The Prometheus Terminal: Worlding Games for the Adoption of Sustainable Datafication and Cybersecurity practices

Franziska Pilling[1], Michael Stead[2], Adrian Gradinar[3]

[1]Lancaster University
f.pilling@lancaster.ac.uk
[2] Lancaster University
m.stead1@lancaster.ac.uk
[3]Lancaster University
a.gradinar@lancaster.ac.uk

Abstract

Edge Computing is being promoted as a more secure, private, and an increasingly better sustainable option for data generation and processing. Nevertheless, the rapid surge in the number of Internet of things (IoT) devices being integrated into networks and accompanying Edge Computing devices to process data closer to the source creates more opportunities and entry points for cyber-attacks. These attacks are labour intensive, with energy consumption increasing two-fold, contributing to climate change. Catalysing the situation further is the current illegibility and illiteracy of sustainable datafication and cybersecurity practices when using IoT devices and, to a more significant extent, the “networkification” (Pierce & DiSalvo, 2017) of connected devices.

To respond to these emergent issues and to make legible the domain for users’ sustainable and secured adoption of edge and IoT systems, this paper describes a Research through Design process for the design of a digital ‘Choose Your Own Adventure’ game, portraying a hacker’s voyage through a perceptible world of computer networks and sustainable data practices. In addition to attempting to disambiguate the network ecology of IoT and Edge Computing, we describe our ‘worlding’ method used to create the game’s narrative to illustrate; the various edge and IoT operations, how their systems are impacted by security threats, and how these technologies could be operated more sustainably. We conclude by showcasing the final physical-digital game console –*The Prometheus Terminal*– and gameplayers’ response to it. We also take the opportunity to discuss the next phase of this research, which focuses on project impact through the design of an immersive experience, providing the opportunity to gather and reiterate research back to users concerning the legibility, negotiability, and agency within edge and IoT systems for the adoption of sustainable and secure practices within a network ecology.

Author keywords
Sustainable Datafication; Edge Computing; Cybersecurity; Legibility; Adoption; Worlding.

Introduction

The pervasiveness of IoT, Edge Computing (EC), Fog Computing (FC) and Cloud Computing (CC) is affording end-users with more significant levels of connectivity, convenience, and personalisation across society as well as providing opportunities for new enterprise and innovation (Brous et al., 2020; Sulieman et al., 2022). However, the legibility and user awareness of the outlined network assemblage and the associated socio-technical impacts on users is minimally known, due to the technologies' radical development and adoption, resulting in no universally accepted definition of EC and FC among experts (Caprolu et al., 2019). Adding to the perplexity: these computing paradigms are often used interchangeably for the other, as frequently evidenced in both academic and industry literature, with one archetype often being considered the sum total of the network endeavour (c.f. Cisco, 2015; Fan et al., 2018; Maia et al., 2019; Wen et al., 2017). Critically, experts' understanding of the technologies are constantly evolving, while already in use and integrated into operational systems, leading to problems occurring in the 'wild' with detrimental implications to users. The state of affairs also leads to a lack of general user knowledge, impacting agency and negotiability of the technology (Mortier et al., 2014), and compromising user security and adoption sustainable of practices (Stead et al., 2020).

Nevertheless, EC is promoted as a more secure and private method for data generation and processing in lieu of the Cloud (Shi et al., 2016). A problem arises, however, in the increased use of IoT and EC technology forming unwittingly insecure networks, creating opportunities for external actors (human and machine) to carry out cyber-attacks upon devices and systems, such as denial-of-service and ransomware attacks (Alrowaily & Lu, 2018; Fan et al., 2018). These incursions are 'labour-intensive' requiring more processing power, where energy consumption can increase twofold during an attack (Kepçeoğlu et al., 2019), directly contributing to climate change (Morley et al., 2018). These environmental impacts are further compounded by the copious amounts of data generated by IoT systems, as almost half of the total data created globally originates from these systems (Reinsel et al., 2018).

To begin to respond to these outlined issues and to improve the legibility of the domain for users' secure and overall sustainable adoption of edge and IoT systems, this paper describes a Research through Design process (Durrant et al., 2017; Gaver, 2012) for the design of an interactive digital 'Choose Your Own Adventure' game, housed in a specially designed terminal, whereupon the gameplay is of a hacker's voyage through a perceptible world of computer networks and sustainable and cybersecurity data practices.

To situate the context of the game, we will first unpack the ontology of EC, FC, and CC systems, noting their challenges, differences and establishing our rationale to focus primarily on EC for this research. Secondly, we summarise a series of online workshops we held with computer science and sustainability experts. Thirdly, we describe our 'worlding' method utilised to support creating the game's narrative, and to visually communicate the various edge and IoT systems operations to everyday users of these technologies. As will be discussed, our worlding approach is a combination of chiefly Design Fiction as World Building approach (DFasWB) (Coulton et al., 2017; F. Pilling et al., 2021), flavoured with the novel practice of More-Than Human Centered Design (MTHCD) and 'Worlding' emanating from the likes of Donna Haraway, who turn our attention to certain experiences of non-human things for a deeper look at human-world relations (Haraway, 2011, 2016). Crucially, our worlding approach is used to disseminate our key research workshop findings, and expand knowledge of IoT and EC sustainable practices and security issues through gameplay. We conclude by showcasing the final physical-digital game console – *The Prometheus Terminal*– and gameplayers' response to it, while also framing future research stemming from this work.

Network Ontology & Challenges

Before discussing EC and FC, it is essential to understand CC (Figure 1). CC is focused on data storage and operates as an online delivery of computer services (including databases, software, intelligence, and servers) offered to users by technological companies to operate their proprietary IoT devices and services. According to Statista (2021), by 2026, the number of IoT devices connected to the internet and cloud services is expected to double and reach 21.5 billion active connections. With IoT flourishing daily and the increased development of digital services, CC has transpired, despite its widespread success, as not being a one-size-fits-all solution owing to its centralised computing paradigm. This inflexibility has resulted in an amplified separation between users' devices and their clouds processing operational data that, across the spectrum of billons of active devices and services, are collectively and progressively demanding higher volume, variety, and velocity rates from data. Thus, resulting in, to list a few consequences: low latency and jitter impacting time-sensitive applications (Caprolu et al., 2019); diminished context awareness and support (Roman et al., 2018); increased consumption and energy use of network bandwidth; a larger expanse of cyber-attack continuum, and decreased reliability of IoT devices operating as expected or as advertised (Cisco, 2015).

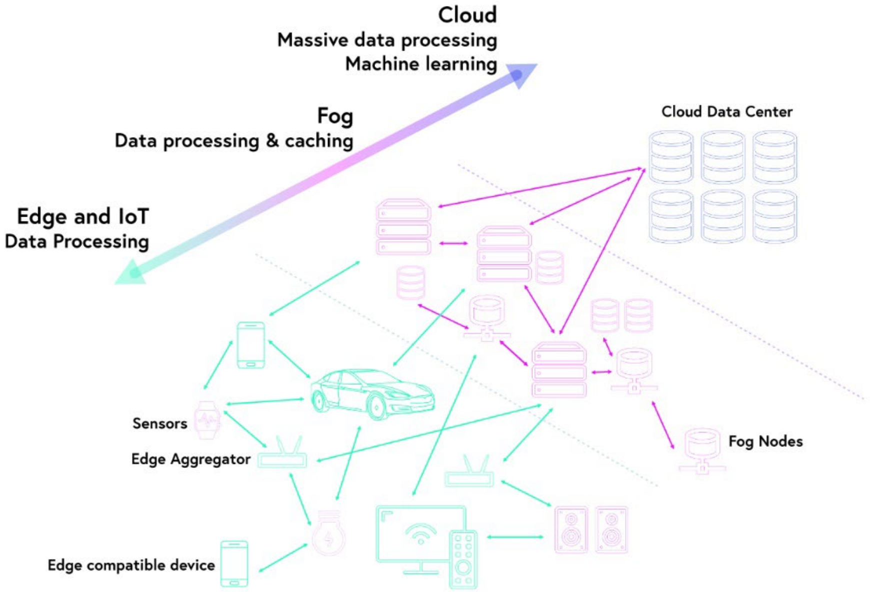


Figure 1. This diagram maps and traces the ontology of a typical network assemblage (Pilling, Stead & Gardinar 2022).

EC and FC share many similarities; specifically, they enable data traffic to the cloud and process operational data in closer proximity to devices. Nevertheless, to make a distinction between the two paradigms, EC is a distributed computing program constituting of a network topology operating at the 'edge' of a network allowing IoT data to be gathered, processed, and distributed closer to the IoT devices themselves, rather than sending data out to a fog or globally dispersed cloud network (Shi & Dustdar, 2016). Based on the previous passage, one can assume a distinction between EC and IoT; however, it is a common misconception that IoT is synonymous with EC. Though at risk of confusing the characterisation, some IoT devices are edge compatible, with the capability to form edge networks and process data (also partially) within themselves or ping data to another edge device in the same network – such as mobile phones, wearables, and open-source single-board computers (Raspberry Pi) and constrained devices (Arduinos) (Caprolu et al., 2019).[1] In summary: it is not currently legible which IoT products aid in forming an edge network, a feature that is also addressed in the game by highlighting which devices are more likely to be part of the edge configuration. Our research will predominantly focus its attention on the sustainable and security implications of EC networks, as typically, these are more easily adaptable or unwittingly formed by users through their adoption of edge compatible IoT devices. FC, however, is a network paradigm characteristically made up of servers outside of a user's network but geographically closer to the origin of the data, acting as a mediator between the edge and cloud. Some experts describe FC as extending the cloud via servers, as certain data packets commanded through programming not ordained for the cloud stay at the fog level, and are processed and cached here, with relevant data distributed to the cloud or back to the edge with excess data disposed of (Wen et al., 2017). As a result, both EC and FC are reshaping the

[1] Constrained devices are small devices with limited CPU, memory, and power resources which are often used as sensors and smart devices such as home automation, automotive and surveillance devices.

operational computation of data-driven technologies. Therefore, the distribution of logic to different network nodes introduces new challenges, such as dynamic scalability (Maia et al., 2019), specialised security mechanisms and user acceptability to perform maintenance in the event of a cyber-attack (Zhang et al., 2018).

The Workshops: Methodology

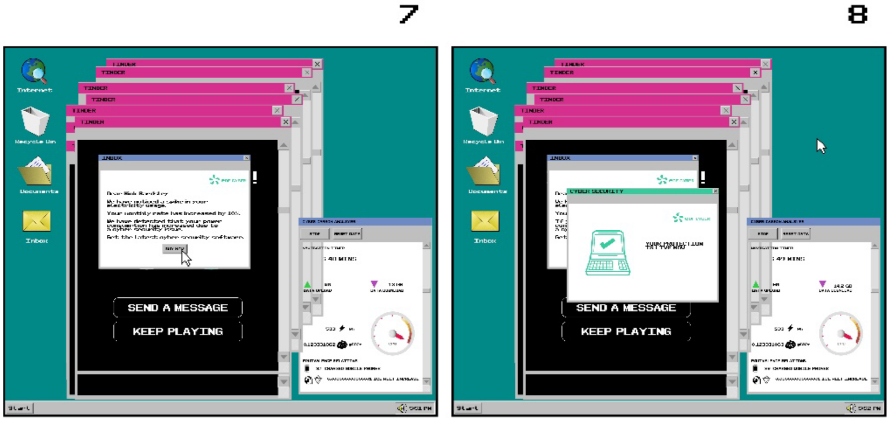
To gather progressive and forefront information about the three themes of EC, cybersecurity, and sustainability, we designed and facilitated three 'guided discussion workshops' with a mixed focus group of twenty experts from the fields cited (Hennink et al., 2020, p. 139). The workshops were staged and captured online using a combination of *Zoom* and the interactive whiteboard application *Miro*. Data was taken by recording the sessions with ethics approval and participant consent and transcribed for analysis, with the material used as context for worlding the 'Choose Your Own Adventure' narrative. Participants were also encouraged to note prominent feedback directly on the interactive whiteboard, although advised that the conversation was the primary source of data collection.

An initial template of probing questions and discussion points were designed to initiate and pilot conversations, which reflected our preliminary research. The questions were also designed to be semi-improvised, flexible, and responsive to effectively follow topics as they were spontaneously raised or followed through by experts (Hennessy, 2015; Hennink et al., 2020, p. 174). As the workshops progressed, our qualitative methodology enabled us to adapt talking points with the knowledge attained from the previous workshops. Regarding the discussion template and group interaction, participants were able to synthesise speculations on sustainable edge computing. As Morgan states, the "hallmark of focus groups is their explicit use of group interaction to produce data and insights that would be less accessible without the interaction found in a group" (1997, p. 2).

The structure of the guided discussions was broken up into the three primary themes (EC, cybersecurity, and sustainability), with each theme being carried through to the next theme's discussion point. The first focus was EC, thus situating, familiarising, and probing the technology in question. Challenges and developments concerning cybersecurity at the edge followed, with the distinctive theme of sustainability concentrated on at the end. However, general enquiries into the sustainability facet were also queried at the close of each succeeding theme to increase the prospects of considering how sustainability translated into a digital context.

As we suspected, because of the uncharted territory of sustainable edge computing and experts' tendency to know a lot about their area of knowledge, it proved challenging to ground the conversations in practical fleshed-out examples. Consequently, the last workshop task had a speculative emphasis, which started with a demonstration and an example of the Design Fiction approach to lead participants into a speculative discussion, with an opportunity for them to create Design Fiction narratives, focusing on sustainable edge futures (Figure 2). To demonstrate: a workshop participant speculated on a localised solar panel server farm that would cast an extensive edge network for neighbouring houses with a scheduled network activation, theorising a complete change in user behaviour and a more significant network field to secure.[2] A high-level thematic analysis was conducted after the workshops to identify and analyse the themes that materialised (Braun & Clarke, 2006). The following section will detail the analysis results as the motifs and contexts we employed for worlding the interactive game.

[2] We have since found a similar example of this speculation for cloud computing in the online magazine Branch, who are committed to designing a sustainable and just internet for all, originating from the Mozilla community (Brain et al., 2021).



We have noticed a spike in your electricity usage.
Your monthly rate has increased by 10%.
We have detected that your power consumption has increased due to a cyber security issue.
Get the latest cyber security software.

Figure 2. A Design Fiction showing a hack that can be identified through the energy widget, which reacted to the energy surge caused by the attack (Pilling, Stead & Gardinar 2022).

Workshop Results: Game Thematics for Worlding

During the workshops, we confirmed via experts' knowledge that despite its cybersecurity issues, EC's inherent potential for reducing data traffic, thus mitigating energy usage and carbon emissions, signifies the technology as a possible solution for developing more sustainable computing models (Stead et al., 2020). EC also creates opportunities to implement additional sustainable technology within its systems. An example of, is for the design and execution of machine learning software to reduce the duplication of data processed at the edge (Kim & Wu, 2020)

However, as we established during the workshops, the fact remains that the security applied to an edge network has to contend with the dynamic nature of virtual networks that the EC forms, with traditional firewalls designed for a static network topology not flexible or adaptive enough to contend with the dynamic nature of an EC network. This system, therefore, also comes with escalated maintenance required by users to keep services up to date for the subsequent payoff of better user experiences seen through faster response times to real-world stimuli thru local processing/computations and data buffering.

Moreover, during the workshops, a cybersecurity expert revealed that due to the ease, accessibility, and customisation afforded to users to create edge networks via their adoption of edge compatible IoT devices, can result in creating 'back doors' into personal data networks. The common culprit is default factory passwords left in operation by users on their various IoT devices. Furthermore, the peculiar hack of a Las Vegas casino's smart fish tank (Schiffer, 2017) also highlighted that hackers can find a 'back door' through a wide variety of mundane IoT devices that do not form the edge network, however are part of it. Consequently, the fish tank 'permitted' access to the casino's edge network for hackers to steal data. In contrast, in a CC scenario, this data would have been routed and stored in the cloud with a different method of entry and perhaps with more robust security protocols imposed by online security systems. As a result of the thematic analysis, the cybersecurity themes along with the different reasons why attacks occur (ethical, financial, cyberwarfare[3]), the various types of possible attacks that happen at the edge (ransomware, Denial of Service, data tampering, trojan, account hacking, network communication tampering (Caprolu et al., 2019; Martin et al., 2018)), and finally the numerous routes to enter the edge network (service provider, devices, evil-twin WIFI) gave us sufficient material for worlding and developing a cybersecurity thread of the narrative.

The sustainability element of EC and IoT networks is the next theme to be addressed. As previously noted, cyber-attacks do trigger an energy surge, however, discussed at great length in one workshop in particular, keeping a network secure also requires plenty of energy, even though "it's difficult to quantify the energy rate used over time as it doesn't necessarily spike like an attack does" (workshop participant). Keeping users' data secure is one of the significant

[3] In addition to the devastating 'ground' war in Ukraine, Russia has been sabotaging Ukrainian hardware through cyber-attacks with officials calling it the first 'hybrid war' (McLaughlin, 2022)

challenges emerging since all components on a network are communicating and exchanging significant amounts of data through symmetric encryption, decryption, and authentication processes, again resulting in high energy usage (Sulieman et al., 2022).

Evaluating sustainability practices with (and perhaps over) security protocols is a challenging proposition, yet, debatably, keeping one's data safe can mitigate personal and immediate harm, especially when there are other potential avenues to execute sustainable datafication and edge practices. The key sustainable EC practices that emerged from the workshop included:

- AI-assisted streamlining of storage would avoid the build-up of so-called 'data swamps' and limit opportunities for clandestine data mining and surveillance by platforms and providers, as well as reduce bait for hackers.
- The right to repair edge and IoT devices (Perzanowski, 2022; Stead et al., 2020), as their manufacture, materials mining and global distribution consume vast amounts of energy and generate massive Co2 emissions.
- Technological and data legibility can be applied to many modes and levels of user interaction. For instance, it is little-known that a user of the streaming service *Netflix* can adjust the streaming resolution in settings, as the platform automatically streams in 4K resolution with many users watching on devices not 4K compatible.

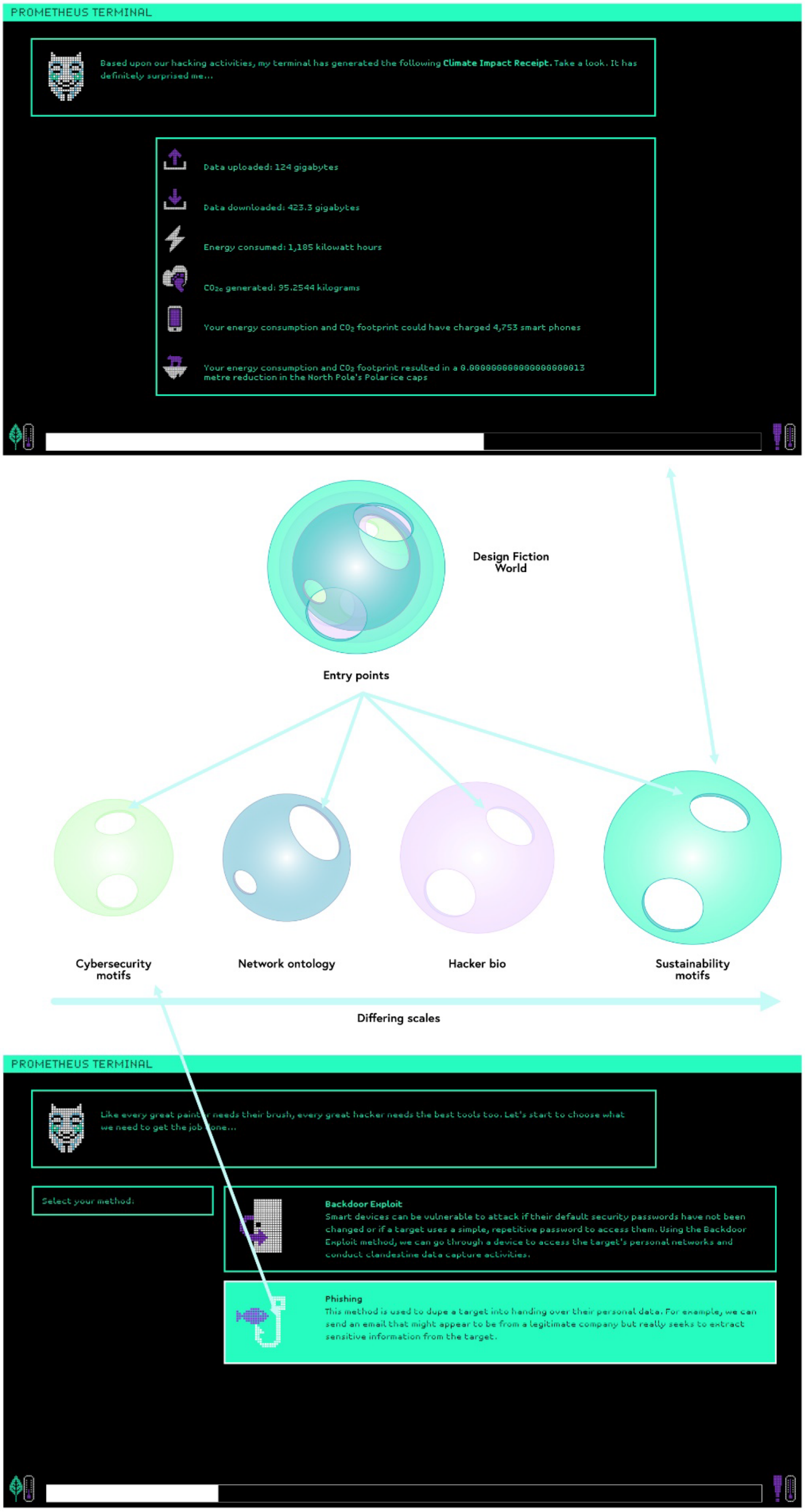
Derived from the workshop data, the legibility factor can be rated high in the taxonomy of users' adoption of sustainable edge data practices, as it empowers user negotiability and agency across technological interactions. Improved user awareness and knowledge of technology is a faster call for change than technological advances, or governances alone can offer sustainability efforts; however, it goes without saying that these sectors too need to be cultivated simultaneously. Therefore, the game's narrative is principally grounded in the here and now. It also includes speculative elements pointing to near-future technological advancements, such as how hackers could theoretically cause a disturbance, triggering energy spikes and stealing data. The following section details our approach to worlding the game via a brief outline of the Design Fiction and MTHCD worlding approach, which will situate our practice by which we developed the game's narrative.

Discussion: Worlding A Game About Sustainable and Secure Datafication

For the narrative context of the Prometheus game: the player takes on the persona of a hacker, aiming to steal or encrypt data for a ransom. Using the hacker as the protagonist opened up the 'worlding narrative arch' for a deeper perception of what happens in a cyberattack, enabling the player to learn un-customarily from both viewpoints. The game does not teach someone how to hack; however, it is designed to be an abstract illustration of the motive, waypoints, and decisions that go into hacking and encountering defence mechanisms from applied security. Therefore, from a 'typical' user's point of view, one can appreciate real-world hacking processes and apply the appropriate security. In addition to the goal of securing the most loot, a player also wins through the less energy used for the hack. This principle is not highlighted in the onboarding of the game, as it has been designed to be deciphered by players via a Co2 contribution readout on the player's in-game status bar (Figure 3), that monitors and quantifies the sustainability of the narrative choices they make; with each narrative option realistically programmed in the back end to have a high, medium, or low energy output revealed on the status bar. Game designers regularly use this 'elusive' game mechanic to entice players' curiosity, and once a covert element is realised by players, they often place significant meaning and value on to it, as it has been a product of their perception, which we hoped would extend out into real-world practices (Salen & Zimmerman, 2003). The game mechanic also served as a way to reflect the obfuscation of whether an action is sustainable or not across an edge network, grounding an immaterial practice into a measurable and perceptual narrative for players to encapsulate the problem and take information from the game and apply these to real-world situations.

Turning to the approach of worlding the gameplay, the science fiction author Bruce Sterling coined the term Design Fiction while describing the influence design thinking had on his writing, noting that "[D]esign [F]iction reads a great deal like science fiction; in fact, it would never occur to a normal reader to separate the two" (Sterling, 2005, p. 30). Sterling went on to describe the practice as "the deliberate use of diegetic prototypes to suspend disbelief about change" (Sterling quoted in Bosch, 2012, para 3). For reference: a diegetic prototype is an artefact, not limited to a specific materiality, that presents an interior view of a fictional world in status; the designer James Auger explains that the core motivation of Design Fiction and the creation of diegetic prototypes is to shift the discussions of technology beyond the fields of experts (Auger, 2013, p. 11).

Sterling also wrote that Design Fiction “tells worlds rather than stories” (Sterling quoted in Bosch, 2012, para 3), inspiring the approach of DFasWB, which can be summarised as the collection of diegetic prototypes that, when viewed together, build a fictional world (Coulton et al 2017). Additionally, we would argue to – tell a world — is an act of narration whereby we narrate using the game player’s avatar embodying a hacker’s point of view, the diegetic prototypes, the construction of the world, and waypoints through the game. These worlds are therefore narrated with a “rhetorical intentionality” (Coulton et al., 2017, p. 167) using “educated guesswork” by their designers for the creation of rhetoric within a world (Bogost, 2012, p. 30), which enables those engaging or playing within the world to explore that rhetoric, rather than being forced down a prescribed path (Coulton et al., 2016). For clarity, the game plays out as a non-linear narrative; therefore, players can make strategic choices about the sustainability of their hack. The collection of diegetic prototypes used in the game are the elective choices, as each represents a contextual element or digital artefact in the narrative and provides an entry point into the hacker’s ‘fictional’ world. Each element is displayed using graphical symbology and a textual description to flesh out the elements’ diegesis. Hence, the game itself can be considered to encompass many layers of entry points for players, much like how the earth is divided into four layers – crust, mantle, outer core, and inner core – with each layer forming the world (Figure 3).



PROMETHEUS TERMINAL

Based upon our hacking activities, my terminal has generated the following **Climate Impact Receipt.** Take a look. It has definitely surprised me...

Data uploaded: 124 gigabytes

Data downloaded: 423.3 gigabytes

Energy consumed: 1,185 kilowatt hours

CO_{2e} generated: 95.2544 kilograms

Your energy consumption and CO_2 footprint could have charged 4,753 smart phones

Your energy consumption and CO_2 footprint resulted in a 0.0000000000000000000013 metre reduction in the North Pole's Polar ice caps

PROMETHEUS TERMINAL

Like every great painter needs their brush, every great hacker needs the best tools too. Let's start to choose what we need to get the job done...

Select your method:

Backdoor Exploit
Smart devices can be vulnerable to attack if their default security passwords have not been changed or if a target uses a simple, repetitive password to access them. Using the Backdoor Exploit method, we can go through a device to access the target's personal networks and conduct clandestine data capture activities.

Phishing
This method is used to dupe a target into handing over their personal data. For example, we can send an email that might appear to be from a legitimate company but really seeks to extract sensitive information from the target.

Figure 3. In the middle is a visual analogy for DFasWB, highlighting the entry points the diegetic prototypes form into the fictional world/s and which the players enter through. The top and bottom of the diagram identifies some of the game's diegetic prototypes in operation via screenshots of the game (Pilling, Stead & Gradinar).

The MTHD approach (Coulton & Lindley, 2019; Wakkery, 2021), however small, did play a part in conceiving the diegetic prototypes that personified the digital ecology and things the players traverse. This particular more-than human approach is based on readings of the philosophical ideology of Object-Oriented Ontology as promoted by Graham Harman (2018), Ian Bogost (2012) and Timothy Morton (2013, 2017), and Haraway's approach to articulate intertwined worlds of human and non-human ecologies (2011, 2016). Expanding upon these in fine detail is beyond the scope of the paper[4]; however, OOO propositions that the perspectives derived from human beings are not the only one's worth considering and speculates that all things have a way of 'being'. Within the confinements of more traditional design approaches such as Human Centered Design (HCD), which promotes the human-being as a central consideration amounts to HCD's core axiom of simplification in interaction through the cutting out 'excessive' information (Norman, 1998). Don Norman, who notably founded HCD has also argued against an anthropocentric view in his article titled *Human-Centred Design Considered Harmful* (2005). In which he criticised the blind commitment and attention on users, which ironically creates designs that lack cohesion, increases complexity, and obfuscates the functionality and operation of technology; thus, hindering agency and negotiability in technology, ultimately designed to be human conscientious. On the other hand, as designers forming a Design Fiction and a MTHCD worlding approach we can trace, speculate on, and articulate digital beings through the practice of ontography; a taxonomy of being by speculatively mapping the many possible relations within a network assemblage between digital objects and humans, highlighting both interdependent relationships and independent perspectives. As Bogost writes: "ontograph involves cataloging things, but also drawing attention to the couplings of and chasms between them" (Bogost, 2012,p.50), where, as M.Pilling et al state, "revelation invites speculation" (2022). This approach exemplifies Haraway's embrace of "staying with the trouble" by reflecting the entangled ecology of all things human and non-human (Haraway, 2016). Mapping the ontography of the network assemblage also translated into mapping the games narrative and the different narrative branches players elect (Figure 4).[5]

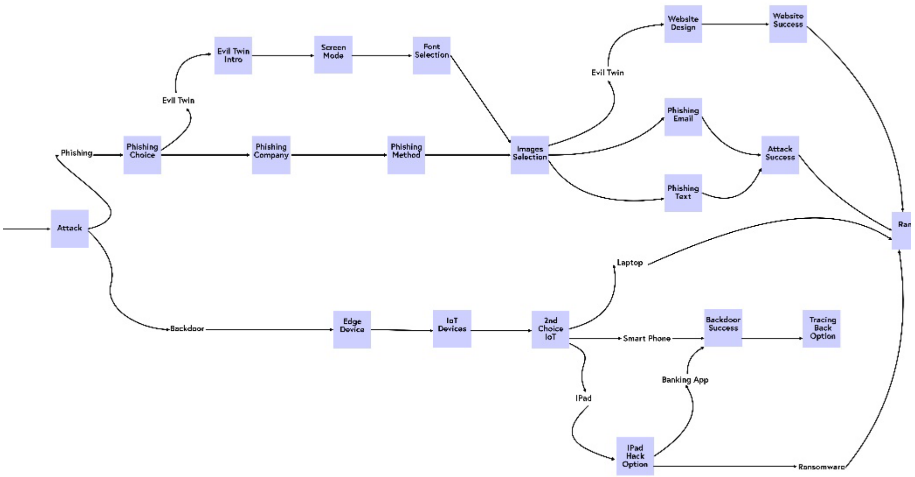


Figure 4. A snippet of the speculative and ontological mapping we did to produce narrative branches for the game.

[4] For further detail on the adoption of OOO in design practice see (Lindley et al., 2020; F. Pilling et al., 2021; F. Pilling & Coulton, 2021)

[5] See also Coulton et al for an example on onto-graphical storyboarding (Coulton et al., 2017).

To give an overview of the gameplay, after detailing the design approach of the game narrative: players set up what type of hacker they are, either acting in a group or as an individual and then select their motive for the hack – picking from either an ethical, disruptor or financial point of view. As a characteristic of 'Choose Your Own Adventure' games, the options a player takes will guide players down a particular path of possibilities; while this does curb some narrative electives on offer to the players, the game mechanic maintains a logical and realistic narrative. Yet, to ensure the game's narrative was not restrictive, we provided sufficient and alternative narrative branches to choose from that followed a similar configuration. For instance, after a player chooses their motivation, they progress on to picking their method of a 'way in' to a victim's edge network, such as phishing, evil-twin WIFI, or a backdoor exploit. Next, the player navigates their way through the edge network jumping from an IoT device to the next, looking for data to either steal or to ransom through encryption software. Thereafter, the player encounters security protocols through AI-assisted and adaptable firewalls. Once a 'hacker' has secured their spoils, a conclusive energy receipt is calculated of their hack that also quantifies the energy readings into tangible implications, such as the amount of energy consumed to charge X number of mobile phones (Figure 3). The game is played on a physical platform with a screen and navigational pad reminiscent of retro-computer terminals (Figure 5), a style that harmonises with the conventional 8-bit style of text-based games we were emulating.

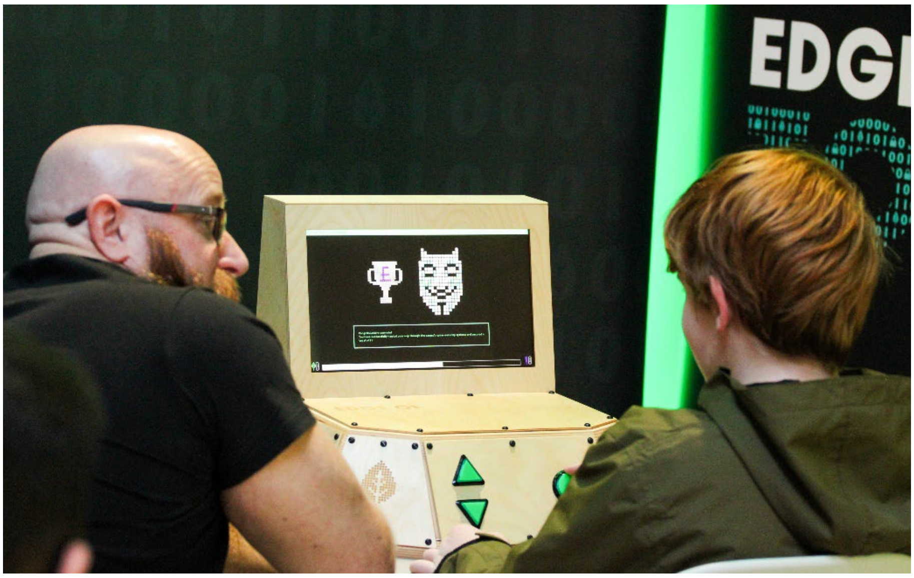


Figure 5. The Prometheus Terminal being used at an event. Many players opted to play as a team to discuss strategy, the worlding of the game, and its underlying messages of sustainable and secure practices.

The Prometheus Terminal in Action and Future Research: Fostering the Adoption of Sustainable and Secure Computing Models

The aim of the Edge of Tomorrow project was twofold –to research and create design guidelines for sustainable and secure edge network practices (see Stead et al., 2022) and to embed these into an interactive platform for public dissemination; thus, communicating and making legible computing paradigms for increased user agency and negotiation to adopt sustainable and secure networks and interactions. The second-mentioned aim was examined when we showcased the *Prometheus Terminal* at several public engagement events. The overall response to the game and its worlding was positive. Numerous gamers described the experience of playing the game empowered them to understand a hacker's logistics while increasing their awareness about the network's ontology, IoT devices, security measures and practices they could implement. However, the crucial finding for our research was that many players had not associated sustainability with datafication or considered the implications of their digital interactions on the environment: stressing the current lack of legibility concerning sustainability in a digital context, imploring further research and public engagement.

Constructive criticism about the *Prometheus Terminal* concerned the delivery and gameplay via text, which took considerable time and effort for players to plough through the narrative branches, thereby affecting the project's overall aim for communicating a sustainable and secure approach to forming an edge network. Therefore, to improve the impact of the research project and players' experiences in future work, we are currently developing the second iteration of the game and its worlding by distilling them into an immersive game experience that involves visual, kinaesthetic, and auditory dimensions. The approach of the experience is to "dietetically situate" players directly into the same artificial world as the game (M. Pilling et al., 2022). In this sense, the player will enter the world and interact with the game in a physical setting. In detail, a player will enter a mundane set-up of a physical furnished living room complete with IoT devices. The player will be tasked to set up and form their edge network by considering and balancing their sustainable and security preferences. A disembodied AI assistant will take the player through this procedurally, acting as the overall game narrator and guide via voice interaction, evoking common household smart home assistances. The aim of the game for a player will be to stop a hacker from entering the edge network through strategic security measures. In this interpretation, we have taken the worlding from the first iteration and flipped the perspective to suit the reimagining of the Future Mundane project, which researched the negotiability and agency of smart devices and their operations within our own homes (Ibid). As the research parameters of both projects are comparable, it served as an opportune instance to redesign and 'load' an experience in an interactive and physical simulation that lent itself to be adapted through backend programming and interactive game design. As well as harnessing the embodied interaction, the other pivotal characteristic we are adopting from the game's reinterpretation is the unique execution of the experience being installed into a self-contained mobile research platform housed in a teardrop caravan. The pertinent aspect of being mobile is the opportunity to expand the audience outreach beyond those who would usually frequent a university or gallery setting, in which research projects are typically showcased at. The potential to increase project impact, as well as a redesign of the game interaction and develop the narrative through ontological research and worlding, provides the opportunity to continue to focus on improving users' legibility of the unsustainable effects of smart devices datafication, and create practical guidance towards sustainable data practices.

Conclusion

How data is created, processed, and stored is increasingly affecting the planet's natural environment and leading to cyber-security issues. With that in mind, the adoption of edge networks will undoubtedly continue to increase due to the perceived benefits the technology brings as an alternative to contest issues associated with cloud scalability. As well as EC's ability to facilitate better user experiences with respect to handling requests and processing 'data exhausts' created by the proliferation of IoT devices, services, software, and associated networks. Nevertheless, whilst EC diminishes issues relating to latency management and some security and sustainability problems associated with cloud services, it is also starting to generate its own range of difficulties in terms of both data security and sustainability. To this end, our paper describes the exchange of issues from cloud computing for comparable ones at the edge, although unfurling in unique challenges due to ontological differences between CC and EC. Through our research, we have sought to make the complex and obscured nature of edge networks and their data processes legible via a public engagement tool, which imparted sustainable and secure data practices through play. Notably, the iterative designs described here only scratch the surface of the challenges we have outlined. However, we detail how worlding games can communicate the often imperceptible and entangled nature of new technologies (Murray-Rust et al., 2019) into tangible and situated experiences that users can easily understand. The expansion of the research's themes and scope into a more experiential and interactive platform as part of our future work, will offer the opportunity to identify and tease out further sustainability and security criteria arising from EC adoption. These points will be communicated to a much wider audience outside of academia and establish salient points to feedback towards industry –digital technology developers, service platforms, and data storage providers. Concerning the latter point, this project has been carried out in collaboration with BBC R&D, our project partner, who will utilise the findings and design guidelines (Stead et al., 2022) and embed these into the design of their future edge-based digital services and platforms, in addition to conveying findings to users in the form of technical guidance. Whilst this paper only explores a small niche in tackling climate change, it does begin to underscore the imperative for design research projects like this and transdisciplinary collaboration to make our computing practices more secure and sustainable.

References

Auger, J. (2013). Speculative design: Crafting the speculation. *Digital Creativity*, *24*(1), 11–35. https://doi.org/10.1080/14626268.2013.767276

Bogost, I. (2012). *Alien phenomenology, or, What it's like to be a thing*. University of Minnesota Press.

Bosch, T. (2012). Sci-Fi Writer Bruce Sterling Explains the Intriguing New Concept of Design Fiction. *Slate*, 5.

Brain, T., Nathanson, A., & Piantella, B. (2021, Spring). Solar Protocol. *Branch*, *2*. https://branch.climateaction.tech/issues/issue-2/solar-protocol/#

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*, 77–101.

Brous, P., Janssen, M., & Herder, P. (2020). The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations. *International Journal of Information Management*, *51*, 101952. https://doi.org/doi: 10.1016/j.ijinfomgt.2019.05.008

Caprolu, M., Di Pietro, R., Lombardi, F., & Raponi, S. (2019). *Edge Computing Perspectives: Architectures, Technologies, and Open Security Issues*.

Cisco. (2015). *Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are*. https://www.researchgate.net/profile/Mohamed_Mourad_Lafifi/post/Is_there_any_simulation_tool_for_fog_computing/attachment/59d638c079197b8077995f4c/AS%3A398883160117248%401472112564706/download/Fog+Computing+and+the+Internet+of+Things++Extend+the+Cloud+to+Where+the+Things+Are.pdf

Coulton, P., Burnett, D., & Gradinar, A. (2016). Games as Speculative Design: Allowing Players to Consider Alternate Presents and Plausible Futures. *Design Research Society*, *4*, 1609–1626. https://doi.org/10.21606/drs.2016.15

Coulton, P., & Lindley, J. G. (2019). More-Than Human Centred Design: Considering Other Things. *The Design Journal*, *22*(4), 463–481. https://doi.org/10.1080/14606925.2019.1614320

Coulton, P., Lindley, J., Gradinar, A., Colley, J., Sailaja, N., Crabtree, A., Forrester, I., & Kerlin, L. (2017). Experiencing the Future Mundane. *Proceedings of RTD 2019*, 10. https://doi.org/10.6084/m9.figshare.7855790.v1

Coulton, P., Lindley, J., Sturdee, M., & Stead, M. (2017). Design Fiction as World Building. *Proceedings of Research through Design Conference*. https://doi.org/10.6084/M9.FIGSHARE.4746964

Durrant, A. C., Vines, J., Wallace, J., & Yee, J. S. R. (2017). Research Through Design: Twenty-First Century Makers and Materialities. *Design Issues*, *33*(3), 3–10.

Fan, K., Pan, Q., Wang, J., Liu, T., & Li, H. (2018). Cross-Domain based Data Sharing Scheme in Cooperative Edge Computing. *IEEE*, 87–92.

Gaver, W. (2012). What should we expect from research through design? *CHI '12: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 937–946. https://doi.org/10.1145/2207676.2208538

Haraway, D. (2011). *SF: Science Fiction, Speculative Fabulation, String Figures, So Far*. https://people.ucsc.edu/~haraway/Files/PilgrimAcceptanceHaraway.pdf

Haraway, D. (2016). *Staying with the Trouble Making Kin in the Chthulucene*. Duke University Press.

Harman, G. (2018). *Object-Oriented Ontology: A New Theory of Everything*. Penguin Random House.

Hennessy, D. (2015). *Frameworks for effective improvised facilitation*. Lancaster University.

Hennink, M., Hutter, I., & Bailey, A. (2020). *Qualitative Research Methods*. Sage Publications Ltd.

Kepçeoğlu, B., Murzaeva, A., & Demirci, S. (2019). *Performing energy consuming attacks on IoT devices*. 1–4. https://doi.org/10.1109/TELFOR48224.2019.8971102

Lindley, J., Akmal, H. A., & Coulton, P. (2020). Design Research and Object-Oriented Ontology. *Open Philosophy*, *3*(1), 11–41.

Maia, A. M., Ghamri-Doudane, Y., Vieira, D., & de Castro, M. F. (2019). Optimized Placement of Scalable IoT Services in Edge Computing. *IFIP/IEEE*, 189–197.

Martin, A., Raponi, T., Combe, T., & Di Pietro, R. (2018). Docker ecosystem–vulnerability analysis. *Computer Communications*, *122*, 30–43.

McLaughlin, J. (2022). A digital conflict between Russia and Ukraine rages on behind the scenes of war. *National Public Radio*. https://www.npr.org/2022/06/03/1102484975/a-digital-conflict-between-russia-and-ukraine-rages-on-behind-the-scenes-of-war?t=1654608495426

Morgan, D. L. (1997). *Focus groups as qualitative research* (2nd ed.). Sage Publications Ltd.

Morley, J., Widdicks, k, & Hazas, M. (2018). Digitalisation, energy and data demand: The impact of Internet traffic on overall and peak electricity consumption. *Energy Research & Social Science*, *38*, 128–137. https://doi.org/10.1016/j.erss.2018.01.018

Mortier, R., Haddadi, H., Henderson, T., McAuley, D., & Crowcroft, J. (2014). Human-Data Interaction: The Human Face of the Data-Driven Society. *ArXiv:1412.6159 [Cs]*. http://arxiv.org/abs/1412.6159

Morton, T. (2013). *Hyperobjects: Philosophy and Ecology After the End of the World*. University of Minnesota Press.

Morton, T. (2017). *Humankind: Solidarity with Non-Human People*. Verso Books.

Norman, D. (1998). *The Invisible Computer: Why Good Products Can Fail, the Personal Computer is So Complex, and Information Appliances are the Solution.* MIT.

Norman, D. (2005). Human-Centered Design Considered Harmful. *IX Interactions*, *XII*. https://interactions.acm.org/archive/view/july-august-2005/human-centered-design-considered-harmful1

Perzanowski, A. (2022). *The Right to Repair: Reclaiming the Things We Own*. Cambridge University Press.

Pierce, J., & DiSalvo, C. (2017). Dark Clouds, Io&#!+, and [Crystal Ball Emoji]: Projecting Network Anxieties with Alternative Design Metaphors. *Proceedings of the 2017 Conference on Designing Interactive Systems*, 1383–1393. https://doi.org/10.1145/3064663.3064795

Pilling, F., & Coulton, P. (2021). Carpentered Diegetic Things: Alternative Design Ideologies for AI Material Relations. *The Ecological Turn. Design, Architecture and Aesthetics beyond 'Anthropocene'*.

Pilling, F., Lindley, J., Akmal, H. A., & Coulton, P. (2021). Design (Non) Fiction: Deconstructing/Reconstructing The Definitional Dualism of AI. *International Journal of Film and Media Arts*, *6*(1), 6–32.

Pilling, M., Coulton, P., Lodge, T., Crabtree, A., & Chamberlain, A. (2022). Experiencing mundane AI futures. *DRS2022: Bilbao*. https://doi.org/doi.org/10.21606/drs.2022.283

Reinsel, D., Gantz, J., & Rydning, J. (2018). *The Digitization of the World From Edge to Core*. IDC. https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf

Roman, R., Lopez, J., & Mambo, M. (2018). Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges. *Future Generation Computer Systems*, *78*(2), 680–698. https://doi.org/doi.org/10.1016/j.future.2016.11.009

Salen, K., & Zimmerman, E. (2003). *Rules of Play*. The MIT Press.

Schiffer, A. (2017). How a fish tank helped hack a casino. *The Washington Post*. https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/

Stead, M., Gradinar, A., & Coulton, P. (2020). Must All Things Pass?: Designing for the Afterlife of (Internet of) Things. *ThingsCon The State of Responsible Internet of Things Report 2020*, *11*(4), 45–52.

Stead, M., Pilling, F., Gradinar, A., & Forrester, I. (2022). *SUSTAINABLE X SECURE EDGE: Design Guidelines for Future Data-Driven Edge-IoT Devices and Services*. PETRAS Research Centre of Excellence.

Sterling, B. (2005). *Shaping Things*. The MIT Press.

Sulieman, A. N., Celsi, R. L., Li, W., Zomaya, A., & Villari, M. (2022). Edge-Oriented Computing: A Survey on Research and Use Cases. *Energies*, *15*(452). https://doi.org/10.3390/en15020452

Wakkery, R. (2021). *Things We Could Design: For More Than Human-Centered Worlds*. The MIT Press.

Wen, Z., Yang, R., Garraghan, P., Xu, J., & Rovatsos, M. (2017). *Fog Orchestration for IoT Services: Issues, Challenges and Directions*. https://doi.org/10.1109/MIC.2017.36