»Eine Gesellschaft, die ihr Verhältnis zur Zukunft im Zeichen der Prävention begreift und organisiert, fürchtet stets das Schlimmste, und ihre Hoffnungen sind darauf zusammengeschnurrt, dass es vielleicht am Ende ganz so schlimm doch nicht kommt.«
Ulrich Bröckling

Wild Cards. Imagination als Katastrophenprävention

Jutta Weber

»›Mommy, Daddy, the synsects stung me!‹ Julie ran into the house in a fluster. Martin, who just sat down to deal with the administrative stuff for his organic farm, looked over at his eleven-year-old daughter. On her face and all over her arms were red marks that looked like mosquito bites. ›What happened?‹ Julie had just been inspecting the rabbit hutches. Apparently, a swarm of these synsects had flown at her and attacked her« (Peperhove 2012: 72).

Die Horrorgeschichte vom unvorhergesehenen Angriff eines Schwarms künstlicher Insekten stammt nicht aus einer Science Fiction-Story. Sie ist eines mehrerer Katastrophen-Szenarios des EU-Sicherheitsforschungsprojektes FESTOS, um »potentielle zukünftige Gefahren durch neue Technologien in den Händen von organisierter Kriminalität und Terroristen« (Festos 2012) zu identifizieren. Andere Szenarien thematisieren unter anderem die Erpressung von Menschen mit gehackten DNA-Daten, die Zerstörung von Nanotech-Produkten per Funksignal oder die terroristische Verhaltensmanipulation der Bevölkerung durch Freisetzung biologischer Viren. Was mehr als bizarr klingt, hat in diesem Fall System: Bei der Entwicklung der Szenarien, die in Form von Kurzgeschichten ausgearbeitet wurden, um »[d]ie dunkle Seite neuer Technologien« (Peperhove 2012) abzuschätzen, legt man explizit »besonderes Augenmerk auf Szenarien […], deren Eintreten zwar als wenig wahrscheinlich angesehen werden kann, bei deren Eintreten allerdings mit besonders großen Folgen gerechnet werden muss, sogenannten Wild Cards« (Festos 2012).

Aktuelle Sicherheitsforschung, Katastrophenschutz und Technikfolgenabschätzung arbeiten gerne mit der Szenarientechnik (u. a. Grunwald 2012, Kaufmann 2011, Wright et al. 2008) und *Wild Cards* (Steinmüller/Steinmüller 2004; DeWar 2006, Hiltunen 2006). Letztere entstammen dem Kontext der Futurologie. Den Begriff der *Wild Card* prägte der Leiter des Think Tanks Arlington Institute, John Peterson, in seinem Buch *Out of The Blue – How to Anticipate Big Future Surprises* (2000). Andere populärwissenschaftliche Arbeiten – wie z. B. von den Futurolog*innen und Science Fiction-Autor*innen (!) Angela und Karl-Heinz Steinmüller, Wild Cards: Wenn das Unwahrscheinliche eintritt,

ZfK – Zeitschrift für Kulturwissenschaften 2|2014
urn:nbn:de:hbz:6:3-2014100752

in der sie für die Exploration des Unwahrscheinlichen werben – haben das Thema weiter ausgebaut (vgl. auch DeWar 2003, Mendonça 2004).

Die Szenarientechnik ist, genauso wie die Monte Carlo-Methode bzw. -Simulation,[1] ein wesentlicher Ansatz der Sicherheitsforschung, die aus dem Methodenarsenal der Kybernetik – und hier vor allem aus dem *operation research* – stammt. Die Methoden und Ansätze der Szenarientechnik wurden insbesondere in militärischen Planspielen atomarer Erstschläge eingesetzt (Ghamari-Tabrizi 2000, Pias 2008).

Im Rahmen des 7. EU-Forschungsprogramms etwa wurden sechs Foresight-Projekte gefördert, deren Aufgabe es sprichwörtlich war, ins Blaue hineinzudenken und teilweise auch systematisch *Wild Cards* zu erforschen (http://community.iknowfutures.eu/).

Neuen Auftrieb erhielt die Idee der Szenarienmethode nicht zuletzt nach 9/11, als das Eintreten eines völlig unerwarteten Ereignisses die Verletzbarkeit westlicher Systeme durch unerwartete *Low-Tech*-Angriffe vor Augen führte. So forderte der Bericht der 9/11-Untersuchungskommission als Lehre aus dem Attentat einen routinemäßigen Einsatz der Imagination. Der Bericht des Britischen *Intelligence and Security Committees,* das die Bombenanschläge 2005 in London untersuchte, appellierte an seine Leser*innen, sich gedanklich auf das Unbekannte einzulassen. Es bedürfe phantasievoller, von der Imagination geleitete Wege, um die Arbeit des Geheimdienstes effektiver zu machen und um terroristische Aktionen sowie zukünftige terroristische Strategien wahrnehmen und verstehen zu können (De Goede 2008: 156).

Man will die schlimmsten Szenarien vorwegnehmen, um ihnen zuvorkommen zu können (vgl. u. a. Daase et al. 2007, Mythen et al. 2008). Diese Idee ist nicht neu, aber als Post 9/11-Imagination – wie Marieke de Goede (2008) sie nennt – im *war on terror,* gewinnt sie eine ganz eigene Dynamik. Angesichts der Konfrontation mit ungewöhnlichen aber effektiven phantasievollen *Low-Tech*-Angriffen scheint systematisierte Imagination bzw. Vorwegnahme möglicher Szenarien noch attraktiver zu werden. Aber auch andere Phänomene arbeiten der strategisch eingesetzten Imagination der Sicherheitspolitik zu: Nach einer kurzen Verschnaufpause am Ende des Kalten Krieges, in der die Drohung eines Nuklearkrieges der Supermächte in den Hintergrund trat, erschienen neue Gespenster, etwa das Problem der *failed states* oder des nuklearen Terrorismus bzw. die Möglichkeit von Massenvernichtungswaffen in kriminellen Händen. Der US-amerikanische Sicherheitsberater Graham Allison und sein russischer Kollege Andrej Kokoshin malten ein mögliches Szenario folgendermaßen aus:

»Consider this hypothetical, […] a crude nuclear weapon constructed from stolen materials explodes in Red Square. A fifteen kiloton blast would instantaneously destroy the Kremlin, Saint Basil's Cathedral, the ministries of foreign affairs and defense,

1 »Mit ›Monte-Carlo-S.‹ bezeichnet man eine Klasse von Algorithmen, die ihre Ergebnisse mit Hilfe von Zufallszahlen errechnen. Hierbei wird zunächst eine Domäne möglicher Eingaben bestimmt und eine Reihe von Zufallszahlen aus dieser Domäne generiert, dann eine deterministische Berechnung mit den Zufallszahlen durchgeführt und zum Schluss werden die einzelnen Ergebnisse zusammengeführt« (Reiss 2010, 2458b). Zur Rolle des Computers im Kalten Krieg vgl. auch Edwards 1996.

> the Tretyakov Gallery, and tens of thousands of individual lives. In Washington, an equivalent explosion near the White House would completely destroy that building, […] and all of their occupants« (Allison/Kokoshin 2002: 35).

Die systematisierte Imagination von wenig wahrscheinlichen, aber höchst fatalen Katastrophenszenarien à la *Wild Cards* hat heute zunehmend Konjunktur. Hier möchte ich der Rolle der Imagination in den Diskursen und Praktiken aktueller, präventiver und ›prämediatisierter‹[2] Sicherheitsforschung und -politik nachgehen und analysieren, inwieweit sie auf veränderte mediale, epistemologische und gesellschaftliche Bedingungen reagiert und sich dabei transformiert. Dabei werde ich zuerst einen Blick auf die Rollen von Zukunftsszenarien und Imagination bei der strategischen Bearbeitung des nuklearen Kriegs werfen. Im Anschluss daran werde ich nach den aktuellen Bedingungen fragen, die diese höchst spekulativen Ansätze – die mehr den Eindruck literarischer Verfahren als klassisch wissenschaftlicher Methoden erwecken – attraktiv erscheinen lassen.

»Thinking about the Unthinkable«: Wissensproduktion unter Bedingungen großer Unsicherheit

Die professionalisierte, szenarienbasierte Zukunftsschau im Zeitalter des Kalten Krieges lässt sich als Antwort der Atomstrategen auf eine völlig neue Situation großer Unsicherheit lesen: Auf den Eintritt in das Atomzeitalter und die Möglichkeit der kompletten Auslöschung der Menschheit.[3] Niemand hatte Erfahrung in atomarer Kriegsführung und es war auch völlig unklar, wie mit dieser Situation militärisch-politisch umzugehen ist. In dieser Situation schien offensichtlich das klassische Methodenarsenal der Militärs, aber auch der ›defense intellectuals‹ (Cohn 1987), nicht mehr ausreichend. Gerade letztere verabschiedeten sich zumindest implizit von den bisherigen klassischen wissenschaftlichen Kriterien wie Objektivität und Wiederholbarkeit der Experimente oder Strategien. Gerade das Kriterium der Wiederholbarkeit war angesichts der Totalität eines Atomkriegs obsolet geworden. Vor diesem Hintergrund stellte die Vorwegnahme möglicher Kriegskonstellationen durch Szenarien (zuerst auf dem Papier oder als Brettspiel, später als Computer-Simulation) eine Alternative dar, um neue Strategien für neue Situationen zu erkunden. Traditionelle Vorstellungen von Wissenschaftlichkeit wurden zugunsten der Evidenzerzeugung durch Imagination aufgegeben.

2 Während im Deutschen der Begriff der ›Prävention‹ sowohl Vorbeugung wie Vorsorge einschließt, sind für den anglo-amerikanischen Diskurs noch die Begriffe *precaution* und *preemption* zentral, die auf die Vorwegnahme und Vermeidung von unwahrscheinlichen, aber fatalen Ereignissen zielen (vgl. Bröckling 2012). Erweitert wurden diese Begriffe in der aktuellen Diskussion durch den der ›Prämediation‹ (de Goede 2008, Grusin 2010).

3 Zu den Kontroversen zwischen traditionellen, kriegserfahrenen Militärs und den szenario-orientierten Militärstrategen siehe Ghamari-Tabrizi 2000.

Paradigmatisch für diese Haltung steht Hermann Kahn, *defense intellectual* und Experte des US-amerikanischen Think Tanks RAND. Euphorisch schreibt er über die Bedeutung der Imagination:

»Is there a danger of bringing too much imagination to these problems? Do we risk losing ourselves in a maze of bizarre improbabilities? […] It has usually been lack of imagination […] that caused unfortunate decisions and missed opportunities.« (Kahn 1963: 3, zit. n. Ghamari-Tabrizi 2005: 146).

Der Medientheoretiker Claus Pias betont gleichfalls, dass *Think Tanks,* szenarien-basierte Imagination und Computer-Simulation als Reaktionen auf eine nukleare Bedrohung zu verstehen sind, welche sich nicht mehr sinnvoll analytisch und auf der Basis von Experimenten oder vorangegangenen Erfahrungen bearbeiten lassen:

»Was die Computersimulation für die Entwicklung der Wasserstoffbombe bedeutete, bedeutet das Szenario für das Denken möglicher Zukünfte im Zeichen nuklearer Bedrohung. Denn auch deren Realität entzieht sich sowohl analytischen Kategorien, die sich an vergangenen Krieg erarbeiten ließen, als auch dem Experiment eines Krieges, der verheerende Folgen hätte« (Pias 2009: 13).

Eine mögliche Zukunft bestünde dementsprechend auch im Gewinnen eines nuklearen Krieges – wovon Kahn in seinem Buch *On Thermonuclear War* (1960) ausging. Er spielte alle un/vorstellbaren Szenarien eines Erst- oder Zweitschlags im Nuklearkrieg durch, ungeachtet irgendwelcher Wahrscheinlichkeitsüberlegungen (Kaplan 1983, Ghamari-Tabrizi 2005, Pias 2008). Desinteressiert an moralischen, aber ausgesprochen interessiert an strategisch-futurologischen Fragen kalkulierte er mit dem Tod von Hundertmillionen Menschen und entwarf Überlebensstrategien sowie biopolitische Maßnahmen für das post-nukleare Zeitalter. Kahns zweites Buch, das 1962 als Replik auf diverse Kritiken erschien, trug dann auch explizit den Titel *Thinking about the Unthinkable* (1962). Wie (wenig) überzeugend die Vorstellungen Kahns auch gewesen sein mochten – eines leisteten sie auf jeden Fall: Mit Hilfe des Szenarien-Denkens wurden die Ungeheuerlichkeiten nuklearer Abschreckung in Form unterschiedlicher Strategien, Konzepte und Handlungsoptionen denk- und diskursivierbar.

Aber was macht die Attraktivität der Szenarientechniken in der heutigen Sicherheitsforschung aus? Und haben wir es bei der Imagination von *Wild Cards* – also von Ereignissen mit geringer Wahrscheinlichkeit, aber fatalen Auswirkungen – wie den eingangs zitierten, wild gewordenen Cyberinsekten-Schwärmen, tele-operierbaren Nano-Produkten oder von Terrorist*innen induzierten Virusinfektionen – mit einer ähnlichen Problematik zu tun, auf die die Erst- und Zweitschlag-Szenarien Kahns und anderer *defense intellectuals* im Atomzeitalter zu antworten suchten?

Zukunftsfixierung und technikzentrierte Sicherheit

Die Attraktivität der Szenarienmethode hängt nicht zuletzt mit der Selbsteinschätzung der Gesellschaften des globalen Nordens zusammen. ›Zukunft als Katastrophe‹ (Horn 2014) – so ließe sich bündig ein dominanter Strang der Selbstwahrnehmung beschreiben. Es scheint ein weit verbreitetes Gefühl der Unsicherheit, wenn nicht gar der Bedrohung, zu herrschen. Die Absicherung gegen Gewalt, Krankheit und Tod nimmt heute einen sehr zentralen Stellenwert in unserem Denken, unserer Weltwahrnehmung und dementsprechend in unseren Sicherheitsdebatten ein.[4] Woher aber stammt das Gefühl der Bedrohung? Die Grundlage hierfür ist nicht mehr (primär) die nukleare Bedrohung. Auf der politischen Bühne wird gerne mit der Erfahrung von 9/11 argumentiert, aber in den Surveillance- und kritischen Security Studies sind sich die meisten Wissenschaftler*innen einig, dass die Entwicklung hin zu einer ubiquitären und präventiven Sicherheitspolitik deutlich früher einsetzt. Viele Theoretiker*innen verweisen auf die Globalisierung, die die Vereinzelung weiter antreibende Neoliberalisierung heutiger Gesellschaften und die digitale Aufrüstung der letzten Jahrzehnte als Ursachen dafür, dass sich Ängste – nicht nur vor terroristischen Anschlägen – vervielfältigten.

Schon 1985 diagnostizierte die Technikforscherin Donna Haraway die Entstehung einer *New World Order* von High-Tech-Gesellschaften bzw. von Technowissenschaftskulturen, deren gesellschaftliche, politische, technische, epistemische und normative Grundlagen sich radikal wandeln. Diese Gesellschaften zeichnen sich durch die stark beschleunigte und intensivierte Hybridisierung von Mensch und Maschine, von Organischem und Nicht-Organischem, von Wissenschaft und Technik aus. Hybride wie die Oncomouse oder intelligente Software ließen sich nicht mehr im Rahmen der traditionellen humanistischen Ordnung einsortieren. Haraway skizziert das Zeitalter der *Technosciences* als neue Episteme, in der die kausal-lineare Logik des Newtonschen Zeitalters von einer nicht-linearen, multiplen Techno-Rationalität abgelöst wurde. Gleichzeitig konfiguriere sich eine neue, globalisierte, politische Weltordnung, eine Biotechnomacht mit neuen Geostrategien, Selbsttechnologien, Produktions- und Verwertungslogiken (vgl. auch Weber 2003). Kurz darauf, im Jahre 1986, machte Ulrich Becks These von der Entstehung einer ›Risikogesellschaft‹ Furore. Ihm zufolge sind potentielle und technisch induzierte Bedrohungen wie nukleare Desaster oder die globale Erwärmung nicht mehr vorherseh- und kalkulierbar. Ein zunehmend expandierendes Gefühl der Bedrohung diagnostizierte dann wiederum der britische Soziologe Anthony Giddens in den 1990er Jahren. Er verwies darauf, dass die Gesellschaften des globalen Nordens sich vermehrt mit ihrer Zukunft bzw. ihren Zukünften beschäftigen und dabei ein wachsendes Gefühl der Gefährdung evozieren würden.

Javier Solana, ehemaliger Generalsekretär der NATO und Hoher Vertreter für die Gemeinsame Außen- und Sicherheitspolitik der EU bis 1999, legte im Dezember 2003 ein Konzeptpapier zur Europäischen Sicherheitsdoktrin vor, in welchem er die neue Situation folgendermaßen skizziert: Die Zahl der korrupten bzw. *rogue states* würde

4 Wenn auch gleichzeitig das Thema soziale Sicherheit (bis vor kurzem?) weitgehend von der politischen Tagesordnung verschwunden ist.

zunehmen – ebenso wie die Armut. Damit einher gingen mehr regionale Konflikte, Korruption, Kriminalität sowie Migrationsbewegungen. Letztere seien auch induziert durch den globalen Temperaturanstieg. Ein weiterer Unsicherheitsfaktor sei die große Abhängigkeit Europas von Energieimporten. Die großen Bedrohungen seien dementsprechend ein global und skrupellos agierender Terrorismus – teilweise auf der Basis eines gewaltbereiten Fundamentalismus –, die Verbreitung von Massenvernichtungswaffen, organisierte Kriminalität und wachsende Migrant*innenströme, welche durch die gescheiterten Staaten und die globale Erwärmung hervorgebracht würden. Die Differenz zu alten Bedrohungen charakterisiert er folgendermaßen:

> »Unser herkömmliches Konzept der Selbstverteidigung, das bis zum Ende des Kalten Krieges galt, ging von der Gefahr einer Invasion aus. Bei den neuen Bedrohungen wird die erste Verteidigungslinie oftmals im Ausland liegen. Die neuen Bedrohungen sind dynamischer Art. Wenn sie nicht beachtet werden, erhöht sich die Gefahr. […] Daher müssen wir bereit sein, vor dem Ausbrechen einer Krise zu handeln. Konflikten und Bedrohungen kann nicht früh genug vorgebeugt werden. Im Gegensatz zu der massiven und sichtbaren Bedrohung zu Zeiten des Kalten Krieges ist keine der neuen Bedrohungen rein militärischer Natur, auch kann gegen sie nicht mit rein militärischen Mitteln vorgegangen werden. Jede dieser Bedrohungen erfordert ein ›gemischtes‹ Instrumentarium« (Solana 2003).

Im Verlauf betont Solana weiterhin, dass man eine proaktive Politik bräuchte, um »neuen, sich ständig ändernden Bedrohungen« entgegenzuwirken.

Zentrale Differenz zu den Gefahren des Kalten Krieges ist also die Dynamisierung und Ausweitung der Bedrohung auf zivile Bereiche, die präventives Handeln und massives Investieren in Sicherheitsmaßnahmen, -infrastrukturen und -technologien erfordere – eine Entwicklung, die zu diesem Zeitpunkt schon längst eingesetzt hatte und sich seither weiter beschleunigt und intensiviert hat.

Als Politiker wahrt Solana noch eine gewissen Zurückhaltung und fokussiert weniger auf mögliche technologisch induzierte Probleme, aber auch hier erscheint die Zukunft bzw. unsere Welt als bedroht und massiv gefährdet (Horn 2014). Diese Bedrohungen werden in ihrer Dynamik und Globalität (als) zunehmend unkalkulierbar (wahrgenommen).

Die permanente Diskursivierung wahrscheinlicher und vor allem auch ›possibilistischer‹ (vgl. Clarke 1999) – also unwahrscheinlicher, aber (technisch) möglicher – Risiken, geht mit der Beschwörung ubiquitärer Gefahren Hand in Hand und heizt das Gefühl von Bedrohung weiter an. Pat O'Malley beschrieb diese Entwicklung lange vor 9/11 folgendermaßen: »the structural demand for knowledge relating to risk becomes insatiable. As well because the accumulation of such knowledge adds awareness to new sources of risk, the risk-knowledge process gains its own internal momentum« (O'Malley 1999, 139).

Die *defense intellectuals* des Kalten Krieges sahen sich einer neuen Bedrohung (nuklearer Krieg, Erst- oder Zweitschlag) gegenüber, die man nicht mehr mit herkömmlichen Mitteln bearbeiten konnte. Aber diese Bedrohung war (relativ) konkret und hatte

einen klar identifizierbaren Gegner: den Ostblock bzw. die Sowjetunion. Heutige Sicherheitsstrategen bearbeiten dagegen dynamische, vielfältige und zugleich recht vage Bedrohungen. *Wild Cards* sind ein Teil dieses possibilistischen Risikomanagements, das versucht, allen möglichen (imaginierbaren) Bedrohungen gerecht zu werden: Der Sicherheitsdiskurs mäandert, multipliziert und weitet sich rasant aus – was durchaus auch wieder ganz reale Bedrohungen schafft: Im Zuge erhöhter Finanzierung von Sicherheitsforschung und -technologien ist beispielsweise die Zahl der Labore, die mit gefährlichen pathogenen Substanzen arbeiten – und aus deren Sicherheitsbereich manipulierte Organismen entweichen oder gestohlen werden können – rasant gewachsen (Kaufmann 2011). Die Imagination neuer Gefahren und deren Bearbeitung durch die Sicherheitsforschung bringen also wiederum neue Gefahren hervor. Die Ausweitung der Sicherheitszone im Allgemeinen und der Fokus auf *Wild Cards* mit ihren möglichen, possibilistischen Szenarien unwahrscheinlicher Bedrohungen (Clarke 1999) schüren Bedrohungsgefühle, legitimieren die Ausweitung von Sicherheitsmaßnahmen und treiben in toto die Sicherheitsspirale weiter voran.

Techno-Security Culture

Je mehr Risiken identifiziert und als grenzenlos klassifiziert werden, desto plausibler erscheinen Forderungen nach umfassenden, vorbeugenden Maximalmaßnahmen (Amoore/De Goede 2008; Kaufmann 2011), die letztlich aber in meist recht phantasielose Vorschläge und Maßnahmen weit reichender High-Tech-Überwachung und Sicherheitsaufrüstung münden.

Diese Logik beachtet politische, soziale oder ökonomische Ursachen von Unsicherheit kaum – etwa im Hinblick auf Terrorismus, Organisierte Kriminalität oder Migration. Statt dessen wird Technik in Form von Datenbanken, Simulationen, aber auch als (smarte) Videoüberwachung, Biometrie oder Datenvorratsspeicherung deterministisch als die einzige Lösung betrachtet (Marx 2001; Aas et al. 2009).

Gut beobachten lässt sich das auch im deutschen Sicherheitsforschungsprogramm. So wird die Notwendigkeit für szenarienorientierte Sicherheitsforschung (jedoch nicht primär *Wild Cards*) folgendermaßen erläutert:

> »Die Szenarienorientierung vermeidet isolierte Einzellösungen. Sie ermöglicht anwendungsnahe Systeminnovationen, aus denen sich praxistaugliche Sicherheitsprodukte und -dienstleistungen erfolgreich entwickeln lassen, die sich am Bedarf der Endnutzer orientieren und zu einer freiheitlichen Gesellschaft passen« (BMBF 2014).

Über die Szenarienorientierung lassen sich gesellschaftlich relevante Bedrohungen normativ festlegen. Gleichzeitig werden sie als Systeminnovationen im technischen Sinne konfiguriert. So wird der *technological fix* schon im Forschungsprogramm verankert.

So kommt es zu einer Konvergenz von Sicherheit und Überwachung. Man geht nicht nur in den Szenarien dazu über, fast jeden gesellschaftlichen Bereich zu überwachen. Man durchsucht und erstellt Profile im Bereich der Wirtschaft, in der Politik,

im Militär oder im Alltagsleben. CCTV, RFID-Chips, Drohnen oder Scanner werden eingesetzt, um nach Terroristen zu suchen, Sportveranstaltungen und Geldschalter oder die eigenen Mitarbeiter*innen zu überwachen. Sicherheit als zentraler und zugleich umkämpfter Wert moderner Gesellschaften wird primär technikzentriert interpretiert und umgesetzt.

Armand Mattelart prägte mit Blick auf die Entwicklung des Militärs den Begriff der »Techno-Security«, um auf die »Globalisierung der Überwachung« im Anschluss an 9/11 aufmerksam zu machen, welche zunehmend vom »Techno-Fetischismus« aktueller Militärkonzepte wie der technikgetriebenen »revolution in military affairs« geprägt würde. Bei Mattelart meint *Techno-Security* einen »exclusively technological approach to intelligence gathering, at the expense of human intelligence« (Mattelart 2010: 138). Die aktuelle militärische Logik moderner netzwerkzentrierter High-Tech-Kriegsführung lässt sich als eine Logik des Zielens, Identifizierens und Verfolgens beschreiben. Auf der Basis eines komplexen digitalen Rechner- und Sensorennetzwerkes soll ein umfassender Überblick über den jeweiligen Kampfraum in Echtzeit hergestellt werden. Dieser Idee liegt die Prämisse zugrunde, dass sich militärischer Erfolg durch Informationshoheit, technische Überlegenheit und die enge Verzahnung von Aufklärung, Kommandozentrale(n) und Waffentechnologie herstellen lässt, und erstaunlicherweise findet sich diese militärstrategische Logik auch in der zivilen Sicherheit im Rahmen demokratisch legitimierter Sicherheitspolitik wieder. Ein paradigmatisches Beispiel hierfür ist DAS: das neue *Domain Awareness System* der New Yorker Polizei, das in Kooperation mit Microsoft entwickelt wurde und welches in Echtzeit nicht nur Bilder von 3.000 Überwachungskameras, 1.600 Strahlungssensoren sowie über hundert stationärer und mobiler Nummernschild-Scanner sammelt, sondern auch Polizeifunk und Notrufe einspeist und Daten von Verdächtigen in riesigen Datenbanken der Kriminal- und Terrorismusbekämpfung abgleicht. Es erlaubt auch, die Bewegungen von Personen oder Fahrzeugen über weite Strecken in Echtzeit zu verfolgen oder über die vergangenen Wochen nachzuvollziehen. Ein eng gestricktes, multiples Sensorensystem wurde zusammengeführt, um sicherzustellen, dass nichts im öffentlichen Raum undokumentiert bleibt. Nun könnte man argumentieren, dass wir es gerade in New York mit den Spätfolgen des US-amerikanischen 9/11-Traumas zu tun haben und dass eine ähnliche Situation schon aufgrund der Datenschutzgesetzgebung in Europa undenkbar wäre. Doch findet sich die militärische Logik von C4 – *Command, Control, Computers, Communication* – die auf ISR – *Intelligence* (Aufklärung), *Surveillance* (Überwachung) und *Reconnaissance* (Nahaufklärung) – basiert, zunehmend im zivilen Bereich wieder. Man denke an die Olympischen Spiele, die 2012 in London stattgefunden haben. Dort waren über 13.000 britische Soldaten sowie Flugzeugträger, Boden-Luft-Raketen und unbemannte Drohnen im Einsatz bzw. einsatzbereit. Temporär wurden Datenschutz und Grundrechte außer Kraft gesetzt, etwa als friedliche Demonstranten kurzzeitig verhaftet wurden, um ihnen im Anschluss das Betreten der Olympischen Zone für die Dauer der Spiele zu verbieten (Boyle/Haggerty 2012, Graham 2012). Was man bisher nur von G8-Gipfeln kannte, wird zur Normalität bei Großveranstaltungen.

Nicht zuletzt angesichts der Ausweitung der militärischen Logik auf das Zivile, der erweiterten Wahrnehmung der Gefahrenbereiche und der gesellschaftlichen Konzen-

tration auf den biopolitischen Wert der Sicherheit (von Leib und Leben), scheint es mir sinnvoll, Sicherheit heute eher im Sinne einer Sicherheitskultur (Daase 2012) zu verstehen. Dadurch bekommt man nicht nur institutionelle Akteure wie Militär oder Polizei in den Blick, sondern kann ein umfassenderes Verständnis von Sicherheitsregimen in der Alltagskultur entwickeln. Kultur wird hier als vielfältige und dynamische soziokulturelle Praxis mit vielen heterogenen Agenten und Aktanten gefasst. Leider stellt Technik im Großteil der *surveillance and critical security studies* eine Leerstelle dar (Aas et al. 2009). Es gilt, gerade *Techno-Security* als komplexe soziotechnische Praxis mit heterogenen menschlichen und nicht-menschlichen Akteur*innen zu verstehen. Entsprechend sind nicht nur Polizeien, Geheimdienste oder *Think Tanks,* sondern auch Algorithmen, Social Media, Militärdoktrinen oder Software-Ingenieur*innen Akteure der *Techno-Security Culture.* Sicherheit im Sinne der *Techno-Security* zu konzipieren, ermöglicht es, danach zu fragen, warum Imagination eine so zentrale Rolle im Kontext der Sicherheit spielt, wie sich wiederum neue (Überwachungs-)Technologien auf unser Denken, unsere Wahrnehmung, Verhalten und Techno-Imaginationen, oder auch, wie sich neue Epistemologien und Ontologien auf die Konfiguration von Gesellschaft auswirken. In diesem Zusammenhang wird Technik bzw. werden Medien nicht nur als ein spezialisiertes (Kontroll-)Werkzeug interpretiert, sondern als Diskurs, Praxis und Artefakt. Diesen werden Skripte (Akrich 1992) bzw. Handlungsanweisungen eingeschrieben, die mit Visionen, epistemischen Paradigmen, aber auch Werten und Normen verknüpft sind und die Kategorisierungen und Standardisierungen transportieren (Bowker/Star 1999) sowie »soziales Sortieren« (Lyon 2003) ermöglichen. Um nur drei Beispiele zu nennen: Givens und andere haben darauf hingewiesen, dass Gesichtserkennungssoftware einen geschlechtlichen, rassistischen oder Alters-Bias haben kann, wenn bestimmte Altersgruppen oder Hautfarben besser erkannt werden als andere (Givens et al. 2004). Torin Monahan (2009) hat die diskriminierenden Effekte US-amerikanischer *Electronic Benefit Transfer Systems* vor allem für Wohlfahrtsempfängerinnen beschrieben. Bowker et al. (2009) haben gezeigt, dass die soziale Netzwerkanalyse – wie man sie auch in der Polizeiarbeit verwendet – zwar riesige Datenmengen sammelt, aber als primär quantitativer Ansatz dahin tendiert, Formales über Inhaltliches zu stellen und lebensweltliche Praktiken und Bedeutungen zu ignorieren.

Technologien sind damit nicht nur Werkzeuge, sondern auch Vergegenständlichungen von Kategorien, Gewohnheiten, Denkweisen, und Imaginationen, die als Machtverhältnisse wirken. In diesem Kontext stellt sich nicht nur die Frage, wie bestimmte Weisen der Imagination Technologien der Securitization vorantreiben, sondern auch, ob und wie Technologien selbst Praktiken der Imagination beeinflussen: Treibt die mediale Logik der Datenbank möglicherweise wiederum ›Verdatung‹ bzw. Datenvorratsspeicherung an? Das liegt nahe, denn eine Datenbank ist umso besser, je mehr Datensätze sie aufweist (Manovich 2001, Gugerli 2009). Man bedient sich der Computersimulationen (Bogard 2012), der Technologie der Szenarienplanung, des *Data-Minings* und der *Worst Case-Imagination,* um Unsicherheit und unvorhersehbare Risiken in den Griff zu bekommen (de Goede 2008; Salter 2008; Kaufmann 2011; Bröckling et al. 2011). Die Logik des Zuvorkommens und der Prävention zieht die Imagination der Kraft des Faktischen vor – *der Verdacht wird wichtiger als die Evidenz* (Salter 2008: 243). Die präventive Logik

ist eine Logik der Risikoabschätzung, die möglichst viele potentielle Gefahren abschätzt, aber nicht konkrete Gefahren, die ganz manifest ein Sicherheitsakteur für einen anderen produziert. Während die Logik konkreter Gefahrenabwehr einer linearen Zweck-Mittel-Relation folgt, ist die Logik des Risikos notwendig vage, unklar und offen und lebt von der Imagination von Eventualitäten.

Entsprechend sind Imagination und der Entwurf (un)möglicher Szenarien auf der Basis automatisierter Prozesse der Rekombination heute die epistemologische Grundlage für Risikomanagement. Automatisierte Technologien der präventiven, vorhersagenden Analyse, der Echtzeit-Verfolgung und des individualisierten *targetings* werden als adäquate Mittel zur Bekämpfung unvorhersehbarer Risiken betrachtet, was wiederum die Illusion von bzw. Sehnsucht nach technologischer Überlegenheit nährt (u.a. Bigo/Jeandesboz 2009; Graham 2006), die ironischerweise genau in ihr Gegenteil umschlagen kann. So steigt mit dem Ausbau der Geheimdienste und ihrer *Big Data*-Sammlungen auch die Gefahr des *Whistle Blowing*. Und es finden sich erste Stimmen, die laut darüber nachdenken, inwieweit die Datenmassen der Geheimdienste diese wiederum überfordern und handlungsunfähig machen (Möchel 2014).

Angetrieben von dem Begehren nach immer mehr Wissen bzw. Information werden komplexe Sicherheitsnetzwerke entwickelt, die alle möglichen verfügbaren Daten unterschiedlicher, meist vernetzter Quellen sammeln sollen. Die präventive Analyse soll das Unkalkulierbare kalkulierbar machen. Gleichzeitig ermöglicht die *datification,* das permanent wachsende Netz sozialer Medien, die multimediale Interaktion zwischen Menschen und Dingen, eine Sammlung riesiger Datenmengen, welche wiederum durchsucht, nach Mustern gescannt und zur Profilproduktion verwendet werden kann (Grusin 2010).

Im Alltag der Sicherheitsbehörden scheint diese Praxis häufig in eine recht banale bzw. bürokratisierte Imagination in Form des *Scenario Testing* als Rekombination schon bekannter Szenarien zu münden – in der Hoffnung, so möglichen terroristischen Aktionen, Katastrophen oder auch Pandemien zuvorzukommen. Und je mehr Daten, Profile, Verhaltensmuster in der Datenbank lagern, desto besser fühlt man sich gegen zukünftige Desaster gewappnet. Oder auch wieder nicht: Denn gleichzeitig ist klar, dass dieser Prozess unabschließbar ist:

> »Security is less about reacting to, controlling or prosecuting crime than addressing the conditions precedent to it. The logic of security dictates earlier and earlier interventions to reduce opportunity, to target harden and to increase surveillance even before the commission of crime is a distant prospect« (Zedner 2007: 265).

Ein Effekt dieser bürokratisierten Imagination ist ein Datensammeleifer neuen Ausmaßes. Die aktuelle NSA-Affäre ist hierfür sicherlich das beste Exempel; andere Beispiele sind die bis vor kurzem auch in der EU weitverbreitete Datenvorratsspeicherung oder der zunehmende Ausbau digitaler Grenzsicherungssysteme. Man denke etwa an das US *VISIT*-Programm, bei dem Ausländer*innen bei der Einreise in die USA fotografiert und die biometrischen Fingerabdrücke von *TSA-Officers* abgenommen werden. Diese Daten werden in einer Datenbank abgelegt, auf die 30.000 Angestellte unterschiedli-

cher US-amerikanischer Behörden zugreifen können.[5] Ein ähnliches System soll auch bald an den Grenzen Europas eingeführt werden (Europäische Kommission 2013). Für Asylbewerber*innen gibt es ein solches System schon lange unter dem Namen *Eurodac*.

Die Idee des Risikomanagements via Überwachung und Datenmonitoring begann spätestens in den 1990er-Jahren und wurde nach 9/11 immer mehr ausgeweitet. Hierbei geht es nicht primär um die Verfolgung eines konkreten Tatverdachts, sondern vielmehr um eine präventive ›Sicherung‹ der Sicherheit. In dieser präventiven Logik der Überwachung, der Strafverfolgung – und damit verbunden auch des Strafvollzugs – geht es weniger um konkrete Gefahrenabwehr als um Prävention, Premediation und darum, Risiken und Kosten zu managen. Typische Phänomene dieser Logik sind die Datenvorratsspeicherung, *predictive policing,* oder das Operieren mit Vorfeldtatbeständen wie das Verwenden von verdächtigen Begriffen (vgl. den Fall Andrej Holm[6]) oder der längere Aufenthalt in einem Land, welches nicht als touristisches Ziel gilt, wie der Jemen oder Syrien.

Systematisierte Imagination und High-Tech Aufrüstung

Es gilt, das Verständnis von Sicherheit als unabschließbar, als eine Idee, die Alles und Jedes als Bedrohung problematisiert und damit die Imagination in immer neue Höhen treibt und damit wiederum eine militär- wie sicherheitsstrategische Logik des ubiquitären *Worst Case* vorantreibt, noch weiter zu analysieren. Wir brauchen einen theoretischen Zugang zur *Techno-Security,* der gleichermaßen Wissenspolitiken, Techno-Imaginationen, in Technologien implementierte Werte und Normen wie technische Infrastrukturen als auch Effekte aktueller Software, die »power through the algorithm« (Lash 2007) in klassisch hierarchisch wie interaktiv organisierten Überwachungsdiskursen und -praxen untersucht. Bis heute sind Studien rar, die die Logik und Konsequenz z.B. von biometrischer oder Datamining-Software analysieren, um die Effekte der Technologien genauer in den Blick zu bekommen und *Techno-Security-Governance* im 21. Jahrhundert besser zu verstehen. Es stellt sich die Frage, inwiefern etwa bestimmte Techno-Logiken die Wahrnehmung unserer Welt *als ubiquitär* gefährdet vorantreiben – und damit Forderungen nach einer technikzentrierten Maximal-Sicherheit.

5 http://www.dhs.gov/ynews/testimony/testimony_1237563811984.shtm, Zugriff vom 14.9.2014.

6 Das BKA war auf den Soziologen Dr. Andrej Holm durch eine Internetrecherche aufmerksam geworden, da er angeblich ähnliche Vokabeln (Gentrifizierung, Prekarisierung, Reproduktion) wie die gesuchte so genannte ›militante gruppe‹ benutzt hatte. Nach einem Jahr der Observierung wurde er im Juli 2008 verhaftet. Indizien für seine Mitgliedschaft in der Gruppe waren neben den Keywords konspirative Treffen mit vermuteten weiteren Mitgliedern der Gruppe, aber auch das Nicht-Mitführen seines Handys bei verschiedenen Treffen. Aufgrund (inter)nationaler Proteste – Richard Sennett und Saskia Sassen sprachen von ›Guantanamo in Germany‹ – wurde er drei Wochen später freigelassen. Vor kurzem wurde er im Gerichtsverfahren freigesprochen (vgl. Holm 2007, Roth 2013).

Gleichzeitig scheinen die *Wild Cards* Ausdruck einer tiefgehenden Verunsicherung dahingehend zu sein, welches denn nun wirklich die relevanten Bedrohungen sind. Da man sich nie ganz sicher ist, ob es um den (un)gestörten Fluss von Waren, Hochwasserbekämpfung oder Terrorattacken am Flughafen geht, baut man noch ein paar *Wild Cards* für den Fall der Fälle ein. Die Effekte erinnern an die Aporien, in die sich die Kalten Krieger der 1950er-Jahre verstrickt hatten:

»Obsessed with preparedness, they sometimes did not scruple about overstating the threat for which preparation was necessary. They practiced psychological warfare on their own people. Strategists like Kahn and Wohlstetter […] were not responsible for starting the arms race, but the more they speculated on the unknown terrors of the future, the faster the race was run« (Menand 2005).

Wer in multistaatlich finanzierten Forschungsprojekten äußerst unwahrscheinliche, wenn auch theoretisch mögliche Horrorgeschichten von Attacken losgelassener Cyberinsekten-Schwärme entwirft oder über den möglichen Psychoterror durch manipulierte Viren schwadroniert, befeuert möglicherweise eine ähnliche High-Tech-Aufrüstung – nur diesmal im Bereich der zivilen Sicherheit.

Danksagung: Vielen Dank an die Reviewer*innen sowie Katrin M. Kämpf für kritische Kommentare und hilfreiche Hinweise zu einer früheren Fassung dieses Aufsatzes.

Dieser Beitrag hat ein peer review-*Verfahren mit double-blind-Standard durchlaufen.*

Literatur

Aas, Katja Franko/Gundhus, Helene Oppen/Lomell, Heidi Mork (Hg.) (2009): T*echnologies of inSecurity: The Surveillance of Everyday Life,* Abingdon, GB/New York: Routledge-Cavendish.

Allison, Graham/Kokoshin, Andrej (2002): »The New Containment: An Alliance Against Nuclear Terrorism«. In: *The National Interest* Nr. 69 (Fall 2002).

Amoore, Louise/de Groede, Marieje (Hg.) (2008): *Risk and the War on Terror,* New York: Routledge.

Beck, Ulrich (1986): *Risikogesellschaft: Auf dem Weg in eine andere Moderne,* Frankfurt a.M.: Suhrkamp.

Beer, David (2009) »Power Through the Algorithm? Participatory Web Cultures and the Technological Unconscious«. In: *New Media & Society* 11, no. 6 (2009), 985-1002.

Bigo, Didier/Jeandesboz, Julian: »Border Security, Technology and the Stockholm Programme«. INEX Policy Brief No. 3, November 2009 (2009). 17.02.2014, http://aei.pitt.edu/14993/.

BMBF (2014): Bewilligte Projekte der Programmlinie »Szenarienorientierte Sicherheitsforschung«. 08.08.2014, http://www.bmbf.de/de/12876.php.

Bogard, William (2012): »Simulation and Post-panopticism«. In: *Routledge Handbook of Surveillance Studies,* hg. v. Kirstie Ball, Kevin D. Haggerty und David Lyon, New York:

Routledge, 30-37.

Bowker, Geoffrey C./Star, Susan Leigh (1999): *Sorting things out: classification and its consequences,* Cambridge, Mass.: MIT Press.

Bowker, Geoffrey C./Baker, Karen/Millerand, Florence/Ribes, David (2009): »Toward Information Infrastructure Studies: Ways of Knowing in a Networked Environment«. In: *International Handbook of Internet Research,* hg. v. J. Hunsinger et. Al, Springer Science+Business Media, 97-117.

Boyle, Philip/Haggerty, Kevin D. (2012): »Planning for the worst: risk, uncertainty and the Olympic Games«. In: *The British Journal of Sociology,* Vol. 63, 2, 241-259.

Bröckling, Ulrich (2012): »Dispositive der Vorbeugung: Gefahrenabwehr, Resilienz, Precaution«. In: *Sicherheitskultur. Soziale und politische Praktiken der Gefahrenabwehr,* hg v. Christopher Daase, Philipp Offermann und Valentin Rauer, Frankfurt a.M./New York: Campus, 93-108.

Castells, Manuel (1996): *The Rise of the Network Society. Information Age,* Malden, Mass.: Blackwell.

Clarke, Lee (1999): *Mission Improbable: Using Fantasy Documents to Tame Disaster,* Chicago: University of Chicago Press.

Cohn, Carol (1987): »Sex and Death in the Rational World of Defense Intellectuals«. In: *Signs: Journal of Women in Culture and Society* Vol. 12, No. 4, 687-718.

Daase, Christopher (2012): »Sicherheitskultur als interdisziplinäres Forschungsprogramm«. In: *Sicherheitskultur. Soziale und politische Praktiken der Gefahrenabwehr,* hg. v. Christopher Daase, Philipp Offermann und Valentin Rauer, Frankfurt a.M./New York: Campus, 23-44.

Daase, Christopher/Kessler, O. (2007): »Knowns and Unknowns in the ›War on Terror‹: Uncertainty and the Political Construction of Danger«. In: *Security Dialogue* 38, no. 4, 411-434.

De Goede, Marieke (2008): »Beyond Risk: Premediation and the Post-9/11 Security Imagination«. In: *Security Dialogue* 39, no. 2-3, 155-176.

DeWar, James (2003): »The Importance of Wild Card Scenarios«, http://www.au.af.mil/au/awc/awcgate/cia/nic2020/dewar_nov6.pdf.

Edwards, Paul N. (1996): The Closed World: *Computers and the Politics of Discourse in Cold War America,* Cambridge, Mass./London: MIT Press.

Europäische Kommission (Hg.) (2014): Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über ein Einreise-/Ausreisesystem (EES) zur Erfassung der Ein- und Ausreisedaten von Drittstaatsangehörigen an den Außengrenzen der Mitgliedstaaten der Europäischen Union. Brüssel, den 28.2.2014, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0095:FIN:DE:PDF.

FESTOS (Hg.) (2012): Foresight of Evolving Security Threats Posed by Emerging Technologies. Website am Zentrum Technik und Gesellschaft. TU Berlin. http://www.tu-berlin.de/ztg/menue/forschungprojekte/projekte_-_abgeschlossen/foresight_of_evolving_security_threats_posed_by_emerging_technologies_festos/ 2012, 13.08.2014.

Ghamari-Tabrizi, Sharon (2000): »Simulating the Unthinkable: Gaming Future War in the 1950s and 1960s«. In: *Social Studies of Science,* 30 (April 2000), 163-223.

Ghamari-Tabrizi, Sharon (2005): *The Worlds of Herman Kahn: The Intuitive Science of*

Thermonuclear War, Cambridge/New York/London: Harvard University Press.

Giddens, Anthony (1999): »Risk and Responsibility«. In: *Modern Law Review* 62, no. 1, 1-10.

Givens, Geof; J./Beveridge, Ross/Draper, Bruce A./Grother, Patrick/Philips, P. Jonathon (2004): »How features of the human face affect recognition: A statistical comparison of three face recognition algorithms«. In: *IEEE Computer Society Conference on Computer Vision and Pattern Recognition,* 2 (2004), 381-388.

Graham, Stephen (2006): »Surveillance, Urbanization and the US ›Revolution in Military Affairs‹«. In: *Theorizing Surveillance. The Panopticon and Beyond,* hg. v. David Lyon, Cullompton/Devon, 247-270.

Graham, Stephen (2012): »Olympics 2012 Security«. In: *City: Analysis of Urban Trends, Culture, Theory, Policy, Action* 16, no. 4, 446-451.

Grunwald, Armin (2012): »Technikzukünfte als Medium von Zukunftsdebatten und Technikgestaltung«. Karlsruher Studien Technik und Kultur, Bd. 6, Karlsruhe: KIT Scientific Publishing

Grusin, Richard (2010): *Premediation: Affect and Mediality After 9/11,* New York: Palgrave Macmillan.

Gugerli, David (2009): *The Culture of the Search Society. Data Management as a signifying practice,* Amsterdam 2009, http://www.networkcultures.org/public/The_Culture_of_the_Search_Society_DavidGugerli.pdf, 15.11.2013.

Haraway, Donna (1985): »Manifesto for Cyborgs: Science, Technology, and Socialist Feminism in the 1980s«. In: *Socialist Review* no. 80, 65-108.

Hiltunen, Elina (2006) »Was it a Wildcard or Just Our Blindness to Gradual Change?« In: *Journal of Futures Studies,* 11 (2), 61-74.

Holm, Andrej: Im Kreis. Überwachung Von der Logik von 129a-Verfahren – statt Straftaten aufzudecken, werden Verdächtige geschaffen. Der Freitag. 23.11.2007, https://www.freitag.de/autoren/der-freitag/im-kreis.

Horn, Eva (2014): *Zukunft als Katastrophe,* Frankfurt a.M.: Fischer.

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

Kahn, Hermann (1962): *Thinking About the Unthinkable*, New York: Horizon Press.

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

Kaufmann, Stefan (2011): »Zivile Sicherheit: Vom Aufstieg eines Topos«. In: *Sichtbarkeitsregime. Überwachung, Sicherheit und Privatheit im 21. Jahrhundert,* hg. v. Leon Hempel, Susanne Krasmann und Ulrich Bröckling, Wiesbaden: VS Verlag für Sozialwissenschaften, 101-123.

Lash, Scott (2007): »Power After Hegemony: Cultural Studies in Mutation?« In: *Theory, Culture & Society* 24, no. 3, 55-78.

Lyon, David (Hg.) (2003): *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination,* London/New York: Routledge.

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

Marx, Gary T. (2001): »Technology and Social Control: The Search for the Illusive Silver Bullet«. In: *International Encyclopedia of the Social and Behavioral Sciences,* http://web.mit.edu/gtmarx/www/techandsocial.html, 17.02.2013.

Mattelart, Armand (2010): T*he Globalization of Surveillance: the Origin of the Securitarian Order,* Cambridge: Polity.

Menand, Louis (2005): »Fat Man. Herman Kahn and the nuclear age«. In: T*he New Yorker,* 27. Juni 2005, http://www.newyorker.com/archive/2005/06/27/050627crbo_books?currentPage=all, 06.06.2014.

Mendonça, Sandro/Cunha, M.P/Kaivooja, Jari/Ruff, Frank (2004): »Wild Cards, Weak Signals and Organisational Improvisation, Futures«. In: *The Journal of Forecasting,* Planning and Policy 36, 2, 201-218.

Möchel, Erich (2014): »Whistleblower: ›NSA hat sich selbst ausgeschaltet‹«. FM4/ORF, 14.08.2014, http://fm4.orf.at/stories/1744256/.

Monahan, Torin (2009): »Dreams of Control at a Distance: Gender, Surveillance, and Social Control«. In: Cultural Studies <=> Critical Methodologies 9, 2, 286-305.

Mythen, Gabe/Walklate, Sandra (2008): »Terrorism, Risk and International Security: The Perils of Asking ›What If?‹«. In: *Security Dialogue* Vol. 39, 2-3, 221-242.

O'Malley, Pat (1999): »Governmentality and the Risk Society«. In: *Economy and Society* 28, no. 1, 138-148.

Peperhove, Roman (2012): »Die dunkle Seite neuer Technologien – Projektbericht FESTOS«. In: *Zeitschrift für Zukunftsforschung* Vol. 1, 64-78.

Petersen, John (2000): *Out of The Blue: Wild cars and other big future surprises. How to Anticipate Big Future Surprises,* Long Island City: Madison Books.

Pias, Claus (Hg.) (2008): *Herman Kahn – Szenarien für den Kalten Krieg,* Zürich/Berlin: Diaphanes.

Pias, Claus (2009): »›One-Man Think Tank‹. Hermann Kahn, oder wie man das Undenkbare denkt«. In: *Zeitschrift für Ideengeschichte* III/3, Herbst 2009.

Reiss, Julian (2010): »Simulation«. In: *Enzyklopädie Philosophie,* hg. v. Hans Jörg Sandkühler, Hamburg: Felix Meiner, 2457bu-2461.

Roth, Anne: Innenansicht einer Überwachung. 27.11.2013. http://annalist.noblogs.org/post/category/uberwachung-im-alltag/.

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

Solana, Javier (2003): Ein sicheres Europa in einer besseren Welt. EUROPÄISCHE SICHERHEITSSTRATEGIE. Brüssel, den 12. Dezember 2003 http://consilium.europa.eu/uedocs/cmsUpload/031208ESSIIDE.pdf.

Steinmüller, Karlheinz/Steinmüller, Angela (2004): *Wild Cards. Wenn das Unwahrscheinliche eintritt,* Hamburg: Murmann.

Weber, Jutta (2011): »Techno-Security, Risk and the Militarization of Everyday Life«. In: *The Computational Turn: Past, Presents, Futures? Proceedings of the International Association for Computing and Philosophy,* hg. v. Charles Ess, Ruth Hagengruber. Münster: Aarhus University, MV Wissenschaft, 193-200.

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

Wright, David./Friedewald, Michael/Schreurs, Wim et al. (2008): »The Illusion of Security«. In: *Communications of the ACM* 51/3, 56-63.

Zedner, Lucia (2007): »Pre-crime and Post-criminology?« In: *Theoretical Criminology* 11, no. 2, 261-281.