Published as **Big Data-Kriege. Über Tötungslisten, Drohnen und die Politik der Datenbanken. In: Christoph Engemann, Andreas Sudmann (Hg.): Machine Learning – Medien, Infrastrukturen und Technologien der Künstlichen Intelligenz. Bielefeld: transcript, S.219-246**. Pre-print version.

Big-Data-Kriege

Über Tötungslisten, Drohnen und die Politik der Datenbanken[1]

Jutta Weber

> *»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/Star, 2000: 50*

›Disposition Matrix‹: Über Tötungslisten, Datenbanken und die Produktion von Zielen

Seit 9/11 ist die Anzahl der US-amerikanischen Tötungs-und Überwachungslisten konstant angestiegen und sie spielen eine immer größere Bedeutung in der Politik der gezielten Tötung. Dieser Artikel untersucht die materielle Logik und epistemologische Dimension der ›Disposition Matrix‹, der wichtigsten Datenbank unterschiedlicher Tötungslisten im US-amerikanischen ›War on Terror‹. Wie aber sind soziotechnische Artefakte wie Datenbanken und Algorithmen mit menschlichen Entscheidungsprozessen bei der Produktion von Tötungszielen verflochten? Im Folgenden werde ich die kulturelle Logik dieser datenzentrierten Kriegsführung analysieren, um die *nicht-humanen* soziopolitischen Akteure sichtbar zu machen, die im Kontext einer post-Newtonischen Technorationalität der Rekombination und (Ko-)relation entstehen, die das Unberechenbare als Ressource nutzen und die präventive Kultur von Technosicherheit (weiter) befeuern.

---

[1] | *Dieser Text erschien zuerst unter dem Titel »Keep Adding. Kill Lists, Drone Warfare and the Politics of Databases«, in: Environment and Planning D. Society and Space, February 2016, 34 (1): 107-125; http://epd.sagepub.com/content/34/1/107. Der Text wurde von der Autorin übersetzt.*

Die ›Disposition Matrix‹, die wichtigste Tötungsliste der US-Regierung, wurde 2010 vom CIA-Direktor John Brennan – Barack Obamas ehemaligem Anti-Terror Berater – entworfen und führt diverse Tötungslisten des Pentagons, der Central Intelligence Agency (CIA) und des Joint Special Operations Command (JSOC) zusammen. Einige Kritiker_innen spekulieren, dass die ›Disposition Matrix‹ eingeführt wurde, um den kill/capture-Prozess zwischen diesen Organisationen zu regulieren und zu rationalisieren und dabei den Generalstab des Militärs zu umgehen (Miller 2012). Ich werde im Folgenden zeigen, dass diese ›Harmonisierung‹ der verschiedenen Tötungslisten auch der Dynamik von ›Big Data‹ bzw. von Datenanalyseverfahren geschuldet ist. Ein großer Teil der Informationen über die ›Disposition Matrix‹ und andere Tötungs- oder Beobachtungslisten von ›Terrorist_innen‹ ist geheim und unter Verschluss. Die wenigen Dokumente, die zugänglich sind, wurden sowohl von regierungsfreundlichen als auch von kritischen Forscher_innen zur Verfügung gestellt sowie von investigativen Journalist_innen oder NGOs, die zumindest teilweise Informationen über die Diskurse und Praktiken der ›Disposition Matrix‹ liefern können. Ihre Existenz wurde 2012 durch mehrere Artikel in der *Washington Post* öffentlich bekannt, die sich auf Aussagen von erfahrenen Mitgliedern der Obama-Administration bezogen (Miller 2012; de Young 2012; Whitlock 2012).[2] Datenbanken wie die ›Disposition Matrix‹ sowie auch andere Tötungs- oder Beobachtungslisten sind Instrumente in der Profilierung von Terroristen oder Verdächtigen, die auf menschlicher Aufklärungsarbeit (›human intelligence‹ bzw. HUMINT) und, vor allem, auf technischer bzw. elektronischer Aufklärung (›signal intelligence‹ bzw. SIGINT [3]) basieren. Neue Dateninfrastrukturen und -analyseverfahren (Kitchin 2014) haben eine zunehmende Bedeutung im Bereich der Aufklärung und der gezielten Tötung in der aktuellen US-amerikanischen Kriegsführung (Belcher 2014; González 2015).

Die Geographen Ian Shaw and Majed Akhter umschreiben die Funktion der ›Disposition Matrix‹ folgendermaßen:

›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

---

2 | *Vgl. auch Greenwald 2012; Gettinger 2015; Woods 2015.*

3 | *Elektronische Aufklärung (SIGINT) wird defininiert als »[i]ntelligence derived from communications, electronic, and foreign instrumentation signals« (Department of Defense 2007: 224).*

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/Akhter, 2014: 211; eigene Hervorhebung)

Die menschlichen Ziele der ›Disposition Matrix‹ werden entweder in Drohnenattacken oder bei nächtlichen Razzien des Militärs gefangen genommen bzw. getötet. Soweit allgemein bekannt, wurden die meisten der gezielten Gefangennahmen bzw. Tötungen des Pentagon in Afghanistan, Libyen oder im Irak vorgenommen. Außerhalb von konventionellen Kriegsschauplätzen werden Drohnen von der CIA und der JSOC in Ländern wie Pakistan, Jemen, Somalia und Syrien benutzt. Tausende der nächtlichen Razzien wurden überwiegend von JSOC im Irak und in Afghanistan durchgeführt (Gregory 2013; Woods 2015).

Die wahrscheinlich detaillierteste Beschreibung wie die ›Disposition Matrix‹ erstellt wird, stammt vom Rechtsprofessor Gregory S. McNeal in seiner Studie »Targeted Killing and Accountability« (2014). Diese ist eine höchst informative wenn auch problematische Studie, insofern sie häufig die sehr unspezifischen Definitionen wie ›Terrorist‹ und weitere damit verbundene Begriffe der US-amerikanischen Regierung übernimmt. Grundlage seiner Studie sind militärische Strategiepapiere, Antworten der Regierung auf Anfragen nach dem *Freedom of Information Act* (*FOIA*), Gerichtsdokumente, Presseberichte und wissenschaftliche Studien sowie teilnehmende Beobachtung des offiziellen Trainings als auch Interviews mit Angehörigen des Militärs, der JSOC sowie der Geheimdienste, die in den Tötungsprozess involviert sind.

Targeting ›Methodology‹: Wie Terrorist_innen konstruiert werden

Laut McNeal besteht die Nominierung eines Ziels für die ›Disposition Matrix‹ aus vier Schritten: der Identifizierung, Sicherheitsüberprüfung, Validierung und Nominierung – letzteres oftmals mit der Bewilligung des US-Präsidenten. Am sogenannten ›Terror Tuesday‹ hält Barack Obama Rücksprache mit seinen Sicherheitsexpert_innen, für welche der Personen die Anschläge autorisiert werden sollen:

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/Shane 2012)

Kürzlich hat die investigative Journalismusplattform *The Intercept* auf der Grundlage von zugespieltem Material berichtet, dass Aufklärungsanalytiker_innen eine kurze Beschreibung der/des Verdächtigen und der Bedrohung, die sie oder er darstellt, in der Form einer ›Baseballkarte‹ erstellen, die – zusammen mit operationalen Informationen – für das weitere Verfahren auf eine höhere Ebene durchgereicht werden. Im Durchschnitt benötigt der Präsident 58 Tage um ein Ziel zu nominieren (Scahill 2015). Dieser Genehmigungsprozess ist nicht ganz neu: er wurde von US-Präsident Lyndon B. Johnson erfunden, der persönlich Ziele während des Vietnamkrieges ausgewählt hat (Humphreys 1984; Gregory 2012) – diese Ziele waren jedoch mehrheitlich Objekte und keine menschlichen Wesen wie auf Obamas Liste. Heutzutage ist jedoch die ›Disposition Matrix‹ eine wichtige Komponente der US-amerikanischen, computergestützten Widerstandsbekämpfung und Bestandteil des »distanced, computer-centric approach of RMA [Revolution in Military Affairs; JW]« (Belcher 2014: 51). Als flexible Datenbank enthält sie strukturierte und unstrukturierte Daten, kleine sowie auch große Datenmengen, die mittels neuerer Data Mining-Algorithmen systematisch durchsucht werden können. Sie stellt ein neues und zentrales Werkzeug im ›Globalen Krieg gegen den Terror‹ dar und basiert auf einer Technorationalität, die mit einer Logik des ›Tinkerings‹, des systematischen Ausprobierens, arbeitet, welche das ›Unbekannte‹ und dabei jedwede (oftmals auch sehr unwahrscheinliche) Möglichkeit(en) durchforstet. Dabei werden riesige Datenmengen durchsucht und gebündelt um Beziehungsmuster zwischen Daten *herzustellen* und so ›Wissen‹ in Datenbanken zu entdecken (Hildebrandt/Gutwirth 2008; Kitchin 2014). Dieser auf *Entdeckung* fokussierte Ansatz arbeitet nicht mit einer Idee von Korrelation, die auf kausalen Verbindungen basiert, sondern folgt der Annahme, dass (mögliche) Verbindungen, die in der Vergangenheit auftraten, auch in der Zukunft wieder auftreten.

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/Hildebrandt 2010: 7)

Je größer die Datensammlung ist, desto mehr Möglichkeiten gibt es, um durch Rekombination ›Wissen‹ zu produzieren (was primär mit interessanten Kombinationen bzw. Mustern gleichgesetzt wird). Somit wird die Zentralisierung von Tötungs- und Beobachtungslisten nicht nur durch politische Strategien und Entscheidungsträger_innen, sondern auch durch die innere Logik von Datenanalysen vorangetrieben.

Definitionen

In den letzten Jahrzehnten haben US-amerikanische militärische Organisationen und Geheimdienste große Mengen an Informationen über – als Terrorist_innen verdächtigte – (Widerstands-)Kämpfer_innen in unterschiedlichen Datenbanken gespeichert und in diverse Tötungs- und Überwachungslisten aufgenommen, um das Herausfiltern von spezifischen ›terroristischen‹ Eigenschaften und Verhaltensmustern via Data Mining möglich zu machen.

Dieses Vorgehen ist offensichtlich eine höchst komplizierte und selektive Aufgabe, insbesondere da es keine internationale und gesetzlich verbindliche Definition von Terrorismus gibt und die Definitionen, die von der US-amerikanischen Regierung gebraucht werden, ausgesprochen weit variieren (Schmid 2011). Aufgrund der Geheimhaltung, die das Prozedere umgibt, stellt sich als zentrale Frage: Wer gilt als Terrorist_in und warum? Und dementsprechend: Welche Daten sollten gesammelt werden? Wie kommt es, dass jemand in einer Datenbank namens TIDE (Terrorist Identities Datamart Environment) gelistet wird – die größte Liste von bekannten und verdächtigten Terrorist_innen, die sensitive und militärische Aufklärungsdaten versammelt unter Einbezug geheimer Informationen, die vom NCTC (National Counterterrorism Center) verwaltet wird? Oder auch in der Terrorist Screening Database (TSD), die vom FBI verwaltet wird und in der zwischen 680.000 (Scahill/Devereaux: 2014b) und 875.000 Personen (de Goede 2013) verzeichnet sind? Die TSD Datenbank ist eine

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/Devereaux 2014b; meine Hervorhebung).

Die ›Disposition Matrix‹ wurde 2010 unter Verwendung der oben genannten sowie weiterer Datenbanken zusammengestellt. Es ist jedoch unklar, wie genau die Informationen der Datenbanken zusammengeführt und welche spezifischen Targeting-Methodologien und Algorithmen verwendet werden[4].

---

4 | *Man kann beim Studium der Datenbank ›Intelligence Community Watch‹ (ICWatch 2015) der Gruppe ›Transparency Toolkit‹, die unterdessen bei Wikileaks beheimatet ist, gut studieren, wie viele US Analyst_innen sich unterdessen darauf konzentrieren Ziele zu produzieren und dabei mit Data Mining-Software wie IBM's Analyst's Notebook oder Palantir arbeiten.*

McNeal (2014) zufolge ist die Mitgliedschaft in einer ›organisierten und bewaffneten Gruppe‹ eine hinreichende Bedingung für die Obama-Regierung um auf eine Tötungsliste zu kommen. Doch was gilt als bewaffnete und organisierte Gruppe? Die verwendete Definition könnte ebenso gut auf eine USamerikanische Familie zutreffen, in der alle erwachsenen Familienmitglieder eine Waffe besitzen. Oder sie könnte eine Gruppe von Stammesältesten in Wasiristan beschreiben, die traditionell als Statuszeichen Waffen tragen. Manchmal werden sogar Personen zu den Listen hinzugefügt, die als wichtig für eine Gruppierung erachtet werden, auch wenn sie keine Mitglieder dieser Gruppierung sind. Auch hier gibt es keine strengen Kriterien dafür, wann auch NichtMitglieder hinzugefügt werden dürfen.

Im Juli 2014 wurde der journalistischen Plattform *The Intercept* ein Dokument namens ›Watchlisting Guidance‹ zugespielt, welches offensichtlich vom NCTC im März 2013 erstellt worden war (NCTC 2014). Das Dokument enthält Kriterien für das Hinzufügen von Individuen in die TSDC- oder TIDEDatenbank. Es offenbart, wie vage die Auswahlkriterien hierfür sind – und erklärt damit zumindest teilweise, warum die Anzahl der Ausgewählten für die Tötungs- und Beobachtungslisten so hoch ist. Das Dokument definiert ›terroristische Aktivität‹ nicht nur als Handlungen wie Geiselnahme, Hinrichtung oder Bomben legen, sondern auch als »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/Devereaux 2014a; meine Hervorhebung). Diese vagen Definitionen von ›terroristischen Verdächtigen‹ und ›Terrorist_innen‹ fördern die Inklusion einer enormen Bandbreite von Daten in den ›Terror‹-Datenbanken. Die Datenbanken enthalten zunehmend auch Daten von nicht-gewalttätigen politischen Aktivist_innen und Individuen, welche das herrschende politische System ganz allgemein in Frage stellen. In diesem Kontext haben Forscher_innen des Militärs damit angefangen, auch Informationen von sozialen Medien wie Twitter oder Facebook via Data Mining zu analysieren und auszuwerten (social media intelligence bzw. SOCMINT) in der Hoffnung, damit das ›Puzzle (möglicher Einzelinformationen zu terroristischen Anschlägen) zusammensetzen zu können‹. Die Folgen davon sind jedoch hochproblematisch. Aus Angst, mögliche potenzielle Verdächtige zu übersehen, werden die Suchkriterien ganz breit konstruiert. Entsprechend werden immer mehr Daten in die Datenbanken der Tötungs- und Beobachtungslisten eingespeist und die Algorithmen zur Entdeckung von Terroristen sehr breit definiert um jedwede Korrelationen und Muster zu ›entdecken‹ bzw. konstruieren zu können. Dadurch steigt die Anzahl der ›false positives‹ rasant:

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; meine Hervorhebung)

Meta Daten, Soziale Netzwerkanalyse (SNA) & Skynet

Die datenzentrierte Analyse arbeitet mit einer großen Breite an Instrumenten und Herangehensweisen wie z.B. mit Sozialer Netzwerkanalyse (SNA), mit Link-, Video-[5], Inhalts- und Sentiment-Analyse um Ziele auf der Basis von menschen- und datengestützter Aufklärung auszuwählen und zu verfolgen (HUMINT und SIGINT) (vgl. Joint Warfighting Center 2011; Ressler 2006; Sageman 2004; ICWatch 2015). In Ländern wie Pakistan, Jemen und Syrien, in welchen wenig US-amerikanische Bodentruppen präsent sind, werden die meisten Informationen mittels signalgesteuerter bzw. datengestützter Aufklärung (SIGINT) zusammengetragen. Informationen der SIGINT wird aus Videoströmen, Mobiltelefonaten, geolokalen Informationen sowie aus Daten von Emails, sozialen Medien und anderen Internetservices für die Datenanalyse gewonnen – oftmals auf der Grundlage einer rein quantitativen Linkanalyse-Methodologie. Das hat zur Folge, dass eine Person umso verdächtiger wird, je öfter sie eine bereits als verdächtig eingestufte Person kontaktiert – und das auch, wenn es sich um eine/n Verwandte/n oder Freund_innen – und keine Mitglieder eines sogenannten terroristischen Netzwerks – handelt. Sicherheitsbehörden wie die CIA oder die NSA nutzen dieses Vorgehen in ihren Datensammlungen häufig sogar über zwei (bis drei) Schritte hinweg, um Verbindungen zu anderen verdächtigen ›Terroristen‹ oder Mitgliedern von ›Terrororganisationen‹ herzustellen [6], wodurch die Kreise immer weiter gezogen werden. Währenddessen bietet die Soziale Netzwerkanalyse (SNA)

---

5 | *So wurden z.B. im Jahre 2014 ungefähr sieben Terabyte an Bildmaterial von Drohnen vom Air Force's Distributed Common Ground System (DCGS) bereitgestellt (Gettinger 2015).*

6 | *Greg Miller hat darauf hingewiesen, dass die CIA die Identifikation von Zielen für die gezielte Tötung zu einem »designated career track« (Miller and Tate, 2011) gemacht hat.*

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).

Organisierte und bewaffnete ›terroristische‹ Gruppierungen werden dabei häufig als soziale Netzwerke interpretiert (Sageman 2004; Ressler 2006). Die Bedeutung eines Mitglieds einer vermuteten terroristischen Organisation wird mittels der SNA im Rahmen einer Kosten-Nutzen-Analyse festgelegt. Steve Ressler vom US-Ministerium für innere Sicherheit (Homeland Security) betont, dass eine solche Analyse »on the value of the network structure rather than the characteristics of the individual« erstellt wird (Ressler 2006: 2). Man interpretiere terroristische Organisationen als nicht-hierarchisch, deren Mitglieder oftmals nur lose miteinander in Verbindung stehen, deshalb werden nicht nur Anführer der Taliban und Al-Qaida als potenzielle Ziele angesehen, sondern im Prinzip jegliche Personen, die in losem Kontakt zu den Mitgliedern eines Netzwerkes stehen. Diese Beschreibung von ›terroristischen‹ Netzwerken entspricht der Herangehensweise der SNA, die große Mengen von Metadaten kartographiert und visualisiert und in quasi-naturalisierten Soziogramme ›zusammenführt‹.[7] Das *Commander's Handbook for Attack of the Network* (2012) des US Joint Warfighting Center beschreibt die Methodologie und Vorgehensweise, um die Verwundbarkeit von terroristischen Netzwerken auszubeuten recht unverblümt: »SNA helps to identify which nodes in the network can be killed, captured or influenced to achieve desired effects« (Joint Warfighting Center 2011, IV-3).

Während das Handbuch (›terroristische‹) Netzwerke – wie sie mittels SNA ermittelt werden – als gegeben annimmt, verweist es im gleichen Zug auf die Defizite dieser Data Mining-Analyse:

[…] 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. (Ebd; meine Hervorhebung)

---

7 | *Dieser Ansatz wurde vor allem von Valdis Krebs entwickelt, der als erster SNA benutzt hat um die Karte eines terroristischen Netzwerks zu erstellen – in diesem Fall war dieses das Netzwerk der 9/11-Angreifer (vgl. Krebs 2002).*

Die SNA kartiert Beziehungen zwischen Menschen, Orten und Dingen um sogenannte ›Lebensmuster‹ (›pattern of life‹) zu entwickeln, welches die »process-based relationship between key nodes« (Shaw 2013) herausarbeitet. Somit werden nicht nur die Anführer_innen von ›terroristischen‹ Gruppierungen als zulässige Objekte gezielter Tötungen angesehen, sondern jede beliebige Person, die (von einem Algorithmus oder einer Analytikerin) als unerlässlich für die Gruppierung identifiziert wird – und zwar aufgrund ihrer oder seiner strategischen Position im Netzwerk. Deshalb ist es wichtig nachzuvollziehen, ›wie und warum eine Verbindung hergestellt wurde‹: diese Logik würde ansonsten eine rasante Multiplizierung der Zielobjekte mit sich bringen. Jedoch ist die genaue Herstellung der Verbindungen und die dabei genutzten Kriterien für militärische Endbenutzer_innen oftmals nicht nachvollziehbar, da viele selbst keine gelernten Softwareexpert_innen sind[8]. Das ›wie‹ und ›warum‹ der Verbindung wird z.B. im Fall der Data Mining-Software *Analyst's Notebook* noch weniger nachvollziehbar, denn diese beinhaltet u.a. sogenannte ›intuitive‹ Mensch-Maschine-Interfaces, welche die Effekte der verwendeten Kategorien und Repräsentationen unsichtbar werden lässt (Bowker/Star 2000; Dourish 2001; Suchman 1994). Ein Beispiel einer eingebauten Kategorie ist die Annahme der SNA, dass aufständische Gruppierungen Netzwerke *sind*, in der dementsprechend die Zentralität von Akteur_innen durch die pure Quantität von Kontakten mit anderen Verdächtigen bestimmt wird. In diesem Zusammenhang haben Stohl und Stohl darauf hingewiesen, dass die SNA nicht wirklich zwischen der Fähigkeit sich zu vernetzen auf der Basis von Kommunikation und Konnektivität auf der einen Seite und »the ability to mobilize, control and coordinate members for specific planned acts« (Stohl/Stohl 2007: 110) unterscheiden kann. Relevante Kategorien für die Analyse von ›Lebensmustern‹ basieren dementsprechend auf problematischen Annahmen – zum Beispiel auf der Annahme, dass wiederholte Reisen auf bestimmten Routen, das Aufsuchen verdächtiger Orte oder das Kontaktieren von Verdächtigen immer auf die Signatur von Terrorist_innen verweist. Jeremy Scahill und Glenn Greenwald haben deutlich gemacht, dass nicht nur die Identifikation von

---

8 | *Bände spricht hier z. B die Selbstbeschreibung eines Analysten, wie man sie in der Datenbank IC Watch findet. Dort gibt er folgende Software-›Kompetenzen‹ an: »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-javor55587789OhioHIDTACriminalIntelligenceAnalystIntern2013-05-01.*

Zielobjekten, sondern auch deren physikalische Verortung und damit die Attacken selber, auf Metadaten basieren:

[…] 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/Greenwald 2014)[9]

In diesem Zusammenhang gab der pensionierte US-General und ehemalige Direktor der NSA und CIA Michael Hayden unverblümt zu: »We kill people based on metadata« (Cole 2013). Ein Effekt der Logik dieser Targeting-Methodologie lässt sich paradigmatisch im Dokument »Skynet. Courier Detection via Machine Learning« (National Security Agency, 2012), welches von Edward Snowden veröffentlich wurde, untersuchen. Gemäß dem NSA-Dokument wurde der renommierte Al Jazeera-Journalist Ahmad Muaffaq Zaidan wegen seiner Reisemuster, seinen Telefonverbindungen und aufgrund der Quellen, die er benutzt hat, auf eine Beobachtungsliste gesetzt. Er wird als Beispiel aufgeführt

»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/Greenwald/Fishman 2015).

Ahmad Muaffaq Zaidan wurde offensichtlich auf die Liste gesetzt, da er sich durch seine beruflichen Tätigkeiten als Journalist mit al-Qaida und Taliban Bewegungen beschäftigt und in diesem Zusammenhang auch Aufständische wie Osama Bin Laden kontaktiert und getroffen hat. Jeder (menschliche) Analyst, der die Landessprache spricht und sich mit der Politik und dem soziokulturellen Kontext von Pakistan auskennt, hätte schnell erkannt, dass die Kontakte des

---

[9] | *»[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/Greenwald 2014b).*

Journalisten auf seine beruflichen Aktivitäten zurück zu führen sind und nicht notwendigerweise auf terroristische Tätigkeiten hinweisen. Wird der Targeting-Prozess jedoch automatisiert – in einer Zeit, in der kompetente Analyst_innen rar sind[10] – wird der Prozess des Targeting nicht mehr nachvollziehbar und produziert immer mehr Verdächtige, die auf Tötungs- und Beobachtungslisten gesetzt werden.

Die ›Disposition Matrix‹ lässt sich als eine sich ständig weiterentwickelnde Datenbank verstehen, die nicht nur aus Biographien besteht, sondern auch die Ergebnisse aus Datenanalyse enthält, welche hauptsächlich auf der Grundlage von Metadaten erstellt wurden. Insgesamt ähnelt diese Analyse von sogenannten ›Lebensmustern‹ (pattern of life analysis) Strategien der Strafverfolgung, da hier primär Daten über kriminelles Verhalten gesammelt werden. Und obwohl die ›Disposition Matrix‹ zum Teil auf Narrativen ›terroristischer‹ Biographien aufbaut (z.B. de Goede 2013; Kessler und Wouter 2013), ist sie zugleich auch eine Suchvorrichtung, in der große Datenmengen zueinander in Relation gebracht und rekombiniert werden – um Profile der angeblich gefährlichsten Verdächtigen zu erstellen. Daraus resultiert, dass man Menschen offensichtlich nicht tötet, weil sie als hochrangige Mitglieder eines bestimmten ›terroristischen‹ Netzwerks identifiziert werden, sondern weil sie bestimmte Verhaltensweisen oder Verbindungsmuster aufzeigen, die entweder von Analyst_innen oder Software-Designer_innen als verdächtig eingestuft werden oder welche sich aus der Datenanalyse ›ergeben‹. Die Analyse soll »persistent anomalies in normal rhythms of activity, which are read as signs (›signatures‹) of imminent threat […] » zu erkennen geben, aber »[t]he principal limitation – and *the grave danger – lies in mistaking form for substance*« (Gregory 2013; meine Hervorhebung). Die quantitative Methodik kann keine qualitativen Unterschiede zwischen den Verbindungen der verschiedenen ›Knoten‹ machen und subsumiert diese deshalb als Teil der Terrornetzwerke. Dementsprechend werden die Verwandten, Freund_innen und Arbeitskolleg_innen, die mehrere Verbindungen zu Verdächtigen oder Zieleobjekten haben, in die Liste aufgenommen. Der Historiker und Journalist Gareth Porter weist in diesem Zusammenhang darauf hin, dass viele Menschen im südlichen oder östlichen Paschtunistan Handynummern von Taliban-Kommandeuren in ihren Mobiltelefonen haben, die als

---

10 | *Das wird u.a daran deutlich, dass das US-amerikanische Militär die Idee geäußert hatte, ›Reachback Research Centers‹ für die Human Terrain Teams zu bauen, von denen aus Sozialwissenschaftler_innen, Analyst_innen, und andere Expert_innen den kulturellen Kontext liefern solle (vgl. González/Price 2015); allgemein zum Thema (vgl. auch Engemann 2013).*

›Überlebensmechanismus‹ dienen – das Gleiche könnte auch auf Menschen in Wasiristan zutreffen. Und obwohl die in der ›Disposition Matrix‹ enthaltenen Zielobjekte als Personen identifiziert sind, sind die hochrangigen Ziele über ein Targeting-Verfahren erzeugt worden, das auf vordefinierten Kategorien beruht, keine kausalen Beziehungen herstellt und nur formal Beziehungsmuster auf der Grundlage von Metadaten beschreibt.

Auf der Grundlage von Methoden wie SNA, Geodatenanalyse oder Sentiment Analyse produzieren Analyst_innen Ziellisten. Das Wissen darüber ›wie und warum eine Verbindung erstellt wurde‹, geht während diesem vielschichtigen Prozess der Zusammenführung und Filterung von riesigen Mengen an Metadaten zwangsläufig verloren.

Keines dieser Probleme lässt sich durch eine genauere Definition von Terrorismus lösen, durch die Verfeinerung der Kriterien, die bestimmen, wer auf die Listen gesetzt wird oder die ›Perfektionierung‹ der Algorithmen – denn *der eigentliche Fehler, das buchstäbliche Verkennen von Form als Inhalt, ist integraler Bestandteil des Verfahrens.* Es scheint keine Erklärungen zu geben, die auf kausalen Zusammenhängen basieren, die nach Ursache und Wirkung fragen, um dann zu erklären, weshalb jemand als ›Terrorist_in‹ betrachtet wird, der oder die eine unmittelbare Bedrohung darstellt. Es gibt keine transparente oder konsistente Argumentation, die versucht, die Kriterien zu rechtfertigen und kohärent zu machen. In diesem Prozess scheint es nicht den Anspruch zu geben, Wahrheit zu produzieren oder zumindest mit einer gewissen Sinnhaftigkeit zu operieren. Der ›Lebensmuster‹-Ansatz stützt sich auf eine technowissenschaftliche Logik der Rekombination, (Ko-)relation und der Möglichkeiten – und diese Logik beruht stets auf sehr schwachen Wahrscheinlichkeiten und ist höchst konstruiert. Zugleich wird dieser Ansatz von dem Wunsch (oder der vermeintlichen Notwendigkeit) befeuert, immer mehr Daten zu sammeln: Denn je größer die Menge der gespeicherten Daten und je höher die Anzahl der möglichen Kombinationen dieser Ausbeuten (von Netzwerkknoten beispielsweise), desto mehr hochwertige Ziele können ›identifiziert‹ werden. Und es sind nicht nur die »hundreds of people [who] make incremental contributions to a well-oiled killing machine« (McNeal, 2014: 685), sondern auch diese innere Logik der postrelationalen Datenbanken und die Big-Data Analyse im Allgemeinen.

Aus dieser Perspektive heraus werde ich im Folgenden versuchen mit Hilfe der Science und Technology Studies (STS) und vor allem der Software Studies diese innere Logik sichtbarer zu machen und ein detaillierteres und materialbasiertes Verständnis dieser Praktiken zu entwickeln. Dieser Ansatz hat jedoch seine Grenzen, insofern die spezifischen Softwareprogramme des Targeting-Prozesses geheim gehalten werden und daher nicht für eine genauere

Analyse zur Verfügung stehen. Trotzdem scheint es mir sinnvoll, die Effekte und die allgemeinen Grundsätze moderner Datenbanken und Data Mining-Algorithmen nachzuvollziehen. Diese können entscheidend unser Verständnis des Targeting-Prozesses verbessern, denn dadurch wird die epistemologische Logik dieser ›killing machine‹ deutlich.

Die Epistemologie und Materialität von Datenbanken

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)

STS und vor allem die Software Studies haben darauf hingewiesen, dass Software heute ubiquitär geworden ist: »[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/French 2002: 309) Dies gilt allem voran auch für die heutige Kriegsführung und ihre militärische Organisation. Ich möchte deshalb die innere Logik von Datenbanken als auch von Techniken des *Data Mining* und des Machine Learning aufzeigen, indem ich ihre epistemologischen und materialen Grundlagen sichtbar mache – und das heißt die Methoden und Logiken zu analysieren, derer sich Analyst_innen bedienen um Ziele zu erstellen.

Im Folgenden werde ich auf die historische Verschiebung von der hierarchischen zur relationalen bzw. vor allem postrelationalen Datenbank eingehen und wie sie sich von einem Speichergerät zu einem Suchgerät entwickelt. Die postrelationale Datenbank kann als verteiltes System riesige, semi- oder unstrukturierte Datenmengen durchsuchen[11]. Schließlich werde ich Techniken des Maschinenlernens analysieren und dabei vor allem auf genetische Algorithmen eingehen. Aufzuzeigen wie Techniken des Data Mining in Verbindung mit postrelationalen NoSQL-Datenbanken auf automatisierten Prozessen eines systematisierten Tinkering und dem Prinzip der Rekombination

---

11 | *Strukturierte Daten beruhen auf einem zuvor festgelegten Datenmodell, während semi-strukturierte Daten nur lose und unregelmäßig strukturiert sind und insofern nicht in relationalen Datenbanken verarbeitet werden können. »(U)nstructured data do not have a defined data model or common identifiable structure« (Kitchin 2014: 6).*

aufbauen[12], hilft die ›Disposition Matrix‹ zu analysieren und zu erklären, wie es dazu kommt, dass auch durch die Technologie die Produktion und Sammlung von Daten, Verdächtigen und Zielobjekten weiter angetrieben wird.

Was ist eine Liste und was ist eine Datenbank?

Listen sind dazu da, um Dinge hinzuzufügen, zu kombinieren und zu ordnen, ohne dass es vorab eine vorgegebene Reihenfolge gäbe (Stäheli 2012: 234-236). Jede Liste ist so gesehen ein Werkzeug der Abstraktion und oftmals auch eine Antwort auf ein Problem. Und: »the criteria of selection are not fixed at the outset but evolve during the list's use« (ebd.: 237). Die Kriterien sind der Liste nicht inhärent und entsprechend können die Regeln der Aufnahme oder des Ausschlusses in die jeweilige Liste auch geändert werden.

Darstellungsformen (wie Listen oder Datenbanken) sind untrennbar mit Wissen verflochten (Goody 1977) und dieses Potential der Liste zur Abstraktion gründet in der damit einhergehenden Diskontinuität und Dekontextualisierung – anders wie wir es z.B. aus Narrativen (wie z.B. von Ursache und Wirkung) kennen, die auf einer vorgegebenen Struktur aufbauen. Nach Stäheli (2012) stellt die Liste eine Art (einfache) Datenbank dar. Datenbanken sind strukturierte Ansammlungen von Daten. Sie sind theoretisch unbegrenzt. Lev Manovich hat darauf hingewiesen, dass sie weder Anfang noch Ende haben und keine Entwicklung durchmachen. Sie erzählen keine Geschichten und haben keine integrale grammatische Struktur »Instead, […databases] are collections of individual items, where every item has the same significance as any other« (Manovich 2001: 218).

Datenbanken hingegen sind anders strukturiert – auf hierarchische Weise, netzwerkartig oder in postrelationaler Weise. Es ist wichtig, zwischen der traditionellen Form der Liste (oder der Datenbank) und einer neueren kulturellen Variante der Liste zu unterscheiden: der postrelationalen Datenbank[13].

Früher waren Datenbanken primär hierarchisch in einer baumartigen Struktur organisiert. Die Nutzerin musste für den Gebrauch dieser Datenbanken wissen, wie die Datenbank strukturiert ist und welche Daten sie enthält. In diesem Modell enthält jedes Datenelement eine physikalische Speicheradresse und die Art und Weise, wie Informationen abgerufen werden, hängt davon ab, wie die Daten organisiert sind. Diese Datenbanken sind weniger dynamisch als die relationalen, weil sie nur die Art von Fragen beantworten können, die den Programmierer_innen bewusst waren, als sie sie entworfen haben.

---

12 | *Hierzu siehe weiter unten.*

13 | *Ausführlich zum Medium Datenbank vgl. auch Burkhardt 2015.*

In den frühen 1970er Jahren haben Edgar F. Codd (1970) und andere relationale Datenbankmodelle entwickelt und machten es damit möglich, die Speicherung und den Abruf von Daten zu trennen (Dourish 2014; Kitchin 2014). In diesen Datenbanken werden Daten nicht nach einem hierarchischen, baumartigen Muster organisiert, welches sich von einer ›Wurzel‹ aus nach oben hin verzweigt, sondern in einer Tabelle, so dass jedes Segment von Daten in mehrfache Verbindungen zu anderen Elementen gebracht werden kann. Datenbanken wurden dadurch von einem Mittel der Organisation zu einer Suchmaschine (Gugerli 2009). Relationale Datenbanken sind höchst flexibel, dynamisch und offen strukturierte Systeme. Genau dies wurde nicht nur durch diesen Übergang von hierarchischen zu relationalen Datenbanken als Managementsysteme möglich, sondern auch durch die rasant steigende Leistung der CPUs. Die relationale Datenbank ist unerlässlich für das Management von komplexen, dynamischen und offenen Systemen in Echtzeit:

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)

Dies wurde das vorherrschende Datenbankmanagementsystem und ließ die Datenbank von einer Speicher- und Abfragemaschine zu einer Suchmaschine werden (Hildebrandt/Gutwirth 2008; Amoore 2013). Im frühen 21. Jahrhundert wurde dann die postrelationale NoSQL (= not only SQL) Datenbank entwickelt. Mittels dieser Datenbanken ist es möglich, enorme Datenmengen zu speichern und abzufragen sowie auch halb- oder unstrukturierte Daten zu verwalten – dies ist beispielsweise bei stark zentralisierten Web-Services wie Google, Facebook oder den Datenbanken der Geheimdienste erforderlich (Kitchin 2014: 86). Postrelationale Datenbanken sind auf mehrere Servern verteilt, die flexibel organisiert sind und als einfach erweiterbare Big-Data-Systeme funktionieren: »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) Während die traditionelle Liste ein perfektes Mittel ist, um jegliche Daten zu (re-)kombinieren und miteinander in Verbindung zu setzen, ermöglichen das Design der NoSQL-Datenbank als auch die Techniken des Data Mining den »access to very large, exhaustive, dynamic, fine-grained, indexical, varied, relational, flexible and scalable data« (ebd.: 79). Neue Formen von Big-Data-Analyse werden durch den veränderten Aufbau der Datenbanken, durch

die erhöhte Rechenleistung sowie deren verteilte Infrastrukturen, die durch Technologien wie MapReduce verwaltet werden (ebd.: 86f), möglich. Gegenwärtig sind es jedoch nicht nur die neuartigen Datenbankstrukturen, welche die Art und Weise, Daten zu kombinieren und abzufragen umgestaltet, sondern auch die Algorithmen des *Data Minings*: »Together, data structures and algorithms are two halves of the ontology of the world according to a computer« (Manovich 2001: 223). Wie zuvor bereits erwähnt, sind Techniken der sog. Wissensentdeckung (›Knowledge Discovery‹) sprich Data Mining wie z.B. Text Mining, Sentiment-Analyse oder die Analyse sozialer Netzwerke die maßgeblichen Techniken bei dem Versuch, relevante Muster aus den Stapeln von militärischen und zivilen Informationen zu extrahieren.

Eine neue technowissenschaftliche Rationalität

Die geschilderte Verschiebung von hierarchischen zu postrelationalen, verteilten Datenbanken und die Entstehung neuer, flexibler Algorithmen können als Teil einer grundlegenden Rekonfiguration der Epistemologie und Ontologie der Wissenschaften im Zeitalter der ›Technoscience‹ verstanden werden.

Technowissenschaftliche Kultur zeichnet sich dadurch aus, dass das alltägliche Leben weitgehend durch technowissenschaftliche Diskurse und Praktiken durchdrungen ist. Letztere sind auch zentral für die Rekonfiguration von kulturell umkämpften Begriffen wie ›Natur‹, ›Körper‹ oder ›Subjektivität‹. Die Verschmelzung von Wissenschaft und Technik zur Technowissenschaft spätestens seit den 1980er Jahren ist ein umfassendes unternehmerisches und pragmatisches Projekt geworden, in welchem der Technologie eine führende Rolle bei der Entwicklung von innovativen Lösungen für die Probleme der Gesellschaft zugeschrieben wird. Wie ich an anderer Stelle argumentiert habe (Weber 2003/2011), ist die neue technowissenschaftliche Rationalität wesentlich flexibler und zeichnet sich durch ein starkes Interesse am Unberechenbaren, an Prozessen der Emergenz und dem Unbekannten aus. Diese epistemologische Verschiebung ist auch in eine globalisierte Medienkultur eingebettet, in der neue Medien keine Geschichte mehr erzählen, denn sie sind »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, 219; meine Hervorhebung). Diese neue epistemologische Logik hat ihre historischen Wurzeln in der Systemtheorie und der Kybernetik, welche zusammen die Grundlage für die gegenwärtig vorherrschenden technowissenschaftlichen Diskurse und Praktiken bilden (Weber 2003/2010). Technowissenschaften wie die Robotik, KI und Informatik sind wesentlich von diesen neuen Epistemologien und Ontologien bestimmt, die mit neuen

konzeptionellen Rahmen, Identitäten und Regierungsformen einhergehen (vgl. Haraway 1991 [1985]; Latour 1986). Die wichtigsten Merkmale der technowissenschaftlichen Rationalität sind formalisiertes und systematisiertes Tinkering, sowie Trial-und-Error-Verfahren, Bottom-up-Suchheuristiken und Post-Processing, mit dem komplexe Probleme gelöst werden sollen.

Adaption, Imitation und Imagination sind dabei die wichtigsten Mittel für eine Rationalität, die darauf abzielt, das Unberechenbare zu erschließen und überschüssige Prozesse durch technische Mittel nutzbar zu machen (Haraway 1991 [1985]; Weber 2003; Nordmann 2006). Im Gegensatz zur modernen wissenschaftlichen Rationalität ist diese Rationalität nicht an den intrinsischen Eigenschaften von Objekten interessiert (Organismen, Maschinen), sondern konzentriert sich stattdessen auf ihr Verhalten, ihre Beziehungen und auf mögliche Rekombinationen von Modulen, Code-Fragmenten sowie das Erstellen von Systemblöcken. So ersetzt die Technowissenschaft zunehmend die Prinzipien der Repräsentation und des Verstehens mit den Prinzipien der Investigation und Intervention (Weber 2003). Diese neue post-Newtonsche Rationalität hat sich auch in die Logik der Liste, des Datensammelns und der Suchheuristiken im sogenannten globalen Krieg gegen den Terror eingeschrieben. Louise Amoore hat kürzlich darauf hingewiesen, dass Techniken wie »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‹

Tötungslisten aber auch Listen im Allgemeinen sind flexibel und dynamisch, weil sie nicht notwendigerweise auf klaren Auswahlkriterien basieren. Es kann alles Mögliche zu einer Liste hinzugefügt werden, wenn sich die Regeln für die Auswahl ständig ändern. Tötungslisten wie die ›Disposition Matrix‹ basieren auf Suchverfahren und -maschinen, die dafür entwickelt wurden, riesige Datenmengen zu analysieren – vom Drohnenvideomaterial bis zu den Inhalten der sozialen Netzwerke. Sie sollen dieses riesige Datenuniversum durchsuchen in der Hoffnung, dass man so sicherheitsrelevante Aspekte (›Connecting the Dots‹) miteinander in Verbindung bringen kann. Es sollen versteckte Bedrohungen oder ›Terrorist_innen‹ gefunden werden, indem Daten automatisch angepasst werden, Algorithmen nach Mustern suchen und Chatrooms nach Schlüsselwörtern durchsucht werden. Gesucht werden keine vorab definierten Einheiten, sondern Muster, Unregelmäßigkeiten und Möglichkeiten.

In den 1980er Jahren entstanden neue Data Mining-Algorithmen – wie z.B. genetische Algorithmen – die diese Weise der Suche ermöglichen. Klassische

Algorithmen arbeiten primär in einer ›Top-down‹-Logik, um das vorgegebene Problem direkt in einer rational-kognitiven Weise zu lösen. Genetische Algorithmen funktionieren eher ›Bottom-up‹ – normalerweise in dem man versucht das Problem zu umschreiben und sich dann auf eine Lösung hinzubewegen. Innerhalb dieser Logik ist der effektivste Lösungsweg, eine gute Beschreibung des Problemraums zu erstellen, robuste Parameter zu definieren und dann mit Hilfe von Trial-und Error-Verfahren – die ich hier auch als systemtisches ›Tinkering‹ bezeichnet habe – genau diesen Raum zu durchsuchen.

Das Objekt der Suche bzw. Untersuchung ist nicht ein genau definiertes Problem, sondern eher ein sehr breit definiertes Ziel unter angegebenen Randbedingungen unter denen man das Ziel erreichen soll – etwa einen Terroristen zu finden. Diese Weise des Vorgehens weicht signifikant von den traditionellen Werten der Wissenschaft ab – man denke an das Ziel einer objektiven Beschreibung universaler Gesetze, die Repräsentation von Natur, Konsistenz oder auch die Subjekt-Objekt-Trennung. Diese neue Technorationalität basiert auf einem systematisiertem Tinkering und darauf, die Randbedingungen von emergenten Verhalten zu erforschen – in einer Weise, die nicht wirklich reproduzierbar ist. Dieses Vorgehen nutzt eine Suchheuristik, Algorithmen, welche die Evolution via Tinkering und Techniken des Post-Prozessierens simulieren wollen. Ich möchte dafür ein Beispiel geben. Im Jahre 1992 veröffentlichte John Holland einen Artikel mit dem Titel »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). Es mutet seltsam an, dass hier ein Wissenschaftler verspricht, dass er eine Lösungsstrategie für Probleme entwickelt, die man (selbst) noch nicht wirklich verstanden hat. Aber gerade dieses Vorgehen könnte man als ein Leitmotiv der Technorationalität betrachten.

Holland entwickelte sogenannte selbstoptimierende, selbstlernende Computerprogramme für diverse Aufgaben – wie z.B. einen Algorithmus für das Sortieren von Zahlen. Dieser arbeitet folgendermaßen: Zuerst wird ein Fitnessfaktor für die entsprechende Aufgabe definiert. Dann produziert ein Computer nach dem Zufallsverfahren Algorithmen, die entsprechend dem Fitnessfaktor, der den jeweiligen ›Erfolg‹ angibt, gerankt und ausgewählt werden. Ein festgelegter Anteil der besten Algorithmen wird reproduziert, während alle anderen Programme gelöscht werden. Die erfolgreichen Algorithmen werden miteinander gekreuzt, indem man gleich lokalisierte Teile der Algorithmen untereinander austauscht. Dann fängt man wieder von vorne an. Diese Prozedur kann man als ›smartes‹, optimiertes und systematisiertes Trial-und-Error-Verfahren beschreiben, da es in iterativen Schleifen solange

durchgeführt wird, bis eine annehmbare Lösung des jeweiligen Problems gefunden wurde.

Und obwohl man auch Abermillionen von unnützen Programmen produziert, entwickelt man neue Lösungen mit Hilfe der genetischen Algorithmen auf der Grundlage von prozessorstarken Rechnern und der entsprechenden Zeit. Diese Bottom-up-Methode kann mit traditionellen, rational-kognitiven Top-down-Verfahren durchaus mithalten bzw. produziert oft sogar bessere Resultate.

Diese transklassische Weise des Rechnens bzw. des Data Minings von Information sind heute zentrale Verfahren der Technowissenschaftskultur, in denen die Welt primär als flexibel, offen und unvorhersehbar rekonfiguriert wird, als ein Ort der Kombination, der Rekombination und des Redesigns (Haraway 1985/1991). Genetische Algorithmen sind heute wichtige Anwendungen im Bereich der Data Mining-Verfahren. Die Datenbank (oder spezifische Teile davon) werden als Suchraum definiert und genetische Algorithmen durchsuchen riesige Datenmengen nach Mustern, Beziehungen, Assoziationen und ›Anomalien‹. Auf diese Weise können Daten klassifiziert (indem man bekannte Kategorien auf neue Daten anwendet) und gruppiert werden (indem man nach noch unbekannten Gruppen oder Strukturen in den Daten) sucht und Muster können extrahiert werden. Diese können dann dafür benützt werden, um Vorhersagen zu machen, Hypothesen zu testen und Suchstrategien zu optimieren (z.B. um optimale Assoziationsregeln zu finden). Zufällig produzierte Relationen und Rekombinationen sind zentral für dieses Data Mining der ›Disposition Matrix‹ und speist den Wunsch nach immer mehr Daten, um noch mehr ›Treffer‹ – sprich Verdächtige – produzieren zu können.

Führt man sich die aktuellen präemptiven Sicherheitsmaßnahmen vor Augen, kommen einem diese technowissenschaftlichen Strategien irgendwie bekannt vor: Das systematische Scannen eines (vor-definierten) Raums nach Lösungsmöglichkeiten, die endlose Rekombination von Daten in der Hoffnung eine mögliche Bedrohung oder einen ›Gefährder‹ auszumachen. Das riesige und permanent wachsende Ausmaß an Daten wie sie von der NSA gesammelt werden, korrespondiert mit einer Form von Technorationalität, die den ›Bedarf‹ an immer mehr Daten antreibt.

Im nächsten Abschnitt werde ich ausführlicher die Affinitäten zwischen dieser neuen Technorationalität mit ihrer offenen Suchheuristik und der postmodernen, präemptiven Technosecurity, die alle möglichen Bedrohungen vorwegnehmen und abwehren möchte, diskutieren. Ich möchte verdeutlichen, dass diese Praktiken der Imagination partiell in der Sicherheitskultur des Kalten Krieges verwurzelt sind und wie sie sich aber auch von der heutigen Technosicherheitskultur unterscheiden.

Die präemptive Kultur der Technosicherheit

Die Eigenschaften dieser neuen Technorationalität finden sich auch sehr ausgeprägt in unseren aktuellen Kultur präemptiver Technosicherheit wieder, die primär darauf konzentriert ist, die ›unknown unknowns‹ (Daase/Kessler 2007) – unbekannte Risiken von unbekannten Akteur_innen – zu antizipieren, anstatt sich mit empirisch und kausal begründeten objektive(re)n und konkreten Bedrohungen von identifizierbaren Risikofaktoren auseinanderzusetzen (Aradau et al. 2008).

Dagegen konzentriert man sich auf elaborierte Überwachungstechnologien wie Data Mining oder Computersimulation (Bogard 2012), auf Techniken der Szenarioplanung oder gar auf die pure Imagination von möglicherweise noch verheerenden Bedrohungen (de Goede 2008), die sich alle um Fragen der Ungewissheit und von unberechenbaren Risiken drehen (Salter 2008; Bröckling et al. 2011).

Dass hier die geschilderte Technorationalität die Targeting-Methoden wesentlich bestimmt, wird auch daran deutlich, wie die gezielten Tötungen etwa vom CIA-Direktor John Brennan gerechtfertigt werden:

[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; meine Hervorhebung)

Wieder sieht man wie vage die Kriterien für ein hochgeranktes Ziel sind: Man muss kein erfahrener al-Qaida-Führer sein, um auf Tötungsliste namens ›Disposition Matrix‹ zu landen – einen Angriff nur zu planen oder auch nur die entsprechenden Fähigkeiten für einen solchen Angriff zu haben scheint ausreichend zu sein. Das lässt einen unglaublichen Interpretationsspielraum: Wann weiß man sicher, dass jemand einen Anschlag plant? Nur der Besitz von spezifischen Fähigkeiten allein scheint schon auszureichen, um jemanden zu einem Verdächtigen zu machen oder eventuell sogar eine präemptive Tötung (!) zu rechtfertigen. Es wird offensichtlich, dass »(t)he logic of preemption prioritizes the power of imagination over the power of fact – suspicions over evidence« (Salter 2008: 243). Potenzielle Bedrohungen werden so breit definiert, dass im Prinzip jede/r eine Gefahr in der nahen Zukunft schon darstellen kann, wenn sich die Analyse primär auf Indizien und die Beobachtung von Verhalten stützt. Dieses Vorgehen ist diametral zu einem klassischen wissenschaftlichen

Verständnis von Ursache und Wirkung – aber sie passt erstaunlich gut zur technorationalen Logik des Tinkerings. Die epistemologische Grundlage für das Risikomanagement sind inkrementelle und automatisierte Prozesse der Re-/Kombination von Daten – ein Verfahren, das primär auf der Basis von vordefinierten Kategorien, aber auch auf Imagination basiert, insofern die Projektion von (un-)möglichen Szenarien, Verbindungen und Zusammenhängen eine zentrale Rolle spielt. Man betrachtet halbautomatisierte Technologien der prädiktiven Analyse, präemptive Handlungen, Echtzeitverfolgung und -targeting als angemessene Antwort auf die Herausforderung von unvorhersehbaren Risiken – ein Ansatz, der der klassischen Hoffnung auf den ›technological fix‹ verpflichtet ist und insofern auf technische Überlegenheit setzt (vgl. Der Derian 2009; De Goede 2008).

Allerdings ist der Gebrauch von Imagination im Rahmen von Sicherheitspraktiken nicht völlig neu. Worst-Case-Szenarien und Computersimulationen, die auf Techniken der Imagination aufbauen, wurden schon im Kalten Krieg eingesetzt. Die einmalige Bedrohung eines nuklearen Krieges wie sie in den 1940er Jahren entstand, ließ eine völlig neue und Situation der Unsicherheit entstehen – letztere konnte man weder auf der Basis von Erfahrung noch durch Experimente in den Griff bekommen. In den 1960ern entwarfen dann berühmte ›defence intellectuals‹ wie z.B. der US-amerikanische RAND-Experte Hermann Kahn (1960) alle (un)möglichen Szenarien des Nuklearangriffs und -gegenangriffs – jenseits jeglicher Wahrscheinlichkeitsüberlegungen (Kaplan 1983; Ghamari-Tabrizi 2005). In diesen Szenarien wurde mit der Möglichkeit von Hundert Millionen von Toten gespielt, mit ausgesprochen unwahrscheinlichen Überlebensstrategien oder biopolitische Maßnahmen für ein postnukleares (!) Zeitalter entworfen. Doch während man im Sicherheitsdiskurs des Kalten Krieges immerhin mit einer konkreten Situation und konkreten Akteur_innen arbeitete, drehen sich die heutigen Sicherheitsdiskurse zunehmend um rein possibilistische Bedrohungen und mögliche Akteur_innen.

Nun wird Unsicherheit schon sehr lange durch statistische Verfahren zum Teil von Kalkulationen gemacht: »[…] 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 market« (Amoore 2009: 52). Aber aktuell verschiebt sich der Fokus immer mehr – es gibt einen »*change in emphasis from the statistical calculation of probability to the algorithmic arraying of possibilities* […]« (Amoore 2013: 23; meine Hervorhebung). Jene Algorithmen die systematisch Möglichkeiten eruieren, dominieren zunehmend die Diskurse und Praktiken der zivilen und militärischen Sicherheitsagenturen.

Sie ersetzen die traditionelle Frage nach der Wahrscheinlichkeit mit der »imagination of possibilities« (ebd.: 24).

In der Angst potenzielle Singularitäten zu verpassen, rekombiniert man Daten solange, bis man einen spezifischen Problemraum systematisch durchgespielt hat – auch wenn 99 Prozent der Lösungen völlig unbrauchbar und unwahrscheinlich sind, wenn sie auch technisch möglich wären. Was man zuvor primär mit Hilfe von Worst-Case-Szenarien getestet hat, wird nun mit Hilfe eines systematisierten und formalisierten Tinkering mit Hilfe von Data Mining und großen, flexiblen, postrelationalen Datenbanken mit Unmengen von ›Big Data‹ bearbeitet.

Entsprechend möchte ich im nächsten Abschnitt den Einfluss und die Konsequenzen dieser Amalgamisierung einer neuen Technorationalität und Technosicherheitskultur mit Blick auf die Rolle der ›Disposition Matrix‹ analysieren.

Das Unvorhersehbare als Ressource: Technorationalltät und die ›DIsposItIon MatrIx‹

Post-relationale Datenbanken und genetische Algorithmen könnte man als paradigmatische Medien dieser post-Newtonschen Rationalität sowie als bevorzugte Medien der Intelligence-Community bezeichnen, welche alles daran setzt, diese Welt möglichst engmaschig zu kartieren – eine Welt, die als inkohärent, unvorhersehbar und voller Risiken wahrgenommen wird (Aradau/ van Munster 2007). Durch das Sammeln von riesigen Datenmengen mit Hilfe von menschlicher und datenzentrierter Aufklärung (inklusive der Daten aus sozialen Netzwerken) will man Surplus-Prozesse emergenten Verhaltens ausbeuten.

Man durchsucht die Datenbanken meist auf einer quantitativen bzw. assoziativen Basis, mit der Hilfe von flexiblen Algorithmen, die nach Links, Verbindungen, Ähnlichkeiten oder Mustern suchen. Diese Logik folgt nicht jener von Ursache und Wirkung, sondern einer der Präemption oder der Possibilität. Im Versuch die (vermeintlichen?) ›unknown unknowns‹ in den Griff zu bekommen, stützt man sich nicht mehr auf Zurechenbarkeit und traditionelle wissenschaftliche Strenge um Bedrohungen zu bekämpfen, sondern auf die technische Ausbeutung von Zufall und Imagination mit Hilfe von systematisiertem Tinkering und formalisierten Prozessen von Trial-und-Error. Entsprechend dieser datengetriebenen Logik intensiver (Re-)Kombination kann jede/r zur Zielscheibe werden:

Über die Sammlung riesiger Mengen von Überwachungsdaten »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).

Die objektive Repräsentation der Welt, der klassische Anspruch traditioneller Naturwissenschaften, spielt in dieser technowissenschaftlichen Logik kaum eine Rolle mehr – wenn auch Politiker_innen, die Polizei, das Militär und die Geheimdienste die wissenschaftliche Validität des Verfahrens in ihrem öffentlichen Legitimationsdiskurs verteidigen.

Wie schon ausgeführt: ein zentraler Teil der Konstruktion der ›Disposition Matrix‹ beruht auf ausgesprochen vagen Kategorisierungen davon, was als Terrorismus und als ein zentraler Knoten im Netzwerk des Terrorismus betrachtet wird.

Die ›Disposition Matrix‹ beruht auf der Geheimhaltung darüber, was jemanden ›auszeichnet‹, um in die Liste aufgenommen zu werden oder das Ziel von einer gezielten Tötung via Drohne oder Razzia zu werden. Die ›Entscheidung‹ beruht auf Metadaten und Data Mining-Methoden wie z.B. soziale Netzwerkanalyse (SNA) – eine Methode, die selbst den Analyst_innen selbst nicht durchsichtig ist und oft einer rein quantitativen Logik folgt, die jeglichen sozialen, politischen und kulturellen Kontext ignoriert, in dem die Daten stehen.

Diese Logik beruht nicht auf objektiven, reproduzierbaren Methoden in der Weise, wie wir sie aus den Naturwissenschaften kennen. Es gibt keine kohärente Erzählung darüber, warum eine bestimmte Person gefährlicher ist als eine andere und warum sie unbedingt hingerichtet werden muss. Während numerische Listen Prioritäten aufstellen, die manche Leute über andere präferieren (bei dem z.B. eine Person als der gefährlichste Terrorist signifiziert wird), sammelt eine Datenbank jede verfügbare Information. Die Art und Weise, wie Muster ›erkannt‹ werden, ändert sich mit jedem neuen hinzugefügten Informationsdetail. Im Rahmen dieser Technorationalität (die jegliche auch unwahrscheinliche Möglichkeit vorwegnehmen will) ist es unmöglich zu erklären, warum jemand möglicherweise der gefährlichste Terrorist oder der zentrale Knoten im Netzwerk ist. Dieses Verfahren möchte jegliche mögliche Gefahr eliminieren. Und in dieser Logik ist die Datenbank das perfekte Medium für präemptive Sicherheitsmaßnahmen, da sie nicht auf der Logik von Ursache und Wirkung aufbaut. Sie weitet den Suchraum aus und bietet immer wieder neue Muster von möglichen Netzwerken an.

Es geht hier nicht nur darum, dass »extraordinary and exclusionary political measures are activated through the invocation of an existential threat« (Opitz 2011: 94), die neue Technorationalität, welche das Unvorhersehbare durch systematisierte Suchpraktiken zur Ressource macht, liefert auch eine neue Basis für die Sicherheitskultur – eine Kultur, die davon getrieben ist, möglichst jedem

auch noch so vagen, sprich possibilistischem, Risiko zuvorzukommen. Angesichts dieser dominanten Technorationalität erscheinen dann auch illiberale Praktiken wie schwarze Listen und gezielte Tötungen zunehmend ›rational‹. Zugleich macht man den großen Einfluss der nichtmenschlichen Handlungsfähigkeit von Algorithmen und Datenbanken unsichtbar, in dem man die Macht des Souverän in den Vordergrund stellt: An den Terror-Dienstagen ist es (so scheint es) primär der Souverän der über Tod und Leben entscheidet.

Danksagung

Ich danke Louise Amoore, Marieke de Goede, Derek Gregory, Anna Leander, Urs Stäheli, Lucy Suchman und vielen anderen Kolleg_innen, die wertvolle Hinweise zum Text gaben, als ich den Text auf dem COST Workshop »The Politics of List: Law, Security, Technology« in Canterbury an der Kent Law School, Universität von Kent, im November 2013 sowie während des Symposium »Security by Remote Control« am Centre for Science Studies an der Lancaster Universität im Mai 2014 präsentiert habe. Mein herzlicher Dank geht auch an die vier anonymen Reviewer_innen, die mit ihren ausgesprochen kenntnis- und hilfreichen Kommentaren zur weiteren Klärung und Verbesserung meiner Überlegungen beitrugen. Kathleen Cross und Maike Niehaus danke ich für die ausgezeichnete redaktionelle Arbeit.

Literatur

Amoore, Louise (2013): *The Politics of Possibility. Risk and Security Beyond Probability*. Durham, London: Duke University Press. DOI: https://doi.org/10.1215/9780822377269

Amoore, Louise (2009): »Algorithmic War: Everyday Geographies of the War on Terror«. In: *Antipode: A Radical Journal of Geography* 41: 49-69. DOI: https://doi.org/10.1111/j.1467-8330.2008.00655.x

Aradau, Claudia/Lobo-Guerrero, Luis/Van Munster, Rens (2008): »Security, Technologies of Risk, and the Political: Guest Editors' Introduction«. In: *Security Dialogue* 39 (2-3): 147-154. DOI: https://doi.org/10.1177/0967010608089159

Aradau, Claudia/Van Munster, Rens (2007): »Governing Terrorism Through Risk: Taking Precautions, (un)Knowing the Future«. In: *European Journal of International Relations* 13 (1): 89-115. DOI: https://doi.org/ 10. 11 77/ 1354066107074290

Becker, Jo/Shane, Scott (2012): »Secret ›Kill List‹ Proves a Test of Obama's Principles and Will«. In: *New York Times*. 29.05.

Belcher, Oliver Christian (2014): *The Afterlives of Counterinsurgency: Postcolonialism, Military Social Science, and Afghanistan 2006-2012*. PhD thesis. https://circle.ubc.ca/bitstream/handle/2429/45520/ubc_2014_spring_belcher_oliver.pdf?sequence=5

Bogard, William (2012): »Simulation and Post-panopticism«. In: Kirstie Ball/Kevin Haggerty/David Lyon (Hg.): *Routledge Handbook of Surveillance Studies*. New York: Routledge: 30-37. DOI: https://doi.org/10.4324/9780203814949. ch1_1_b

Bowker, Geoffrey C./Star, Susan Leigh (2000): *Sorting Things Out: Classification and Its Consequences.* Cambridge, MA: MIT Press.

Brennan, John O. (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‹«. 30.04. www.wilsoncenter.org/event/the-efficacy-and-ethics-us-counterterrorism-strategy

Bröckling, Ulrich/Krasmann, Susanne/Lemke, Thomas (2011): *Governmentality: Current Issues and Future Challenges*. New York: Routledge.

Burkhardt, Markus (2015): *Digitale Datenbanken: Eine Medientheorie im Zeitalter von Big Data.* Bielefeld: transcript. http://fox.leuphana.de/portal/de/publications/digitale-datenbanken(67e82b95-7d1e-49f1-b904-ffd3dde2ca0a). html DOI: https://doi.org/10.14361/9783839430286

Codd, Edgar F. (1970): »A Relational Model of Data for Large Shared Data Banks«. In: *Communications of the ACM* 13 (6): 377-387. DOI: https://doi.org/10.1145/362384.362685

Cole, David (2013): »We Kill People Based on Metadata«. In: *The New York Review of Books*. 15.08. www.nybooks.com/articles/archives/2013/aug/15/nsathey-know-much-more-you-think/?insrc=rel

Currier, Cora/Greenwald, Glenn./Fishman, A. (2015): »US Government Designated Prominent Al Jazeera Journalist as ›Member of Al Qaeda‹«. In: *The Intercept*. 08.05. https://firstlook.org/theintercept/2015/05/08/u-s-government-designated-prominent-al-jazeera-journalist-al-qaeda-member-putwatch-list/

Daase, Christopher/Kessler, Oliver (2007): »Knowns and Unknowns in the ›War on Terror‹: Uncertainty and the Political Construction of Danger«. In:

Security Dialogue 38 (4): 411-434. DOI: https://doi.org/10.1177/0967010607084994

De Goede, Marieke (2008): »Beyond Risk: Premediation and the Post-9/11 Security Imagination«. In: *Security Dialogue* 39 (2-3): 155-176. DOI: https://doi. org/10.1177/0967010608088773

De Goede, Marieke (2013): »The Politics of Security Listing. Classification, Criteria, Consequence, Critique«. Vortrag. COST-Workshop: *The Politics of Lists: Law, Security, Technology*. 31.10., 31 – 01.11.: Kent Law School.

Department of Defense (2007): »Dictionary of Military and Associated Terms«. www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

Der Derian, James (2009): *Virtuous War: Mapping the Military-industrial-media-entertainment Network*. 2. Auflage. New York: Routledge.

de Young, Karen (2012): »A CIA Veteran transforms US Counterterrorism Policy«. In: *Washington Post*. 24.10. http://articles.washingtonpost.com/2012-10-24/world/35499428_1_drone-strikes-brennan-obama-administration

Dourish, Paul (2001): *The Foundations of Embodied Interaction*. Cambridge, MA: MIT Press.

Dourish, Paul (2014): »NoSQL: The Shifting Materialities of Database Technology«. In: *Computational Culture* 4 http://computationalculture.net/article/ no-sql-the-shifting-materialities-of-database-technology

Engemann, Christoph (2013): »Human Terrain System: Soziale Netzwerke und die Medien militärischer Anthropologie«. In: Inge Baxmann/Timon Beyes/Claus Pias (Hg.): *Soziale Massen – Neue Medien*. Berlin; Zürich; Paris: Diaphanes: 205-230.

Gettinger, Dan (2015): »The Disposition Matrix«. In: *Center for the Study of Drones Blog*. 25.04. http://dronecenter.bard.edu/the-disposition-matrix/

Ghamari-Tabrizi, Sharon (2005): *The Worlds of Herman Kahn: The Intuitive Science of Thermonuclear War*: Harvard University Press. DOI: https://doi. org/10.4159/9780674037564

González, Roberto J. (2015): »Seeing into Hearts and Minds. Part 2. ›Big Data‹, Algorithms and Computational Counterinsurgency«. In: *Anthropology Today* 31(4): 13-18. DOI: https://doi.org/10.1111/1467-8322.12188

González, Roberto J./Price, David (2015): »Remaking the Human Terrain: The US Military's Continuing Quest to Commandeer Culture«. In: *www.counterpunch.org*. 31.07. www.counterpunch.org/2015/07/31/remaking-the-hu man-terrain-the-us-militarys-continuing-quest-to-commandeer-culture/

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

Greenwald, Glenn (2012): »Obama moves to make the War on Terror permanent«. In: *The Guardian*. 24.10. www.theguardian.com/commentisfree/2012/oct/24/obama-terrorism-kill-list

Gregory, Derek (2013): »Theory of the Drone 3: Killing Grounds«. In: *Geographical Imaginations Blog*. 29.07. http://geographicalimaginations.com/2013/07/29/theory-of-the-drone-3-killing-grounds/

Gregory Derek (2012): »I don't like Tuesdays«. In: *Geographical Imaginations Blog*. 26.10. http://geographicalimaginations.com/2012/10/26/i-dont-liketuesdays/).

Gugerli, David (2009): *Suchmaschinen. Die Welt als Datenbank*. Frankfurt a.M.; New York: Suhrkamp.

Gutwirth, Serge/Hildebrandt, Mireille (2010): »Some Caveats on Profiling«. In: Serge Gutwirth/Yves Poullet/Paul de Hert (Hg.): *Data Protection in a Profiled World*. Dordrecht: Springer: 31-41. DOI: https://doi.org/10.1007/97890-481-8865-9_2

Haraway, Donna (1991 [1985]): »Manifesto for Cyborgs: Science, Technology, and Socialist Feminism in the 1980s«. In: Haraway, Donna (1991): *Simians, Cyborgs, and Women: the Reinvention of Nature*. London; New York: Routledge: 149-181.

Hildebrandt, Mireille/Gutwirth, Serge (2008): *Profiling the European Citizen. Cross-Disciplinary Perspectives*. Dordrecht: Springer. DOI: https://doi.org/10.1007/978-1-4020-6914-7

Holland, John H. (1992): »Genetic Algorithms Computer programs that ›evolve‹ in ways that resemble natural selection can solve complex problems even their creators do not fully understand«. In: *Scientific American* 267: 66-72. DOI: https://doi.org/10.1038/scientificamerican0792-66

Humphrey, David (1984): »On the Tuesday Lunch at the Johnson White House: a preliminary assessment«. In: *Diplomatic History* 8: 81-101. DOI: https://doi.org/10.1111/j.1467-7709.1984.tb00402.x

ICWatch (Intelligence Community Watch) (2015): 05.05. https://icwatch.wikileaks.org/

Joint Warfighting Center (2011): *Joint Doctrine Support Division. Commander's Handbook for Attack the Network*. Version 1.0. Suffolk; Virginia. 20.05. www.dtic.mil/doctrine/doctrine/jwfc/atn_hbk.pdf

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

Kaplan, Fred (1983): *The Wizards of Armageddon*. New York: Simon and Schuster.

Kessler, Oliver/Wouter, Werner (2013): »A Grim Debating Society«. Vortrag, COST-Workshop: *The Politics of Lists: Law, Security, Technology*. 31.10., 31 – 01.11.: Kent Law School.

Kitchin, Rob (2014): *The Data Revolution. Big Data, Open Data, Data Infrastructures & Their Consequences*. Los Angeles: Sage. DOI: https://doi.org/10.4135/9781473909472

Krebs, Valdis (2002): »Uncloaking Terrorist Networks«. In: *First Monday* 7 (4). http://firstmonday.org/ojs/index.php/fm/article/view/941/863/ DOI: https://doi.org/10.5210/fm.v7i4.941

Latour, Bruno (1986): *Science in Action*. Milton Keynes: Open University Press.

Manovich, Lev (2001): *The Language of New Media*. Cambridge, MA: MIT Press.

McNeal, Greg (2014): »Kill-Lists and Accountability«. In: *Georgetown Law Journal* 102: 681-794.

Miller, Greg (2012): »Plan for Hunting Terrorists Signals US Intends to Keep Adding Names to Kill Lists«. In: *The Washington Post*. 23.10. www.washingtonpost.com/world/national-security/plan-for-hunting-terrorists-signalsus-intends-to-keep-adding-names-to-kill-lists/2012/10/23/4789b2ae-18b3-11e2-a55c-39408fbe6a4b_story.html

Miller, Greg/Tate, Julie (2011): »CIA shifts focus to killing targets«. In: *The Washington Post*. 01.09. www.washingtonpost.com/world/national-security/cia-shifts-focus-to-killing-targets/2011/08/30/gIQA7MZGvJ_story.html

National Counterterrorism Center (NCTC) (2014): *Watchlisting Guidance*. https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/ HASH01d1/4a00c36e.dir/doc.pdf

National Security Agency (2012): *Skynet. Courier Detection via Machine Learning*. 6.06. https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASHc939.dir/doc.pdf

Nordmann, Alfred (2006): »Collapse of Distance: Epistemic Strategies of Science and Technoscience«. In: *Danish Yearbook of Philosophy* 41: 7-34. DOI: https://doi.org/10.1163/24689300_0410102

Opitz, Sven (2011): »Government Unlimited: The Security Dispositif of Illiberal Governmentality«. In: Ulrich Bröckling/Susanne Krasmann/Thomas Lemke (Hg.): *Governmentality. Current Issues and Future Challenges*. New York; London: Routledge: 93-114.

Porter, Gareth (2011): »How McChrystal and Petraeus Built an Indiscriminate ›Killing Machine‹«. In: *Truthout Monday*. 26.09. www.truth-out.org/

news/item/3588-how-mcchrystal-and-petraeus-built-an-indiscriminate-killing-machine

Ressler, Steve (2006): »Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research«. In: *Homeland Security Affairs* 2 (2): 1-10.

Sageman, Marc (2004): *Understanding Terrorist Networks, Philadelphia*: University of Pennsylvania Press.

Salter, Mark (2008): »Risk and Imagination in the War on Terror«. In: Louise Amoore/Marieke de Goede (Hg.): *Risk and the War on Terror*. New York; London: Routledge: 233-246.

Scahill, Jeremy/Devereaux, Ryan (2014a): »The Secret Government Rulebook For Labeling You a Terrorist«. In: *The Intercept*. 23.07. https://firstlook.org/theintercept/article/2014/07/23/blacklisted/

Scahill, Jeremy/Devereaux, Ryan (2014b): »Barack Obama's Secret Terrorist-Tracking System, by the Numbers«. In: *The Intercept*. 5.08. https://firstlook.org/theintercept/2014/08/05/watch-commander/

Scahill, Jeremy/Greenwald, Glenn (2014): »The NSA's Secret Role in the US Assassination Program«. In: *The Intercept*. 10.02. https://firstlook.org/theintercept/article/2014/02/10/the-nsas-secret-role/

Scahill, Jeremy (2015): »The Assassination Complex. Secret military documents expose the inner workings of Obama's drone wars«. In: *The Intercept*. 15.10. https://theintercept.com/drone-papers/the-assassination-complex/

Schmid, Alex (2011): »The Definition of Terrorism«. In: Alex Schmid (Hg.): *The Routledge Handbook of Terrorism Research*. Abingdon, Virginia: Routledge: 39-99.

Schneier, Bruce (2006): »Data Mining for Terrorists«. In: *Schneier Blog*. 3.03. https://www.schneier.com/blog/archives/2006/03/data_mining_for.html

Shaw, Ian (2013): »Bureaucratic Assassination – How do US Targeted Killings Work?« In: *Understanding Empire Blog*. 3.10. http://understandingempire.wordpress.com/2013/10/03/bureaucratic-assassination-how-do-u-s-targeted-killings-work

Shaw, Ian/Akhter, Majed (2014): »The Dronification of State Violence«. In: *Critical Asian Studies* 46 (2): 211-234. DOI: https://doi.org/10.1080/14672715.20 14.898452

Stäheli, Urs (2012): »Listing the Global: Dis/Connectivity beyond Representation?« In: *Distinktion: Scandinavion Journal of Social Theory* 13 (3): 233-246.

Stohl, Cynthia/Stohl, Michael (2007): »Networks of Terror: Theoretical Assumptions and Pragmatic Consequences«. In: *Communication Theory*. 17.07.: 93-124. DOI: https://doi.org/10.1111/j.1468-2885.2007.00289.x

Suchman, Lucy (1994): »Do Categories Have Politics? The Language/Action Perspective Reconsidered«. In: *Computer Supported Cooperative Work (CSCW)* 2: 177-190. DOI: https://doi.org/10.1007/BF00749015

Thrift, Nigel/French, Shaun (2002): »The Automatic Production of Space«. In: *Transactions of the Institute of British Geographers* NS 27: 309-335. DOI: https://doi.org/10.1111/1475-5661.00057

Weber, Jutta (2003): *Umkämpfte Bedeutungen: Naturkonzepte im Zeitalter der Technoscience*, Frankfurt a.M.; New York: Campus.

Weber, Jutta (2011): »Blackboxing Organisms, Exploiting the Unpredictable: Control Paradigms in Human-Machine Translation«. In: Martin Carrier/ Alfred Nordmann (Hg.): *Science in the Context of Application*. Dordrecht et al.: Springer: 409-429. DOI: https://doi.org/10.1007/978-90-481-90515_24

Whitlock, Craig (2012): »Remote US base at core of secret operations«. In: *The Washington Post*. 26.10. www.washingtonpost.com/world/national-security/remote-us-base-at-core-of-secret-operations/2012/10/25/a26a9392-197a11e2-bd10-5ff056538b7c_story.html

Woods, Chris (2015): »Covert drone strikes and the fiction of zero civilian casualties«. In: Mike Aaronson/Wali Asla/Tom Dyson/Regina Rauxloh (Hg.): *Precision Strike Warfare and International Intervention. Strategic, Ethico-legal, and Decisional Implications*. New York; London: Routledge: 95-113.