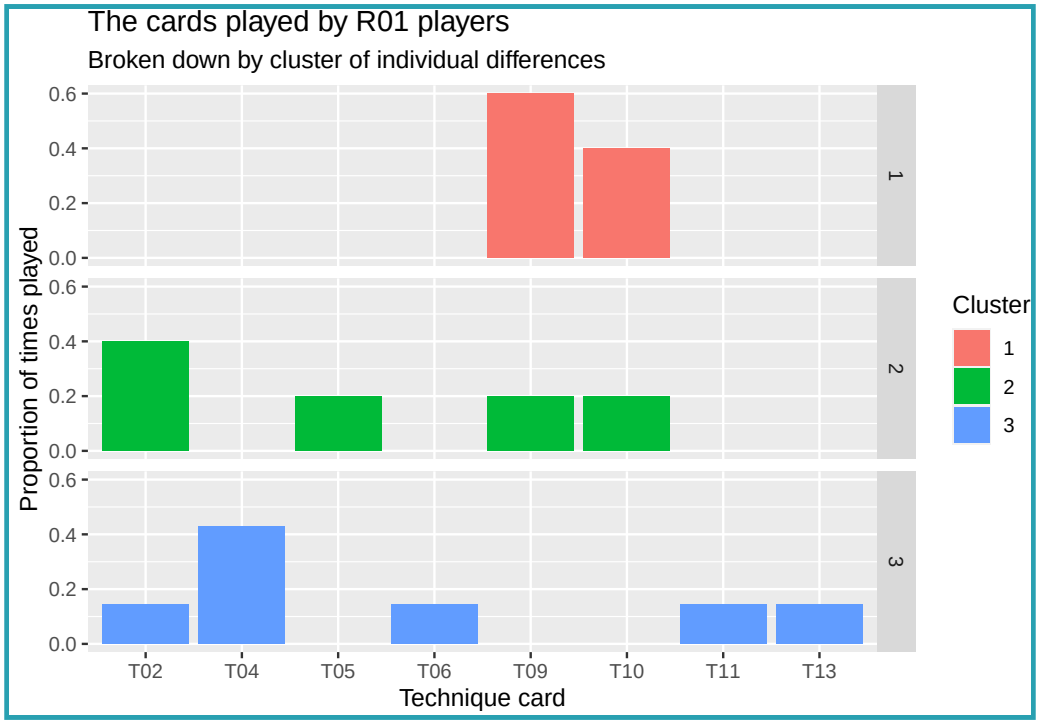


Figure 6.16: The cards played by R01 players

Up to this point we have assumed the cards are independent of each other. However, a technique viewed out of context can only disclose a limited amount of information about the current attack and about the attacker. We would want to see techniques used in context, as this way it is possible to see attacks being formed by the attacker to achieve a specific goal. ***Technique card chains*** will let us examine cards played in a specific order. For this, we take the sequences of cards played and make a transition matrix, which we then convert into a graph (Figure 6.17). Here, we can see that some techniques used enable other techniques, such as T04, while others do not get followed up by other techniques, and are instead terminating nodes, such as T06.

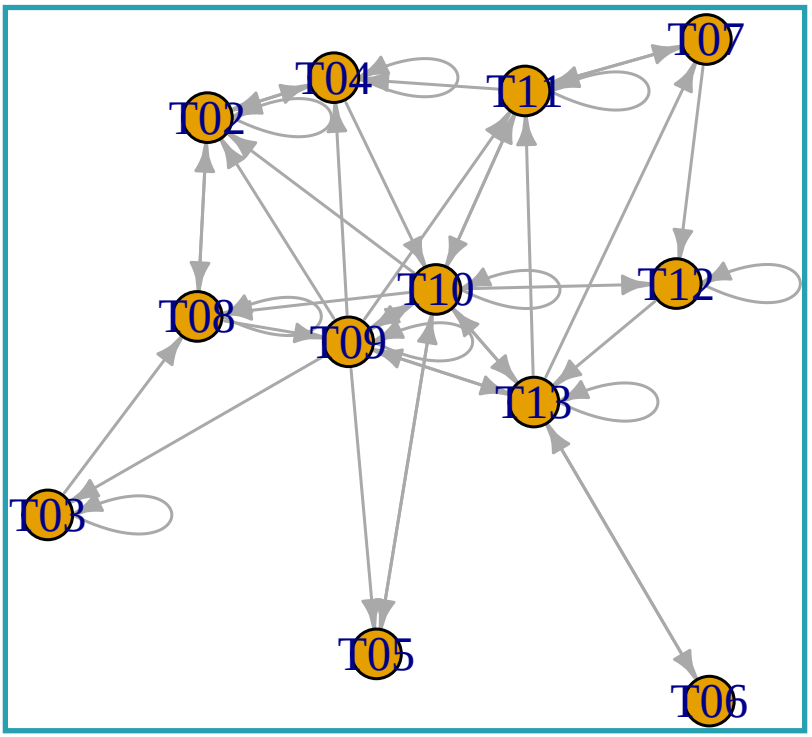


Figure 6.17: Technique transitions

To explore the role techniques play in enabling the outcome, let us measure the ***betweenness*** of all technique nodes. Mathematically, suppose we want to find the shortest path between point A and B. Betweenness measures the number of shortest paths that go through a node that is located between A and B. The formula for calculating betweenness is given in equation 6.1:

$$g(v) = \sum_{s \neq v \neq t} \frac{\sigma_{st}(v)}{\sigma_{st}} \tag{6.1}$$

v is the node for which the betweenness needs to be calculated. s and t are the points A and B in this case. σ_{st} is the total number of shortest paths from node s to node t, $\sigma_{st}(v)$ is the number of shortest paths that pass through v.

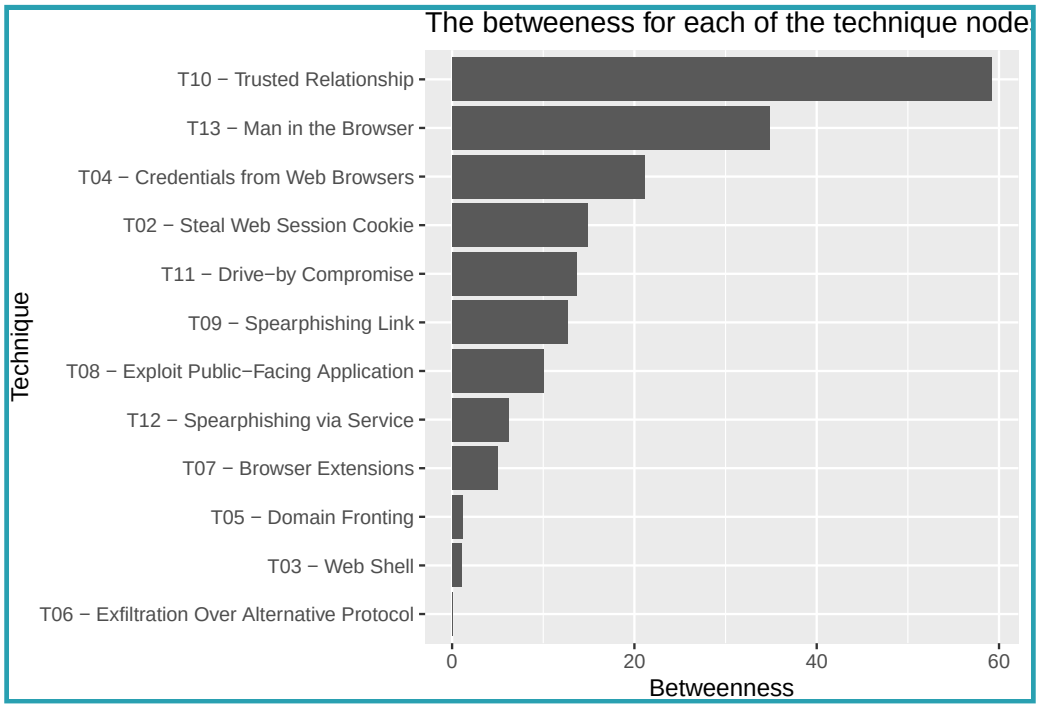


Figure 6.18: The betweeness for each of the technique node

When put in the game context, betweenness of the node would indicate how many attack graphs can be enabled by a given technique. This will allow us to compare, which technique nodes enable more complete attacks, and which ones do not contribute to an attack as much as expected. The resulting bar chart is shown in Figure 6.18. We can see that `T10` (Trusted Relationship), `T13` (Man in the Browser), and `T04` (Credentials from Web Browsers) have the highest betweenness, and a higher degree on the previous graph (Figure 6.17). The lowest betweenness is for `T06` (Exfiltration Over Alternative Protocol), `T03` (Web Shell), and `T05` (Domain Fronting).

We know which techniques have the highest betweenness. How does this compare to how often those techniques are chosen by the players? Do players choose the techniques that are beneficial in the short term, or would they favour the techniques that enable more possibilities? The graph below (Figure 6.19) shows the betweenness of a technique plotted against the pick rate. Notably, `T10` (Trusted Relationship) has both high betweenness and a high pick rate, but `T09` (Spearphishing Link) is picked often while having a low betweenness.

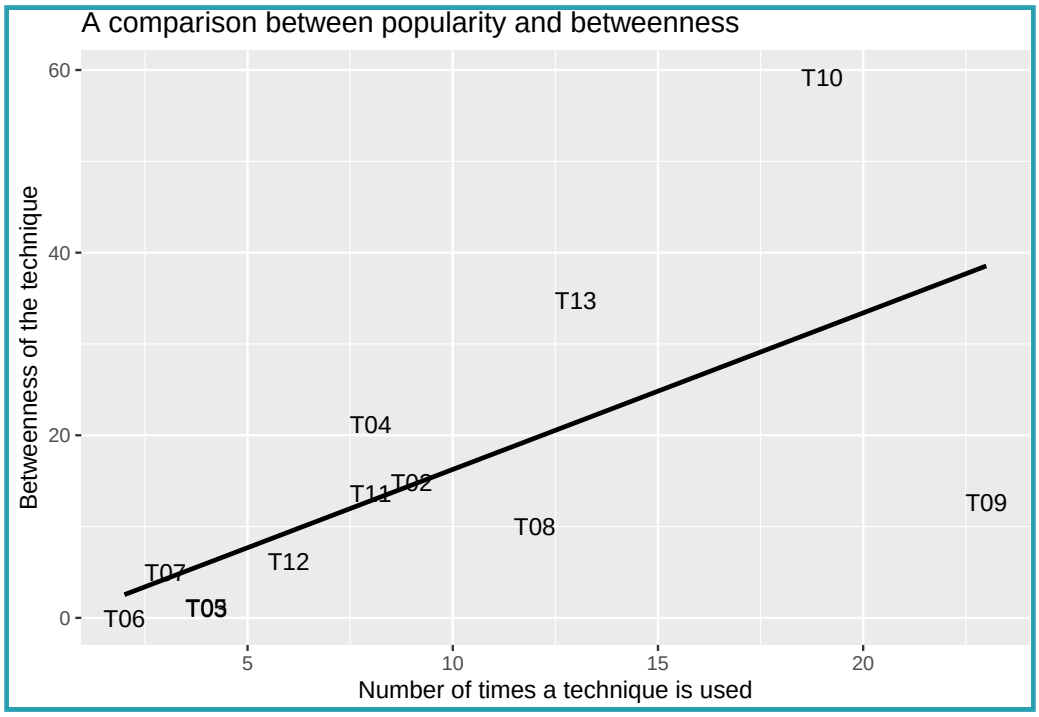
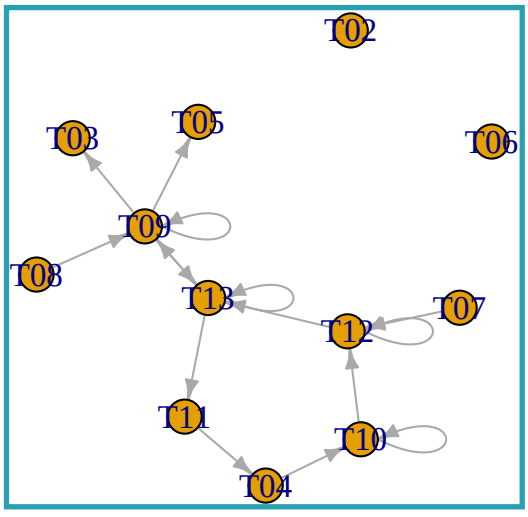
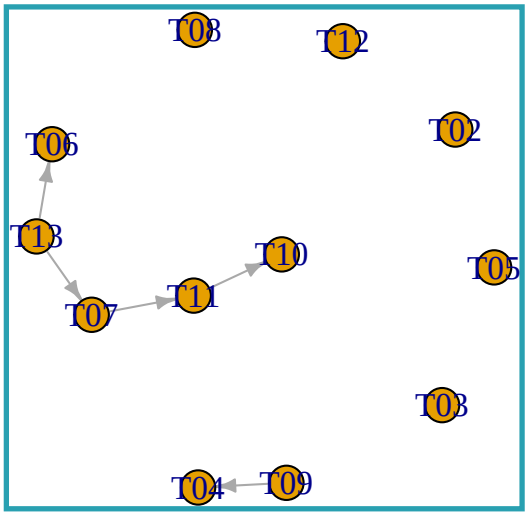


Figure 6.19: A comparison between Technique card popularity and betweenness



(a) R03 (Counter-culture) Technique transition graph



(b) R06 (State-backed [low capability]) Technique transition graph

Figure 6.20: Role-specific technique card transitions.

Let us examine whether an individual role played has any effect on the Technique card chains and whether the selected techniques are followed up often. Depending on the role there can be different card usage patterns, as can be seen in Figure 6.20. On the left-hand-side (Figure 6.20a) we can see the transition graph for `R03` (Curious Lone Wolf, a Counter-culture sub-type), where many sequences of techniques can be seen, it is a far more connected graph than the graph on the right-hand-side (Figure 6.20b). The graph on the right-hand side belongs to `R06` (The Observer from the Island, or State-backed [low capability]), and has far fewer techniques that are connected together.

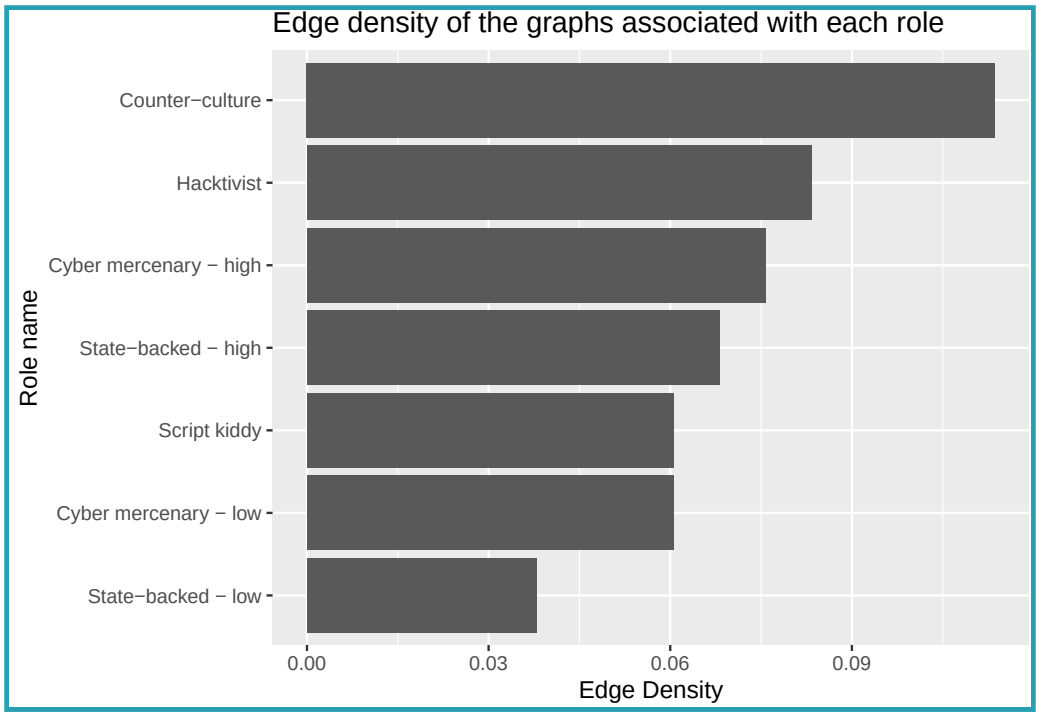


Figure 6.21: Edge density of the graphs associated with each role

Continuing with the subject of usage patterns, Figure 6.21 shows how connected are the graphs (their edge density) for every single role. The edge density indicates how many different techniques does each role use. Having a high edge density would indicate the variability of techniques. A low edge density would be akin to following a pre-defined path of techniques, such as in organisations with rigorous attack procedures. The highest edge density belongs to `R03`, the Counter-culture sub-type (which corresponds to the graph on Figure 6.20a), followed by `R04` (A Group with a Purpose, Hacktivist), while the lowest edge density occurs in `R06`

(The Observer from the Island, or State-backed [low capability]), corresponding to the graph on Figure 6.20b.

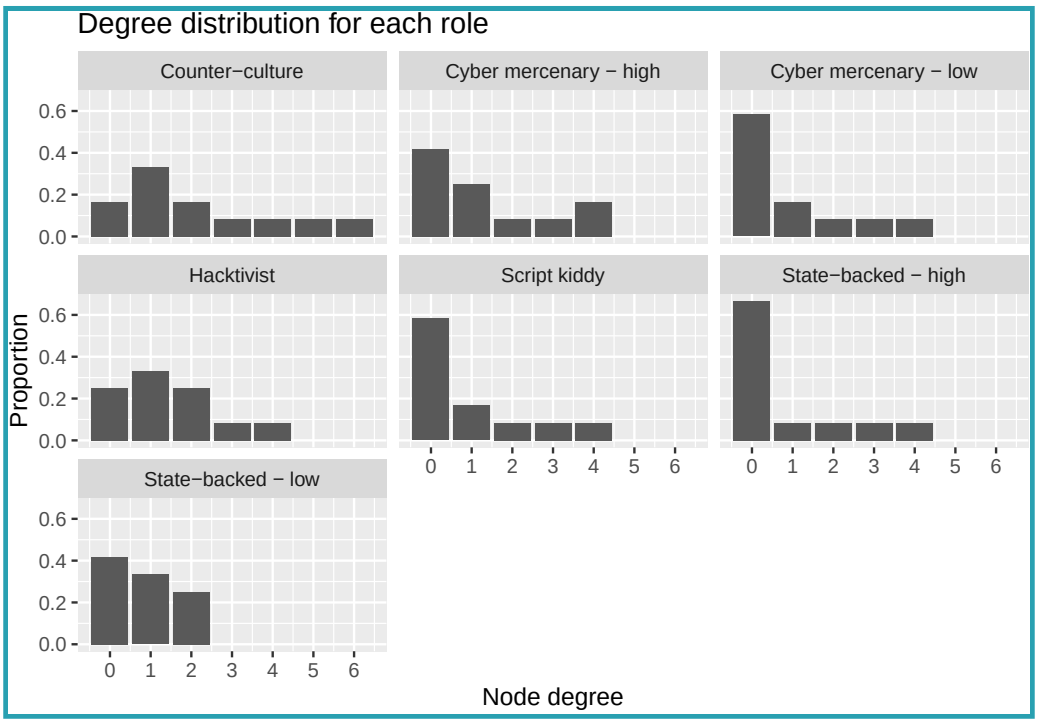


Figure 6.22: Degree distribution for each role

Figure 6.22 shows the ***degree distribution*** per specific role. The lower-capability roles tend to have less complex graphs, while the higher-risk-point roles tend to have a higher graph complexity.

Now let us examine whether the individual differences have any effect on the edge density. The resulting graph is plotted in Figure 6.23. Here, a more noticeable difference can be observed, with the individual differences in cluster number one using a wider variety of different approaches, while cluster three prefers to rely on a set pattern of activity.

Figure 6.24 shows the degree distribution per every individual difference cluster, with group one having the highest degree distribution, while group three has the lowest degree distribution per all nodes.

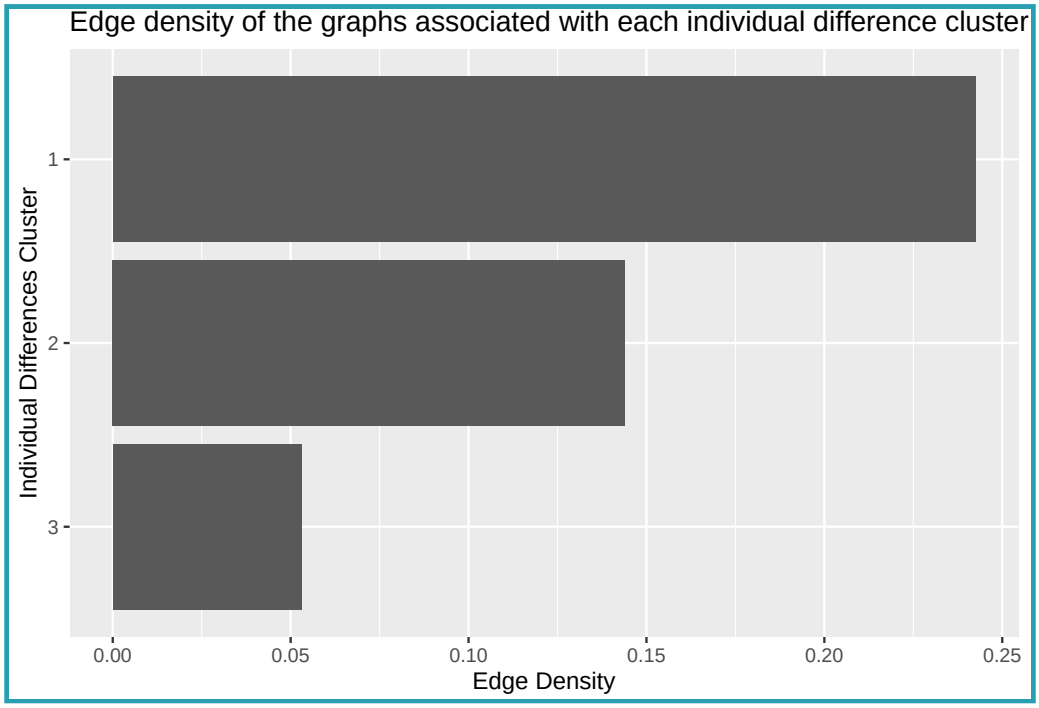


Figure 6.23: Edge density of the graphs associated with each individual difference cluster

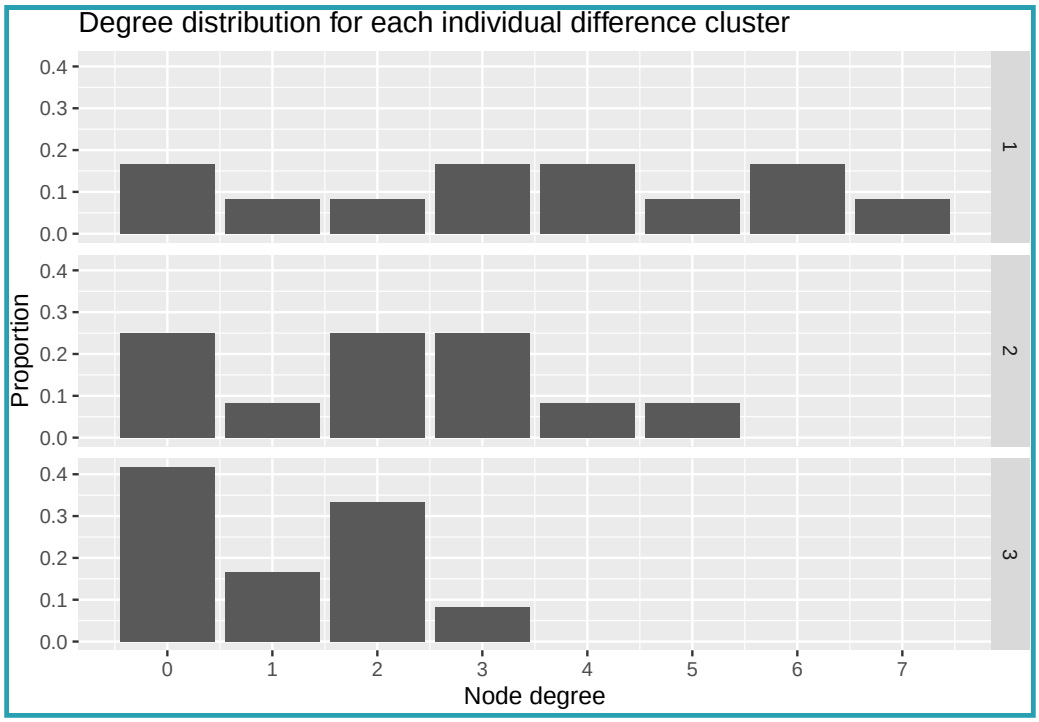


Figure 6.24: Degree distribution for each individual difference cluster

6.4 Simulation results

The simulation provides a visual aid of the game library - it illustrates the agents and matches them to the respective games. It is possible to see the progress of every role by viewing the next steps, which in turn, provides a comparison mechanism for the roles.

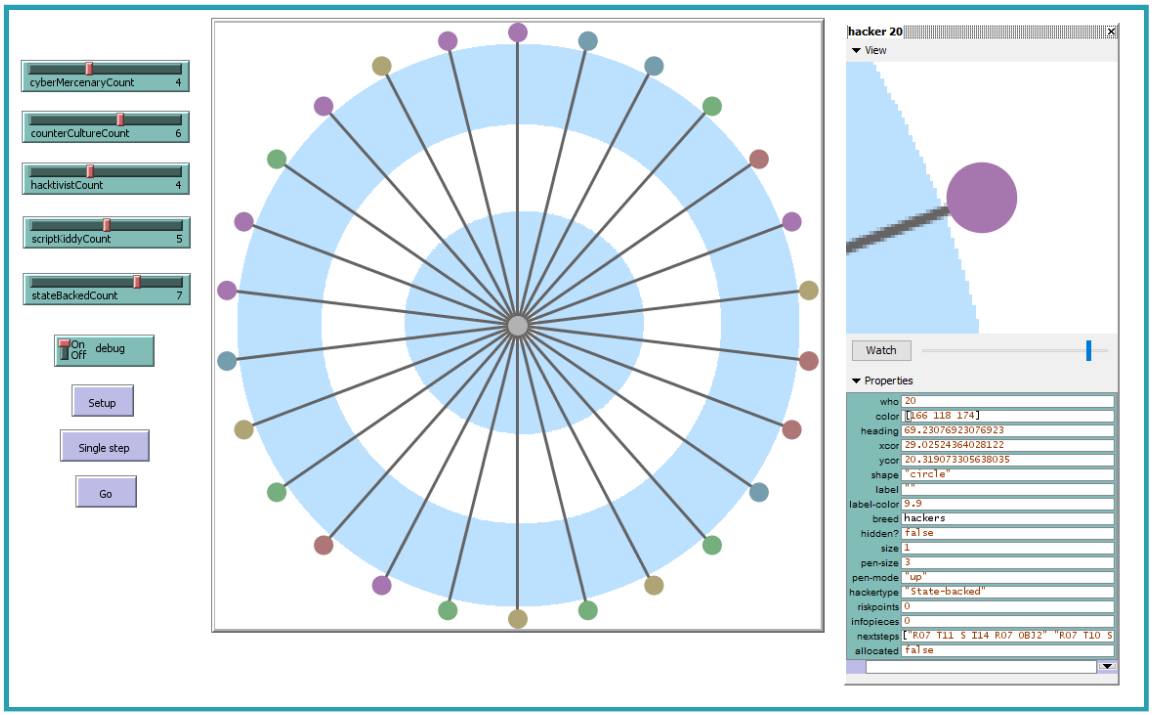


Figure 6.25: The simulation showing progression steps. The numbers and types of agents in this screenshot are: 7 State-backed (purple), 4 Cyber Mercenary (blue), 6 Counter-Culture (green), 5 Script Kiddies (mustard) and 4 Hacktivists (red). The progression is indicated by the `nextSteps` field.

An arbitrary number of attackers within the roles can be created, which allows to model different attack scenarios. A screenshot of the simulation is shown in Figure 6.25.

Summary

At the beginning of this project, we have set out the following research objectives:

> *1. To build a realistic game based on rigorous evidence*

As we have seen from the card usage patterns, some simpler TTPs, such as Spearphishing Link (T09), which is a technique that also frequently gets used in malicious cyber operations, even by state-backed actors to establish an initial foothold. Other TTPs, such as Trusted Relationship (T10) gets used to enable other pathways, similar to supply chain attacks. Thus, by using realistic TTPs, the patterns that emerge can be mapped to the attacks that can happen in the real world.

> *2. To ensure that the game enables players to make decisions that reflect their true intention*

Players have individual differences, and every role has a set of goals that players need to achieve. Players can move towards these goals, and to declare intention they can write the technique that they are going to use in the dedicated text channel space. We can also note that the decisions players make vary not only in their choice of a technique but also in how these techniques are put together to form attacks.

> *3. To devise an efficient approach to the recording of the game decisions*
> *4. To ensure the events within a game can be restored from the recording, with semantics preserved*

We have two key stages - during the game, where the decisions are made and after the game, where the decisions get processed. As the decisions are made by the player, a snapshot of them is stored in a dedicated text channel. This text channel is subsequently locked to prevent players from potentially editing their responses and stored for future processing. As the information is processed, it is put into a text file into a condensed format, together with the player's identifying number and date the game has taken place. This ensures that at every stage game decisions are recorded and retrieved efficiently. The text file contains information on what Technique cards have been used, what role has been played (allowing to restore a set of objectives associated with that role), and the outcome of every move, along with any actions that followed from the GM.

5. To ingest the game decisions into a simulation

The simulation is capable to store game decisions. Each agent has an attacker type that corresponds directly to the role in-game, and also a malicious cyber attacker type. Each agent is matched with a game file that stores decisions from the game and maps them into a simulation.

Overall, players have enjoyed the resulting game and found the overall look and feel of the game fun and aesthetically pleasing. Players have also indicated that the addition of an interactive collaboration mechanic (players interacting with each other) would highly benefit the game, as well as including some cards that would permit the players to do the enumeration.

The results from the individual differences questionnaires have found that there are three different groups of people with similar characteristics, that also seem to have an effect on the play styles that those players use.

The two most used techniques are Sphearphishing Link and Trusted Relationship, and the effects from using these two techniques are completely opposite of each other - one seems to enable very few further techniques, while the other seems to be quite important in enabling the rest of the attack graph.

Roles also have different attack graph complexities. Higher capabilities seem to have access to a broader set of TTPs, while lower capabilities seem to have little variety in the techniques that they employ.

Finally, the simulation displays the decisions made by the players in the game.

Chapter 7

Discussion

This chapter will discuss the results and their implications. At the beginning of this project, we have set out to accomplish the following objectives:

1. *To build a realistic game based on rigorous evidence*
2. *To ensure that the game enables players to make decisions that reflect their true intention*
3. *To devise an efficient approach to the recording of the game decisions*
4. *To ensure the events within a game can be restored from the recording, with semantics preserved*
5. *To ingest the game decisions into a simulation*

In the previous chapter, we have demonstrated that we have achieved all of the objectives specified here.

It is also important to note that all of the above have been achieved with the following constraints in mind:

1. *Each player can represent an entity, such as an APT group or a Hacktivist group. However, there is only one player for one entity, and the*

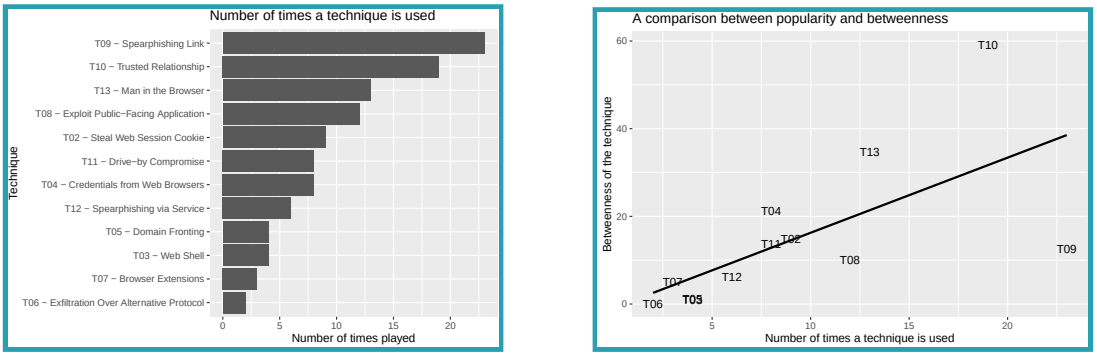
collaborations between players or entities are not explored.

2. *This project does not focus on insiders and insider threat - it only considers external attacks and attackers*

3. *An Agent-Based model does not feature agent-to-agent interactions*

7.1 The game outcome

In the previous chapter, we explored the results from the research project. We have seen that certain cards get played more frequently than others, especially `T09` (Spearphishing Link) and `T10` (Trusted relationship). The frequency did not always necessarily reflect how much additional lateral movement this technique enables; the comparison between usage frequency and betweenness (enabling additional attack complexity) is shown in Figure 7.1.



(a) Overall Technique card frequency, in descending order

(b) Card popularity and betweenness, compared

Figure 7.1: Role-specific technique card transitions.

Firstly, the two most prevalent techniques are spearphishing and trusted relationship, both relatively straightforward techniques that have been effective nevertheless.

As explored before, spearphishing is a simple technique that requires little technical knowledge. However, there are two factors that make it incredibly effective. Number one is if the spearphishing link or message can be crafted to look very believable. The emulated website looks legitimate, and the only factor that gives it away is, for example, that it is a homograph attack (Gabrilovich & Gontmakher,

2002) (one of the letters in the domain name of the website is replaced by a character that looks identical but is from a different alphabet). Alternatively, there could be an extra letter in the domain name (e.g. `faceboook.com` instead of `facebook.com`). Factor number two is if this letter appears to be anticipated, e.g. it is a subscription service renewal letter). With these two factors, even security researchers can fall prey to this attack. These two factors, coupled with its simplicity, are the reasons why it is still actively in use both during APT campaigns and with the lone-wolf attackers. We can see the same trend in the game as well, where players representing all attacker roles have resorted to using this technique.

The second most popular technique is, again, a technique that requires less technical setup and more of the open-source intelligence — trusted relationship. This technique is evidently popular with malicious state-backed attackers and non-state APT groups that use supply chain attacks to sabotage a specific organisation. This is again a very common attack seen in critical national infrastructure (SANS, 2019). Techniques that come after these two are more technical. One exception is the Spearphishing via Service card, but this could probably be due to players preferring Spearphishing via Link instead. These two techniques serve as an entry point, both in-game and in the real world, so we could expect them to be more common than others.

Another point that is worth mentioning is that the least popular Technique card is Exfiltration over Alternative Protocol. Out of all cyber attacks that occur in the real world, only the minority get to successful completion, and out of these attacks, not many require an alternative protocol to exfiltrate data (unless it is part of a sophisticated campaign). Then again, this could be due to there not being a need to explicitly declare data exfiltration during the scenario, as the goal is deemed complete as the player first accesses the required information, as opposed to downloading it.

A rather unusual occurrence is the number of times a web shell has been used as part of a campaign. Web Shell has ended up to be only the third least played card, while the expectation has been that it would get played far more often (as it is a technique for establishing persistence). However, not all of the roles in this scenario

needed to establish persistence via specifically using a web shell (as opposed to a regular shell and a link sent via a spearphishing email), so this still aligns with what would happen in the real world.

Secondly, during the above analysis, we have viewed each card independently, but what happens when the cards are examined in sequence? In the real world, attacks are rarely viewed independently; they group together, allowing the broader attack context to be seen. An example of an attack context would be the underlying goal that the attacker is pursuing or looking at the attacks as part of a single kill chain. An attacker would use an attack technique to gather initial recon, some techniques to gain initial access, another technique to establish persistence, and then some techniques for lateral movement and exfiltration of data. Although not every campaign follows the kill chain perfectly, and some attacks can happen in parallel, these stages tend to be present in most attacks involving breaching security and extracting the necessary information. After plotting the graph of all transitions that our players-attackers have made (Figure 6.17 in the previous chapter) and the betweenness graph (Figure 6.18 in the previous chapter) we have found that specific techniques tend to enable other techniques, while some cards were not followed up by any other technique. Again, looking at the betweenness, we can see that the Technique cards with the highest betweenness are Trusted Relationship, Man in the Browser and Credentials from Web Browsers. There is little surprise in these techniques topping the chart, as a Trusted relationship can serve as a simple yet effective entryway into the target infrastructure. A man in the browser attack is most commonly used to access credentials, often required as part of the campaign. Hence this technique is another gateway that enables many other attacks. The same can be said about stealing credentials from web browsers. However, that implies the presence of a connection to the victim's web browser or a victim's device, which is also reflected in a slightly lower betweenness. We also have a technique involving web session cookies that is excellent at enabling subsequent lateral movement and is often used by bug bounty hunters to find security vulnerabilities in web applications.

Next, when we have analysed the reason for choosing a specific Technique card over the other, we have found out that the Technique card's individual characteristics

tend to play a far smaller role than we have initially anticipated. Table 6.5 has shown the effect of the card's individual properties on the Technique card pick rate, and none of the characteristics had any effect on the choice of an individual Technique card. Thus, we can conclude that a specific card was picked not because of its characteristics but because of the allocated role of the player, hence that player's goal.

Now, let us consider how do these results map to OWASP (2021) Top 10 list. OWASP Top 10 is a list of web vulnerabilities that are based on the contributed data breaches and a community survey of experts to provide an up-to-date web vulnerability list. The following table (7.1) correlates the OWASP Top 10 list and the frequency-based list of game techniques.

Technique card	**OWASP Top 10**
T09 – Spearphishing Link	Not a web technique
T10 – Trusted Relationship	Not exclusively a web technique
T13 – Man in the Browser	A02:2021-Cryptographic Failures A03:2021-Injection
T08 – Exploit Public–Facing Application	A05:2021-Security Misconfiguration A06:2021-Vulnerable and Outdated Components
T02 – Steal Web Session Cookie	A07:2021-Identification and Authentication Failures
T11 – Drive–by Compromise	A07:2021-Identification and Authentication Failures
T04 – Credentials from Web Browsers	Can be accomplished or enabled by A03:2021-Injection
T12 – Spearphishing via Service	Not in OWASP
T05 – Domain Fronting	A10:2021-Server-Side Request Forgery
T03 – Web Shell	More a tool than a vulnerability
T07 – Browser Extensions	A03:2021-Injection
T06 – Exfiltration Over Alternative Protocol	Not exclusively a web technique

Table 7.1: OWASP Top 10:2021 correlated with the frequency table for the Technique cards

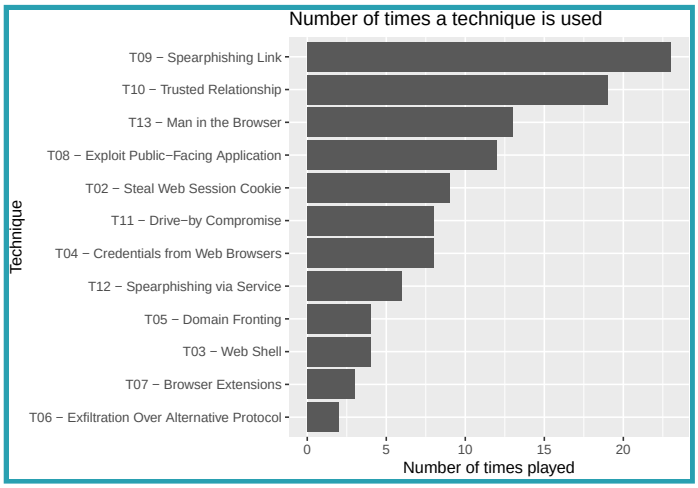
As can be seen, although not every OWASP Top 10 technique is present in the list of Technique cards, this can be justified by the fact that not every technique is a web-based technique, and considering this detail, the technique usage aligns well

with OWASP Top 10.

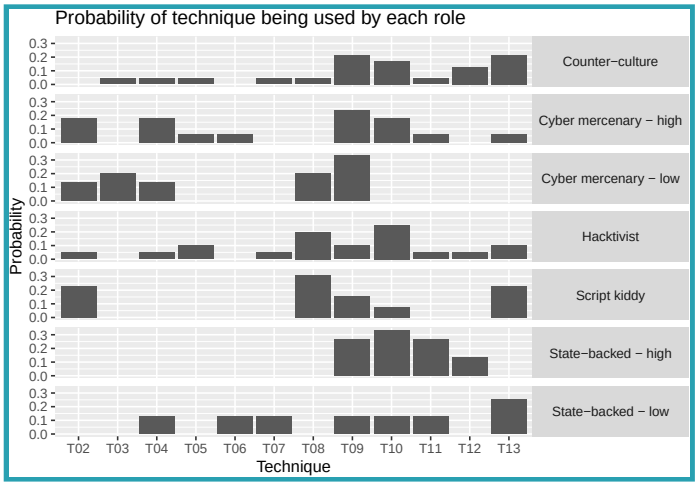
Lastly, Lallie et al. (2021) have done a timeline of the cybersecurity events during the initial outbreak of COVID-19. A global epidemic is an example of a global state change. During a state change, there is a global condition that affects a large number of devices. COVID-19 is an example of a socio-economic state change. Another example would be a sudden global patch of Windows systems, rendeding a certain attack vector unusable. The method presented in this thesis would allow for accounting global state changes in numerous ways. Firstly, by changing the working set of Technique cards. Techniques can be added or removed, allowing players to only see and use the techniques that are relevant. Secondly, by accounting for such change in a scenario, if, for example it is a socio-economic change. This would allow to put certain attacks in context. Furthermore, with the existing Technique cards it is possible to amend existing attributes, for example reducing the Impact factor of a certain technique. Overall, it would be reasonable to assume that the game would adequately respond to a global state change. In the case of COVID-19, an increased amount of social engineering and phishing attacks has been observed, which correlates to the results seen in this data analysis.

7.2 Individual differences

There is not enough data to make any conclusions about whether there are specific card preferences that each individual differences group favours. Nevertheless, from the data that we have, we can see (Figure 7.2) that since Spearphishing Link was the most used technique, it is highly likely that nearly all of the roles will use it at some point during their campaign. A Hacktivist role or a Counter-culture are more likely to employ different techniques. Typically, these types of attackers tend to be the least regulated in the real world, as counter-culture attackers are not motivated by financial or ideological means. They typically work alone; hence they can use a diverse set of tools. Hacktivists are likely to have less regulation than nation-state actors, so the toolset that they use would also be quite broad.



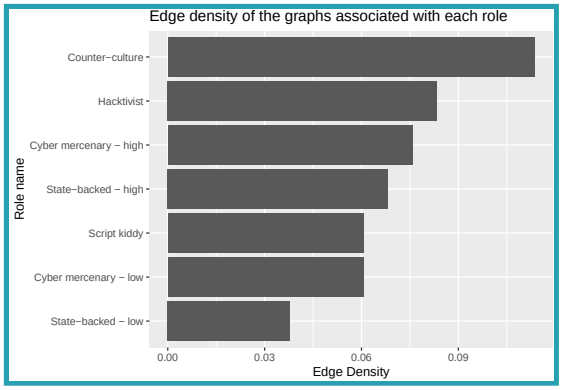
(a) Overall Technique card frequency



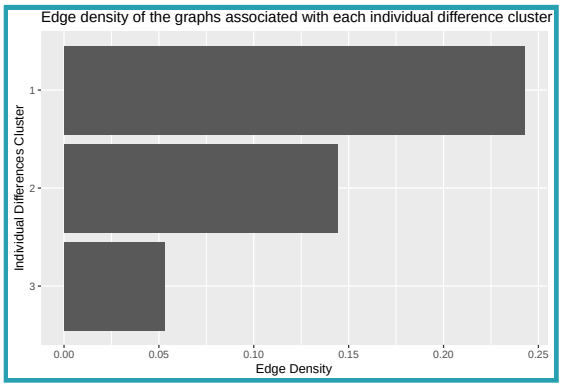
(b) Technique card distribution by role

Figure 7.2: Card usage versus probability of usage per each role

Next, consider the cards played in a sequence. Here, we can start to see some patterns. Figure 7.3 shows the edge densities of the graphs. On the one hand, we can see that certain roles (e.g. `R03`, Counter-culture) and certain individual differences clusters have a tendency to generate more complicated Technique card transition graphs. On the other hand, we can see that low capability state-backed attackers tend to have less variety in their techniques and less complexity in their attack graphs. When translated to the real world, it would probably mean that the low capability prevents them from using more costly techniques and preferring simple attacks constructed from well-understood techniques. To prevent detection, they would sometimes have to discard their current campaign.



(a) Edge density of the graphs associated with each role



(b) Edge density of the graphs associated with each individual difference cluster

Figure 7.3: Edge densities per role compared to edge densities per each individual difference cluster

Similarly, at the top of the edge density graphs, we have the roles that have a higher capability. After Counter-culture, we have hacktivists, cyber mercenaries with high capability and high capability nation-state actors. Hacktivists, cyber mercenaries and nation-states of high capability are not short on resources. They can afford to execute more costly techniques and execute complex and diverse kill chain patterns.

It would be reasonable to assume that participants with specific individual differences (for example, group one) would have a stronger preference to play roles that lead to more complex attack graphs. A similar pattern can be seen with team-based video games, where every player has a specific role. For example, a 'dps' – the main damage-dealer in the team, a 'tank' – a character that is difficult to kill, and acts as a living shield for other players, absorbing the damage from the enemy team, and a support – a character that is focused on keeping the rest of the team alive. Players usually have a strong preference towards a particular role, as the set of skills required for every role is different, and these roles have different purposes and priorities (Hodges & Buckley, 2018). Therefore, going forward, matching the types of individual differences to the role can give us more accurate role-playing from our players. In the real world, attackers can all be different people and have different backgrounds. They can be of different cultures and have different economic situations, both in the country (Watters et al., 2012) and in individual families. Thus

the individual differences clusters could reflect this in the real world.

During this study, players were not explicitly assigned a type. However, going forward, it would be valuable to study the effects of the following patterns when people are playing the game:

- Individual differences cluster 1 when assigned a low-risk role
- Individual differences cluster 1 when assigned a high-risk role
- Individual differences cluster 3 when assigned a low-risk role
- Individual differences cluster 3 when assigned a high-risk role

So far, there is not enough data to assess how the permutations above would differ, but it could provide an excellent avenue to investigate in the future.

More complex attack graphs, in turn, lead to more Technique card usage patterns forming. If we are playing `R03` (Counter-culture), after using a particular Technique card, `T13` (Man in the Browser), for example, we can either use the same technique again, use `T09` (Spearphishing Link), or `T11` (Drive-by Compromise). These transitions are not consistent across every role, if we play `R06` instead (State-backed, low capability) then our options would become to transition to `T06` (Exfiltration Over Alternative Protocol), or `T07` (Browser Extensions). These differences in complexities could be dependent on role-specific goals.

7.3 Enabling capability (simulation)

This project has enabled the generation of a complete simulation by using the attack data gathered from individuals playing the board game.

First of all, using a simulation opens up a possibility to compare different roles with each other. If we had one hacktivist and one script kiddy in a game, we would be able to make a simulation run consisting only of script kiddies, enabling us to compare them with each other.

Furthermore, having a more complex simulation would allow us to emulate the conditions in the real world. We could achieve this by, for example, restricting a

particular attack technique, as in the game, no attack technique restrictions were in place, and the attackers were able to use all techniques freely. In the real world, this might not always be the case. For example, if a technique is obsolete (it is for an older version of the software than the one installed on the target system), or the defensive measure of a company is robust. Hence it might not always be possible for an attacker to execute a specific attack technique.

Another possibility is to be able to emulate the attack graph with different possibilities. We have a set of player decisions that follow a specific path; at every point of the decision, a player has rolled a die. What if at every stage of the game, this die roll would have produced a different outcome, causing a Technique card to succeed instead of failing or instead of succeeding a technique would fail. Re-playing the same scenario with the player would be more time-consuming while examining the possibilities in a simulation would provide a better insight into matters that would otherwise be difficult to explore.

To translate the above to the real world, it is like having many attackers perform actions to attack a specific target simultaneously and in multiple timelines. Being able to receive the data from every timeline would help us better understand what the attackers are capable of and the best conditions for an attack to succeed.

Summary

This chapter has established that our players-attackers favoured Spearphishing Link and Trusted relationship Technique cards. Much like in the real world, both of these attacks tend to be less technical yet very practical and used a lot to this day.

By examining the betweenness of the cards and plotting the sequences on the graphs, we have found that some techniques serve as a gateway and enable other techniques. One such example is the Trusted Relationship card mentioned above, which translates into a supply chain attack in the real world, and serves as an entryway into the target organisation.

Our attackers have also played the game very differently, with lower capability actors having more fixed attack patterns. As a result of a lower capability, they

use the techniques that have been thoroughly tested and are known to work instead of experimenting with potentially more risky techniques. On the other end of the spectrum, there are malicious attackers with less regulation (lone-wolf or part of a more liberal entity, such as a hacktivist group). We have also found that individual differences also play a part in determining the choice of a technique, revealing that there could be a link between the specific role type and the individual differences of a person and their natural predisposition to play a particular role.

Finally, we have explored what possibilities would having a more complex simulation entail. More specifically, it is the opportunity to explore more outcomes consecutively and on a much larger scale than doing the same with human players.

Chapter 8

Conclusions and Contribution

This chapter will summarise the project and discuss the original contributions of this research project, examine future work and the implications this future work will bring to the research.

The research question that we have set out to answer is:

> *Can specifically tailored games (also known as 'serious games') be used for informing computer simulations?*

To answer this question, we have achieved the following objectives:

> *1. To build a realistic game based on rigorous evidence*

We have built a board game that emulates cyber operations, where players role-play as a variety of attackers, each with unique goals. Players have a choice of TTPs that allow them to advance their goals. Game resources were created from historical cases, an existing attack taxonomy and enrichment from security enthusiasts and professionals.

When the data from the games was analysed, many parallels with real cyber operations were observed.

- Simpler and more effective techniques were favoured over more complex attacks
- Attacks that are commonly used in cyber operations have also prevailed in the games

- Roles with less capability had simpler attack chains
- Techniques put in context have provided more insight into the nature of attacks, as opposed to being examined in isolation

2. To ensure that the game enables players to make decisions that reflect their true intention

By using a board game format with the GM players have the opportunity to interact with the game world and to freely choose the tools that would enable them to accomplish their desired outcome.

Although there is some limitation to what decisions players can make (there are currently 13 Technique cards), players were able to assess the situation by first receiving the instructions from the GM, then by having an opportunity to ask GM any questions. The research identified that the cards played were not significantly affected by the characteristics of the card, e.g. impact, recon, risk. However, they were impacted by the player role. This implies techniques were used in accordance with the role assigned, as opposed to them being dependent on the individual characteristics of the card.

The attack graphs demonstrated that different roles resulted in varying complexity attacks, e.g. the Counter-culture role has demonstrated high complexity, while the State-backed has less variation in the attacks. This observation further indicates that the roles have variation in how they are played, otherwise attack graphs would have been very similar.

A similar pattern has been observed with the individual differences. Participants were clustered into three distinct groups based on the scores of the following three measures: risk perception, self-monitoring and impulsiveness. Each of these distinct clusters resulted in varying complexity graphs. This indicates a potential opportunity to map the players to the roles that better align with their individual differences.

3. To devise an efficient approach to the recording of the game decisions

4. To ensure the events within a game can be restored from the recording, with semantics preserved

The game is a rich social experience, requiring a pragmatic approach to capturing the decisions taken throughout the course of the game. To achieve this, a shorthand notation akin to the algebraic notation used in chess was engineered. This enabled efficient capture of the attacks played out in the game. This notation has lead to efficient post-processing allowing the game to be restored from the shorthand notation. This allowed the capture of the elements such as the Technique used, the role of the player, the outcome of the Technique, what role-specific goals have been completed, consequences and any GM actions.

5. To ingest the game decisions into a simulation

The final research objective enabled the ingestion of this shorthand directly to create software agents in a simulation. This simulation allowed replaying of recorded games and the creation of new combinations of recorded attacks. Future avenues for simulation development will be expanded in Section 8.2.

All of the research objectives have been accomplished. It was identified that games can provide an environment, where players can role-play as cyber attackers and perform attacks that show similarities with those seen in the real world (as shown in the Chapter 6). This game data is a source of rich behaviours to enable the simulation of cyber attacks in order to gain a better understanding of the effect of defensive interventions.

8.1 Contributions

This section will explore the contributions this research project has made. The original contributions of this project are split into two parts. The first part is using games to capture decisions. The second part is the interaction between the individual differences of a player and how they role-play.

The first original contribution is generating an evidence-based game built from accounts of real-world historic cyberattack cases, an attack framework and input

from practitioners and enthusiasts. Furthermore, we have identified that players in the game have exhibited similar attack patterns we would observe in the real world. An example is the use of spearphishing over more complex techniques, we also see that the complexity of an attack is related to a role's capability and risk appetite. The role of the player has had a significant impact on the way the game is played. Different people have diverse approaches to the same role. As part of the research, a mechanism to use the output from the game as an input to the simulation has been provided, allowing us to put the game output into context and to use the game output as part of more advanced processing.

The second original contribution is deriving the links between card usage and individual differences. Throughout this project, it has been discovered that how often the technique is used is not the only determining factor on the pick rate of a technique. A far more significant factor is enabling other techniques, which has a close link to the attacker role the player is impersonating, and to the specific individual differences the player has. Individual differences in this project involve three factors: self-monitoring, risk perception, and impulsiveness. We have identified three key groups by collecting the eight most consistent dimensions across the three of these measures.

The individual differences group 1 has higher complexity in their attack graphs, meaning a more diverse toolset and more complex attacks. The individual differences group 3 has the least complexity in their attack graphs, indicating a more limited toolset and attacks that are more predictable. A similar pattern has been observed with the roles the attacker had. Lower capability roles also had more predictable attacks, whilst higher capability roles had greater complexity in their attacks. Thus, the role of the attacker (specifically, whether they have the capability to execute desired attacks) has a significant impact on the complexity of the attacks in sequence. To summarise, the novel contribution is in the roles and individual differences having a noticeable impact on the attack complexities. The link between roles and individual differences would imply that players would benefit from being assigned a role that best fits their individual differences. In the real world, a similar method of matching based on individual differences could be used to select individu-

als for cybersecurity jobs - whether it is cyber intelligence, penetration testing or red teaming.

8.1.1 Applications of contributions

There are three key applications that these contributions can be considered for. The first application is using the game outcomes as an alternative method for analysing what areas are the most susceptible to risk in an organisation, as a visual representation of a risk-based approach.

The second application that could be considered for this is to use this as an alternative method of evaluating the defensive posture of a company. With the help of the attack graphs and having the employees role-play as attackers will help to have an initial impression of the areas that require to be improved, even before a company decides to hire penetration testers, and potentially eliminate some of the more obvious vulnerabilities.

Finally, the idea that different individuals have a certain pre-disposition to role-play as a specific type of attacker has previously been mentioned in this thesis. It has been demonstrated that there is a correlation based on the individual differences and the gameplay patterns by deriving three distinct groups of individual differences. What if a similar mechanism is employed when searching for particular qualities and skills when recruiting individuals for cybersecurity jobs? Based on a number of individual differences and performance in the cyberattack simulation game it would be possible to make recommendations to individuals about what cybersecurity roles would suit them best, or use this method to reallocate individuals within the company.

8.2 Future work

This section is split into two different parts - future work that could be added to the game and future work that could be done to the simulation.

8.2.1 Game: Add more scenarios

The first aspect that could be improved about the game is adding more scenarios to the game. Possible expansion scenarios or locations include a port, power grid system, SCADA systems, IoT networks.

Adding these scenarios to the game will help test the Technique cards' transferability and see whether the Technique usage patterns will change depending on the scenario. It may be the case that some techniques that have not been used as much before will play a more critical role in the alternative scenarios. Alternatively, it could be that the use of techniques is tied only to the specific goals each role has, which may be very similar across some of these scenarios (e.g. deface front page of the website can apply to more than one of these scenarios).

It would also be interesting to see how the Technique card usage sequences will change depending on the scenario. It could be that roles that previously had more complex technique usage graphs will now have less complex usage graphs, just because the set of goals has changed for that particular role. Alternatively, roles that right now have simpler attack graphs might have a more complex card usage chain with the introduction of a different scenario.

8.2.2 Game: Exploring defensive capabilities and MITRE D3FEND

The second point to complement the scenario argument is that a constant set of Countertechnique cards has been used for all games in this research project. By using a constant set of Countertechnique cards, we assume that the same company has a constant defensive posture. Changing that posture may potentially affect Technique card usage patterns by the attackers (as there will be a different set of Technique cards that will be countered)

We could augment the above by introducing the Mitre D3FEND taxonomy (MITRE, 2021b) into the game. This taxonomy has been launched after the project was complete, hence it was not part of the Countertechnique card deck. Using these

cards would allow to model a more extensive defence capability and allow a company to pick a set of techniques from a broader range of them to see how it affects the attack patterns of a player. The impact from this change would not be as significant as restricting specific attack techniques, but it could allow for tailoring the defensive posture to more companies that could use this game as a training tool.

There is a game mechanics implication associated with including more defensive capabilities. With the limited toolkit, the attackers would not be able to do many actions against such sophisticated defences. Suppose for every Technique card there is a Countertechnique card, and there is enough of them to counter all of the Technique cards without repetition. In that case, we may no longer observe attackers achieve their goals and any lateral movement. Instead, we could modify the game mechanics to include the defences or mitigations failing for a specific reason. For example, the system administrator forgets to launch an update script to patch security vulnerabilities, enabling the attackers to execute a particular privilege escalation technique. An alternative could be a tired employee misreading a phishing email address and mistaking it for the actual email, allowing another attack technique to succeed. This mechanic enables the modelling of a system that should be secure in theory but allows some freedom and speculation and modelling various what-if scenarios. Currently, the game mechanics are in favour of the attackers. The suggestion above is an approach to modify the mechanics to be a little more even.

8.2.3 Game: Collaboration

The next point is inspired by the player's feedback, it is to integrate more advanced elements of collaboration. As mentioned before, a single player can represent an entity (such as a hacktivist group), yet currently, there is no option in the game mechanics to collaborate with other roles. Additionally, two players cannot be given one role to play together.

Integrating the elements of collaboration might cause a new set of patterns to emerge. Players can reach a consensus on what Technique card to play, or there is a potential for them to be affected by 'group think'. Attack patterns may also

differ depending on the set of shared beliefs and values shared by individuals. Hence we can hypothesise that players with a particular set of individual differences may synergise better than other players. There is an entirely different avenue in exploring the combinations of individual differences that will enable the best collaboration of players when engaging in a team cyber attack.

8.2.4 Game: Insider threat

Attacks originating from insider actors are very prevalent, and at present the threat from internal actors is not represented in the game.

Following on from the previous point about collaboration, what will happen if we add insider threats into the game? How will the external attackers collaborate with insiders, and what will be the effect on the attack graph? This way, attackers will have an extra reconnaissance channel in the face of the insider that will provide the information that the GM will not be able to provide.

Integrating insiders can give us a better insight into their decision-making processes and the effect the presence of a known insider has on the decisions and the choice of the techniques by the external malicious attackers.

8.2.5 Simulation: Restricting techniques

Another future work suggestion is to implement the possibility of varying the techniques that will be in use by the simulation. The upper bound of techniques will be restricted by the amount of Technique cards available (a total of 13), but out of these 13 techniques, it is possible to take certain ones out to see how this will affect the agents' decisions. In the real world, this completely removes an attack vector, modifying the attack landscape. This procedure will also identify the existence of any techniques that can replace the removed techniques.

The Technique cards that could be excluded without significantly affecting the gameplay are the cards with high usage and a low betweenness. Perhaps, a change in the betweenness in existing Techniques can be expected if we remove the Technique

cards with higher betweenness. One such example is `T09`, which had low betweenness, as most of its links could be replicated by `T10` instead. Thus, if we remove `T10`, maybe the betweenness of `T09` will increase, as this will become the only possible way to connect specific Techniques in the graph together.

The main difficulty for the players will arise when there is a very limited set of Technique cards that they can use (or a limited set of attack techniques that the attackers can use). However, at this point of the game, the balance of the attackers and defenders will suffer greatly, thus is undesirable. Nevertheless, it would be useful to try and remove every single technique from the set, running the simulation, and see how the outcome is affected. The techniques should then be returned to the set so that the experiment can be repeated with other cards too. This procedure would allow us to see precisely how significant each technique is. The next step would be to remove all of the least significant techniques and see if the goals can still be achieved with that minimal set of highly significant techniques.

8.2.6 Simulation: Variable risk appetite

Currently, the simulation only has the initial risk appetite that is hard-coded and is only affected by using techniques. This suggestion proposes to give the observer (the person running the simulation) the option to vary the risk appetite of every individual role and observe any changes. The aim of this change is to be able to capture a point where, for example, a low-capability actor transforms into a high-capability actor, what is the threshold for a low-risk appetite, and what is the threshold for a high-risk appetite.

To take this idea even further is to introduce yet another dimension of risk appetite, with this dimension representing the individual behind the role (the player or the attacker as a person), and to see how adjusting the individual risk appetite would affect the outcome of the simulation. With this change, we are trying to find out the point where a person stops being comfortable playing the dedicated role, and to investigate the effect the role has when correlated with the person's individual differences.

8.2.7 Simulation: Agents learning from the player actions

During this project, agents are only capable of re-playing past player actions. The next step is to enable the agents to use the techniques on their own. This could perhaps be achieved using a random algorithm that chooses from a pool of available techniques (this pool can be modified by external factors, as explained above, e.g. by restricting techniques or increasing/reducing the risk appetite). The next step would be to add a die-rolling mechanic that would represent luck, just like in the game. The final step would be to let the agent access the gameplay files of the players. This access would enable the agent to see the outcome of this technique succeeding, and whether executing this technique would bring it closer to the goal required by the role that this agent is representing.

Implementing this functionality would allow running many simulations, exceeding the number of games that can be hosted with human participants, and exploring more variations and outcomes, all while changing the different parameters.

8.2.8 Simulation: Agent collaboration

At the beginning of the project, we have set a restriction that every player in the game would represent an entity. However, there will be no collaboration intended within a role (two or more people representing a specific role) or between roles (a hacktivist and a cyber mercenary forming a marriage of convenience). By implementing this change, we will be able to gain more information on the following aspects:

1. Whether collaborating together when playing a specific role would affect the ultimate decisions this entity takes in the game

2. Whether collaborating between roles would have any outcome on the decisions in the game. Currently, the expectation is that the two entities would share information, allowing them to conserve risk points, effectively translating to the shared responsibility and some degree of relying on each other when it comes to malicious cyber operations. For example, if one party gets discovered,

the other party is now also at risk.

Summary

This project has set out to answer the following research question:

> *Can specifically tailored games (also known as 'serious games') be used for informing computer simulations?*

As demonstrated in the earlier chapters, this question can be answered affirmatively. At every stage of the project, the process has felt refined, starting with building the game, gathering players and gameplay data, and finally translating the transcribed game data into the simulations. During the game stage, players have willingly participated in the game and found it fun and enjoyable; the notation to capture the games has been easy to use by both players and the GM, essentially allowing games to be transcribed as they are played and requiring minimal time spent post-processing, and the output was suitable for the use in simulations and machine-processing ready.

Throughout the course of the project, interesting observations have been made about the decision-making processes of the players, allowing us to draw strong parallels with the real world. Players favoured simpler but effective attack techniques, and their individual differences have played a part in how sophisticated their attack was. The roles players had have also influenced the attack graphs, with greater capability resulting in greater complexity.

Appendix A

Published poster for International conference on Behavioural and Social Sciences in Security, 2018 (BASS18): Agent-Based Modeling of Offensive Actors in Cyberspace

Agent-Based Modeling of Offensive Actors in Cyberspace

START

Simulating hackers?

The project aims to create a simulation of a network with cyber attacks occurring over a period of time with hackers trying to pursue their goals within the system.

Each hacker will be based on natural world prototypes. Although it is impossible to model humans with 100% accuracy the model will be made using the best knowledge available.

In order to gather such data an online game will be created to capture certain characteristics of each participant.

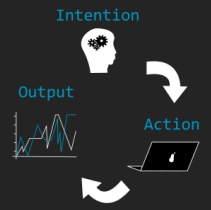
Base of a model

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command & Control
- Actions on objectives

One way of understanding a cyber attack is breaking it into steps, one example of this is the Cyber Kill Chain, shown on the left.

This can be used for the simulation, since it allows observing what stage of an attack a hacker is in.

Representing actions



We are interested in gathering the set of actions an individual would take in a particular scenario.

Why Agent-Based Modeling?

ABM can help visualising how agents (hackers) interact with the environment (network), whilst representing their actions.

Measuring effort

The trace left by a hacker on the network may help with determining their level of committment. The more comitted an individual is, the larger the trace left by them on the network will be.

We think the motivation affects the actions of hackers.

Sample agents

Different hackers may have different goals in mind. Below are some example types of hackers along with their goals and styles of attack. Hackers can belong to more than one type and the list is not conclusive.

Black hat

Goals:
- Steal information for profit

Characteristics of attack:
- Malware through spam
- Social engineering
- Target sensitive information

"Counter culture"

Goals:
- Unpredictable, their motives remain a mystery.

Characteristics of attack:
- Persistent when breaking into the network
- Lose interest when achieve their target

Hacktivist

Goals:
- Get the attention of their target/target's audience

Characteristics of attack:
- Aim for the website
- Sometimes will publish stolen data to convey the message.

Researcher

Goals:
- Bug bounties
- Testing out their skills
- Do not intend to do any harm

Characteristics of attack:
- Scanning the network
- Their fingerprint in the system will be small

FINISH

Gathering data

A large part of the simulation will depend on meeting individuals willing to contribute their knowledge and their way of reasoning so that it can be used in the research. Examples of people being asked to participate include ethical hackers and cybersecurity enthusiasts.

This will be the process of capturing the Tools, Techniques and Procedures (TTPs). In order to collect them a range of creative individuals will be asked to play a game, which will aim to be both entertaining and will assist in capturing the TTPs of said individuals.

Tatjana Sidorenko, Cranfield University (tatjana.sidorenko@cranfield.ac.uk); Dr. Duncan Hodges, Cranfield University (d.hodges@cranfield.ac.uk); Dr. Oliver Buckley, University of East Anglia (o.buckley@uea.ac.uk)

Centre for Electronic Warfare, Information & Cyber, Cranfield University, Defence Academy - College of Management and Technology, Shrivenham, Wilts, SN6 8LA

www.cranfield.ac.uk

Appendix B

Published poster for Defence and Security Doctoral Symposium (DSDS19): Automated Question Generation for Delphi Studies

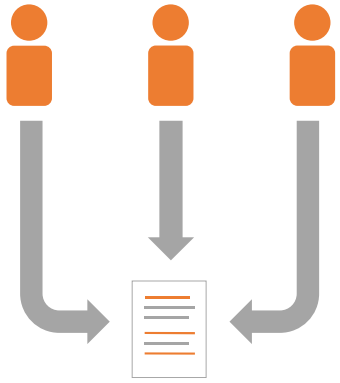
Automated Question Generation for Delphi Studies

Tatjana Sidorenko

CASE STUDY

We are developing a cyber security game that will be used to explore how hackers or hacking groups attack systems. In order to understand different tools, techniques and procedures (TTPs) a list of potential attack possibilities needs to be created. To generate this list and to gather different opinions about the characteristics of the TTPs we chose to undertake a Delphi study. However, there is a lack of flexible, free and computerized solutions available, which meant that a need for new tool-support has arisen.

WHAT & WHY



Problem The Delphi approach works by sourcing and refining expert opinion of the characteristics of various techniques, until a consensus is reached. In our application, the list of items that was considered was very large (314 items), which is beyond the scope of current solutions.

Solution Qualtrics Delphi Toolkit (QDT) was designed to automate the generation of questions used in the study. It also allowed the use of random subsets of questions to ensure even distribution of questions across experts.

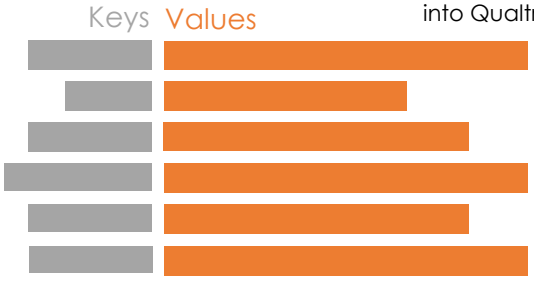
Qualtrics is a well-established and flexible platform for making surveys, however it lacks the capabilities for carrying out a Delphi study – there is currently no functionality to automatically generate questions or randomly select a subset of questions from a larger pool. Therefore an augmentation to the existing platform has been developed.

HOW

Qualtrics supports importing and exporting the surveys. It is these exported files that are processed in QDT.

QDT generates output files in the Qualtrics format, these can then be imported back into Qualtrics to create the final survey.

ID: QID%ID%



The principle behind the application is as follows:

1. A Qualtrics survey with question templates is exported. This template will later become complete questions. Additional settings, such as the order questions come in are also saved at this step.
2. The template file is loaded into the QDT application.
3. A separate list of question topics is also entered.
4. A set of automatically generated questions is then added to the template survey file.
5. A output file is generated and imported back into Qualtrics.

QDT is…

- Designed to help researchers to create automated Delphi studies
- Currently more functionally advanced than the existing solutions
- An intuitive template format that allows greater flexibility

WHERE

The code will be available on **Github** at http://github.com/tasidonya

Tatjana Sidorenko, Cranfield University (tatjana.sidorenko@cranfield.ac.uk);
Dr. Duncan Hodges, Cranfield University (d.hodges@cranfield.ac.uk);
Dr. Oliver Buckley, University of East Anglia (o.buckley@uea.ac.uk)

Centre for Electronic Warfare, Information & Cyber, Cranfield University,
Defence Academy - College of Management and Technology, Shrivenham,
Wilts, SN6 8LA

www.cranfield.ac.uk

Appendix C

Published paper for Defence and Security Doctoral Symposium (DSDS20): Board games as a behavioural collection method

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

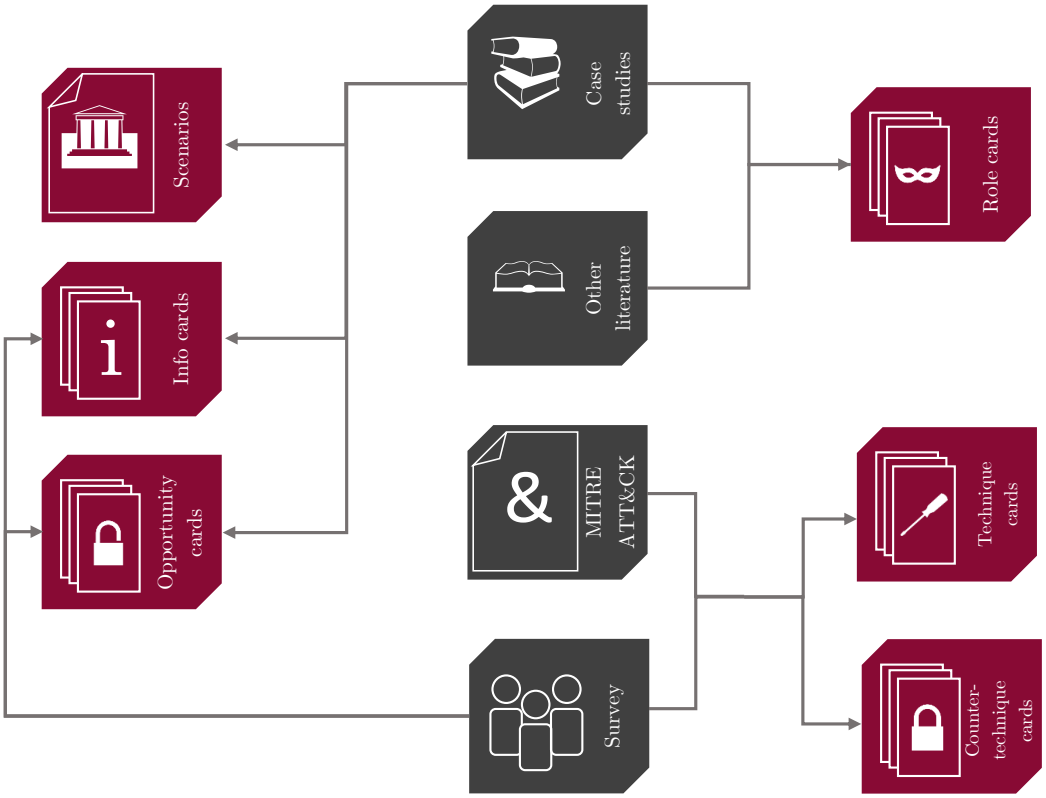


Fig. 1. *Information sources*. **Scenarios** come from the news stories and use-cases. **Role cards** come from attacker taxonomies outlined in Section II and motivations for these roles come from case studies. **Info** and **Opportunity** cards will also depend on the scenario, although some have been 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.

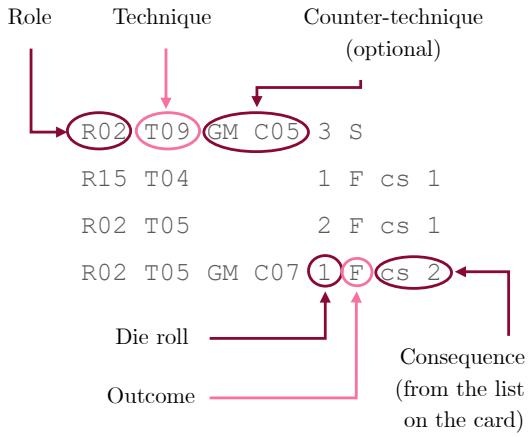


Fig. 2. *An example transcription of a move set using custom notation.*

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

Appendix D

Techniques Survey Participant Information Sheet and Consent Form

A survey on the use of computer attack techniques

Tatjana Sidorenko (tatjana.sidorenko@cranfield.ac.uk)
Duncan Hodges (d.hodges@cranfield.ac.uk)
Oliver Buckley (o.buckley@uea.ac.uk)

In this study you will be presented with a list of cyber attack techniques, for each technique you will be asked to answer a series of questions. Please answer to the best of your knowledge. In the survey you will have the opportunity to share your knowledge about a particular technique.

The data that you provide will be used to populate a deck of cards in a hacking-themed board game, if you are interested in piloting this game please do not hesitate to contact us.

You have the right to withdraw from this study immediately if you wish and not participate in the research. Alternatively, if you wish to withdraw at a later date please inform the researchers named above. If you do not receive a satisfactory response please contact the Cranfield University Ethics Committee (CUREC) curec@cranfield.ac.uk.

Informed consent form

Title of the project:	Agent-Based Modelling for Offensive Actors in Cyberspace
Name of the researcher:	Tatjana Sidorenko
Researcher's contact details:	*Tatjana.sidorenko@cranfield.ac.uk* d.hodges@cranfield.ac.uk
Cranfield University Ethics Committee (CUREC)	*curec@cranfield.ac.uk.*
Participant number:	
Date:	

Participation consent

1. I confirm that I have been informed about this research project and I agree to take part.
2. I understand that all personal information I provide will be treated with confidence and my name will not be used in any report, publication or presentation.
3. I have been provided with a participant number as shown above. The researcher(s) will record data against my participant number instead of recording my name. The file linking my name to my participant number will be accessible only to the main researchers.
4. I understand that I can withdraw from this project at any stage by informing a member of the research team, for whom contact details have been provided. I understand that if I have any questions about the research and I cannot contact the researchers listed I can contact the Cranfield University Ethics Committee, for which the details have been provided above. I also understand that I can withdraw my data any time after the study.

Data integrity

I understand that the data I provide will only be accessed by the named researchers for the purpose of research only.

Data storage

- Responses to the survey will be securely stored on encrypted hard drives. These text files will be securely deleted as soon as they are no longer required.

Anonymised records will be created, by removing or replacing identifiers such as name, age and location. These anonymised records may be quoted from, in support of findings (e.g. in journal articles, conference papers).

- Analytical software will be used to aggregate the results of the research and every reasonable step will be taken to anonymise the data.

I understand that the aggregated data will be published in support of the research findings. ☐

I confirm that I have read and understand the information provided on this form and give my consent to taking part in this research.

Participant's signature:		**Date:**	
Participant's name:			
Researcher's signature:		**Date:**	

One copy of this form must be given to the participant and one copy held by the researcher.

Appendix E

Game Participant Information Sheet and Consent Form

Cyberattack simulation game participant information sheet

Tatjana Sidorenko (tatjana.sidorenko@cranfield.ac.uk)
Duncan Hodges (d.hodges@cranfield.ac.uk)
Oliver Buckley (o.buckley@uea.ac.uk)

In this study you will be participating in a game that simulates a cyberattack, where you will be playing the role of an attacker. You will have a chance to pick a specific attacking role and to win the game you will need to complete the role-specific objectives.

This game requires a certain degree of technical knowledge. You will be briefed on the scenario and game rules before the session, you will also receive a copy of the "Attacker's manual" that will contain the bitesize reminders about the gameplay.

One session will consist of the game itself, which will last ___ minutes followed by a feedback session after the game finishes. You can take part in multiple sessions; however, you will need to pick a different attacking role for the next game.

The video of the gameplay will be recorded to capture your decision-making process. This decision-making process will be used to power a software agent in a computer-based model of the same game. You have the option to participate without a video but your voice still has to be recorded.

Video and audio recordings will be stored on an encrypted hard drive and will not be shared with anyone but the researchers listed above.

You have the right to withdraw from this study immediately if you wish and not participate in the research. Alternatively, if you wish to withdraw at a later date please inform the researchers named above. If you do not receive a satisfactory response please contact the Cranfield University Ethics Committee (CUREC) curec@cranfield.ac.uk.

Informed consent form

Title of the project:	Agent-Based Modelling for Offensive Actors in Cyberspace
Name of the researcher:	Tatjana Sidorenko, Dr Duncan Hodges
Researcher's contact details:	*Tatjana.sidorenko@cranfield.ac.uk* *d.hodges@cranfield.ac.uk*
Cranfield University Ethics Committee (CUREC)	*curec@cranfield.ac.uk.*
Participant number:	
Date:	

Participation consent

1. I confirm that I have been informed about this research project and I agree to take part.
2. I understand that all personal information I provide will be treated with confidence and my name will not be used in any report, publication or presentation.
3. I have been provided with a participant number as shown above. The researcher(s) will record analysed data against my participant number instead of recording my name. The file linking my name to my participant number and the recording of the game will be accessible only to the main researchers.
4. I understand that I can withdraw from this project at any stage by informing a member of the research team, for whom contact details have been provided. I understand that if I have any questions about the research and I cannot contact the researchers listed I can contact the Cranfield University Ethics Committee, for which the details have been provided above. I also understand that I can withdraw my data any time after the study.

Data integrity

I understand that the data I provide will only be accessed by the named researchers for the purpose of research only.

Data storage

- Video and audio recordings of gameplay will be stored on encrypted hard drives. These media files will be securely deleted as soon as they are no longer required.

- As part of the research anonymised analysis records will be created by removing or replacing identifiers such as name, age and location. These anonymised records may be quoted from in support of findings (e.g., in journal articles, conference papers).

I have read and understand the consent form and participant information sheet and agree to take part in the study.

Signed

Date

Appendix F

Game Assets

F.1 Game Rules

GAME RULES

Including the GM manual

Sidorenko, Tatjana

Contents

Player

On your turn

- **Listen to the Game Master (GM)** to get an understanding of your environment and the current situation.
- If able to, **pick a technique** from the techniques deck.
- Feel free to **ask the GM any questions about the target**, and the GM will disclose as much as they see appropriate.
- If the GM hands you the **Opportunity card**, take it and read out what it says to everyone.

Risk appetite

Each player gets a role at the beginning of the game. Each role has a number associated with it, representing how much risk this particular role is willing to take. Every technique has a cost associated with it; if a technique fails to execute, this cost is subtracted from the overall risk. If you run out of risk points throughout the game - you have lost it without completing the specified objectives. To prevent this from happening, choose your techniques wisely and only commit to them if you have thought it through.

Techniques

Techniques are your primary weapon in this game. Use them to discover essential information and utilise what you have already discovered to complete the game.

Each technique has a Risk number associated with it. Depending on what kind of role you get, you might not have enough risk appetite to execute a particular technique. On your turn, a technique can either succeed or fail. Here is what is going to happen to your overall risk number in all the cases:

- Technique succeeds: Restore one risk point (cannot exceed your role's maximum)
- Multiple techniques succeed more than once without failures in between (chaining success bonus): Restore 2 points (cannot exceed your role's maximum)
- Technique fails: Lose the number of points indicated by the "Risk" number on the technique card. Any chaining success bonuses get reset.

Interacting with other players

Do not collaborate with other players unless told by the GM. However, another player's actions may open up more possibilities for you. In this case, you can seize the opportunity and use the newly-discovered vulnerability to your advantage.

GM

As a GM, guide the players. Do not solve the puzzles for them, but if they appear to be stuck or have any problems, you are allowed to give them a gentle nudge in the right direction. There is a whole deck provided for your convenience called 'Opportunity' (more on that in "Decks") to disclose individual bits of information critical to the plot, ranging from lightweight to obvious.

Decks

There are several decks in the game.

- **Role** - These are the roles that are concerned with this specific scenario. At the beginning of the game hand out the role cards, making note of who plays what role. The same player cannot get the same card in subsequent games, i.e., one player can only play the same role once.
- **Technique** - These are the main cards designed to be used by the players. They represent the Tools, Techniques and Procedures (TTPs) that players use throughout the game.
- **Countertechnique** - These represent mitigations to these Tools, Techniques and Procedures. They can cancel out a successful technique. That means that the player who would have otherwise had a successful roll will have a consequence, equivalent to technique not executing. It does not contribute to the otherwise incrementing consequence count (if the player tries rerunning the same technique for some reason, and the said technique will fail - they will get the first consequence from the list, not the second).
- **Opportunity** - A deck that provides an alternative way to get Information cards for players that are either struggling or have gone the wrong way in trying to break into the system.
- **Information** - Resources that players have to capture in the game. Depending on their winning conditions capturing a specific resource can get a player to complete the game.

Timeline

Before the game

- At the beginning of the game, hand out the role cards, note who plays what role. The same player cannot get the same role in subsequent games.

Start of the game

- In the beginning, explain the scenario given to you in the scenario booklet. Do not disclose network architecture. Explain the geographical and geopolitical contexts, as well as some basic information about the company.
- Give players some time to familiarise themselves with the Technique cards, as well as their role card. Explain the principle of Risk Appetite and that players' resources are limited by the number of risk points decided by their role. Also, talk them through how they lose and gain those risk points throughout the game.
- Explain that the players need to write down the card deck number to commit to a technique.
- Decide on the turn order. Follow the same order throughout the game.
- Once the turn order has been decided, begin by reading out a complete scenario for each player's role, one-by-one. They will have a summary on their cards, and you will have a full version. Make sure they understand who they are role-playing as.

Turns

- Give the first player at the start of the game about 30 seconds to ponder their first move. For the subsequent players and turns, the waiting time will be less, as everyone would get more familiar with the game and will have time to think on their next move while watching others. Next, ask the player what would they like to do. They might pick out a technique or ask you a question (see "Questions asked by the players" section on how to handle them).
- Once the player feels ready, they will choose an attack technique and roll a die. If they appear to be hesitating with their choice, ask them if they need assistance.
- Depending on the outcome, you have one of the three possible options. Details of those outcomes are listed below.
    1. Their **die roll succeeds, and you use a Countertechnique**. If you have a matching Countertechnique card in your deck - respond now.
    2. Their **die roll succeeds, and you do not have a matching Countertechnique**. Provide the player with some Information cards that you think are the most appropriate for the scenario. Then, just move on to the next player. Also, note that if they have succeeded with a technique on their previous turn, they are entitled to 1 risk appetite point refunded back to them as long as it does not exceed their initial risk appetite value.
    3. Their **die roll fails**. In this case, you can propose to re-try the same technique, but with risk points deducted for the technique that has just failed. You cannot respond with a Countertechnique to a Technique that has failed. The re-trying can happen once on this turn, or the player

has to wait until the next turn. You also increment the consequence counter that preserves with every use of that technique. That means that if last time they used the same technique and it failed the consequence applied was number 1, while now the consequence applied will be number 2. Next time the same technique fails it will be consequence number 3.

Players discovering information

- Throughout the game, players will find specific information that will help them with subsequent game progression. This information can include system details, credentials or assets. These artefacts are linked to each player's winning conditions; thus, they will need this information to complete the game.
- Upon discovering such information, check if there is a corresponding Information card that can be given out to the player.
- If there is no corresponding Information card, make a note of this specific piece of information. Such tracking will help to improve future revisions of the game.

Completing the game

- Once a player gathers enough Information cards to complete one or more of their winning conditions, they have finished the game.

Transcribing the game

- Every card has a number to indicate where it came from and a number to distinguish it from others in that deck unambiguously. This number takes the format of L DD - Letter, Digit, Digit.
- The first letter corresponds to the card deck:
    - R = Role
    - T = Technique
    - C = Counter-technique
    - I = Info
    - O = Opportunity
- The space between the first letter and digits is not mandatory; it exists so that the first letter is not confused for a number, such as in "O 01"; therefore, when transcribing, the space can be omitted.

Examples

SCENARIO 1

> A hacktivist decides to use the "Man in the Browser" technique, rolling a die and getting a 4 (success). GM chooses not to respond with a counter-technique. As a result of this action, a player discovers a page and a pair of credentials to access a public-facing website's admin web console.

To transcribe this, we need to look in the top left corner of the cards that got played. First, let us look up the deck number of a hacktivist role card (R 04), the "Man in the Browser" technique card (T 13), then write down whether it was a Success (S) or Failure (F). We then find and Information card corresponding to "Admin console access" (I 02).

The transcription becomes:

```
R04 T13 S I02
```

SCENARIO 2

> A hacktivist decides to use the "Man in the Browser" technique, rolling a die and getting a 4 (success) with a GM responding with "User Training" Counter-technique.

To transcribe this, we need to look in the top left corner of the cards that got played. First, let us look up the deck number of a hacktivist role card (R 04), the "Man in the Browser" technique card (T 13), then write down whether it was a Success (S) or Failure (F). We then need to capture that the GM chose to respond by writing "GM". We then look up the "User Training" card (C 19).

The final line becomes:

```
R04 T13 S GM C19
```

SCENARIO 3

> A hacktivist decides to use the "Man in the Browser" technique, rolling a die and getting a 1 (failure), causing a consequence to be applied. They decide to re-roll for the same technique and fail, causing the second level of consequences to be used.

To transcribe this, we need to look in the top left corner of the cards that got played. First, let us look up the deck number of a hacktivist role card (R 04), the "Man in the Browser" technique card (T 13), then write down whether it was a Success (S) or Failure (F). In our case, it was a Failure. Following the rules, if the Counter-technique fails, we need to apply a consequence every time a technique fails and depending on

the consequence, the player can lose the game. The corresponding numbers on the consequence are as follows:

- 1 - Light consequence
- 2 - Medium consequence
- 3 - Heavy consequence

The transcription of the following actions will look like this:

```
R04 T13 F cs1

R04 T13 F cs2
```

Questions asked by the players

- Throughout the game, players may ask questions to clarify certain aspects. Here are examples of a question that you can and cannot answer.
    - Can answer: "How far I am from the organisation right now? Do I have physical access to the building?", "Do they have a contact phone number that I can attempt to call?" Questions like these are clarification-type questions and help players understand the game's limits and their capabilities within it. As long as these questions concern the information that is openly accessible - almost every organisation has a public phone number that one can call or information that is not accounted for in the game but is not restricted, such as player's current location you are free to answer it.
    - Cannot answer: "What is the password to this machine?", "What is the email address format?", "Can I get her laptop?", or if they are trying to find creative loopholes - "What if I live next door from the company and can see the desks through my binoculars, can I have read off the password from there?" Questions like these are testing the boundaries of what information can they get. You cannot answer these questions directly. Answer with a vague hint, for example "you might find the password elsewhere if you keep looking" or "there are no roles in this scenario that live near the site location". If the players get genuinely stuck or frustrated, hand them a corresponding Opportunity card and the accompanying Information card and ask them to read it.

  No matter what the question is, do make a brief note of it, as it helps to understand the players' mindset. If there are some genuinely creative loopholes that the scenario does not account for - it is useful information to us, the game creators.

On every turn

- You interact with players one by one.
- A player chooses an attack technique and rolls a die. If they appear to be hesitating with their choice, ask them if they need assistance. If they are indeed stuck, refer to the "Opportunities" section to see how you can help them out.
- Refer to the "Questions asked by the players" to respond to players' questions.
- Refer to the "Risk appetite" and "Techniques" sections to understand how does the consumable resource (risk appetite) work
- Refer to the "Turns" section to learn more about possible outcomes of a player's turn.
- If you have a matching Countertechnique card, refer to the "Countertechniques" section to see how and when can you use it.
- Refer to "Transcribing the game" to see how you can write down what happened this turn

Countertechniques

Countertechnique cards represent mitigations that an organisation can do to reduce the impact of a specific technique or ensure it does not succeed. It is also entirely possible for a Technique to not have a corresponding Countertechnique or the same Countertechnique to apply to more than one Technique. It is also possible for a Countertechnique to exist but not to be used in an organisation. For each scenario, you get a limited subset of Countertechniques that you can use once at the earliest possible opportunity.

Each Countertechnique card has a list of Technique cards it counters. As soon as you see a player using a technique that can be countered by any of the Countertechnique cards in your deck - use it. You cannot use the same Countertechnique card again afterwards, whether it is for the same or a different player in the game. Each Countertechnique card can be used once per round.

Once you decide to present the player with a Countertechnique on their turn, do so only if their technique has succeeded. In this case, any chaining success bonuses of this player are preserved (the streak continues), but the player does not get any bonus points this turn even though they rolled successfully (as the outcome of their technique negated). They also do not get any points deducted from them to represent the technique failing safely.

Opportunities

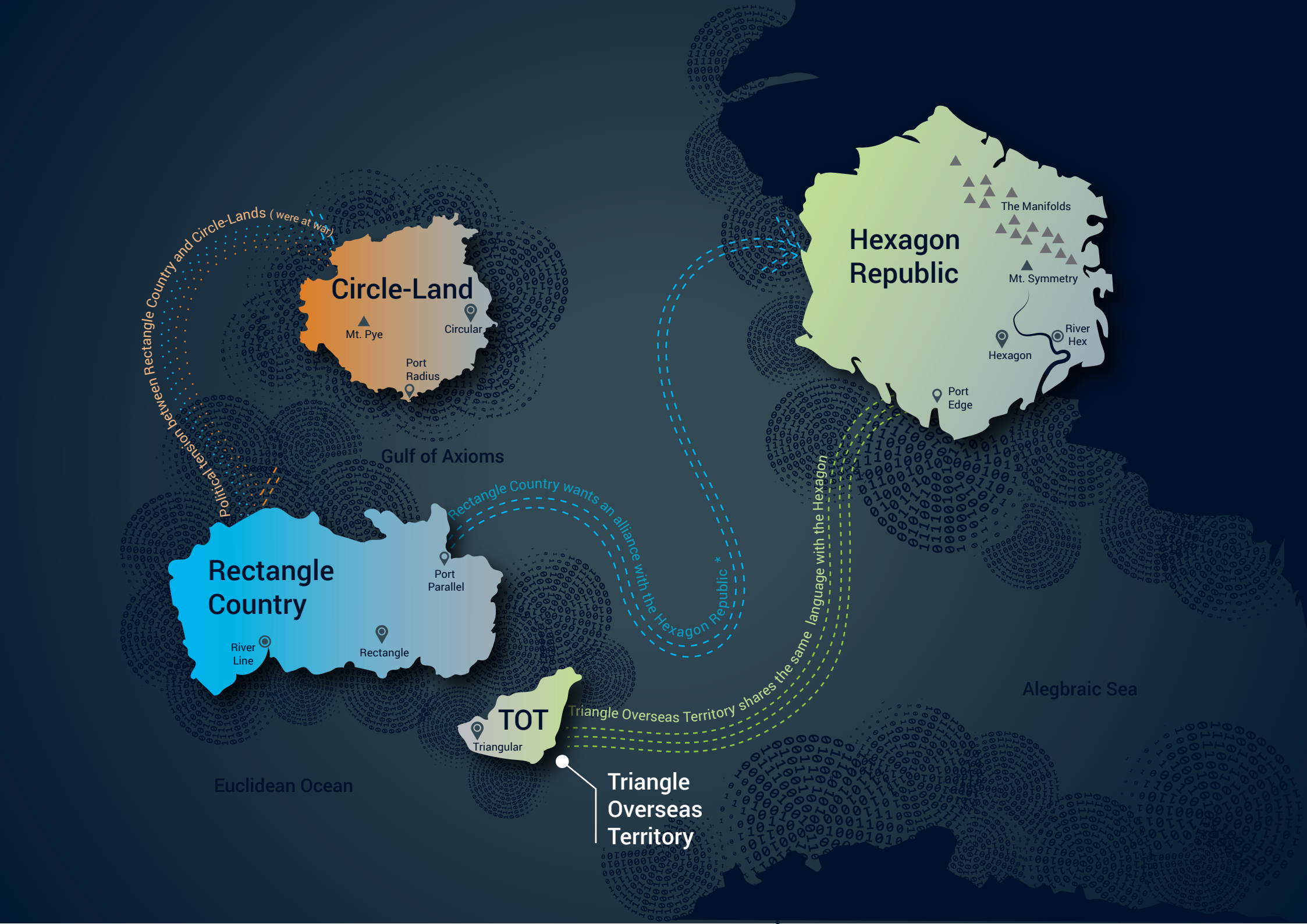
If a player is stuck or is attempting a dead end (and you are willing to do something about it), a deck is designed to help you out with this.

Each Opportunity card has one or more matching Information card that a player receives due to being handed this Opportunity.

When you hand an Opportunity card to a player, make sure they read that card aloud and once they do - give them a corresponding Information card.

Currently, there is no limit as to how many Opportunity cards a player can receive, but try not to get players relying on Opportunities too much, only use them as a last resort.

F.2 Game scenario


Political tension between Rectangle Country and Circle-Lands (were at war)
Circle-Land
Mt. Pye
Circular
Port Radius
Gulf of Axioms
Hexagon Republic
The Manifolds
Mt. Symmetry
River Hex
Hexagon
Port Edge
Rectangle wants an alliance with the Hexagon Republic *
Rectangle Country
Port Parallel
River Line
Rectangle
Triangle Overseas Territory shares the same language with the Hexagon
TOT
Triangular
Triangle Overseas Territory
Euclidean Ocean
Alegbraic Sea

GAME SCENARIO

Including full role descriptions

Sidorenko, Tatjana

Contents

Scenario

Countries

The world that the events take place in has three conveniently geometric significant forces.

On the North East, we have the **Hexagon Republic**, a large country that makes its own rules. It is the most developed country in this world and has the highest living standard for its nation. Although it has a large army, Hexagon prefers not to interfere in any conflicts unless it provides aid for one of the sides, as Hexagon itself is already wholly self-sufficient. It is also the most common immigration location, both legal and illegal, due to the living standards. Hexagon and Rectangle have signed an agreement in the past, where Hexagon would make Triangle their overseas territory. What did Hexagon offer in this agreement is not entirely clear. To date, Rectangle Country's government wants an alliance with the Hexagon Republic and has not made any anti-Hexagon comments in public.

The Hexagon Republic has a small overseas territory in the South East, called **Triangle**. Triangle itself has been used as a condition of negotiations many times in history, so it must always be on the lookout as to what will happen next. Hexagon has been good at protecting it from any external forces. However, small conflicts with non-state armed groups of Rectangle Country still occur close to the TOT's water border, and TOT does not want to rely wholly on Hexagon. Since it joined Hexagon, its infrastructure has significantly expanded. It is now a leading producer of consumer goods, such as personal computers, mobile phones and other electronics, TOT-produced goods always mean quality. Despite this improvement, TOT wants to preserve some of its armed forces and its government with at least some degree of independence. The Hexagon cannot give it full autonomy, as they are aware that every other country wants to annex it due to its gold mines - one of four gold mines in this world, so releasing them will mean immediate war for the people of TOT.

On the North West is **Circle-Land**, which dreams of becoming a big empire. Although it does not have any overseas territories, it has a sufficient army, technological progress and a very resource-rich land. With all of this, it can become an empire, so other countries are quite cautious. Circle-Land uses this caution to its advantage and has a hard time disappearing from the news headlines thanks to the abundance of witty statements from the diplomats. Twenty years ago, there was a war with the neighbouring Rectangle Country, although, to this date, historians still debate about what caused it to begin in the first place. Rectanguliers believe that the Circs have attacked first, as they wanted some of that crude oil. Circs believe it is the Rectanguliers who have struck first, as they did not want another technologically advanced country nearby; they wanted to be the sole owners of all the cutting-edge

technologies. With a fair amount of evidence for both of these theories, there are still political tensions between the two countries.

Finally, in the South East, there is a **Rectangle Country**. Historically, very poor, it has been famous for its fishermen. Ever since the agreement with the Hexagon Republic, several crude oil spots have been found in the deserts of Rectangle. Additionally, this country has seen the golden era of scientists and inventors, rapidly raising this country's profile in the world arena. With successful desert greenification projects and one of the most reliable weapons ever manufactured, Rectangle Country has become the second most developed country in a very short span. Although it has massively improved in the past thirty years, the long-term consequences from the war that happened twenty years ago with the neighbouring Circle-Land are continuously resurfacing. The two nations cannot stand each other, and although the war is over, the rivalry for technology and resources between the two is not. Rectangle Country's government wants to ally with the Hexagon Republic to crush Circle-Land once and for good; however, Hexagon Republic has not expressed any interest in such alliance.

Ground, Aerospace and Marine of Rectangle (GAMR)

Scenario

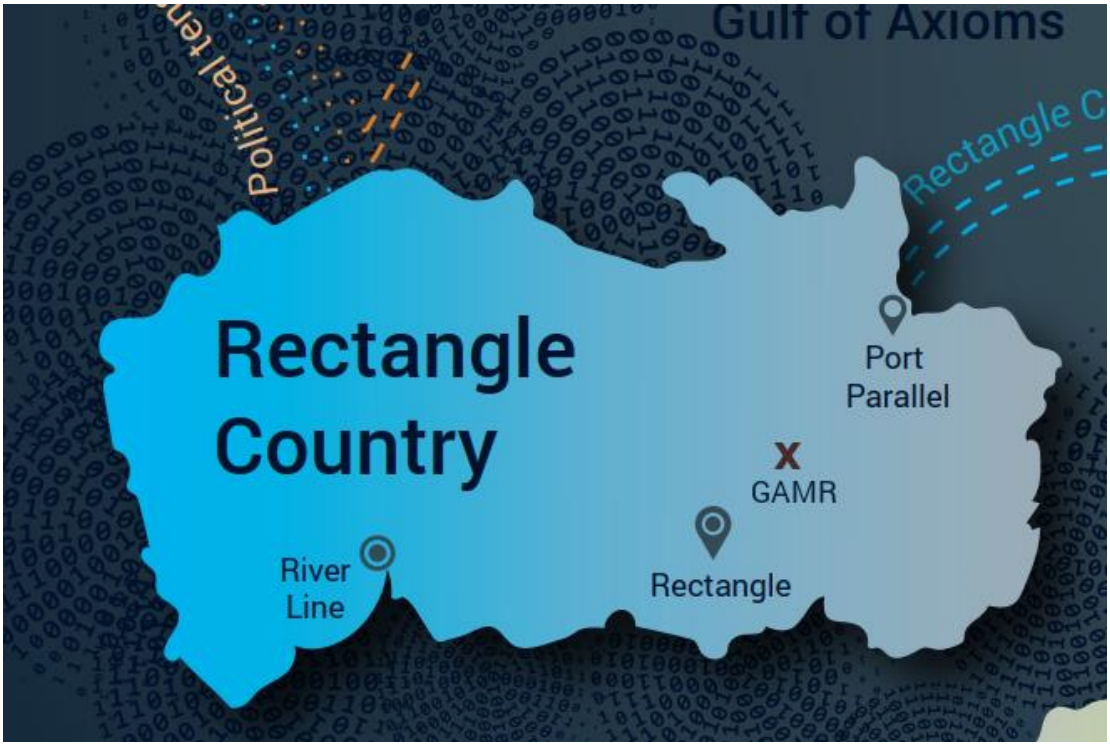
You are a new hire for the Ground, Aerospace and Marine of Rectangle's (GAMR) incident response team. As a defence contractor, quite a few entities would love to get their hands on the intellectual property, plans, and data that GAMR holds. Your job is to monitor the system for any external intrusions and counter them wherever you can.

Fact file

CEO: Q. U. Adrilateral

Defence contractor, tightly linked to Rectangle government. They were part of the Ministry of Defence until it was privatised ten years ago. Develops vehicles and weapons. Actively cooperates with the Rectangle Country's government. It is the most successful defence prime in the country; the second most successful is Future Industries, with whom they hold an active rivalry.

GAMR is based between Rectangle city and Port Parallel.



Roles

Stock trader (Cyber mercenary I)

Proposed scenario

You have been earning your income by purchasing credit card dumps and verifying whether they are still active using a custom script that you wrote. You then re-sell working credit card numbers for a price much much greater than the original. On the dark web, you are known as "the carder". Recently you have learned about investing and figured it would be highly beneficial to put all of that income to good use. You picked out a company with generous dividends and excellent growth prospects and stability on a stock market; this company was GAMR. The plan is simple - get the news about a data breach out there and watch the stock price go down. You then purchase as many shares as you can and when the price comes back up, so do your shares!

Options trading is more likely in this case. (a promise to buy a stock with an expectation for it to go up or down. 95% of these expire worthless.)

Objectives

- Deface the front page so that the screenshot would be newsworthy

OR

- Leak the data about GAMR to the black market, make sure the news about it spread fast.

OR

- Compromise the CEO's (Q. U. Adrilateral) Twitter account to impact the reputation of the company

APT for hire (Cyber mercenary II)

Proposed scenario

You are a member of "The sQUAD", a group that provides APT-for-hire services on the dark web. The sQUAD is a group of five people based in Triangle Overseas Territory that employs state of the art techniques. You do not know who the other four members are as a precaution, so that information is not disclosed. Should one person attempt to betray the organisation - they would not lead the police or

intelligence to the other four people. You could piece together some information from the group's git commits on the internal GitLab - one of the four is very expressive and loves puns. Another listens to Bob Dylan and puts references to his songs in the code. Another does not have Hexagonian as their first language. And the leader is just a complete enigma. He likes to call himself "the orchestrator".

Your responsibilities in the group include finding new potential clients - you are their point of contact with the group. One of the clients has reached out to you and has offered twice the amount that The sQUAD usually charges. It was Mr Sato, the CEO of Future Industries, GAMR's number one competitor, also a defence contractor. You passed the message to your colleagues and were given the green light. Expose GAMR and damage their reputation so that Future Industries gets the Rectangle Country's funding for the mass production of revolutionary weapons.

Objectives

- Obtain access to the Q. U. Adrilateral's inbox (CEO of GAMR) for any potential clues that can help expose him
- Download as many confidential reports as you can find
- Avoid exposing your client. They must not be found out, and your group also has to cover tracks carefully; otherwise, it would be the end of a successful career as an APT-for-hire.

Counter-culture

Proposed scenario

Recently you have obtained your Hexagonian citizenship, and now you can proudly call yourself a Hexer. You have immigrated to the Hexagon Republic from Rectangle Country due to the lower taxes and generally better living conditions. Now you work as a web developer as your day job. The company is quite conservative - it does not want to switch to every new JavaScript framework that comes out; it has stuck with a very well-known tech stack for years. The job is not particularly challenging or fun - everything is predictable, and only after a year and a bit you have found yourself reaching your maximum technological potential. In other words, - you got bored.

You are saving up to purchase a gaming computer since you came to this country with very little personal belongings. In the meantime, you are using your old dusty laptop as your daily driver. Deep in your heart, you still love Rectangle Country and want to come back there one day, as well as keep coming back for visiting your friends and family that you left behind. You have a friend who is working as a civil servant back home, and from the sound of it, it looks like the computers used by the government of rectanguliers (people of Rectangle Country) might be quite vulnerable. An idea that was born in your head that you cannot entirely shut down is

to test how resilient those machines genuinely are, as well as get the latest insight on what Rectangle Country is planning to do next, both for its citizens and for its neighbouring countries.

Objectives

- Gain access to one of the GAMR's internal machines

AND

- Gain access to at least one future development plan (it does not matter whether it is infrastructure, law, economics, politics or other)

OR

- Obtain access to the Q. U. Adrilateral's inbox (CEO of GAMR) for any potential ongoing negotiations that have not been published or exposed

Hacktivist

Proposed scenario

You keep a blog with your commentary on political events and frequent highly conservative groups online.

"Square independence. Two compelling words. Our country does not need an alliance, and we are independent. Calling all square-independers to take action."

'Square' is how the conservatives call Rectangle Country - an improved fortified place equally protected from all sides.

This call for action was posted on one of the social media community pages. The event this was responding to is the negotiations of two presidents - the president of Rectangle Country and the Hexagon Republic president. Rectangle Country has raised the topic of a possible alliance with Hexagon multiple times, yet no decision or any definite answer was given yet. You do not like the government's current direction and how they are actively seeking to ally with another, rather than focusing on improving the internal situation.

The post itself followed with a proposed date of the cyber attack. Another thread was linked with a great list of targets with government contractors or various online government services among all the entries. This post resonated with you. You joined the group preparing this operation and virtually met many like-minded and highly

technically skilled individuals. The group itself is spread across the entire country; some members are even based overseas. You found a place where you belong.

Objectives

- Deface the front page of GAMR, leaving a message about how the government is indecisive.
- Publish the data dumps on the group's torrent server.
- Obtain access to the Q. U. Adrilateral's inbox (CEO of GAMR) for any other information that has not been publicised but may be critically important

Script Kiddy

Proposed scenario

You are a 1-st year university student on an Artificial Intelligence course. You are repeating a year. University life did not go as expected - you have continued from school with precisely zero friends. The subjects were not particularly interesting during your first year - you lost track of them very quickly, and then it was impossible to catch up. However, one subject in this pile of very urgent coursework and recommended reading or rather one lecturer stood out. The subject that he has taught was something to do with networks in the first semester. The exciting part was that he ran an information security enrichment program; just when you thought of quitting university, that lecturer caught your interest. You two had a long conversation after a lecture while he was going out to grab a coffee. He has convinced you to join the enrichment program. But the disappointment came quick - with your current grades, you would not be able to participate in the Capture the Flag challenges representing the university team. To qualify, you have to meet a certain grade threshold. The decision came quick - re-sit the failed subjects by repeating a year and apply for the team. And while you are not allowed to attend the cyber enrichment program, you have decided to study yourself, except that you prefer to start at the deep end.

You frequent the dark web. You have some accounts on the black hat forums, but you rarely post anything to prevent it from seeming n00b. You specifically love following posts of a user with the nickname "PWRs" that often posts open-source exploit kits. Whoever that user is, they always make their instructions crystal clear - change this IP, run this first, read this first. And their tools work, every time. It's incredible how they do it. First, you have launched a DDoS attack on the website of your former school. They have to pay back for always giving you detentions. Your attack has been so overwhelmingly successful that the story made the local news, with you not getting caught. PWRs knows their job well - every tool that they write encrypts the channel. Next, you have installed a RAT on the university network, just in case one of the exams does not go as planned. Of course, you have left a note on

every lecturer's personal webpage, except for the one running the cyber enrichment program, just in case. The department has launched an investigation but ultimately shut it down, not finding the culprit, attributing it only to a prank. The network has been redesigned, and now your RAT is no longer installed. You don't want to get in trouble with the university, so you had to pick out a new target. Then you recalled being rejected in a very humiliating manner during an interview at GAMR when you applied for their summer internship. That really did hurt. They did not have to phrase it like this.

Objectives

- Put, "You can't make planes if you reject people who care!" on the front page of the contractor's website.
- Avoid getting caught. You still have a university to finish and a cyber enrichment program to join.

State-backed (low risk)

Proposed Scenario

(the attacker is from TOT)

Triangle has never been a significant figure on the political scene. Just an overseas territory belonging to the Hexagon Republic. But even Triangle has its cyber warfare unit - the Triangle Cyber Force (TCF). The geographical location of TOT and some history between Triangle and Rectangle Country means that Triangle's forces must always keep track of what happens in the land of its geographical neighbour. However, such a unit's existence has not been welcomed by the Hexagon Republic; hence, TCF's capabilities are minimal.

Morning at TCF begins at 8:30 AM local time. On the agenda is operation Sunray - target the two most notable defence primes in Rectangle Country and make sure Triangle is safe... for now.

Objectives

- Gain access to at least one future development plan (it does not matter whether it is infrastructure, law, economics, politics or other)
- Avoid getting detected; otherwise, Hexagon Republic might shut down Triangle Cyber Force.

F.3 GM helper notes

PROCEDURE EXAMPLES

Contains examples of every Technique card retrieved straight from MITRE. Use this document to check if a player is trying to conduct a legitimate attack and not making up information as they go.

Contents

T 01 - Exploitation for Client Execution

TL;DR

Uses vulns in programs like Word/Flash/etc on the client computer to execute a malicious script.

Procedure Examples

Name	Description
admin@338	admin@338 has exploited client software vulnerabilities for execution, such as Microsoft Word CVE-2012-0158.[1]
APT12	APT12 has exploited multiple vulnerabilities for execution, including Microsoft Office vulnerabilities (CVE-2009-3129, CVE-2012-0158) and vulnerabilities in Adobe Reader and Flash (CVE-2009-4324, CVE-2009-0927, CVE-2011-0609, CVE-2011-0611).[2][3]
APT28	APT28 has exploited Microsoft Office vulnerability CVE-2017-0262 for execution.[4]
APT29	APT29 has used multiple software exploits for common client software, like Microsoft Word and Adobe Reader, to gain code execution as part of.[5]
APT32	APT32 has used RTF document that includes an exploit to execute malicious code. (CVE-2017-11882)[6]
APT33	APT33 has attempted to exploit a known vulnerability in WinRAR (CVE-2018-20250), and attempted to gain remote code execution via a security bypass vulnerability (CVE-2017-11774).[7][8]
APT37	APT37 has used Flash Player (CVE-2016-4117, CVE-2018-4878) and Word (CVE-2017-0199) exploits for execution.[9][10][11]
APT41	APT41 leveraged the follow exploits in their operations: CVE-2012-0158, CVE-2015-1641, CVE-2017-0199, CVE-2017-11882, and CVE-2019-3396.[12]
Bankshot	Bankshot leverages a known zero-day vulnerability in Adobe Flash to execute the implant into the victims' machines.[13]
BlackTech	BlackTech has exploited multiple vulnerabilities for execution, including Microsoft Office vulnerabilities CVE-2012-0158, CVE-2014-6352, CVE-2017-0199, and Adobe Flash CVE-2015-5119.
BRONZE BUTLER	BRONZE BUTLER has exploited Microsoft Office vulnerabilities CVE-2014-4114, CVE-2018-0802, and CVE-2018-0798 for execution.[14][15]
Cobalt Group	Cobalt Group had exploited multiple vulnerabilities for execution, including Microsoft's Equation Editor (CVE-2017-11882), an Internet Explorer vulnerability (CVE-2018-8174), CVE-2017-8570, CVE-2017-0199, and CVE-2017-8759.[16][17][18][19][20][21][22][23]
DealersChoice	DealersChoice leverages vulnerable versions of Flash to perform execution.[24]
Elderwood	Elderwood has used exploitation of endpoint software, including Microsoft Internet Explorer Adobe Flash vulnerabilities, to gain execution. They have also used zero-day exploits.[25]
EvilBunny	EvilBunny has exploited CVE-2011-4369, a vulnerability in the PRC component in Adobe Reader.[26]

Frankenstein	Frankenstein has used CVE-2017-11882 to execute code on the victim's machine.[27]
HAWKBALL	HAWKBALL has exploited Microsoft Office vulnerabilities CVE-2017-11882 and CVE-2018-0802 to deliver the payload.[28]
Inception	Inception has exploited CVE-2012-0158, CVE-2014-1761, CVE-2017-11882 and CVE-2018-0802 for execution.[29][30][31][32]
InvisiMole	InvisiMole has installed legitimate but vulnerable Total Video Player software and wdigest.dll library drivers on compromised hosts to exploit stack overflow and input validation vulnerabilities for code execution.[33]
Lazarus Group	Lazarus Group has exploited Adobe Flash vulnerability CVE-2018-4878 for execution.[13]
Leviathan	Leviathan has exploited multiple Microsoft Office and .NET vulnerabilities for execution, including CVE-2017-0199, CVE-2017-8759, and CVE-2017-11882.[34][35]
MuddyWater	MuddyWater has exploited the Office vulnerability CVE-2017-0199 for execution.[36]
Patchwork	Patchwork uses malicious documents to deliver remote execution exploits as part of. The group has previously exploited CVE-2017-8570, CVE-2012-1856, CVE-2014-4114, CVE-2017-0199, CVE-2017-11882, and CVE-2015-1641.[37][38][39][40][41][42][43]
Ramsay	Ramsay has been embedded in documents exploiting CVE-2017-0199 and CVE-2017-11882.[44]
Sandworm Team	Sandworm Team has exploited vulnerabilities in Microsoft PowerPoint via OLE objects (CVE-2014-4114) and Microsoft Word via crafted TIFF images (CVE-2013-3906).[45][46][47]
SpeakUp	SpeakUp attempts to exploit the following vulnerabilities in order to execute its malicious script: CVE-2012-0874, CVE-2010-1871, CVE-2017-10271, CVE-2018-2894, CVE-2016-3088, JBoss AS 3/4/5/6, and the Hadoop YARN ResourceManager. [48]
TA459	TA459 has exploited Microsoft Word vulnerability CVE-2017-0199 for execution.[49]
The White Company	The White Company has taken advantage of a known vulnerability in Microsoft Word (CVE 2012-0158) to execute code.[50]
Threat Group-3390	Threat Group-3390 has exploited the Microsoft SharePoint vulnerability CVE-2019-0604.[51]
Tropic Trooper	Tropic Trooper has executed commands through Microsoft security vulnerabilities, including CVE-2017-11882, CVE-2018-0802, and CVE-2012-0158.[52][53]
Xbash	Xbash can attempt to exploit known vulnerabilities in Hadoop, Redis, or ActiveMQ when it finds those services running in order to conduct further execution.[54][55]

T 02 - Steal Web Session Cookie

TL;DR

The name is quite descriptive here – used to steal cookies from any browser or RealNetworks applications.

Procedure Examples

Name	Description
CookieMiner	CookieMiner can steal Google Chrome and Apple Safari browser cookies from the victim's machine. [6]
TajMahal	TajMahal has the ability to steal web session cookies from Internet Explorer, Netscape Navigator, FireFox and RealNetworks applications.[2]

T 03 - Web Shell

TL;DR

An attacker can use a publicly available web shell to gain or maintain access to victim's network. Or run a web shell payload. Or access a website. Can be used during initial foothold stage (to stay on the network) or persistence stage (to make the connection stable).

Procedure Examples

Name	Description
APT32	APT32 has used Web shells to maintain access to victim websites.[2]
APT39	APT39 has installed ANTAK and ASPXSPY web shells. [3]
ASPXSpy	ASPXSpy is a Web shell. The ASPXTool version used by Threat Group-3390 has been deployed to accessible servers running Internet Information Services (IIS).[4]
China Chopper	China Chopper's server component is a Web Shell payload.[1]
Deep Panda	Deep Panda uses Web shells on publicly accessible Web servers to access victim networks.[5]
Dragonfly 2.0	Dragonfly 2.0 commonly created Web shells on victims' publicly accessible email and web servers, which they used to maintain access to a victim network and download additional malicious files.[6][7]
Leviathan	Leviathan relies on web shells for an initial foothold as well as persistence into the victim's systems. [8]
OilRig	OilRig has used Web shells, often to maintain access to a victim network.[9][10]
OwaAuth	OwaAuth is a Web shell that appears to be exclusively used by Threat Group-3390. It is installed as an ISAPI filter on Exchange servers and shares characteristics with the China Chopper Web shell.[4]
SEASHARPEE	SEASHARPEE is a Web shell.[10]
Soft Cell	Soft Cell used Web shells to persist in victim environments and assist in execution and exfiltration.[11]
TEMP.Veles	TEMP.Veles has planted Web shells on Outlook Exchange servers.[12]

Threat Group-3390	Threat Group-3390 has used a variety of Web shells.[13]
Tropic Trooper	Tropic Trooper has started a web service in the target host and wait for the adversary to connect, acting as a web shell.[14]

T 04 - Credentials from Web Browsers

TL;DR

A technique that can gather credentials from browsers (sometimes other programs too, e.g. Outlook), either by using a plug-in, stored passwords function in browser, or from profile folders, or from local storage (AppData), or by querying the SQLite database. Located passwords get stored in a convenient database in some cases.

Procedure Examples

Name	Description
APT3	APT3 has used tools to dump passwords from browsers.[6]
APT33	APT33 has used a variety of publicly available tools like LaZagne to gather credentials.[7][8]
APT37	APT37 has used a credential stealer known as ZUMKONG that can harvest usernames and passwords stored in browsers.[9]
Azorult	Azorult can steal credentials from the victim's browser.[10]
Backdoor.Oldrea	Some Backdoor.Oldrea samples contain a publicly available Web browser password recovery tool.[11]
BlackEnergy	BlackEnergy has used a plug-in to gather credentials from web browsers including FireFox, Google Chrome, and Internet Explorer.[12][13]
Carberp	Carberp's passw.plug plugin can gather passwords saved in Opera, Internet Explorer, Safari, Firefox, and Chrome.[14]
ChChes	ChChes steals credentials stored inside Internet Explorer.[15]
CookieMiner	CookieMiner can steal saved usernames and passwords in Chrome as well as credit card credentials.[16]
CosmicDuke	CosmicDuke collects user credentials, including passwords, for various programs including Web browsers.[17]
Crimson	Crimson contains a module to steal credentials from Web browsers on the victim machine.[18]
Emotet	Emotet has been observed dropping browser password grabber modules. [19][20]
Empire	Empire can use modules that extract passwords from common web browsers such as Firefox and Chrome.[21]

FIN6	FIN6 has used the Stealer One credential stealer to target web browsers.[22]
H1N1	H1N1 dumps usernames and passwords from Firefox, Internet Explorer, and Outlook.[23]
Imminent Monitor	Imminent Monitor has a PasswordRecoveryPacket module for recovering browser passwords.[24]
Inception	Inception used a browser plugin to steal passwords and sessions from Internet Explorer, Chrome, Opera, Firefox, Torch, and Yandex.[25]
jRAT	jRAT can capture passwords from common web browsers such as Internet Explorer, Google Chrome, and Firefox.[26]
KeyBoy	KeyBoy attempts to collect passwords from browsers.[27]
Kimsuky	Kimsuky has used a Google Chrome extension to steal passwords and cookies from their browsers.[28]
KONNI	KONNI can steal profiles (containing credential information) from Firefox, Chrome, and Opera.[29]
LaZagne	LaZagne can obtain credentials from web browsers such as Google Chrome, Internet Explorer, and Firefox.[30]
Leafminer	Leafminer used several tools for retrieving login and password information, including LaZagne.[31]
Lokibot	Lokibot has demonstrated the ability to steal credentials from multiple applications and data sources including Safari and the Chromium and Mozilla Firefox-based web browsers.[32]
Machete	Machete collects stored credentials from several web browsers.[33]
Magic Hound	Magic Hound used FireMalv, custom-developed malware, which collected passwords from the Firefox browser storage.[34]
Mimikatz	Mimikatz performs credential dumping to obtain account and password information useful in gaining access to additional systems and enterprise network resources. It contains functionality to acquire information about credentials in many ways, including from DPAPI.[35][36][37][38]
Molerats	Molerats used the public tool BrowserPasswordDump10 to dump passwords saved in browsers on victims.[39]
MuddyWater	MuddyWater has run a tool that steals passwords saved in victim web browsers.[40]

njRAT	njRAT has a module that steals passwords saved in victim web browsers.[41][42][43]
OilRig	OilRig has used credential dumping tools such as LaZagne to steal credentials to accounts logged into the compromised system and to Outlook Web Access.[44][45][46][47] OilRig has also used tools named VALUEVAULT and PICKPOCKET to dump passwords from web browsers.[47]
OLDBAIT	OLDBAIT collects credentials from Internet Explorer, Mozilla Firefox, and Eudora.[48]
Olympic Destroyer	Olympic Destroyer contains a module that tries to obtain stored credentials from web browsers.[1]
Patchwork	Patchwork dumped the login data database from \AppData\Local\Google\Chrome\User Data\Default\Login Data.[49]
PinchDuke	PinchDuke steals credentials from compromised hosts. PinchDuke's credential stealing functionality is believed to be based on the source code of the Pinch credential stealing malware (also known as LdPinch). Credentials targeted by PinchDuke include ones associated with many sources such as Netscape Navigator, Mozilla Firefox, Mozilla Thunderbird, and Internet Explorer. [17]
PLEAD	PLEAD has the ability to steal saved credentials from web browsers.[50][51]
PoetRAT	PoetRAT has used a Python tool named Browdec.exe to steal browser credentials.[52]
Prikormka	A module in Prikormka gathers logins and passwords stored in applications on the victims, including Google Chrome, Mozilla Firefox, and several other browsers.[53]
Proton	Proton gathers credentials for Google Chrome.[54]
Pupy	Pupy can use Lazagne for harvesting credentials.[55]
QuasarRAT	QuasarRAT can obtain passwords from common web browsers.[56][57]
RedLeaves	RedLeaves can gather browser usernames and passwords.[58]
ROKRAT	ROKRAT steals credentials stored in Web browsers by querying the sqlite database.[59]
Sandworm Team	Sandworm Team's CredRaptor tool can collect saved passwords from various internet browsers.[60]

Smoke Loader	Smoke Loader searches for credentials stored from web browsers.[61]
Stealth Falcon	Stealth Falcon malware gathers passwords from multiple sources, including Internet Explorer, Firefox, and Chrome.[62]
Stolen Pencil	Stolen Pencil has used tools that are capable of obtaining credentials from web browsers.[63]
TA505	TA505 has used malware to gather credentials from Internet Explorer.[64]
TrickBot	TrickBot can obtain passwords stored in files from web browsers such as Chrome, Firefox, Internet Explorer, and Microsoft Edge, sometimes using esentutl.[65][66]
Trojan.Karagany	Trojan.Karagany can steal data and credentials from browsers.[67]
TSCookie	TSCookie has the ability to steal saved passwords from the Internet Explorer, Edge, Firefox, and Chrome browsers.[68]
Unknown Logger	Unknown Logger is capable of stealing usernames and passwords from browsers on the victim machine.[69]
XAgentOSX	XAgentOSX contains the getFirefoxPassword function to attempt to locate Firefox passwords.[70]
Zebrocy	Zebrocy has the capability to upload dumper tools that extract credentials from web browsers and store them in database files.[71]

T 05 - Domain Fronting

TL;DR

From the examples observed in the wild it is to hide the destination of network traffic using the server on the same CDN as the destination.

Procedure Examples

Name	Description
APT29	APT29 has used the meek domain fronting plugin for Tor to hide the destination of C2 traffic.[2]
meek	meek uses Domain Fronting to disguise the destination of network traffic as another server that is hosted in the same Content Delivery Network (CDN) as the intended desitnation.

T 06 - Exfiltration Over Alternative Protocol

TL;DR

This TTP is mostly concerned with extracting and downloading information via different means, such as email, DNS tunneling or connecting to a pre-defined port.

Procedure Examples

Name	Description
FrameworkPOS	FrameworkPOS can use DNS tunneling for exfiltration of credit card data.[2]
Hydraq	Hydraq connects to a predefined domain on port 443 to exfil gathered information.[3]
PoetRAT	PoetRAT has used a .NET tool named dog.exe to exiltrate information over an e-mail account.[4]

T 07 - Browser Extensions

TL;DR

Using browser extensions to serve ads/download passwords or cookies, or even read data from any website accessed.

Procedure Examples

Name	Description
Bundlore	Bundlore can install malicious browser extensions that are used to hijack user searches.[10]
Kimsuky	Kimsuky has used a Google Chrome extension to infect victims and steal passwords and cookies from their browsers.[11]
OSX/Shlayer	OSX/Shlayer can install malicious Safari browser extensions to serve ads.[12][13]
Stolen Pencil	Stolen Pencil victims are prompted to install malicious Google Chrome extensions which gave the threat actor the ability to read data from any website accessed. [14]

T 08 - Exploit Public-Facing Application

TL;DR

Conducting attacks like buffer overflow, SQL injection and utilising various exploits against public-facing websites, application delivery controllers (next generation of load balancers, typically located between the firewall/router and the web server farm.), UI and Control panels.

Procedure Examples

Name	Description
APT28	APT28 has conducted SQL injection attacks against organizations' external websites.[8]
APT29	APT29 has exploited CVE-2019-19781 for Citrix, CVE-2019-11510 for Pulse Secure VPNs, CVE-2018-13379 for FortiGate VPNs, and CVE-2019-9670 in Zimbra software to gain access.[9]
APT39	APT39 has used SQL injection for initial compromise.[10]
APT41	APT41 exploited CVE-2020-10189 against Zoho ManageEngine Desktop Central, and CVE-2019-19781 to compromise Citrix Application Delivery Controllers (ADC) and gateway devices.[11]
Axiom	Axiom has been observed using SQL injection to gain access to systems.[12][13]
BlackTech	BlackTech has exploited a buffer overflow vulnerability in Microsoft Internet Information Services (IIS) 6.0, CVE-2017-7269, in order to establish a new HTTP or command and control (C2) server.[14]
Blue Mockingbird	Blue Mockingbird has gained initial access by exploiting CVE-2019-18935, a vulnerability within Telerik UI for ASP.NET AJAX.[15]
GOLD SOUTHFIELD	GOLD SOUTHFIELD has exploited Oracle WebLogic vulnerabilities for initial compromise.[16]
Havij	Havij is used to automate SQL injection.[17]
Night Dragon	Night Dragon has performed SQL injection attacks of extranet web servers to gain access.[18]
Rocke	Rocke exploited Apache Struts, Oracle WebLogic (CVE-2017-10271), and Adobe ColdFusion (CVE-2017-3066) vulnerabilities to deliver malware.[19][20]
Soft Cell	Soft Cell exploited a publicly-facing server to gain access to the network.[21]
SoreFang	SoreFang can gain access by exploiting a Sangfor SSL VPN vulnerability that allows for the placement and delivery of malicious update binaries.[22]
sqlmap	sqlmap can be used to automate exploitation of SQL injection vulnerabilities.[23]
UNC2452	UNC2452 exploited CVE-2020-0688 against the Microsoft Exchange Control Panel to regain access to a network.[24]

T 09 - Spearphishing Link

TL;DR

The objective here is to get the victim to click on the link, which might be sent in an email with lookalike branding (to appear legitimate). Sometimes the link can be obfuscated by a URL shortener. The hyperlink can point to malicious Word documents that contain macros, redirect the user to credential harvesting websites, point to a malicious zip (or any other archive) file, .hta files that are capable of executing scripts. They can also point to cloud services, execute PowerShell scripts and so forth, the possibilities are endless. The malicious code is often used to gain initial access to the victim's machine.

Procedure Examples

Name	Description
APT1	APT1 has sent spearphishing emails containing hyperlinks to malicious files.[2]
APT28	APT28 sent spearphishing emails which used a URL-shortener service to masquerade as a legitimate service and to redirect targets to credential harvesting sites.[3][4][5]
APT29	APT29 has used spearphishing with a link to trick victims into clicking on a link to a zip file containing malicious files.[6]
APT32	APT32 has sent spearphishing emails containing malicious links.[7][8][9]
APT33	APT33 has sent spearphishing emails containing links to .hta files (HTA contains hypertext code, VBScript or JScript code depending on the program set up.).[10][11]
APT39	APT39 leveraged spearphishing emails with malicious links to initially compromise victims. [12]
BlackTech	BlackTech has used spearphishing e-mails with links to cloud services to deliver malware.[13]
Cobalt Group	Cobalt Group has sent emails with URLs pointing to malicious documents.[14]
Dragonfly 2.0	Dragonfly 2.0 used spearphishing with PDF attachments containing malicious links that redirected to credential harvesting websites.[15]
Elderwood	Elderwood has delivered zero-day exploits and malware to victims via targeted emails containing a link to malicious content hosted on an uncommon Web server.[16][17]
Emotet	Emotet has been delivered by phishing emails containing links. [18][19][20][21][22][23][24][24][25]
FIN4	FIN4 has used spearphishing emails (often sent from compromised accounts) containing malicious links.[26][27]
FIN8	FIN8 has distributed targeted emails containing links to malicious documents with embedded macros.[28]
Hancitor	Hancitor has been delivered via phishing emails which contained malicious links.[29]
Kimsuky	Kimsuky has used an email containing a link to a document that contained malicious macros.[30]

Leviathan	Leviathan has sent spearphishing emails with links, often using a fraudulent lookalike domain and stolen branding.[31]
Machete	Machete has sent phishing emails that contain a link to an external server with ZIP and RAR archives.[32][33]
Magic Hound	Magic Hound sent shortened URL links over email to victims. The URLs linked to Word documents with malicious macros that execute PowerShells scripts to download Pupy.
Mofang	Mofang delivered spearphishing emails with malicious links included.[34]
Molerats	Molerats has sent phishing emails with malicious links included.[35]
Night Dragon	Night Dragon sent spearphishing emails containing links to compromised websites where malware was downloaded.[36]
OilRig	OilRig has sent spearphising emails with malicious links to potential victims.[37]
Patchwork	Patchwork has used spearphishing with links to deliver files with exploits to initial victims. The group has also used embedded image tags (known as web bugs) with unique, per-recipient tracking links in their emails for the purpose of identifying which recipients opened messages.[38][39][40][41]
Pony	Pony has been delivered via spearphishing emails which contained malicious links.[42]
Stolen Pencil	Stolen Pencil sent spearphishing emails containing links to domains controlled by the threat actor.[43]
TA505	TA505 has sent spearphishing emails containing malicious links.[44][45][46][47]
TrickBot	TrickBot has been delivered via malicious links in phishing e-mails.[48]
Turla	Turla attempted to trick targets into clicking on a link featuring a seemingly legitimate domain from Adobe.com to download their malware and gain initial access.[49]
Valak	Valak has been delivered via malicious links in e-mail.[50]
Windshift	Windshift has sent spearphishing emails with links to harvest credentials and deliver malware.[51]
Wizard Spider	Wizard Spider has sent phishing emails containing a link to an actor-controlled Google Drive document or other free online file hosting services.[52][53]

T 10 - Trusted Relationship

TL;DR

The name is pretty self-explanatory. Abusing trust and legitimate access given to access information of interest, deliver malware or compromise resources.

Procedure Examples

Name	Description
APT28	Once APT28 gained access to the DCCC network, the group then proceeded to use that access to compromise the DNC network.[1]
GOLD SOUTHFIELD	GOLD SOUTHFIELD has breached Managed Service Providers (MSP's) to deliver malware to MSP customers.[2]
menuPass	menuPass has used legitimate access granted to Managed Service Providers in order to access victims of interest.[3][4]

T11 - Drive-by Compromise

TL;DR

A watering hole attack is a malware attack in which the attacker observes the websites often visited by a victim or a particular group, and infects those sites with malware. Most of the applications of this technique are targeted against a particular group of interest. The means vary – malicious ads, torrent files spreading malware, code injected into web pages, embedded iframes, malware in pirated software, browser plugins.

Procedure Examples

Name	Description
APT19	APT19 performed a watering hole attack on forbes.com in 2014 to compromise targets.[3]
APT32	APT32 has infected victims by tricking them into visiting compromised watering hole websites.[4]
APT37	APT37 has used strategic web compromises, particularly of South Korean websites, to distribute malware. The group has also used torrent file-sharing sites to more indiscriminately disseminate malware to victims. As part of their compromises, the group has used a Javascript based profiler called RICECURRY to profile a victim's web browser and deliver malicious code accordingly.[5][6]
APT38	APT38 has conducted watering holes schemes to gain initial access to victims.[7]
BRONZE BUTLER	BRONZE BUTLER compromised three Japanese websites using a Flash exploit to perform watering hole attacks.[8]
Bundlore	Bundlore has been spread through malicious advertisements on websites.[9]
Dark Caracal	Dark Caracal leveraged a watering hole to serve up malicious code.[10]
Darkhotel	Darkhotel used embedded iframes on hotel login portals to redirect selected victims to download malware.[11]
Dragonfly	Dragonfly has has compromised targets via strategic web compromise (SWC) utilizing a custom exploit kit.[12]
Dragonfly 2.0	Dragonfly 2.0 compromised legitimate organizations' websites to create watering holes to compromise victims.[13]
Elderwood	Elderwood has delivered zero-day exploits and malware to victims by injecting malicious code into specific public Web pages visited by targets within a particular sector.[14][15][16]
KARAE	KARAE was distributed through torrent file-sharing websites to South Korean victims, using a YouTube video downloader application as a lure.[6]
Lazarus Group	Lazarus Group delivered RATANKBA to victims via a compromised legitimate website.[17]
Leafminer	Leafminer has infected victims using watering holes.[18]
LoudMiner	LoudMiner is typically bundled with pirated copies of Virtual Studio Technology (VST) for Windows and macOS.[19]

Patchwork	Patchwork has used watering holes to deliver files with exploits to initial victims.[20][21]
PLATINUM	PLATINUM has sometimes used drive-by attacks against vulnerable browser plugins.[22]
POORAIM	POORAIM has been delivered through compromised sites acting as watering holes.[6]
PROMETHIUM	PROMETHIUM has used watering hole attacks to deliver malicious versions of legitimate installers.[23]
REvil	REvil has infected victim machines through compromised websites and exploit kits.[24][25][26][27]
RTM	RTM has distributed its malware via the RIG and SUNDOWN exploit kits, as well as online advertising network Yandex.Direct.[28][29]
Threat Group-3390	Threat Group-3390 has extensively used strategic web compromises to target victims.[30][31]
Turla	Turla has infected victims using watering holes.[32]
Windshift	Windshift has used compromised websites to register custom URL schemes on a remote system.[33]

T 12 - Spearphishing via Service

TL;DR

Conducting spearphishing campaigns via social media, fake job postings and fake personas online.

Procedure Examples

Name	Description
Dark Caracal	Dark Caracal spearphished victims via Facebook and Whatsapp.[1]
FIN6	FIN6 has used fake job advertisements sent via LinkedIn to spearphish targets.[2]
Lazarus Group	Lazarus Group has used fake job advertisements sent via LinkedIn to spearphish victims.[3]
Magic Hound	Magic Hound used various social media channels to spearphish victims.[4][5][6]
OilRig	OilRig has used LinkedIn to send spearphishing links.[7]
Windshift	Windshift has used fake personas on social media to engage and target victims.[8]

T13 - Man in the Browser

TL;DR

Can spoof a website and make it appear legitimate; steal credentials and authenticated sessions or use HTML codes to steal creds. Most frequently used to steal credentials.

Procedure Examples

Name	Description
Agent Tesla	Agent Tesla has the ability to use form-grabbing to extract data from web data forms.[5]
Carberp	Carberp has captured credentials when a user performs login through a SSL session.[6][7]
Cobalt Strike	Cobalt Strike can perform browser pivoting and inject into a user's browser to inherit cookies, authenticated HTTP sessions, and client SSL certificates.[4]
Dridex	Dridex can perform browser attacks via web injects to steal information such as credentials, certificates, and cookies.[8]
IcedID	IcedID has used web injection attacks to redirect victims to spoofed sites designed to harvest banking and other credentials. IcedID can use a self-signed TLS certificate in connection with the spoofed site and simultaneously maintains a live connection with the legitimate site to display the correct URL and certificates in the browser.[9][10]
TrickBot	TrickBot uses web injects and browser redirection to trick the user into providing their login credentials on a fake or modified web page.[11][12][13][14]
Ursnif	Ursnif has injected HTML codes into banking sites to steal sensitive online banking information (ex: usernames and passwords).[15]

F.4 Game Decks

Roles

R 01

Stock Trader

TYPE Cyber Mercenary

RISK APPETITE 8/10

GOALS

- Deface the front page so that the screenshot would be newsworthy
- Leak the data about GAMR to the black market, make sure the news about it spread fast.
- Compromise the CEO's (Q.U. Adrilateral) Twitter account to impact the reputation of the company

SCENARIO

You picked out a company with generous dividends and excellent growth prospects and stability on a stock market; this company was GAMR. The plan is simple - get the news about a data breach out there and watch the stock price go down. You then purchase as many shares as you can and when the price comes back up, so do your shares!

R 02

APT for hire

TYPE Cyber Mercenary

RISK APPETITE 8/10

GOALS

- Obtain access to the Q.U. Adrilateral's inbox (CEO of G MR) for any potential clues that help expose him
- Download as many confidential reports as you can find
- Avoid exposing your client. They must not be found out, and your group also has to cover tracks carefully; otherwise, it would be the end of a successful career as an APT-for-hire.

SCENARIO

You are a member of "The sQUAD", a group that provides APT-for-hire services on the dark web. One of the clients has reached out to you and has offered twice the amount that The sQUAD usually charges. It was Mr Sato, the CEO of Future Industries, GAMR's number one competitor, also a defence contractor. You passed the message to your colleagues and were given the green light. Expose GAMR and damage their reputation so that Future Industries gets the Rectangle Country's funding for the mass production of revolutionary weapons.

R 03

Curious Lone Wolf

TYPE Counter-Culture

RISK APPETITE 5/10

GOALS

- Gain access to one of the GAMR's internal machines
- Gain access to at least one future development plan (it does not matter whether it is infrastructure, law, economics, politics or other)
- Obtain access to the Q.U. Adrilateral's inbox (CEO of GAMR) for any potential ongoing negotiations that have not been published or exposed

SCENARIO

You have immigrated to the Hexagon Republic from Rectangle Country due to the lower taxes and generally better living conditions. But you still have friends and family back home and you hope to return there one day. You have a friend who is working as a civil servant back home, and from the sound of it, it looks like the computers used by the government of rectanguliers (people of Rectangle Country) might be quite vulnerable. You have been itching to test how resilient those machines truly are, as well as get the latest insight on what Rectangle Country is planning to do next, both for its citizens and for its neighbouring countries.

R 04

A Group with a Purpose

TYPE Hacktivist

RISK APPETITE 10/10

GOALS

- Deface front page ofGAMR, leaving a message about how the government is indecisive.
- Publish the data dumps on the group's torrent server.
- Obtain access to the Q. U. Adrilateral's inbox (CEO of GAMR) for any other information that has not been publicised but may be critically important

SCENARIO

"Square independence. Remember these two words. Our country does not need an alliance, we are independent. Calling all square-independers to take action." This call for action was posted on one of the social media community pages. You as a Rectangle Country patriot do not like the government's current direction and how they are actively seeking to ally with another, rather than focusing on improving the internal situation. You joined the group preparing this operation and have truly found a place where you belong.

R 05

The Upset Undergraduate

TYPE Script Kiddy

RISK APPETITE 3/10

GOALS

- Put, "You can't make planes if you reject people who care!" on the front page of the contractor's website.
- Avoid getting caught. You still have a university to finish and a cyber enrichment program to join.

SCENARIO

You are a 1-st year university student, who is repeating a year. Life did not exactly go as planned but one lecturer has convinced you to keep going and to join a cyber enrichment programme. Your grades do not let you join just yet, but in the meantime, you have started breaching the security of various places on your own using pre-made tools from the dark web. You did place a backdoor in the university's network to ensure your exam resits go smoothly but nearly got caught. You don't want to get in trouble with the university, so you had to pick out a new target. Then you recalled being rejected in a very humiliating manner during an interview at GAMR when you applied for their summer internship, and now it's time for a little revenge.

R 06

The Observer from the Island

TYPE State-Backed

RISK APPETITE 4/10

GOALS

- Gain access to at least one future development plan (it does not matter whether it is infrastructure,law, economics, politics or other)
- Avoid getting detected, otherwise Hexagon Republic might shut down Triangle Cyber Force and/ or send their own military units to TOT.

SCENARIO

Triangle has never been a major figure on the political scene. Just an overseas territory belonging to Hexagon Republic. But even Triangle has its cyber warfare unit - the Triangle Cyber Force (TCF). The geographical location of TOT and some history between Triangle and Rectangle Country means that Triangle's forces must always keep track of what happens in the land of its geographical neighbour. However, such a unit's existence has not been welcomed by the Hexagon Republic; hence, TCF's capabilities are minimal. On the agenda is operation Sunray - target the two most notable defence primes in Rectangle Country and make sure Triangle is safe... for now.

R 07

A Force to be Reckoned With

TYPE State-Backed

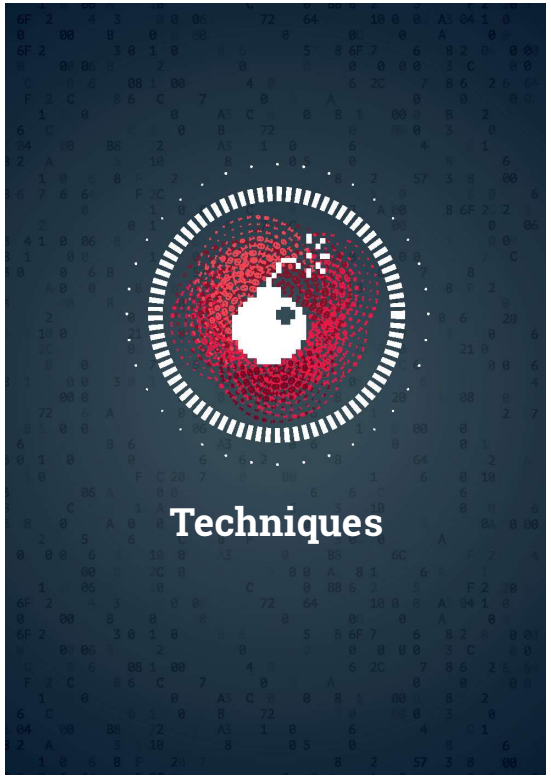
RISK APPETITE 10/10

GOALS

- Download as many confidential reports as you can find
- Obtain access to the Q. U. Adrilateral's inbox (CEO of GAMR) for any other information that has not been publicised but may be critically important
- [OPTIONAL] Break into the company's CRM to get some insider data on current contracts

SCENARIO

You have been enlisted into the Circle-land's cyber division. There is no forgiveness to what the Rectangles have done to your people twenty years ago. Two countries exchange provocative public statements as people on both sides fear another war is coming. You are working for the Division - an elite cyber warfare unit that specialises in Advanced Persistent Threats and covert operations. It is not the end of the world if your operations get found out, as Circle-land has some sharp-witted diplomats and a powerful military force to back you up.



Techniques

T 01

4 RISK

4 ROLL

Exploitation for Client Execution

PRE-REQUISITES

Psychological skills, Pre-existing vulnerability

PLAYFUL DESCRIPTION

"All it took was a torpedo to a thermal exhaust port to explode a Death Star."

Recon

Impact

CONSEQUENCES

Heavy: Being discovered

Medium: Technique not executed

Light: Technique not executed

SERIOUS DESCRIPTION

Adversaries can take advantage of certain vulnerabilities through targeted exploitation for the purpose of arbitrary code execution.

T 02

1 RISK

2 ROLL

Steal Web Session Cookie

PRE-REQUISITES

Pre-existing vulnerability

PLAYFUL DESCRIPTION

"No cookies for you!"

Recon

Impact

CONSEQUENCES

Heavy: Being discovered

Medium: Technique not executed

Light: Technique not executed

SERIOUS DESCRIPTION

An adversary may steal web application or service session cookies and use them to gain access web applications or Internet services as an authenticated user without needing credentials.

T 03

3 RISK

4 ROLL

Web Shell

PRE-REQUISITES

Pre-existing vulnerability

PLAYFUL DESCRIPTION

"I will take my shell with me anywhere on the web. Everything I have I carry with me after all!"

Recon

Impact

CONSEQUENCES

Heavy: Being discovered

Medium: Technique not executed

Light: Technique not executed

SERIOUS DESCRIPTION

Web shells may serve as Redundant Access or as a persistence mechanism in case an adversary's primary access methods are detected and removed.

T 04

1 RISK

3 ROLL

Credentials from Web Browsers

PRE-REQUISITES

Pre-existing vulnerability, Distracted/lazy user, Resource compromised, Exfiltration channel, OSINT/Preparation

PLAYFUL DESCRIPTION

"Browser wars - now in your file system!"

Recon

Impact

CONSEQUENCES

Heavy: Countermeasures taken by target

Medium: Being discovered

Light: Technique not executed

SERIOUS DESCRIPTION

Adversaries may acquire credentials from web browsers by reading files specific to the target browser

T 05

4 RISK

3 ROLL

Domain Fronting

PRE-REQUISITES

Psychological skills, Pre-existing vulnerability

PLAYFUL DESCRIPTION

"Just like the tracking of my AliExpress parcel!"

Recon

Impact

CONSEQUENCES

Heavy: Technique not executed

Medium: Technique not executed

Light: Technique not executed

SERIOUS DESCRIPTION

Domain fronting takes advantage of routing schemes in Content Delivery Networks (CDNs) and other services which host multiple domains to obfuscate the intended destination of HTTPS traffic or traffic tunnelled through HTTPS.

T 06

4 RISK

4 ROLL

Exfiltration Over Alternative Protocol

PRE-REQUISITES

Exfiltration channel

PLAYFUL DESCRIPTION

"It would be safer to just post USB drives at this point..."

Recon ●●●○○

Impact ●●●●○

CONSEQUENCES

Heavy: Being discovered

Medium: Technique not executed

Light: Technique not executed

SERIOUS DESCRIPTION

Data exfiltration is performed with a different protocol from the main command and control protocol or channel. The data is likely to be sent to an alternate network location from the main command and control server.

T 07

2 RISK

3 ROLL

Browser Extensions

PRE-REQUISITES

Distracted/lazy user

PLAYFUL DESCRIPTION

Download more RAM now as a handy browser extension! Enjoy the portability and performance

Recon ●●○○○

Impact ●●○○○

CONSEQUENCES

Heavy: Being discovered

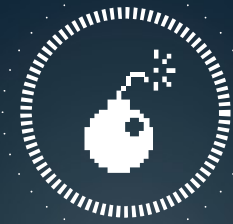
Medium: Target damaged in an unintended way

Light: Technique not executed

SERIOUS DESCRIPTION

Malicious extensions can be installed into a browser through malicious app store downloads masqurading as legitimate extensions, through socia engineering or by an adversary that has already compromised a system.

T 08



2 RISK

2 ROLL

Exploit Public-Facing Application

PRE-REQUISITES

Pre-existing vulnerability

PLAYFUL DESCRIPTION

"Next one in line to hack Pentagon."

Recon ●●○○○

Impact ●●●○○

CONSEQUENCES

Heavy: Being discovered

Medium: Technique not executed

Light: Technique not executed

SERIOUS DESCRIPTION

Adversaries can take advantage of a weakness in an Internet-facing computer system.

T 09

2 RISK

3 ROLL

Spearphishing Link

PRE-REQUISITES

OSINT/Preparation, Masquerading, Custom hosted website

PLAYFUL DESCRIPTION

"If there is a link then I must click it, right?"

Recon ●●●○○

Impact ●●●●○

CONSEQUENCES

Heavy: Attacker's infrastructure discovered

Medium: Being discovered

Light: Technique not executed

SERIOUS DESCRIPTION

This technique employs the use of links to download malware contained in email, instead of attaching malicious files to the email itself.

T 10

2 RISK

3 ROLL

Trusted Relationship

PRE-REQUISITES

Psychological skills

PLAYFUL DESCRIPTION

"Trust no one, not even your shelf."

Recon ●●●●○

Impact ●●●○○

CONSEQUENCES

Heavy: Technique not executed

Medium: Technique not executed

Light: Technique not executed

SERIOUS DESCRIPTION

Exploits an existing connection that may not be protected or receives less scrutiny than standard mechanisms of gaining access to a network.

T 11

2 RISK

3 ROLL

Drive-by Compromise

PRE-REQUISITES

OSINT/Preparation, Resource compromised

PLAYFUL DESCRIPTION

"I am just a little benign browser tab..."

Recon ●●●○○

Impact ●●●●○

CONSEQUENCES

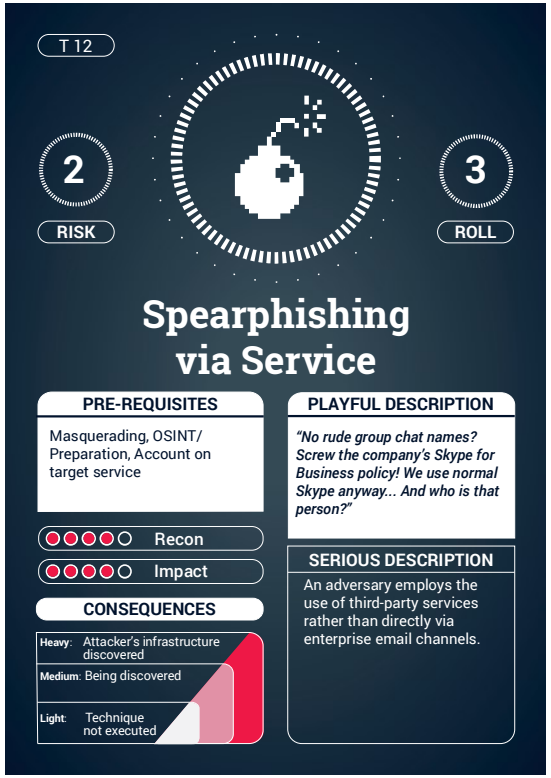
Heavy: Technique not executed

Medium: Technique not executed

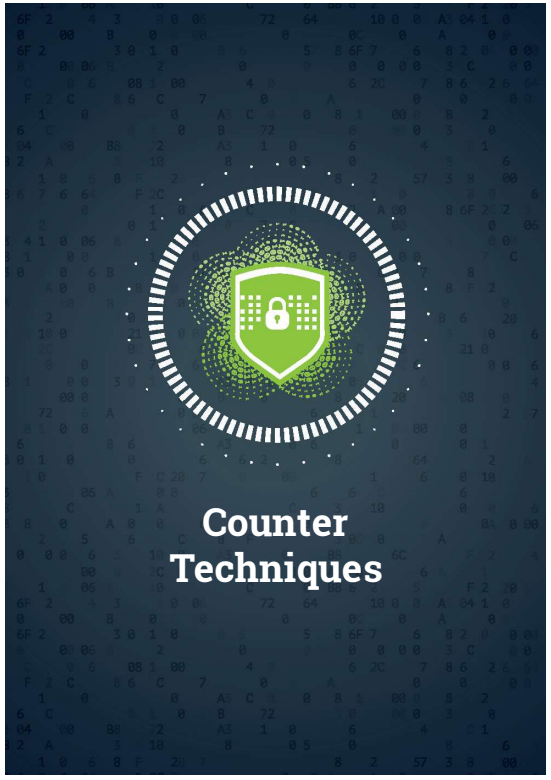
Light: Technique not executed

SERIOUS DESCRIPTION

An adversary gains access to a system through a user visiting a website over the normal course of browsing.


T 12
2
RISK
3
ROLL
Spearphishing via Service
PRE-REQUISITES
Masquerading, OSINT/ Preparation, Account on target service
PLAYFUL DESCRIPTION
"No rude group chat names? Screw the company's Skype for Business policy! We use normal Skype anyway... And who is that person?"
Recon
Impact
SERIOUS DESCRIPTION
An adversary employs the use of third-party services rather than directly via enterprise email channels.
CONSEQUENCES
Heavy: Attacker's infrastructure discovered
Medium: Being discovered
Light: Technique not executed

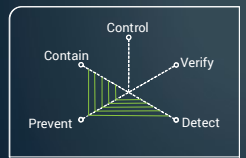

T 13
1
RISK
2
ROLL
Man in the Browser
PRE-REQUISITES
None
PLAYFUL DESCRIPTION
"I am not the FBI, but I am listening!"
Recon
Impact
SERIOUS DESCRIPTION
Adversaries can take advantage of security vulnerabilities and inherent functionality in browser software to change content, modify behaviour, and intercept information as part of various man in the browser techniques.
CONSEQUENCES
Heavy: Technique not executed
Medium: Technique not executed
Light: Technique not executed



Counter Techniques

C 01

Antivirus/ Antimalware



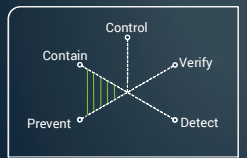
COUNTERS

- Command-Line Interface
- Spearphishing via Service

Use signatures or heuristics to detect malicious software.

C 02

Application Isolation and Sandboxing



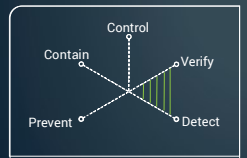
COUNTERS

- Drive-by Compromise
- Exploit Public-Facing Application
- Exploitation for Client Execution

Restrict execution of code to a virtual environment on or in transit to an endpoint system.

C 03

Audit



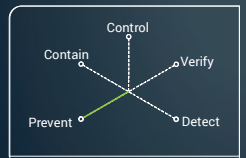
COUNTERS

- Browser Extensions

Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses.

C 04

Execution Prevention



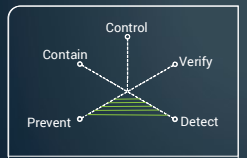
COUNTERS

- Browser Extensions

Block execution of code on a system through application control, and/or script blocking.

C 05

Exploit Protection



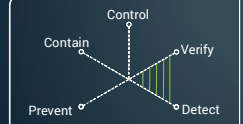
COUNTERS

- Drive-by Compromise
- Exploit Public-Facing Application
- Exploitation for Client Execution

Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring.

C 06

Filter Network Traffic



Your packets are going through me!

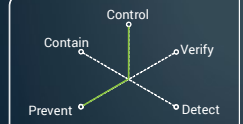
COUNTERS

- Exfiltration Over Alternative Protocol

Use network appliances to filter ingress or egress traffic and perform protocol-based filtering. Configure software on endpoints to filter network traffic.

C 07

Limit Software Installation



No, you cannot install Steam on our machines!

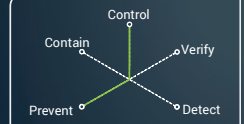
COUNTERS

- Browser Extensions

Block users or groups from installing unapproved software

C 08

Multi-factor Authentication



The numbers, Mason! What's the 5-digit code from the text message?

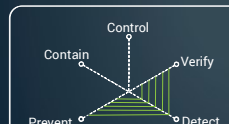
COUNTERS

- Steal Web Session Cookie

Use two or more pieces of evidence to authenticate to a system; such as username and password in addition to a token from a physical smart card or token generator.

C 09

Network Intrusion Prevention



Imposter, imposter!

COUNTERS

- Exfiltration Over Alternative Protocol

Use intrusion detection signatures to block traffic at network boundaries.

C 10

Network Segmentation

That's why it's called deFENCE, get it?

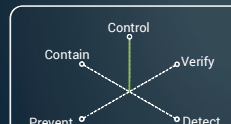
COUNTERS

- Exfiltration Over Alternative Protocol
- Exploit Public-Facing Application
- Trusted Relationship

Architect sections of the network to isolate critical systems, functions, or resources, such as physical and logical segmentation, DMZ, and VPC.

C 11

Password Policies



*hunter1... It shows as *******, right?*

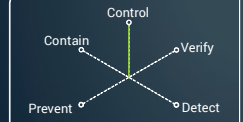
COUNTERS

- Credentials from Web Browsers

Set and enforce secure password policies for accounts.

C 12

Privileged Account Management



One account to rule them all!

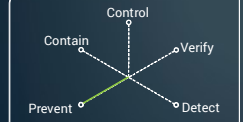
COUNTERS

- Exploit Public-Facing Application

Manage the creation, modification, use, and permissions associated to privileged accounts, including SYSTEM and root.

C 13

Restrict Web-Based Content



What do you mean I can't go on Facebook?

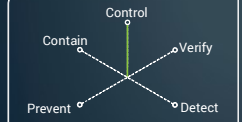
COUNTERS

- Spearphishing Link
- Spearphishing via Service
- Drive-by Compromise

Restrict use of certain websites, block downloads/attachments, block Javascript, restrict browser extensions, etc.

C 14

Software Configuration



Your cookies have gone missing. I hid them... in a very reliable place!

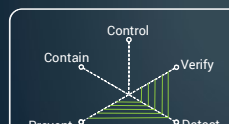
COUNTERS

- Steal Web Session Cookie

Implement configuration changes to software (other than the operating system) to mitigate security risks associated to how the software operates.

C 15

SSL/TLS Inspection



Say no to bleeding hearts!

COUNTERS

- Domain Fronting

Break and inspect SSL/TLS sessions to look at encrypted web traffic for adversary activity.

C 16

Update Software

Just why Windows updates pop up at the most inconvenient times?!

COUNTERS

- Drive-by Compromise
- Exploit Public-Facing Application

Perform regular software updates to mitigate exploitation risk.

C 17

User Account Control

Can you hear this sound?

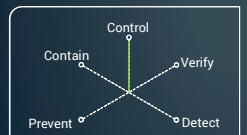
COUNTERS

- Trusted Relationship

Configure Windows User Account Control to mitigate risk of adversaries obtaining elevated process access.

C 18

User Account Management



COUNTERS

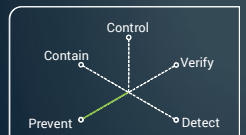
- Man in the Browser

How many Jo Bloggses does our organisation even have?

Manage the creation, modification, use, and permissions associated to user accounts.

C 19

User Training



COUNTERS

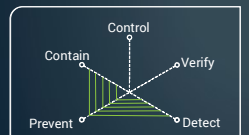
- Browser Extensions
- Man in the Browser
- Spearphishing Link
- Spearphishing via Service
- Steal Web Session Cookie

Wait, so I cannot help the Nigerian prince?

Train users to to be aware of access or manipulation attempts by an adversary to reduce the risk of successful spearphishing, social engineering, and other techniques that involve user interaction.

C 20

Vulnerability Scanning

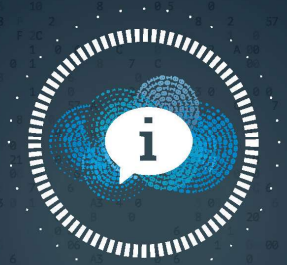


COUNTERS

- Exploit Public-Facing Application

There is no such thing as a bulletproof system, but we will surely try to make it such!

Vulnerability scanning is used to find potentially exploitable software vulnerabilities to remediate them.



Information

I 01

Public-facing website system information

DESCRIPTION	TRAIL
It's on an nginx Linux box. The website itself is running Django with Node.js frontend and Bootstrap as a css framework	Website

I 02

Admin console access

DESCRIPTION	TRAIL
This is webmaster's access to a user-friendly admin console that allows easy creation of new pages as well as management of what's already there, such as databases and images.	Website

I 03

Lowest privilege user access

DESCRIPTION	TRAIL
Access to the automatically generated user in the system that handles running automated website tasks.	Website

I 04

Windows user access (inside a VM)

DESCRIPTION	TRAIL
As all user spaces are in fact virtual machines, establishing access to one of them will allow you to get inside one of such machines. It's up to you what to do with this information.	Windows Active Directory

I 05

VM management access

DESCRIPTION	TRAIL
This is the console that is responsible for allocation of virtual machine user spaces.	Windows Active Directory

I 06

Windows Active directory admin access

DESCRIPTION	TRAIL
Access to the interface that allows to manage users - create, delete, view and modify.	Windows Active Directory

I 07

Access to node1

DESCRIPTION	TRAIL
node1 stores technical data. That is weapon and transport system plans, but the sensitivity level of stored information is up to Tier 2.	Intranet

I 08

Access to node2

DESCRIPTION	TRAIL
node2 stores administrative, HR and financial data with sensitivity level of stored information up to Tier 2.	Intranet

I 09

Access to node3

DESCRIPTION	TRAIL
Inode3 stores different types of data, but with the highest sensitivity - Tier 3.	Intranet

I 10

CEO's Twitter username

DESCRIPTION	TRAIL
He used his personal email to create his Twitter... How unsurprising.	Twitter

I 11

CEO's Twitter password

DESCRIPTION	TRAIL
Has CEO even heard of a password manager? Maybe. But definitely not for Twitter!	Twitter

I 12

Email platform information

DESCRIPTION	TRAIL
The company is running Office 365 Outlook on the cloud, which is externally hosted.	Email

I 13

CEO's email address

DESCRIPTION	TRAIL
This is his work email address: queadr1@gamr.org.rec. Fun fact, his first name is Quentin.	Email

I 14

CEO's email password

DESCRIPTION	TRAIL
That looks generated by a password manager. Too bad you've got access to the same generation algorithm.	Email

I 15

CEO's physical laptop access

DESCRIPTION	TRAIL
CEO's laptop. Well done for getting that! Now the question is, can you get access to what's inside?	Physical Domain

I 16

CEO's laptop access password

DESCRIPTION	TRAIL
The laptop has been protected by a PIN. The PIN itself is fairly short, so it can be easily brute forced, which is what you did to reveal a sequence of 4 digits.	Physical Domain

I 17

CRM software information

DESCRIPTION	TRAIL
The company is running Salesforce on the cloud, which is externally hosted	CRM software

I 18

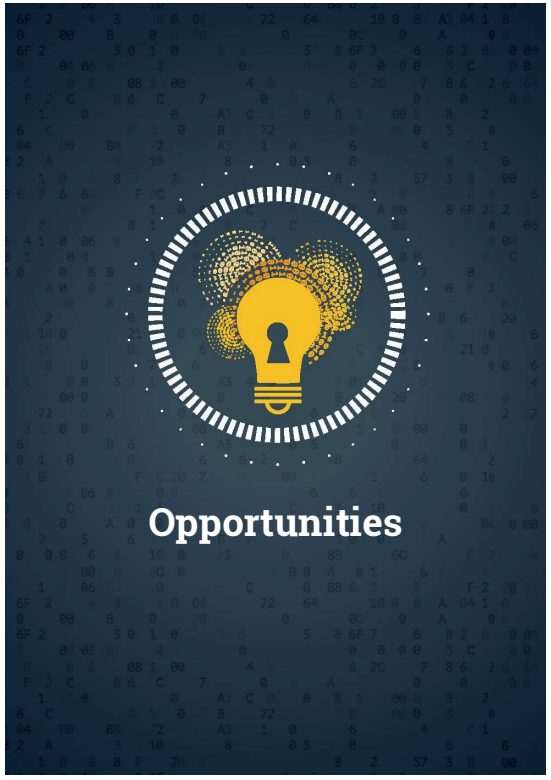
Details of one of the sales managers

DESCRIPTION	TRAIL
John Icegold is one of the sales team employees. John uses his work email to log in to company's Salesforce instance, so the only thing remaining to get access to his account is the password.	CRM software

I 20

Salesforce password

DESCRIPTION	TRAIL
The password is not automatically generated. It is the name of his wife followed by their marriage date. What a happy family!	CRM software



Opportunities

O 01

It works!

Use this card to help a struggling player or direct a player into a different route.

DESCRIPTION

Accidentally, you have navigated to a non-existent webpage on the website and got some system information due to an incorrectly configured server.

UNLOCKS

Public-facing website system information I 01

O 02

.../user/login

Use this card to help a struggling player or direct a player into a different route.

DESCRIPTION

By running a directory scan you have found a webpage that allows you to log in. After some fuzzing you have managed to log into the admin console using default credentials.

UNLOCKS

Admin console access I 02

O 03

/inetpub/wwwroot/

Use this card to help a struggling player or direct a player into a different route.

DESCRIPTION

After running some payloads on Metasploit you have gotten access into the **../uploads/** directory. Running whoami reveals that you are the automatically generated user, so next you will need to figure out how to give yourself more privileges.

UNLOCKS

Lowest privilege user access I 03

O 04

UntitledVM14

Use this card to help a struggling player or direct a player into a different route.

DESCRIPTION

By phishing a user, you have managed to get them to execute a reverse shell that has allowed you to establish a connection to their machine. Once you're in though, you quickly realise that you are running inside a virtual machine.

UNLOCKS

Windows user access (inside a VM) I 04

O 05

VBoxManage

Use this card to help a struggling player or direct a player into a different route.

DESCRIPTION

Using your skills (and I will leave it up to you, if you went via hardware or networking route) you manage to break out of the virtual machine that you got stuck in. Moreover you got to the very origins by discovering where these machines are generated.

UNLOCKS

VM management access I 05

O 06

Trust me, I am a security principal

Use this card to help a struggling player or direct a player into a different route.

DESCRIPTION

You have discovered a bat script that had a plaintext password contained in it and with some luck you got the Domain Admin privileges.

UNLOCKS

Windows Active directory admin access I 06

O 07

The good stuff (part 1)

Use this card to help a struggling player or direct a player into a different route.

DESCRIPTION

You have seen very mysterious 'node1', 'node2' and 'node3' mentioned all over this network. The exact contents, however were never clearly specified. You have spent hours on what you thought was just a rabbit hole, but eventually, bypassing another firewall has revealed something rather interesting!

UNLOCKS

Access to node1 I 07

O 08

The good stuff (part 2)

Use this card to help a struggling player or direct a player into a different route.

DESCRIPTION

This place surely has a lot of firewalls! Getting this far was not easy, but since you are here now, you get to browse the important information!

UNLOCKS

Access to node2 I 08

O 09

The good stuff (part 3)

Use this card to help a struggling player or direct a player into a different route.

DESCRIPTION

Bypassing yet another firewall you have hit a wall, this time an abstract one. This server seems to be slightly better protected than the other ones. But the better is the protection, the more important is whatever they are trying to protect, right? Many sleepless hours and cups of coffee later you have completely exhausted your options, until on a forgotten forum post you stumble upon a very curious proof of concept. You attempt it as a last resort and miraculously it has worked. You are in!

UNLOCKS

Access to node3 I 09

O 10

Chirp, chirp!

Use this card to help a struggling player or direct a player into a different route.

DESCRIPTION

CEO's personal email address was available in one of the data dumps that you have acquired on the dark web. Plus, you know they are an avid Twitter user... It is probably worth a try to get access to their Twitter!

UNLOCKS

CEO's Twitter username I 10

O 11

#BugBountyTips

Use this card to help a struggling player or direct a player into a different route.

DESCRIPTION

Using a mixture of information that CEO has tweeted about at different points in time you manage to guess the password to the CEO's Twitter account. Now quick, do what you need to do before he sees the new device alert on his inbox!

UNLOCKS

CEO's Twitter password I 11

O 12

Guinness MX record

Use this card to help a struggling player or direct a player into a different route.

DESCRIPTION

By getting one of the employees to reply to your phishing email from their corporate email address. This way you were able to track where this email came from. Now you have system information as well as a good idea about naming convention is used for those corporate email addresses.

UNLOCKS

- Email platform information I 12

O 13

You've got Mail!

Use this card to help a struggling player or direct a player into a different route

DESCRIPTION

Since you already have an email address belonging to Leigh Quadro, with the format of leiqua1 @gamr.org.rec, you try your best to guess Mr. Adrilateral's address. You succeed!

UNLOCKS

- CEO's email address I 13

O 14

In the name of the great Thunderbird!

Use this card to help a struggling player or direct a player into a different route.

DESCRIPTION

Unlike for his Twitter, this time the CEO appears to have generated a password using a password manager, as none of the dictionary words match. But do not panic, you can generate very similar passwords, so you are covered!

UNLOCKS

- CEO's email password I 14

O 15

I like trains

Use this card to help a struggling player or direct a player into a different route

DESCRIPTION

The CEO had to take a train to get to a summit that took place in Port Parallel. An urgent phone call causes him to leave the passenger area of the carriage for privacy, leaving his laptop unattended. You sat next to them. What a happy coincidence! Except that it was not a coincidence. You've got ten minutes to try and retrieve what you need.

UNLOCKS

- CEO's physical laptop access I 15

O 16

1337

Use this card to help a struggling player or direct a player into a different route.

DESCRIPTION

Currently you are sitting in the train next to Mr. Adrilateral's seat, while he went out to have an important call. You have access to his laptop and you notice it is protected by a pin. With luck on your side, you have managed to type in the correct one on the fifth try - 5555. That's not very secure, Mr. CEO!

UNLOCKS

- CEO's laptop access password I 16

O 17

Let me write that down!

Use this card to help a struggling player or direct a player into a different route.

DESCRIPTION

By sending yet another phishing email pretending to be a potential customer you managed to get a response. A closer inspection of the source code and format of the message revealed something familiar to you - this email has been sent from a CRM!

UNLOCKS

- CRM software information
- Details of one of the sales managers

O 18

Don’t let me write that down!

Use this card to help a struggling player or direct a player into a different route.

DESCRIPTION

Knowing the details of Mr. Icegold you manage to find their Facebook account, where you find a couple of noteworthy facts about him. He seems to willingly share information about many activities he has been up to with his wife. There is a photo of their skiing trip together, and here they tried to cook an ambitious meal together! Something lights up in your head - could it be?

UNLOCKS

Salesforce password

Appendix G

Techniques Survey

MITRE ATT&CK techniques survey

Start of Block: Default Question Block

Q58 **A survey on the use of computer attack techniques** In this study you will be presented with a list of cyber attack techniques, for each technique you will be asked to answer a series of questions. Please answer to the best of your knowledge. You will have the opportunity to share your knowledge about a particular technique.

The data that you provide will be used to populate a deck of cards in a hacking-themed board game, if you are interested in piloting this game please do not hesitate to contact us. You have the right to withdraw from this study immediately if you wish and not participate in the research. Alternatively if you wish to withdraw at a later date please inform the researchers named below. If you do not receive a satisfactory response please contact the Cranfield University Ethics Committee (CUREC) curec@cranfield.ac.uk. **Tatjana Sidorenko (tatjana.sidorenko@cranfield.ac.uk) Duncan Hodges (d.hodges@cranfield.ac.uk) Oliver Buckley (o.buckley@uea.ac.uk)** This survey will take about 15 minutes to complete. You may want to save your responses in a text file as a backup as you are going through the survey.

Page Break

Q60 In this survey you will be presented with a range of hacking techniques for which you will be asked to provide some insight on the use of techniques listed.

Please feel free to comment on the techniques, there will be space for you to do so throughout the survey. Feel free to also list concrete scenarios if this will help you to provide a more complete answer.

Q64 Please provide your email address to be entered into a prize draw for a chance to win a £50 or a £30 Amazon voucher or if you want to participate in the playtests. Alternatively, leave the field blank.

_____

Q61 Please select all that apply.

☐ I am interested in participating in the game playtests (email is required to contact you) (1)

☐ I have provided my email but I **do not** want to be entered into the prize draw (4)

Page Break

Q62 **Informed consent form**

1. I confirm that I have been informed about this research project and I agree to take part.
2. I understand that all personal information I provide will be treated with confidence and my name will not be used in any report, publication or presentation.

3. I understand that I can withdraw from this project at any stage by informing a member of the research team, for whom contact details have been provided. I understand that if I have any questions about the research and I cannot contact the researchers listed I can contact the Cranfield University Ethics Committee, for which the details have been provided below. I also understand that I can withdraw my data any time after the study.

Title of the project:	Agent-Based Modelling for Offensive Actors in Cyberspace
Name of the researcher:	Tatjana Sidorenko, Duncan Hodges
Researcher's contact details:	tatjana.sidorenko@cranfield.ac.uk d.hodges@cranfield.ac.uk
Cranfield University Ethics Committee (CUREC)	curec@cranfield.ac.uk

Data integrity

I understand that the data I provide will only be accessed by the named researchers for the purpose of research only.

Data storage

- Responses to the survey will be securely stored on encrypted hard drives. These text files will be securely deleted as soon as they are no longer required.

Anonymised records will be created, by removing or replacing identifiers such as name, age and location. These anonymised records may be quoted from, in support of findings (e.g. in journal articles, conference papers).

- Analytical software will be used to aggregate the results of the research and every reasonable step will be taken to anonymise the data.

Please select both choices to proceed.

☐ I understand that the aggregated data will be published in support of the research findings. (1)

☐ I confirm that I have read and understand the information provided on this form and give my consent to taking part in this research. (4)

Page Break

Q1 Please select one or more of the following technique categories that you are familiar with

- [ ] **Web** - Any technique related to the Web, servers and websites, e.g. defacement. (1)
- [ ] **Code execution** - Any technique that involves either local or remote code execution, e.g. file deletion. (2)
- [ ] **Priviledge escalation and credentials management** - Any technique that involves using credentials, handling user passwords and escalating priviledges, e.g. account manipulation. (3)
- [ ] **Network** - Any attack technique that involves the network, e.g. port knocking. (4)
- [ ] **Physical** - Any technique that requires physical access to a machine, e.g. physically inserting a USB pen drive into a machine. (5)
- [ ] **Low-level** - firmware level techniques, or techniques that involve manipulations with binaries or memory, e.g. system firmware. (6)
- [ ] **Social Engineering and OSINT** - Techniques that involve gathering information and manipulating users, e.g. spearphishing link. (7)
- [ ] **OS-level or OS-specific** - Includes the techniques that are executed on the level of the operating system, e.g. bootkit, or techniques that are specific to a concrete operating system, e.g. modify registry - specific to only Windows machines. (8)
- [ ] **Exploit** - Any technique that involves taking advantage of a vulnerability, e.g. Office application startup. (9)
- [ ] **Recon** - Any technique carried out for the purpose of information gathering, e.g. audio capture. (10)
- [ ] **Keeping a low profile** - Any attack technique that prioritises disguising information, action or traffic from anti-viruses or intrusion detection systems, e.g. indicator blocking. (11)

Display This Question:

If Please select one or more of the following technique categories that you are familiar with = Web - Any technique related to the Web, servers and websites, e.g. defacement.

Q2
You have selected:

${Q1/ChoiceDescription/1}

If you had a chance to select a perfect toolkit for compromising the online security of an organisation, what techniques would you select? (Select all that apply). If you have already filled in the same technique in a different category then you do not need to fill it out again. If you are not sure what a technique is referring to, please check the following: https://attack.mitre.org/

- [ ] Browser Extensions (1)
- [ ] Credentials from Web Browsers (2)
- [ ] Defacement (3)
- [ ] Domain Fronting (4)
- [ ] Domain Generation Algorithms (5)
- [ ] Drive-by Compromise (6)
- [ ] Exfiltration Over Alternative Protocol (7)
- [ ] Exploit Public-Facing Application (8)
- [ ] Exploitation for Client Execution (9)
- [ ] Man in the Browser (10)
- [ ] Shared Webroot (11)
- [ ] Spearphishing Link (12)
- [ ] Spearphishing via Service (13)

- [ ] Steal Web Session Cookie (14)
- [ ] Trusted Relationship (15)
- [ ] Web Service (16)
- [ ] Web Shell (17)

Page Break

Display This Question:

If Please select one or more of the following technique categories that you are familiar with = Code execution - Any technique that involves either local or remote code execution, e.g. file deletion.

Q3
You have selected:

${Q1/ChoiceDescription/2}

If you had a chance to select a perfect toolkit for compromising the online security of an organisation, what techniques would you select? (Select all that apply). If you have already filled in the same technique in a different category then you do not need to fill it out again. If you are not sure what a technique is referring to, please check the following: https://attack.mitre.org/

- [ ] .bash_profile and .bashrc (1)
- [ ] AppCert DLLs (2)
- [ ] AppInit DLLs (3)
- [ ] AppleScript (4)
- [ ] Application Deployment Software (5)
- [ ] Application Shimming (6)
- [ ] Authentication Package (7)
- [ ] Automated Collection (8)
- [ ] Automated Exfiltration (9)
- [ ] Bash History (10)
- [ ] BITS Jobs (11)
- [ ] Browser Extensions (12)
- [ ] Change Default File Association (13)

- [ ] CMSTP (14)
- [ ] Command-Line Interface (15)
- [ ] Communication Through Removable Media (16)
- [ ] Compile After Delivery (17)
- [ ] Compiled HTML File (18)
- [ ] Component Firmware (19)
- [ ] Component Object Model and Distributed COM (20)
- [ ] Control Panel Items (21)
- [ ] Custom Cryptographic Protocol (22)
- [ ] Data Destruction (23)
- [ ] Data Encrypted for Impact (24)
- [ ] Deobfuscate/Decode Files or Information (25)
- [ ] Disabling Security Tools (26)
- [ ] Disk Content Wipe (27)
- [ ] Disk Structure Wipe (28)
- [ ] DLL Search Order Hijacking (29)
- [ ] Dylib Hijacking (30)
- [ ] Dynamic Data Exchange (31)

- [ ] Emond (32)
- [ ] Execution through API (33)
- [ ] Execution through Module Load (34)
- [ ] Exploitation for Client Execution (35)
- [ ] File Deletion (36)
- [ ] File System Logical Offsets (37)
- [ ] File System Permissions Weakness (38)
- [ ] Firmware Corruption (39)
- [ ] Gatekeeper Bypass (40)
- [ ] Hidden Window (41)
- [ ] Hooking (42)
- [ ] Image File Execution Options Injection (43)
- [ ] Indirect Command Execution (44)
- [ ] Inhibit System Recovery (45)
- [ ] InstallUtil (46)
- [ ] Kernel Modules and Extensions (47)
- [ ] Launch Agent (48)
- [ ] Launch Daemon (49)

- [ ] Launchctl (50)
- [ ] Local Job Scheduling (51)
- [ ] Login Item (52)
- [ ] Logon Scripts (53)
- [ ] LSASS Driver (54)
- [ ] Modify Existing Service (55)
- [ ] Mshta (56)
- [ ] Netsh Helper DLL (57)
- [ ] Network Share Connection Removal (58)
- [ ] New Service (59)
- [ ] Office Application Startup (60)
- [ ] Path Interception (61)
- [ ] Plist Modification (62)
- [ ] Port Monitors (63)
- [ ] PowerShell (64)
- [ ] PowerShell Profile (65)
- [ ] Rc.common (66)
- [ ] Re-opened Applications (67)

- [ ] Registry Run Keys / Startup Folder (68)
- [ ] Regsvcs/Regasm (69)
- [ ] Regsvr32 (70)
- [ ] Replication Through Removable Media (71)
- [ ] Rootkit (72)
- [ ] Rundll32 (73)
- [ ] Scheduled Transfer (74)
- [ ] Screensaver (75)
- [ ] Scripting (76)
- [ ] Security Support Provider (77)
- [ ] Server Software Component (78)
- [ ] Service Execution (79)
- [ ] Service Registry Permissions Weakness (80)
- [ ] Setuid and Setgid (81)
- [ ] Shared Webroot (82)
- [ ] Shortcut Modification (83)
- [ ] Signed Binary Proxy Execution (84)
- [ ] Signed Script Proxy Execution (85)

- [ ] SIP and Trust Provider Hijacking (86)
- [ ] Source (87)
- [ ] Space after Filename (88)
- [ ] Spearphishing Attachment (89)
- [ ] Spearphishing Link (90)
- [ ] Spearphishing via Service (91)
- [ ] Startup Items (92)
- [ ] Stored Data Manipulation (93)
- [ ] System Firmware (94)
- [ ] System Shutdown/Reboot (95)
- [ ] Systemd Service (96)
- [ ] Taint Shared Content (97)
- [ ] Template Injection (98)
- [ ] Third-party Software (99)
- [ ] Time Providers (100)
- [ ] Trap (101)
- [ ] Trusted Developer Utilities (102)
- [ ] User Execution (103)

- [ ] Video Capture (104)
- [ ] Web Shell (105)
- [ ] Windows Management Instrumentation (106)
- [ ] Windows Management Instrumentation Event Subscription (107)
- [ ] Windows Remote Management (108)
- [ ] XSL Script Processing (109)

Page Break

Display This Question:

If Please select one or more of the following technique categories that you are familiar with = Priviledge escalation and credentials management - Any technique that involves using credentials, handling user passwords and escalating priviledges, e.g. account manipulation.

Q4
You have selected:

${Q1/ChoiceDescription/3}

If you had a chance to select a perfect toolkit for compromising the online security of an organisation, what techniques would you select? (Select all that apply). If you have already filled in the same technique in a different category then you do not need to fill it out again. If you are not sure what a technique is referring to, please check the following: https://attack.mitre.org/

- [ ] Access Token Manipulation (1)
- [ ] Accessibility Features (2)
- [ ] Account Manipulation (3)
- [ ] AppCert DLLs (4)
- [ ] AppInit DLLs (5)
- [ ] Application Shimming (6)
- [ ] Brute Force (7)
- [ ] Bypass User Account Control (8)
- [ ] CMSTP (9)
- [ ] Command-Line Interface (10)
- [ ] Credential Dumping (11)
- [ ] Credentials from Web Browsers (12)
- [ ] Credentials in Files (13)

- [ ] Credentials in Registry (14)
- [ ] DCShadow (15)
- [ ] DLL Search Order Hijacking (16)
- [ ] Dylib Hijacking (17)
- [ ] Elevated Execution with Prompt (18)
- [ ] Emond (19)
- [ ] Exploitation for Credential Access (20)
- [ ] Exploitation for Privilege Escalation (21)
- [ ] Extra Window Memory Injection (22)
- [ ] File and Directory Permissions Modification (23)
- [ ] File System Permissions Weakness (24)
- [ ] Forced Authentication (25)
- [ ] Graphical User Interface (26)
- [ ] Group Policy Modification (27)
- [ ] Hidden Users (28)
- [ ] Hooking (29)
- [ ] Image File Execution Options Injection (30)
- [ ] Input Capture (31)

- [ ] Input Prompt (32)
- [ ] Install Root Certificate (33)
- [ ] Kerberoasting (34)
- [ ] Keychain (35)
- [ ] Launch Daemon (36)
- [ ] Launchctl (37)
- [ ] Logon Scripts (38)
- [ ] Mshta (39)
- [ ] New Service (40)
- [ ] Parent PID Spoofing (41)
- [ ] Pass the Hash (42)
- [ ] Pass the Ticket (43)
- [ ] Password Policy Discovery (44)
- [ ] Path Interception (45)
- [ ] Permission Groups Discovery (46)
- [ ] Plist Modification (47)
- [ ] Port Monitors (48)
- [ ] PowerShell Profile (49)

- [ ] Private Keys (50)
- [ ] Process Injection (51)
- [ ] Regsvcs/Regasm (52)
- [ ] Remote Services (53)
- [ ] Scheduled Task (54)
- [ ] Securityd Memory (55)
- [ ] Service Execution (56)
- [ ] Service Registry Permissions Weakness (57)
- [ ] Setuid and Setgid (58)
- [ ] SID-History Injection (59)
- [ ] Signed Binary Proxy Execution (60)
- [ ] Signed Script Proxy Execution (61)
- [ ] Startup Items (62)
- [ ] Steal Web Session Cookie (63)
- [ ] Sudo (64)
- [ ] Sudo Caching (65)
- [ ] System Owner/User Discovery (66)
- [ ] Trusted Developer Utilities (67)

- [ ] Two-Factor Authentication Interception (68)
- [ ] Valid Accounts (69)
- [ ] Web Shell (70)
- [ ] Windows Remote Management (71)

Page Break

Display This Question:

If Please select one or more of the following technique categories that you are familiar with = Network - Any attack technique that involves the network, e.g. port knocking.

Q5
You have selected:

${Q1/ChoiceDescription/4}

If you had a chance to select a perfect toolkit for compromising the online security of an organisation, what techniques would you select? (Select all that apply). If you have already filled in the same technique in a different category then you do not need to fill it out again. If you are not sure what a technique is referring to, please check the following: https://attack.mitre.org/

- [ ] Account Access Removal (1)
- [ ] AppleScript (2)
- [ ] Application Deployment Software (3)
- [ ] BITS Jobs (4)
- [ ] Commonly Used Port (5)
- [ ] Component Object Model and Distributed COM (6)
- [ ] Connection Proxy (7)
- [ ] Create Account (8)
- [ ] Custom Command and Control Protocol (9)
- [ ] Custom Cryptographic Protocol (10)
- [ ] Data Destruction (11)
- [ ] Data Encoding (12)
- [ ] Data Encrypted for Impact (13)

- [ ] Data from Network Shared Drive (14)
- [ ] Data Staged (15)
- [ ] Data Transfer Size Limits (16)
- [ ] Defacement (17)
- [ ] Domain Fronting (18)
- [ ] Domain Generation Algorithms (19)
- [ ] Email Collection (20)
- [ ] Endpoint Denial of Service (21)
- [ ] Execution Guardrails (22)
- [ ] Exfiltration Over Alternative Protocol (23)
- [ ] Exfiltration Over Command and Control Channel (24)
- [ ] Exfiltration Over Other Network Medium (25)
- [ ] Exploitation for Credential Access (26)
- [ ] Exploitation of Remote Services (27)
- [ ] External Remote Services (28)
- [ ] Fallback Channels (29)
- [ ] Forced Authentication (30)
- [ ] LLMNR/NBT-NS Poisoning and Relay (31)

- [ ] Multi-hop Proxy (32)
- [ ] Multi-Stage Channels (33)
- [ ] Multiband Communication (34)
- [ ] Multilayer Encryption (35)
- [ ] Network Denial of Service (36)
- [ ] Network Service Scanning (37)
- [ ] Network Share Discovery (38)
- [ ] Network Sniffing (39)
- [ ] Port Knocking (40)
- [ ] Redundant Access (41)
- [ ] Remote Access Tools (42)
- [ ] Remote Desktop Protocol (43)
- [ ] Remote File Copy (44)
- [ ] Remote System Discovery (45)
- [ ] Spearphishing Attachment (46)
- [ ] SSH Hijacking (47)
- [ ] Standard Application Layer Protocol (48)
- [ ] Standard Non-Application Layer Protocol (49)

- [ ] System Network Configuration Discovery (50)
- [ ] System Network Connections Discovery (51)
- [ ] Taint Shared Content (52)
- [ ] Third-party Software (53)
- [ ] Transmitted Data Manipulation (54)
- [ ] Trusted Relationship (55)
- [ ] Uncommonly Used Port (56)
- [ ] Windows Admin Shares (57)
- [ ] Windows Remote Management (58)

Page Break

Display This Question:

If Please select one or more of the following technique categories that you are familiar with = Physical - Any technique that requires physical access to a machine, e.g. physically inserting a USB pen drive into a machine.

Q6
You have selected:

${Q1/ChoiceDescription/5}

If you had a chance to select a perfect toolkit for compromising the online security of an organisation, what techniques would you select? (Select all that apply). If you have already filled in the same technique in a different category then you do not need to fill it out again. If you are not sure what a technique is referring to, please check the following: https://attack.mitre.org/

- [ ] Communication Through Removable Media (1)
- [ ] Exploitation for Credential Access (2)
- [ ] Hardware Additions (3)
- [ ] Peripheral Device Discovery (4)
- [ ] Replication Through Removable Media (5)
- [ ] Supply Chain Compromise (6)
- [ ] Trusted Relationship (7)
- [ ] Two-Factor Authentication Interception (8)

Page Break

Display This Question:

If Please select one or more of the following technique categories that you are familiar with = Low-level - firmware level techniques, or techniques that involve manipulations with binaries or memory, e.g. system firmware.

Q7
You have selected:

${Q1/ChoiceDescription/6}

If you had a chance to select a perfect toolkit for compromising the online security of an organisation, what techniques would you select? (Select all that apply). If you have already filled in the same technique in a different category then you do not need to fill it out again. If you are not sure what a technique is referring to, please check the following: https://attack.mitre.org/

- [ ] Audio Capture (1)
- [ ] Component Firmware (2)
- [ ] Data from Removable Media (3)
- [ ] Disk Content Wipe (4)
- [ ] Disk Structure Wipe (5)
- [ ] Exfiltration Over Physical Medium (6)
- [ ] Exploitation for Credential Access (7)
- [ ] Firmware Corruption (8)
- [ ] Hardware Additions (9)
- [ ] LC_MAIN Hijacking (10)
- [ ] Masquerading (11)
- [ ] Peripheral Device Discovery (12)
- [ ] Process Injection (13)

- [ ] Runtime Data Manipulation (14)
- [ ] System Firmware (15)
- [ ] Two-Factor Authentication Interception (16)
- [ ] Video Capture (17)

Page Break

Display This Question:

If Please select one or more of the following technique categories that you are familiar with = Social Engineering and OSINT - Techniques that involve gathering information and manipulating users, e.g. spearphishing link.

Q8
You have selected:

${Q1/ChoiceDescription/7}

If you had a chance to select a perfect toolkit for compromising the online security of an organisation, what techniques would you select? (Select all that apply). If you have already filled in the same technique in a different category then you do not need to fill it out again. If you are not sure what a technique is referring to, please check the following: https://attack.mitre.org/

- [ ] Browser Bookmark Discovery (1)
- [ ] Browser Extensions (2)
- [ ] Graphical User Interface (3)
- [ ] Input Prompt (4)
- [ ] Internal Spearphishing (5)
- [ ] Runtime Data Manipulation (6)
- [ ] Spearphishing Attachment (7)
- [ ] Spearphishing Link (8)
- [ ] Spearphishing via Service (9)
- [ ] Supply Chain Compromise (10)
- [ ] System Time Discovery (11)
- [ ] Trusted Relationship (12)
- [ ] Valid Accounts (13)

Page Break

Display This Question:

If Please select one or more of the following technique categories that you are familiar with = OS-level or OS-specific - Includes the techniques that are executed on the level of the operating system, e.g. bootkit, or techniques that are specific to a concrete operating system, e.g. modify registry - specific to only Windows machines.

Q9
You have selected:

${Q1/ChoiceDescription/8}

If you had a chance to select a perfect toolkit for compromising the online security of an organisation, what techniques would you select? (Select all that apply). If you have already filled in the same technique in a different category then you do not need to fill it out again. If you are not sure what a technique is referring to, please check the following: https://attack.mitre.org/

- [ ] .bash_profile and .bashrc (1)
- [ ] Accessibility Features (2)
- [ ] Account Access Removal (3)
- [ ] AppCert DLLs (4)
- [ ] AppInit DLLs (5)
- [ ] AppleScript (6)
- [ ] Application Shimming (7)
- [ ] Application Window Discovery (8)
- [ ] Authentication Package (9)
- [ ] Bash History (10)
- [ ] Binary Padding (11)
- [ ] Bootkit (12)
- [ ] Bypass User Account Control (13)

- [ ] Change Default File Association (14)
- [ ] Clear Command History (15)
- [ ] Clipboard Data (16)
- [ ] Compile After Delivery (17)
- [ ] Compiled HTML File (18)
- [ ] Component Object Model Hijacking (19)
- [ ] Control Panel Items (20)
- [ ] Create Account (21)
- [ ] Credentials in Registry (22)
- [ ] Custom Cryptographic Protocol (23)
- [ ] Data Destruction (24)
- [ ] Data Encrypted for Impact (25)
- [ ] DCShadow (26)
- [ ] DLL Search Order Hijacking (27)
- [ ] DLL Side-Loading (28)
- [ ] Domain Trust Discovery (29)
- [ ] Dylib Hijacking (30)
- [ ] Dynamic Data Exchange (31)

- [ ] Elevated Execution with Prompt (32)
- [ ] Emond (33)
- [ ] Execution through API (34)
- [ ] Execution through Module Load (35)
- [ ] Exploitation for Credential Access (36)
- [ ] Extra Window Memory Injection (37)
- [ ] File System Logical Offsets (38)
- [ ] Forced Authentication (39)
- [ ] Gatekeeper Bypass (40)
- [ ] Graphical User Interface (41)
- [ ] Hidden Files and Directories (42)
- [ ] Hidden Users (43)
- [ ] Hidden Window (44)
- [ ] HISTCONTROL (45)
- [ ] Hooking (46)
- [ ] Hypervisor (47)
- [ ] Image File Execution Options Injection (48)
- [ ] Indicator Blocking (49)

- [ ] Indirect Command Execution (50)
- [ ] InstallUtil (51)
- [ ] Kernel Modules and Extensions (52)
- [ ] Keychain (53)
- [ ] Launch Agent (54)
- [ ] Launch Daemon (55)
- [ ] Launchctl (56)
- [ ] LC_LOAD_DYLIB Addition (57)
- [ ] LLMNR/NBT-NS Poisoning and Relay (58)
- [ ] Local Job Scheduling (59)
- [ ] Login Item (60)
- [ ] LSASS Driver (61)
- [ ] Modify Existing Service (62)
- [ ] Modify Registry (63)
- [ ] Netsh Helper DLL (64)
- [ ] Network Share Connection Removal (65)
- [ ] New Service (66)
- [ ] NTFS File Attributes (67)

- [ ] Obfuscated Files or Information (68)
- [ ] Password Filter DLL (69)
- [ ] Path Interception (70)
- [ ] Plist Modification (71)
- [ ] Port Knocking (72)
- [ ] Port Monitors (73)
- [ ] PowerShell (74)
- [ ] PowerShell Profile (75)
- [ ] Process Doppelgänging (76)
- [ ] Query Registry (77)
- [ ] Rc.common (78)
- [ ] Re-opened Applications (79)
- [ ] Registry Run Keys / Startup Folder (80)
- [ ] Regsvcs/Regasm (81)
- [ ] Regsvr32 (82)
- [ ] Resource Hijacking (83)
- [ ] Rundll32 (84)
- [ ] Screen Capture (85)

- [ ] Screensaver (86)
- [ ] Security Support Provider (87)
- [ ] Securityd Memory (88)
- [ ] Server Software Component (89)
- [ ] Service Execution (90)
- [ ] Service Registry Permissions Weakness (91)
- [ ] Service Stop (92)
- [ ] Setuid and Setgid (93)
- [ ] Shortcut Modification (94)
- [ ] SID-History Injection (95)
- [ ] SIP and Trust Provider Hijacking (96)
- [ ] Source (97)
- [ ] Startup Items (98)
- [ ] Stored Data Manipulation (99)
- [ ] System Firmware (100)
- [ ] System Information Discovery (101)
- [ ] System Service Discovery (102)
- [ ] Time Providers (103)

- [ ] Trusted Developer Utilities (104)
- [ ] Virtualization/Sandbox Evasion (105)
- [ ] Windows Admin Shares (106)
- [ ] Windows Management Instrumentation (107)
- [ ] Windows Management Instrumentation Event Subscription (108)
- [ ] Windows Remote Management (109)

Page Break

Display This Question:

If Please select one or more of the following technique categories that you are familiar with = Exploit - Any technique that involves taking advantage of a vulnerability, e.g. Office application startup.

Q10
You have selected:

${Q1/ChoiceDescription/9}

If you had a chance to select a perfect toolkit for compromising the online security of an organisation, what techniques would you select? (Select all that apply). If you have already filled in the same technique in a different category then you do not need to fill it out again. If you are not sure what a technique is referring to, please check the following: https://attack.mitre.org/

- [ ] Application Deployment Software (1)
- [ ] Application Shimming (2)
- [ ] Audio Capture (3)
- [ ] Authentication Package (4)
- [ ] Bootkit (5)
- [ ] Communication Through Removable Media (6)
- [ ] Compile After Delivery (7)
- [ ] DLL Side-Loading (8)
- [ ] Domain Fronting (9)
- [ ] Exploitation for Client Execution (10)
- [ ] Exploitation for Credential Access (11)
- [ ] Exploitation for Defense Evasion (12)
- [ ] Exploitation for Privilege Escalation (13)

- [ ] Exploitation of Remote Services (14)
- [ ] Hidden Files and Directories (15)
- [ ] Hypervisor (16)
- [ ] Indicator Removal from Tools (17)
- [ ] LC_LOAD_DYLIB Addition (18)
- [ ] Office Application Startup (19)
- [ ] Path Interception (20)
- [ ] Server Software Component (21)
- [ ] Signed Script Proxy Execution (22)
- [ ] Third-party Software (23)
- [ ] Trap (24)

Page Break

Display This Question:

If Please select one or more of the following technique categories that you are familiar with = Recon - Any technique carried out for the purpose of information gathering, e.g. audio capture.

Q11
You have selected:

${Q1/ChoiceDescription/10}

If you had a chance to select a perfect toolkit for compromising the online security of an organisation, what techniques would you select? (Select all that apply). If you have already filled in the same technique in a different category then you do not need to fill it out again. If you are not sure what a technique is referring to, please check the following: https://attack.mitre.org/

- [ ] Account Manipulation (1)
- [ ] Application Window Discovery (2)
- [ ] Audio Capture (3)
- [ ] Automated Exfiltration (4)
- [ ] Bash History (5)
- [ ] Browser Bookmark Discovery (6)
- [ ] Clear Command History (7)
- [ ] Credentials from Web Browsers (8)
- [ ] Credentials in Files (9)
- [ ] Credentials in Registry (10)
- [ ] Data from Information Repositories (11)
- [ ] Data from Local System (12)
- [ ] Data from Network Shared Drive (13)

- [ ] Data from Removable Media (14)
- [ ] Domain Trust Discovery (15)
- [ ] Email Collection (16)
- [ ] File and Directory Discovery (17)
- [ ] Network Share Discovery (18)
- [ ] Peripheral Device Discovery (19)
- [ ] Permission Groups Discovery (20)
- [ ] Process Discovery (21)
- [ ] Query Registry (22)
- [ ] Remote System Discovery (23)
- [ ] Screen Capture (24)
- [ ] Security Software Discovery (25)
- [ ] Software Discovery (26)
- [ ] System Information Discovery (27)
- [ ] System Network Configuration Discovery (28)
- [ ] System Network Connections Discovery (29)
- [ ] System Owner/User Discovery (30)
- [ ] System Service Discovery (31)

- [ ] System Time Discovery (32)
- [ ] Windows Management Instrumentation (33)

Page Break

Display This Question:

If Please select one or more of the following technique categories that you are familiar with = Keeping a low profile - Any attack technique that prioritises disguising information, action or traffic from anti-viruses or intrusion detection systems, e.g. indicator blocking.

Q12
You have selected:

${Q1/ChoiceDescription/11}

If you had a chance to select a perfect toolkit for compromising the online security of an organisation, what techniques would you select? (Select all that apply). If you have already filled in the same technique in a different category then you do not need to fill it out again. If you are not sure what a technique is referring to, please check the following: https://attack.mitre.org/

- [ ] Binary Padding (1)
- [ ] Code Signing (2)
- [ ] Data Compressed (3)
- [ ] Data Encoding (4)
- [ ] Data Encrypted (5)
- [ ] Data Obfuscation (6)
- [ ] Data Transfer Size Limits (7)
- [ ] Execution Guardrails (8)
- [ ] Exfiltration Over Alternative Protocol (9)
- [ ] File Deletion (10)
- [ ] Hidden Window (11)
- [ ] HISTCONTROL (12)
- [ ] Indicator Blocking (13)

- [ ] Indicator Removal from Tools (14)
- [ ] Indicator Removal on Host (15)
- [ ] Masquerading (16)
- [ ] Obfuscated Files or Information (17)
- [ ] Parent PID Spoofing (18)
- [ ] Process Doppelgänging (19)
- [ ] Process Injection (20)
- [ ] Rootkit (21)
- [ ] Scheduled Transfer (22)
- [ ] Software Packing (23)
- [ ] Standard Application Layer Protocol (24)
- [ ] Standard Cryptographic Protocol (25)
- [ ] Template Injection (26)
- [ ] Timestomp (27)
- [ ] Transmitted Data Manipulation (28)
- [ ] Virtualization/Sandbox Evasion (29)
- [ ] Web Service (30)

Page Break

Start of Block: Per technique I

Q19
You have selected ${lm://Field/1}. Please select a statement that best applies to this technique.

	No impact on the target organisation/individual (1)	Little impact on the target organisation/individual (2)	Some impact on the target organisation/individual (3)	Significant impact on the target organisation/individual (4)	Critical impact on the target organisation/individual (5)	Not applicable (6)
Impact (1)	○	○	○	○	○	○

Q21
You have selected ${lm://Field/1}. Please select a statement that best applies to this technique.

	The technique provides no information about the organisation/individual (1)	The technique provides little information about the organisation/individual (2)	The technique provides some useful information about the organisation/individual (3)	The technique provides more useful information about the organisation/individual (4)	The technique provides a lot of information about the organisation/individual (5)	Not applicable (6)
Recon (1)	○	○	○	○	○	○

Q23
You have selected ${lm://Field/1}.

What would you consider to be an essential list of **pre-requisites** for this technique? (e.g. an SQL editor, internet connection and a form vulnerable to SQL injection) Feel free to use any specific examples from your own experience if you feel that it would benefit the description.

_____

_____

_____

_____

_____

Q27
You have selected ${lm://Field/1}.

What, if any, would be potential **consequences** if the technique **fails to execute**? (e.g. no consequence for a failed SQL injection) Feel free to use any specific examples from your own experience if you feel that it would benefit the description.

_____

_____

_____

_____

_____

End of Block: Per technique I

Appendix H

Individual differences Questionnaire

Risk perception study

Start of Block: Informed Consent

Q1
Risk Perception Study

Welcome to the research study!
To complement your game play data, we are running a survey to help us understand how you perceive risk. Each person is different and what may seem very risky to one might be a regular action for another. The game, for which this survey is ran accounts for different cyber attacker types, however it does not account for individual perception of risk. Your email address will be used as an identifier to connect your survey data to your gameplay data, therefore make sure it is the same address that you are using to participate in the games. This address will not be used for anything else. Survey results will not be used for anything apart from what has been outlined above and will be stored on an encrypted hard drive and on University's network. You have the right to withdraw from this study immediately if you wish and not participate in the research. Alternatively, if you wish to withdraw at a later date please contact **Tatjana Sidorenko (tatjana.sidorenko@cranfield.ac.uk)** or **Duncan Hodges (d.hodges@cranfield.ac.uk)**. If you do not receive a satisfactory response please contact the **Cranfield University Ethics Committee (CUREC) curec@cranfield.ac.uk**.
By clicking the button below, you acknowledge:

Your participation in the study is voluntary.You are 18 years of age.You are aware that you may choose to terminate your participation at any time for any reason.

- ○ I consent, begin the study (1)
- ○ I do not consent, I do not wish to participate (2)

End of Block: Informed Consent

Start of Block: Email address

*

Q7 Please provide your email address to identify your record to your game runs.

_____

End of Block: Email address

Start of Block: Snyder's self monitoring scale

Q3 The self monitoring scale measures the extent to which an individual has the will and ability to modify how they are perceived by others. Answer the following questions quickly, without overthinking.

	Select True or False	
	True (1)	False (2)

1. I find it hard to imitate the behavior of other people. (1)	○	○
2. My behavior is usually an expression of my true inner feelings, attitudes, and beliefs. (2)	○	○
3. At parties and social gatherings, I do not attempt to do or say things that others will like. (3)	○	○
4. I can only argue for ideas which I already believe. (4)	○	○
5. I can make impromptu speeches even on topics about which I have almost no information. (5)	○	○
6. I guess I put on a show to impress or entertain people. (6)	○	○
7. When I am uncertain how to act in a social situation, I look to the behavior of others for cues. (7)	○	○
8. I would probably make a good actor. (8)	○	○
9. I rarely seek the advice of my friends to choose movies, books, or music. (9)	○	○
10. I sometimes appear to others to be experiencing deeper emotions than I actually am. (10)	○	○
11. I laugh more when I watch a comedy with others than when alone. (11)	○	○
12. In groups of people, I am rarely the center of attention. (12)	○	○
13. In different situations and with different people, I often act like very different persons. (13)	○	○

14. I am not particularly good at making other people like me. (14)	○	○
15. Even if I am not enjoying myself, I often pretend to be having a good time. (15)	○	○
16. I'm not always the person I appear to be. (16)	○	○
17. I would not change my opinions (or the way I do things) in order to please someone else or win their favor. (17)	○	○
18. I have considered being an entertainer. (18)	○	○
19. In order to get along and be liked, I tend to be what people expect me to be rather than anything else. (19)	○	○
20. I have never been good at games like charades or improvisational acting. (20)	○	○
21. I have trouble changing my behavior to suit different people and different situations. (21)	○	○
22. At a party, I let others keep the jokes and stories going. (22)	○	○
23. I feel a bit awkward in company and do not show up quite as well as I should. (23)	○	○
24. I can look anyone in the eye and tell a lie with a straight face (if for a right end). (24)	○	○
25. I may deceive people by being friendly when I really dislike them. (25)	○	○

End of Block: Snyder's self monitoring scale

Start of Block: DOSPERT scale

Q4 People often see some risk in situations that contain uncertainty about what the outcome or consequences will be and for which there is the possibility of negative consequences. However, riskiness is a very personal and intuitive notion, and we are interested in **your gut level assessment of how risky** each situation or behavior is.

For each of the following statements, please indicate **how risky you perceive** each situation. Provide a rating from Not at all Risky to Extremely Risky, using the following scale:

	Not at all Risky (1)	Slightly Risky (2)	Somewhat Risky (3)	Moderately Risky (4)	Risky (5)	Very Risky (6)	Extremely Risky (7)
1. Admitting that your tastes are different from those of a friend. (1)	○	○	○	○	○	○	○
2. Going camping in the wilderness. (2)	○	○	○	○	○	○	○
3. Betting a day's income at the horse races. (3)	○	○	○	○	○	○	○
4. Investing 10% of your annual income in a moderate growth diversified fund. (4)	○	○	○	○	○	○	○
5. Drinking heavily at a social function. (5)	○	○	○	○	○	○	○
6. Taking some questionable deductions on your income tax	○	○	○	○	○	○	○

return. (6)							
7. Disagreeing with an authority figure on a major issue. (7)	○	○	○	○	○	○	○
8. Betting a day's income at a high-stake poker game. (8)	○	○	○	○	○	○	○
9. Having an affair with a married man/woman. (9)	○	○	○	○	○	○	○
10. Passing off somebody else's work as your own. (10)	○	○	○	○	○	○	○
11. Going down a ski run that is beyond your ability. (11)	○	○	○	○	○	○	○
12. Investing 5% of your annual income in a very speculative stock. (12)	○	○	○	○	○	○	○
13. Going whitewater rafting at high water in the spring. (13)	○	○	○	○	○	○	○
14. Betting a day's	○	○	○	○	○	○	○

income on the outcome of a sporting event. (14)							
15. Engaging in unprotected sex. (15)	○	○	○	○	○	○	○
16. Revealing a friend's secret to someone else. (16)	○	○	○	○	○	○	○
17. Driving a car without wearing a seat belt. (17)	○	○	○	○	○	○	○
18. Investing 10% of your annual income in a new business venture. (18)	○	○	○	○	○	○	○
19. Taking a skydiving class. (19)	○	○	○	○	○	○	○
20. Riding a motorcycle without a helmet. (20)	○	○	○	○	○	○	○
21. Choosing a career that you truly enjoy over a more secure one. (21)	○	○	○	○	○	○	○
22. Speaking your mind about an unpopular	○	○	○	○	○	○	○

issue in a meeting at work. (22)							
23. Sunbathing without sunscreen. (23)							
24. Bungee jumping off a tall bridge. (24)							
25. Piloting a small plane. (25)							
26. Walking home alone at night in an unsafe area of town. (26)							
27. Moving to a city far away from your extended family. (27)							
28. Starting a new career in your mid-thirties. (28)							
29. Leaving your young children alone at home while running an errand. (29)							
30. Not returning a wallet you found that contains $200. (30)							

End of Block: DOSPERT scale

Start of Block: Barratt's impulsiveness scale

Q5 People differ in the ways they act and think in different situations. This is a test to measure some of the ways in which you act and think. Read each statement and put an X on the appropriate circle on the right side of this page. Do not spend too much time on any statement. Answer quickly and honestly.

	Rarely/Never (1)	Occcasionally (2)	Often (3)	Almost Always/Always (4)
1. I plan tasks carefully. (1)	○	○	○	○
2. I do things without thinking. (2)	○	○	○	○
3. I make-up my mind quickly. (3)	○	○	○	○
4. I am happy-go-lucky. (4)	○	○	○	○
5. I don't "pay attention". (5)	○	○	○	○
6. I have "racing" thoughts. (6)	○	○	○	○
7. I plan trips well ahead of time. (7)	○	○	○	○
8. I am self controlled. (8)	○	○	○	○
9. I concentrate easily. (9)	○	○	○	○
10. I save regularly. (10)	○	○	○	○
11. I "squirm" at plays or lectures. (11)	○	○	○	○
12. I am a careful thinker. (12)	○	○	○	○
13. I plan for job security. (13)	○	○	○	○

14. I say things without thinking. (14)	○	○	○	○
15. I like to think about complex problems. (15)	○	○	○	○
16. I change jobs. (16)	○	○	○	○
17. I act "on impulse". (17)	○	○	○	○
18. I get easily bored when solving thought problems. (18)	○	○	○	○
19. I act on the spur of the moment. (19)	○	○	○	○
20. I am a steady thinker. (20)	○	○	○	○
21. I change residences. (21)	○	○	○	○
22. I buy things on impulse. (22)	○	○	○	○
23. I can only think about one thing at a time. (23)	○	○	○	○
24. I change hobbies. (24)	○	○	○	○
25. I spend or charge more than I earn. (25)	○	○	○	○
26. I often have extraneous thoughts when thinking. (26)	○	○	○	○
27. I am more interested in the present than the	○	○	○	○

future. (27)				
28. I am restless at the theater or lectures. (28)	○	○	○	○
29. I like puzzles. (29)	○	○	○	○
30. I am future oriented. (30)	○	○	○	○

End of Block: Barratt's impulsiveness scale

Bibliography

Aarseth, E. (2014). I fought the law: Transgressive play and the implied player. *From literature to cultural literacy* (pp. 180–188). Palgrave Macmillan UK. https://doi.org/10.1057/9781137429704_13. (Cit. on p. 38)

Abraham, A., Von Cramon, D. Y. & Schubotz, R. I. (2008). '**Meeting George Bush versus meeting Cinderella: The neural response when telling apart what is real from what is fictional in the context of our reality**'. *Journal of Cognitive Neuroscience*, *20*(6), 965–976. https://doi.org/10.1162/jocn.2008.20059 (cit. on p. 98)

Abt, C. C. (1987). Serious games. University press of America. (Cit. on p. 38).

Al-ahmad, W. & Mohammad, B. (2013). '**Addressing Information Security Risks by Adopting Standards**'. *International Journal of Information Security Science*, *2*(2), 28–43. http://eds.a.ebscohost.com.libezproxy.open.ac.uk/eds/pdfviewer/pdfviewer?sid=e1bf8be9-84ad-4d50-91fa-f9414e22825c@sessionmgr4003&vid=0&hid=4210 (cit. on p. 23)

Anderson, J. R. & Lebiere, C. J. (1998). '**The atomic components of thought**'. Lawrence Erlbaum Associates Publishers. http://act-r.psy.cmu.edu/book/. (Cit. on p. 28)

Andrijcic, E. & Horowitz, B. (2006). '**A macro-economic framework for evaluation of cyber security risks related to protection of intellectual**

property'. *Risk Analysis*, *26*(4), 907–923. https://doi.org/10.1111/j.1539-6924.2006.00787.x (cit. on p. 6)

Applebaum, A., Miller, D., Strom, B., Korban, C. & Wolf, R. (2016). '**Intelligent, automated red team emulation**'. *Proceedings of the 32nd Annual Conference on Computer Security Applications*. https://doi.org/10.1145/2991079.2991111 (cit. on p. 35)

Arcserve. (2020). '**The 2020 Data Attack Surface Report**'. https://info.arcserve.com/en/the-2020-data-attack-surface-report (cit. on p. 2)

Arnab, S., Lim, T., Carvalho, M. B., Bellotti, F., de Freitas, S., Louchart, S., Suttie, N., Berta, R. & Gloria, A. D. (2014). '**Mapping learning and game mechanics for serious games analysis**'. *British Journal of Educational Technology*, *46*(2), 391–411. https://doi.org/10.1111/bjet.12113 (cit. on pp. 39, 40, 85, 118)

Ashenden, D. & Sasse, A. (2013). '**CISOs and organisational culture: Their own worst enemy?**' *Computers & Security*, *39*, 396–405. https://doi.org/10.1016/j.cose.2013.09.004 (cit. on p. 21)

Avedon, E. (1981). '**The structural elements of games**'. *The psychology of social situations. Selected readings*, 11–17 (cit. on p. 38).

AxCrypt. (2021a). '**AxCrypt**'. Retrieved July 1, 2021, from https://www.axcrypt.net/. (Cit. on p. 78)

AxCrypt. (2021b). '**Features - AxCrypt**'. Retrieved July 1, 2021, from https://www.axcrypt.net/information/features. (Cit. on p. 78)

Bach, J. (2009). '**Principles of synthetic intelligence psi: An architecture of motivated cognition**' (Vol. 4). Oxford University Press. https://doi.org/10.1093/acprof:oso/9780195370676.001.0001. (Cit. on p. 29)

Bada, M. & Nurse, J. R. (2019). '**Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs)**'. *27*(3), 393–410. https://doi.org/10.1108/ics-07-2018-0080 (cit. on p. 8)

Bada, M., Sasse, A. M. & Nurse, J. R. C. (2019). '**Cyber security awareness campaigns: Why do they fail to change behaviour?**' *CoRR, abs/1901.02672*. http://arxiv.org/abs/1901.02672 (cit. on p. 8)

badthingsdaily. (2017). '**Tabletop scenarios (badthingsdaily)**'. Retrieved May 27, 2021, from https://twitter.com/badthingsdaily. (Cit. on p. 39)

Bakarich, K. M. & Baranek, D. (2019). '**Something phish-y is going on here: A teaching case on business email compromise**'. *Current Issues in Auditing, 14*(1), A1–A9. https://doi.org/10.2308/ciia-52706 (cit. on p. 2)

Balsera, L. & Engard, B. (2018). '**Fate core**'. Retrieved December 24, 2018, from https://www.evilhat.com/home/fate-core/. (Cit. on p. 83)

Barber, R. (2001). '**Hackers Profiled — Who Are They and What Are Their Motivations?**' *Computer Fraud & Security, 2001*(2), 14–17. https://doi.org/10.1016/S1361-3723(01)02017-6 (cit. on pp. 24, 25)

Bari, A., Kellermann, T. S. & Studer, B. (2016). Impulsiveness and inhibitory mechanisms. *Neuroimaging personality, social cognition, and character* (pp. 113–136). Elsevier. https://doi.org/10.1016/b978-0-12-800935-2.00006-3. (Cit. on p. 126)

Barlette, Y., Gundolf, K. & Jaouen, A. (2017). '**CEOs' information security behavior in SMEs: Does ownership matter?**' *22*(3), 7. https://doi.org/10.3917/sim.173.0007 (cit. on p. 8)

Barnard-Wills, D. & Ashenden, D. (2013). '**Playing with privacy: Games for education and communication in the politics of online privacy**'.

Political Studies, *63*(1), 142–160. https://doi.org/10.1111/1467-9248.12049 (cit. on p. 38)

Batty, M. & Torrens, P. M. (2005). '**Modelling and prediction in a complex world**'. *Futures*, *37*(7), 745–766. https://doi.org/10.1016/j.futures.2004.11.003 (cit. on p. 32)

BBC. (2008). '**Profile: Gary McKinnon**'. Retrieved May 16, 2021, from http://news.bbc.co.uk/1/hi/technology/4715612.stm. (Cit. on p. 25)

Beautement, A., Sasse, M. A. & Wonham, M. (2008). '**The compliance budget: Managing security behaviour in organisations**'. *Proceedings of the 2008 New Security Paradigms Workshop*, 47–58. https://discovery.ucl.ac.uk/id/eprint/1301853/1/compliance_budgetfinal.pdf (cit. on pp. 19, 21)

Blais, A.-r. & Weber, E. U. (2006). '**A Domain-Specific Risk-Taking (DOSPERT) scale for adult populations**'. *A Domain-Specific Risk-Taking (DOSPERT) scale for adult populations*, *1*(1), 33–47. https://sites.google.com/a/decisionsciences.columbia.edu/dospert/home (cit. on pp. 126, 139)

BoardGameGeek. (2018a). '**Android: Netrunner | board game | boardgamegeek**'. Retrieved July 13, 2021, from https://www.boardgamegeek.com/boardgame/124742/android-netrunner. (Cit. on p. 83)

BoardGameGeek. (2018b). '**Boardgamegeek | gaming unplugged since 2000**'. Retrieved December 26, 2018, from https://www.boardgamegeek.com/. (Cit. on p. 83)

Bolgan, S. (2018). *Securing cyberspace: Development and evaluation of a novel research toolset* (Doctoral dissertation). Abertay University. https://rke.abertay.ac.uk/en/studentTheses/securing-cyberspace. (Cit. on p. 23)

Bolland, B. (2006). '**Re-thinking Coercion**'. *The RUSI Journal*, *151*(4), 42–46. https://doi.org/10.1080/03071840609442034 (cit. on p. 37)

Bowman, S. L. (2015). '**Bleed: The spillover between player and character**'. Retrieved June 4, 2021, from https://nordiclarp.org/2015/03/02/bleed-the-spillover-between-player-and-character/. (Cit. on p. 37)

Bratman, M. E. (1999). '**Intention, Plans, and Practical Reason**'. CSLI Publications. https://web.stanford.edu/group/cslipublications/cslipublications/site/1575861925.shtml. (Cit. on p. 26)

Bryman, A. (2012). '**Social Research Methods**' (4th ed.). Oxford University Press. (Cit. on p. 57).

Bugert, N. (2019). '**Risk budget planning through assessing the criticality and vulnerability of supply network entities facing disruption risks**'. *IFAC-PapersOnLine*, *52*(13), 1295–1300. https://doi.org/10.1016/j.ifacol.2019.11.377 (cit. on p. 31)

Bulletproof. (2021). '**Comprehensive penetration testing - uk pen testing consultants - bulletproof.co.uk**'. Retrieved May 25, 2021, from https://blog.rsisecurity.chttps://www.bulletproof.co.uk/penetration-testing. (Cit. on p. 36)

Caldwell, T. (2011). '**Ethical hackers: Putting on the white hat**'. *Network Security*, *2011*(7), 10–13. https://doi.org/10.1016/S1353-4858(11)70075-7 (cit. on p. 25)

Campbell, W. (2018). '**Understanding discrete-event simulation, part 1: What is discrete-event simulation?**' Retrieved July 19, 2018, from https://uk.mathworks.com/videos/understanding-discrete-event-simulation-part-1-what-is-discrete-event-simulation--1494873178760.html. (Cit. on p. 30)

Cappelli, D. M., Moore, A. P. & Trzeciak, R. F. (2012). The cert guide to insider threats: How to prevent, detect, and respond to information technology crimes (theft, sabotage, fraud). Addison-Wesley. (Cit. on p. 24).

Carnegie Mellon University. (2013a). '**ACT-R - About**'. Retrieved May 11, 2021, from http://act-r.psy.cmu.edu/about/. (Cit. on p. 28)

Carnegie Mellon University. (2013b). '**ACT-R - Home**'. Retrieved May 11, 2021, from http://act-r.psy.cmu.edu/. (Cit. on p. 28)

'**Chapter 3 – individual differences**'. (2021). Retrieved August 3, 2021, from https://nios.ac.in/media/documents/secpsycour/English/Chapter-3.pdf. (Cit. on p. 125)

Cheek, R. G., Kunz, M. B. & Osborne, P. (2001). *Web advertising: A look at types and costs* (tech. rep.). Citeseer. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.591.306&rep=rep1&type=pdf. (Cit. on p. 5)

CIS. (2021). '**The solarwinds cyber-attack: What you need to know**'. Retrieved May 1, 2021, from https://www.cisecurity.org/solarwinds/. (Cit. on p. 4)

Clark, C. A. (1970). '**Serious games**'. *New York: Viking* (cit. on p. 38).

Clarke, V. & Braun, V. (2014). Thematic analysis. In T. Teo (Ed.), *Encyclopedia of critical psychology* (pp. 1947–1952). Springer New York. https://doi.org/10.1007/978-1-4614-5583-7_311. (Cit. on p. 109)

CMS. (2021). '**Gdpr enforcement tracker**'. Retrieved October 17, 2021, from https://www.enforcementtracker.com. (Cit. on p. 2)

Colicchia, C., Creazza, A. & Menachof, D. A. (2019). '**Managing cyber and information risks in supply chains: Insights from an exploratory analysis**'. *Supply Chain Management: An International Journal*, *24*(2), 215–240. https://doi.org/10.1108/scm-09-2017-0289 (cit. on p. 10)

Collier, D. & Mahoney, J. (1996). '**Insights and pitfalls: Selection bias in qualitative research**'. *World Politics*, *49*(1), 56–91. http://www.jstor.org/stable/25053989 (cit. on p. 52)

Constantin, L. (2020). '**APT-style mercenary groups challenge the threat models of many organizations**'. Retrieved May 16, 2021, from https://www.csoonline.com/article/3573081/apt-style-mercenary-groups-challenge-the-threat-models-of-many-organizations.html. (Cit. on p. 25)

Cornish, D. B. & Clarke, R. V. (2003). '**Opportunities, precipitators and criminal decisions: A reply to wortley's critique of situational crime prevention**'. *Crime prevention studies*, *16*, 41–96 (cit. on p. 28).

Crooks, A. T. & Heppenstall, A. J. (2011). Introduction to agent-based modelling. *Agent-based models of geographical systems* (pp. 85–105). Springer Netherlands. https://doi.org/10.1007/978-90-481-8927-4_5. (Cit. on p. 32)

Crooltall, D., Oxford, R. & Saunders, D. (1987). '**Towards a reconceptualization of simulation: From representation to reality**'. *Simulation/games for learning*, *17*(4), 147–71. http://sites.unice.fr/sg/resources/articles/Article_Reconceptualization-simulation_200bw-upright.pdf (cit. on p. 37)

Crotty, M. (1998). '**The foundations of social research: Meaning and perspective in the research process**' (1st ed.). SAGE Publications Ltd. https://uk.sagepub.com/en-gb/eur/the-foundations-of-social-research/book207972. (Cit. on p. 47)

Cuganesan, S., Steele, C. & Hart, A. (2017). '**How senior management and workplace norms influence information security attitudes and self-efficacy**'. *Behaviour & Information Technology*, *37*(1), 50–65. https://doi.org/10.1080/0144929x.2017.1397193 (cit. on p. 22)

Daniau, S. (2016). '**The transformative potential of role-playing games—: From play skills to human skills**'. *Simulation & Gaming*, *47*(4), 423–444. https://doi.org/10.1177/1046878116650765 (cit. on p. 37)

DARPA. (2005). '**Bica, biologically-inspired cognitive architectures, proposer information pamphlet (pip) for broad agency announcement**', 05–18 (cit. on p. 29).

Dautlich, M. (2004). '**Penetration testing — the legal implications**'. *Computer Law & Security Review*, *20*(1), 41–43. https://doi.org/10.1016/s0267-3649(04)00008-1 (cit. on p. 12)

DeMarco, J. V. (2018). '**An approach to minimizing legal and reputational risk in red team hacking exercises**'. *Computer Law & Security Review*, *34*(4), 908–911. https://doi.org/10.1016/j.clsr.2018.05.033 (cit. on p. 35)

Denning, T., Lerner, A., Shostack, A. & Kohno, T. (2013). '**Control-alt-hack**'. *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security - CCS '13*. https://doi.org/10.1145/2508859.2516753 (cit. on pp. 38, 39)

Dennis, A. (2011). Pragmatism and symbolic interactionism. In I. C. Jarvie & J. Zamora-Bonilla (Eds.). SAGE Publications. https://uk.sagepub.com/en-gb/eur/the-sage-handbook-of-the-philosophy-of-social-sciences/book232751. (Cit. on p. 49)

Dimensional Research. (2016). '**Trends in Security Framework Adoption Trends in Security Framework Adoption**'. (March), 1–10. Retrieved May 7, 2021, from https://www.tenable.com/press-releases/nist-cybersecurity-framework-adoption-linked-to-higher-security-confidence-according (cit. on p. 9)

Doctorow, C. (2010). '**Cory Doctorow: Persistence Pays Parasites**'. Retrieved May 17, 2021, from https://locusmag.com/2010/05/cory-doctorow-persistence-pays-parasites/. (Cit. on p. 2)

Doodle. (2021). '**Free online meeting scheduling tool - doodle**'. Retrieved July 15, 2021, from https://doodle.com/en/. (Cit. on p. 112)

Dörner, D. (1999). '**Bauplan für eine seele**' (cit. on p. 29).

Dörner, D. & Güss, C. D. (2013). '**PSI: A computational architecture of cognition, motivation, and emotion**'. *Review of General Psychology*, *17*(3), 297–317. https://doi.org/10.1037/a0032947 (cit. on p. 29)

Du Toit, E. C. (2016). *Making a game of chess sound* (Doctoral dissertation). Stellenbosch University. Retrieved July 18, 2021, from http://hdl.handle.net/10019.1/100179. (Cit. on p. 123)

Duncan, B. & Whittington, M. (2014). '**Compliance with standards, assurance and audit**'. *Proceedings of the 7th International Conference on Security of Information and Networks - SIN '14*. https://doi.org/10.1145/2659651.2659711 (cit. on p. 19)

EC-COUNCIL. (2011). '**Penetration Testing: Procedures & Methodologies**'. EC Council Press. https://www.academia.edu/35711304/Penetration_Testing_Procedures_and_Methodologies. (Cit. on p. 35)

Emma, M. (2017). '**Story of Jonathan James who hacked NASA and Pentagon in age of 15**'. Retrieved May 16, 2021, from https://techasli.com/story-jonathan-james-hacked-nasa-pentagon-age-15/. (Cit. on p. 25)

Epstein, J. M. (2012). '**Generative social science: Studies in agent-based computational modeling**'. Princeton University Press. https://doi.org/10.1515/9781400842872. (Cit. on p. 32)

Fagade, T., Maraslis, K. & Tryfonas, T. (2017). '**Towards effective cybersecurity resource allocation: The monte carlo predictive modelling approach**'. *International Journal of Critical Infrastructures*, *13*(2/3), 152. https://doi.org/10.1504/ijcis.2017.088235 (cit. on p. 32)

Federal Bureau of Investigation. (2021). '**Internet crime report 2020**'. Retrieved April 5, 2021, from https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf. (Cit. on p. 1)

Figueira, G. & Almada-Lobo, B. (2014). '**Hybrid simulation–optimization methods: A taxonomy and discussion**'. *Simulation Modelling Practice and Theory*, *46*, 118–134. https://doi.org/10.1016/j.simpat.2014.03.007 (cit. on p. 31)

FireEye. (2020). '**This is not a test: Apt41 initiates global intrusion campaign using multiple exploits**'. Retrieved May 2, 2021, from https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html. (Cit. on p. 4)

Fischer, Jan; and Vander Laan, S. (2002). '**Improving approaches to multicultural education: Teaching empathy through role playing**'. *Multicultural Education*, *9*(4), 25–26. https://www.proquest.com/openview/f17102fdb806811cee6a252e8691dfff/1?pq-origsite=gscholar&cbl=33246 (cit. on p. 37)

Franklin, S., Madl, T., D'Mello, S. & Snaider, J. (2014). '**LIDA: A systems-level architecture for cognition, emotion, and learning**'. *IEEE Transactions on Autonomous Mental Development*, *6*(1), 19–41. https://doi.org/10.1109/TAMD.2013.2277589 (cit. on p. 29)

Fujimoto, R. M. (1990). '**Parallel discrete event simulation**'. *Communications of the ACM*, *33*(10), 30–53. https://doi.org/10.1145/84537.84545 (cit. on p. 30)

Fujs, D., Mihelič, A. & Vrhovec, S. L. R. (2019). '**The power of interpretation**'. *Proceedings of the 14th International Conference on Availability, Reliability and Security*. https://doi.org/10.1145/3339252.3341479 (cit. on p. 10)

Gabriella Coleman. (2014). Hacker, Hoaxer, Whistleblower, Spy The Many Faces of Anonymous. Verso. (Cit. on p. 25).

Gabrilovich, E. & Gontmakher, A. (2002). '**The homograph attack**'. *Communications of the ACM*, *45*(2), 128. https://doi.org/10.1145/503124.503156 (cit. on p. 164)

Gai, K., Qiu, M. & Hassan, H. (2016). '**Secure cyber incident analytics framework using monte carlo simulations for financial cybersecurity insurance in cloud computing**'. *Concurrency and Computation: Practice and Experience*, *29*(7), e3856. https://doi.org/10.1002/cpe.3856 (cit. on p. 32)

Garner Jr, M. W. (2017). *Nation state threat actions against critical energy infrastructures* (Doctoral dissertation). Utica College. https://www.proquest.com/docview/1977404167. (Cit. on p. 4)

Geddes, B. (1990). '**How the cases you choose affect the answers you get: Selection bias in comparative politics**'. *Political Analysis*, *2*, 131–150. http://www.jstor.org/stable/23317768 (cit. on p. 52)

Geenens, P. (2020). '**How worried should you be about nation-state attacks?**' *Network Security*, *2020*(3), 17–19. https://doi.org/10.1016/s1353-4858(20)30032-5 (cit. on p. 4)

Gondree, M., Peterson, Z. N. & Pusey, P. (2016). '**Talking about talking about cybersecurity games**'. *login Usenix Mag.*, *41*(1). https://www.usenix.org/system/files/login/articles/login_spring16_07_gondree.pdf (cit. on p. 38)

Goodman, J. (2005). '**Pay-per-percentage of impressions: An advertising method that is highly robust to fraud**'. *Workshop on Sponsored Search Auctions*. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.73.595&rep=rep1&type=pdf (cit. on p. 5)

GOV.UK. (2017). '**Cyber security for defence suppliers (def stan 05-138)**'. Retrieved August 4, 2021, from https://www.gov.uk/government/publications/cyber-security-for-defence-suppliers-def-stan-05-138. (Cit. on p. 9)

GOV.UK. (2020). '**UK Cyber Security Breaches Report 2020**'. (June), 58. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020 (cit. on p. 21)

Gray, D. E. (2004). '**Doing research in the real world**' (1st ed.). SAGE Publications. (Cit. on pp. 45–47, 50, 52, 55, 56, 106).

Greitzer, F. L., Strozer, J., Cohen, S., Bergey, J., Cowley, J., Moore, A. & Mundie, D. (2014a). '**Unintentional insider threat: Contributing factors, observables, and mitigation strategies**'. *2014 47th Hawaii International Conference on System Sciences*, 2025–2034. https://doi.org/10.1109/HICSS.2014.256 (cit. on p. 24)

Greitzer, F. L., Strozer, J., Cohen, S., Bergey, J., Cowley, J., Moore, A. & Mundie, D. (2014b). '**Unintentional insider threat: Contributing factors, observables, and mitigation strategies**'. *2014 47th Hawaii International Conference on System Sciences*. https://doi.org/10.1109/hicss.2014.256 (cit. on p. 21)

Griffiths, P. (2016). '**Risk-based auditing**'. Routledge. https://doi.org/10.4324/9781315606545. (Cit. on p. 22)

Grobmeier, C. (2016). '**How i got phished**'. Retrieved May 17, 2021, from https://www.linkedin.com/pulse/how-i-got-phished-christian-grobmeier. (Cit. on p. 2)

Gundu, T. (2019). '**Acknowledging and reducing the knowing and doing gap in employee cybersecurity complaince**'. *ICCWS 2019 14th International Conference on Cyber Warfare and Security*, 94–102. http://hdl.handle.net/20.500.12821/340 (cit. on p. 8)

HackTheBox. (2021). '**Hackthebox: Hacking training for the best**'. Retrieved July 16, 2021, from https://www.hackthebox.eu/. (Cit. on p. 106)

Harviainen, J. T. (2009). '**A Hermeneutical Approach to Role-Playing Analysis**'. *International Journal of Role-Playing*, (1), 66–78. http://marinkacopier.nl/ijrp/wp-content/uploads/2009/01/harviainen_hermeneutical_approach_to_rp_analysis.pdf (cit. on p. 37)

Heaton, R. (2019). '**I was 7 words away from being spear-phished**'. Retrieved May 17, 2021, from https://robertheaton.com/2019/06/24/i-was-7-words-away-from-being-spear-phished/. (Cit. on p. 2)

Helbing, D. (2012). Agent-Based Modeling. *Social self-organization* (pp. 25–70). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-24004-1_2. (Cit. on p. 32)

Herath, T. & Rao, H. R. (2009). '**Protection motivation and deterrence: A framework for security policy compliance in organisations**'. *18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6 (cit. on p. 20)

Hicks, F. (2018). '**What do i focus on in a fate core one shot to showcase its differences to my d&d group? - role-playing games stack exchange**'. Retrieved December 24, 2018, from https://rpg.stackexchange.

com/questions/113918/what-do-i-focus-on-in-a-fate-core-one-shot-to-showcase-its-differences-to-my-dd. (Cit. on p. 83)

Hodges, D. & Buckley, O. (2018). '**Deconstructing who you play: Character choice in online gaming**'. *Entertainment Computing*, *27*, 170–178. https://doi.org/10.1016/j.entcom.2018.06.002 (cit. on p. 170)

Hodges, D., Creese, S. & Goldsmith, M. (2012). '**A model for identity in the cyber and natural universes**'. *2012 European Intelligence and Security Informatics Conference*. https://doi.org/10.1109/eisic.2012.43 (cit. on p. 23)

Hoshmand, L. T. (2003). '**Can lessons of history and logical analysis ensure progress in psychological science?**' *Theory & Psychology*, *13*(1), 39–44. https://doi.org/10.1177/0959354303131003 (cit. on p. 49)

Hussain, M. Z., Hasan, M. Z., Taimoor, M., Chughtai, A., Taimoor, M. & Chughtai, A. (2017). '**Penetration Testing In System Administration**'. *International Journal of Scientific & Technology Research*, *6*(6), 275–278. https://www.ijstr.org/paper-references.php?ref=IJSTR-0617-17102 (cit. on p. 36)

Hutchins, E. M., Cloppert, M. J., Amin, R. M. et al. (2011). '**Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains**'. *The Proceedings of the 6th International Conference on Information Warfare and Security*, 113–125 (cit. on pp. 8, 39).

Information Comissioner's Office. (2021). '**Personal data breaches**'. Retrieved October 17, 2021, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/?q=72. (Cit. on p. 2)

INTSIGHTS. (2017). *The Rise of State-Sponsored Attacks Against the Financial Services Industry* (tech. rep.). http://wow.intsights.com/rs/071-ZWD-900/

images/The%20Rise%20of%20State%20Sponsored%20Attacks%20Against%20the%20Financial%20Services%20Industry.pdf. (Cit. on p. 25)

Islam, M. S., Farah, N. & Stafford, T. F. (2018). '**Factors associated with security/cybersecurity audit by internal audit function: An international study**'. *Managerial Auditing Journal*, *33*(4), 377–409. https://doi.org/10.1108/MAJ-07-2017-1595 (cit. on p. 9)

ISO. (2007). '**Iso - iso 28000:2007 - specification for security management systems for the supply chain**'. Retrieved May 21, 2021, from https://www.iso.org/standard/44641.html. (Cit. on p. 18)

ISO. (2018). '**Iso - iso 31000:2018 - risk management — guidelines**' (2nd ed.). Retrieved May 21, 2021, from https://www.iso.org/standard/65694.html. (Cit. on p. 18)

ISO. (2021a). '**ISO - Frequently Asked Questions (FAQs)**'. Retrieved May 21, 2021, from https://www.iso.org/frequently-asked-questions-faqs.html. (Cit. on p. 18)

ISO. (2021b). '**Iso/iec 27001 - information security management**'. Retrieved August 4, 2021, from https://www.iso.org/isoiec-27001-information-security.html. (Cit. on p. 9)

IT Governance. (2021). '**Gdpr fines**'. Retrieved October 17, 2021, from https://www.itgovernance.co.uk/dpa-and-gdpr-penalties#:~:text=The%20UK%20GDPR%20and%20DPA,whichever%20is%20greater%20%E2%80%93%20for%20infringements.. (Cit. on p. 2)

Jakobsson, M. & Ramzan, Z. (2008). '**Crimeware: Understanding new attacks and defenses**'. Addison-Wesley Professional. (Cit. on p. 25).

Jakobsson, M., Taveau, S. & Extricatus, L. (2012). '**The case for replacing passwords with biometrics**'. *Mobile Security Technologies*, 1–6. https://www.academia.edu/download/32551958/3.pdf (cit. on p. 20)

Jones, A. & Colwill, C. (2008). '**Dealing with the malicious insider**'. *Proceedings of 6th Australian Information Security Management Conference*, (December 2006), 70–86. https://doi.org/10.4225/75/57b562dab876e (cit. on p. 10)

Jones, R. M., Lebiere, C. & Crossman, J. A. (2007). '**Comparing modeling idioms in act-r and soar**'. *Proceedings of the 8th international conference on cognitive modeling*, 49–54 (cit. on p. 29).

Kaspersky. (2015). '**Equation Group : Questions and Answers**'. (February), 1–44. http://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf (cit. on p. 25)

Kerr, N. L., Nerenz, D. R. & Herrick, D. (1979). '**Role playing and the study of jury behavior**'. *Sociological Methods & Research*, *7*(3), 337–355. https://doi.org/10.1177/004912417900700305 (cit. on p. 37)

Kigerl, A. C. (2016). '**Email spam origins: Does the CAN SPAM act shift spam beyond united states jurisdiction?**' *Trends in Organized Crime*, *21*(1), 62–78. https://doi.org/10.1007/s12117-016-9289-9 (cit. on p. 5)

Kimball, M. S. (1993). '**Standard risk aversion**'. *Econometrica*, *61*(3), 589. https://doi.org/10.2307/2951719 (cit. on p. 22)

Kindlund, D., Moran, N. & Rachwald, R. (2014). '**WORLD WAR C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks**'. https://www.fireeye.com/content/dam/legacy/resources/pdfs/fireeye-wwc-report.pdf (cit. on p. 4)

Klabbers, J. H. (2009). '**The magic circle: Principles of gaming & simulation**'. Brill Sense. (Cit. on p. 38).

Knowles, W., Baron, A. & McGarr, T. (2016). '**The simulated security assessment ecosystem: Does penetration testing need standardisation?**' *Computers & Security*, *62*, 296–316. https://doi.org/10.1016/j.cose.2016.08.002 (cit. on p. 35)

Kotenko, I., Konovalov, A. & Shorov, A. (2010). Simulation of botnets: Agent-based approach. *Studies in computational intelligence* (pp. 247–252). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-15211-5_26. (Cit. on p. 34)

Laird, J. & Newell, A. (1983). *A Universal Weak Method* (Doctoral dissertation). Carnegie Mellon University. Retrieved May 11, 2021, from http://shelf2.library.cmu.edu/Tech/9997759.pdf. (Cit. on p. 28)

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C. & Bellekens, X. (2021). '**Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic**'. *Computers & Security*, *105*, 102248. https://doi.org/10.1016/j.cose.2021.102248 (cit. on p. 168)

Lean, T. (2016). '**Prestel: The british internet that never was**'. Retrieved May 4, 2021, from https://www.historytoday.com/history-matters/prestel-british-internet-never-was. (Cit. on p. 5)

Lee, K., Rucker, M., Scherer, W. T., Beling, P. A., Gerber, M. S. & Kang, H. (2017). '**Agent-based model construction using inverse reinforcement learning**'. *2017 Winter Simulation Conference (WSC)*, (1971), 1264–1275. https://doi.org/10.1109/WSC.2017.8247872 (cit. on p. 34)

Levy, S., Martens, K. & van der Heijden, R. (2016). '**Agent-based models and self-organisation: Addressing common criticisms and the role of agent-based modelling in urban planning**'. *Town Planning Review*, *87*(3), 321–338. https://doi.org/10.3828/tpr.2016.22 (cit. on p. 32)

Levy, S. & Crandall, J. R. (2020). '**The program with a personality: Analysis of Elk cloner, the first personal computer virus**'. *arXiv*, 1–8 (cit. on p. 3).

Leyden, J. (2015). '**How a hack on prince philip's prestel account led to uk computer law**'. Retrieved May 4, 2021, from https://www.theregister.com/2015/03/26/prestel_hack_anniversary_prince_philip_computer_misuse/. (Cit. on p. 5)

Liao, J. (, Welsch, H. & Moutray, C. (2008). '**Start-up resources and entrepreneurial discontinuance: The case of nascent entrepreneurs**'. *Journal of Small Business Strategy*, *19*(2), 1–16. https://libjournals.mtsu.edu/index.php/jsbs/article/view/112 (cit. on p. 36)

Lieto, A. (2021). '**Cognitive design for artificial minds**'. Routledge. https://doi.org/10.4324/9781315460536. (Cit. on p. 28)

Lieto, A., Bhatt, M., Oltramari, A. & Vernon, D. (2018). '**The role of cognitive architectures in general artificial intelligence**'. *Cognitive Systems Research*, *48*, 1–3. https://doi.org/10.1016/j.cogsys.2017.08.003 (cit. on p. 28)

Liu, X., Shahidehpour, M., Cao, Y., Wu, L., Wei, W. & Liu, X. (2017). '**Microgrid risk analysis considering the impact of cyber attacks on solar PV and ESS control systems**'. *IEEE Transactions on Smart Grid*, *8*(3), 1330–1339. https://doi.org/10.1109/tsg.2016.2622289 (cit. on p. 32)

Lumbroso, D. & Davison, M. (2018). '**Use of an agent-based model and Monte Carlo analysis to estimate the effectiveness of emergency management interventions to reduce loss of life during extreme floods**'. *Journal of Flood Risk Management*, *11*, S419–S433. https://doi.org/10.1111/jfr3.12230 (cit. on pp. 31, 34)

Lune, H. & Berg, B. L. (2017). '**Methods for the Social Sciences Global Edition**' (9th ed.). pearson. (Cit. on pp. 52, 56, 58, 64).

Magd, H. & Curry, A. (2003). '**ISO 9000 and TQM: are they complementary or contradictory to each other?**' *The TQM Magazine*, *15*(4), 244–256. https://doi.org/10.1108/09544780310486155 (cit. on p. 9)

Maimon, D., Babko-Malaya, O., Cathey, R. & Hinton, S. (2017). '**Re-thinking Online Offenders' SKRAM: Individual Traits and Situational Motivations as Additional Risk Factors for Predicting Cyber Attacks**'. *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)*, 232–238. https://doi.org/10.1109/DASC-PICom-DataCom-CyberSciTec.2017.50 (cit. on p. 27)

Malkin, G. S. & Parker, T. L. (2008). '**Rfc1392**'. Retrieved June 30, 2020, from https://web.archive.org/web/20080117174639/http://rfc.net/rfc1392.html. (Cit. on p. 3)

Malleson, N., Heppenstall, A. & See, L. (2010). '**Crime reduction through simulation: An agent-based model of burglary**'. *Computers, Environment and Urban Systems*, *34*(3), 236–250. https://doi.org/10.1016/j.compenvurbsys.2009.10.005 (cit. on p. 34)

Marczewski, A. (2017). '**A revised gamification design framework**'. Retrieved December 5, 2021, from https://www.gamified.uk/2017/04/06/revised-gamification-design-framework/. (Cit. on pp. 41, 43)

Marczewski, A. (2021). '**The intrinsic motivation ramp**'. Retrieved December 6, 2021, from https://www.gamified.uk/gamification-framework/the-intrinsic-motivation-ramp/. (Cit. on p. 42)

Martin, W. R. (2012). '**Challenges and prospects for whole-core monte carlo analysis**'. *Nuclear Engineering and Technology*, *44* (2), 151–160. https://doi.org/10.5516/NET.01.2012.502 (cit. on p. 31)

Maurer, T. (2018). '**Cyber mercenaries**'. Cambridge University Press. https://doi.org/10.1017/9781316422724. (Cit. on pp. 3, 4)

Mauriras-Bousquet, M. (1984). '**Théorie et pratique ludiques**'. FeniXX. (Cit. on p. 37).

McKinnel, D. R., Dargahi, T., Dehghantanha, A. & Choo, K.-K. R. (2019). '**A systematic literature review and meta-analysis on artificial intelligence in penetration testing and vulnerability assessment**'. *Computers & Electrical Engineering*, *75*, 175–188. https://doi.org/10.1016/j.compeleceng.2019.02.022 (cit. on pp. 12, 35)

Meyers, C., Powers, S. & Faissol, D. (2009). *Taxonomies of cyber adversaries and attacks: A survey of incidents and approaches* (tech. rep.). Lawrence Livermore National Lab.(LLNL), Livermore, CA (United States). https://www.osti.gov/biblio/967712. (Cit. on p. 24)

Microsoft. (2020a). '**Adv200006 - security update guide - microsoft - type 1 font parsing remote code execution vulnerability**'. Retrieved May 24, 2021, from https://msrc.microsoft.com/update-guide/vulnerability/ADV200006. (Cit. on p. 21)

Microsoft. (2020b). '**Microsoft report shows increasing sophistication of cyber threats - microsoft on the issues**'. Retrieved April 28, 2021, from https://blogs.microsoft.com/on-the-issues/2020/09/29/microsoft-digital-defense-report-cyber-threats/. (Cit. on pp. 2, 4, 5)

MITRE. (2021a). '**Mitre ATT&CK**'. Retrieved May 27, 2021, from https://attack.mitre.org/. (Cit. on pp. 39, 103)

MITRE. (2021b). '**Mitre D3FEND**'. Retrieved July 29, 2021, from https://d3fend.mitre.org/. (Cit. on p. 180)

Morgenthaler, G. W. (1961). '**The theory and application of simulation and operations research, progress in operations research**'. (Cit. on p. 31).

Muncaster, P. (2020). '**Kaspersky uncovers new apt "mercenary" group**'. Retrieved May 2, 2021, from https://www.infosecurity-magazine.com/news/kaspersky-uncovers-new-apt/. (Cit. on p. 6)

Nance, R. E. (1996). '**A history of discrete event simulation programming languages**'. *Discrete Event Simulation Languages Session*, 369–427. https://doi.org/10.1145/234286.1057822 (cit. on pp. 30, 31)

Nathan, A. J. & Scobell, A. (2020). '**2020 Data Breach Investigations Report**'. *Verizon*. https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf (cit. on pp. 4, 5)

National Institute of Standards and Technology (NIST). (2018). '**Nist cybersecurity framework**'. Retrieved May 6, 2021, from https://www.nist.gov/cyberframework. (Cit. on p. 7)

NCSC. (2016). '**How cyber attacks work**'. Retrieved July 13, 2021, from https://www.ncsc.gov.uk/articles/how-cyber-attacks-work. (Cit. on p. 91)

NCSC. (2021). '**Penetration testing - ncsc.gov.uk**'. Retrieved June 8, 2021, from https://www.ncsc.gov.uk/guidance/penetration-testing. (Cit. on p. 36)

Netragard. (2020). '**How to scope a penetration test (the right way) – netragard**'. Retrieved June 9, 2021, from https://www.netragard.com/how-to-scope-a-penetration-test-the-right-way/. (Cit. on p. 35)

Newell, A. (1990). '**Unified theories of cognition**'. Harvard University Press. (Cit. on p. 29).

Ngo, T. A. & See, L. (2011). Calibration and validation of agent-based models of land cover change. *Agent-based models of geographical systems* (pp. 181–197). Springer Netherlands. https://doi.org/10.1007/978-90-481-8927-4_10. (Cit. on pp. 32, 33)

NIST. (2016). '**The cybersecurity framework (video)**'. Retrieved May 6, 2021, from https://www.nist.gov/video/cybersecurity-framework-0. (Cit. on p. 7)

NIST. (2018). '**Nist cybersecurity framework: The five functions**'. Retrieved May 6, 2021, from https://www.nist.gov/cyberframework/online-learning/five-functions%202018. (Cit. on p. 8)

NIST. (2019). '**Nvd - cve-2019-2215**'. Retrieved May 24, 2021, from https://nvd.nist.gov/vuln/detail/CVE-2019-2215. (Cit. on p. 21)

NIST. (2020). '**Nvd - cve-2020-12271**'. Retrieved May 24, 2021, from https://nvd.nist.gov/vuln/detail/CVE-2020-12271. (Cit. on p. 21)

OWASP. (2021). '**Owasp top 10: 2021**'. Retrieved December 27, 2021, from https://owasp.org/Top10/. (Cit. on p. 167)

Palmer, M. E., Robinson, C., Patilla, J. C. & Moser, E. P. (2001). '**Information security policy framework: Best practices for security policy in the e-commerce age**'. *Information Systems Security*, *10*(2), 1–15. https://doi.org/10.1201/1086/43314.10.2.20010506/31399.4 (cit. on pp. 18, 19)

Parker, D. B. & Parker, D. B. (1998). '**Fighting computer crime: A new framework for protecting information**'. Wiley New York. (Cit. on p. 27).

Parunak, H., Savit, R. & Riolo, R. (1998). '**Agent-based modeling vs. equation-based modeling: A case study and users' guide**'. *Proceedings of Multi-agent systems and Agent-based Simulation (MABS'98)*, 10–25. https://doi.org/10.1007/10692956_2 (cit. on pp. 30, 32)

Patton, J. H., Stanford, M. S. & Barratt, E. S. (1995). '**Factor structure of the barratt impulsiveness scale**'. *Journal of Clinical Psychology*, *51*(6), 768–774. https://doi.org/10.1002/1097-4679(199511)51:6<768::AID-JCLP2270510607>3.0.CO;2-1 (cit. on pp. 126, 141)

Paul, G. & Irvine, J. (2016). '**IEDs on the road to fingerprint authentication: Biometrics have vulnerabilities that PINs and passwords don't**'. *5*(2), 79–86. https://doi.org/10.1109/mce.2016.2521978 (cit. on p. 20)

Paulsen, C. (2016). '**Cybersecuring small businesses**'. *49*(8), 92–97. https://doi.org/10.1109/mc.2016.223 (cit. on p. 8)

PCI Security Standards Council. (2021). '**Securing the future of payments together**'. Retrieved August 4, 2021, from https://www.pcisecuritystandards.org/. (Cit. on p. 9)

PentesterLab. (2021). '**Pentesterlab: Learn web penetration testing: The right way**'. Retrieved July 16, 2021, from https://www.pentesterlab.com/. (Cit. on p. 106)

Peterson, J. (2021). '**Forty years of adventure - dungeons & dragons**'. Retrieved October 12, 2021, from https://dnd.wizards.com/dungeons-and-dragons/what-dd/history/history-forty-years-adventure. (Cit. on p. 82)

Posthumus, S. & von Solms, R. (2004). '**A framework for the governance of information security**'. *Computers & Security*, *23*(8), 638–646. https://doi.org/10.1016/j.cose.2004.10.006 (cit. on p. 21)

Prensky, M. (2003). '**Digital game-based learning**'. *Computers in Entertainment*, *1*(1), 21–21. https://doi.org/10.1145/950566.950596 (cit. on p. 38)

Punzo, V. (2016). How crime spreads through imitation in social networks: A simulation model. *New frontiers in the study of social phenomena* (pp. 169–190).

Springer International Publishing. https://doi.org/10.1007/978-3-319-23938-5_10. (Cit. on p. 34)

Purple Squad Security. (2017a). '**Episode 15 – Infosec Tabletop D&D with Brakeing Down Security**' [Timestamp:]. Retrieved May 27, 2021, from https://purplesquadsec.com/episode/d1cc212c63164e6b/episode-15-infosec-tabletop-d-d-with-brakeing-down-security. (Cit. on p. 39)

Purple Squad Security. (2017b). '**Episode 15 – Infosec Tabletop D&D with Brakeing Down Security**'. Retrieved May 27, 2021, from https://purplesquadsec.com/episode/d1cc212c63164e6b/episode-15-infosec-tabletop-d-d-with-brakeing-down-security Timestamp: 37:12. (Cit. on p. 39)

Rao, A. S. & Georgeff, M. P. (1995). '**BDI Agents: From Theory to Practice**'. *Proceedings of the First International Conference on Multiagent Systems*, *95*, 312–319. https://www.aaai.org/Papers/ICMAS/1995/ICMAS95-042.pdf (cit. on p. 26)

Raymond, E. S. (2003). '**Hacker - the jargon file – online version of the new hacker's dictionary**' [2020-06-30]. http://www.catb.org/~esr/jargon/html/H/hacker.html. (Cit. on p. 3)

Rhysider, J. (2020). '**Darknet diaries - ep 78: Nerdcore**'. Retrieved May 4, 2021, from https://darknetdiaries.com/transcript/78/. (Cit. on p. 5)

Robinson, D. & Bellotti, V. (2013). '**A preliminary taxonomy of gamification elements for varying anticipated commitment**'. *Proc. ACM CHI 2013 Workshop on Designing Gamification: Creating Gameful and Playful Experiences* (cit. on pp. 38, 119).

Rodney L. Custer, B. R. S., Joseph A. Scarcella. (1999). '**Jvte v15n2: The modified delphi technique - a rotational modification**'. Retrieved December

28, 2018, from https://scholar.lib.vt.edu/ejournals/JVTE/v15n2/custer.html. (Cit. on p. 104)

Roepke, R. & Schroeder, U. (2019). '**The problem with teaching defence against the dark arts: A review of game-based learning applications and serious games for cyber security education**'. *Proceedings of the 11th International Conference on Computer Supported Education*. https://doi.org/10.5220/0007706100580066 (cit. on p. 39)

Rosenbloom, P. S., Demski, A. & Ustun, V. (2016). '**The Sigma Cognitive Architecture and System: Towards Functionally Elegant Grand Unification**'. *Journal of Artificial General Intelligence*, *7*(1), 1–103. https://doi.org/10.1515/jagi-2016-0001 (cit. on p. 29)

RSI Security. (2020). '**Average cost of penetration testing | rsi security**'. Retrieved May 25, 2021, from https://blog.rsisecurity.com/what-is-the-average-cost-of-penetration-testing/. (Cit. on p. 36)

SANS. (2019). '**Sans 2019 state of ot/ics cybersecurity survey**'. Retrieved August 3, 2021, from https://www.forescout.com/resources/2019-sans-state-of-ot-ics-cybersecurity-survey/. (Cit. on p. 165)

Schell, J. (2008). '**The art of game design: A book of lenses**'. Morgan Kaufmann Publishers. https://dl.acm.org/doi/book/10.5555/2167319. (Cit. on p. 38)

Schmidt, B. (2002). '**Modelling of Human Behaviour The PECS Reference Model**'. *Artificial Intelligence*, (100), 13–18 (cit. on p. 26).

Schurman, K. (2012). '**Lulzsec: How a handful of hackers brought the us government to its knees: 50 days of lulz**'. Hyperink Inc. https://books.telegraph.co.uk/Product/Kyle-Schurman/LulzSec-How-A-Handful-Of-Hackers-Brought-The-US-Governmen/14145036. (Cit. on p. 25)

Security Audit Systems. (2021). '**Web application penetration testing | security audit systems**'. Retrieved May 26, 2021, from https://www.security-audit.com/application-penetration-testing/. (Cit. on p. 36)

Seebruck, R. (2015). '**A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model**'. *Digital Investigation*, *14*, 36–45. https://doi.org/10.1016/j.diin.2015.07.002 (cit. on pp. 24, 25)

Sen, R., Verma, A. & Heim, G. R. (2020). '**Impact of Cyberattacks by Malicious Hackers on the Competition in Software Markets**'. *Journal of Management Information Systems*, *37*(1), 191–216. https://doi.org/10.1080/07421222.2019.1705511 (cit. on p. 25)

Shah, S. & Mehtre, B. M. (2014). '**An overview of vulnerability assessment and penetration testing techniques**'. *Journal of Computer Virology and Hacking Techniques*, *11*(1), 27–49. https://doi.org/10.1007/s11416-014-0231-x (cit. on pp. 11, 12)

Shah, Y., Choyi, V. & Subramanian, L. (2015). '**Multi-factor authentication as a service**'. https://doi.org/10.1109/mobilecloud.2015.35 (cit. on p. 20)

Sharma, S. & Warkentin, M. (2019). '**Do i really belong?: Impact of employment status on information security policy compliance**'. *Computers & Security*, *87*, 101397. https://doi.org/10.1016/j.cose.2018.09.005 (cit. on p. 21)

Shodan. (2021). '**Shodan search engine**'. Retrieved May 20, 2021, from https://www.shodan.io/. (Cit. on p. 4)

Sidorenko, T., Hodges, D. & Buckley, O. (2020). '**Board games as a behavioural collection method**'. https://doi.org/10.17862/CRANFIELD.RD.13296014.V1 (cit. on pp. 24, 25, 124)

Silverman, D. (2017). '**Doing Qualitative research**' (M. Steele, Ed.; 5th ed.). SAGE Publications. https://uk.sagepub.com/en-gb/eur/doing-qualitative-research/book251108. (Cit. on pp. 45, 56)

Sinigaglia, F., Carbone, R., Costa, G. & Zannone, N. (2020). '**A survey on multi-factor authentication for online banking in the wild**'. *95*, 101745. https://doi.org/10.1016/j.cose.2020.101745 (cit. on p. 20)

Sky News. (2018). '**Uk infrastructure being targeted by hackers**'. Retrieved May 16, 2021, from https://news.sky.com/story/uk-infrastructure-being-targeted-by-hackers-11319033. (Cit. on p. 25)

Snieder, R. & Larner, K. (2009). '**The Art of Being a Scientist**'. Cambridge University Press. https://doi.org/10.1017/cbo9780511816543. (Cit. on p. 50)

Snyder, M. (1974). '**Self-monitoring of expressive behavior.**' *Journal of Personality and Social Psychology*, *30*(4), 526–537. https://doi.org/10.1037/h0037039 (cit. on pp. 126, 139)

SOAR. (2021). '**What is soar?**' Retrieved May 12, 2021, from https://soar.eecs.umich.edu/. (Cit. on p. 29)

Soares, A. N., Gazzinelli, M. F., de Souza, V. & Araújo, L. H. L. (2015). '**The role playing game (RPG) as a pedagogical strategy in the training of the nurse: An experience report on the creation of a game**'. *Texto & Contexto - Enfermagem*, *24*(2), 600–608. https://doi.org/10.1590/0104-07072015001072014 (cit. on p. 37)

Sophos. (2019). '**Sophos 2020 threat report**'. https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophoslabs-uncut-2020-threat-report.pdf (cit. on pp. 3, 5, 6)

Steiger, S. (2016). '**Maelstrom - are you playing with a full deck? : Using a newly developed attack life cycle game to educate, demonstrate and**

evangelize'. Retrieved May 27, 2021, from https://youtu.be/n-xsYvjOyk8. (Cit. on p. 39)

Sterling, B. (1998). '**The hacker crackdown: Law and disorder on the electronic frontier**'. Open Road Media. (Cit. on p. 5).

Sterman, J. D. (2001). '**System Dynamics Modeling: Tools for Learning in a Complex World**'. *California Management Review*, *43*(4), 8–25. https://doi.org/10.2307/41166098 (cit. on pp. 30, 31)

Stobert, E. & Biddle, R. (2013). '**Memory retrieval and graphical passwords**'. *Proceedings of the Ninth Symposium on Usable Privacy and Security - SOUPS '13*. https://doi.org/10.1145/2501604.2501619 (cit. on p. 20)

Strom, B. (2019). '**ATT&CK 101 - MITRE ATT&CK™- Medium**'. Retrieved October 29, 2019, from https://medium.com/mitre-attack/att-ck-101-17074d3bc62. (Cit. on p. 103)

Stuttard, D. & Pinto, M. (2011). '**The web application hacker's handbook: Finding and exploiting security flaws**'. John Wiley & Sons. (Cit. on p. 10).

Sun, R. (2006). '**The CLARION cognitive architecture: Extending cognitive modeling to social simulation**'. *Cognition and multi-agent interaction*, 79–99 (cit. on p. 29).

Tamara Denning, A. S. & Kohno, T. (2014). '**Practical lessons from creating the control-alt-hack card game and research challenges for games in education and research**'. *2014 USENIXSummit on Gaming, Games, and Gamification in Security Education*. https://www.usenix.org/conference/3gse14/summit-program/presentation/denning. Video timestamp: 01:13 (cit. on p. 39)

Tang, A. (2014). '**A guide to penetration testing**'. *Network Security*, *2014*(8), 8–11. https://doi.org/10.1016/s1353-4858(14)70079-0 (cit. on p. 11)

The National Archives/Cabinet Office (NA). (2017). '**'Responsible for Information' for SMEs**'. Retrieved October 27, 2021, from http://web.archive.org/web/20170206002608/http://www.nationalarchives.gov.uk/sme/. (Cit. on p. 8)

Trend Micro. (2021). '**A Constant State of Flux Trend Micro 2020 Annual Cybersecurity Report**'. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2021 (cit. on pp. 4, 6, 25)

van der Hoog, S. (2016). '**Deep Learning in Agent-Based Models: A Prospectus**'. *SSRN Electronic Journal*, 1–19. https://doi.org/10.2139/ssrn.2711216 (cit. on p. 34)

Veksler, V. D., Buchler, N., Hoffman, B. E., Cassenti, D. N., Sample, C. & Sugrim, S. (2018). '**Simulations in cyber-security: A review of cognitive modeling of network attackers, defenders, and users**'. *Frontiers in Psychology*, *9*(MAY), 1–12. https://doi.org/10.3389/fpsyg.2018.00691 (cit. on pp. 9, 12, 13)

Verdugo, J. & Rodrìguez, M. (2019). Assessing data cybersecurity using ISO/IEC 25012. *Communications in computer and information science* (pp. 33–46). Springer International Publishing. https://doi.org/10.1007/978-3-030-29238-6_3. (Cit. on p. 18)

Viana, J., Simonsen, T. B., Dahl, F. A. & Flo, K. (2018). '**A HYBRID DISCRETE EVENT AGENT BASED OVERDUE PREGNANCY OUTPATIENT CLINIC SIMULATION MODEL**'. *2018 Winter Simulation Conference (WSC)*. https://doi.org/10.1109/wsc.2018.8632282 (cit. on p. 34)

Volexity. (2020). '**Oceanlotus: Extending cyber espionage operations through fake websites**'. Retrieved May 2, 2021, from https://www.volexity.com/blog/2020/11/06/oceanlotus-extending-cyber-espionage-operations-through-fake-websites/. (Cit. on pp. 4, 25)

von Solms, R. & von Solms, B. (2004). '**From policies to culture**'. *Computers & Security*, *23*(4), 275–279. https://doi.org/10.1016/j.cose.2004.01.013 (cit. on p. 21)

Walton, R. (2006). '**The computer misuse act**'. *Information Security Technical Report*, *11*(1), 39–45. https://doi.org/10.1016/j.istr.2005.11.002 (cit. on p. 5)

Warner, M. (2012). '**Cybersecurity: A pre-history**'. *Intelligence and National Security*, *27*(5), 781–799. https://doi.org/10.1080/02684527.2012.708530 (cit. on p. 4)

Watad, M., Washah, S. & Perez, C. (2018). '**It security threats and challenges for small firms: Managers' perceptions**'. *International Journal of the Academic Business World*, *12*(1), 23–30. https://www.jwpress.com/Journals/IJABW/BackIssues/IJABW-Spring-2018.pdf#page=29 (cit. on p. 8)

Watters, P. A., McCombie, S., Layton, R. & Pieprzyk, J. (2012). '**Characterising and predicting cyber attacks using the cyber attacker model profile (CAMP)**'. *Journal of Money Laundering Control*, *15*(4), 430–441. https://doi.org/10.1108/13685201211266015 (cit. on p. 170)

Weber, E. U., Blais, A.-R. & Betz, N. E. (2002a). '**A Domain-specific risk-attitude scale: Measuring risk perceptions and risk behaviors**'. *Journal of Behavioral Decision Making*, *15*(4), 263–290. https://doi.org/10.1002/bdm.414 (cit. on p. 140)

Weber, E. U., Blais, A.-R. & Betz, N. E. (2002b). '**A domain-specific risk-attitude scale: Measuring risk perceptions and risk behaviors**'. *Journal of Behavioral Decision Making*, *15*(4), 263–290. https://doi.org/10.1002/bdm.414 (cit. on p. 126)

Whitton, N. (2010). '**Learning with digital games: A practical guide to engaging students in higher education**'. Routledge. (Cit. on pp. 38, 84).

Wikipedia. (20021). '**List of security hacking incidents**'. Retrieved December 13, 2021, from https://en.wikipedia.org/wiki/List_of_security_hacking_incidents. (Cit. on p. 53)

Wilensky, U. & Rand, W. (2015a). '**An introduction to agent-based modeling**'. (Cit. on p. 32).

Wilensky, U. & Rand, W. (2015b). '**An introduction to agent-based modeling**'. (Cit. on p. 129).

Williams, M. (2016). '**Key Concepts in The Philosophy of Social Research**' (1st ed.). SAGE Publications. (Cit. on pp. 46, 48, 49).

Xynos, K., Sutherland, I., Read, H., Everitt, E. & Blyth, A. (2010). '**Penetration Testing and Vulnerability Assessments: A Professional Approach**'. *Proceedings of the 1st International Cyber Resilience Conference*, *2*(August), 150–155. http://ro.ecu.edu.au/icr/16/ (cit. on p. 35)

Yeo, J. (2013). '**Using penetration testing to enhance your company's security**'. *Computer Fraud & Security*, *2013*(4), 17–20. https://doi.org/10.1016/s1361-3723(13)70039-3 (cit. on pp. 11, 12)

Yin, R. K. (2009). '**Case study research: Design and methods**' (4th ed.). SAGE. (Cit. on p. 52).

Yu, S. (2019). '**Cyber defense matrix reloaded**'. Retrieved August 4, 2021, from https://www.slideshare.net/sounilyu/cyber-defense-matrix-reloaded. (Cit. on p. 8)

yubico. (2021). '**Yubikey strong two factor authentication**'. https://www.yubico.com. (Cit. on p. 20)

Zainudin, Z. S. & Molok, N. N. A. (2018). '**Advanced persistent threats awareness and readiness: A case study in malaysian financial institutions**'. *2018 Cyber Resilience Conference (CRC)*. https://doi.org/10.1109/cr.2018.8626835 (cit. on p. 10)

Zhang, Y., Xiao, Y., Ghaboosi, K., Zhang, J. & Deng, H. (2011). '**A survey of cyber crimes**'. *Security and Communication Networks*, *5*(4), 422–437. https://doi.org/10.1002/sec.331 (cit. on p. 23)

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F. & Basim, H. N. (2020). '**Cyber security awareness, knowledge and behavior: A comparative study**'. *Journal of Computer Information Systems*, 1–16. https://doi.org/10.1080/08874417.2020.1712269 (cit. on p. 6)

Zyda, M. (2005). '**From visual simulation to virtual reality to games**'. *Computer*, *38*(9), 25–32. https://doi.org/10.1109/mc.2005.297 (cit. on p. 38)

Нефёдова, М. (2021). '**MEGANews. Самые важные события в мире инфосека за март**'. Retrieved April 5, 2021, from https://xakep.ru/2021/04/01/meganews-264/. (Cit. on p. 1)