JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 1(1), 2015, 93–108
doi: 10.1093/cybsec/tyv004
Advance Access Publication Date: 1 December 2015
Research Article

Research Article

Critical visualization: a case for rethinking how we visualize risk and security

Peter Hall[1,*] **Claude Heath**[2] **and Lizzie Coles-Kemp**[2]

[1]Central St Martins University of the Arts London, 1 Granary Square, London N1C 4AA and [2]Royal Holloway University of London, Surrey, TW200EX, UK

*Correspondence address. Royal Holloway University of London, Surrey TW200EX, UK. Tel: +44(0)1784434455; E-mail: peter@peterahall.com

Received 29 May 2015; accepted 28 September 2015

Abstract

In an era of high-profile hacks, information leaks and cybercrime, cybersecurity is the focus of much corporate and state-funded research. Data visualization is regarded as an important tool in the detection and prediction of risk and vulnerability in cybersecurity, but discussion tends to remain at the level of the usability of visualization tools and how to reduce the cognitive load on the consumers of the visualizations. This focus is rooted in a desire to simplify the complexity of cybersecurity. This article argues that while usability and simplification are important goals for the designers of visualizations, there is a much wider discussion that needs to take place about the underlying narratives upon which these visualizations are based. The authors take the position that the narratives on which cybersecurity visualizations are based ignore important aspects of cybersecurity and that their visual form causes the producers and users of these visualizations to focus too narrowly on adversarial security issues, ignoring important aspects of social and community-based security. By situating the discussion of security visualization in a larger socio-historical context, the limitations and implications of current ways of seeing risk become more apparent. Cybersecurity 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 article 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 to stimulate reflection on underlying principles and the implications of different approaches to operationalizing those principles. Finally, case studies of participatory modelling and crowdsourcing projects are discussed that aim to foster resilience through social and spatial practices. These case studies illustrate the potential for a wider range of visualizations.

Key words: visualization; risk; resilience

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’ (e.g. public administrations, finance and banking, energy, transport, health) [10, p.12]. This suggests a complex problem permeating all levels of society, but news headlines are increasingly preoccupied with cyberterrorism and counterterrorism (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 cybersecurity is better surveillance, and information visualization that has assumed an important role in fuelling this hope by

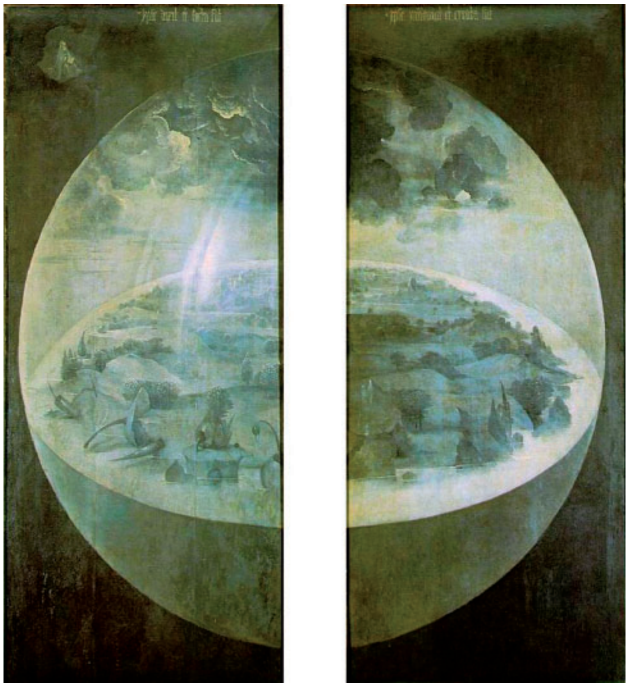


Figure 1. Hieronymus Bosch, *Garden of Earthly Delights*, 1503–4. Oil on hinged oak panels, 220 x 389 cms, Museo del Prado, Madrid, seen here in folded state. Public domain.

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 its typical visualization forms—such as network diagrams and tree maps—currently achieve.

The argument of this article is that the predominant mode of visualization 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 cybersecurity narrative. The dominant narrative is one of cybersecurity as 'control', whereas critics argue that we are in fact, 'post control' [8] in many senses and need to look to human as well as technological security to respond to cybersecurity challenges.

Drawing from the lessons of critical cartography, this article proposes that our visualization 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' [26, 1, 7]. If, as its critics suggest, the discourse and visualization 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?

Faith in data spheres

According to the German philosopher Peter Sloterdijk, the impulse to make visualizations, 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 neither enclosed by protective domes, nor 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 civilization, the welfare state, the world market and the media sphere. We might add to that list the recent obsession with visualizing spheres of data:

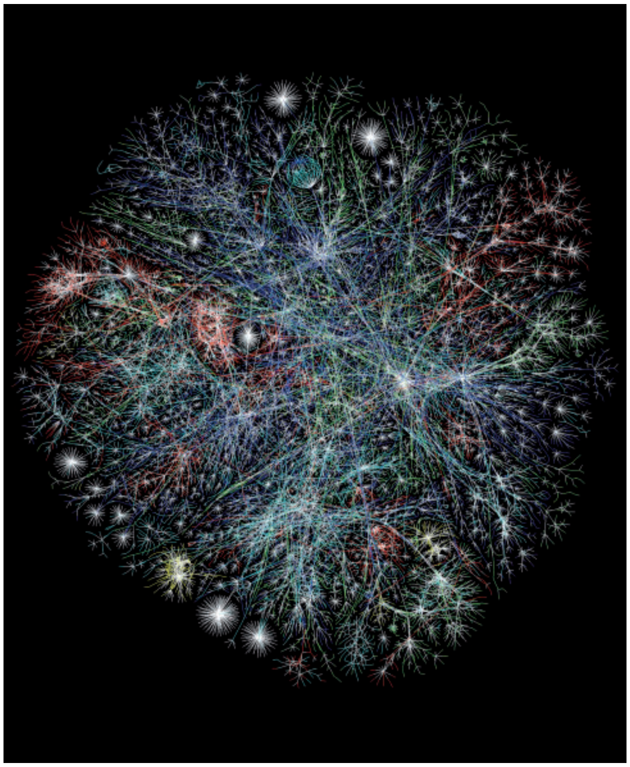


Figure 2. *The Opte Project Map of the Internet*, Barrett Lyon, 2003. Creative Commons.

> all these large-scale projects aim, in a shell-less time, for an imitation of the now impossible, imaginary spheric security. Now networks and insurance policies are meant to replace the celestial domes [34, p. 25].

Many current visualizations of internet traffic demonstrate this same spheric faith, such as Barrett Lyon's map of the Internet from 2003 (http://www.opte.org/prints-licences/), showing traffic between the major Internet Service Providers (ISPs) (Fig. 2). On a par perhaps with the 'blue marble' photograph (http://earthobservatory.nasa.gov/IOTD/view.php?id=1133) 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 visualization 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 (Fig. 4), 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' [21, pp. 33–41]. Trees have proven popular memes in predictive methods of visualizing 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.

Figure 3. Earth, photographed from on board NASA mission *Apollo 17*, 1972. Public domain.

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 modelled and visualized and what can be left out.

Reducing complexity

This brings us to a central paradox of visualization; we visualize to make complex problems easier to understand and easier to navigate, but to do this we must simplify the complexity. It is this process of reduction and abstraction that often reveals the intent of visualization. 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 [15] and [43].

Designers aim to achieve simplicity or clarity in visualizations by making them persuasive and/or easy to use, which suggests two categories of visualization; the rhetorical and explorative. Rhetorical visualizations 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 (see, for example, Fig. 5)). 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 [36] and [37].

Explorative visualizations tend to pose questions, and are often dynamic and interactive (Fig. 6). The discourse is 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' [32]. 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 [21, 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 cybersecurity researchers and practitioners.

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–visualization interaction, it is important to situate such aims in a larger historical discourse to understand the wider potential for the development of cybersecurity visualization. The history of data visualization can be traced back to the emergence of 'thematic maps' and information intensive graphics in the 17th century (Fig. 7), 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. 37]. Linking this discourse to contemporary practices of geosurveillance, Crampton follows Michel Foucault in tracking how such technologies of management emerged as a means to: (i) think of people and space as resources that required management and protection, and (ii) to normalize through the gathering and categorizing of data about populations, such as censuses.

Standard approaches of visualizing threats to cybersecurity deploy the Tufte and Shneiderman vocabulary in technologies designed to extend the categorization and identification of abnormal behaviours. For example, Raffael Marty's 2009 text 'Applied Security Visualisation' 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 patterns of distribution [22]. This way, Marty arrives at a suspect botnet controller. Visualization, 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 recognize patterns. A link graph (Fig. 8), showing 'malicious insider threat' derived from network traffic data is developed by listing 'precursors' (suspicious behaviours) 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 [12, p. 57].

Marty's visualization 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, authorization, empowerment and control [4].

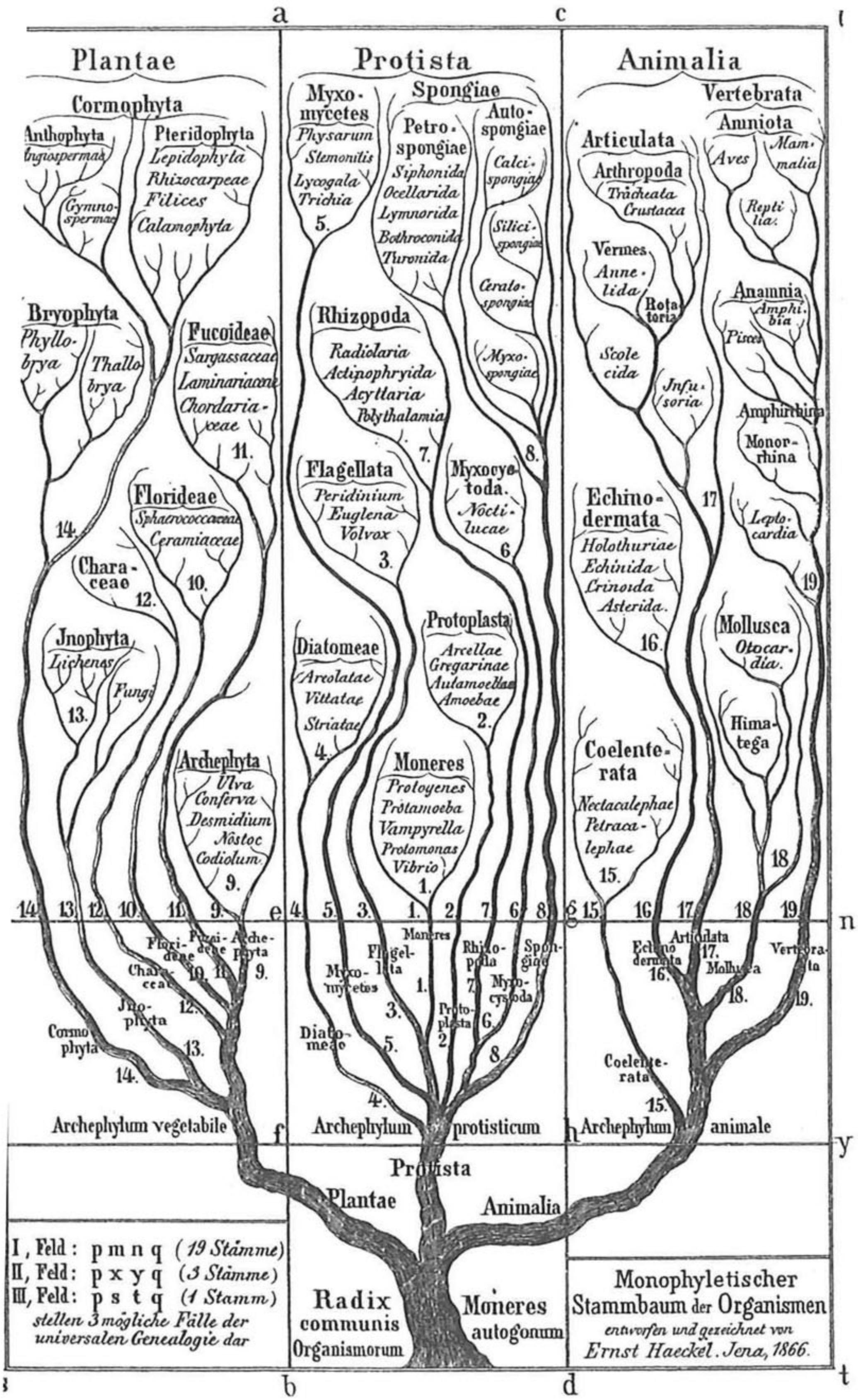


Figure 4. Ernst Haeckel, *General Morpohology of Organisms*, 1866. Public domain.

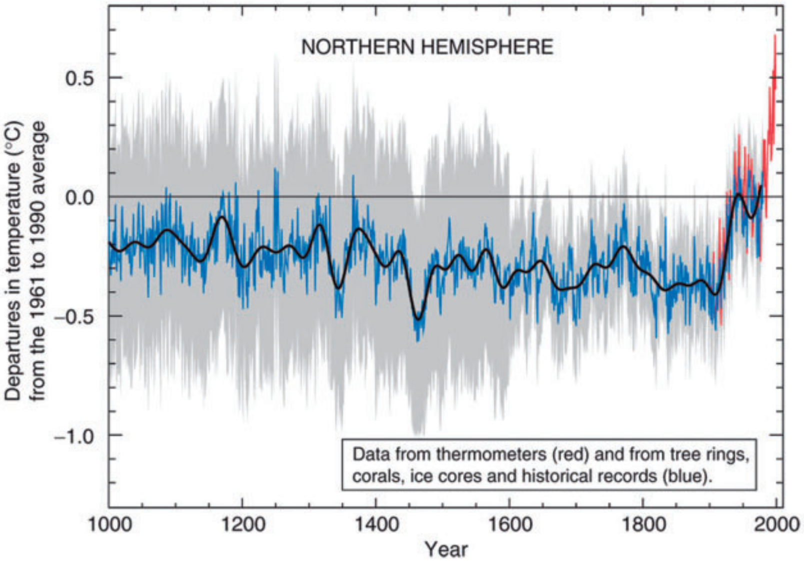
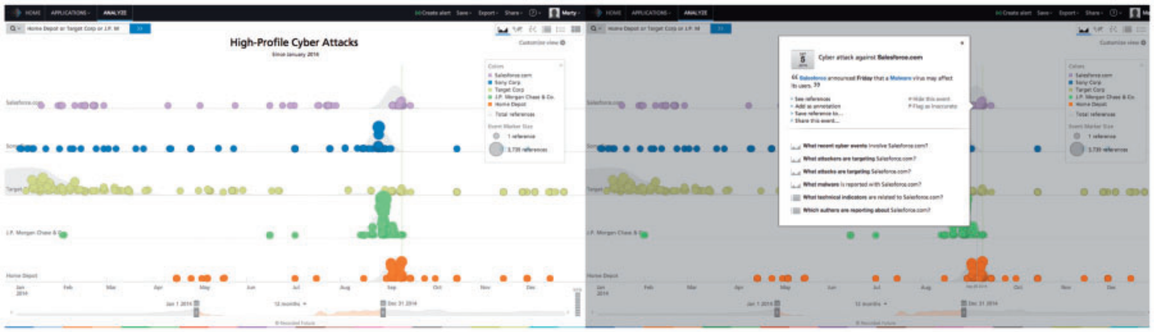


Figure 5. The ‘Hockey Stick’ graph (named because of its shape), from the 2001 Intergovernmental Panel on Climate Change (IPCC). This graph mobilized world-wide debate on the topic of global warming. Image courtesy of IPCC, available at: www.grida.no.



Cyber attack against Salesforce.com

“Salesforce announced Friday that a Malware virus may affect its users.”

- See references
- Add as annotation
- Save reference to...
- Share this event...
- Hide this event
- Flag as inaccurate

What recent cyber events involve Salesforce.com?

What attackers are targeting Salesforce.com?

What attacks are targeting Salesforce.com?

What malware is reported with Salesforce.com?

What technical indicators are related to Salesforce.com?

Which authors are reporting about Salesforce.com?

Figure 6. Explorative visualization showing progressive disclosure. Reproduced with permission: www.recordedfuture.com.

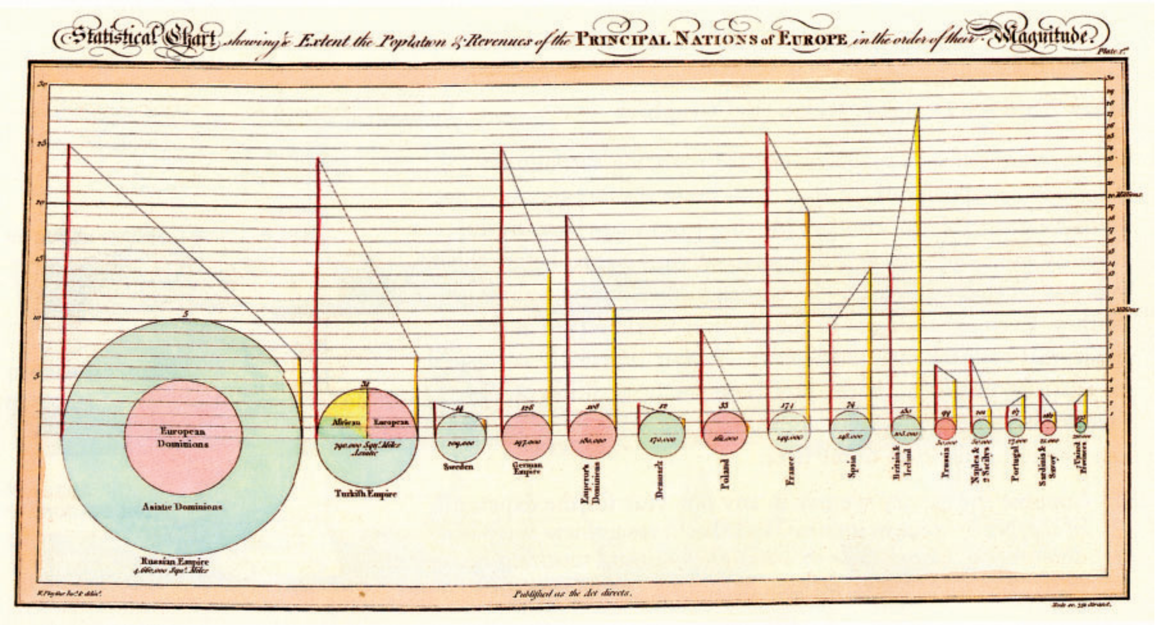


Figure 7. Pie charts, William Playfair, 1801. From, *The Commercial and Political Atlas: Representing, by Means of Stained Copper-plate Charts, the Progress of the Commerce, Revenues, Expenditure and Debts of England During the Whole of the Eighteenth Century*, 3rd edn. Public domain.

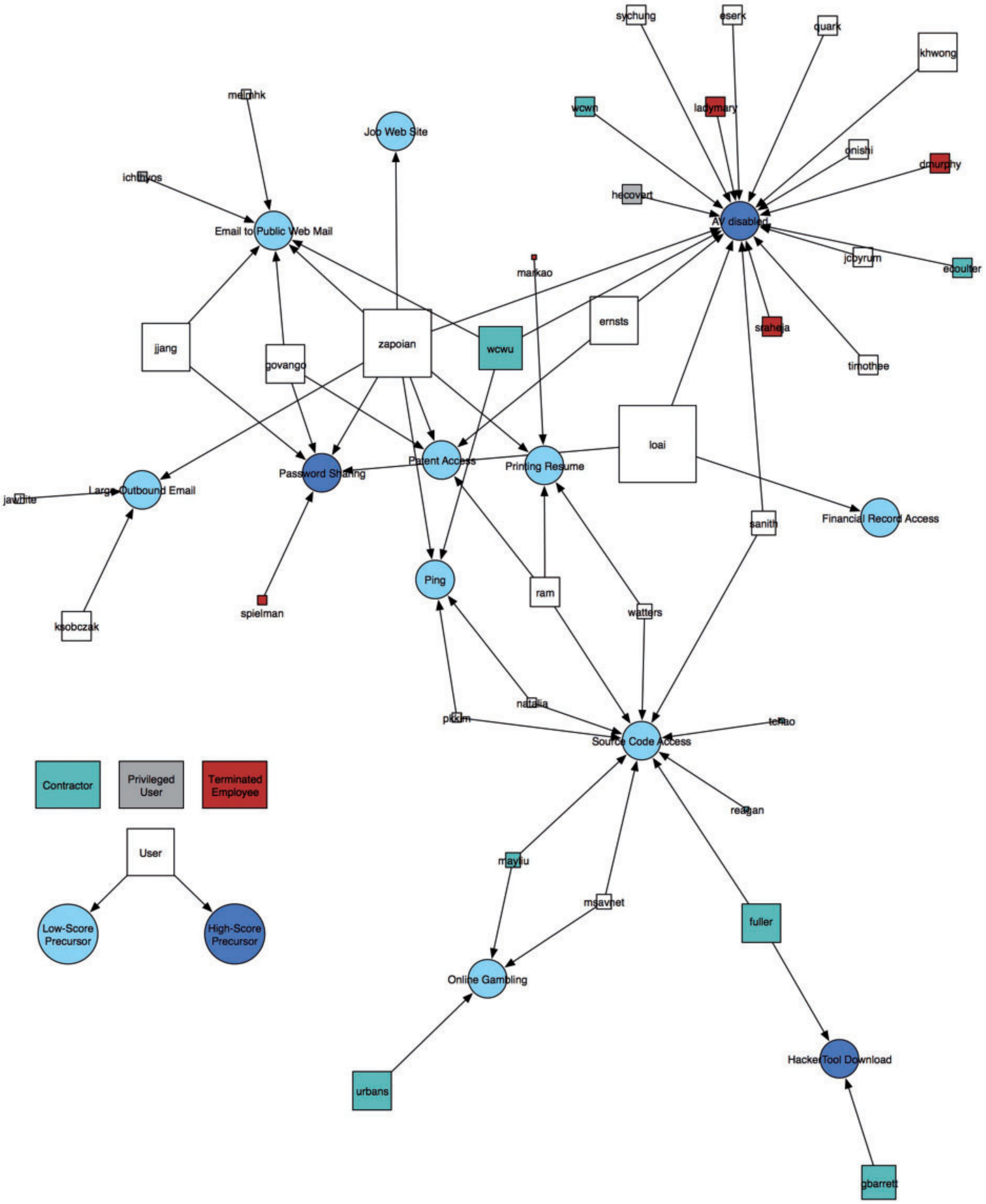


Figure 8. 'Insider candidate list', shown as a link graph, referring to insider threat. Reproduced with permission from Raffael Marty, *Applied Security Visualization*, 2009.

Socio-technical problems and the AI legacy

Recent developments in information security, including the EU-funded TREsPASS project, from which this article draws evidence and a research framework, explore the limits and possibilities of visualization 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 characterized, 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 [24]. This point seems to support the phrase, popular in the security community, that humans represent the 'weakest link' [41], suggesting that if the machines were left to themselves, there would be no security threat.

But this position overlooks the fact that the interaction often provides forms of security for the individual which may override the security needs of the data. The question here is whether the referent object is the person and the security of the person or the data and the security of the data. If the referent object is the person then the security of the data is only a means to the security of the person. The critique of classical artificial intelligence (as derived from Turing) that was most famously furthered by Hubert Dreyfus [9] 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 behaviour to the logic and requirements of machines. Terry Winograd and Fernando Flores [42] 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, visualization appears to sit firmly in a cognitivist position premised on a disembodied intelligence.

Both the rhetorical and explorative approaches to visualization tend to aspire to establishing a coherent and universal set of rules so that visualizations 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 [40]. Ware cites a neural network model of structural object perception, developed by Hummel and Biederman [18], 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' [40, 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 universalize 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, cybercrime is typically modelled by assessing precursors based on both suspicious behaviour patterns in network traffic and targeted insiders with a potential to turn 'bad' (e.g. a disgruntled employee). Yet, predictive assessments used in information security struggle to identify behaviour that is improvised rather than maliciously premeditated.

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 [6, p. 120]. 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 visualization being explored as part of ongoing research. Based on predictive modelling 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 puts it, 'once you can see the target you can expect to destroy it' [38, 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 I, to the spy satellites, video missiles and drones in World War II 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 [11], with its inclination to observe and normalize, 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 (Fig. 9). 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. Visualizations that depict potential risks as well as actual attacks seem to contribute to the performance of panoptic surveillance. The word performance is operative, however, since the great facilitator of cyberattacks is anonymity. Much as the watchman in the panopticon could not physically watch all inmates, neither could information visualization capture all threats to a system's security. So the 'search and destroy' visualization 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 debates. Security has become so all-encompassing a theme that it marginalizes all others [25, p. 185]. By extension, then, do the visualizations 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

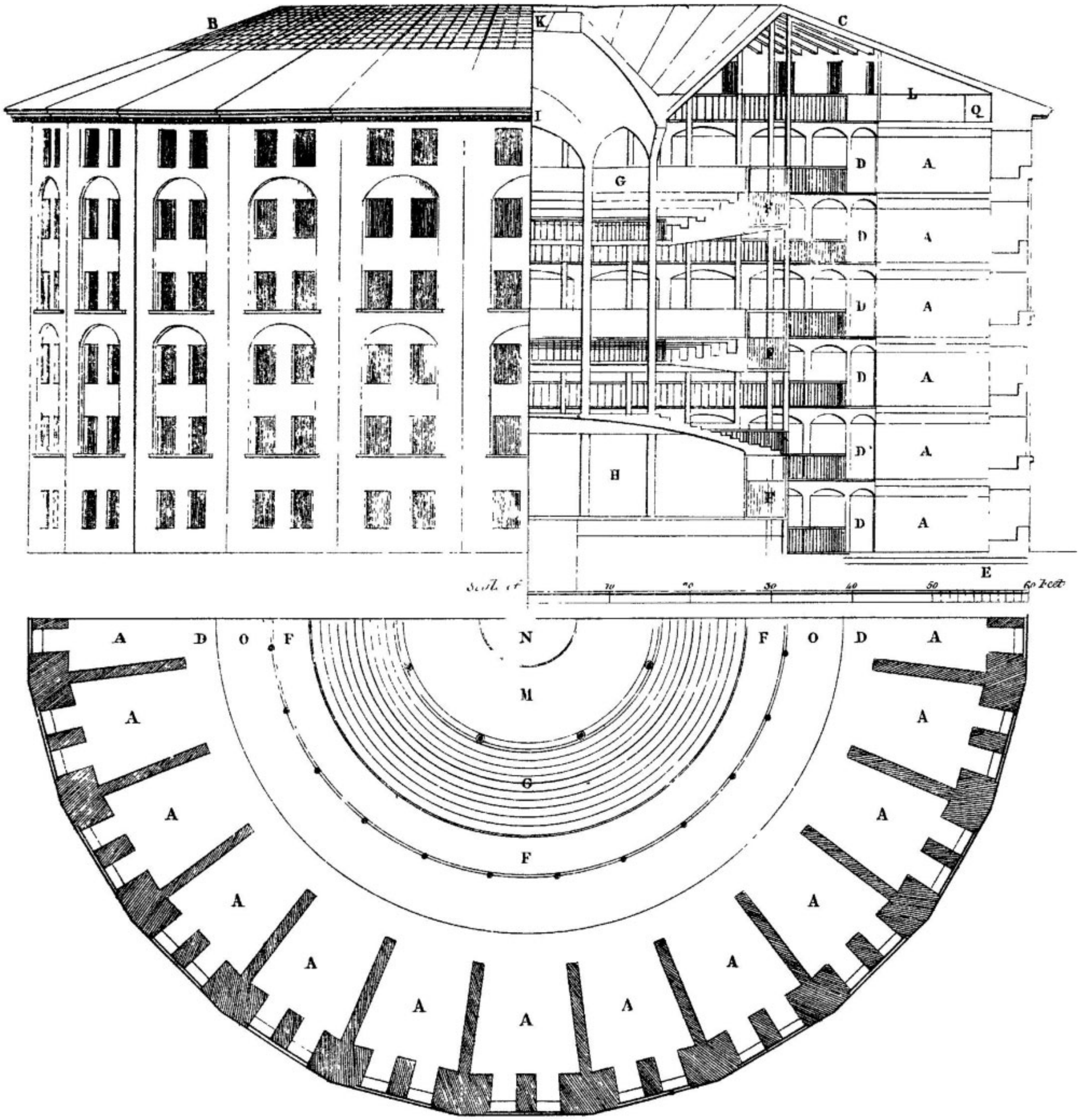


Figure 9. 'Panopticon', Jeremy Bentham. From 'The works of Jeremy Bentham Vol. IV', 172–3. Licensed under Public domain via Wikimedia Commons.

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 visualization is governed by nothing more than a kind of pageantry, to give the appearance of doing something.

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' [25] 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 operationalized in political rhetoric and as part of public policy and then arguing for a broader conceptualization of security that includes networks of resilience, solidarity and cooperation. Security as resilience is a particularly strong theme in the work of security theorist Bill McSweeney [23] 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 [27].

Relational security is the security derived from trusted relationships upon whom an individual is reliant 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 cybersecurity because the mission of cybersecurity is, in part, about enabling the individual, the community and wider society [38] to conduct their everyday lives in environments that have been (and continue to be) transformed by a spectacular variety of digital media.

This type of security thinking changes the referent object from data to people and considers the security of people through the security of data not the security of data as an end in itself. 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, 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 [19] 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; Secondly, there must be 'eyes upon the street, eyes belonging to those we might call the natural proprietors of the street' [19, p. 35]. And thirdly, 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' [19, p. 35]. Jacobs presents watching as a form of looking, a form of observation that takes part on behalf of the community and by the community. This is not watching to report to a separate agency but a form of observation that is there to protect the values of the community as decided by the community and as protected by the community. This perspective on security is an example of Smith's generic description of security [35] as the protection of an ordered set of values where those who decide order also determine the threats.

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 that began 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 focusing on the security of people by 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 hypothesize that information exchange is a social and embodied practice. The working atmosphere in an organization's headquarters and its communication patterns may be, for instance, as important to trust and resilience as its procedural practices. Standard network visualizations 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.

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' [17, 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 (Fig. 10). 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 (Fig. 11). 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' [17, p. 18].

Space syntax analysis has developed a considerable array of visualization methods, including ways of combining it with social network analysis to study communication patterns. One recent 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 has had an impact on the redesign of a Vancouver hospital [28]. While clearly communication in and between outpatient clinics could be visualized 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.

Case studies

Research into participatory modelling of information exchange practices has also informed this article [30]. 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 cybersecurity (a dimension sometimes referred to as the 'weakest link'). Differing degrees of trust and solidarity lead to different perceptions of security, and are difficult to visualize, let alone quantify.

To respond to this difficulty, a specially developed form of participatory diagramming and physical modelling was used to visualize and examine networks of trust and solidarity. A four-stage case study was undertaken. The first stage used The 'Archimate'

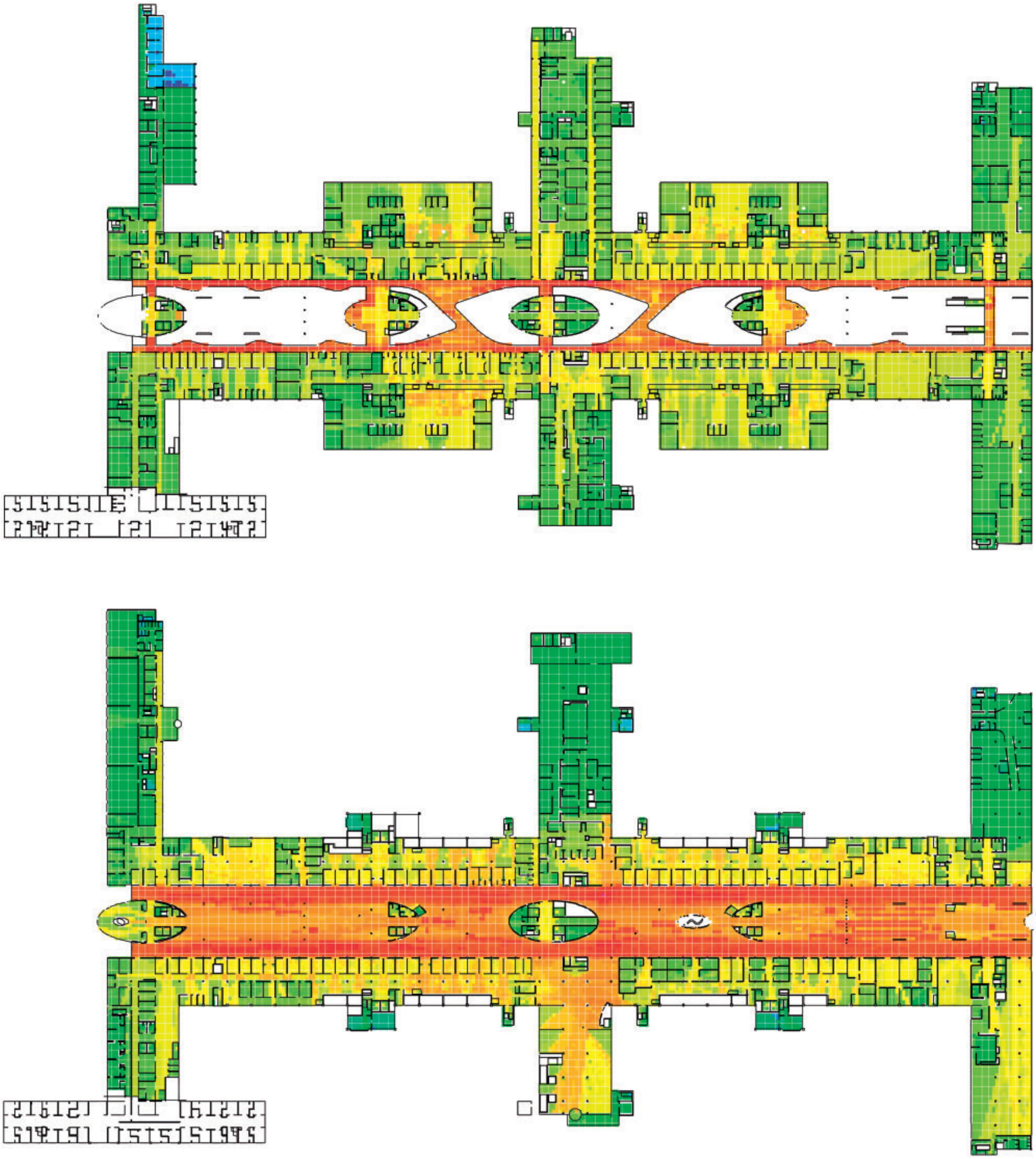


Figure 10. Communication Patterns in Outpatient Clinics in Canada and the Netherlands. Reproduced with permission from The Bartlett School of Architecture, University College, London.

framework to traditionally model the risks to the design of a micropayment service that was to be implemented using IPTV. The risks elicited in this stage did not reflect the networks of trust and solidarity that were very apparent in the security thinking when interviewing the service providers. In the next stage, the service providers identified their core values and the basis for engagement with their customer base. In the last two 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. 12). The Archimate framework for enterprise and risk analysis is referred to by the colour of bricks [20], organizing the dimensions of the scenario that were social, technical and infrastructural, while the organizational core values that had previously been mapped from early engagements were carried through the subsequent stages of analysis and interaction with the participants (Fig. 13).

Physical modelling and its closely related co-design techniques helped the group to construct a narrative, one which not always

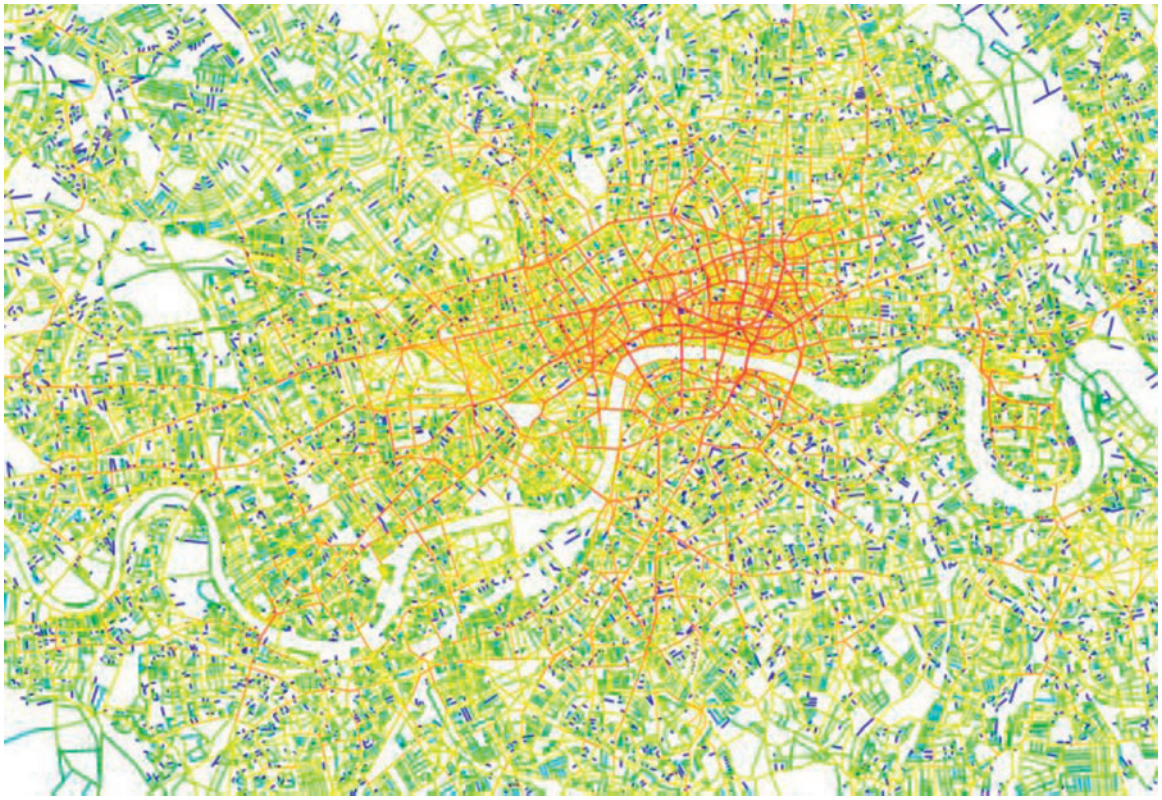


Figure 11. Urban Layout Value Map of the South East of England. Reproduced with permission from Space Syntax Limited and The Bartlett School of Architecture, University College, London.

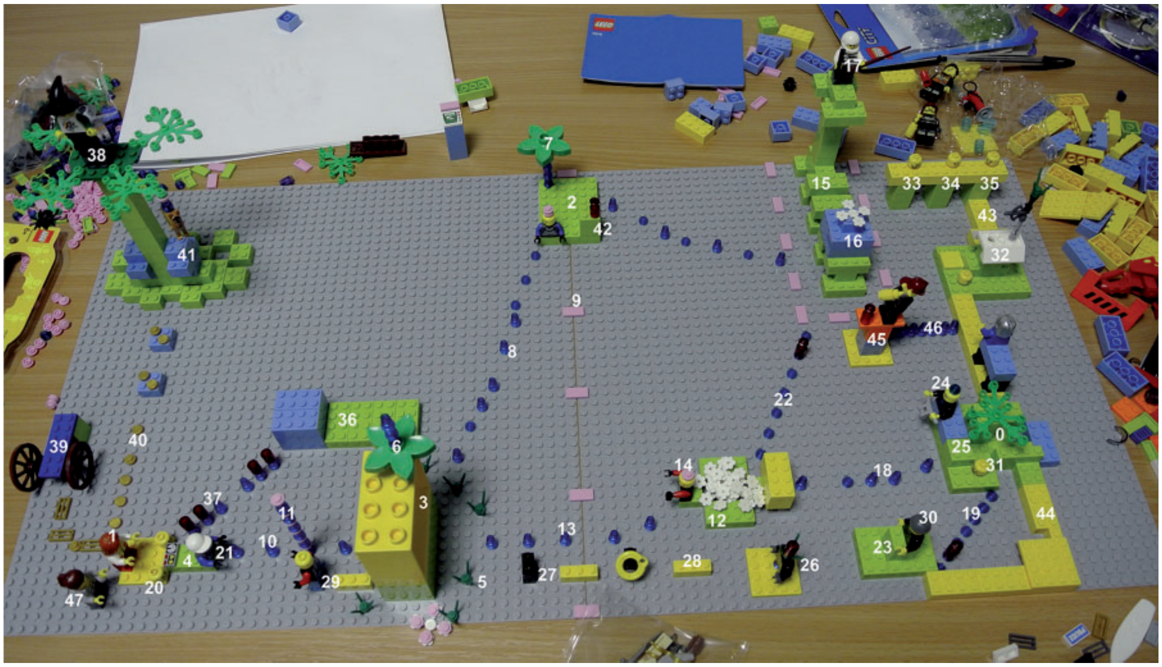


Figure 12. *LEGO* model from participatory sessions, 2015. Royal Holloway, London/TREsPASS. Key: 0 = Participant; 1 = Client; 2 = Card; 3 = TV; 4 = Remote; 5 = Client's sphere of interest; 6 = Antenna on TV; 7 = Antenna on Card; 8 = Data TV to Card; 9 = Boundary between Client and Participant; 10 = Data 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 Participant; 19 = Data Participant to Partner 23; 20 = Children; 21 = Security on Remote; 22 = Data Bank to Cloud; 23 = Partner 23; 24 = Participant Data management; 25 = Participant Server; 26 = Partner 26; 27 = Intervention in progress; 28 = Intervention pathway; 29 = Partner 29; 30 = Staff at Partner 23; 31 = Staff at Participant; 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.

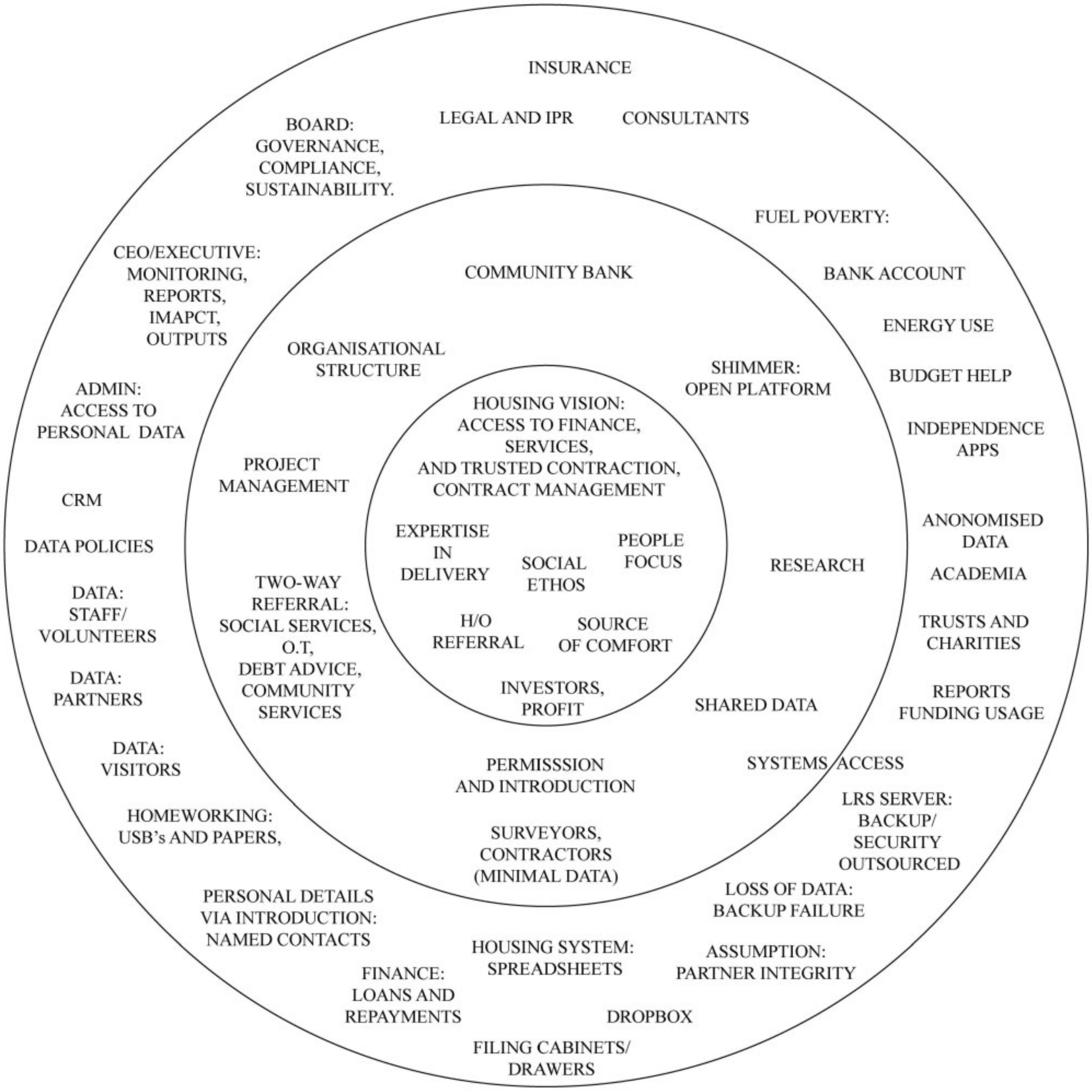

INSURANCE
LEGAL AND IPR
CONSULTANTS
BOARD: GOVERNANCE, COMPLIANCE, SUSTAINABILITY.
FUEL POVERTY:
BANK ACCOUNT
ENERGY USE
BUDGET HELP
INDEPENDENCE APPS
ANONOMISED DATA
ACADEMIA
TRUSTS AND CHARITIES
REPORTS FUNDING USAGE
CEO/EXECUTIVE: MONITORING, REPORTS, IMAPCT, OUTPUTS
ADMIN: ACCESS TO PERSONAL DATA
CRM
DATA POLICIES
DATA: STAFF/ VOLUNTEERS
DATA: PARTNERS
DATA: VISITORS
HOMEWORKING: USB's AND PAPERS,
COMMUNITY BANK
ORGANISATIONAL STRUCTURE
SHIMMER: OPEN PLATFORM
PROJECT MANAGEMENT
RESEARCH
TWO-WAY REFERRAL: SOCIAL SERVICES, O.T, DEBT ADVICE, COMMUNITY SERVICES
SHARED DATA
HOUSING VISION: ACCESS TO FINANCE, SERVICES, AND TRUSTED CONTRACTION, CONTRACT MANAGEMENT
EXPERTISE IN DELIVERY
SOCIAL ETHOS
PEOPLE FOCUS
H/O REFERRAL
SOURCE OF COMFORT
INVESTORS, PROFIT
PERMISSSION AND INTRODUCTION
SYSTEMS/ACCESS
LRS SERVER: BACKUP/ SECURITY OUTSOURCED
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 13. Picture of Participant natural areas of interest, concern and resilience. Royal Holloway, University of London/TREsPASS.

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 the representation. The physical modelling also clearly shows how communities interact with each other. In ‘LEGO’, the participants created groups of service users and service providers and reflected how each group shared and protected data. The physical model could be explored topologically to look at where there were joins between these networks, query the nature of trust, resilience and solidarity in these networks and how those values travel between networks (Fig. 14).

Unravelling the many interwoven and layered elements of their story, and visualizing the developing insights and understanding as the group wrestle with complex service design issues, requires the development of a new method for stabilizing 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. Visualizing 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 visualized as

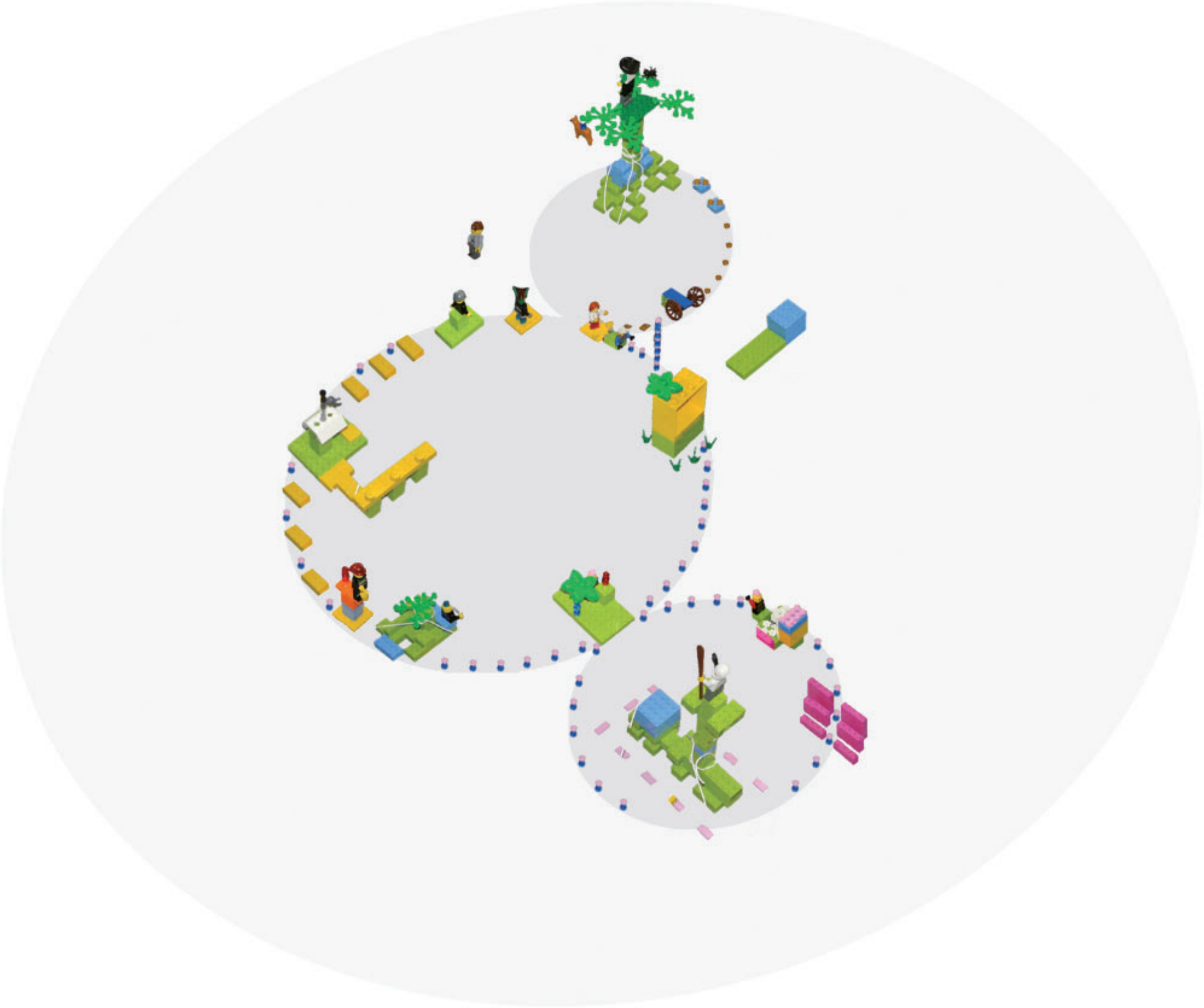


Figure 14. The elements of the *LEGO* model have here been rearranged into a digital collage. The central area defines the essential relationships that are required for the smooth transaction of the service, and this is supported by the outlying banking (bottom) and state systems (top). Royal Holloway, University of London/ TREsPASS.

cumulative temporal and spatial patterns [13], or even as 'manifolds' of social practice [29]. General patterns, at higher levels of societal analysis, have previously only been schematically visualized, creating pictorial metaphors for contrasting types of interlocking shapes and mechanisms that have been found in social practices [33].

The situated and participatory approaches to visualization that have been discussed here clearly have their limitations. A standard critique is to ask how a delocalized 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 universalize intelligence and, on that basis, predict behaviour. One difficulty faced by the allied but nevertheless distinct fields of information security visualization 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' [16]. As a result, it becomes difficult to conceive of visualization 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' visualizations of technologically dense environments should reduce the complexity to a manageable level by using the type of participatory data discussed above, 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 philosopher Nelson Goodman called a more 'graphically *replete* representation' [14], 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' [14, p. 170]. An interface design and visualization 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 15 and 16). In the process it supercedes the traditionally attenuated and technically slanted forms of visualization that are to be found in the literature. Visualizations 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 visualizations, criteria which will most usefully provide specific reference to the categories

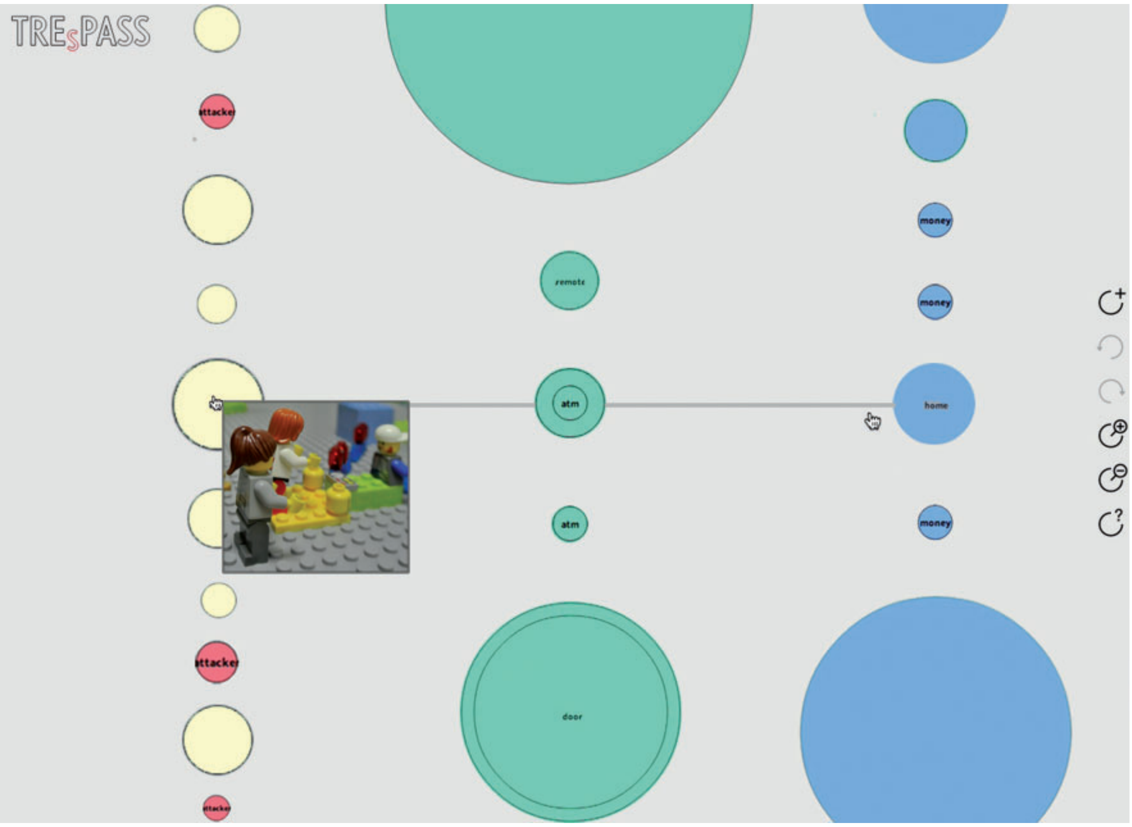


Figure 15. Prototype graphical user interface sketch, showing how excerpts from the qualitative data 'pop-up' on request and add further dimensions to the two-dimensional diagrammatic representation of the service design. Royal Holloway, University of London/TREsPASS.

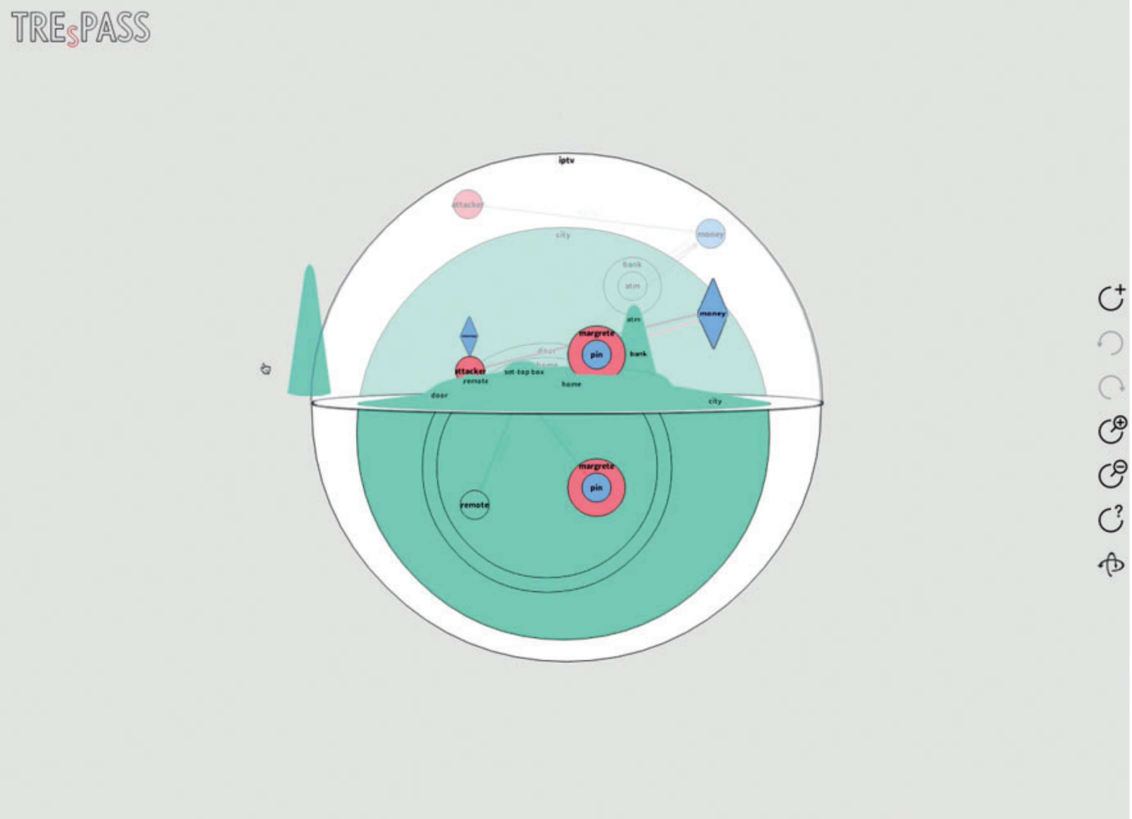


Figure 16. Prototype graphical user interface sketch for constructing a navigator map for the business scenario, seen in circular plan view and as a superimposed relief version of the same mapping, seen in side view. The reliefs are generated from values obtained from the participatory engagements. Royal Holloway, University of London/TREsPASS.

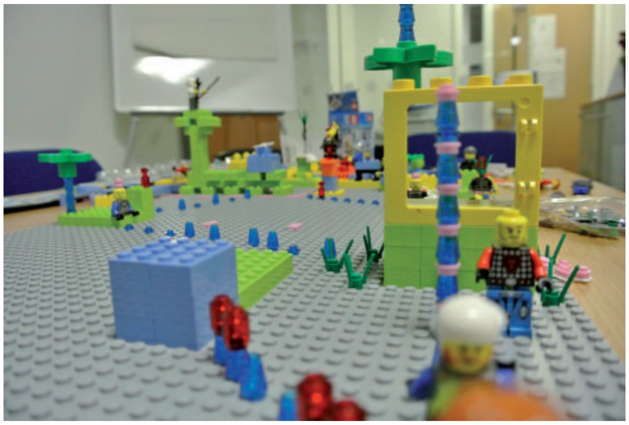


Figure 17. Of the 23 actors that were included in the model, the one most often referred to was the client who is using the service. Their perspective upon the rest of the model and the other actors is shown here. Taking the viewpoint of various actors was also a feature of discussions during the sessions. Royal Holloway University of London/TREsPASS.

and qualities found in the data itself. Moreover, the multiple perspectives and interpretations embedded in these 'rich' visualizations (Fig.17) are especially suited to the increasingly multidisciplinary nature of this work.

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 to understand not just how, why and as part of what social practices human error created a 'weak link', but where and how organizations have successfully avoided being made into the targets of attacks and where and how strong, resilient social networks are formed.

Situated, participatory approaches to visualization can then be positioned as a complement to the more familiar visualization 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 networks across distances is crowdsourcing, 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 [31, n.56]. The system, called 'Ushahidi', proved particularly powerful after the Haitian earthquake of 2010 as a crisis-mapping operation through which people and organizations 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.

Conclusions

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' [34, 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 cannot 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, multivalent, multicultural world, we need not one tool, but lots of them, tuned to the needs of different social and cultural practices.

Another metaphor and potentially useful model is provided by the prolific business of visualization 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)' [21, 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, centralized and static. Biologist Johann Peter Gogarten has suggested that a net provides a better metaphor for visualizing the 'rich exchange and cooperative effects of HGT among microbes' [21, p. 69].

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

Acknowledgement

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. Anderson C. The end of theory: the data deluge makes the scientific method obsolete. WIRED *magazine*, June 23 2008.
2. Bleikertz S, Mastelic T, Pape S. *et al*. Defining the cloud battlefield-supporting security assessments by cloud customers. In: *Cloud Engineering (IC2E), 2013 IEEE International Conference on*, pp. 78–87. Redwood City, CA: IEEE, 25-27 March 2013.
3. Brey P. Hubert Dreyfus: humans versus machine. In: Achterhuis H. (ed). *American Philosophy of Technology: The Empirical Turn*. Indiana University Press, 2001, pp.37–63.
4. Coles-Kemp L, Theoharidou M. Insider threat and information security management. In: Probst CW, Hunker J, Gollmann D, Bishop M. (eds). *Insider Threats in Cyber Security*. Advances in Information Security, **Vol 49**. Hoboken New Jersey: Springer, 2010, 45–71.
5. Crampton JW. Cartographic rationality and the politics of geosurveillance and security. *Cartogr Geogr Inf Sci* 2003, **30**:135–48.
6. Crampton JW. *Mapping: A Critical Introduction to Cartography and GIS*, **Vol. 11**. John Wiley & Sons, 2011.
7. Dalton CM, Thatcher J. Inflated granularity: spatial big data and geodemographics. Available at SSRN 2544638, 2015.
8. Deleuze G. *Negotiations 1972-1990*. New York: Columbia University Press, 1995.
9. Dreyfus HL. *What Computers Still Can't Do: A Critique of Artificial Reason*. Cambridge, Mass: MIT Press, 1992.
10. 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.

11. Foucault M. *Discipline and Punish: The Birth of the Prison*. New York: Vintage, 1977.
12. Foucault M, Ewald F. *'Society Must Be Defended': Lectures at the Collège de France, 1975-1976*, **Vol. 1**. New York: Macmillan, 2003.
13. Giddens A. *The Constitution of Society: Outline of the Theory of Structuration*. Cambridge: Polity, 1984.
14. Goodman N. *Languages of Art: An Approach to a Theory of Symbols*. Indianapolis: Hackett Publishing, 1976.
15. Harley JB. Silences and secrecy: the hidden agenda of cartography in early modern Europe. *Imago mundi* 1988, **40**:57–76.
16. Heidegger M. *Basic Writings: Revised and Expanded*. San Francisco: Harper Collins, 1993.
17. Hillier B, Hanson J. *The Social Logic of Space*. Cambridge: Cambridge University Press, 1984.
18. Hummel JE, Biederman I. Dynamic binding in a neural network for shape recognition. *Psychol Rev* 1992, **99**:480.
19. Jacobs J. *The Death and Life of Great American Cities*. New York: Vintage, 1961.
20. Lankhorst MM, Proper HA, Jonkers H. The architecture of the archimate language. In: *Enterprise, Business-Process and Information Systems Modeling*. Springer, 2009, 367–80.
21. Lima M. *Visual Complexity*, New York: Princeton Architectural Press, 2007.
22. Marty R. *Applied Security Visualization*. Addison-Wesley Upper Saddle River, 2009.
23. McSweeney B. *Security, Identity and Interests: A Sociology of International Relations*, **Vol. 69**. Cambridge: Cambridge University Press, 1999.
24. Milner-Barry S. Hut 6: Early days. In: Hinsley FH. (ed). *Codebreakers: The Inside Story of Bletchley Park*. Oxford: Oxford University Press, 1993, 100–12.
25. Neocleous M. *Critique of Security*. Edinburgh: Edinburgh University Press, 2008.
26. Rittel HW, Webber MM. Dilemmas in a general theory of planning. *Policy Sci* 1973, **4**:155–69.
27. Roe P. The 'value' of positive security. *Rev Int Stud* 2008, **34**:777–94.
28. Sailer K, Pachilova R, Kostopoulou E. *et al*. How Strongly Programmed is a Strong Programme Building? A Comparative Analysis of Outpatient Clinics in Two Hospitals, *Proceedings of the Ninth International Space Syntax Symposium*. Seoul: Sejong University, 2013.
29. Schatzki TR. *Social Practices: A Wittgensteinian Approach to Human Activity and the Social*. Cambridge: Cambridge University Press, 1996.
30. Schulz K-P, Geithner S. Creative tools for collective creativity the serious play method using lego bricks. In: Sannino A, Ellis V. (eds). *Learning and Collective Creativity: Activity-Theoretical and Sociocultural Studies*, Abingdon, Oxford, 2013, 179–97.
31. Sheller M. The islanding effect: post-disaster mobility systems and humanitarian logistics in Haiti. *Cult Geogr* 2013, **20**:185–204.
32. Shneiderman B. *Designing the User Interface-Strategies for Effective Human-Computer Interaction*. Reading, Mass: Addison-Wesley, 1992.
33. Shove E. *Comfort, Cleanliness and Convenience: The Social Organisation of Normality*. Oxford: Berg, 2003.
34. Sloterdijk P. *Bubbles: Microspherology*, trans. W. Hoban. Los Angeles, CA: Semiotext (e), 2011.
35. Smith GM. Into cerberus lair: bringing the idea of security to light1. *The British Journal of Politics & International Relations* 2005, **7**:485–507.
36. Tufte ER. *Beautiful Evidence*. Cheshire, CT: Graphics Press, 2006.
37. Tufte ER, Graves-Morris P. *The Visual Display of Quantitative Information*, **Vol. 31**. Cheshire, CT: Graphics Press, 1983.
38. Virilio P. *War and Cinema: The Logistics of Perception*. London: Verso, 1989.
39. Von Solms R, Van Niekerk J. From information security to cyber security. *Comput Secur* 2013, **38**:97–102.
40. Ware C. *Information Visualization*, **Vol. 2**. San Francisco: Morgan Kaufmann, 2000.
41. West R, Mayhorn C, Hardee J. *et al*. The weakest link: A psychological perspective on why users make poor security decisions. *Social and Human Elements of Information Security: Emerging Trends and Countermeasures*, Hershey, PA: Information Science Reference, 2009, 43–60.
42. Winograd T, Flores F. *Understanding Computers and Cognition: A New Foundation for Design*. Norwood, NJ: Ablex Publishing, 1986.
43. Wood D. *Rethinking the Power of Maps*. New York: Guilford Press, 2010.