This paper is a postprint of a paper submitted to and accepted for publication in [journal] and is subject to Institution of Engineering and Technology Copyright. The copy of record is available at the IET Digital Library (http://digital-library.theiet.org/content/conferences/10.1049/cp.2018.0033).

Emerging risks in the IoT ecosystem: Who's afraid of the big bad smart fridge?

Leonie Maria Tanczer *Ine Steenmans* *Miles Elsden* *Jason Blackstock* *Madeline Carr*

Dept. of Science, Technology, Engineering & Public Policy
University College London, 36–38 Fitzroy Square, London, W1T 6EY, UK
{l.tanczer, ine.steenmans, m.elsden, jason.blackstock, m.carr}@ucl.ac.uk

Keywords: Internet of Things, risks, futures and foresight, security, privacy

Abstract

Rapid technological innovations, including the emergence of the Internet of Things (IoT), introduce a range of uncertainties, opportunities, and risks. While it is not possible to accurately foresee IoT's myriad ramifications, futures and foresight methodologies allow for the exploration of plausible futures and their desirability. Drawing on the futures and foresight literature, the current paper employs a standardised expert elicitation approach to study emerging risk patterns in descriptions of IoT risk scenarios. We surveyed 19 IoT experts between January and February 2018 using an online questionnaire. The submitted scenarios provided expert's perception of evolving IoT risk trajectories and were evaluated using thematic analysis, a method used to identify and report patterns within data. Four common themes were extracted: physical safety; crime and exploitation; loss of control; and social norms and structures. These themes provide suitable analytical tools to contextualise emerging risks and help detecting gaps about security and privacy challenges in the IoT.

1 Introduction

The Internet of Things (IoT) is currently all over the news. One barely escapes reports on 'smart' thermostats being prone to software vulnerabilities [1], WiFi-enabled Barbie dolls providing attackers access to audio files by children [2], and cars like the Jeep Cherokee model being hacked [3]. While these cases offer great news for tech journalists and are opportune stories for social media icons like the Twitter account @internetofshit, these articles also reveal some of the fundamental risks that lie beneath the attempt to increasingly interconnect physical systems and embed them in a larger network of devices and appliances.

The IoT is not a stand-alone technology but rather the amalgamation of diverse and interconnected technologies. This emerging IoT ecosystem is characterised by a proliferation of visible and hidden sensors that collect and transmit data (sensing), systems that interpret and make use of the aggregated information (processing), and actuators that, on the basis of this information, take action without direct human intervention (actuation) [4]. These 'smart' or "digitally upgraded" [5, p. 107] products can communicate with each other and/or humans, have unique identifiers such as Internet Protocol (IP) addresses, can be remotely controlled, and function as physical access points to networked services.

Where previous cybersecurity concerns confined to a range of computerised devices, including desktop computers or portable electronic devices such as laptops and phones, the IoT amplifies the scope and scale of products and services that have to be secured. And indeed, the IoT's application areas are wide; they stretch from personal fitness and assisted living devices, from home appliances such as smart fridges to utilities such as smart energy meters, from smart traffic management systems to connected and autonomous vehicles and transport infrastructures. Deployed in the home, workspace or public spaces, the IoT is promising to transform every sector, including, finance, manufacturing, agriculture, and health.

This expansion, however, comes with a multitude of challenges. The academic literature has already highlighted the numerous means through which the IoT creates security and privacy risks [6]. Various publications point out flaws when it comes to ensuring the confidentiality of data [7], the integrity and access control of devices [6], or the exploitation of IoT's architecture [8]. Additionally, the IoT creates challenges to the current regulatory environment through its sophisticated interdependencies across products, users, and producers, as well as the interconnection of physical safety with information security [9].

While the literature on the IoT continues to broaden, it is currently predominantly focused on technical analyses and economic assessments. Investigative studies on new ways to approach the IoT's uncertainties are much less common though equally important. This paper, therefore, provides an exploratory analysis of the evolving IoT risk landscape. Based on survey data as part of the engagement with the larger PETRAS IoT Hub[1] research community, our paper draws on the

[1] The PETRAS Internet of Things (IoT) Hub is a consortium of nine leading UK universities which work across socio-technical boundaries to explore critical issues in privacy, ethics, trust, reliability, acceptability, and security of the IoT.

futures and foresight literature to analyse emerging risk patterns in descriptions of anticipated IoT scenarios.

1.1 Future Technology and Foresight

The systematic practice of anticipating novel and disruptive behaviours and any subsequent opportunities or possible threats is developed within the field of future studies and foresight [10]. While futures and foresight research and practice activities have over the years led to the development of many forward-looking techniques (e.g. trends analysis, forecasting, scenario-based wind-tunnelling, and road mapping), there is, however, no single methodological blueprint for the ways by which one can set out to anticipate future change [11], [12].

The use of futures and foresight methods in predicting the impact of emerging technologies has a history spanning decades [13]. Data collection and analysis approaches have centred primarily on systematically 'scanning the horizon' [14]. Such scanning exercises seek to identify early signals of emerging issues, trends, or drivers of change; compile these, and then analyse them for their likely significance. Data sources that feed into these scans typically comprise expert elicitation, as well as the collection and analysis of diverse sources, including media outlets, academic publications, and practitioner literature. In examining the potential impacts of emergent technologies, the interest is primarily in the interactions *between* trends of change [15]. The exploration and communication of such an analysis is therefore typically framed as 'scenarios' – coherent stories that describe the way the world might look in the future when multiple critical uncertainties combine [16]–[18]. Insight into the nature of emerging technology opportunities and threats are often found embedded within these stories.

Examples of the use of scenarios in IoT foresight exist. These publications include fictional narratives and/or factors that derive from a wide range of surveyed literature [19], interdisciplinary workshops and collaborations [20], interviews [21] and the polling of experts [22], [23]. Shepherd, Akram, and Markantonakis [24], for instance, provided one of the first quantitative investigations of IoT risks anticipated to develop in the financial sector. The authors used an online questionnaire in which security professionals had to judge and rank various assets, threats, and vulnerabilities in the IoT. Their study also involved academic and industry stakeholders, allowing for the collection of diverse viewpoints.

Whilst most futures and foresight studies use standardised data collection methods (e.g., surveys) from which fictional narratives are developed, the current study combines the polling of experts with the narrative scenario development, providing a more formalised way to collect IoT experts' perception of evolving risks. The gathered scenarios, therefore, offer preliminary findings of our ongoing research into the future risk landscape of the IoT, and constitute data upon which we will draw in future workshops with subject specialists. The research has been reviewed and approved by UCL's ethics committee and will feed into a report for the Lloyd's Emerging Risks Series.

2 Methodology

2.1 Participants and Data Collection

The participants were a self-selected sample of N=19 IoT experts who responded to the online survey invitation. The link to the web-based survey tool *Opinio* was sent via email to all PETRAS IoT Hub academics (n=89), a selected group of PETRAS-affiliated industry stakeholders (n=24), and IoT researchers that had previously been in contact with PETRAS Standard, Governance and Policy research team (n=10). The survey was also publicly advertised in the PETRAS newsletter. This sample was chosen because of their involvement in and relationship to PETRAS, which was likely to make them particularly aware of the emerging IoT risk landscape.

Responses were collected over the course of a month (mid-Jan to mid-Feb 2018). The questionnaire did not collect any demographic information. However, the survey offered the opportunity to name other relevant stakeholders to whom this survey should be sent to (i.e., snowball sampling).

The survey included seven items and asked participants to briefly describe one short example ('scenario') of emerging IoT risks, ranging from 'risks to IoT systems' to 'cascading cyber-physical risks'. Participants were shown an exemplary scenario that focused on future IoT risks within the retail sector. Participants were then asked to describe their own futuristic scenario and to categorise the applicability of their scenario to different sectors as well as to indicate the expected likelihood, timescale, and severity of these risks.

Participants had the option to repeat the survey and were asked at the end of the questionnaire to indicate if they would like to be acknowledged in a 'List of Experts Consulted' and/or wish to have their answers attributed to them. Alternatively, participants could indicate if they preferred to remain anonymous.

2.2 Data Analysis

Due to the partial textual nature of the responses, the scenarios were analysed using thematic analysis [25]. Thematic analysis is a method for identifying, analysing and reporting patterns within data. This study applied an inductive approach for identifying themes and examined them on a semantic and interpretative level. Following the guidelines set out by Braun and Clarke [25], we first familiarised ourselves with the data. Principal codes were generated which then turned into potential themes. These themes moved away from the descriptive level of the

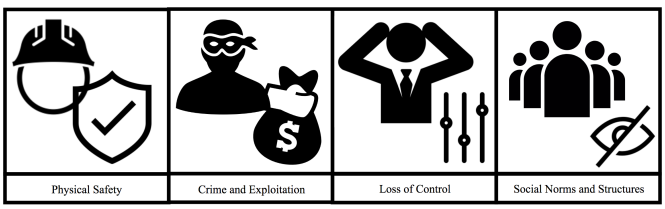

Fig. 1: Themes emerging from the survey.

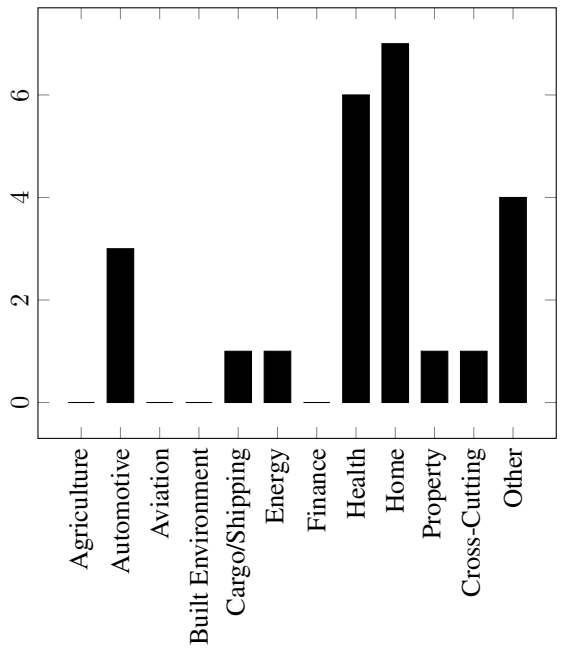

Fig. 2: Sectors analysed in the survey.

earlier analysis stage. They were reviewed and are outlined below.

The upcoming section uses extracts from the survey. Relevant scenario passages for the purposes of this study are being presented in italics. Participants are referred to either by name (i.e., where respondents indicated to a preference to have their answers attributed to them) or as *P* and an identifying number (e.g., P1).

3 Results

Following the futures and foresight approach, the nineteen respondents offered primarily 'severe' risk scenarios (high and medium-high severity level: n=16). Of these, n=11 were considered to be highly likely but they differed in terms of the expected time frame that these were likely to happen (present: n=3; within 5 years: n=6; beyond 10 years: n=5). The scenarios were frequently influenced by an incident that had previously occurred in real life and they focused primarily on the home (n=7), followed by health (n=6), and automotive (n=3). An exact overview of all analysed sectors can be found in Figure 3, which also emphasises the relevance of 'other' sectors that included, for example, critical infrastructure and leisure.

In the next section, four themes that emerged from the thematic analysis will be discussed. The themes "physical safety", "crime and exploitation", "loss of control", and "social norms and structures" frequently overlap but nonetheless provide a suitable analytical tool to contextualise emerging risk trajectories stemming from the IoT. They also help in detecting gaps about security and privacy challenges in this evolving digitised environment.

3.1 Physical Safety

The first theme is very much centred on health impacts, and potentially loss of life, deriving from the IoT. It links to both the "crime and exploitation" and "loss of control" themes but focuses on physical manifestations of impacts rather than their economic consequences. The theme covers a broad range of effects, spanning *fire or excess pressure* in heating systems (Aastha Madaan) to the wider physical security of connected buildings and infrastructure. Many scenarios relate to potential catastrophic failures and, in extreme cases, even to fatalities – for example, accidents with connected or autonomous vehicles (CAVs; P3, P13) or interference with medical devices (P2, P14, P17).

The immaturity of IoT systems, or the inappropriate use of data, is also highlighted in a number of scenarios. Respondents see a risk trajectory derived from the use of artificial intelligence in health care systems leading, if corrupted, to *erroneous treatment decisions* (P14). Similarly, the use of wellness applications and data to push *unsuitable nutritional suggestions* (P16) is mentioned, emphasising the increasing interplay between (and a paradigm shift in) the way society approaches and considers material safety, data integrity, and information security.

While this theme covers a range of intentionally malicious actions as well as accidental IoT system failures at an individual or social level, there were also several scenarios that highlighted future possible national security implications. These include the potential vulnerability of national and *shared infrastructure* (Petar Radanliev) such as *water* systems (P1, Ivana Tomic) or *consumer* IoT devices (P15, P18), for example to disrupt the supplier system; or indirect assaults through information-based attacks such as the injection of *false information* (P6).

An example of the profound safety impacts this evolving IoT system can create is evident in Extract 1. In addition to the obvious physical safety element of CAVs, this scenario also stresses both personal privacy and even national security concerns:

> Extract 1: For example, the heterogeneous nature of cars on roads can create problems: the AI used in autonomous vehicles may not be able to cope with the fact that cars in the environment may react very differently depending on whether a human or an AI is controlling its decisions. (...) Cyber-attacks on electronic control units in cars could have devastating consequences, especially if coupled with attacks onto the machine learning components of cars. (...) Autonomous driving may also lead to more intelligent car sharing services, that may actually increase the use of cars - leading to more road congestion and air pollution. The seamless tracking of car users through companies that build and operate such smart cars may also lead to further erosions of privacy and individual's autonomy and sense of autonomy. Also, if the security mechanism for autonomous cars don't contain sufficient 'bio diversity', then zero-day attacks

> on them may have the ability to take out an entire country's or region's cars. (P3)

As a consequence of the potential proliferation of such interruptions, a few respondents propose to tackle the safety and security of IoT through *quantum* cryptography (P14) as well as the development of *standards* (P17) and *regulations* (P17). However, the worry that such regulative instruments could *slow down innovation* (P17), be circumvented or simply ignored, was also raised by several experts. This in turn suggest that there may be a low level of the trust amongst the survey respondents in possible compliance and enforcement measures.

3.2 Crime and Exploitation

Related to the first theme of "physical security", the theme of "crime and exploitation" is also focused on the safety and security of the IoT, but it embeds these concerns in the larger context of deliberate abuse, primarily through illicit activities for economic, personal or political gain. The analysis of the responses reveals that participants primarily think of risk trajectories that are exploited by *criminals* (P2, 18), *hackers[s]* (P1, P8, P14), *attacker[s]* (P4, P15) and other *unknown third part[ies]* (Ivana Tomic), sometimes including *state actors* (P18) who are using similar obtrusive techniques. This conceptualisation of external, malicious agents by the surveyed experts provides insight into the types of actors that will drive IoT risk trajectories in the upcoming years.

The ability to *ransom* (P2, P10, P15, P18) data and physical assets is mentioned in a number of responses. Across the scenarios, users were frequently locked out of the use of assets through the encryption of control firmware, including *cars* (P13) or home devices such as *smart meters* (P15). IoT's 'dual use ability' (i.e., sold for one purpose but misused for another) is particularly relevant. Just as *botnets* (P18) highlight the failure of current risk assessments to consider assets themselves as an attack platform [26], future threat scenarios may also include the repurposing of IoT systems including generated data for usages than those they were *originally intended for* (Christopher Bull).

Thus, as with "physical safety", the complexity of the IoT environment and issues around errors and poor security awareness all provide the means for criminals to exploit and abuse both the technology and individuals. Besides, IoT gives malicious parties not only new opportunities, but a new scale and scope to project their power.

3.3 Loss of Control

The third prominent theme is "loss of control". It stems from the notion that, as systems are becoming more complex and sophisticated, there is a danger that society and businesses will lose their capability to guarantee important principles like privacy and security. While closely aligned to the theme of "physical safety", this theme focused more explicitly on privacy and economic factors rather than health and safety impacts. For instance, the inability to effectively deal with privacy exploitations is a recurring subject and relates to the idea of the deliberate exploitation of information, discussed above.

An example of a scenario that expresses this risk of being unable to handle and manage the emerging IoT environment is outlined in Extract 2. In it, the respondent emphasises society's increasing reliance on technology. This creates a dependency that, if revoked, has profound consequences on society's ability to engage in simple tasks that we now take for granted.

> Extract 2: In developed countries we are totally reliant on IoT to manage our homes - from the fridges to heating systems to any healthcare we might require, using social robots, apps and other IoT devices. We give up freedom for convenience. However, these systems are also vulnerable to data and network security problems, such as hacks or breaches. When these happen (which they do), our whole home shuts down and we are unable to perform simple tasks like opening the fridge, turning on a tap (since they operate with sensors) or using the microwave to heat up food. We are also unable to fix the systems ourselves even if we had the technical skills given the proprietary 'black box' software and hardware used to power these systems. The systems are controlled by enormous corporations, on the basis of having won government tenders. People living in these houses become increasingly passive and accepting of their situations, including when the houses 'shut down' because of problems. There is no outcry and no need for intervention from the corporations or government unless the shutdown lasts for a protracted period of time. (P19)

Extract 2 exhibits a lot of patterns that are evident across the data set. Firstly, it highlights the frequency of smart home examples, and the prevalence of consumer home device illustrations such as smart fridges that seem to be one of the most accessible IoT reference points that survey respondents drew upon.

Secondly, the scenario underlines the importance of access. As data is not something contained but rather external and in constant transmission, many scenarios hint at the remote and non-remote control of information, as seen in the instance of ransomware. In particular, the 'remote threat, local fix' idea is widely shared. For instance, an attacker may be able to *access data on any computer connected to the Internet* (P8) or continue to *collect data after he leaves the building* (P1). However, while an attacker may be able to access and control IoT systems from afar, many scenarios allude to the situation in which *remote remediation is not possible* (P13) – instead, requiring physical access to IoT systems in order to implement solutions. This creates enormous challenges and touches upon the necessity for speed of response and rapid fixes.

Thirdly, Extract 2 makes an important reference to time. Respondents offer scenarios in the course of which the *process of implementing the anti-jamming system fully took ten days* (Ivana Tomic). As a result of this delay, as well as the asymmetry between the time, scale, and cost of exploiting a software bug versus the time spent to find a remediation, interruptions to everyday life are far more profound.

Lastly, the theme of "loss of control" points to the notion of society's ability and capability to acknowledge, respond, and consequently manage risks deriving from the IoT. On the one hand, the scenarios highlight that people are no longer able and skilled enough to deal with the loss of access to and potential flaws in these systems. On the other hand, the scenarios also emphasise that society is increasingly also not permitted to amend glitches and defects, as restrictions such as intellectual property or 'black box' systems prevail. In this regard, society has reached a state of passivity and dependence that is the epitome of this perceived risk of loss of control.

3.4 Social Norms and Structures

The fourth and final theme is centred on changes to societal behaviours, norms, and structures. It highlights a shift in society's perceptions of things like *privacy and individual autonomy* (P3) or *free speech* (Christopher Bull). This theme is the ultimate manifestation of the large-scale social transformation that IoT may create and the risks that derive from it.

One of the most fundamental changes relates to the status of privacy in the near future. No scenario anticipated an enhancement of privacy; most predicting its erosion. Some respondents emphasised that society will *give up freedom for convenience* (P19) and that even if alternative systems were to be established, nobody would *dare [to] switch* (P4) as products or data are being *held hostage* (P4) and *filter bubble[s]* (Chris Speed) are so common.

Along those lines, participants discussed two potential and contradicting outcomes. One involves a radical transformation such as when *European citizens lose trust* (P17) in IoT and *hysteria* (P15) and *public outcry* (P14) erupts. This could be the result of a significant trigger such as the death of an influential *politician's mother* (P2), the loss of essential utilities like *electricity* (P15), or the outburst of *civil unrest* (Ivana Tomic). The other future is a world in which passivity dominates and society becomes *accepting* of (P19), and somewhat apathetic to, a situation in which individuals are no longer troubled by IoT privacy intrusions and security failures. Extract 3 gives an example of the latter:

> Extract 3: In the year 2025, smart devices are in every part of our homes, they are appliances of convenience (e.g., smart TVs, fridges, ovens and chairs) and those which some of us depend on for our assisted living (e.g., health-related smart technologies). Given the amount of data that these devices begin to amass, one immediate impact is that individuals start to become even more desensitised to privacy and its importance. Privacy is full traded for convenience, and social norms evolve sufficiently that the IoT is considered "normal" and those who shun these novel technologies are viewed as antiquated. (P2)

This change with its clash of 'old' and 'new' paradigms would require amendments to the way society understands and conceptualises labour, free will, and choice. In particular the latter is projected to decrease, stemming in part from restrictions set out in the *service agreements* (P15) or the predominance of big market players such as *Facebook* (Chris Speed) or *Apple* (P13) which hold power over users. Individuals would consequently lack suitable alternatives that provide them with the opportunity to freely give consent and remain in control over how their data is being collected and processed.

In this anticipated future, society becomes accustomed to decisions *being made automatically* (P14), *elections* being interfered with by adversaries (Nader Sohrabi Safa), and data being tracked and used *for something it was not originally intended for* (Christopher Bull). Hence, profoundly dystopian scenarios arise in which the IoT will *exclude particular audiences* (Chris Speed) and in which *unauthorised research* (P16) by app and IoT developers can flourish.

4 Discussion

This research sought to analyse emerging risk patterns in descriptions of anticipated IoT scenarios. Through the use of methodological tools drawn from the futures and foresight literature, we identify four themes in the survey data. These provide valuable analytical frameworks to contextualise emerging risk trajectories and help detecting gaps about security and privacy challenges in the IoT. There are two main avenues for discussion that arise from this study. One avenue is the analysis of the four cross-cutting themes and what can be extracted from them for consideration of future IoT risk trajectories. The second avenue is our reflection of this study's methodological approach and the potential weaknesses in using surveys to develop scenarios to predict risk in emerging technologies.

4.1 Emerging Risks in the IoT

The "physical safety" theme highlights that the coupling of cyber and physical components together in increasingly complex IoT systems will result – and in fact, is already resulting in – the expansion of the cyberattack surface to include potentially life-threatening consequences [27]. This risk is connected with IoT's potential to experience inadvertent system incompatibilities or weaknesses between sub-systems [28]. In this ecosystem, the tradition model for securing assets based on keeping out an unauthorised actor through access controls and erecting barriers such as firewalls, is unlikely to remain effective. The interdependence of components of different origin, age, and provenance, suggests that the security provision of these systems will have

to be both adaptable and timely. Along those lines, various IoT security principles are currently being published, including the UK Department for Transport's CAVs guidelines [29], The Digital Standard [30], and recommendations concerning the communication of IoT policies for manufacturers [31]. Essentially, this theme links the potential for injury or even loss of life to required innovation in cybersecurity on the level of a paradigm shift – significantly distinct from the last four decades of network, device, and information security.

The second theme on "crime and exploitation" reveals how threats will increasingly exploit the cyber-physical dependency of IoT systems to deny access to physical as well as digital assets. This interdependency presents a novel risk vector that not only increases the range of assets susceptible to ransom, but also creates recovery challenges when re-enabling systems. The misuse of systems and data was referred to several times which points to anticipated vulnerabilities in critical systems that can be commoditised or monetised by criminals. It also highlights the greatly expanded threat vector which, if exploited, would be lucrative enough to attract considerable attention from malicious actors.

The third theme, "loss of control" raises questions about people's capabilities, resilience, and needs in this emerging IoT environment. Hence, societies capacity to cope with outages as well as interruptions and technological change (see: Extract 3) creates new skill demands. These require users as much as businesses and policy makers to take appropriate proactive, as well as reactive, actions to increase the IoT's benefits and mitigate against its risks. The potentially grave consequences of a lack of situational awareness combined with legal and technical restrictions in a hugely automated ecosystem were emphasised by various respondents. In particular, society's ability to understand the technologies that they engage with and rely upon, and their capacity to operate, repair, or do without them featured heavily.

This notion of a 'helpless' society, unable to live and fix even basic everyday household tools indicates an expectation that the IoT will potentially undermine resilience [32]. In some ways, this is an enhanced version of a perennial anxiety about technological dependence similar to concerns about a pilot's inability to fly a plane without the autopilot or operate in instances where GPS systems are unavailable. The scenarios seem to suggest that a fully automated future may require similar prearranged or managed experiences for a prospective IoT society no longer familiar with *pen and paper* (P17). Indeed, a recent publication by van Deursen and Mossberg [33] argues that comparative advantages of the IoT will vary based on differentiated skills and resources, enabling smaller groups of people to benefit, and disadvantaging others in new ways. Thus, in order for this future society to prepare and mitigate those potential risks, users' knowledge and strategic skills will have to be heightened and improved.

The last theme on "social norms and structures" also points to expected societal transformations that derive from technical developments. Many respondents echo 'The New Normal' scenario created by scholars at UC Berkley [20] or the reinterpretation of privacy as discussed in the future scenarios of Williams et al. [19]. All of them embody the idea of privacy expectations deteriorating and society's makeup and composition being transformed by the *convenience* (P2) that emerging technologies create. In particular the anticipated clash between generations is thereby noteworthy and contains the idea that *younger generations (. . .) never experienced such privacy and see less value in it* [20, p. 24]. Counter to these arguments about passivity, research shows that young people do still value privacy [34]. A handful of scenarios expected a public outcry following a significant trigger. As privacy issues in particular are far from being settled and as society is still very much struggling with these debates, we might anticipate that the IoT will ultimately complicate these discussions further. Many of the scenarios reflected, to some extent, these ongoing tensions and risks – that not only stretch across generations but different actors, demographics, and contexts. The question that emerges from these scenarios then, is whether the IoT will propel these tensions to a point at which passivity takes hold or the reverse.

4.2 Methodological Considerations

In addition to these risk trajectories and the themes that emerged from them, it is also important to examine the potential for expert elicitation and scenarios to accurately predict risk in emerging technologies. One key issue here is the notable absence in the survey results of certain content and actors. Firstly, the scenarios are very much centred on malicious, third-party actors such as criminals, rather than employees that both deliberately (i.e., insider threat) or accidentally (i.e., human error) create risks. Similarly, failures derived from software updates that result in the incompatibility or compromise of systems are acknowledged in the literature but did not feature in the scenarios. It would appear then that the 'mundane' threat seems more difficult to envision or less likely to feature in threat scenarios when experts are asked to think about future risks.

Secondly, unprecedented attacks were not prevalent in the scenarios. Instead, respondents continue to think of known threats such as the access and restriction of information (e.g., through *ransomware*; P2, P10, P15, P18) or the intentional modification of information (e.g., similar to *fake news*; Nader Sohrabi Safa). Alternative options, such as the withholding of information (e.g., through censorship) are not part of the analysed scenarios and reveal the need to think more thoroughly about the possible changes to attack vectors IoT will pose. The scarce 'thinking outside the box' corresponds to the International Risk Governance Center's [35] perspective that the assessment of future developments, especially in regards to the Internet, goes beyond most people's imaginations.

Thirdly, the absence of small and medium-sized enterprises compared to the prominence of international, established corporations (e.g., Facebook, Apple) raises the question of whether IoT, together with trade integration, globalisation, and industry consolidation, has the potential to make large enterprises even

larger. An example of such a dynamic is the acquisition of AlertMe, a company developing platforms for running various domestic 'smart' devices such as the Hive thermostat, by British Gas in March 2015 [36]. The 65m deal gave the innovative IoT manufacturer greater market penetration but may be a precedent for the accumulation of IoT developers by established market players. Whether this increasing homogeneity and lack of market diversity (see: "Social Norms and Structures") can result in a risk of its own is therefore worth further exploration.

The reflection on the absence of such considerations and radical new ideas – or at least ideas which do not draw on existing anchors such as known corporations or attack vectors – reveals the weakness in using formalised means to collect experts' narrative descriptions of emerging risks. It also emphasises the value in complementing this standardised exercise with other tools and mechanisms to create more diverse anticipatory scenarios.

4.3 Limitations

Limitations of the current research include the study designs' self-selection bias, the difficulty to assess future risk scenarios purely through standardised questionnaires, as well as the restricted user sample which has so far been limited to PETRAS and its affiliated research and industry community. The survey is also set out to assess the perception of respondents, limiting the generalisability of the findings as scenarios may be influenced by participants' distinct research expertise or other salient factors such as the prominence of topics in, for example, the news.

4.4 Conclusion and Future Work

Despite these limitations, this study offers unique avenues for further research and provides important insights for the futures and foresight literature. To this end, we aim to expand our sampling procedure with the hope to increase and enlarge the sample size. Thus, we are exploring various survey design options, and hope to increase the number of survey items through, for example, the inquiry of demographic information, allowing us to draw comparisons between particular categories of respondents (e.g., academics, industry actors). This will require more explicit inclusion and exclusion criteria for participants. In addition, the research team will consider whether to allow for the submission of both risk and opportunity scenarios (i.e., dystopian and utopian futures), which would offer contrasting viewpoints and could provide further insights into measures that will need to be taken to halt risk trajectories.

In the meantime, the current paper prompts useful conversations about the role IoT will play in an increasingly digitalised society. Scenarios, while not representative as such, can inform stakeholder groups such as designers, manufacturers, insurers, policy makers and even the public about anticipated developments. This forward-thinking approach is especially helpful for policy areas where there are global challenges, significant uncertainties, and where society is required to be prepared for all conceivable outcomes. Hence, connecting the scenario methodologies used here with adaptive policy making processes [4] and international developments on IoT [37] can be a worthwhile process for governments and regulatory bodies to prepare for these risks and opportunities and establish a map of potential futures. Over the next months, we will embed the survey results into our broader thinking about the future of IoT and complement the questionnaire with stress-tests through expert workshops which should guarantee a more holistic assessment, encourage deep futures imagining, and helps the creation of representative case studies that move beyond 'big bad smart fridge' scenarios.

Acknowledgements

This research was supported by the Engineering and Physical Sciences Research Council and partner contributions under grant EP/N02334X/1. The authors also received financial support from The Society of Lloyd's.

The authors would like to thank all survey respondents, including the following named participants Aastha Madaan Andrey Nikishin, Carsten Maple, Chris Speed, Christopher Bull, Barnaby Craggs, Jason R.C. Nurse, Ivana Tomic, Jan-Peter Kleinhans, John M Blythe, Nader Sohrabi Safa, Petar Radanliev, Reuben Binns, Richard Milton, Thanassis Tiropanis, as well as the remaining participants that wish to remain anonymous. We are also indebted to Michael Veale and appreciative of his LaTeX skills.

References

[1] L. Franceschi-Bicchierai, "Hackers Make the First-Ever Ransomware for Smart Thermostats," *Motherboard*, 07-Aug-2016. [Online]. Available: https://motherboard.vice.com/en_us/article/aekj9j/internet-of-things-ransomware-smart-thermostat. [Accessed: 09-Jan-2018].

[2] Somerset Recon, "Hello Barbie Security: Part 2 - Analysis," *Somerset Recon*, 25-Jan-2016. [Online]. Available: http://www.somersetrecon.com/blog/2016/1/21/hello-barbie-security-part-2-analysis. [Accessed: 12-Oct-2017].

[3] J. Golson, "Jeep hackers at it again, this time taking control of steering and braking systems," *The Verge*, 02-Aug-2016. [Online]. Available: https://www.theverge.com/2016/8/2/12353186/car-hack-jeep-cherokee-vulnerability-miller-valasek. [Accessed: 12-Oct-2017].

[4] L. Tanczer, I. Brass, M. Elsden, M. Carr, and J. Blackstock, "The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape," in *Cybersecurity Governance*, R. Ellis and V. Mohan, Eds. Wiley, forthcoming.

[5] F. Mattern and C. Flrkemeier, "Vom Internet der Computer zum Internet der Dinge," *Informatik Spektrum*, vol. 33, no. 2, pp. 107–121, Apr. 2010.

[6] F. Loit, A. Sivanathant, H. H. Gharakheilit, A. Radford, and V. Sivaramant, "Systematically Evaluating Security and Privacy for Consumer IoT Devices," in *IoT S&P 2017*, Dallas, Texas, 2017, pp. 1–6.

[7] N. Apthorpe, D. Reisman, S. Sundaresan, A. Narayanan, and N. Feamster, "Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic," *arXiv:1708.05044 [cs]*, Aug. 2017.

[8] N. Cam-Winget, A. R. Sadeghi, and Y. Jin, "Invited: Can IoT be secured: Emerging challenges in connecting the unconnected," in *2016 53nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, 2016, pp. 1–6.

[9] I. Brass, L. M. Tanczer, M. Carr, and J. Blackstock, "Regulating IoT: Enabling or Disabling the Capacity of the Internet of Things?," *Risk & Regulation Magazine of the Centre for Analysis of Risk and Regulation (CARR)*, vol. 33, no. Summer, pp. 12–15, 2017.

[10] J. Gidley, *The future: A very short introduction*. Oxford: Oxford University Press, 2017.

[11] W. Bell, *Foundation of Futures Studies, Volume 1: History, Purposes and Knowledge*. Piscataway, NJ: Transaction Publishers, 2004.

[12] A. Hines and P. Bishop, *Thinking about the Future: Guidelines for Strategic Foresight*. Washington, DC: Social Technologies, 2009.

[13] I. Miles, D. Meissner, N. S. Vonortas, and E. Carayannis, "Technology foresight in transition," *Technological Forecasting and Social Change*, vol. 119, pp. 211–218, 2017.

[14] L. Georghiou, J. Cassingena Harper, M. Keenan, I. Miles, and R. Popper, *The Handbook of Technology Foresight: Concepts and Practice*. Cheltenham: Edward Elgar, 2008.

[15] P. Bishop and A. Hines, *Teaching about the Future*. London: Palgrave Macmillan, 2012.

[16] G. Burt and K. van der Heijden, "First steps: Towards purposeful activities in scenario thinking and future studies," *Futures*, vol. 35, no. 10, pp. 1011–1026, 2003.

[17] J. F. Coates, "Scenario planning," *Technological Forecasting and Social Change*, vol. 65, no. 1, pp. 115–123, 2016.

[18] P. G. Raven and S. Elahi, "The New Narrative: Applying narratology to the shaping of futures outputs," *Futures*, vol. 74, pp. 49–61, Nov. 2015.

[19] M. Williams, L. Axon, J. R. C. Nurse, and S. Creese, "Future scenarios and challenges for security and privacy," in *2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI)*, Bologna, Italy, 2016, pp. 1–6.

[20] CLTC, "Cybersecurity Futures 2020," Center for Long-Term Cybersecurity, University of California, Berkeley, 2016.

[21] ENISA, "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures," European Union Agency For Network And Information Security, Heraklion, Greece, Nov. 2017.

[22] AIG, "Is Cyber Risk Systemic?," American International Group, Unknown, 2017.

[23] R. Tzezana, "High-probability and wild-card scenarios for future crimes and terror attacks using the Internet of Things," *Foresight*, vol. 19, no. 1, pp. 1–14, 2017.

[24] C. Shepherd, F. A. P. Petitcolas, R. N. Akram, and K. Markantonakis, "An Exploratory Analysis of the Security Risks of the Internet of Things in Finance," in *Trust, Privacy and Security in Digital Business*, Cham, 2017, pp. 164–179.

[25] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative research in psychology*, vol. 3, no. 2, pp. 77–101, 2006.

[26] J. R. C. Nurse, S. Creese, and D. D. Roure, "Security Risk Assessment in Internet of Things Systems," *IT Professional*, vol. 19, no. 5, pp. 20–26, 2017.

[27] Y. Sun *et al.*, "Attacks and countermeasures in the internet of vehicles," *Ann. Telecommun.*, vol. 72, no. 5–6, pp. 283–295, Jun. 2017.

[28] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.

[29] Department of Transport and Centre for the Protection of National Infrastructure, "The Key Principles of Cyber Security for Connected and Automated Vehicles," HM Government, London, Aug. 2017.

[30] Consumer Reports, Disconnect, Ranking Digital Rights, The Cyber Independent Testing Lab, and Aspiration, "The Digital Standard," *thedigitalstandard.org*, 2017. [Online]. Available: `https://www.thedigitalstandard.org/the-standard`. [Accessed: 24-Feb-2018].

[31] G. Kaupins and J. Stephens, "Development of Internet of Things-Related Monitoring Policies," *Journal of Information Privacy and Security*, vol. 0, no. 0, pp. 1–14, Jan. 2018.

[32] M. Carr, *US Power and the Internet in International Relations: The Irony of the Information Age*. London: Palgrave Macmillan, 2016.

[33] A. J. A. M. van Deursen and K. Mossberger, "Any Thing for Anyone? A New Digital Divide in Internet-of-Things Skills," *Policy & Internet*, 2018.

[34] A. E. Marwick and danah boyd, "Networked privacy: How teenagers negotiate context in social media," *New Media & Society*, vol. 16, no. 7, pp. 1051–1067, Nov. 2014.

[35] International Risk Governance Center, "IRGC Guidelines for Emerging Risk Governance. Guidance for Governance of Unfamiliar Risks," IRGC, Lausanne, Switzerland, 2015.

[36] I. Lunden and S. O'Hear, "British Gas Buys UK Smart Home Pioneer AlertMe In $100M Deal," *TechCrunch*, 13-Feb-2015. .

[37] L. Tanczer, F. Yahya, M. Elsden, J. Blackstock, and M. Carr, "Review of International Developments on the Security of the Internet of Things," PETRAS IoT Hub; STEaPP, London, 2017.