THE INTERNET OF THINGS GAME: REVEALING THE COMPLEXITY OF THE IOT

Haider Akmal
Lancaster University
Lancaster, United Kingdom
h.a.akmal@lancaster.ac.uk

Paul Coulton
Lancaster University
Lancaster, United Kingdom
p.coulton@lancaster.ac.uk

ABSTRACT
The Internet of Things (IoT) is a phenomenon wherein everyday objects are capable of interacting together through the Internet; producing complex interdependencies between human and non-human actants. However, much of this complexity is not legible to users of IoT and can produce concerns relating to areas such as privacy and security, when the *independent-but-interdependent* motivations and perspectives of the actants are incongruent. To address this issue this paper presents *The Internet of Things Board Game*, which has been designed such that its procedural rhetoric makes legible these *independent-but-interdependent* relationships; and reveal how they manifest in the management of our security and privacy within IoT. The results of play-testing the game through multiple iterations highlight the valuable contribution games can play in revealing the ever-increasing complexity of relationships between the digital and the physical, and the human and non-human.

Keywords
procedural rhetoric, board game, internet of things, game design, games for research

INTRODUCTION
Bogost's (2007) procedural rhetoric is often cited alongside discussions of games as an approach capable of revealing the operations of complex systems in a way that is more accessible to a non-expert audience. While Bogost acknowledges that such games involve a level of persuasion enacted through sequences of computational processing, which he refers to as "persuasive games", the primary consideration of it, is as an approach that utilises the power of rhetoric to reveal to players underlying processes as a series of sequential arguments (Coulton and Hook 2017). Antle and Robinson paraphrase Bogost's definition as:

> *"Procedural Rhetoric is based on the notion that the processes and activities that participants engage in during play are more persuasive than the information that is layered on top of those processes." (Antle and Robinson 2011)*

Therefore, by structuring the process of play in a manner that concretizes underlying information the concepts embodied may be relayed more effectively. They go on to explain, how the playing of games that are developed using a model of procedural rhetoric's may, "communicate a message about related [underlying] issues". The use of real-world sources of information within gameplay may provide "perceptual anchors" for players in the game to associate with their real-life experiences, aiding in the credibility of the rhetoric (Coulton 2015).

Proceedings of DiGRA 2020

This study aligns itself with the use of procedural rhetoric's as a core method in the designing of its key artefact; *The Internet of Things Game*. This game was created with the intention of inducing a practical understanding of the workings of the Internet of Things (IoT) through gameplay. The area it most concerns itself with, is the security of IoT enabled systems and devices. Farooq et al. (2015) are of the view that IoT, in the coming years, has the potential to be a "security disaster" if measure aren't taken towards its fortification.

With intimate and mundane aspects of our lives—like buying clothes or visiting a restaurant with friends—leaving behind a digital trace through our devices, the data we accumulate over the course of our lives has become a "prized commodity" for companies vested in it (West 2019). Given such "data capitalism" has brought with it a rise in cases involving the misuse of data[1], security is no longer the sole matter of concern that could affect the adoption of IoT; as privacy, ethics, risk etc. are also brought into sharp focus. Games may play a role in helping develop an understanding of IoT for the general public.

Whilst the process of designing the game has been presented elsewhere (Akmal and Coulton 2019), some contextualization of the background to the game is require before focusing on the experiences produced.

Insecurities and the Internet of Things

IoT, is the name given to a phenomenon where objects are connected to the Internet. Without going into the technical specifics of how IoT functions, the gist is that through the inclusion of digital networking and computational power, everyday objects are given the capacity to interact with each other via the Internet. Objects of different kinds are available for domestic and industrial applications, which are able to enhance their general functionality through these interactions. These devices are often found associated with the term 'smart' (Smart TV's, Smart Phones, etc.). This research was part of a project called the PETRAS IoT Hub[2] which is an exploratory dive into critical topics around IoT, such as the adoption and acceptability of IoT devices. Lindley et al. (2017a) equate the adoption of new technology to the opening of Pandora's box, where possibilities emerge as people interact with technologies in their environments. Designers attempt to tame this through methods such as human-centered design, though arguments against such approaches point to its inherent messiness and need to acknowledge the role of non-human actants within the IoT (Lindley et al. 2017; Coulton and Lindley 2019).

IoT presents a unique challenge space for designers and developers alike, owing to the oft personal nature of interactions that IoT enabled systems create. This is mainly due to the context in which interactions occur, where information—often of a sensitive nature—is stored, and ultimately who is given access to this information. The privacy and security of such systems has been a topic of concern among users (Farooq et al. 2015; Weber 2010; Gürses et al. 2006; Roman et al. 2011), and when issues are identified hardware and or software revisions are often required. The complexity of IoT enabled systems is by far the biggest hurdle in resolving these issues, as the price of resolving a particular issue might be to accept either an unsupported device, or changes in the terms and conditions over how your data is handled.

Disenchantment of IoT and its adoption

Often users describe their experience of emerging technologies as magical, akin to Arthur C. Clarke's 3rd law that "any sufficiently advanced technology is indistinguishable from magic" (Clarke 1962). However, the adoption of this consideration of technology as magic can be seen as problematic, as it effectively absolves users of the need to understand technology's hidden workings or for designers

to make them legible. This can result in disillusionment when users discover their technology is actually doing something in a way that challenges their existing values[3].

It doesn't help that human-centered design inherently encourages keeping underlying processes hidden in an attempt of simplification (Norman 1999; Lindley and Coulton 2017). The result is a complex network of hidden interactivity occurring when undertaking seemingly simple tasks, with little guarantee of the security of those interactions; such as, the potential security hazards of using a mobile phone to turn on a light bulb. In truth, these simple tasks are not as simple as they seem, because of an array of complex interactions taking place in a concealed digital landscape overlapping our lives.

More-than human-centered design

IoT is a poorly defined construct (Lindley and Coulton 2017) with its operating characteristics primarily dependent on the creators and operators of the products and services it encompasses. Coulton and Lindley (2019) suggest a "more-than human-centered" approach towards designing for IoT that more fully represents their underlying operation. This view incorporates the myriad non-human things (IoT devices, business models, regulations, etc.) that make up the IoT, along with users and their devices. They take inspiration from Object-Oriented Ontology (OOO), a branch of philosophy dealing with the nature of objects. Harman (2018) explains OOO as a viewpoint that sees humans and non-humans having no precedence over each other, in essence, placing them on a level playing field or a "flat ontology". To simplify, this philosophy makes no distinction between humans and non-humans and see all as *Objects or 'things.'* Coulton and Lindley (2019), in turn, use this philosophy in an attempt to raise arguments against the more common preference of human-centered design for IoT.

The foundations of *The Internet of Things Game* lie within an exploration of the use of this object-oriented philosophy, as a framework, for reimagining designing for IoT (Akmal and Coulton 2018). This paper does not attempt to enter the philosophical rabbit-hole that lead to its formulation. Instead, it focuses on the use of the procedural rhetoric ideology as a key element in the exploration of *more-than human perspectives for IoT*, to enable players to develop a deeper insight into the activities present within IoT systems.

A key point pertaining to the philosophy that should be mentioned, is of the use of the metaphor of "constellations" as a way to view IoT (Coulton and Lindley 2019). This metaphor allows a way of concretising the *more-than human* approach, by projecting a flat ontology revealing the underlying *independent-but-interdependent relationships* between things (see Figure 1). To explain this, Coulton et al (2019) give the example of a Smart Lock. Though intended to function similar to regular key locks, IoT enabled smart locks give users enhanced functionality for ease and security purposes. For instance, they can be accessed through a smart phone, but also, through cloud-based servers. They can be programmed to trigger with different actions/reactions; proximity, location, time, etc. This also means that though a physical key is kept on one's person, the actual digital 'key' in a smart lock is stored either on the cloud or the device itself. Furthermore, if the lock is shared with other users (such as through AirBnB), more points of connectivity emerge. One's security is now no longer a personal matter, rather, it concerns the user(s), the device(s), the lock company, additional data brokers, internet access providers, etc. For the user, this all amounts to a singular action of access via a smart phone, but behind that independent action are interdependencies creating the metaphorical constellation of IoT. This metaphor became the main driving force for the design of the game.

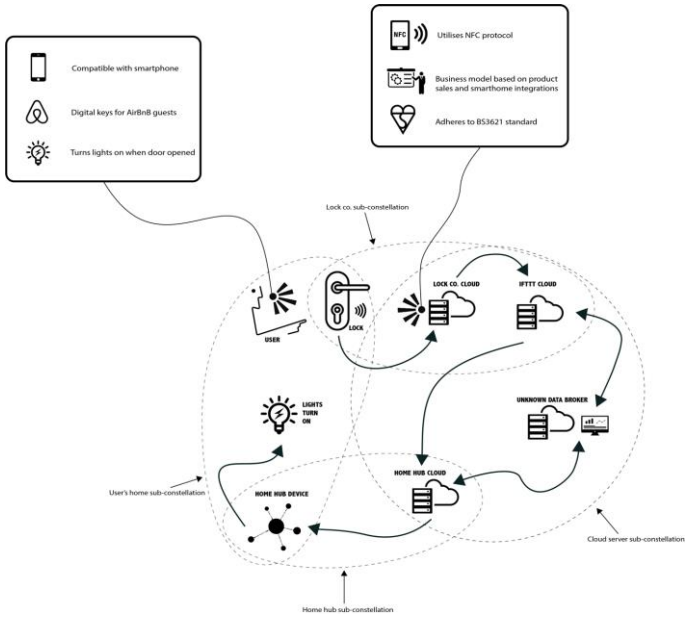

Figure 1: Constellation map (Coulton and Lindley 2019) suggesting multiple perspectives within IoT of a Smart Lock

In the coming sections we will be introducing the game in more detail, along with how and where procedural rhetoric played a part. As the game underwent an iterative development process, all findings and discussions were an outcome of a series of playtests outlining the manner in which the game evolved over time. This is akin to a Research through Design (RtD) methodology (Coulton and Hook 2017) and as such, we see the game as a design artefact intended for a specific purpose rather than a commercial product. All findings are subjected to scrutiny by player reactions and our own empirical study of the playtests. To begin with, what is *The Internet of Things Game* and how do you play it?

THE GAME

The Internet of Things Game in a nutshell, is a collaborative strategy-based board game that involves players working together within the fictional settings of the game to achieve a common goal of security. It began as an artefact to visualize concepts of spatial philosophy in its originating design research, to discuss a relationship between physical and digital spaces (Akmal and Coulton 2018). Interactions that happened within those spaces were the initial core mechanic of play. Players attempted to amass as many connections as they could, with the aim of creating the independent and interdependent relationships of a *more–than human* perspective. Very soon, this mechanic proved tedious and to no end; so, the artefact (as it yet could not be called a game) took on its first iteration. Over time the iterations piled up and the artefact evolved into a game as is oft seen in game development processes.

Initially the game was to be competitive, but soon, the realization came that in order to embed a *more-than human* view of IoT in the game, this format of gameplay would not be applicable. Zagal et al. (2006) place collaboration and competition at opposite ends of a spectrum where the later focuses on personal achievement the former encourages mutual victory by teamwork towards a singular goal. They go on to express how this format helps to "maximize [a] team's utility". This can be seen by the studies of Berland and Lee (2011) in collaborative gaming, that through this coordination between players a "parallel processing" is achieved, effectively teaching the workings of a game without all players having to read the rules. Keeping this logic in mind further iterations of the

game became more collaborative focused, as this better reflected the interdependencies in IoT.

Taking Inspiration

Inspiration for the design of the game was taken from popular mainstream games *Dead of Winter: A Crossroads Game* (Gilmour 2014), *Betrayal at House on the Hill* (Glassco et al. 2004), and *Eldritch Horror* (Fantasy Flight Games 2013), with many of the mechanics being borrowed from them.

Bogost (2011) when speaking of games describes them as "models of experiences rather than textual descriptions or visual depictions of them". The point he raises is that through games one can be placed "in the shoes of someone else", ergo, allowing us to play different roles in different constraints defined within those modelled experiences. This is why games utilize storytelling to allow this exploration of experience. For our game a similar background fiction was established in which the actions of play could exist and later be further defined to model the experience of play.

The backstory resides in a fictional future space as another world technologically parallel to our own. The difference being, all workings are governed by a conglomerate turned government entity known as *The Council*. In this world data has become high commodity, and *The Council* undertakes nefarious activities to keep their hold on global information. Players are part of a group of rebels intending to create their own data-secure spaces where they are in charge of how their data is scrutinized. As such, the main goal of the game becomes the securing of spaces (Tiles) on the board. Conversely, the game acts as an adversary attempting to thwart players' actions, by raising the level of threats throughout the game bringing players closer to failure.

This concept of taking ownership of data through own measures comes from another research project called the *DataBox* (Mortier et al. 2016). The ideology was included in gameplay, keeping the name as well. It was decided early on that the artefact/game should not be focused on the fiction and instead, be more involved with real life research and existing technologies to aid in the procedural rhetoric. Bogost (2011) discusses how world-building can create empathy through games giving the examples of *Darfur is Dying* (Ruiz et al. 2006) and *E.T.* (Warshaw 1982), this can also be achieved he says through "vignettes" as brief descriptions or accounts of characters and events. *Eldritch Horror* creates its air of Lovecraftian fiction through this vignette approach. This concept helped in creating the illusion of a story through the game that further aided in the procedural rhetoric (see Figure 2).

Figure 2: *Eldritch Horror* (left) and *The Internet of Things Game* (right) storytelling through vignettes

Game Contents and Play Through

Tiles and Movement

The game board (in its most current iteration) is comprised of 40 hexagonal tiles coming together in a honeycomb formation, with notches in the corner for placing tokens (see Figure 3). These tiles are all named as physical locations such as a living room, kitchen, etc. and act as physical spaces[4] with which players react. Some spaces are bordered to indicate them as inherently insecure triggering further actions from players that enter them. The spaces function in a manner of ways. Firstly, as a mode of navigation players may enter and exit them. Second, the spaces are used to find items or interact with present permanent items as a requirement to continue play. Third, and perhaps the most important function is to simulate connectivity; players use items they have in hand, or those in the spaces, to fill up the corner notches of each tile denoting the presence of a digital connection in that physical space. Each space, subsequently, has a connection requirement which needs to be fulfilled before it can be secured by turning into a *Databox*.

Figure 3: Full spread of *The Internet of Things Game*

Dice-Count and Skills

Players are dealt a hand of cards each and an avatar to control with its own skill set and unique abilities (see Figure 4). These skills are dice counters, the number associated with them mean how many dice players can roll for that skill—a mechanic taken from *Eldritch Horror*. For instance, *Spook* is an avatar in the game and has a *Security Skill* of 2 which means when the player controlling *Spook* has to roll for *Security*, they get 2 dice to roll with. This dice-count mechanic becomes an integral part of play as different items in hand increase and/or decrease different player skills. So, the same player controlling *Spook* if also has a *Key Card* item, which increases their *Security Skill* by 2, allows them to roll 4 dice as long as that card is in hand. The reason a player would need to have multiple dice is to increase their chances of having a successful roll; a 5 or a 6 on any one dice. By introducing an amount of chance through the dice in the game we mimic the fallibility of IoT systems which though claim to be secure and private, cannot truly ever be.

Throughout the game, these skills become a resource to be managed through items in hand. Initial iterations saw up to six skills being used in the game which in its current iteration has been reduced to three: *Security*, *Observation*, and *Coding*.

Figure 4: Cards in hand increase skills and decrease avatar skills

Actions and Phases

Play occurs in rounds consisting of 2 phases for each player: An *Action Phase*, and a *Risk Phase*[5]. The action phase has the current player enact 2 actions from a list of possible actions allowing players to move, find items, rest, trade items, discard cards, make connections, deploy a *Databox*, or skip their turn. After this, play enters the risk phase where the player must roll for *Security* according to their current security skill level. This is done to see if their actions were secure in that turn, as a way to view the potential consequences of actions within IoT. On a successful roll, play continues to the next player otherwise the player is forced a penalty. Firstly, placing a vulnerability token in the space and all spaces connected to it through the connection tokens, and then playing the top-most card of the *Risks Deck* (more on that ahead). This act of a vulnerability seeping into other physical spaces through digital connections, was one of the ways employed to enact the constellation metaphor in-game. Though not a one-to-one recreation of the metaphor, it presented a direct relation of IoT having hidden linkages.

Tokens and Threats

As play progresses, these linkages become more apparent through tokens that appear throughout the board. Where on the one hand they denote a visual representation of actions conducted in the game, they also serve the purpose of adding to the urgency of play. To start with, we have the previously mentioned *Connectivity Tokens*. These tokens represent physical spaces being connected through digital interactions and physically link tiles on the board. They also appear on player cards, where they denote personal activity. The intention here was to create further subliminal linkages between IoT enabled spaces and their inhabitants.

The next set of tokens present a series of dangers for players. Firstly, we have *Vulnerability Tokens* which appear when players fail certain actions such as the Risk Phase. They easily permeate the board and can be removed with little effort. Over time though, if allowed to accumulate, they may convert into *Threats* which are harder to remove. These tokens play a part in raising the threat level of the game through a *Threat Tracker* similar to the *Doom Track* found in *Eldritch Horror* (see Figure 5). The purpose of the *Threat Tracker* is to count down the end of the game for players. There are also *Privacy Tokens* which act as ticking time bombs, simulating the inevitable fallacy of privacy within IoT enabled spaces. Over the course of play these can turn into multiple vulnerability tokens that appear in succession further creating threats.

Figure 5: *Eldritch Horror Doom Track* (left) compared to *The Internet of Things Threat Tracker* (right) mechanic

Decks

The game consists of 4 decks of cards: *Items*, *Risks*, *Privacy*, and *Daemons*. The *Item Deck*, houses item cards which contain different everyday objects available as IoT enabled devices. Item cards act as the main source for creating connections on the game board (see Figure 6a). Players return items to the game in order to place connection tokens in empty notches around the space their character occupies, at the same time keeping a tally of connections on their person through tokens. The items also include special cards which increase skills, give special abilities, and act as necessary objects or resources to have in hand. For instance, each player requires a primary card in the form of a *Smart Phone* or *Tablet* in order to make connections on the board. Without this card, though they cannot make connections, they can still interact with the game in other ways.

Figure 6: Item Cards (a), Risk Cards (b), Privacy Cards (c), and Daemon Cards (d)

The *Risks Deck*, houses counter measures that the game executes on behalf of *The Council*. It contains a series of insecurities that afflict IoT enabled systems. Players have to endure these effects if they fail to avoid the risk phase. These are targeted attacks by the game that use the dice-count mechanic to affect players (see Figure 6b). For example, the *Cyber Attack* card implies a player's items have been infected. In order to continue, they need to use the collective dice-count of their *Security*, *Observation*, and *Coding* skills but, they must reduce that total by 3 before rolling. This needs to be done for each item they have on hand; with each having its own unique consequence in the event of a failed roll. The risk phase can also issue permanent damage to the player. Finally, it enforces a sense of urgency among players by raising the overall threat level of the game.

The last two decks are *Privacy* and *Daemons*[6]. The *Privacy Deck* is played when a player attempts to deploy a *Databox*—a requirement for winning the game. Taking inspiration from the way cards are played in both *Eldritch Horror* and *Dead of Winter*, the privacy cards act out a scenario where players are entered into a dialog with the

game through the use of dice rolls and vignettes. Essentially, conditional statements in the form of cards. Players must successfully navigate the different conditions otherwise face consequences (see Figure 6c). For example, *The False Prince* card describes a story of receiving the stereotypical exotic prince email scam and makes a player roll for *Observation*. A successful roll means they enter the conditional loop, to cross the second step the card wants a further successful *Coding* roll. Completing the conditional statement successfully awards the player a *Databox* token which they place in the space. This marks the space as secured and incapable of receiving any more vulnerability tokens in further play. Failing any of the conditions on the other hand, immediately breaks the loop and the card issues a consequence.

The *Daemons Deck* takes the conditional statement further by acting like software daemons: programs that run in the background affecting systems in various ways. In this instance the cards slow down players, reducing their skills and ability to play. They can only be removed by spending precious actions (see Figure 6d).

FINDINGS

Having discussed the game in detail, we can now move on to the player generated feedback. The game underwent 14 iterations and 10 playtests with a total of 22 players, some returning for multiple sittings. Players ranged between the ages of 25 and 60, coming from different backgrounds including their knowledge of IoT. The majority of the players were in the 25-35 age bracket. Though all players were familiar with board games very few had played collaborative games before. It was important to include players who were less aware of IoT security and/or its workings to see how much of the rhetoric went across during play.

On the use of games in research, Donchin (1995) is of the view that in order to make a game useful for a researcher, it must be designed in a way that "systemic control" can be exercised through parameters of play. He goes on to say, the game will remain "impoverished" unless it also is capable of being replayed for further results. The playability and re-playability of the artefact as a game were always of importance to the research. In our view, without the game being able to keep players occupied within its narrative, it would not have been able to function enough for the rhetoric to come across. As for systemic control, in many ways the procedural rhetoric established the control itself within play. Where on the one hand, the main proponent for the creation of vulnerabilities within the game is chance—vis-á-vis a dice roll—control was handed over to players to forge secure spaces through their actions. The parameters of research in this regard were not similar to Donchin's *Space Fortress*, rather the research revolved around the conveying of information in a manner that was both conducive for novices and experienced people alike.

This is why the initial variants of playtests, involved the use of a facilitator who acted as *Game Master (GM)* presenting actions for the players. This should not be confused with how a GM functions in a role-playing game like *Dungeons & Dragons* (Gygax and Arneson 1974). Where players in *D&D* still have full autonomy over their actions and the GM functions as orator or higher presence in play, here, the GM functioned as a facilitator of play similar to how one would facilitate a participatory design workshop. This was due to the nature of the RtD methodology, which invoked the presence of a facilitator/researcher to be able to evaluate the experience.

As this still kept the artefact far from being a fully playable game, future iterations focused on keeping the factor of systemic control within the game itself rather than through an external source. This is why in later iterations the GM was discarded, and instead the facilitator/researcher became simply a player in the game.

In the context of a video game, control can be made more apparent through programming while in a board game control becomes limited. Furthermore, several other parameters, such as reaction times, can be extracted from the playing of a video game that can only be done in a board game through an empirical study. That said, the findings of this study can be seen from two perspectives: its ability to play as a game, and its ability to transfer its procedural rhetoric (*more-than human-ness*) through play.

Gameplay

The focus of initial playtests was around creating an experience suitable for play, which also, did not conflict with the narrative or interest of the research. From the start it was clear that the board game medium was capable of easily visualizing the connectivity of IoT, and in a way added to the dialog of 'constellations' (see Figure 7). This was heightened by player feedback which mentioned the visual aspect most out of all other points. It was easier to imagine IoT in this format when they could see the connections happening in front of them. But it soon became apparent that visualizing IoT was not enough to present the message across, as players did not understand the purpose of the artefact in the beginning. Comments ranged from, "It feels boring", to "pointless", and "mundane". This was all coming from the fact that the artefact was treated as a research tool to begin with. The goals that were originally set by the artefact were not enough to create compelling gameplay[7].

Figure 7: During play the *constellation* metaphor became more enhanced through visualization

It was not until the 10th iteration where players were feeling engaged by the game. This was the version that introduced the fictional backstory and the avatars for players to control in game. Till this point, the game was still using rudimentary prototyping techniques, and it was noted that this impacted players attention levels and reaction to the game. The next iteration was designed to tackle that, and the game was redesigned using more conventional board game materials such as grey board and plastic/wooden pieces. The response from players was highly positive claiming the changes made it feel and play more like a game.

Rhetoric

Regarding the rhetoric of IoT privacy/security and the notion of *more-than human-ness*, there were mixed reactions. Where it successfully translated over to some players, others were still seeing it as a game and less true to life even though our efforts were to keep it as close to reality. Those that were aware of IoT interactions did laude the accuracy though. The urgency of threats was still a difficult concept to get across, what did come across the easiest was the notion of fragility through the various vulnerabilities. The game managed to at once bring players closer to an understanding

of IoT and also isolate them. Where some players tackled it as a strategy game focusing on its inherent playability and extracting as much entertainment from that, others mentioned how they *forgot* about IoT in the process of playing.

There were moments when the connection became vividly apparent. One player mentioned how by hearing others use phrases like, *"I'm about to connect the Living Room to the Kitchen with my Shoes!",* helped in imagining the premise of the game further. As a take back, though this does assert the notion of a *more-than human* centered IoT, it should be noted this was not mentioned by the players but rather came from an empirical viewing of the playtest.

Players further expressed how the game could be enhanced by introducing more direct referencing to the idea of security in IoT, where in its current format the message felt more negative than positive. *"It feels like the game is out to get you!"*, was one comment referring to how the counter measures made it seem like their attempts at creating secure spaces was constantly in vain. In some respects, this holds true as security requirements are constantly evolving. Rather than presenting security as a problem that could be fixed, we wanted to highlight it requires constant attention and vigilance.

The introduction of fiction helped the rhetoric considerably over the playtests. It became clear that the stimulation of imagination was an important factor in pushing the rhetoric forward, as players began to associate the narrative with their own lives. An earlier iteration of the privacy cards involved a card that described a scenario of data being stolen from a phone through an *RFID* interaction. This created a stark reaction from players, as they began relating it to events that could happen in their real lives. The game world managed to seep into reality which was a positive take away from the process.

Regarding how much of the philosophical research the game was based on came across to players, is another story. Many parts of the game still associated with its original source; a few of which have been explained previously. The entering and exiting of spaces, hinted towards the spatial philosophy roots of the game. The interdependence of IoT objects and services was scattered throughout play. Furthermore, the privacy deck was riddled with *Easter Eggs* from OOO, to give an illusion of internal agency for IoT. The objective was to keep the game far from being simply a design tool but a game that could exist on its own merit. Hence, the iterative process included a systemic removal of its *tool-ness* over time. But elements such as these were purposefully left behind, and during the playtests they were brought up as potential points of discussion.

Unfortunately, the effectiveness in translating the philosophy across is difficult to measure. Where most players took the philosophy at face value disregarding it as humorous anecdote, those that did engage with it slightly, didn't push it far enough to warrant enough discussion. Having said that, player responses paint a picture of the object-oriented philosophy being subtly embedded within their reactions.

DISCUSSION & CONCLUSION

In a time where data has become an "important commodity" (Evans 2018), companies increasingly attempt to widen their grasp on consumer data by offering purpose for the connectivity of consumers. This raises concern over how to improve these systems to avoid problem spaces and enhance efficiency, while keeping the digital rights of users unharmed. *The Internet of Things Game* presented an opportunity to tackle these concerns by imagining a simplification of IoT; for both experienced and novice users. And through its procedural rhetoric, the potential to demystify (to a certain degree) the underlying workings of IoT enabled devices. The *more-than human* approach for IoT,

allows for the intermingling of notions of digital/physical with human/non-human. The medium of a game afforded a synergy of theory and practice.

Antle and Robinson (2011) are of the agreement that games that utilize procedural rhetoric have the potential for "public engagement", especially if the rhetoric is made "sufficiently entertaining". They structure their argument around the use of procedural rhetoric in games that process larger issues, such as sustainability intended to affect wider audiences. They mention how the act of playing a game designed in this fashion is capable of creating a "state of mind" in the player regarding those issues, effectively communicating the message across.

Earlier iterations were designed with the intent of keeping the rhetoric more direct from its academic philosophical roots. Having players take in as much of it as possible with little attention to the *'play'* aspect of the game. This resulted in an inverse response from players probably because they went into the experience expecting a 'game', but, were greeted with a complex array of information. As iterations went on, the systematic dumbing down of information brought about an experience subtly laced with the procedural rhetoric, giving a more positive response (Akmal and Coulton 2019).

That said, where we did manage to get some of the rhetoric across, it predominantly existed in the background for many of our players. This might owe to the fact that most discussions around procedural rhetoric involve the use of *video games*, and our artefact was a *board game*. When discussing the presence of the rhetoric among the players, a question was asked if it was necessary for the rhetoric to come across so literally? *"Why must the game be so structured, it is after all a board game?"*, they said. The very nature of such games is that processes, which otherwise would be hard set in a video game, are *often more malleable* in a board game as players ultimately control the implementation of rules. Throughout the playtests, the rules were allowed to be pliable to an amount, and this came naturally because of the nature of how collaborative board games are played. There were moments when players decided to retract their steps to avoid certain things happening. Other moments when rules were neglected during play from oversight, and play was allowed to move on. Such actions are not possible in video games unless programmed into them; and even then, only to an extent.

In his book *Play Anything*, Ian Bogost's (2016) main focus of discussion is the presence of *play* and *playgrounds* in our lives, which he eloquently expresses in this passage:

> *"Playgrounds are not thrones built for our proud gratification, but configurations of materials. They are not in our heads, but in the world. The first step in enjoying them is to stop worrying about our possible roles within them, and instead to allow lawns and malls and soccer pitches to show us their desires." (Bogost 2016, 25)*

He talks of the *act of play* as not an act of doing what one wants, but instead, of what one can with the materials at hand by "tinkering with a small part of the world". This could explain how irrespective of the efforts of infusing rhetoric within the game at the end of the day most players experienced the artefact for what it was: *a game*. They played with it, enjoyed it, and took away an experience from it. Although this implies the rhetoric (philosophical or otherwise) in that experience was secondary to the players, it is none-the-less a part of the experience, and thus presenting alternative mental models on the way IoT systems can be perceived.

ENDNOTES

1 See: https://www.theguardian.com/uk-news/cambridge-analytica
2 See: https://www.petrashub.org/
3 See: https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook
4 Taken from the philosophical *Model for Inter-Spatial Interactivity* from earlier research (Akmal and Coulton 2018)
5 Initially this element in the game was called the *Vulnerabilities Phase* as it dealt with literal vulnerabilities in IoT but over the course of iterations player feedback revealed the name as being too wordy and in the current iteration it was changed to *Risks*
6 In earlier iterations called *Resolutions* and *Conditions* respectively also changed after player feedback
7 For a full process of transferring between a research artefact to a designed game in a RtD methodology see, Akmal & Coulton 2019.

BIBLIOGRAPHY

Akmal, Haider, and Paul Coulton. 2018. "Using Heterotopias to Characterise Interactions in Physical/Digital Spaces." In *Proceedings of Drs2018 Limerick*, 1:269–78. Limerick. https://doi.org/10.21606/dma.2017.348.

Akmal, Haider, and Paul Coulton. 2019. "Research Through Board Game Design." In *Proceedings of RtD 2019: Method & Critique*. Delft, Netherlands.

Antle, Alissa N., and John Robinson. 2011. "Procedural Rhetoric Meets Emergent Dialogue: Interdisciplinary Perspectives on Persuasion and Behavior Change in Serious Games for Sustainability."

Berland, Matthew, and Victor R. Lee. 2011. "Collaborative Strategic Board Games as a Site for Distributed Computational Thinking." *International Journal of Game-Based Learning (IJGBL)* 1 (2): 65–81.

Bogost, Ian. 2007. *Persuasive Games: The Expressive Power of Videogames*. MIT Press.

Bogost, Ian. 2011. *How to Do Things with Videogames*. Electronic Mediations 38. Minneapolis: University of Minnesota Press.

Bogost, Ian. 2016. *Play Anything: The Pleasure of Limits, the Uses of Boredom, and the Secret of Games*. New York: Basic Books.

Clarke, Arthur C. 1962. "Hazards of Prophecy: The Failure of Imagination." In *Profiles of the Future*. Harper & Row.

Coulton, Paul. 2015. "The Role of Game Design in Addressing Behavioural Change." In *Proceedings of EAD 2015 the Value of Design Research*. Boulogne, France.

Coulton, Paul, and Alan Hook. 2017. 'Games Design Research through Game Design Practice'. In *Game Design Research*, edited by Petri Lankoski and Jussi Holopainen, 97–116. Pittsburgh: Carnegie Mellon University: ETC Press.

Coulton, Paul, and Joseph G. Lindley. 2019. "More-Than Human Centred Design: Considering Other Things." *The Design Journal 22* (4): 463–81. https://doi.org/10.1080/14606925.2019.1614320.

Donchin, Emanuel. 1995. "Video Games as Research Tools: The Space Fortress Game." *Behavior Research Methods, Instruments, & Computers 27* (2): 217–23.

Evans, Michelle. 2018. “Why Data Is the Most Important Currency Used in Commerce Today.” Forbes. March 12, 2018. https://www.forbes.com/sites/michelleevans1/2018/03/12/why-data-is-the-most-important-currency-used-in-commerce-today/.

Fantasy Flight Games. 2013. *Eldritch Horror*. Boardgame. Fantasy Flight Games

Farooq, M. U., Muhammad Waseem, Anjum Khairi, and Sadia Mazhar. 2015. “A Critical Analysis on the Security Concerns of Internet of Things (IoT).” *International Journal of Computer Applications 111* (7): 1–6. https://doi.org/10.5120/19547-1280.

Gilmour, Jonathan. 2014. *Dead of Winter: A Crossroads Game*. Boardgame. Plaid Hat Games.

Glassco, Bruce, Rob Daviau, Bill McQuillan, Mike Selinker, and Teeuwynn Woodruff. 2004. *Betrayal at House on the Hill*. Boardgame. Avalon Hill

Gürses, Seda, Bettina Brendt, and Thomas Santen. 2006. “Multilateral Security Requirements Analysis for Preserving Privacy in Ubiquitous Environments.” In *Proceedings of the UKDU*.

Gygax, Gary, Dave Arneson. 1974. *Dungeons & Dragons*. Boardgame. Tactical Studies Rules.

Harman, Graham. 2018. *Object-Oriented Ontology: A New Theory of Everything*. 1st ed. Pelican Books.

Lindley, Joseph Galen, and Paul Coulton. 2017. “On the Internet Everybody Knows You’re a Whatchamacallit (or a Thing).” In *CHI 2017 Workshop*.

Lindley, Joseph, Paul Coulton, and Rachel Cooper. 2017. “Why the Internet of Things Needs Object Orientated Ontology.” *The Design Journal 20* (sup1): S2846–S2857. https://doi.org/10.1080/14606925.2017.1352796.

Lindley, Joseph, Paul Coulton, and Miriam Sturdee. 2017a. “Implications for Adoption.” In *The 2017 CHI Conference*, 265–77. New York, New York, USA: ACM Press. https://doi.org/10.1145/3025453.3025742.

Mortier, Richard, Jianxin Zhao, Jon Crowcroft, Liang Wang, Qi Li, Hamed Haddadi, Yousef Amar, Andy Crabtree, James Colley, and Tom Lodge. 2016. “Personal Data Management with the Databox: What’s Inside the Box?” In *Proceedings of the 2016 ACM Workshop on Cloud-Assisted Networking*, 49–54. ACM.

Norman, Donald A. 1999. *The Invisible Computer: why good products can fail, the Personal Computer is so complex, and information appliances are the solution*. MIT Press.

Roman, Rodrigo, Pablo Najera, and Javier Lopez. 2011. “Securing the Internet of Things.” Computer. http://ieeexplore.ieee.org/abstract/document/6017172/.

Ruiz, Susana, Ashley York, Mike Stein, Noah Keating, and Kellee Santiago. 2006. *"Darfur is dying."* Computer software. mtvU.

Warshaw, Howard Scott. 1982. *E.T. the Extra-Terrestrial*. Atari 2600. Atari, Inc.

Weber, Rolf H. 2010. “Internet of Things - New Security and Privacy Challenges.” *Computer Law & Security Review 26* (1): 23–30. https://doi.org/10.1016/j.clsr.2009.11.008.

West, Sarah Myers. 2019. “Data Capitalism: Redefining the Logics of Surveillance and Privacy.” *Business & Society 58* (1): 20–41.

Zagal, José P., Jochen Rick, and Idris Hsi. 2006. “Collaborative Games: Lessons Learned from Board Games.” *Simulation & Gaming 37* (1): 24–40.