Critical Visualisation: A Case for Rethinking How we Visualise Risk and Security

Peter Hall, Lizzie Coles-Kemp and Claude Heath

draft 26th April 2015

Abstract

In an era of high-profile hacks, information leaks and cyber-crime, cyber security is the focus of much corporate and state-funded research. Data visualisation is regarded as an important tool in the detection and prediction of risk and vulnerability in cyber security, but discussion tends to remain at the level of the usability of visualisation tools and how to reduce the cognitive load on the consumers of the visualisations. This focus is rooted in a desire to simplify the complexity of cyber security. This paper argues that whilst usability and simplification are important goals for the designers of visualisations, there is a much wider discussion that needs to take place about the underlying narratives upon which these visualisations are based. The authors take the position that the narratives on which cyber security visualisations are based ignore important aspects of cyber security and that their visual form causes the producers and users of these visualisations to focus too narrowly on adversarial security issues, ignoring important aspects of social and community-based security. By situating the discussion of security visualisation in a larger socio-historical context, the limitations and implications of current ways of seeing risk become more apparent. Cyber security might also learn from other disciplines, specifically critiques of artificial intelligence and the discourse and methods of post-war urban planning. In this way, the paper follows a humanities tradition of situating the focus of analysis in a broader tradition of scholarship and critiquing current practices from this wider context. The purpose of such critique is stimulate reflection on underlying principles and the implications of different approaches to operationalising those principles. Case studies of participatory modelling and crowdsharing projects where discussion is focused on social and spatial practices that foster resilience are discussed in closing.These case studies illustrate the potential for a wider range of visualisations and examples are provided of alternative visualisations.

1 Introduction

In its 2013 impact assessment, the European Commission stated that there is an "insufficient level of protection" against network and information security incidents undermining the services that support our society" (eg. public administrations, finance and banking, energy, transport, health).[1] This suggests a complex problem permeating all levels of society, but news headlines

[1] European Commission. 2013. Executive Summary of the Impact Assessment. Accompanying the document Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union. Strasbourg, July 2013.

are increasingly preoccupied with cyber-terrorism and counter-terrorism (such as the Sony hack of 2014), which tends to constrain discussion of information security to high stakes, high profile incidents. Discussion at the popular level assumes that the best hope of cyber security is better surveillance, and information visualisation has assumed an important role in fuelling this hope by presenting visually compelling images and tools for modelling risk and vulnerability. But with growing and ageing populations and the continuing push to move services online, including tax filing, retirement, banking and medical interactions, the social complexity of information sharing practices presents a far more complex and nuanced picture of security" than typical network diagrams and tree maps currently achieve.

The argument of this paper is that the predominant mode of visualisation in security comes from a statistical and probabilistic approach that perpetuates a particular way of seeing the problem and that is based on a relatively thin cyber security narrative. The dominant narrative is one of cyber security as *control*, whereas critics argue that we are in fact, *post control* in many senses and need to look to human as well as technological security to respond to cyber security challenges.

Drawing from the lessons of critical cartography, this paper proposes that our visualisation tools are wedded to a post-Enlightenment system of beliefs - whether we call it enumerative, rationalistic or military-industrial - tools which have been extensively critiqued as technologies of a disciplinary, or control society. The computing clouds, socio-technical networks and "wicked problems" of today cannot, technically, be contained, despite claims for "big data"[22] of today cannot, technically, be contained, despite claims for "big data" [1] and [6]. If, as its critics suggest, the discourse and visualisation of risk serve to perpetuate a performance of maintaining security rather than investigating what makes social groups, communities, nations, secure, then how else might the issue be approached?

2 Faith in Data Spheres

According to the German philosopher Peter Sloterdijk, the impulse to make visualisations, maps and globes of space, knowledge and our belief systems appears to date back to the 1490s (Fig. 1), specifically the era in which the possibility unfolded that the earth was not only not enclosed by protective domes, neither was it at the centre of the universe. With the loss of those "immunities" as Sloterdijk calls them, Europeans began fetishistically building and examining ball-shaped images of earth, as if this would console them for the fact that they no longer existed inside a ball, only on a ball. He then extends this fetishistic project of building and defining finite spheres of knowledge and belief to industrial scale civilisation, the welfare state, the world market and the media sphere. We might add to that list the recent obsession with visualising spheres of data:

> all these large scale projects aim, in a shelless time, for an imitation of the now impossible, imaginary spheric security. Now networks and insurance policies are meant to replace the celestial domes [30, p.25].

Many current visualisations of internet traffic demonstrate this same spheric faith, such as Barrett Lyon's map of the Internet from 2003, showing traffic between the major ISPs (Fig.

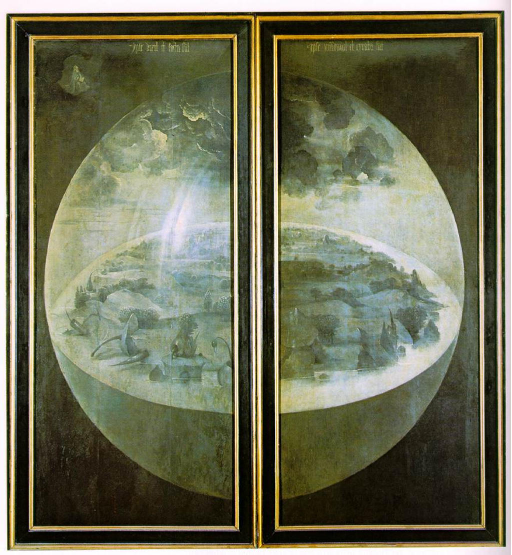

Figure 1: Sloterdijk's spheres: Hieronymus Bosch, Garden of Earthly Delights (1503-4).

2). On a par perhaps with the "blue marble" photograph of the Earth taken by Apollo 17's astronauts in 1972 (Fig. 3), it presupposes a finite project: the entire internet represented as a sphere of data. In many ways, the visualisation is a summation of presumptions. It not only suggests a containable problem-space; it presumes a separation of network traffic from the built environment in which it takes place.

The visual roots, so to speak, of this giant sprawling system, lie in the idea of the tree of knowledge, which as Manuel Lima has shown, similarly reveal a rationalistic faith in finite systems from the early Modern era, "the idea of capturing the entirety of human knowledge and classifying it by means of a tree" [17, p.33-41]. Trees have proven popular memes in predictive methods of visualising potential information security attacks and countermeasures, but come with the recurrent problem of growing. When tree diagrams grow too big, they become difficult to comprehend.

If, to return to Sloterdijk's diagnosis, spheric security is imaginary, then we are left with the familiar compromised goal of achieving *sufficiently secure* status. The compromise is in deciding what can be modeled and visualised and what can be left out.

3 Reducing Complexity

This brings us to a central paradox of visualisation; we visualise to make complex problems easier to understand and easier to navigate, but in order to do this we must simplify the complexity. It is this process of reduction and abstraction that often reveals the intent of a visualisation. In the critical discourse of post-war cartography, decisions made behind the scenes on what to show and what to omit from maps will often reveal their larger, territorial agendas [11] and [37].

Designers aim to achieve simplicity or clarity in visualisations by making them persuasive

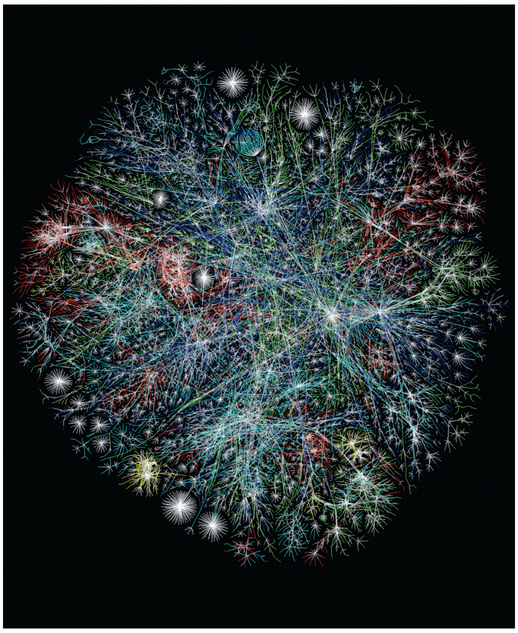

Figure 2: The Opte Project Map of the Internet, by Barrett Lyon (2003).

and/or easy to use, which suggests two categories of visualisation; the rhetorical and explorative. Rhetorical visualisations function primarily to make a point and inform a given audience; these are typically static images governed by a discourse focused on graphical integrity, elegance and clarity typified by the approach of Edward Tufte (show the data, do not distort the data, etc). Tufte's identification of infographic decoration as "chartjunk" or his account of how the oversimplification endemic to Powerpoint presentation software played a part in a Space Shuttle disaster are illustrative of this goal [31] and [32].

Explorative visualisations tend to pose questions, and are often dynamic and interactive. The discourse, focused on reducing cognitive load and making interactions with the computer "user-friendly." The visual information mantra of interactive media-oriented researcher Ben Shneiderman was overview first, zoom and filter, then details on demand" [28]. This position accommodates a technique known as "progressive disclosure" which aims at initial simplification followed by the option of revealing additional content and options. It assumes, after psychologist William Edmund Hick, that the time needed to make a decision increases with the number of variables [17, p.92]. Such an approach can be described as cognitivist, in that it draws a trajectory from rationalistic human-computer interaction approaches associated with classical artificial intelligence. It is this visual tradition that has been primarily adopted by cyber security researchers and practitioners.

Figure 3: Apollo 17.

4 Technologies of Management

While clarity, usability and “details on demand” are uncontroversial standards that are understandably upheld in instrumentalist design discourse focused on improvement of human-computer and human-visualisation interaction, it is important to situate such aims in a larger historical discourse in order to understand the wider potential for the development of cyber security visualisation. The history of data visualisation can be traced back to the emergence of “thematic maps” in the 17th century (Fig. 9), which as geographer Jeremy Crampton has noted, was precisely when enumerative strategies for population management became a pressing concern for industrial and imperial Europe. They became critical to censuses, census mapping, and distributions of populations across territories” [5, p.137]. Linking this discourse to contemporary practices of geosurveillance, Crampton follows Foucault in tracking how such technologies of management emerged as a means to: (a) think of people and space as resources that required management and protection, and (b) to normalize through the gathering and categorizing of data about populations, such as censuses.

Standard approaches of visualising threats to cyber security deploy the Tufte and Shneiderman vocabulary in technologies designed to extend the categorisation and identification of abnormal behaviours. For example, Raffael Marty’s 2009 text Applied Security Visualization uses “progressive disclosure” for iterative elimination of “outliers,” based on analysis of which network nodes are generating traffic with large packet sizes and whether they reveal suspicious

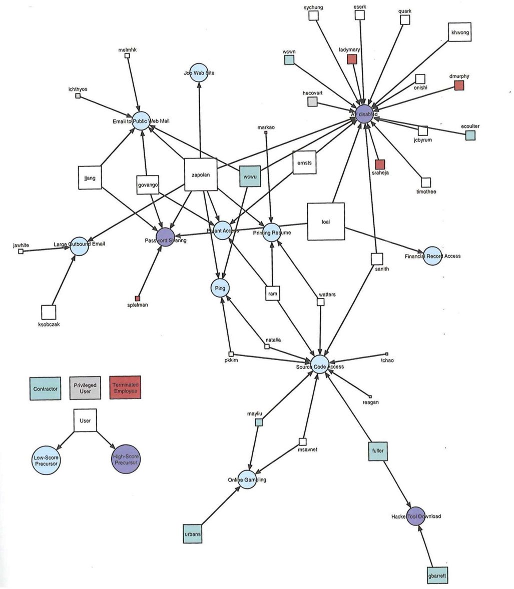

Figure 4: ”Insider candidate list”, shown as a link graph. From Raffael Marty, Applied Security Visualization, 2009.

patterns of distribution [18]. This way, Marty arrives at a suspect botnet controller. Visualisation, according to Marty, is worth “a thousand log records”. A visual, as opposed to textual approach to risk analysis, is argued to facilitate the task of analysing data traffic by relying on the human brain’s efficient ability to process images and recognise patterns. A link graph (Fig. 4), showing “malicious insider threat” derived from network traffic data is developed by listing “precursors” (suspicious behaviour) to an insider attack and ranking them according to a scale of potential danger. This reflects a chief concern of information security in the era of cloud computing; analyses of risks and threats in cloud computing reports concur that insider attacks and malicious insiders are a “major technical risk and among the top 10 threats” [2]. But the surveillance and identification of potential threat also recalls the shift that took place with legal reforms of the 18th and early 19th centuries, famously observed by Foucault, from the punishment of crimes to the identification of criminal potential:

> The idea of dangerousness meant that the individual must be considered by society at the level of his potentialities, and not at the level of his actions; not at the level of the actual violations of an actual law, but at the level of the behavioural potentialities they represented [8, p.57].

Marty’s visualisation presupposes fixed behaviour types: insiders are either loyal or malicious. Such a distinction complies with militaristic approaches of the past, but in cloud computing the distinction between insider and outsider is not easy to make. The concept of insiderness is entwined with notions of trust, homogeneous values, authorisation, empowerment and control [4].

5 Socio-technical problems and the AI legacy

Recent developments in information security, including the EU-funded TREsPASS project, from which this paper draws evidence and a research framework, explore the limits and possibilities of visualisation to support tools focused on predicting "socio-technical" security risk. The hyphen that connects the social and technical attempts to bridge a fundamental disciplinary and philosophical divide. Loosely characterised, it bridges (or hopes to) the fields of cryptography and human-computer interaction with the arts and social sciences. To risk putting too much weight on the hyphen, it also bridges two sides of the artificial intelligence debate: one side that considers it possible for machines to think, the other that does not. To go back to the historical initiation of this debate, it is useful to remember that Alan Turing's machine, which famously cracked the Enigma code in World War II, was part of his larger philosophical inquiry into thinking machines. Turing's "imitation game" proposed behavioural similarity as a measure of machine intelligence: if the output of the machine and the human could not be detected, the machine is, effectively, thinking. As is well known, the cracking of the enigma code was made possible because of human sloppiness in following the security protocols [20]. This point seems to support the phrase, popular in the security community, that humans represent the "weakest link" [33], suggesting that if the machines were left to themselves, there would be no security threat. But the absurdity of that position should give us a clue that the perspective is skewed. The critique of classical artificial intelligence (as derived from Turing) that was most famously furthered by Hubert Dreyfuss makes the point that human intelligence is embodied and situated; it cannot be abstracted and isolated, and reproduced as a set of rules and symbols. The world as we understand it, according to Dreyfuss and his phenomenologist forebears, is not something independent of human perception; its structures change as a result of human activity; it is manifested in human experience [3, p.7]. Critics of our rationalistic age, then, fear that increasingly we are measuring and conforming human behavior to the logic and requirements of machines. Terry Winograd and Fernando Flores have developed the AI critique to argue that computer systems need to be designed to take into account that the machines must function in the human world, communicating with humans [3, p.21]. Despite the apparent advances in AI research, visualisation appears to sit firmly in a cognitivist position premised on a disembodied intelligence.

Both the rhetorical and explorative approaches to visualisation tend to aspire to establishing a coherent and universal set of rules so that visualisations do "function in the human world", but the explorative approach is entrenched in the classical AI camp. A key text by Colin Ware adopts a positivist, rationalistic approach, presuming a universal model of human perception that internally processes images seen in the world [36]. Ware cites a neural network model of structural object perception, developed by Hummel and Biederman [14], who give a highly mechanical account of how the (universal) human brain goes through a hierarchical sequence of processing stages leading to object recognition. "Visual information is decomposed first into edges, then into component axes, oriented blobs and vertices" [36, p.255].

The critique of classical AI is significant for information security issues. If human intelligence is embodied and situated, then the limits to technologies that can detect socio-technical risks and vulnerabilities would seem to loom large. The phenomenological model of intelligence suggests that the uniqueness and situatedness of each risk scenario inevitably thwarts the project to abstract, predict and ultimately universalise human behaviour. The post-Turing school might counter, however, that it is just a matter of building a predictive model fine-grained enough to define all the variables. As noted above, cyber crime is typically modeled by assessing precursors based on both suspicious behaviour patterns in network traffic and targeted insiders with a potential to turn "bad" (eg. a disgruntled employee). Yet predictive assessments used in information security struggle to identify behaviour that is improvised rather than premeditated.

6 Predictive Assessment and Profiling

The surveillance model of information security also poses significant political questions. Automating the identification of abnormal behaviour may seem pragmatic to a security practitioner, but seen as the offshoot of a broadening practice of state and law officials, it speaks to a larger civil liberties debate. Crampton notes how contemporary crime mapping enables geoprofiling to isolate behaviour that does not conform to the norm, but points to a controversial outcome in, for example, the high profile case of racial profiling of African-American drivers by police on the New Jersey turnpike. Foucault's distinction between making criminal judgement based on violations of the law and judgements based on perceived potential for crime is thus made vivid.

This line of critique also has an impact on the attack tree approach to security visualiation being explored as part of ongoing research. Based on predictive modeling of risk, it extends a model of security that depends for support on what Crampton calls a "discourse of risk" [5, p.139].

Crudely characterized, the notion that thinking machines and risk visualizations can be developed to assist in identifying vulnerabilities and malicious insiders represents a "search and destroy" approach to information security that reveals its military underpinnings. As W.J. Perry, the former US undersecretary of State for Defense, famously put it, "once you can see the target you can expect to destroy it" [34, p.4]. Paul Virilio has argued that the logistics of perception are inseparable from the tactics of war, from the use of military photography and film in aerial reconnaissance during world War 1, to the spy satellites, video missiles and drones in World War 2 and the "ubiquitous orbital vision of enemy territory" today. He writes, "There is no war ... without representation".

Foucault's famous theorization of the panopticon as the blueprint for today's disciplinary society [7], with its inclination to observe and normalise, casts security visualization tools in a revealing light. The concept for the panopticon's design, by social theorist Jeremy Bentham was for a structure in which a single watchman could observe all inmates of an institution without the inmates knowing if they were being watched or not. As a result they act as though they are being watched at all times, which, Foucault's contemporary interpreters have argued, is a condition of the networked age: not only is computer work easier to track, our daily social activity is voluntarily recorded and uploaded into vast databases, suggesting that much daily activity is performed in the knowledge that it destined for public view. Visualisations that depict potential risks as well as actual attacks seen to contribute to the performance of panoptic surveillance. The word performance is operative, however, since the great facilitator of cyber-attacks is anonymity. Much as the watchman in the panopticon could not physically watch all inmates, neither can information visualisation capture all threats to a system's security. So the "search and destroy" visualisation must perform a kind of mythical omniscience; it is a weapon in the trajectory of "shock and awe" tactics.

To develop this point, it is worth considering the position of one of security's harshest critics. In Mark Neocleous's view, the fearmongering of security experts, politicians and opinion leaders, serves a specific purpose. While purporting to address security, security politics has suppressed all political debate. Security has become so all-encompassing a theme that it marginalises all others [21, p.185]. By extension, then, do the visualisations of information networks and their risk and vulnerability do anything more than provide dazzling baubles with which to impress a public into thinking that we are in a state of insecurity, but something is being done about it by the experts? Or, perhaps, something is being done about it by the experts' technologies? If subjected to Neocleous's critique, the entire field of applied security visualisation is governed by nothing more than a kind of pageantry, to give the appearance of doing something.

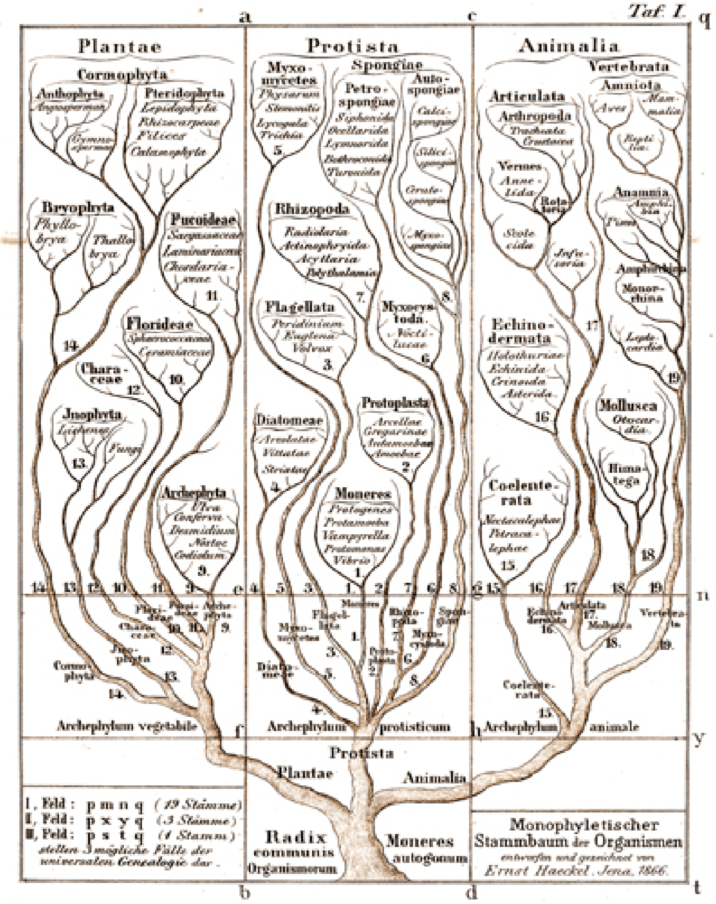

Figure 5: Haeckel.

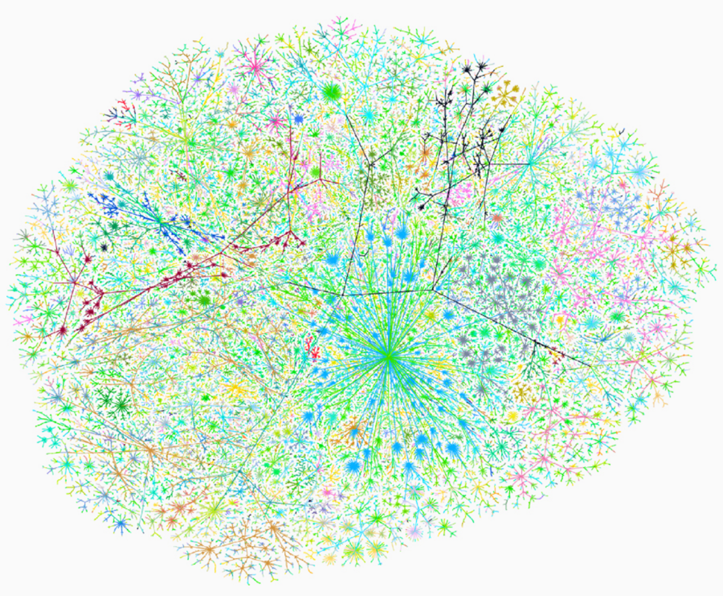

Figure 6: Lumeta jan99.

7 Security as Resilience: An Inverted Approach

The challenge can be faced in a different way, however, by inverting the dominant use of the word security and considering its constituent parts, notably as explicated by other disciplines. Security theorist, Mark Neocleous, argues this point in his work “Critique of Security” [21] where he inverts the dominant use of the word security across a variety of domains, by initially sketching the different ways the term security is operationalised in political rhetoric and as part of public policy and then arguing for a broader conceptualisation of security that includes networks of resilience, solidarity and co-operation. Security as resilience is a particularly strong theme in the work of security theorist Bill McSweeney [19] who outlines an argument for recognition of a form of relational security that supports the sense of everyday security where an individual feels safe and secure when going about their everyday activities [23]. Relational security is the security derived from trusted relationships upon whom an individual is reliant in order to carry out day to day tasks and activities both at work and at home. McSweeney argues that this form of security creates a freedom to take part in the day to day events that are vital for the well being of the individual, the community and the wider society. Without relational security, a form of paralysis is experienced resulting from anxiety in the relationships that are fundamental to day to day experiences. This aspect of security is highly relevant to cyber security because the mission of cyber security is, in part, about enabling the individual, the community and wider society [35] to conduct their everyday lives in environments that have been (and continue to be) transformed by a dazzling variety of digital media.

A parallel for this type of thinking can be found in fields of urban planning and architecture. In the post-war discourse of architecture and urban planning, the issue of security has been opened up by looking not at criminal behaviour and how to design structures that keep it out,

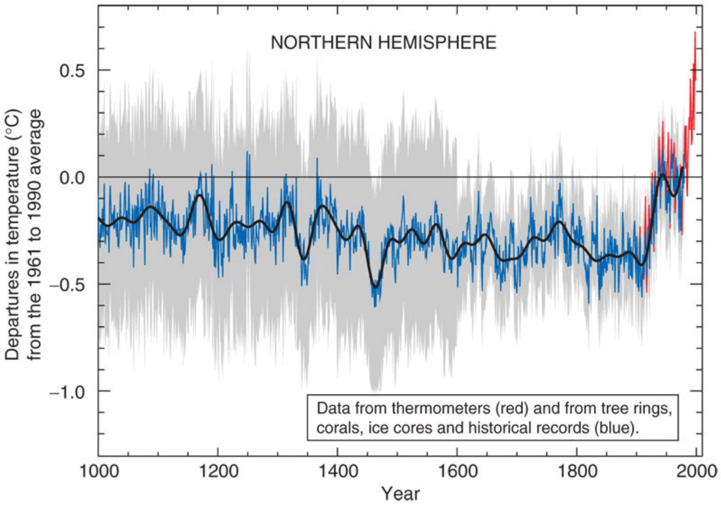

Figure 7: ipcc.

but with a social theory of space, by looking at the way in which social practices are manifest in physical structures. A chapter titled "The uses of sidewalks: safety" in the critic Jane Jacobs's influential book on American cities [15] provided a starting point for this urban planning shift. Noting that the public peace is not primarily kept by the police but by an "intricate, almost unconscious network of voluntary controls and standards among the people themselves, and enforced by the people themselves" Jacobs builds an argument drawing from city crime statistics, a series of observed vignettes from late 1950s New York (where she lived) and an emerging set of guidelines. Cities - like computing clouds - have a constant influx of strangers. For a city neighbourhood to be successful, by which Jacobs means safe, it must have three main qualities: First, it must have a clear demarcation between public and private; Second. there must be "eyes upon the street, eyes belonging to those we might call the natural proprietors of the street" [15, p.35]. And third, the street must be populated fairly continuously, both to increase the number of eyes on the street to give those street watchers something to look at. "Nobody enjoys sitting on a stoop or looking out a window at an empty street"[15, p.35].

Jacobs' polemic jolted post-war planners and architects out of a separatist approach to city building, and helped bring about the mixed use, more pedestrian friendly spaces we have started to see ameliorating the neighbourhoods annexed by highways and high rises in the 1960s and 1970s. To imagine how information security might be better achieved requires temporarily, at least, moving away from the fixation on networks and network traffic and looking at the social practices that surround information exchange, by going back to the physical environments in which trust and resilience are built. From the critique of AI we can hypothesise that information exchange is a social and embodied practice. The working atmosphere in an organisation's headquarters and its communication patterns may be, for instance, as important to trust and resilience as its procedural practices. Standard network visualisations do not typically depict working atmospheres or communication patterns, suggesting that they are hiding the lessons to be learned from situating data in space; how spatial practices relate to livability, communication and safety.

Figure 8: Apollo 17.

A useful point of reference from architecture and urban planning discourse comes from the Space Syntax Lab, which emerged out of Bartlett School of Architecture and Planning in London. In their 1984 book, Bill Hillier and Julienne Hanson argued that rather than describing the built environment and then relating it to use, we need to see how buildings and settlements "acquire their form and order as a result of a social process" [13, p.8]. This is necessary because of the long history of separating humans from buildings and studying the buildings first as artefacts that generate meaning, which set up a problem of space being desocialized at the same time as society was despatialized. By focusing on the aggregations of spaces and how they follow certain patterns in the development of cities - on genotypes rather than phenotypes - Hillier and Hanson established a method for looking at cities in terms of their spaces (and spatial configurations) rather than their built forms. The relations between inhabitants and strangers, they noted, had a big influence on how a settlement grew in terms of the size and scope of the foci, marketplaces and squares, and the connecting streets. In London and cities in Europe, they argued, a governing principle was that important meeting points or foci were usually no more than two axial steps apart, so that there is a point from which both foci could be seen. This had an implication for urban safety. "The system works by accessing strangers everywhere, yet controlling them by immediate adjacency to the dwellings of the inhabitants. As a result, the strangers police the space, while the inhabitants police the strangers" [13, p.18].

Space syntax analysis has developed a considerable array of visualisation methods, including ways of combining it with social network analysis to study communication patterns. One recent

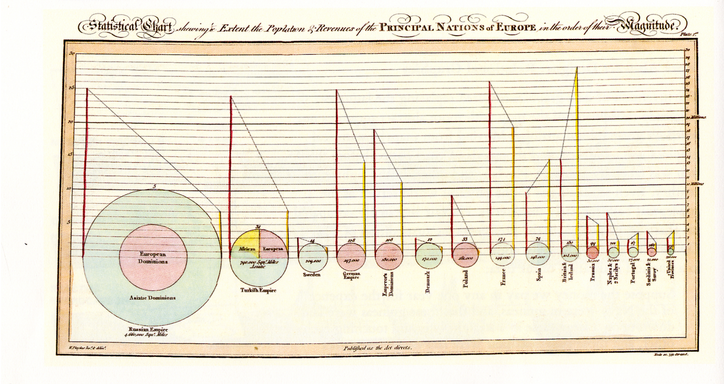

Figure 9: Playfair.

study examined communication patterns in five outpatient clinics in Canada and the Netherlands, based on the knowledge that communication breakdowns are generally blamed for more than half of all medical errors. As with the analysis of city meeting points and connecting streets, the analysis of communication patterns revealed that long lines of sight and shared workspaces have the benefit of increasing chances for encounter and communication, implying that less communication breakdowns would result. The outcome of the project had an impact on the redesign of a Vancouver hospital [24]. While clearly communication in and between outpatient clinics could be visualised in terms of links and nodes a situated communication analysis has revealed and addressed what might be described in other circles as a network vulnerability.

8 Case Studies

Research into participatory modelling of information exchange practices has also informed this paper [26]. It is the seemingly intangible aspects of social behaviour and of information-communication practices that very often affect the core business of social networks and cloud computing, to take one example. Yet the human dimension is usually glossed over in the study of cyber-security (a dimension sometimes referred to as the ‘weakest link’). Differing degrees of trust and loyalty lead to different perceptions of security, and are difficult to visualise, let alone quantify. The chosen medium for research in this area was a specially developed form of participatory diagramming and physical modelling. In the last stages of this process the participants were given *LEGO* building bricks of given types and colours, selected so as to encode the movement of shared information and data, actors, and devices (Fig. 10). The ‘Archimate’ framework for enterprise and risk analysis is referred to by the colour of bricks [16], organising the dimensions of the scenario that were social, technical, and infrastructural, while the organisational core values that had previously been mapped from early engagements were carried through the subsequent stages of analysis and interaction with the participants (Fig. 11).

Physical modelling and its closely related co-design techniques assist the group to construct a narrative, one which not always fully spelled out by participants, and may occasionally appear to be fragmentary, inconclusive, and difficult to decipher for anyone outside the group that has built

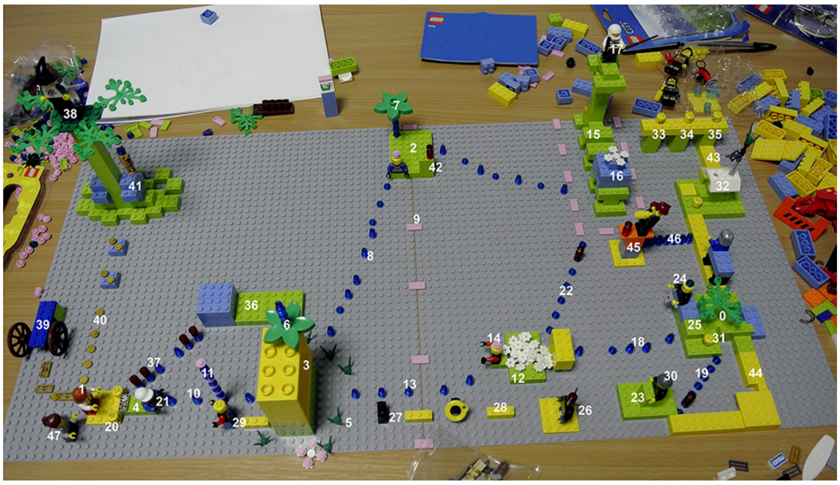

Figure 10: *LEGO* model from participatory service design sessions, 2015. Royal Holloway, London. Key: 0 = LRS; 1 = Client; 2 = Card; 3 = TV; 4 = Remote; 5 = Client's sphere of interest; 6 = Antenna on TV; 7 = Antenna on Card; 8 = Data TV to Card; 9 = Boundary between Client and LRS; 10 = Data Remote to TV; 11 = Raspberry Pi; 12 = Cloud; 13 = Data TV to Cloud; 14 = Protection on Cloud; 15 = Bank; 16 = Account; 17 = Security on Bank; 18 = Data Cloud to LRS; 19 = Data LRS to Partner 23; 20 = Children; 21 = Security on Remote; 22 = Data Bank to Cloud; 23 = Partner 23; 24 = LRS Data management; 25 = LRS Server; 26 = Partner 26; 27 = Intervention in progress; 28 = Intervention pathway; 29 = Partner 29; 30 = Staff at Partner 23; 31 = Staff at LRS; 32 = Partner HA; 33 = Partner 33; 34 = Partner 34; 35 = Partner 35; 36 = Energy provider; 37 = Data Bill to Client; 38 = Governmental welfare agencies; 39 = Income source; 40 = Welfare benefits; 41 = Government systems; 42 = Additional cards; 43 = Partner bridges1; 44 = Partner bridges2; 45 = Troubleshooter; 46 = Data Troubleshooter to Partners; 47 = Carer.

the representation. Unravelling the many interwoven and layered elements of their story, and visualising the developing insights and understanding as the group wrestle with complex service design issues, requires the development of a new method for stabilising and coding this type of 'Serious Play' data, a method which preserves the spoken and shared understanding of the group as it deals with specific questions, directed to distinct parts of the model. Keywords from these discussions can be used to query our qualitative field data as a whole, and can ultimately reveal high-level patterns within the understanding of the group, which for example might display the perceived potential "impact" of "hackers" upon the "security" over different parts of this particular socio-technical story. Visualising these patterns and showing where key issues occur and how they interact with one another, is an opportunity to develop analysis in a way that has not been demonstrated by more formal methods of risk analysis.

Keywords such as 'risk' and 'impact' for example, can be used to detect where participants have linked these concepts to specific places on the model, or, to groups of these nodes. Because the data concerns a symbolic representation of a larger world projected down into a small physical model, these patterns can in theory be visualised as cumulative temporal and spatial patterns

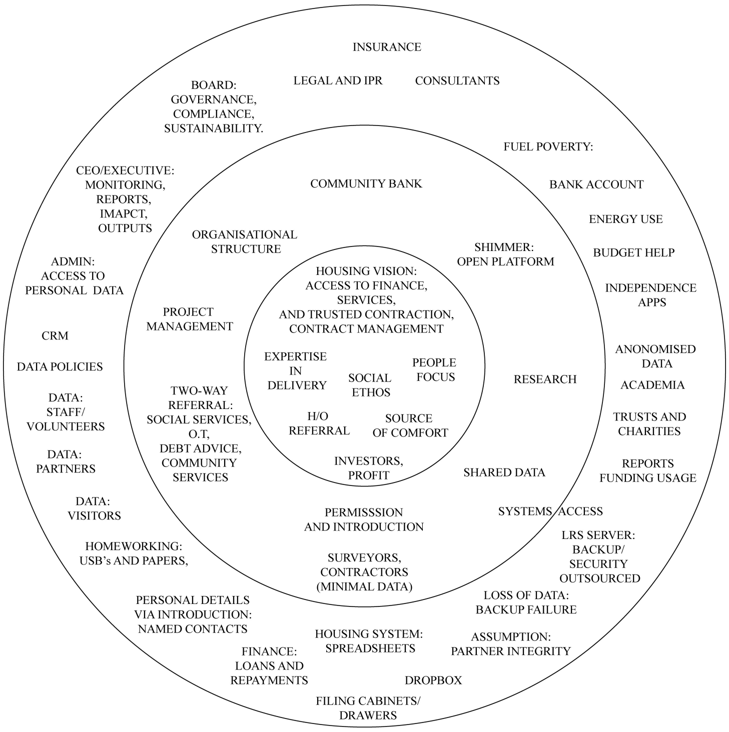
INSURANCE
LEGAL AND IPR
CONSULTANTS
BOARD: GOVERNANCE, COMPLIANCE, SUSTAINABILITY.
FUEL POVERTY:
CEO/EXECUTIVE: MONITORING, REPORTS, IMAPCT, OUTPUTS
COMMUNITY BANK
BANK ACCOUNT
ENERGY USE
ORGANISATIONAL STRUCTURE
SHIMMER: OPEN PLATFORM
BUDGET HELP
ADMIN: ACCESS TO PERSONAL DATA
HOUSING VISION: ACCESS TO FINANCE, SERVICES, AND TRUSTED CONTRACTION, CONTRACT MANAGEMENT
INDEPENDENCE APPS
PROJECT MANAGEMENT
CRM
ANONOMISED DATA
EXPERTISE IN DELIVERY
PEOPLE FOCUS
SOCIAL ETHOS
DATA POLICIES
RESEARCH
ACADEMIA
TWO-WAY REFERRAL: SOCIAL SERVICES, O.T, DEBT ADVICE, COMMUNITY SERVICES
DATA: STAFF/ VOLUNTEERS
H/O REFERRAL
SOURCE OF COMFORT
TRUSTS AND CHARITIES
DATA: PARTNERS
INVESTORS, PROFIT
SHARED DATA
REPORTS FUNDING USAGE
DATA: VISITORS
PERMISSSION AND INTRODUCTION
SYSTEMS ACCESS
LRS SERVER: BACKUP/ SECURITY OUTSOURCED
HOMEWORKING: USB's AND PAPERS,
SURVEYORS, CONTRACTORS (MINIMAL DATA)
LOSS OF DATA: BACKUP FAILURE
PERSONAL DETAILS VIA INTRODUCTION: NAMED CONTACTS
HOUSING SYSTEM: SPREADSHEETS
ASSUMPTION: PARTNER INTEGRITY
FINANCE: LOANS AND REPAYMENTS
DROPBOX
FILING CABINETS/ DRAWERS

Figure 11: Picture of LRS natural areas of interest, concern, and resilience.

[9], or even as ‘manifolds’ of social practice [25]. General patterns, at higher levels of societal analysis, have previously only been schematically visualised, creating pictorial metaphors for contrasting types of interlocking shapes and mechanisms that have been found in social practices [29].

The situated and participatory approaches to visualisation that have been discussed here, clearly have their limitations. A standard critique is to ask how a de-localised information exchange network that is transmitting gigabytes of data around the world might effectively take into account the local and social factors of a situated model. But such a question is framed, once again, by the epistemological legacy that seeks to always abstract and universalise intelligence and, on that basis, predict behaviour. One difficulty faced by the allied but nevertheless distinct fields of information security visualisation and information security, is that their practitioners are embedded in the pre-existing conditions from which their tasks are structured, in what Heidegger called a state of ‘thrownness’ [12]. As a result, it becomes difficult to conceive of visualisation as anything other than the visual display of quantitative evidence (to paraphrase the title of a book by Edward Tufte).

We argue here that ‘improved’ visualisations of technologically dense environments should reduce the complexity to a manageable level by using the type of participatory data discussed above, in order to establish what constitutes a ‘sufficiently secure’ state of affairs for the participants. Data can be structured in such a way that it results in what Nelson Goodman called a more ‘graphically *replete* representation’ [10], that should attain a density appropriate to the source matter but not be overwhelmed by it. ‘What matters with a diagram’ Goodman says, ‘as with the face of an instrument, is how we are to read it’ [10, p.170]. An interface design and visualisation strategy therefore emerges from an immersion in qualitative as well as technical data, an approach which straddles both diagrammatic and pictorial conventions, and offers a schema that takes the best of both worlds (Figs. 12, and 13). In the process it supercedes the traditionally attenuated and technically-slanted forms of visualisation that are to be found in the literature. Visualisations that have been grounded in qualitative field data gathered via inductive research methods (methods refs), thus naturally lead to the development of new criteria for the assessment of visualisations, criteria which will most usefully provide specific reference to the categories and qualities found in the data itself. Moreover, the multiple perspectives and interpretations embedded in these ‘rich’ visualisations (Fig.14) are especially suited to the increasingly multi-disciplinary nature of this work.

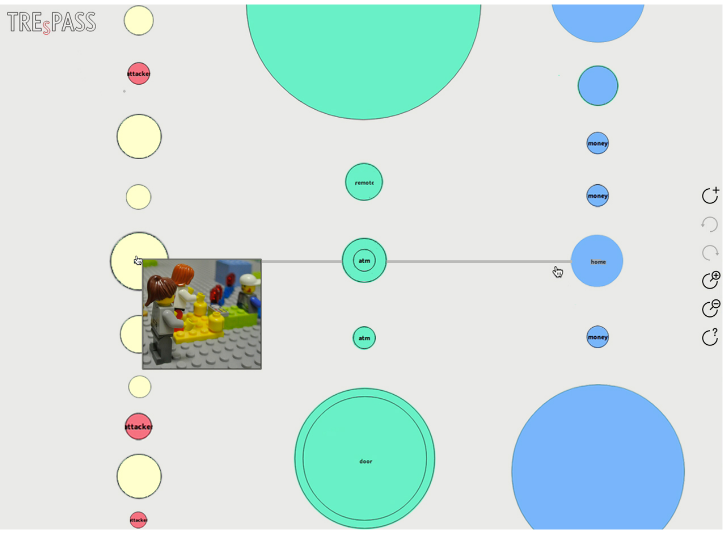

Figure 12: Prototype graphical user interface sketch, showing how excerpts from the qualitative data ‘pop-up’ on request and add further dimensions to the two-dimensional diagrammatic representation of the service design. TREsPASS Project/Royal Holloway, University of London.

If behaviour is embodied and situated, as the Space Syntax lab has demonstrated, it becomes imperative to study the physical places and the social situations where security and security risks typically occur, as well as those where ‘everyday’ routines prevent such events from occurring. This is in order to understand not just how, why and as part of what social practices human error created a ‘weak link’, but where and how organisations have successfully avoided being made into the targets of attacks and where and how strong, resilient social networks are formed.

Situated, participatory approaches to visualisation can then be positioned as a complement to the more familiar visualisation tools used to model global networks and support the ‘search and destroy’ approaches discussed above. The term ‘mesh networks’ has been used to describe how communities of practice are connected across distances, wherein the notion of proximity is extended by communications technology. Another relevant tool for the exploration of trust net-

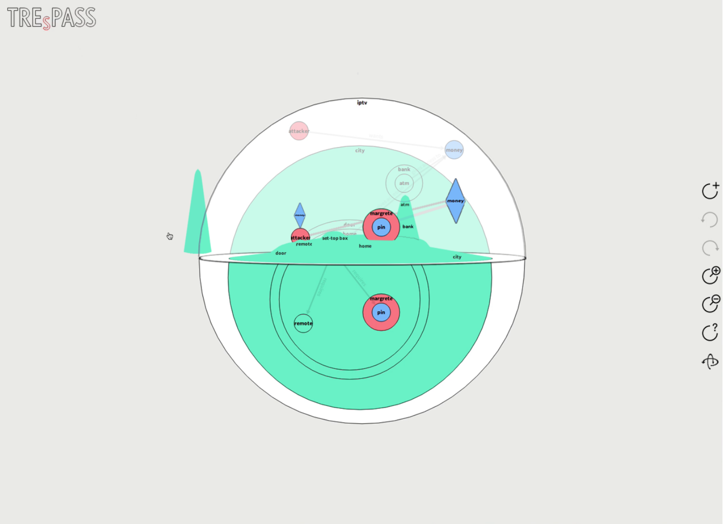

Figure 13: Prototype graphical user interface sketch for constructing a navigator map for the business scenario, seen in circular plan view and as a superimposed relief version of the same mapping, seen in side view. The reliefs are generated from values obtained from the participatory engagements. TREsPASS Project/Royal Holloway, University of London.

works across distances is crowd-sourcing, which typically depends on a high degree of goodwill among its participants to achieve an agreed common goal.

A final example: after post-election violence erupted in Kenya in 2007, a group of volunteers set up an open source platform for tracking and geolocating reports of incidents sent by email and SMS [27, n.56]. The system, called ‘Ushahidi’, proved particularly powerful after the Haitian earthquake of 2010 as a crisis-mapping operation through which people and organisations posted their most urgent needs, and volunteers picked up and translated messages sent via email, SMS, social media and voicemail. The mapping that emerged during these projects shifted the focus of security towards temporary insecure spaces of emergency (that will become increasingly common with population shifts and climate change). It also presents a model that simultaneously identifies vulnerability and builds resilience.

9 Conclusion

At the turn of the 21st Century, Peter Sloterdijk argued that “The guiding morphological principle of the polyspheric world we inhabit is no longer the orb, but rather foam” [30, p.71]. In other words, the era in which humans imagined they could embark on achieving one all-seeing, all-encompassing, omniscient tool, be it a geoscope, datasphere, thinking machine or “the singularity” has irrevocably passed. We can’t see our way through foam as we could in the large orb, but we can at least work out methods, strategies and tactics for navigating through it. To adapt Sloterdijk’s morphology, in today’s complex, multi-valent, multicultural world, we need not one tool, but lots of them, tuned to the needs of different social and cultural practices.

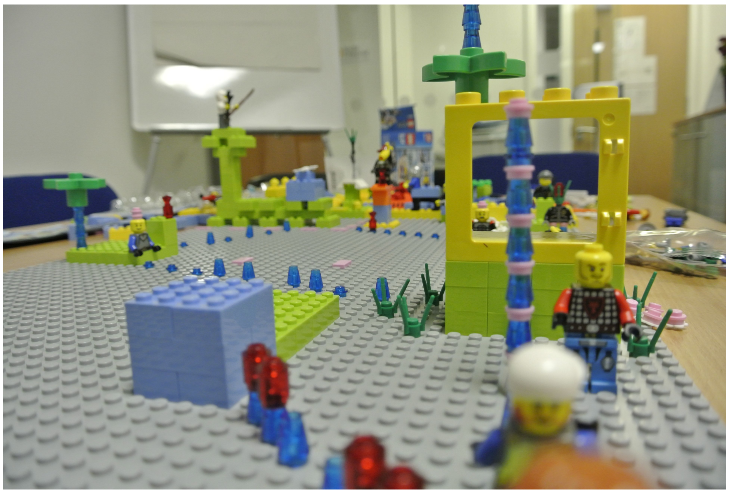

Figure 14: Of the 23 actors that were included in the model, the one most often referred to was the client using the service, and their perspective upon the rest of the model and the other actors is shown here. Taking the viewpoint of various actors was a feature of discussions during the sessions.TREsPASS Project/Royal Holloway, University of London.

Another metaphor and potentially useful model is provided by the prolific business of visualisation in genomics. As Manuel Lima observes, the figure of a tree provided a valuable motif for hundreds of years of biological research, expressing "multiplicity (represented by its boughs, branches, twigs and leaves) from unity (its central foundational trunk)" [17, p.25] But after the discovery of horizontal gene transfer, in which biological organisms incorporate genetic material from different organisms without being their offspring, the tree of life has come to seem too hierarchical, centralised and static. Biologist Johann Peter Gogarten has suggested that a net provides a better metaphor for visualising the "rich exchange and cooperative effects of HGT among microbes" [17, p.69].

One would suspect that information security, which in its true sense has a multi-disciplinary complexity comparable to genomics, will be driven by a similar imperative to develop new metaphors and new ways of visualising the rich exchange and cooperative effects of information among humans.

10 Acknowledgments

Our thanks to the TREsPASS project. This work is funded under the European Commission's Seventh Framework Programme under Grant Agreement No. 318003 (TREsPASS).

References

[1] C. Anderson. The end of theory: The data deluge makes the scientific method obsolete. wired magazine, 2008.

[2] S. Bleikertz, T. Mastelic, S. Pape, W. Pieters, and T. Dimkov. Defining the cloud battlefield-supporting security assessments by cloud customers. In *Cloud Engineering (IC2E), 2013 IEEE International Conference on*, pages 78–87. IEEE, 2013.

[3] P. Brey. Hubert dreyfus: humans versus computers. 2001.

[4] L. Coles-Kemp and M. Theoharidou. Insider threat and information security management. In *Insider threats in cyber security*, pages 45–71. Springer, 2010.

[5] J. W. Crampton. Cartographic rationality and the politics of geosurveillance and security. *Cartography and Geographic Information Science*, 30(2):135–148, 2003.

[6] C. M. Dalton and J. Thatcher. Inflated granularity: Spatial big dataand geodemographics. *Available at SSRN 2544638*, 2015.

[7] M. Foucault. *Discipline and punish: The birth of the prison*. Vintage, 1977.

[8] M. Foucault and F. Ewald. *" Society Must Be Defended": Lectures at the Collège de France, 1975-1976*, volume 1. Macmillan, 2003.

[9] A. Giddens. The constitution of society: Outline of the theory of structuration. *Cambridge: Polity*, 1984.

[10] N. Goodman. *Languages of Art: An approach to a theory of symbols*. Hackett Publishing, 1976.

[11] J. B. Harley. Silences and secrecy: the hidden agenda of cartography in early modern europe. *Imago mundi*, 40(1):57–76, 1988.

[12] M. Heidegger. *Basic Writings: Revised and expanded*. Harper One, 1993.

[13] B. Hillier and J. Hanson. *The social logic of space*. Cambridge university press, 1984.

[14] J. E. Hummel and I. Biederman. Dynamic binding in a neural network for shape recognition. *Psychological review*, 99(3):480, 1992.

[15] J. Jacobs. *The death and life of great American cities*. Vintage, 1961.

[16] M. M. Lankhorst, H. A. Proper, and H. Jonkers. The architecture of the archimate language. In *Enterprise, Business-Process and Information Systems Modeling*, pages 367–380. Springer, 2009.

[17] M. Lima. *Visual Complexity*. 2007.

[18] R. Marty. *Applied security visualization*. Addison-Wesley Upper Saddle River, 2009.

[19] B. McSweeney. *Security, identity and interests: a sociology of international relations*, volume 69. Cambridge University Press, 1999.

[20] S. Milner-Barry. Hut 6: Early days. *Codebreakers: The Inside Story of Bletchley Park (Oxford: Oxford University Press, 1993)*, pages 100–12, 1993.

[21] M. Neocleous. *Critique of security*. Oxford University Press, 2008.

[22] H. W. Rittel and M. M. Webber. Dilemmas in a general theory of planning. *Policy sciences*, 4(2):155–169, 1973.

[23] P. Roe. The valueof positive security. *Review of International Studies*, 34(04):777–794, 2008.

[24] K. Sailer, R. Pachilova, E. Kostopoulou, R. Pradinuk, D. MacKinnon, and T. Hoofwijk. How strongly programmed is a strong programme building? a comparative analysis of outpatient clinics in two hospitals. 2013.

[25] T. R. Schatzki. *Social practices: A Wittgensteinian approach to human activity and the social*. Cambridge Univ Press, 1996.

[26] K.-P. Schulz and S. Geithner. Creative tools for collective creativity the serious play method using lego bricks. *Learning and Collective Creativity: Activity-Theoretical and Sociocultural Studies*, pages 179–197, 2013.

[27] M. Sheller. The islanding effect: post-disaster mobility systems and humanitarian logistics in haiti. *cultural geographies*, 20(2):185–204, 2013.

[28] B. Shneiderman. *Designing the user interface-strategies for effective human-computer interaction*. Pearson Education India, 1986.

[29] E. Shove. *Comfort, cleanliness and convenience: The social organisation of normality*. Berg Oxford, 2003.

[30] P. Sloterdijk. Bubbles: Microspherology. 2011.

[31] E. R. Tufte. Beautiful evidence. 2006.

[32] E. R. Tufte and P. Graves-Morris. *The visual display of quantitative information*, volume 31. Graphics press Cheshire, CT, 1983.

[33] S. Übelacker. Security-aware organisational cultures as a starting point for mitigating socio-technical risks. 2013.

[34] P. Virilio. *War and cinema: The logistics of perception*. Verso, 1989.

[35] R. Von Solms and J. Van Niekerk. From information security to cyber security. *Computers and Security*, 38:97–102, 2013.

[36] C. Ware. *Information visualization*, volume 2. Morgan Kaufmann San Francisco, 2000.

[37] D. Wood. *Rethinking the power of maps*. Guilford Press, 2010.