SECURITY DIALOGUE

Special issue on Preemption, Practice, Politics

Security and the incalculable

Security Dialogue
2014, Vol. 45(5) 423–439
© The Author(s) 2014
Reprints and permissions:
sagepub.co.uk/journalsPermissions.nav
DOI: 10.1177/0967010614539719
sdi.sagepub.com
SAGE

Louise Amoore
Department of Geography, University of Durham, UK

Abstract
In this article, I explore a specific relation between mathematics and security calculations. Recalling the confrontations between the mathematician Alan Turing and the philosopher Ludwig Wittgenstein in the 1930s, I am interested in the relationship between intuition and ingenuity. During Wittgenstein's 1930 lectures on the foundations of mathematics, Turing interjects in order to insist upon the capacity of number: 'one can make predictions'. Wittgenstein replies that mathematics 'makes no predictions', but instead is a form of grammar: 'taken by itself we shouldn't know what to do with it; it's useless. But there is all kind of use for it as part of a calculus'. It is just such a formulation of a calculus or grammar – 'decision trees', 'event trees', 'attribute-based algorithms' – that characterizes contemporary security. As for Turing, the logic comprises 'two faculties, which we may call intuition and ingenuity'. The intuitive realm of imagination and speculation reaches toward a possible solution, while the ingenuity seeks arrangements of propositions. The advent of 'rules-based' and 'risk-based' security decisions, then, are always already political because they precisely involve combinatorial possibilities whose arrangement has effects in the world.

Keywords
algorithm, calculation, data, insecurity, science, security

> Alan Turing: 'From the mathematical theory one can make predictions'
> Ludwig Wittgenstein: 'Yes, one can. But what sort of predictions? What is the relation between the mathematics and the predictions?' (cited in Wittgenstein, 1976: 150)

Introduction: The fault tree

At a public meeting held six days before a major earthquake struck the Italian city of L'Aquila on 6 April 2009, killing 309 people, a panel of scientists had been asked to assess the risk of a major earthquake in the light of the multiple tremor events of preceding months. The panel – appointed to the 'National Commission for the Forecast and Prevention of Major Risks' – stated at the meeting that 'minor shocks do not raise the risk of a major quake' (Nosenga, 2012). In the strict terms

Corresponding author:
Louise Amoore.
Email: louise.amoore@durham.ac.uk

of scientific knowledge, this was entirely accurate – the data they held on a series of past seismic events could not be meaningfully used to calculate the likelihood of a future event. Yet three years later, on 22 October 2012, the six scientists and one civil protection public official were convicted and sentenced to six years in prison. Throughout the trial, the defence case had been that 'no causal link' could be established between the judgements of the scientists before the catastrophic event and the subsequent loss of life in L'Aquila. The absence of causality was similarly emphasized in a letter sent to Italian President Giorgio Napolitano by more than 5000 of the world's leading geophysicists and seismologists, in which they emphasized the limits of what could be inferred from scientific data. 'Predicting the time, location and strength of a future earthquake is technically impossible', they wrote; 'it is … incalculable'.

What is most significant about this case, however, is precisely its signalling of an emerging form of responsibility to calculate the incalculable. The L'Aquila group were not convicted of manslaughter for failing to predict an earthquake, and even the public prosecutor Fabio Picuti reported that 'I'm not crazy, I know they can't predict earthquakes' (*Nature*, 2012). Rather, they were found guilty for failing to arrive at an adequate risk calculus – for failing to infer, intuit, imagine and extrapolate from the available data. Thus, although the data in their possession were insufficient as scientific grounds for inferring anything at all about the future, it was argued in the court that the scientists could have correlated their data with other elements – with the fragility of ancient buildings, for example, or with the possible risks of 'falsely reassuring' a population.[1] In effect, there was no juridical disagreement that a linear causal connection could not be established between the science and the event, but instead non-linear branches of possibility and correlative causality were said not to have been acted upon.

Why does the L'Aquila case matter for how we think about contemporary security and the capacity to secure against an otherwise incalculable future? The case raises the spectre of a calling to account for the failure to assemble data with other things; a failure to make links, to 'connect the dots of available information', to associate and correlate plural components even if they are incomplete or fragmentary (9/11 Commission, 2004: 408).[2] In effect, the earthquake scientists' claim that it would be irresponsible to act on the basis of incomplete or inadequate data confronts a sovereign demand that incompleteness be enhanced by inference across the gaps – nothing is incalculable as such.

The spectre of a search for forms of calculus that open up new ways of dealing with limited or insufficient knowledge also haunts contemporary security. More specifically, it haunts the question of the use of data to infer possible future security threats. When the US Congressional Research Service (2008: 1) prepared an analysis of the use of data mining for homeland security, they explained to Congress the allure of using 'data analysis tools to discover previously unknown patterns and relationships in large data sets'. They then outlined the 'limitations of data mining as a terrorism detection tool', emphasizing that 'it does not tell the user the value or significance of these patterns' (US Congressional Research Service, 2008: 3). There is, then, pressure on the user or the case analyst to infer what this value or significance might be, and to reach a judgement:

> Efforts to fight terrorism can take on an acute sense of urgency. This urgency can create pressure on both data holders and officials who access the data. To leave an available resource unused may appear to some as being negligent. Data holders may feel obligated to make any information available that could be used to prevent a future attack. Similarly, government officials responsible for ensuring the safety of others may be pressured to use or combine existing databases to identify potential threats. (US Congressional Research Service, 2008: 3)

Thus, to have available data – even if they are tangentially related, partial or fragmentary – and to fail to infer across the gaps 'may appear to some as being negligent'. As is illuminated by the case of the conviction of the Italian scientists, the intrinsic value of the data is insufficient; it can tell us nothing about the probability of a future seismic event. What is sought instead is a different mode of calculation, one that loosens the language of modern probability and assembles in its place a set of combinatorial possibilities. Thus, where strict adherence to probabilistic science would place limits on the capacity for prediction – an earthquake cannot be predicted, or a terrorist attack cannot be predicted – the proliferation of 'conditional probabilities' and 'subjective probabilities' appears to allow for new combinations of possibility (Department of Homeland Security, 2010). The logic of fault and culpability that has surfaced in the L'Aquila case adheres less to a juridical convention of probable cause or balance of probability than it does to a form of security that changes the nature of the calculation itself. The US Department of Homeland Security's publication of a 'risk lexicon' for its analysts, for example, establishes a shared vocabulary of possible branching pathways of fault for 'natural disasters' and 'terrorist attacks'. 'A fault tree', explains the security analysts' lexicon, 'can be used to estimate the probability of a program failure, working backwards in time to determine the possible causes' and 'visually displaying and evaluating failure paths' (Department of Homeland Security, 2010: 15). The fault tree, deploying as it does multibranch, non-linear forms of causality, embodies something of the demand for the calculation of the incalculable that is so visibly present in the L'Aquila case. Though no single linear causality may be established, plural failure paths may be visualized and acted upon.

In this article, I propose that contemporary modes of security calculation do not supplant or overturn the strict adherence to number, science and probability with imagination, speculation, inference and conjecture that is at the limit of knowledge or beyond science itself (Ewald, 2002; Aradau and Van Munster, 2011). Rather, the turn to inference and intuition in contemporary security calculation is but one novel formulation of an historical enfolding of the intuitive faculties within mathematical calculation. It is a formulation within which calculability is never in question, where it appears that an arrangement of possible links and connections can always be arrived at. Thus, what we now think of as 'algorithmic' or data-driven security is but one specific set of combinations of intuition and calculation, albeit one with novel and particular effects. For the purposes of my discussion here, I am interested in three aspects: first, how the relation between the intuitive and the calculative faculties can be understood; second, how mathematics supplies a grammar that can be used for security calculation; finally, what the limits of rules or decision procedures are that we may think of as algorithmic calculations.

The confrontations of mathematics and philosophy in the 1930s do much to illuminate the question of how mathematical calculation arranges possibilities. During Ludwig Wittgenstein's 1939 *Lectures On the Foundations of Mathematics* (Wittgenstein, 1976), the young Alan Turing (later to be the Bletchley Park code-breaker and theoretician of the first computer) interjects to assert the capacity of number: 'from the mathematical theory one can make predictions'.[3] Wittgenstein replies that 'pure mathematics makes no predictions', or that number as such has no predictive capacity. When Wittgenstein refers to prediction here, he is indicating the difficulty of abstracting pure mathematics from its application. Though he does not specify what he means by predictive capacity, his examples of chess playing and games suggest a claim on a future outcome. 'The difficulty in looking at mathematics as we do', he proposes, is that 'we cut pure mathematics off from its application' (Wittgenstein, 1976: 150). What matters to Wittgenstein is 'the relation between the mathematics and the predictions', what he calls the 'grammar' of mathematics, or how number is assembled in a calculus so as to make things possible or to have effects in the world. For Wittgenstein, the mathematical concept of calculation 'cannot be separated from its essential normativity' (Shanker, 1987: 616), so that pure mathematics is always in this sense also applied. Without the 'and', 'with', 'if then', 'can be concluded from' of the grammar of mathematical calculus, number as such would have no capacity; it would do nothing.

The Turing–Wittgenstein discussions on number are significant because they show how all forms of mathematics deploy a grammar, a politics of combinatorial possibilities that make calculation possible. As historian of mathematics Keith Devlin (1994: 3) expresses it, mathematics is 'the science of patterns – numerical patterns, patterns of shape, patterns of motion, patterns of behaviour'. For Devlin, mathematics is a language that expresses patterns as 'combinatorial possibilities' (Devlin, 2000; see also Kirby, 2011). Understood thus, the contemporary rearranging of combinatorial possibilities – in algorithmic methods, subjective probabilities or fault trees – does not displace apparently objective scientific rationalities with subjective imagination, but rewrites the grammar of calculation itself. Wittgenstein's 20th-century claim that number, as such, can predict nothing is echoed by the 21st-century claim that probabilistic calculation cannot predict events.[4] There is little political or scientific disagreement that the earthquake data cannot predict a future seismic event, or that data held by the authorities on 'hijacker profiles' could not predict a future terrorist attack (9/11 Commission, 2004: 84). But, the contemporary security calculation is deploying mathematical devices in such a way that it does not matter whether something can be predicted, only that it can be arranged as calculation – as a decision tree, an algorithmic code, or as an association rule that links plural elements.

Intuition and ingenuity

There is nothing at all novel in the incorporation of the mathematical sciences into the domains of security and war. Indeed, during Alan Turing's 1936–1938 residency at the Princeton Institute of Advanced Study (IAS), the conventional divides between pure and applied mathematics were a matter of discussion, not least because pure mathematics began to inform applied work on ballistics and nuclear blast waves.[5] Amid the work of J. Robert Oppenheimer on the mathematics of the H-bomb, and John von Neumann on shock waves, the notes on the meetings of the IAS mathematicians record Albert Einstein emphasizing 'the dangers of war work', fearing that the 'emphasis of such projects will further ideas of preventive wars' (cited in Dyson, 2012: 83). For both Turing and Einstein, working in the ferment of a close group of scholars at the cusp of new mathematical possibilities, the relation between what is possible mathematically and what is actioned as state security strategy is one fraught with political difficulty.

At the heart of the IAS discussions on the proper relation of mathematics and war lay the question of whether the intuitive practices of pure mathematics could be systematized, rendered replicable or codified for broader applications. The World War II question of the relationship between intuitive and imaginative capacities and codified systems continues to dominate contemporary debates on the use of more imaginative forms of calculation for national security. Indeed, Turing's theorization of the universal computing machine made possible the contemporary digital systems that convert complex mathematical thought into routinized security procedures. The report of the 9/11 Commission (2004: 344), for example, finds that 'it is crucial to find a way of routinizing, even bureaucratizing, the exercise of imagination'. Though the deployment of imagination through 'scenarios' and 'difficult what ifs' has been an important element of post-9/11 security practice, the key aspect is to be found not so much in imagination as in the routinization of imaginative faculties (9/11 Commission, 2004: 354). The manifest desire to 'assemble enough of the puzzle pieces' and to 'make some sense of them' has dominated the subsequent 10 years of assessments of the implementation of the Commission's recommendations (Department of Homeland Security, 2011). The imagination of links and associations across items of data, operationalized via data mining and analytics, has become the mainstay of the bureacratization of imagination. It is mathematics that has supplied the means to incorporate intutition and inference into the protocols and routines of security, and it is mathematics that promises the calculability of security problems.

And so, though imagination is part of the picture of emerging forms of security calculation, the vast bulk of such calculation is not imaginative at all. Or, more precisely, it is as concerned with the establishment of routines, subroutines and procedures as it is with intuitively opening onto the uncertain future. One might say even that security calculations are not oriented to the imagination of possible futures, but more precisely to the arrangement of possible combinations. But is it possible to be more specific about the form of imagination that is folded into calculation? As the inferences of multiple layers of software designers, border guards and petty bureaucrats become invited into the security calculation, what is the place of intuition? How is intuition made amenable to procedural routine and bureaucracy?

To reflect on these questions further, I will return to Alan Turing, and to some of his earliest work on his 1937 PhD thesis. In his *Systems of Logic Based on Ordinals*, Turing develops a distinction between what he calls 'intuition and ingenuity'. 'Mathematical reasoning may be regarded', proposes Turing (1936: 242), 'as the exercise of a combination of two faculties, which we may call intuition and ingenuity.' All forms of mathematical calculation, we might say following Turing, engage a twinning of two distinct practices of reason. The exercise of intuition, as Turing (1936: 242) formulates it, 'consists in making spontaneous judgements which are not the result of conscious trains of reasoning'. In letters sent to fellow mathematician Max Newman, Turing proposes intutition as something akin to 'inspiration', in which spontaneous and tacit judgements 'invariably' lead to 'correct' solutions to mathematical problems. The exercise of ingenuity, by contrast, 'consists in aiding the intuition' through 'suitable arrangements of propositions, and perhaps geometrical figures or drawings'. The practice of ingenuity in Turing's analysis connects together the elements of intuition, rendering the intuitive solution 'less open to criticism' (Turing, 1936: 242). The development of a 'formal logic', then, combines the two faculties of intuition and ingenuity in such a way that 'the necessity for using the intuition is then greatly reduced by setting down formal rules for carrying out inferences which are always intuitively valid' (Turing, 1936: 242). The distinguishing of intuition from ingenuity mattered immensely to Turing's subsequent 'Turing machine' and his exposition on computable number:

> Once intuition has supplied the materials from which proofs are to be constructed – the basic inference rules – then a suitably programmed Turing machine is able to grind out all the valid proofs of the system one by one. (Copeland, 2010: 136)

The Turing machine demonstrated an early form of computer programming, establishing a set of inference rules from which a computing machine can calculate all valid proofs.[6] From Turing's groundbreaking thought we begin to see how mathematical calculation embodies both the affective and spontaneous realms of intuition and the apparently structured ingenuity of routine and logic. The relationship between these two faculties of reason is iterative – a back-and-forth rhythm of inspiration and formulation. With intuition one feels one's way toward a solution. This is perhaps most familiar when one holds a puzzle such as a Rubik's cube in one's hands – the steps taken are predominantly intuitive as we feel our way towards a solution. Of course, if a solution is reached intuitively, then it is not provable, not replicable by others without a concomitant ingenuity – the building of a formula, an equation, a rule, an algorithm – that allows for the procedure to be followed. According to Turing, though, the exercise of intuition can never be entirely eradicated by rule or routine, for it is intuition that bridges the gaps of the incalculable elements of proof or theorem.[7]

How, then, do the twinned faculties of intuition and ingenuity function in the contemporary deployment of mathematics and computing for security calculations? I propose that what we are witnessing in the proliferation of what have come to be known as 'risk-based' and 'rules-based' security decisions is just such an intuitive bridging of the gaps in available data and an ingenuity of algorithmic rules to make this routine replicable into the future. A risk-based security technique is based on a set of decision procedures through which a final calculation is produced – 'Is this factor present?', 'Is this variable co-present?', and so on. Though it is a set of association rules – a 'rules-based' programme – that allows for the risk calculation to be made with ingenuity, it is intuition that supplies the identification of patterns.

Let us consider an example of what this combination of ingenuity and intuition might look like. When the world's leading scientific computing society, the Association for Computing Machinery (ACM), gathered to respond to the 9/11 Commission's recommendations, its members made the case for the capacity of the mathematical rules of data mining to identify patterns in large volumes of unstructured data. Noting that 'we cannot always rely on data from the past', and that conventional statistical profiles are useless for counter-terrorism – because 'the profile of a suicide bomber has completely changed from what it once was' – the algorithmic techniques draw together possible relations and associations across data items from otherwise unrelated databases. Existing data on commercial transactions are assembled together with images from websites and text from social networking sites. The assembling is conducted through the already decided algorithmic rules, with the effect that apparently 'unstructured' data become structured and ordered:

> Can we do it? Number of items is extremely large, number of transactions is extremely large. You are talking *all of the possible* names that could become items. You are trying to find out relations that might exist. So, here combining text data and images. This is a site in Pakistan and what is happening here is these sort of different characteristics we are interested in, they are *written into the rules*. It has things like financial support, Islamic leaders and so on … so we can get a profile for the site, and a series of leads to other second level associated sites. (ACM, 2004, emphasis added)

The use of data analytics to make inferences about possible future terrorism threats has become the keystone of what has been widely heralded as a more imaginative approach to intelligence gathering, analysis and decision. What we see in the deployment of a mathematics of algorithmic security is exactly the co-presence of intuition and ingenuity that was proposed by Turing in his theorization of computation. The exercise of intuition is present in the judgements on 'trying to find out relations that might exist', or the 'different characteristics we are interested in', and it is present in the software designer's intuitive reach for a solution to the puzzle. In the process of being 'written into the rules' and into 'associated sites', however, we find the exercise of ingenuity that finds routines and codes that make the intuition replicable in other places and at other moments.

In contemporary security practice, such ingenuity is exercised largely through the use of analytics algorithms that read and make sense of large volumes of data. Yet, despite important debates on the capacities of machines to think, read and write, the precise form of the ingenuity of building a rule is rarely considered (Hayles, 2005, 2012). In a 1947 lecture on 'The Automatic Computing Engine', Turing describes the subroutines or rules that make up the components of a program, suggesting that an 'important idea is that of constructing an instruction' that can be used 'amongst other things for discrimination'. The rules function where 'certain processes are used repeatedly in all sorts of different connections, and we wish to use the same instructions … every time…. We have only to think about how this is done once, and forget then how it is done' (Turing, 1947: 16). And so, it may be that contemporary data analytics offer a more imaginative or speculative approach to security calculation, just as they also discriminate with finite racialized imaginaries of 'characteristics we are interested in'. But it is not the case, as we often read in critique of the politics of security, that such calculations supply a gloss of objectivity and techno-science that obscures the real politics. On the contrary, this is mathematics, and it is a mathematics that is always already political precisely because of its combined faculties of intuition and ingenuity. This is a mathematics that is an arrangement of intuitive propositions that make things happen in the world, that is written into the rules of what is to be secured.

'There is all kind of use for it as part of a calculus': Mathematical grammars of security

In the opening citation of this article, Wittgenstein asked the question that animates my analysis of the specificity of the intersection of mathematics with security: What is the relation between the mathematics and the predictions? If one accepts that mathematics is an arrangement of propositions that does things, makes things happen, then what is the relation between the arrangement and the uncertain future?

The inquest evidence and post-event reports after the terrorist attacks of Washington, New York, Bali, Madrid, London and Mumbai have overwhelmingly concluded that attentiveness to the strict prior probabilities of terrorist attacks – extremely low in these specific parts of the world – distracts the attention of the intelligence and analyst communities from the possibility of a 'low-probability, high-impact event'. As a result, there has been an explicit loosening of the strict calculation of probability in the weighting and assembly of information and material to allow for modified 'conditional' or 'subjective' probabilities. In most instances, this loosening of the conventions of probability follows some variant of a revitalized scientific interest in Bayes' (1763) theorem on conditional probability (Daston, 1986: 258). Bayesian probability understands the strict statistical probability of an event to be an underlying 'prior' probability – a number that can be modified by the observation of subsequent events that supply 'reliability figures' or 'confidence scores' (Devlin, 1997: 263). The significance here is that the Cartesian logics of classical mathematics are breached and the observer's senses are invited into the capacity to calculate. If one heeds Wittgenstein's (1975: 38) caution that 'what is interesting is how we *use* mathematical propositions', then attention is drawn to the specific uses of revived Bayesian assumptions. What does Bayesian calculation do? It arrays together multiple correspondences, making links and associations between them through the use of intuitive judgements. In the 2012 US presidential election, for example, statistician Nate Silver accurately predicted the winner of all 50 US states. Using a variant of Bayesian calculation, Silver (2012: 248) has proposed how the probability of terrorist attacks on the World Trade Center could have been more precisely modified as the events unfolded:

> Consider a somber example: the September 11 attacks. Most of us would have assigned almost no probability to terrorists crashing planes into buildings in Manhattan when we woke up that morning.… However we would also have assigned a very low probability to a plane hitting the World Trade Center by accident. This figure can actually be estimated empirically: in the previous 25,000 days of aviation over Manhattan there had been two such accidents. That would make the possibility of such an accident about 1 chance in 12,500 on any given day. If you use Bayes's theorem to run these numbers, the probability we'd assign to a terror attack increased from 0.005% to 38% the moment the first plane hit. The idea behind Bayes's theorem, however, is not that we update our probability estimates just once. Instead, we do so continuously as new evidence presents itself to us. Thus, our posterior probability of a terror attack after the first plane hit, 38 percent, becomes our *prior* possibility before the second one did. And if you go through the calculation again, to reflect the second plane … the probability that we were under attack becomes a near certainty − 99.99 percent.

Though Silver's comments on probabilistic reasoning for security should be seen in the context of his application of the same formula to stock markets, Major League baseball games and earthquakes, they do reflect a significant new sensibility toward probabilistic reasoning among security analysts. For example, the attribute-based link analysis algorithm underwriting the software of data analytics for risk-based security functions by evaluating and weighting the relation between data points or nodes, identifying patterns of interest and assigning a confidence score to the calculation (Berlinski, 2000).[8] The calculations that are made are non-linear; they allow for multiple possible modifications, arcs and feedback loops, and for multiple possible chains of events to be kept running simultaneously. Using such calculations, one does not need to definitively make a choice about the most probable outcome, filtering out the least likely, but only to differentially assign weight to each of the possible branches of events.

Let us reflect on an example of an arrangement of combinatorial possibilities that allows for the branching points of human and machinic interventions. In the guidance manual for the Department of Homeland Security's intelligence analysts, we find the 'event tree' – a 'graphical tool used to illustrate the range and probabilities of possible outcomes that arise from an initiating event' (Department of Homeland Security, 2010: 6). Though arguably a strikingly rudimentary technique, the branching visualization of the event tree seeks out a form of calculation that incorporates technological failures as well as human error, judgement and intuition (see Figure 1). The suggested uses for the event tree include 'analysts us[ing] an event tree to diagram possible outcomes from a terrorist attack':

> The initiating event is an *Attack Attempted*. From the initiating event, the tree branches into a sequence of random variables, called events. The branching point at which a new random event is introduced is called a node and is depicted by a circle. The first of these random events is *Personnel Action to Stop Attack*. The *Personnel Action to Stop Attack* is successful with probability $1–P^1$ and fails to stop the attack with probability P^1. If *Personnel Action to Stop Attack* is successful, then the branch leads to the final outcome of Unsuccessful Attack, No Damage (Scenario A). If *Personnel Action to Stop Attack* is not successful, then the branch leads to the next node representing the random event of whether the *Security Equipment to Stop Attack* is successful or not with probabilities of $1-P^2$ and P^2 respectively. If the *Security Equipment to Stop Attack* is successful then the branch leads to the final outcome of Unsuccessful Attack, No Damage (Scenario B). If *Security Equipment to Stop Attack* fails then the branch leads to the final outcome of Successful Attack, Damage to System (Scenario C). (Department of Homeland Security, 2010: 13)

The event tree visualizes a series of branches of possible correlated events and interventions with possible associated outcomes. In a sense, it does exercise the intuitive capacity to imagine or infer what an event might look like, what the effects of a particular intervention might be. Of course, the event tree is in many ways a profoundly unimaginative visualization of multiple branching links and pathways. Yet it is precisely this simplicity that renders the decision-tree method amenable to computational processes. In practice, the event tree is one form of a decision-tree method that constructs a set of coded steps and procedures that can be automated within an algorithm (Elder et al., 2012). A numeric conditional probability is assigned at each node, with the multiplication of the first layer of probability (Personnel Action to Stop Attack is not successful, $P_1=0.1$) by the second layer (Security Equipment to Stop Attack Fails, $P_2=0.3$), resulting in an a posteriori probability of a successful attack of 3%. Using predictive analytics, the desk analyst can add or 'prune out' variables to model 'multiple what if scenarios' regarding the effects of a specific security intervention (Ohlhorst, 2013: 5).

One response to the event-tree security calculation may be to ask 'What is the 3%?', 'What does a 3% chance of attack mean?', 'What forms of action by security personnel or technology could be reasonably justified on the basis of that 3%?'. Indeed, one might propose to critique the security calculus on the very basis that the number itself is arbitrary and meaningless. To open the critique at the site of number itself, though, is to miss an important locus of the politics of the contemporary security calculation.

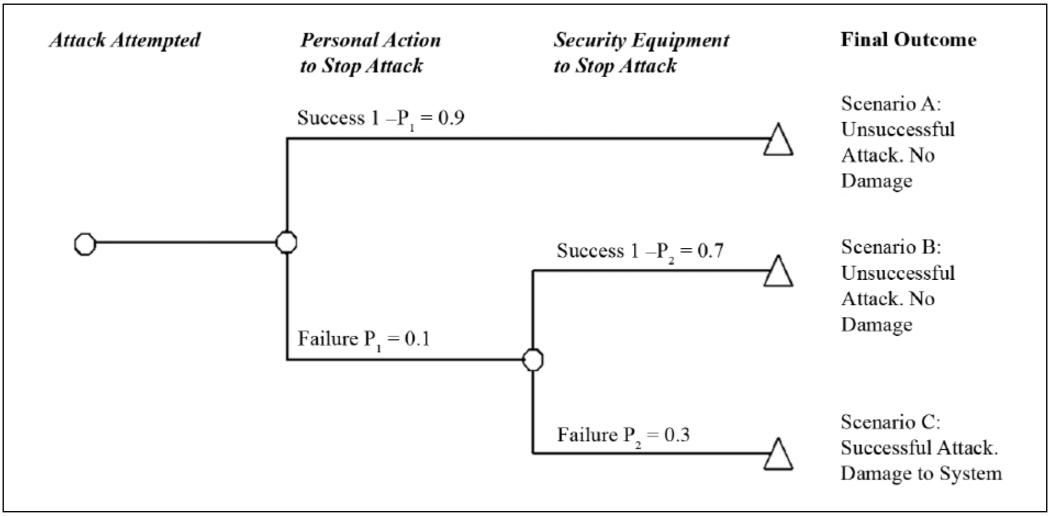
Attack Attempted
Personal Action to Stop Attack
Security Equipment to Stop Attack
Final Outcome
Success 1 –P$_1$ = 0.9
Scenario A: Unsuccessful Attack. No Damage
Success 1 –P$_2$ = 0.7
Scenario B: Unsuccessful Attack. No Damage
Failure P$_1$ = 0.1
Failure P$_2$ = 0.3
Scenario C: Successful Attack. Damage to System

Figure 1. The 'event tree' for a terrorist attack (Department of Homeland Security, 2010: 13).

The data content of the Bayesian-influenced security calculation, the 3% itself, has little meaning when the grammar of the security calculation is a grammar of *if*, *and*, *then* (Berlinski, 2000: 187; Amoore, 2011). If *A* is present (e.g. a previously denied visa application, a specific financial transaction, a particular past travel route) and *B* is co-present (e.g. the name of an associate, a link to past crime data, a series of airline 'no-shows', a listed credit card number), then ╟ (it can be inferred that) a security risk *Y* is posed. The content of the data that enter the decision tree, the nodes of the calculation, the verifiability or otherwise of the sources of intelligence, the number as such: none of these elements are of significance to the capacity to render the problem calculable. What matters are the correspondences and correlations between the elements – how they are held together by inferences across the gaps. As Keith Devlin (2000: 77) explains, one can

> think of the mathematician's abstract patterns as 'skeletons' of things in the world. The mathematician takes some aspect of the world, say a flower or a game of poker, picks some particular feature of it, and then discards all the particulars, leaving just the abstract skeleton.

Returning to the event tree in these terms, what is visualized is a skeletal series of combinatorial possibilities with associated numeric conditional probabilities. The combinations could be almost infinitely reworked for as long as the relations among the elements can be sustained, with branches added or 'pruned out'.

Placed at the service of security calculation, the mathematical sciences offer a grammar of combinatorial possibilities that allows for things – people, objects and data – to be arranged together, for links to be made. Returning to Turing and Wittgenstein for insight on what the implications of such a form of calculation may be:

> Wittgenstein: '2 + 2 = 4 – but this isn't about 2: it is grammatical.'
>
> Turing: 'Isn't it merely a question of how one extends the use of the word "about"?'
>
> Wittgenstein: 'Of course, you can say mathematical propositions are about numbers…. But this brings me to an entirely different sense of how a reality corresponds to mathematics. Because now, if "30 × 30 = 900"

> is not a proposition "about 30", you will look for the reality corresponding to it in an entirely different place; not in mathematics but in its application'. (cited in Wittgenstein, 1976: 251)

In Turing's analysis, there is something 'about' the intrinsic properties of number – in this instance, there is something 'about 2'; 2 has a capacity. Of course, in Turing's world of pure mathematics, the properties of 2 are crucial – number has a vitality, a vitality that propels thought and intuition. For Wittgenstein, though, mathematics is part of the apparatus of language; it is a grammar that makes some propositions sayable and silences others.[9] Reflecting on knowledge in mathematics, he describes how 'one has to keep on reminding oneself of the unimportance of the "inner process" and ask "why should it be important? What does it matter to me?" What is interesting is how we *use* mathematical propositions' (Wittgenstein, 1975: 41). If we follow Wittgenstein here, then our attention is drawn to the application of the proposition, to how it functions in the world. 'Taken by itself we shouldn't know what to do with it; it's useless', says Wittgenstein (1975: 42) of number; 'but there is all kind of use for it as part of a calculus'.

What does it mean to say that there is all kind of use for number as part of a calculus? Reflecting for a moment on how mathematical devices are being used by the UK and European policing and counter-terror authorities to mine and analyse so-called open-source data such as Facebook text or Twitter feeds, there is currently some debate over the intrinsic quality of unstructured data that could be considered to be terrorism-related data.[10] The growth of consumer 'sentiment analysis' to 'take the pulse' of a 'specific target group' through its members' web discussions is now increasingly mirrored by what is called 'meaning extraction' for counter-terrorism (Elder et al., 2012: 57). As I showed in the ACM example of web-based analytics, the linking of unstructured open-source data to existing structured data in work file attributes is thought to enhance the capacity of the analyst to predict some possible emergent threat.

The solution to the problem of how to calculate security risk with unstructured data is thought to be located precisely in the kind of combinatorial possibilities depicted in Keith Devlin's reading of the history of mathematics. In the context of the terabytes of unstructured data thought to be analysed by algorithm in the PRISM and TEMPORA programmes, the possible combinations of elements are precisely what are sought in the partitioning of the data. The value of a particular data point may remain uncertain, but the combinations open up all kinds of new possibilities for calculation. Where the content of the unstructured data is thought to be of variable quality, for instance, a Bayesian-type 'confidence score' or 'reliability index' is assigned. Thus, for example, where the categories *a*, *b*, *c*, *x* describe specific *types* of data (e.g. *a* could be a named individual on a European alerts index; *x* could be a thread on a social networking site), and the scale 1–4 denotes the degree of verifiability of the source, a data item for a Twitter feed may constitute an '*x*4' node. However, by correlating the *x*4 item with elements of *a*1 or *b*1 data, for example, the analyst's confidence score is modulated by the distance or proximity to other elements.

In other words, what might otherwise be considered poor data in terms of forming the basis for a policing or security decision are thought to be 'enhanced' or 'cleaned' by their grammatical proximity to other associated elements. And so, to formulate a security calculation that reads 'item *a* (a credit-card transaction), present with item *b* (a communications data association with a watchlisted individual) and the element *x* (a "text reveal" node on a social networking site) produces a conditional probability of this or that risk' is not to make a proposition about the intrinsic value or properties of the item. Rather, like the assertion that the earthquake scientists could have inferred from their data in correlation with other factors, it does not matter to the mathematical grammar of security what the number is. It can be empty of meaningful content, for, as Wittgenstein puts it, there is 'all kind of use for it as part of a calculus'.

The politics of the decision problem

The mathematical debates of the early 20th century were dominated by a question posed by the German mathematician David Hilbert – the *Entscheidungsproblem* or decision problem: Could provable mathematical propositions be distinguished from non-provable propositions by means of a series of mechanical procedures (See Hilbert and Ackermann, 1928)? Hilbert's theorem, that all mathematical solutions could be reached through a series of predetermined axioms, was fundamentally challenged by the Princeton IAS mathematicians of the 1930s. Austrian mathematician Kurt Gödel developed his incompleteness theorem with which he demonstrated that mathematics will always include undecidable propositions that can be neither definitively proved to be true nor proved to be false. Taking the idea one step further, Alan Turing's (1936) 'On Computable Numbers: With an Application to the *Entscheidungsproblem*' makes the groundbreaking argument that there is no definite method through which to distinguish computable from non-computable numbers in advance. The significance of Turing's contribution to the decision problem, for the purposes of this discussion, is that at the very moment that he makes possible theoretically the first form of programmable computer, he also signals something of the limit point of programming and computability. Taking his points step by step, in his 1936 paper Turing proposes that the 'Hilbert *Entscheidungsproblem* can have no solution' because 'there can be no general process for determining whether a given formula of the functional calculus is provable' (reprinted in Copeland, 2010: 84). It is important to appreciate that undecidability, in Turing's terms, is not the same thing as solvability. A given mathematical problem may indeed be solvable by 'a direct appeal to intuition' (1936: 242) that reaches its way toward a solution, but it is not decidable in advance whether or not there are procedures, rules that can be followed mechanically in order to solve the puzzle. In short, a mathematical problem may be solvable but not computable.

Twenty years later, and with the benefit of having worked on the actualization of programmable computers, Turing (1954: 7) explains the distinction between finding a solution and establishing a decision procedure:

> If one is given a puzzle to solve one will usually, it if proves to be difficult, ask the owner whether it can be done. Such a question should have a quite definite answer, yes or no…. One might equally ask, 'How can one tell whether a puzzle is solvable?', but this cannot be assumed so straightforwardly. The fact of the matter is that there is *no* systematic method of testing puzzles to see whether they are solvable or not…. It has been proved that no such test ever can be found.

When Turing speaks of 'unsolvable problems', then, he does not imply that no solution to the mathematical puzzle can be found, but rather that no decision procedure can be established. For this reason, Turing prefers to speak of 'unsolvable decision problems' rather than unsolvable problems. What Turing proposes is that mathematical problems can never be resolved by what he calls 'ingenuity' alone – there are problems for which no effective decision procedure or protocol can be arrived at. In short, there are limits to the capacity to establish a decision procedure (what we would now call an algorithm). Turing (1954: 23) considers there to be 'certain bounds to what we can hope to achieve purely by reasoning', signalling anew the importance of intuition to mathematics. Intuitively one may arrive at a solution to a puzzle, but still the puzzle may defy the formal writing of a decision procedure or algorithm that would make the solution replicable. 'Within mathematics itself', Turing (1954: 23) reminds us, there is an 'inadequacy of reason unsupported by common sense'. Of course, the common sense Turing describes is also a form of reason, but what is significant here is that (a) there are mathematical problems for which a decision procedure cannot be known in advance, and (b) there are mathematical problems that, while intuitively solvable, are not computable by the formal procedures of algorithm or rule.

What do Turing's insights illuminate in terms of a mathematical turn in contemporary security calculation that precisely seeks to know in advance, to establish a decision procedure that can be automated, and to render imagination itself amenable to routinized procedures? Though the contemporary turn to the mathematics of data mining and analytics in one sense mobilizes Turing's vision of the digital universal computing machine, in another significant aspect it breaks with Turing's crucial distinction between decidable and undecidable problems. In contemporary security calculations, everything is rendered amenable to the formulation of a decision procedure – border-security algorithms that know a risky subject in advance; intelligence visualizations that attribute weight to some associations over others; automated gates in urban transport systems that know when to open and close. The procedures and rules are written as algorithmic code, in such a way that two things are forgotten: first, that these are problems for which it is possible that no definitive decision procedure can be arrived at; and second, that the ingenuity of the algorithm was written in large part intuitively. Indeed, where the impossibility of a decision procedure is confronted (there being insufficient or inadequate data on terrorism events, for example), the solution is found via the incorporation of the residue of a past event into the decision procedure. Thus, for instance, the contingent fragment of a past singular event – two flight tickets bought on one credit card but not seated together (9/11); student visas that fail to correlate to higher education records (Manchester bomb plot); specific travel to, and duration of stay in, Pakistan (2006 transatlantic airliner liquid bomb plot) – becomes perennially lodged in the algorithms designed for future security risk. This is despite the fallibility of algorithm-based security systems in place before 9/11, whose manifest failings were detailed in the 9/11 Commission's findings.[11]

Contemporary security systems have mobilized the techniques and routines of mathematical combinatorial possibilities – Turing's 'ingenuity' – but they have done so indifferent to the implications of the combination of intuition and ingenuity that underlies these very techniques. Consider, for example, the 2012 report of the US Senate Permanent Subcommittee on Investigations, detailing the devastating failings of the more than 70 fusion centres established to mine, share and analyse so-called terrorism-related information. The data analytics-driven fusion centres have been consistently represented as 'the spearhead of counter-terrorism' and 'the highlights of progress' in implementing 'more imaginative approaches to intelligence' (Department of Homeland Security, 2011: 14). As the Secretary of the Department of Homeland Security Janet Napolitano (2012) testified before the US House of Representatives Subcommittee on Homeland Security Appropriations in 2012, the 2013 budget 'focuses on the enhancement of data fusion centers, intelligence analysis, and information sharing' and 'continues to build analytic capabilities through the national network of fusion centres'.

Yet, despite the manifest faith placed in data analysis, the 2012 Senate Permanent Subcommittee's detailed investigation of the fusion centres found that 'Department of Homeland Security fusion centers forwarded "intelligence" of uneven quality – oftentimes shoddy, rarely timely, irrelevant, useless, and more often than not unrelated to terrorism' (US Senate Permanent Subcommittee on Investigations, 2012: 1). During two years of investigations, the Subcommittee was unable to identify any data-led alerts that pertained to a terrorist threat. The conclusions of the report echo those of European studies of the use of data analytics for counter-terrorism – that the use of mirror databases, attribute-based link analysis algorithms and so on produces reports 'not about terrorists or possible terrorist plots, but about criminal activity, largely pertaining to drugs, cash or human smuggling' (US Senate Permanent Subcommittee on Investigations, 2012: 3; see also De Goede, 2012; Wesseling et al., 2012; Amoore, 2013). Among the interview findings of the US subcommittee team, the fusion-centre data were reported by Department of

Homeland Security (DHS) analysts to be 'predominantly useless information' and a 'bunch of crap coming through'. However, because what has come to count as calculation in the fusion centres is overwhelmingly the capacity to establish an arrangement of propositions, a calculus of routines and subroutines that can be followed and replicated, the critical findings of the Subcommittee fall some way short of gaining purchase on the political problem. The content of the data items themselves ceases to matter – there is, recalling Wittgenstein, 'all kind of use for it as part of a calculus'. In terms of the effects in the world, such is the dominance of the drive to calculate the incalculable that calculability itself is never in question.[12] Where I understand the incalculable to be that for which there can be no decision procedure established in advance, the drive to calculate renders all potential futures knowable and resolvable (Amoore, 2013).

The critique of contemporary security calculation that targets the inadequacy or paucity of data, then, is unable to find political purchase because what counts is not the *accuracy* of the number, but rather the *precision* of the decision procedure itself. As the historian of science Lorraine Daston (1995: 9) has argued so compellingly, the mathematics of probability reveals not strictly a desire for ever greater degrees of accuracy and objectivity, but in fact a quite distinct emphasis on precision, on the 'intelligibility of concepts' that 'by itself stipulates nothing about whether and how these concepts match the world'. For Daston, the history of the mathematical sciences is characterized by a desire to share an intelligible language, to always know 'what is meant by 2' even if one considers the number itself to be inaccurate or not to match the world. Citing Leibniz's claim that 'lack of clarity is at the root of most controversy', Daston suggests that 'attempts to silence dissent' rely less upon an idea of scientific objectivity than on a consensus achieved through precise grammar. 'Even when the truth of the matter was not to be had', writes Daston (1995: 9–10), 'numbers could be invented, dispersed to correspondents at home and abroad, and, above all, mentally shared. You and I may disagree about the accuracy of a set of numbers, but we understand the same thing by them'. Bringing Daston into our speculative conversation with Turing, then, mathematics has prized the ingenuity of the rule or algorithm because it affords a precision, an intelligibility of concepts that is shared as a procedure across borders.

In the light of Daston's insights, it is of little consequence whether or how the mathematical models that grind out security alerts and reports have any sense of a match to the world. What is of consequence is the capacity to arrange propositions, to establish an algorithmic decision procedure through which *any form* of data can be processed. Turing tells us that there are some mathematical problems for which no effective decision procedure can be reached, and we cannot know in advance which problems these will be. In today's security practice, and in spite of its reliance on a *mathematics for homeland security* that combines the faculties of ingenuity and intuition, there is present a ubiquitous decision procedure that claims always to know in advance. Calculation and intuition are enfolded together in ways that are disavowed by a system of *analytics* that can never be in any sense *analysis*, can never ask a question that is not already present in the decision procedure itself, can never open itself onto an incalculable future.

Conclusions: For calculability is never in question

The defence case of the L'Aquila earthquake scientists dramatizes a particular claim about the incalculability of the future, a claim made on the basis of accuracy – 'on the basis of this data we cannot know the future and we cannot predict'. It is a claim that runs against the grain of what I propose is the logic of contemporary security: calculability is never in question, a precise arrangement of combinatorial possibilities can always be arrived at in advance. The assumption here is that, in effect, there can be no incalculable that cannot be acted upon. Thus, there can be no insecurity – everything is securable.

Yet, as contemporary security practices deploy mathematics to calculate the incalculable, this is not, as has commonly been argued, because the conventions of science and objective data analysis have given way to the inculcation of imagination and inference in intelligence gathering. On the contrary, contemporary security does not displace calculative rationalities with inferential speculation, but deploys a mathematical science that already enfolded the intuitive and inferential in its very objectivity (Daston and Galison, 2007: 357). A turn to the debates of 20th-century mathematics reminds us of the grammatical arrangement of combinatorial possibilities that is the very basis of inference rules. In short, the form of mathematical rationality was always already intuitive and always already political. Because the arrangement of combinatorial possibilities that is the contemporary algorithm establishes the associative conditions also of what is politically possible – what is sayable, what claims can be made – the appeal to objective or neutral machinic decision is superficial. Beneath the visible surface of the techno-scientific fix of analytics software surges a vast array of connectives and associations of machine reading and human decision. The grammar of contemporary security calculations effaces the aporia, the difficulty and fallibility of arriving at a judgement. And so, the problem is not science as such, for the mathematical science so publicly debated by Turing and Wittgenstein in the 1930s shows itself to be political, one possibility among a number of possibilities, open to its own fallibility. The problem instead is the erasure of that fallibility in such a way that the public space for critique and dissent is closed out. We find ourselves in a world where, as in L'Aquila, we will call to account those who confront the incalculability and say it is undecidable in advance; we will say that they failed to secure us. But we will also silence the critique of the calculus, the claims of those who wish to make a political claim from a place not registered within the grammar.

Acknowledgements

In memory of Dr Alan Thomas – an inspirational mathematician greatly missed. This article was presented as a keynote lecture at the 'Anticipate and Pre-empt' workshop, University of Amsterdam, March 2013. My thanks to Marieke de Goede, Marijn Hoijtink, Rens van Munster, Veronique Pin-Fat, Ben Anderson, Volha Piotukh and tectonic geomorphology scientist Alex Densmore. The three reviewers for *Security Dialogue* have been extraordinarily helpful, thank you.

Funding

The research from which this article is drawn received funding from the RCUK Global Uncertainties Fellowship 'Securing Against Future Events', ES/K000276/1.

Notes

1. One of the convicted scientists, Dr Giulio Selvaggi (2013), has argued that the scientific community had consistently warned the Italian public authorities of L'Aquila's high seismicity since at least 1985. He suggests that the governmental emphasis on close to 'real-time' risk assessment has distracted attention from the long-term lack of investment in buildings and infrastructure.
2. Beyond the 9/11 Commission report, there are further 21st-century instances when the calling to account for security decisions has had recourse to the association or correlation of elements. The UK Intelligence and Security Committee's report on the London bombings raises questions of possible 'missed opportunities' to associate before the event Mohammed Siddique Khan and Shazad Tanweer when they 'crossed the paths' of Operation Crevice, and to correlate their points of contact in crimes 'unrelated to national security' (UK Intelligence and Security Committee, 2009: 20; see also De Goede, 2012). By contrast with the L'Aquila case, though, in the national security domain to date there have not been juridical convictions for the failure to imagine possibilities.
3. Alan Turing's engagements with Ludwig Wittgenstein should be read in the context of a vibrant and open dialogue between the pure mathematicians and the philosophers. During Turing's fellowship at

Princeton, he would send his paper reprints to his mother with an accompanying list of the scholars who should receive a copy – Wittgenstein and Bertrand Russell were recipients (Copeland, 2010: 130).

4. In juxtaposing the Turing–Wittgenstein debates on mathematics and the statistical probabilities of earthquakes or terrorism, I do not suggest that these are equivalent. Instead, the juxtaposition draws attention to the co-presence of inference, intuition and calculation in each example. Following Lorraine Daston's (1986: 125) account of the histories of probabilistic reasoning, I am interested in precisely how inference and calculation become fused together in particular ways. Daston reminds us that 19th-century statistical approaches to probability are pre-dated by classical probabilities that incorporated the mathematics of chance, experience and belief. Indeed, she has also argued that conditional calculations 'much in vogue' in the late 20th century 'harken back to the reasonable calculus of the eighteenth century' (Gigerenzer et al., 1989: 264). Thus, it would be a mistake to abstract debates on the capacity to calculate with statistical probabilities from the theory of pure mathematics – they have conjoined histories. As Theodore Porter (1986: 93) has written, 'early probability mathematics first arose in the context of games of chance'.
5. In a letter sent home to his mother Sara, Alan Turing reflects upon the possible applications of his work, and the question of the ethical relationship between mathematics and security: 'I have just discovered a possible application of the kind of thing I am working on at present. It … enables one to construct a lot of particular and interesting codes. I expect I could sell them to HM Government for quite a substantial sum, but am rather doubtful about the morality of such things' (14 October 1936, Turing Papers, King's College, Cambridge). In a sense, the dilemma confronted by Turing in relation to war work involved precisely the ethics of establishing proofs or routines so that a set of mathematical principles could be used by public officials and decisionmakers.
6. Turing's (1936) paper 'On Computable Numbers, with an Application to the *Entscheidungsproblem*' represents the grounding theoretical work for the modern digital computer. As Jack Copeland (2010: 6) has captured the contribution of this paper, 'in this one article, Turing ushered in both the modern computer and the mathematical study of the uncomputable'. A Turing machine comprises a scanner and an infinite tape (memory) that moves left or right beneath the scanner head. Reading one square at a time, the scanner may read a 0, 1 or a blank square. The scanner's actions are determined by a program of instructions – or algorithms – that instruct it what to do, dependent on the square that is read and the combinations of past readings. So, for example, the program could instruct the scanner 'if in state a and the square scanned is blank, then print 0 on the scanned square, move the scanner one square to the right, and change to state b' (Copeland, 2010: 8). The Turing machines were abstract mathematical concepts designed to demonstrate the problem of what is and is not computable. Of course, Turing's early work on computing machines was based on a human 'computer'. As Ludwig Wittgenstein (1980: 61) commented, 'Turing's "machines": these machines are humans who calculate'.
7. In his work 'On Computable Numbers', Turing (1936) stipulates that, for the purposes of the logic of the paper, he is addressing only automatic machines capable of fully following the steps of the program. He comments that there are other 'axiomatic' processes where 'choice machines' might be used – where 'the machine cannot go on until some arbitrary choice has been made by an external operator'. It is useful to think of the contemporary use of security algorithms as involving multiple arbitrary choices by external operators, from the writers of the code, to the analysts who analyse and action the data.
8. Perhaps the best-known everyday use of an attribute-based link analysis algorithm is Google's PageRank system.
9. It is important not to overplay the confrontational aspect of Turing and Wittgenstein's relationship. The Turing papers show that when Alan Turing had received the offprints of his 'On Computable Numbers', he compiled a list of scholars to whom his mother was instructed to forward copies – Wittgenstein and Bertrand Russell were among those on the list (Dyson, 2012). The significance of the 1930s discussions is perhaps that the philosophical question of what number is, of how it acts in the world, was engaged across mathematics and philosophy. As N. Katherine Hayles (2005: 18) has suggested, in the 21st century, the philosophical debate on what kind of thought is possible in computation has tended to become obscured.
10. According to Europol (2009: 26), 'terrorist groups often communicate through public websites. These groups will issue threats, claim credit for attacks or spread indoctrination material over the internet.

So-called terror manuals offer detailed instructions on how to organise attacks or build weapons and bombs. Europol may monitor those websites and analyse their information … the agency has added a Check the Web portal to its Analysis Work Files, where relevant information is gathered and processed in order to gain an overview of worldwide Islamist terrorist activity'.

11. The Computer-Assisted Passenger Pre-Screening (CAPPS) system in place at US airports from the 1990s was identified as having missed opportunities to stop the 9/11 hijackers. Though nine of the individuals were identified by the CAPPs algorithm for additional screening, at the time this applied only to additional checks of hold luggage. In the case of Mohammad Atta, the CAPPs did flag him for additional screening, but because he had no checked luggage there was no further intervention. CAPPS illustrates how past events become sedimented into the algorithm: since at the time terrorist events on airliners were thought always to pertain to explosives in checked luggage, if the correlation between passenger and luggage was not present there would be no action taken. Arguably, in the original CAPPS system the past event of the 1988 Lockerbie bombing of Pan Am flight 103 became lodged in subsequent security risk calculations that sought to correlate passenger to checked luggage. In CAPPs II and Secure Flight, the successor systems to CAPPs, the residue of the past event remains, but now of course it is the absence of checked luggage that becomes one element of value.
12. It has become possible for the US and UK data analytics systems to fail beyond all redemption, and yet for the establishment of new counter-terrorism analytics units to be accelerated. For example, the initial draft 2011 European Union Directive on Passenger Name Record data mandates the use of fusion-style passenger information units in every member-state (Commission of the European Community, 2011).

References

9/11 Commission (2004) *The 9/11 Commission Report: Final Report of the National Commission on the Terrorist Attacks upon the United States*. New York: WW Norton & Co.

Amoore L (2011) Data derivatives: On the emergence of a security risk calculus for our times. *Theory, Culture & Society* 28(6): 24–43.

Amoore L (2013) *The Politics of Possibility: Risk and Security Beyond Probability*. Durham, NC: Duke University Press.

Aradau C and Van Munster R (2011) *Politics of Catastrophe: Genealogies of the Unknown*. London: Routledge.

Association for Computing Machinery (ACM) (2004) *The Mathematical Sciences' Role in Homeland Security*. Proceedings of a Workshop. Washington, DC: National Research Council.

Bayes T (1763) An essay towards solving a problem in the doctrine of chances. *Philosophical Transactions of the Royal Society* 53: 370–418.

Berlinski D (2000) *The Advent of the Algorithm*. New York: Harcourt.

Commission of the European Community (2011) EU–US agreement on the transfer of Passenger Name Record (PNR) data. Available at: http://europa.eu/rapid/press-release_IP-11–1368_en.html (accessed 20 May 2014).

Copeland BJ (ed.) (2010) *The Essential Turing: The Ideas that Gave Birth to the Computer Age*. Oxford: Oxford University Press.

Daston L (1986) *Classical Probability in the Enlightenment*. Princeton, NJ: Princeton University Press.

Daston L (1995) The moral economy of science. *Osiris* 2: 2–24.

Daston L and Galison P (2007) *Objectivity*. New York: Zone Books.

De Goede M (2012) *Speculative Security: The Politics of Pursuing Terrorist Monies*. Minneapolis, MN: University of Minnesota Press.

Department of Homeland Security (2010) *DHS Risk Lexicon*. Washington, DC: Department of Homeland Security.

Department of Homeland Security (2011) *Implementing the 9/11 Commission Recommendations, Progress Report*. Washington, DC: Department of Homeland Security.

Devlin K (1994) *Mathematics: The Science of Patterns*. New York: Henry Holt & Co.

Devlin K (1997) *The Language of Mathematics: Making the Invisible Visible*. New York: Holt Paperbacks.

Devlin K (2000) *The Maths Gene*. London: Weidenfeld & Nicolson.

Dyson G (2012) *Turing's Cathedral: The Origins of the Digital Universe*. London: Penguin/Allen Lane.

Elder J, Milner G and Nisbet B (2012) *Practical Text Mining and Statistical Analysis for Non-structured Text Data Applications*. Oxford: Elsevier.

Europol (2009) Rules applicable to Europol work analysis files. Available at: https://www.europol.europa.eu/sites/default/files/rules_applicable_to_europol_analysis_files.pdf (accessed 20 May 2014).

Ewald F (2002) The return of Descartes' malicious demon: An outline of a philosophy of precaution. In: Baker T and Simon J (eds) *Embracing Risk: The Changing Culture of Insurance and Responsibility*. Chicago, IL: University of Chicago Press, pp. 273–301.

Gigerenzer G, Swijtink Z, Porter T, et al. (1989) *The Empire of Chance: How Probability Changed Science and Everyday Life*. Cambridge: Cambridge University Press.

Hayles NK (2005) *My Mother Was a Computer: Digital Subjects and Literary Texts*. Chicago, IL: University of Chicago Press.

Hayles NK (2012) *How We Think: Digital Media and Contemporary Technogenesis*. Chicago, IL: University of Chicago Press.

Hilbert D and Ackermann W (1928) *Grundzüge der Theoretischen Logik* [Principles of Theoretical Logic]. Berlin: Springer.

Kirby V (2011) *Quantum Anthropologies: Life at Large*. Durham, NC: Duke University Press.

Napolitano J (2012) Statement for the record, before the US House of Representatives Subcommittee on Homeland Security Appropriations. Washington, DC, 15 February.

Nature (2012) Shock and law. 490 (25 October): 7421.

Nosengo N (2012) Italian court find seismologists guilty of manslaughter. *Nature*, 22 October.

Ohlhorst F (2013) *Big Data Analytics*. Hoboken, NJ: Wiley.

Porter T (1986) *The Rise of Statistical Thinking 1820–1900*. Princeton, NJ: Princeton University Press.

Selvaggi G (2013) Injustice at L'Aquila: Scientists on trial. Presentation at Durham University, 25 October.

Shanker SG (1987) Wittgenstein versus Turing on the nature of Church's thesis. *Notre Dame Journal of Formal Logic* 28(4): 615–649.

Silver N (2012) *The Signal and the Noise: Why Most Predictions Fail but Some Don't*. New York: Penguin.

Turing A (1936) On computable numbers, with an application to the *Entscheidungsproblem*. *Proceedings of the London Mathematical Society* 42: 230–265.

Turing A (1947) The Automatic Computing Engine. Typescript of lecture in the Turing Archives. Available at: www.turingarchive.org/browse.php/B/1 (accessed 21 February 2014).

Turing A (1954) Solvable and unsolvable problems. *Science News* 31: 7–23.

UK Intelligence Security Committee (2009) *Could 7/7 Have Been Prevented? A Review of the Intelligence on the London Terrorist Attacks on July 7 2005*. London: HMSO.

US Congressional Research Service (2008) *Data Mining and Homeland Security: An Overview*. 27 August. Available at: https://opencrs.com/document/RL31798/ (accessed 20 May 2014).

US Senate Permanent Subcommittee on Investigations (2012) *Federal Support For, and Involvement In, State and Local Fusion Centres*. Washington, DC, 3 October 2012.

Wesseling M, De Goede M and Amoore L (2012) Data wars beyond surveillance: Opening the black box of Swift. *Journal of Cultural Economy* 5(1): 49–66.

Wittgenstein L (1975) *On Certainty*. Oxford: Blackwell.

Wittgenstein L (1976) *Wittgenstein's Lectures on the Foundations of Mathematics, Cambridge 1939*, ed. Diamond C. Chicago, IL: Chicago University Press.

Wittgenstein L (1980) *Remarks on the Philosophy of Psychology*, Vol. I. Oxford: Blackwell.

Louise Amoore is Professor of Political Geography at Durham University and ESRC Global Uncertainties Fellow (2012–2015). Her recent book *The Politics of Possibility: Risk and Security Beyond Probability* was published by Duke University Press in 2013. Her current research project, 'Securing Against Future Events' focuses on the use of advanced analytics to act upon future events.