Article

Society and Space

Environment and Planning D: Society and Space
2016, Vol. 34(1) 107–125

DOI: 10.1177/0263775815623537
epd.sagepub.com
SAGE

Keep adding. On kill lists, drone warfare and the politics of databases

Jutta Weber
Institut für Medienwissenschaften, Universität Paderborn, Germany

Abstract
Alongside drones and Special Forces, the 'disposition matrix' – a kill/capture list and database – is a key device in the US government's global 'war on terror', in which targeting individuals has become increasingly institutionalized. The majority of studies to date have focused on the human world of the military, insurgents and policy makers with a limited access to reliable knowledge. Using insights from technoscience and software studies, I seek here to develop a material-based perspective focusing on the neglected non-human world of software artefacts, which codify, standardize and sort our world. I will first present available knowledge about the 'disposition matrix' and the 'targeting methodology'. Second, I will elaborate on the materiality of databases and data mining algorithms, showing how their technorationality is built on recombination, which fosters the production of possible future targets for a data-driven killing apparatus, in which human and non-human decision-making processes are intimately intertwined. In the third part of my article, I will discuss how computational actors make the messy targeting process more opaque and less traceable – not at least because of their underlying technorationality with its open-ended search heuristics – which advances a possibilistic, preemptive culture of technosecurity.

Keywords
Database, data mining, kill list, post-Newtonian rationality, algorithm, drone warfare

> The magic of modern technoscience is a lot of hard work, smoke-filled rooms, and boring lists of numbers and settings. Tyranny or democracy, its import on our lives cannot be denied. (Bowker and Star, 2000: 50)

Corresponding author:
Jutta Weber, Institut für Medienwissenschaften, Universität Paderborn, Warburgerstr. 100, D-33098 Paderborn, Germany.
Email: jutta.weber@upb.de

The 'disposition matrix': Kill lists, databases and the production of targets

Since 9/11, the number of US kill and watch lists is constantly growing, and they are playing an ever more crucial role in the politics of targeted killing. This article explores the material agency and epistemological dimensions of the 'disposition matrix', the key database of diverse kill lists in the US 'war on terror'. Its aim is to understand how sociotechnical artefacts such as databases and algorithms are intertwined with human decision-making processes in the production of targets. Analysing the cultural logic of data-driven warfare, I want to make visible the non-human sociopolitical actors, which emerge from a post-Newtonian technorationality of recombination and (cor)relation which resources the unpredictable and advances a preemptive culture of technosecurity.

The 'disposition matrix', the US government's main kill list, was devised in 2010 by CIA director John Brennan (formerly Barack Obama's counterterrorism adviser) and merges the diverse kill lists maintained by the Pentagon, the Central Intelligence Agency (CIA) and the Joint Special Operations Command (JSOC). Some critics speculate that the 'disposition matrix' was introduced to regulate and thereby streamline the kill/capture process between the diverse organizations and to bypass the Joint Chiefs of Staff (Miller, 2012). But, it will become obvious that the 'harmonization' of these different kill lists is also a result of the dynamics of data analytics.

Most information about the 'disposition matrix' – as well as about other 'terrorist' kill or watch lists – is secret or classified. There are very few documents available, produced by government-friendly as well as by critical researchers, investigative journalists or NGOs, that provide a limited amount of information about the discourses and practices of the 'disposition matrix'. Its existence was publicly disclosed in 2012 by a series of Washington Post articles based on pronouncements made by senior members of the Obama administration (Miller, 2012; de Young, 2012; Whitlock, 2012).[1]

Databases such as the 'disposition matrix' as well as other watch or kill lists are devices for profiling terrorists or suspects based on human intelligence (HUMINT) and, especially, on signals intelligence (SIGINT).[2] New data infrastructures and analytics (Kitchin, 2014) are playing a crucial and increasing role in the politics of intelligence production and targeted killing in contemporary US warfare (Belcher, 2014; González, 2015). Geographers Ian Shaw and Majed Akhter circumscribe the function of the 'disposition matrix' in the following way:

> Electronic Targeting Folders' store information on terror suspects from around the planet. These documents exist in a database referred to as 'disposition matrix', which forms the bureaucratic knife-edge of the Barack Obama administration's program of targeted killings. The 'disposition matrix' contains the names of 'dangerous individuals' listed against the resources marshalled to kill or capture them, either by drones or Special Forces. The institutional tool harmonizes the kill lists that exist across the US Central Intelligence Agency (CIA) and the Department of Defense, *thereby centralizing the management of life and death in the White House*. (Shaw and Akhter, 2014: 211; my emphasis)

The targets of the 'disposition matrix' are killed in drone attacks or night raids. As far as is generally known, most targeted killings by drones have been undertaken by the Pentagon in Afghanistan, Iraq and Libya. Outside conventional war theatres, drones are used by the CIA and JSOC in countries such as Pakistan, Yemen, Somalia and Syria. Thousands of night raids have been conducted primarily by JSOC in Iraq and Afghanistan (Gregory, 2013; Woods, 2015).

Perhaps the most detailed description of how the 'disposition matrix' is compiled has been given by law professor Gregory S. McNeal (2014) in his case study 'Targeted Killing and Accountability'. It is a highly informative but equally problematic study insofar as it embraces the often quite unspecific definition of 'terrorist' and other, related terms used by the US government. It is not only based on military policy documents, governmental answers to Freedom of Information Act (FOIA) requests, court documents, press reports and academic work – but also on participant observation of the official training of and 'confidential interviews with members of the military, special operations, and intelligence community involved in the targeted killing process' (McNeal, 2014: 681).

Targeting 'methodology': How to define and select a 'terrorist'

According to McNeal, the nomination of a target for the 'disposition matrix' includes four steps: identification, vetting, validation and nomination – the latter often with presidential approval. On so-called 'Terror Tuesday', US President Obama confers with his security experts about which individuals are those against whom strikes are to be personally authorized:

> Every week or so, more than 100 members of the government's sprawling national security apparatus gather, by secure video teleconference, to pore over terrorist suspects' biographies and recommend to the president who should be the next to die. This secret 'nominations' process is an invention of the Obama administration, a grim debating society…. (Becker and Shane, 2012)

Recently, the investigative journalism platform 'The Intercept' reported, on the basis of leaked material, that intelligence analysts produce a short description of the suspect and the threat s/he poses in the form of a 'baseball card', which – together with operational information – is then '"staffed up to higher echelons" for action. On average, it took 58 days for the president to sign off on a target' (Scahill, 2015).

This process of approval is not entirely new: it was invented by US President Lyndon B. Johnson, who personally selected targets during parts of the Vietnam War (Humphreys, 1984; Gregory, 2012) – though these targets were not primarily human beings, as with Obama's list, but objects.

Nowadays, however, the 'disposition matrix' is a crucial component of computational counterinsurgency and, as such, is part of the 'distanced, computer-centric approach of RMA [Revolution in Military Affairs; JW]' (Belcher, 2014: 51). It is a flexible database based on structured and unstructured data and on small as well as big data that can be searched systematically using advanced data mining algorithms. It is a unique and key device in the 'global war on terror'. Its technorationality draws upon a logic of tinkering that data mines the unknown, exploring all manner of (often highly unlikely) possibilities. Huge amounts of data are searched and clustered to *produce* patterns of correlations between data and thus to 'discover knowledge in databases' (Hildebrandt and Gutwirth, 2008, Kitchin, 2014). The discovery approach does not rest on the idea of correlations based on causal relationships but assumes that a (possible) past correlation will appear again at some point in the future.

> With smart applications, however, the target is to collect and aggregate as much data as possible, in order to mine them for relevant patterns that allow the profiler to anticipate future behaviours. The hiding of data in fact diminishes the 'intelligence' of the applications. (Gutwirth and Hildebrandt, 2010: 7)

The bigger the data collection, the more possibilities there are to produce 'knowledge' (interesting combinations/patterns) through recombination. Thus, it is not only policy but also the inner logic of data analytics that drives the centralization of various watch and kill lists.

Definitions

In the last few decades, military and intelligence services in the United States have collected information on suspected insurgents – so-called terrorists – in diverse databases for the purpose of including them on watch and kill lists and for the purpose of filtering out specific features and behavioural patterns linked to 'terrorism' by means of data mining. This is clearly a delicate and highly selective task, not least given the fact that there is no clear international or legally binding definition of terrorism and that the definitions used by US government institutions vary quite widely (Schmid, 2011).

Given the secrecy surrounding the procedure, the relevant question is: Who counts as a terrorist, and why? And, consequently, what kind of data are to be collected? How does somebody come to be listed in databases such as the Terrorist Identities Datamart Environment (TIDE) – the biggest list of known and suspected terrorists, which gathers sensitive military and civil intelligence including classified information managed by the National Counterterrorism Center (NCTC) – or the Terrorist Screening Database (TSD), managed by the FBI, in which between 680,000 (Scahill and Devereaux, 2014b) and 875,000 people (de Goede, 2013) are registered? The TSD database is

> a watchlist of 'known or suspected terrorists' that is shared with local law enforcement agencies, private contractors, and foreign governments—*more than 40 percent of the persons on the watchlist are described by the government as having 'no recognized terrorist group affiliation'*. (Scahill and Devereaux, 2014b; my emphasis)

Since 2010, the 'disposition matrix' has been compiled using these and other databases. It is unclear exactly how the information in these databases has been collected and what specific targeting methodologies and algorithms are used.[3]

McNeal (2014) states that for the Obama government, a sufficient condition for being listed on any kill list is to be a member of an 'organized armed group'. But what counts as an organized armed group? The definition could easily fit a US American family, in which all adults possess a firearm. Or again, it might describe a group of tribal elders in Waziristan who traditionally carry weapons as a sign of their status. Sometimes, even non-members of such 'groups' are added to the list if they are regarded as being important for the group – again, there are no strict criteria for cases when non-members might be added.

In July 2014, a 'Watchlisting Guidance' document (NCTC, 2014) – issued in March 2013 by the NCTC – was leaked to 'The Intercept'. It contains guidelines for placing individuals on the TSDC or TIDE database and thereby reveals just how vague the selection criteria are – this at least partially explains the high number of selectees on the watch and kill lists. The document describes as 'terrorist' activity not only actions such as hostage taking, assassination or bombing but also 'destruction of government property and damaging computers used by financial institutions.... They also define as *terrorism any act that is 'dangerous' to property and intended to influence government policy through intimidation*' (Scahill and Devereaux, 2014a; my emphasis). This vagueness in defining 'terrorist suspects' and 'terrorists' facilitates the inclusion of highly diverse data in the terrorist databases. Increasingly, they contain data on non-violent political activists and individuals who challenge the dominant political order in general. In this context, military

researchers have recently begun to mine social media intelligence (SOCMINT), from Twitter to Facebook, in the hope of 'connecting the dots'. The effects of this, however, are highly problematic. In the fear of failing to spot potential suspects, the search criteria are constructed very broadly; accordingly, more and more data are included in watch and kill lists, while detection algorithms are defined very broadly to pick up on any possible correlations and patterns. The number of false positives is increased rapidly:

> To reduce both those numbers (of false negatives and positives), you need *a well-defined profile*. And that's a problem when it comes to terrorism. In hindsight, it was really easy to connect the 9/11 dots and point to the warning signs, but it's much harder before the fact. Certainly, there are common warning signs that many terrorist plots share, but each is unique, as well. The better you can define what you're looking for, the better your results will be. Data mining for terrorist plots is going to be sloppy, and it's going to be hard to find anything useful. (Schneier, 2006; my emphasis)

Meta-data, social network analysis (SNA) and Skynet

Intelligence uses a variety of data mining tools and approaches such as social network, link, video[4] and content or sentiment analysis to select and track targets on the basis of HUMINT and SIGINT (Joint Warfighting Center, 2011; Ressler, 2006; Sageman, 2004; ICWatch, 2015). In countries such as Pakistan, Yemen and Syria, which have few US armed forces on the ground, most of the intelligence gathered is based on SIGINT. SIGINT from video feeds, mobile phones, geo-locational information as well as data from email, social media and other internet services are used for data analysis – often based on quantitative link analysis methodology. This means that the more often somebody contacts a suspect, the more suspicious the person becomes – even though s/he might be a cousin or a friend who is not part of any so-called terrorist network. It works on the basis of a two (or three) -hop query through data collections often provided by security agencies such as the CIA or the National Security Agency (NSA) to find connections to other suspected 'terrorists' or members of 'terrorist' organizations.[5]

Meanwhile, SNA had

> provided a framework for construction of models of networks by measuring the number of direct interactions between individuals, or 'nodes'. With a quantitative tool called 'link analysis' and accompanying software, intelligence analysts could see the raw data from drone surveillance and links among telephones transformed into a 'map' of the insurgent 'network' in each locality. (Porter, 2011)

Organized armed 'terrorist' groups are frequently interpreted as social networks (Sageman, 2004; Ressler, 2006). The importance of a member of an assumed terrorist organization is weighed according to the outcome of the SNA in a kind of cost–benefit analysis: Steve Ressler from the Department of Homeland Security stresses that such an analysis focuses 'on the value of the network structure rather than the characteristics of the individual' (Ressler, 2006: 2), because these 'terrorist' organizations are interpreted as non-hierarchically organized networks with often only loosely connected individuals. Therefore, not only Taliban and al-Qaida leaders are regarded as a possible targets but also indeed, in principle, anybody who is in loose contact with members of the network. This description of a 'terrorist' network corresponds quite well to SNA approaches, which map and visualize huge amounts of metadata and fuse them into quasi-naturalized sociograms.[6] The 'Commander's Handbook for Attack of the Network' (2012) by the

former US Joint Warfighting Center describes the methodology and actions needed to exploit 'terrorist network vulnerabilities' quite bluntly: 'SNA helps to identify which nodes in the network can be killed, captured or influenced to achieve desired effects' (2011, IV-3). While it takes ('terrorist') networks (as identified by SNA) for granted, at the same time, it issues a serious warning concerning the shortcomings of the data mining approach:

> ... there is a significant caveat when using SNA – the link analysis is unique to the analyst developing the picture of the network. Additionally in developing a link analysis it is critical to ensure that there is an understanding of how or why a link was made between two nodes. (Joint Warfighting Center, 2011, IV-3; my emphasis)

SNA focuses on mapping relationships between people, places and things to develop a so-called 'pattern of life' analysis, which carves out the 'process-based relationship between key nodes' (Shaw, 2013). It is not only senior leaders of a 'terrorist' group who are regarded as valid objects for targeted assassination but also anybody who is identified (by an algorithm or an analyst) as being vital to the group – according to their strategic position in the network. This is why it is important to understand 'how or why a link was made': otherwise, this logic would rapidly lead to a multiplicity of targets. And yet exactly how these links are established and what the specific criteria are is often not obvious to military end-users, many of whom are not trained as software developers.[7] The 'how' or 'why' of the link becomes even less clear in the case of data mining software such as Analyst's Notebook, which includes 'intuitive' human-machine interfaces that make the work of inbuilt categories and representations invisible (Bowker and Star, 2000; Dourish, 2001; Suchman, 1994). One example of inbuilt criteria is SNA's assumption that insurgent groups *are* networks, in which the centrality of an actor is determined by the quantity of his or her contacts with other suspects. Stohl and Stohl have pointed out that SNA cannot effectively distinguish the ability to network by means of communication and connectivity from 'the ability to mobilize, control and coordinate members for specific planned acts' (2007: 110). The relevant categories for the 'pattern of life' analysis rest on problematic assumptions, such as that travelling certain routes frequently, visiting suspicious locations or contacting suspects is undoubtedly the signature of a 'terrorist'. Jeremy Scahill and Glenn Greenwald point to the fact that not only the identification of targets, but also the identification of their physical locations and the attacks themselves are based on meta-data analysis:

> ... the NSA, ... often identifies targets based on controversial metadata analysis and cell-phone tracking technologies. Rather than confirming a target's identity with operatives or informants on the ground, the CIA or the US military then orders a strike based on the activity and location of the mobile phone a person is believed to be using. (Scahill and Greenwald, 2014)[8]

Retired US general and former NSA and CIA director Michael Hayden bluntly admitted that 'We kill people based on metadata' (Cole, 2013).

One effect of the logic of this targeting methodology can be studied paradigmatically in the document 'Skynet. Courier Detection via Machine Learning' (NSA, 2012) leaked by Edward Snowden. According to the NSA document, the renowned Al Jazeera journalist Ahmad Muaffaq Zaidan was placed on a watch list because of his travel patterns, phone call logs and the sources he was using. He is cited

> as an example to demonstrate the powers of SKYNET, a program that analyses location and communication data (or 'metadata') from bulk call records in order to detect suspicious patterns. [...] According to the presentation, the NSA uses its version of SKYNET to identify

> people that it believes move like couriers used by Al Qaeda's senior leadership. The program assessed Zaidan as a likely match. (Currier et al., 2015)

Ahmad Muaffaq Zaidan was obviously listed because of his professional work as a journalist working on the al-Qaida and Taliban movement thereby meeting insurgents including Osama Bin Laden. Any analyst who has a profound knowledge of the language, policy and socio-cultural context of Pakistan would have realized that the contacts of the journalist result from his professional work and do not necessarily indicate any insurgent activity. When the targeting process is automated – particularly at a time when competent analysts are few and far between[9] – it makes the targeting increasingly non-reproducible while nevertheless producing ever more suspects and including them on watch and kill lists.

In general, the 'disposition matrix' can be understood as a constantly evolving database, which includes not only biographies but also conclusions drawn from data analysis, primarily on the basis of metadata. Overall, the 'pattern of life' analysis resembles law enforcement strategies of collecting data on criminal behaviour. And though the 'disposition matrix' partly builds on narratives of 'terrorist' biographies (e.g. de Goede, 2013; Kessler and Wouter, 2013), it is also a searching device in which big datasets are placed in relation to one another and recombined – establishing profiles of the supposedly most dangerous suspects.

Obviously, people are killed not because they are identified as high-ranking members of a specific 'terrorist' network, but because they show specific behaviours or link patterns, which are regarded by analysts or software designers as suspect or which 'emerge' from the data analysis. The analysis seeks to detect 'persistent anomalies in normal rhythms of activity, which are read as signs (''signatures'') of imminent threat... The principal limitation – and *the grave danger – lies in mistaking form for substance*' (Gregory, 2013; my emphasis). The quantitative methodology cannot make qualitative distinctions between relationships of different 'nodes', which are easily subsumed into terror networks. Accordingly, relatives, friends and co-workers who have multiple connections to suspects or targets are added to the list.

The historian and journalist Gareth Porter also points out that many people living in the Southern or Eastern Pashtun area have a few mobile numbers of Taliban commanders in their mobile as a 'survival mechanism' – and the same might be true for people living in Waziristan. And although the targets included in the 'disposition matrix' are identified persons, the indicators which made them high-value targets are often derived from a targeting method which rests on predefined categories, does not establish causal relationships and describes only formally patterns of relations on the basis of meta-data. On the basis of methodologies such as SNA, geospatial or sentiment analysis, analysts produce target lists and the knowledge about 'how and why a link was made' will necessarily get lost during this multi-layered process of merging and filtering huge amounts of metadata.

None of these problems can be resolved by having more accurate definitions of terrorism or by honing the criteria used to add someone to the list or by perfecting algorithms – because the process of mistaking form for substance is occurring in a very literal way and is an integral part of the procedure: there seems to be no narrative based on cause and effect trajectories to explain why somebody is considered a 'terrorist' who poses an imminent threat. There is no transparent or consistent line of argument, which would justify the criteria and render them coherent. There is no (open) claim to produce truth or at least some meaning in this process. The pattern of life approach draws on a technoscientific logic of recombination, (cor)relation and possibilities – and this logic rests on very weak

probabilities and is highly constructed. At the same time, this approach spurs on the desire (or the perceived need) to collect more and more data: the larger the amount of data stored in the database and the higher the numbers of possible combinations this yields (of nodes of networks, for example), the more high-value targets can be 'identified'. And it is not only 'hundreds of people [who] make incremental contributions to a well-oiled killing machine' (McNeal, 2014: 685) but also the inner logic of databases and big data analysis.

Based on this perspective, I will draw on insights from technoscience and software studies to render this inner logic more visible and to develop a more detailed, material-based understanding of these practices. This approach has its own limitations, because the specific programs used in the targeting process are secret and therefore not available for closer analysis. Nevertheless, I would argue that understanding the impact of the general principles of contemporary databases and data mining algorithms can decisively improve our understanding of the targeting process as the epistemological underpinning of the apparatus becomes visible.

The epistemology and materiality of databases

> Information systems are material objects, but so too is information as it is manifest within them. Its specific materialities shape the forms of processing that it allows. Any account of what information is, or what it does within social, cultural, or institutional settings must, then, be grounded in an examination of these material considerations. (Dourish, 2014: 1)

Technoscience and especially software studies have pointed out that software permeates every realm of contemporary life: '(M)ore and more of the spaces of everyday life come loaded up with software, lines of code, that are installing a new kind of automatically reproduced background and whose nature is only now starting to become clear' (Thrift and French, 2002: 309). This is especially true of contemporary warfare and military organizations. Accordingly, my aim here is to make the inner logic of the database as well as data mining and machine learning techniques visible by examining their epistemological and material basis – that on which analysts draw in order to search for and predict potential targets.

First, I will discuss the shift from the hierarchical to the relational as well as post-relational database, from the storage to the search device used to examine structured (small) data to the distributed system that can search semi- or unstructured (big) data in parallel.[10] I will then have a closer look at machine learning techniques – especially genetic algorithms.

Rethinking the 'disposition matrix' from this perspective, I want to show how mining techniques in combination with post-relational NoSQL databases build on automated processes of systematized tinkering and recombination and thus fuel the production and collection of data, suspects and targets.

What is a list and what is a database?

Lists are made to add, combine and, eventually, order items *without* relying on a pre-given order (Stäheli, 2012: 234–236). Any list is a tool of abstraction and often an answer to a problem. Furthermore, 'the criteria of selection are not fixed at the outset but evolve during the list's use' (Stäheli, 2012: 237). They are not inherent to the list. Its rules of inclusion or exclusion can be changed according to the circumstances.[12] Representational forms (such as a list or a database) and knowledge are intrinsically intertwined (Goody, 1977) and the

potential of abstraction in lists relies on discontinuity and decontextualization – in contrast to narratives which have a pre-given structure, for example.

Stäheli (2012) interprets the list as a kind of (simple) database. Databases are structured collections of data. They are theoretically indefinite. Lev Manovich pointed out that they have no beginning, end or development. They are not telling stories and they have no internal grammar. 'Instead, [. . .databases] are collections of individual items, where every item has the same significance as any other' (Manovich, 2001).

Databases are structured differently – in hierarchical, network-like or post-relational ways. It is important to differentiate between the traditional form of the list (or database) and a more recent cultural expression of the list, namely, the post-relational database.

Early databases were organized in a hierarchical way with a tree-like structure. For these traditional databases, the user needs to know how the database is structured and what data it contains. In this model, every data item contains a physical storage address, and the way information is retrieved depends on how the data are organized. These databases are less dynamic than relational ones, because they can only answer the kinds of questions the programmers were aware of when they designed them.

In the early 1970s, Codd (1970) and others developed relational database models and made it possible to separate storage and retrieval (Dourish, 2014; Kitchin, 2014). In such a database, data are not organized in a hierarchical, tree-like pattern that branches out from a root but rather in a table, so that each segment of data can be placed in multiple relationships to other items. Databases thus went from being a means of organization to becoming a means of querying. Relational databases are highly flexible, dynamic and open-ended systems. This became possible because of the shift from hierarchical to relational database management systems and the rapidly increased power of central processing units (CPUs). The relational database is indispensable for the real-time management of complex, dynamic and open systems:

> Relational databases enabled more efficient and sophisticated organization and querying of structured data (using SQL – structured query languages). Alongside relational databases, the development of spreadsheets allowed large volumes of numeric data to be structured and stored and for formulae to be applied to the data to produce new derived data. (Kitchin, 2014: 32)

This became the dominant database management system, turning the database from a storage and retrieval device into a search device (Amoore, 2013; Hildebrandt and Gutwirth, 2008).

The post-relational NoSQL (not only SQL) database emerged in the early years of the 21st century. It is capable of storing and querying enormous amounts of structured as well as semi- or unstructured data, as required for highly centralized web services such as Google, Facebook or Amazon – or the databases of the intelligence services (Kitchin, 2014: 86).

Post-relational databases are distributed on many servers, which are flexible and easily extendable big data systems 'holding the traits of extensionality (can add new fields easily) and scalability (can expand rapidly) regardless of volume. . . The use of NoSQL databases means that changeable data can be managed at high velocity, adapting to new fields' (Kitchin, 2014: 78). And while the traditional list is a perfect medium to (re-)combine and relate all kinds of data, NoSQL database design as well as smart knowledge discovery techniques make 'access to very large, exhaustive, dynamic, fine-grained, indexical, varied, relational, flexible and scalable data' (Kitchin, 2014: 79) possible. New database design, increased computational power and distributed infrastructures managed by techniques such as MapReduce (Kitchin, 2014: 86f) enable new forms of (big) data analysis.

Nowadays, it is not only new database structures that define the way data are related and combined but also data mining algorithms: 'Together, data structures and algorithms are two halves of the ontology of the world according to a computer' (Manovich, 2001: 198). As mentioned above, knowledge discovery techniques such as data or text mining, sentiment and SNA are used massively in the hope of extracting relevant patterns from the piles of military and civil intelligence.

A new technoscientific rationality

The shift in cultural expression from narrative to (post-relational) databases and the emergence of new, flexible algorithms can be seen as part of a profound reconfiguration of epistemology and ontology within a new epoch called 'technoscience' (Latour, 1986). Technoscience culture itself can be characterized by the observation that everyday life is thoroughly pervaded by discourses and practices of technosciences such as computer science, genetics or Artificial Intelligence. All these discourses and practices are in the process of reconfiguring culturally contested concepts such as 'nature', 'the body' and 'subjectivity'. The fusion of science and technology in technoscience has become an entrepreneurial and pragmatic project, in which technology assumes a lead role in the development of innovative solutions for most of the core problems of our societies. As I have argued elsewhere (Weber, 2003, 2011), the new technoscientific rationality is much more flexible and is characterized by a strong interest in the unpredictable, in processes of emergence, and in the unknown. This epistemological shift is also embedded in globalized media culture, in which

> [m]any new media objects do not tell stories. Instead, they are collections of individual items, [...] on which the user can perform various operations: view, navigate, search. *The user experience of such computerized collections is therefore quite distinct from reading a narrative*. (Manovich, 2001; my emphasis)

This new epistemological logic is rooted historically in systems theory and cybernetics, which provide the common ground for today's dominant technoscientific discourses and practices (Weber, 2003, 2011). Technosciences such as robotics, genetics and computer science are built on new epistemologies and ontologies, and on the new conceptual frameworks, identities and modes of governance which emerged in the second half of the 20th century (cf. Haraway, 1985/1991; Latour, 1986). The key features of technoscientific rationality include formalized and systematized tinkering as well as the use of trial and error, bottom-up search heuristics and post-processing for the solution of complex problems.

Adaptation, imitation and imagination are key to a rationality aimed at resourcing the unpredictable and to attempts to find ways of exploiting surplus processes by technical means (Haraway, 1985/1991; Nordmann, 2006; Weber, 2003). In contrast to modern scientific rationality, it is not interested in the analysis of intrinsic properties of entities (organisms, machines) but focuses instead on their behaviour, on their (inter)relations and on possible recombination of modules, fragments of code and building blocks of systems. Technoscience increasingly substitutes representation and understanding with investigation and intervention (Weber, 2003). This new post-Newtonian rationality has also imprinted itself deeply on processes of listing, data collection and search heuristics in the so-called 'global war on terror'. As Louise Amoore has recently pointed out, techniques such as 'risk profiling, algorithmic modelling, information integration, and data analytics [have] become the authoritative knowledges of our time' (Amoore, 2013: 9).

'How to solve problems you do not fully understand'

Kill lists as well as lists in general are flexible and dynamic because they are not based on clear selection criteria. Anything can be added to a list when the rules governing what qualifies as an item to be listed can be changed constantly. Kill lists such as the 'disposition matrix' are founded upon search procedures and devices designed to sift through tremendous amounts of data – from drone feeds to social media – and to scan this data universe in the hope of connecting 'the' dots. In this way, the hope is to find hidden threats or 'terrorists', while data are adjusted automatically, problem spaces of algorithms are searched for patterns, and chat room conversations are scanned for keywords. It is not a specific entity that is being searched for but patterns, irregularities and possibilities.

New forms of data mining algorithms that are ruled by a similar logic, such as genetic algorithms, emerged in the 1980s. While algorithms had previously been designed 'top-down' to solve a specific problem in a straightforwardly rational-cognitive way, genetic algorithms work in a 'bottom-up' way, usually by describing a problem and converging the solution towards said problem. Within this logic, the most effective way to find a solution is to give a sound description of the 'problem space', to define robust parameters and to then use processes of trial and error (referred to elsewhere in this article as systematic 'tinkering') to search this space. In both cases, it is not a clearly defined problem that is the object of the (re)search but rather a broadly defined target or problem along with a few boundary conditions within which the goal is to be achieved (to find the terrorist or to solve another problem). This approach departs significantly from the core norms of traditional science – such as the objective description of universal laws, the representation of nature, consistency, and the subject-object divide. This technorationality is based on systematized tinkering and on exploring the boundary conditions of emergent behaviour; it makes use of search heuristics, algorithms that simulate 'evolution' via tinkering, and techniques of post-processing. I seek to illustrate this more clearly in the following: In 1992, John Holland published an article entitled '*Genetic Algorithms. Computer Programs - that "evolve" in ways that resemble natural selection can solve complex problems even their creators do not fully understand*' (Holland, 1992). It seems that Holland was promising something one cannot reasonably promise: to develop a problem-solving strategy for problems which are not (yet?) understood. However, what sounds absurd initially might also be seen as the leitmotif of technoscientific rationality.

Holland developed so-called optimized, self-learning computer programs that were designed to solve certain tasks – such as finding the most effective algorithm for sorting different numbers according to their size. It works as follows: first, a fitness factor for the task is defined. Then, a computer randomly produces diverse algorithms, which are rated and selected according to the fitness factor that indicates their 'success'. A pre-defined percentage of the computer programmes that match the task best according to the fitness factor are reproduced, while all the other programmes are deleted. The successful algorithms are crossed over by swapping those parts of the programme's digital code that are located at the same position in the code. Then, the process is started over again. In effect, the procedure can be described as a smart, optimized and systematized process of trial and error, because it is conducted in iterative loops until an appropriate solution is found for the problem at hand. *And although millions of useless programmes are produced, new solutions arise with the help of genetic algorithms* (which are an underclass of evolutionary algorithms) on the basis of processing power and time. This bottom-up method can compete with and often produces better results than traditional programmes designed by software engineers in a top-down, rational-cognitive way.

These trans-classic ways of computing and, especially, of data-mining information are key to a technoscience culture in which the world is reconfigured as flexible, open-ended and unpredictable, while at the same time becoming a place of combination, recombination and re-design (Haraway, 1985/1991). Alongside other applications, genetic algorithms are central to contemporary methods of data mining. The database (or specified parts of the database) is defined as the search space, and genetic algorithms are used to search vast amounts of data for patterns, relations, associations and 'anomalies'. In this way, data can be classified (by applying known categories to new data) and clustered (by searching for as yet unknown groups or structures in the data), and patterns can be extracted. These can be used to predict, to test hypotheses and to optimize search strategies (for finding optimal association rules, for example). Randomly producing relations and recombinations is a key part of mining the 'disposition matrix' and fuels the desire for more data while producing more 'hits' (that is, suspects). The idea of systematically scanning a (pre-defined) space for a possible solution, of endlessly recombining data in the hope to 'identify' a possible threat or a possible suspect, looks familiar when we think of today's pre-emptive technosecurity measures. The huge amount of ever expanding data gathered by the NSA can be seen as part of this technorationality, which fuels the 'need' for ever more data.

In the next section, I will discuss the affinities between the new technorationality, with its open-ended search heuristics, and a postmodern preemptive technosecurity, which seeks to anticipate and avert all potential threats. I will point out how today's practices of imagination are rooted in Cold War security culture and will also highlight their key differences to contemporary technosecurity culture.

Preemptive culture of technosecurity

Features of the new technorationality can be found prominently in a culture of preemptive technosecurity, which focuses on anticipating 'unknown unknowns' (Daase and Kessler, 2007) – unknown risks posed by unknown actors – rather than concentrating on the empirical, causal assessment of objective and concrete threats posed by identifiable 'risk' actors (Aradau et al., 2008). Sophisticated surveillance applications such as data mining, computer simulations (Bogard, 2012), scenario-planning techniques and worst-case imagination (de Goede, 2008) are primarily directed towards uncertainty and unpredictable risks (Salter, 2008; Bröckling et al., 2011). This technorationality at work in the targeting process becomes obvious from the way targeted killings are justified by CIA director John Brennan:

> [W]e conduct targeted strikes because they are necessary to mitigate an actual ongoing threat... And what do we mean when we say significant threat?... A significant threat might be posed by an individual who is an operational leader of al-Qaida or one of its associated forces. Or perhaps the individual is himself an operative, in the midst of actually training for or planning to carry out attacks against US persons and interests. *Or perhaps the individual possesses unique operational skills that are being leveraged in a planned attack*. (Brennan, 2012; my emphasis)

Again, the criteria for a high-value target are more than vague: not only does being a senior al-Qaida leader make you eligible to be listed in the 'disposition matrix' but also planning an attack or even having certain skills that might be needed in a planned attack. This leaves ample room for interpretation: when do we know for sure that somebody is planning an attack? It seems that even possessing certain skills makes you a (possible) suspect and might justify your preemptive assassination. Evidently, '(t)he logic of preemption prioritizes the power of imagination over the power of fact – suspicions over evidence' (Salter, 2008: 243).

Potential threats come to be defined so broadly that in principle anybody can pose one in the near future,[13] while the analysis rests on indicators and observations of behaviour. This way of defining possible targets is contrary to the modern scientific understanding of cause and effect, but it fits very well to the tinkering logic of today's technorationality. Today, incremental and automated processes of recombining and interrelating data (provided largely via SIGINT) are the epistemological foundation for risk management – a procedure that is organized on the basis of predefined categories and is dominated by imagination in the sense of projecting (im)probable scenarios, connections and circumstances. Semi-automated technologies of predictive analysis and preemptive action, real-time tracking and targeting are regarded as appropriate ways to handle the challenge of unpredictable risks – an approach reminiscent of the desire to find a 'technological fix' and thus to achieve technological 'preparedness' or indeed superiority (cf. Der Derian, 2009; de Goede, 2008).

Yet the use of imagination in security practices is not entirely new. Worst-case scenarios and computer simulations that used techniques of imagination were already deployed during the Cold War when the unprecedented threat of nuclear war in the 1940s created an entirely new situation marked by insecurity. The latter could be addressed neither on the basis of previous experience nor by experimentation. In the 1960s famous 'defence intellectuals', such as US think tank RAND expert Hermann Kahn (1960) devised all manner of (in)conceivable scenarios resulting from a nuclear strike or counter strike that went *beyond the question of probability* (Ghamari-Tabrizi, 2005; Kaplan, 1983); such scenarios included the deaths of hundreds of millions of people, survival strategies for highly improbable scenarios and biopolitical measures for a post-nuclear (!) age. However, whereas in the Cold War security discourse, strategists were dealing with a *concrete* situation with *concrete* actors, today's security discourses are increasingly about possibilistic threats and their presumed actors.

Uncertainty has long been incorporated into calculations by way of statistics: '... algorithmic logics have already begun to define the management of uncertain futures of many kinds – from flood risk in the insurance industry to catastrophe risk in the financial markets' (Amoore, 2009: 52). What we are experiencing today, however, is 'a *change in emphasis from the statistical calculation of probability to the algorithmic arraying of possibilities* [...]' (Amoore, 2013: 23; my emphasis). It seems that these algorithms are increasingly dominating the discourses and practices of civil and military security agencies, substituting traditional probability with the 'imagination of possibilities' (Amoore, 2013: 24). Today – for fear of failing to spot potential singularities – data segments are recombined to put a defined problem space into a grid as completely as possible, even if 99% of the solutions, though technically possible, are unfeasible or highly unlikely. What used to be tested in worst-case scenarios is now perfected in a kind of systematized and formalized tinkering on the basis of data mining and huge, flexible, post-relational databases hoarding big data.

In the following, I want to highlight the impacts and consequences of this technorationality combined with the new culture of technosecurity and examine the role of the 'disposition matrix' in this context.

Resourcing the unpredictable: Technoscientific rationality and the 'disposition matrix'

Post-relational databases and genetic algorithms can be regarded as the paradigmatic media of a post-Newtonian rationality and the preferred medium of an intelligence community

keen to map a world perceived as incoherent, unpredictable and full of risks (Aradau and van Munster, 2007). Surplus processes of 'emergent' behaviour are exploited by collecting a huge amount of data on the basis of HUMINT and especially SIGINT, including SOCMINT. These databases are searched, mostly on a quantitative or associative basis, by flexible algorithms looking for links, connections, similarities or patterns. The logic followed here is not one of cause-and-effect but rather one of preemption and possibility. In the face of unknown unknowns, it is no longer accountability and traditional scientific rigour that are used to counter threats but rather the technical exploitation of chance and imagination by means of systematized tinkering and formalized processes of trial and error. Consequently, according to the data-driven logic of comprehensive (re-)combination, anybody and everybody can become a target: while massive amounts of surveillance data are gathered

> without any judicial review let alone search warrants . . . a surveillance state and a secretive, unaccountable judicial body . . . analyzes who you are and then decrees what should be done with you, how you should be 'disposed' of, beyond the reach of any minimal accountability or transparency. (Greenwald, 2012)

An important part of this logic is driven by technoscientific practices, which decline to engage in any kind of objective representation of the world – even though politicians, police, military and secret services personnel vehemently claim the scientific validity of the technologies used in their public rhetoric of legitimation. A core part of the construction of the 'disposition matrix' consists of extremely vague categorizations of what counts as terrorism and what is a 'central' node in a 'terrorist network'. The 'disposition matrix' depends on maintaining secrecy about what makes somebody 'eligible' to be included in it or to become the target of a drone strike or a raid. It relies on metadata and on data mining tools such as SNA (which is opaque even to the analysts themselves), often follows a purely quantitative logic and/or ignores the social, political and cultural context, in which the data are gathered. This logic is not grounded in objective, reproducible methods and there is not even a coherent narrative about why a person is more dangerous than another person, or why they 'need' to be assassinated. While a numerical list gives priority to some people over others (qualifying him or her as *the* most dangerous terrorist, for example), a database collects all the information that is available. The way patterns are constructed changes with every new piece of information collected. Within this technorational framework (the purpose of which is to preempt highly unlikely possibilities), it is impossible to explain why somebody is supposedly *the* most dangerous terrorist or the most important one for the network. The process seems to follow a logic of eliminating every possible danger. Within this logic, the database is the perfect tool for preemptive security measures, because it has no need of the logic of cause and effect. It widens the search space and provides endless new patterns of possibilistic networks.

It is not only that 'extraordinary and exclusionary political measures are activated through the invocation of an existential threat' (Opitz, 2011: 94), the new technoscientific rationality built on resourcing the unpredictable by means of systematized search practices also provides a new basis for a security culture – a culture driven by the (necessarily vain) wish to preempt any possibilistic risk. Given this new technorationality, illiberal security discourses and practices such as secret blacklisting and targeted assassinations appear increasingly rational. And to make the increasingly powerful non-human agency of algorithms and database systems invisible, the symbolic power of the sovereign is emphasized: on 'Terror Tuesdays' it (appears that it) is only the sovereign who decides about life and death.

Acknowledgements

I would like to thank Louise Amoore, Claudia Aradau, Marieke de Goede, Derek Gregory, Anna Leander, Urs Stäheli, Lucy Suchman and many more who provided helpful advice on earlier versions of this article when it was presented at the COST workshop '*The Politics of List: Law, Security, Technology*' at the Kent Law School, University of Kent in Canterbury in November 2013 and the symposium *Security by Remote Control* at the Centre for Science Studies at Lancaster University in May 2014. Many thanks for helpful critical insights also to the four anonymous reviewers and the guest editors who helped very much to clarify these thoughts. I am also indebted to Katrin M. Kämpf for research assistance. All remaining errors remain my own.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This research was made possible in part by a sabbatical in the spring and summer term 2015 granted by the University of Paderborn.

Notes

1. See also Greenwald (2012), Gettinger (2015) and Woods (2015).
2. Signals intelligence (SIGINT) is defined as '[i]ntelligence derived from communications, electronic, and foreign instrumentation signals' (Department of Defense, 2007: 224). The term communications signals (COMINT) signifies voice information or messages sent between people who have been intercepted from foreign sources, while electronic intelligence (ELINT) is '(t)echnical and geolocational intelligence derived from foreign noncommunications electromagnetic radiations' (Department of Defense, 2007: 77). Foreign instrumentation signals (FISINT) includes data from foreign sources of telemetry or video data links transmitted by satellites, UAVs, missiles, etc.
3. However, the newly released database Intelligence Community Watch (ICWatch, 2015) developed by the group 'Transparency Toolkit' and now hosted by Wikileaks shows that many US analysts now concentrate on producing targets and work with data mining software such as IBM's Analyst's Notebook or Palantir.
4. For example, around 7 terabytes of drone imagery data are disseminated every day by the Air Force's Distributed Common Ground System (DCGS) (Gettinger, 2015).
5. Greg Miller has pointed out that the CIA has made identifying targets for targeted killing by drones 'a designated career track' (Miller and Tate, 2011).
6. This approach is based on work by Valdis Krebs, who was the first to use SNA to map a terrorist network – in this case, the network of the 9/11 attackers; see Krebs (2002).
7. See, for example, the self-description of an 'intelligence analyst' at ICWatch who has the following software-related 'skills': 'i2 Analyst Notebook, Microsoft Office, Internet,... PowerPoint, Analyst Notebook,... Microsoft Excel, Time Management, Facebook,..., Microsoft Word, Social Networking, Research', https://icwatch.wikileaks.org/nsadocs/andrea-javor55587789Ohio HIDTACriminalIntelligenceAnalystIntern2013-05-01.
8. '[Th]is account is bolstered by top-secret NSA documents previously provided by whistleblower Edward Snowden. It is also supported by a former drone sensor operator with the US Air Force, Brandon Bryant, who has become an outspoken critic of the lethal operations in which he was directly involved in Iraq, Afghanistan and Yemen. In one tactic, the NSA ''geolocates'' the SIM card or handset of a suspected terrorist's mobile phone, enabling the CIA and US military to

conduct night raids and drone strikes to kill or capture the individual in possession of the device' (Scahill and Greenwald, 2014b).

9. This becomes apparent, for example, in the wish expressed by the US military to build 'Reachback Research Centers' for Human Terrain Teams, from where social scientists, analysts and others are supposed to provide cultural context; see González and Price (2015, no pagination).
10. Structured data rest on a predefined data model, while semi-structured data are loosely, irregularly structured and cannot be processed in relational databases. '(U)nstructured data do not have a defined data model or common identifiable structure' (Kitchin, 2014: 6).
11. See the sections on technorationality.
12. Although they are also linked to the algorithms used.
13. Which is not to say that some people are more likely to be targeted according to categories such as race, class or gender.

References

Amoore L (2009) Algorithmic war: everyday geographies of the war on terror. *Antipode: A Radical Journal of Geography* 41: 49–69.

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

Aradau C, Lobo-Guerrero L and van Munster R (2008) Security, technologies of risk, and the political: Guest editors' introduction. *Security Dialogue* 39(2–3): 147–154.

Aradau C and van Munster R (2007) Governing terrorism through risk: Taking precautions, (un)knowing the future. *European Journal of International Relations* 13(1): 89–115.

Becker J and Shane S (2012) Secret 'kill list' proves a test of Obama's principles and will. *New York Times*, 29 May.

Belcher O (2014) *The afterlives of counterinsurgency: Postcolonialism, military social science, and Afghanistan 2006-2012*. PhD Thesis. Available at: https://circle.ubc.ca/bitstream/handle/2429/45520/ubc_2014_spring_belcher_oliver.pdf?sequence=5 (accessed 10 December 2015).

Bogard W (2012) Simulation and post-panopticism. In: Ball K, Haggerty K and Lyon D (eds) *Routledge Handbook of Surveillance Studies*. New York: Routledge, pp. 30–37.

Bowker GC and Star SL (2000) *Sorting Things Out: Classification and its Consequences*. Cambridge, MA: MIT Press.

Brennan JO (2012) Transcript of remarks by John O. Brennan, Assistant to the President for Homeland Security and Counterterrorism. The Ethics and Efficacy of the President's Counterterrorism Strategy. Available at: http://www.wilsoncenter.org/event/the-efficacy-and-ethics-us-counterterrorism-strategy (accessed 10 December 2012).

Bröckling U, Krasmann S and Lemke T (2011) *Governmentality: Current Issues and Future Challenges*. New York: Routledge.

Codd E (1970) A relational model of data for large shared data banks. *Communications of the ACM* 13(6): 377–387.

Cole D (2013) We kill people based on metadata. *The New York Review of Books,* 15 August, Available at: http://www.nybooks.com/articles/archives/2013/aug/15/nsa-they-know-much-more-you-think/?insrc=rel (accessed 10 December 2012).

Currier C, Greenwald G and Fishman A (2015) US government designated prominent Al Jazeera journalist as member of Al Qaeda. *The Intercept*, 8 May. Available at: https://firstlook.org/theintercept/2015/05/08/u-s-government-designated-prominent-al-jazeera-journalist-al-qaeda-member-put-watch-list/ (accessed 10 December 2012).

Daase C and Kessler O (2007) Knowns and unknowns in the 'war on terror': Uncertainty and the political construction of danger. *Security Dialogue* 38(4): 411–434.

de Goede M (2008) Beyond risk: Premediation and the post-9/11 security imagination. *Security Dialogue* 39(2–3): 155–176.

de Goede M (2013) The politics of security listing. Classification, criteria, consequence, critique. In: *COST-workshop, the politics of lists: Law, security, technology*, Canterbury, UK, 31st October–1st November, Kent Law School.

Department of Defense (2007) *Dictionary of military and associated terms*. Available at: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (accessed 10 December 2012).

Der Derian J (2009) *Virtuous War: Mapping the Military-Industrial-Media-Entertainment Network*, 2nd ed. New York: Routledge.

de Young K (2012) A CIA veteran transforms US counterterrorism policy. *Washington Post* 24 October, Available at: http://articles.washingtonpost.com/2012-10-24/world/35499428_1_drone-strikes-brennan-obama-administration (accessed 10 December 2012).

Dourish P (2001) *The Foundations of Embodied Interaction*. Cambridge: MIT Press.

Dourish P (2014) NoSQL: The shifting materialities of database technology. *Computational Culture* 4, Available at: http://computationalculture.net/article/no-sql-the-shifting-materialities-of-database-technology (accessed 10 December 2012).

Gettinger D (2015) The disposition matrix. *Center for the Study of Drones Blog*, 25 April. Available at: http://dronecenter.bard.edu/the-disposition-matrix/ (accessed 10 December 2012).

Ghamari-Tabrizi S (2005) *The worlds of Herman Kahn: The intuitive science of thermonuclear war*. Cambridge, Massachusetts: Harvard University Press.

González RJ (2015) Seeing into hearts and minds. Part 2. 'Big data', algorithms and computational counterinsurgency. *Anthropology Today* 31(4) August, 13–18.

González RJ and Price D (2015) Remaking the human terrain: The US military's continuing quest to commandeer culture. Available at: http://www.counterpunch.org/2015/07/31/remaking-the-human-terrain-the-us-militarys-continuing-quest-to-commandeer-culture/ (accessed 31 July 2015).

Goody J (1977) *The Domestication of the Savage Mind*. Cambridge: Cambridge University Press.

Greenwald G (2012) Obama moves to make the War on Terror permanent. *The Guardian*, 24 October. Available at: http://www.theguardian.com/commentisfree/2012/oct/24/obama-terrorism-kill-list (accessed 10 December 2015).

Gregory D (2013) Theory of the drone 3: Killing grounds. *Geographical Imaginations Blog*, 29 July. Available at: http://geographicalimaginations.com/2013/07/29/theory-of-the-drone-3-killing-grounds/ (accessed 10 December 2015).

Gregory D (2012) I don't like Tuesdays, *Geographical Imaginations Blog*, 26 October. Available at: http://geographicalimaginations.com/2012/10/26/i-dont-like-tuesdays/ (accessed 10 December 2015).

Gutwirth S and Hildebrandt M (2010) Some caveats on profiling. In: Gutwirth S, Poullet Y and de Hert P (eds) *Data Protection in a Profiled World*. Dordrecht: Springer.

Haraway D (1985/1991) Manifesto for cyborgs: Science, technology, and socialist feminism in the 1980s. *Socialist Review* Vol 80: 65–108 (Reprinted in Haraway D (1991) *Simians, Cyborgs, and Women: the Reinvention of Nature*. London/New York: Routledge, pp.149–181).

Hildebrandt M and Gutwirth S (2008) *Profiling the European Citizen. Cross Disciplinary Perspectives*. Dordrecht: Springer.

Holland JH (1992) Genetic Algorithms Computer programs that 'evolve' in ways that resemble natural selection can solve complex problems even their creators do not fully understand. *Scientific American* 267: 66–72.

Humphreys D (1984) On the Tuesday Lunch at the Johnson White House: a preliminary assessment. *Diplomatic History* 8: 81–101.

ICWatch (2015) Intelligence community watch 5 May. Available at: https://icwatch.wikileaks.org/ (accessed 10 December 2015).

Joint Warfighting Center (2011) *Joint Doctrine Support Division. Commander's Handbook for Attack the Network, Version 1.0*. Suffolk/Virginia, 20 May. Available at: http://www.dtic.mil/doctrine/doctrine/jwfc/atn_hbk.pdf (accessed 10 December 2015).

Kahn H (1960) *On Thermonuclear War*. Princeton: Princeton University Press.

Kaplan F (1983) *The Wizards of Armageddon*. New York: Simon and Schuster.
Kessler O and Wouter W (2013) A grim debating society. In: *COST-Workshop, the politics of lists: law, security, technology*, Canterbury, UK, 31st October–1st November, Kent Law School.
Kitchin R (2014) *The Data Revolution. Big Data, Open Data, Data Infrastructures & Their Consequences*. Los Angeles: Sage.
Krebs V (2002) Uncloaking terrorist networks. *First Monday* 7(4). Available at: http://firstmonday.org/ojs/index.php/fm/article/view/941/863/ (accessed 10 December 2015).
Latour B (1986) *Science in Action*. Milton Keynes: Open University Press.
Manovich L (2001) *The Language of New Media*. Cambridge: MIT Press.
McNeal G (2014) Kill-lists and accountability. *Georgetown Law Journal* 102: 681–794.
Miller G (2012) Plan for hunting terrorists signals US intends to keep adding names to kill lists. *The Washington Post*, 23 October. Available at: http://www.washingtonpost.com/world/national-security/plan-for-hunting-terrorists-signals-us-intends-to-keep-adding-names-to-kill-lists/2012/10/23/4789b2ae-18b3-11e2-a55c-39408fbe6a4b_story.html (accessed 10 December 2015).
Miller G and Tate J (2011) CIA shifts focus to killing targets. *The Washington Post,* 1 September. Available at: http://www.washingtonpost.com/world/national-security/cia-shifts-focus-to-killing-targets/2011/08/30/gIQA7MZGvJ_story.html (accessed 10 December 2015).
National Counterterrorism Center (NCTC) (2013) Watchlisting guidance march. Available at: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH01d1/4a00c36e.dir/doc.pdf (accessed 10 December 2015).
National Security Agency (2012) Skynet. Courier detection via machine learning. 6 June. Available at: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASHc939.dir/doc.pdf (accessed 10 December 2015).
Nordmann A (2006) Collapse of distance: Epistemic strategies of science and technoscience. *Danish Yearbook of Philosophy* 41: 7–34.
Opitz S (2011) Government unlimited: The security dispositif of illiberal governmentality in *governmentality*. In: Bröckling U, Krasmann S and Lemke T (eds) *Current Issues and Future Challenges*. New York, London: Routledge, pp. 93–114.
Porter G (2011) How McChrystal and Petraeus built an indiscriminate 'killing machine'. *Truthout Monday*, 26 September. Available at: http://www.truth-out.org/news/item/3588-how-mcchrystal-and-petraeus-built-an-indiscriminate-killing-machine (accessed 10 December 2015).
Ressler S (2006) Social network analysis as an approach to combat terrorism: Past, present, and future research. *Homeland Security Affairs* 2(2): 1–10.
Sageman M (2004) *Understanding Terrorist Networks*. Philadelphia: University of Pennsylvania Press.
Salter M (2008) Risk and imagination in the war on terror. In: Amoore L and de Goede M (eds) *Risk and the War on Terror*. New York/London: Routledge, pp. 233–246.
Scahill J and Devereaux R (2014a) The Secret Government Rulebook for labeling you a terrorist. *The Intercept*, 23 July. Available at: https://firstlook.org/theintercept/article/2014/07/23/blacklisted/ (accessed 10 December 2015).
Scahill J and Devereaux R (2014b) Barack Obama's Secret Terrorist-tracking system, by the numbers. *The Intercept*, 5 August. Available at: https://firstlook.org/theintercept/2014/08/05/watch-commander/ (accessed 10 December 2015).
Scahill J and Greenwald G (2014) The NSA's secret role in the US assassination program. *The Intercept*, 10 February. Available at: https://firstlook.org/theintercept/article/2014/02/10/the-nsas-secret-role/ (accessed 10 December 2015).
Scahill J (2015) The Assassination complex. Secret military documents expose the inner workings of Obama's drone wars. *The Intercept*, 15 October. Available at: https://theintercept.com/drone-papers/the-assassination-complex/ (accessed 10 December 2015).
Schmid A (2011) The Definition of terrorism. In: Schmid A (ed.) *The Routledge Handbook of Terrorism Research*. Abingdon, VA: Routledge, pp. 39–99.
Schneier B (2006) Data mining for terrorists. *Schneier Blog*, 3 March. Available at: https://www.schneier.com/blog/archives/2006/03/data_mining_for.html (accessed 10 December 2015).

Shaw I (2013) Bureaucratic assassination—How do US targeted killings work? *Understanding Empire Blog*, 3 October. Available at: http://understandingempire.wordpress.com/2013/10/03/bureaucratic-assassination-how-do-u-s-targeted-killings-work (accessed 10 December 2015).

Shaw I and Akhter M (2014) The dronification of state violence. *Critical Asian Studies* 46(2): 211–234.

Stäheli U (2012) Listing the global: Dis/Connectivity beyond representation? *Distinktion: Scandinavion Journal of Social Theory* 13(3): 233–246.

Stohl C and Stohl M (2007) Networks of terror: Theoretical assumptions and pragmatic consequences. *Communication Theory* 17: 93–124.

Suchman L (1994) Do categories have politics? The language/action perspective reconsidered. *Computer Supported Cooperative Work (CSCW)* 2: 177–190.

Thrift N and French S (2002) The automatic production of space. *Transactions of the Institute of British Geographers NS* 27: 309–335.

Weber J (2003) *Umkämpfte Bedeutungen: Naturkonzepte im Zeitalter der Technoscience*. Frankfurt, New York: Campus.

Weber J (2011) Blackboxing organisms, exploiting the unpredictable: Control paradigms in human-machine translation. In: Carrier M and Nordmann A (eds) *Science in the Context of Application*. Dordrecht/Heidelberg/London/New York: Springer, pp. 409–429.

Whitlock C (2012) Remote US base at core of secret operations. *The Washington Post*, 25 October. Available at: http://www.washingtonpost.com/world/national-security/remote-us-base-at-core-of-secret-operations/2012/10/25/a26a9392-197a-11e2-bd10-5ff056538b7c_story.html (accessed 10 December 2015).

Woods C (2015) Covert drone strikes and the fiction of zero civilian casualties. In: Aaronson M, Aslam W, Dyson T, et al. (eds) *Precision Strike Warfare and International Intervention: Strategic, Ethico-Legal, and Decisional Implications*. New York, London: Routledge, pp. 95–113.

Jutta Weber is a STS Scholar, Philosopher of Technology and Professor for Media Studies at the University of Paderborn. Her research focuses on epistemological, ontological and sociopolitical dimensions of computational technoscience culture(s) asking how and for whom the non/human actors work.