Sicherheitsforschung – Beiträge zu einer Bilanz

Wolf R. Dombrowsky

Die gegenwärtige Ausgestaltung von ›Sicherheitsforschung‹ wurde ganz wesentlich mit den Anschlägen vom 11. September 2001 begründet. ›Sicherheit‹ wird seitdem überwiegend als Bekämpfung gezielt induzierter Gefährdungen interpretiert, wodurch sich *security* immer mehr zu einem personalisierenden *targeting* wandelte, dem man *safety*, als Bearbeitung von Risiken, nach- und unterordnete. Am deutlichsten zeigen sich diese Veränderungen im politischen Risikodiskurs. Wurde vor 9/11 versucht, legislative wie regulative Interventionen durch Eintrittswahrscheinlichkeiten zu begründen und öffentliche Risikoakzeptanz durch Risikovergleiche zu erzeugen, beendete 9/11 weitgehend die Bezugnahme auf ›Risiko‹ als auch auf Risikovergleiche. Stattdessen rückten die Figuren der ›abstrakten Gefahr‹ und des ›Gefährders‹ in den Vordergrund und mit ihnen ein Denken, dem es auf Verhältnismäßigkeit zu anderen Risiken und zu deren Priorisierung in Relation zum erforderlichen Mitteleinsatz nicht mehr ankam.

Um also zu verstehen, warum und mit welcher Intention Sicherheitsforschung in den Fokus staatlicher Forschungsförderung rückte, muss als erstes die affektive Wucht einer Traumatisierung verstanden werden, welche die Führungsmacht der westlichen Welt erschütterte. 9/11 begründete und rechtfertigte ›den‹ Krieg gegen ›den‹ Terror. Er begann mit einem konkreten Krieg, mündete aber sehr schnell in Formen des verdeckten Kampfes, die weder die USA verschonten, noch die Prinzipien, die sie weltweit propagieren.[1] Dem Schlag nach außen folgten die Abschottung nach außen und die Absicherung im Inneren. Flughäfen und Häfen wurden zu Hochsicherheitstrakten, Güter-, Kapital- und Verkehrsströme wurden umfassender Kontrollen unterworfen, die nationale und internationale Kommunikation wurde in ihrer Gesamtheit überwacht, aus Bibliotheken und aus dem Internet wurde entfernt, was Behörden für riskant einstuften. Die Forschungsan-

1 Weltweite Empörung lösten Guantanamo (Rose 2004; Wolf 2005) und gezielte Tötungen durch Drohnen (Neskovic 2013; Rudolf 2013) aus.

strengungen der USA folgten dieser Entwicklung und sie unterstützten oder initiierten Anwendungen, die einerseits selbst eine neue Industrie samt einem neuen Markt hervorbrachten, die andererseits aber auch alle Interaktionspartner der USA zwangen, sich diesen Anwendungen und den darauf fußenden Prozeduren zu unterwerfen. Die EU leistete verschiedentlich Widerstand,[2] um letztlich aber einzusehen, dass es einer neuen Grundlage bedarf, um die Freizügigkeit des globalen Austauschs mit ebenso globalen Kontrollansprüchen geeignet auszubalancieren. Die angestrebte ›Transatlantische Handels- und Investment-Partnerschaft‹ umreißt dieses Erfordernis, während zugleich die so genannte ›NSA-Affäre‹ schlaglichtartig sichtbar machte, auf welche Weisen globale Kontrolle bereits durchgesetzt worden ist – und, wie zuvor durch ›Stuxnet‹ eindrücklich demonstriert worden war, sofort umgesetzt werden kann in operative Intervention bis hin zum Cyberwar.[3]

Die zentralen Triebkräfte zur Initiierung von Sicherheitsforschungsprogrammen auf europäischer und nationalstaatlicher Ebene ergaben sich somit beinahe zwangsläufig aus dem massiven Kontrolldruck der USA auf die Daten-, Kapital-, Personen- und Güterströme des Weltverkehrs, der Vormachtstellung der USA in allen IT-Bereichen, vor allem der Software-Entwicklung, der Hardware/Software-Ökologie, der Bereitstellung und des Betriebs von Datenbanken und Clouds und vor allem des Internets. Zudem und maßgeblich aus der Entstehung einer Sicherheitsindustrie, die für den Weltmarkt ›Sicherheitslösungen‹ anbot, die systematisch die Vorteile so zu integrieren wussten, dass ihre Nutzung die Nachteile auf Dritte überwälzte und dadurch, hinterrücks wie unvermeidbar, die reale Kontrolle verstärkte und dadurch die Vormachtstellung der USA weiter ausbaute.

Völlig zu Recht argwöhnten deshalb Unternehmen wie Sicherheitsexperten, dass ›Terror-Bekämpfung‹ nur ein trojanisches Pferd sei, mit dem in Wahrheit sowohl flächendeckende Wirtschaftsspionage betrieben als auch deutliche Entschleunigungen der Mitbewerber durch kostentreibende Kontrollmaßnahmen verursacht würden. Hinter den Kulissen wuchs der Druck

2 Beispielsweise bei der Speicherung und Weitergabe von *Passenger Name Records* (PNR) aller Fluggäste an die USA-Sicherheitsbehörden, oder von Bankdaten durch den Finanzdienstleister SWIFT.

3 Funktionsweise und Programmierung derart komplexer Backdoor-Rootkits beschreiben Nicolas Falliere, Liam O Murchu und and Eric Chien (2011). Nach Aussagen von Edward Snowden (zit. nach Thomson 2013) wurde Stuxnet von den USA und Israel entwickelt. Eine Sammlung von Artikeln und Hintergründen zur NSA-Affäre und zu Stuxnet veröffentlicht der Spiegel unter http://www.spiegel.de/thema/stuxnet/; 17.09.2013.

der Exportwirtschaft auf die Bundesregierung, diesen Wettbewerbsnachteilen Einhalt zu gebieten und zugleich Mittel bereit zu stellen, um die EU insgesamt und Deutschland im Besonderen zu unterstützen, um für die *emerging markets* eines entstehenden ›Sicherheitsindustriellen Komplexes‹[4] eigene ›Sicherheitslösungen‹ entwickeln und wettbewerbsfähig machen zu können.

Darüber hinaus gehende Bedenken existierten nicht; weder in Richtung Datenschutz noch bei Anwendungen, die kommerziell interessierende Verhaltensweisen auswerten oder im weitesten Sinne ›Muster‹ zu erkennen versuchen, aus denen sich Verhaltensprofile herleiten lassen.[5] Letztlich decken sich hier die Interessen aller Weltmarktwettbewerber, weil es jedem Teilnehmer darauf ankommt, möglichst frühzeitig ›Absichten‹ und ›Entwicklungen‹ ablesen zu können, die ›bedeutsam‹ sind. Ob es sich dabei um potenzielle Kaufabsichten von Individuen handelt, für die personalisierte Werbung adressiert wird, oder um ›Trends‹ innerhalb von ›Szenen‹, oder um politische Absichten, die bereits im Vorfeld identifiziert und dann zu ›Gefährderprofilen‹ verdichtet werden sollen, ist aus Sicht der dazu notwendigen Erhebungs- und Auswertungsinstrumente unerheblich. Von daher wäre jede Analyse falsch, die die gemeinsamen Interessen der globalen Akteure übersieht. Viel zu lange wurde die Tatsache vernachlässigt, dass ›soziale Kontrolle‹ eine Beziehungsleistung zwischen zusammen lebenden Menschen ist und diese Leistung verloren geht, wenn sich die sozialen Bande des Zusammenlebens durch die Verhaltenserfordernisse globalisierender Freizügigkeiten auflösen. Flexibilität, Mobilität und Individualisierung, vor allem aber multikulturelle Durchmischungen führen ganz zwangsläufig dazu, dass die dadurch verlierenden sozialen Kontrollen durch funktionale Äquivalente technisch instrumentell kompensiert werden müssen. Aus dieser Entwicklung speiste sich eine weitere Triebkraft zur Initiierung von Sicherheitsforschung, nämlich ein soziales Sicherheitsbedürfnis gegenüber rapidem und radikalem sozialem Wandel.

4 Dwight D. Eisenhower prägte in seiner Abschiedsrede am 17. 01. 1961 den Begriff ›military-industrial complex‹, den zuvor C. Wright Mills als »military establishment« beschrieben hatte (1956: 75). Heute ist, als Folge mehrfacher Nutzungsdurchdringungen aller involvierten Komponenten weit über Dual-use hinaus, aus dem militär-industriellen Komplex ein sicherheitsindustrieller Komplex geworden.

5 Das Unternehmen hunch.inc, New York (http://www.hunch.com) demonstriert mit seinem ›taste graph‹, was passiert, wenn man verfügbare Daten aus sozialen Netzwerken zusammenführt.

Die gesamte Security-Branche sah in diesem Wandel ihre Chance, ihre spezifischen funktionalen Äquivalente breiter verwerten und mit Hilfe staatlicher Förderung ausbauen und zudem mit Entwicklungen kombinieren zu können, die bislang vor allem auf militärische Nutzungen abgestellt waren.[6] Auch hier eröffneten sich Mehrfachnutzungen weit über das ursprüngliche Verständnis von Dual-use und von ›Synergie‹ hinaus. Seit langem verwischen sich die traditionellen Grenzziehungen zwischen Innen- und Außenpolitik, zwischen Militär- und Polizeieinsätzen, zwischen humanitärer Sofort-, Katastrophen- und Entwicklungshilfe und zunehmend auch zwischen ehedem verfassungsrechtlich strikt getrennten Diensten und hoheitlichen und privaten Aufgaben. Von daher lässt sich heute nicht mehr trennscharf zwischen Aufgabenstellungen, ›innerer‹ und ›äußerer‹ Sicherheit oder *safety* und *security* unterscheiden. Den Durchmischungen im Organisatorischen, Operativen und Politisch-Strategischen entsprechen die Kongruenzen von Verfahren und Techniken. Längst schon ist die globale Ökonomie die Organisation von Prozessen, die auf der Basis der Daten gesteuert werden müssen, die sich aus den Interdependenzen dieser Prozesse selbst ergeben, vermehrt um all jene Daten, die befördernd oder behindernd intervenieren (vgl. Baecker 1999; Miebach 2009; Ortmann 2008). Von daher ist die reale Welt weit über das hinaus, was Lars Clausen (1978; 1994) als Sonder- oder Extremform sozialen Wandels zu fassen suchte: außergewöhnlich beschleunigte (rapide) und grundlegend umwälzende (radikale) Veränderungen. Sie schrecken jedoch vor allem jene, denen die Welt zu schnelllebig erscheint, vor allem natürlich deshalb, weil sie nicht über die Mittel und Fähigkeiten verfügen, die Prozesse, denen auch sie unterworfen sind, analysieren, geschweige denn kontrollieren und am wenigsten steuernd in sie eingreifen zu können.[7]

Als politisch relevantes Potenzial schrecken diese von der modernen ›Netzwerkgesellschaft‹[8] Ent- und Abgekoppelten gleichwohl. Ihre Selbstwahrnehmung als Opfer der Modernisierung, sei es durch Verbrechen, ökonomische, soziale oder kulturelle Deprivation, forcierte die Funktions-

6 Dies gilt vor allem für die zivile Nutzung von autonomen Systemen für optische Zwecke (zum Beispiel Aufklärungsdrohnen für den Katastrophenschutz), für Bewegungsstromanalysen und für integrierte Leit- und Kommandosysteme.

7 Wer besitzt schon die Mittel und Fähigkeiten eines George Soros, »who broke the Bank of England« (Litterick 2002)?

8 So hatte Manuel Castells (2004) in seinem Werk über das Informationszeitalter das Entstehen eines neuen Gesellschaftstypus bezeichnet und daraufhin seine Kritik an deren sozialen Verwerfungen wiederholt (2012).

träger und Eliten, ›Sicherheit‹ über die klassische Interpretation von sozialer Sicherheit und Kriminalitätsbekämpfung hinaus zumindest ansatzweise in den Weiterungen der Menschenrechtspakte der Vereinten Nationen auch zum innenpolitischen Diskurs zuzulassen. Dies entbehrt nicht einer gewissen Ironie, weil die erste Generation der Menschenrechte, ohne den UN-Sozialpakt und die Fakultativprotokolle, außenpolitisch zur Legitimierung von Interventionen regelmäßig herangezogen wird.

Insgesamt ergab sich aus alledem eine ganz eigentümliche Mischung, eher ein Mischmasch, aus äußerster Interessiertheit bei gleichzeitiger Ungeklärtheit in der Sache. Jedes Partialinteresse hatte von ›Sicherheit‹ eine andere Vorstellung und folgerichtig auch andere Gründe, ›Sicherheitsforschung‹ nutzen und betreiben zu wollen. Den Forschungsgebern in der EU und deren Mitgliedsstaaten konnte dies nur Recht sein. Die Breite der Interessiertheit ließ keine grundlegenden Gegnerschaften oder Widerstände erwarten, sondern eher Gerangel bei der Zuwendung. Tatsächlich erwies sich das Forschungsprogramm als politischer Erfolg, der sich keineswegs nur der bloßen Breite von Interessiertheit verdankt.

Mit Hilfe der Sicherheitsforschungsprogramme ist es der EU und den Mitgliedsstaaten gelungen, ›Sicherheit‹ als Grundbedingung immaterieller Infrastruktur nicht nur kenntlich zu machen, sondern als gemeinsames Projekt ins Bewusstsein zu heben.

Dass ›Sicherheit‹ als gemeinsames Projekt entstehen konnte, ergab sich aus der Programmstruktur, die Forscher, Entwickler, Produzenten und Anwender zur Kooperation zwang. Trotz substantiierbarer Kritik, vor allem aus den Geistes- und Sozialwissenschaften, führten in toto die Kooperationen zu einem besseren wechselseitigen Verständnis über Fächer- und Branchengrenzen hinweg und insgesamt zur Entstehung ›kritischer Massen‹ in dem Sinne, dass nunmehr, dank der Fördermittel, mehr Menschen mehr über einschlägiges Fachwissen, branchenspezifisches Know-how, marktgerechte Anforderungen und praxistaugliche Anwendbarkeit wissen als je zuvor.

Damit korrespondiert ein pro-intuitiver Effekt: Die zahlreichen Kooperationen überwanden auch Vorurteile und Aversionen zwischen Berufsgruppen und Disziplinen, so dass eine Art ›Pool des Einvernehmlichen‹ entstand, Menschen also, die aufgrund ihrer Kooperation innerhalb des sensiblen Sicherheitsbereichs kenntlich machten, dass sie de facto verlässlicher sind, als es ihnen im Vorhinein zugetraut worden ist. Insofern hat das Sicherheitsforschungsprogramm eine Demokratisierung von Sicherheitsin-

teressen bei gleichzeitiger Nationalisierung des Bedrohungsgefühls hervorgetrieben.

Die Nationalisierung besteht vor allem darin, dass ›Sicherheitslösungen‹ für den Weltmarkt gefordert und gefördert wurden. Darin kommt notwendig die Zweischneidigkeit einer Zielsetzung zum Ausdruck, die sich aus den massiven Kontrollansprüchen der USA herleitete. Um die eigene Wirtschaft gegen Ausspähung zu schützen und international konkurrenzfähig zu machen, muss nationalisiert werden, auch gegen die EU-Mitglieder, weil sie gleichwohl Mitbewerber auf gleichen Märkten sind. An diesem Zwiespalt wird besonders deutlich, dass ›Sicherheit‹ konzeptionell weit unterkomplex angesetzt worden ist.

Noch deutlicher wird diese Unterkomplexität angesichts der großen Breite an beteiligter Interessiertheit. So sehr sie einerseits legitimiert, so sehr konterkariert sie die Entstehung eines sachlich überzeugenden Konzeptes von ›Sicherheit‹. In einem deduktiven Sinne müsste ›Sicherheit‹ zu allererst als adäquate Infrastruktur für eine globalisierte Welt verstanden werden, aus der sich dann fügende Komponenten bis hinunter zum Lokalen ableiten lassen. Der Sache nach hätten alle Komponenten der Prozesskontrolle und -steuerung und den Menschenrechtspakten zu dienen, woraus sich ganz folgerichtig die zentralen Aufgaben von Sicherheit herleiten ließen: Umwelt, Ernährung, Bildung, Arbeit und Teilhabe an Ressourcen und Kultur. Das aber wären Aufgaben, um die im globalen Zusammenhang nicht mehr konkurriert, sondern nur noch kooperiert werden kann, was wiederum zu einem ganz anderen Verständnis von sozialer Sicherheit führte.

Statt dessen führen die Sicherheitsforschungsprogramme dieser Welt zu Effekten, die so gar niemand gewollt und geplant hat und die insgesamt kontraproduktiv wirken und die globale Sicherheit hintertreiben werden: Die Scannersysteme für Häfen und Flughäfen, die Überwachungskameras und Beobachtungsdrohnen für Bewegungsströme, die Sensorik für Produktionsabläufe, die Daten der Erdbeobachtung und Navigation, die Steuerungen der Logistik, die Irisabtaster für Computerzugänge, die Chipkarten für Geldterminals – all diese hunderttausend Einzelmaßnahmen der ›Sicherheit‹ führen für jede Nation zu einer neuen, gesamtgesellschaftlichen Qualität, aus der sich wiederum eine globale Qualität ergibt. Keinem Akteur wäre eingefallen, sie vorab planen zu wollen. Sie ›entstehen‹, national wie global, und ergeben hinterrücks ›Zustände‹, deren Facetten von jedem Entwickler wie Anwender als Zuwachs von Sicherheit angepriesen werden.

Tatsächlich aber weiß niemand, um welche Zustände es sich insgesamt handelt und wie man mit ihnen umgehen sollte.

Insofern stückeln wir uns tatsächlich unter dem Verheißungsbegriff ›Sicherheit‹ eine neue Gesellschaft zusammen, die aus Tausenden alter, neuer und neuester Komponenten besteht, die, jede für sich, ein dingliches Element zu ›Sicherheit‹ beiträgt, ohne dass wir auch nur annähernd wissen, was alle Komponenten in ihrem Wirken und Zusammenwirken technisch, organisatorisch und sozial hervortreiben werden. ›Sicher‹ in einem empirischen Sinne ist dagegen nur, dass jede Komponente Daten generiert, die auf irgendeine Weise selbst wiederum ›sicherheitsrelevant‹ sind. Letztlich sollen sie ›Handeln‹ auslösen, von Menschen oder ›Nicht-Menschen‹,[9] doch wird gar nicht wirklich gehandelt, sondern nur noch exekutiert, was an Daten anschließende Daten zum Handlungsdatum machen. In dieser Konsequenz zeigt sich das Problem gegenwärtiger Sicherheitsforschung: Weil sie keine inhaltliche Bestimmung von Sicherheit zugrunde legen konnte, muss ihr jedes Mittel gleich gültig sein. Die Gleichgültigkeit der Mittel generiert jedoch eine Welt, in der jedes Mittel an seine nächste Generation anschließt, als ›Entwicklungs‹- und ›Verbesserungs‹-verheißung, ohne dass darüber ›Sicherheit‹ ihr Ziel – und noch weniger ihr Maß findet.

Literatur

Baecker, Dirk 1999: Organisation als System. Aufsätze, Frankfurt a.M.

Castells, Manuel 2004: Der Aufstieg der Netzwerkgesellschaft. Wirtschaft, Gesellschaft, Kultur. Teil 1: Das Informationszeitalter, Opladen.

Castells, Manuel 2012: Kampf in den Städten. Gesellschaftliche Widersprüche und politische Macht, Hamburg.

Clausen, Lars 1978: Tausch. Entwürfe zu einer soziologischen Theorie, München.

Clausen, Lars 1994: Krasser sozialer Wandel, Opladen.

9 Mark Weiser (1991) hatte erstmals Visionen einer Computer-Allgegenwart entwickelt, durch die sich das menschliche Zusammenleben grundlegend ändern würde. Mattern und Flörkemeier (2010) trieben die Idee des *ubiquitous computing* weiter voran. Interessanter noch sind die Überlegungen zu Menschen, die unter bestimmten Bedingungen wie ›Trivial-Maschinen‹ agieren und entsprechende Fehler generieren (vgl. Probst 1987: 46–52)

Falliere, Nicolas/O Murchu, Liam/Chien, Eric 2011: W32.Stuxnet Dossier, in: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf; 24.11.2013.

Litterick, David 2002: Billionaire who broke the Bank of England, in: http://www.telegraph.co.uk/finance/2773265/Billionaire-who-broke-the-Bank-of-England.html; 24.11.2013.

Mattern, Friedemann/Flörkemeier, Christian 2010: Vom Internet der Computer zum Internet der Dinge, in: Informatik-Spektrum 33: 2, 107–121.

Miebach, Bernhard 2009: Prozesstheorie. Analyse, Organisation und System, Wiesbaden.

Mills, C. Wright 1956: The Power Elite, New York.

Neskovic, Wolfgang 2013: Obamas Drohnenkrieg ist völkerrechtswidrig, in: http://www.cicero.de/weltbuehne/usa-obamas-drohnenkrieg-widerspricht-dem-voelkerrecht/54739; 24.11.2013.

Ortmann, Günther 2008: Organisation und Welterschließung. Dekonstruktionen, Wiesbaden.

Probst, Gilbert J.B. 1987: Selbstorganisation. Ordnungsprozesse in sozialen Systemen aus ganzheitlicher Sicht, Berlin.

Rose, David 2004: Guantanamo. The War on Human Rights, New York.

Rudolf, Peter 2013: Präsident Obamas Drohnenkrieg, in: SWP-Aktuell 37: 1–8, in: http://www.swp-berlin.org/fileadmin/contents/products/aktuell/2013A37_rdf.pdf; 24.11.2013.

Thomson, Ian 2013: Snowden: US and Israel did create Stuxnet attack code, in: http://www.theregister.co.uk/2013/07/08/snowden_us_israel_stuxnet/; 24.11.2013.

Weisser, Mark 1991: The Computer for the 21st Century, in: Scientific American 9: 94–100

Wolf, Conradin 2005: Ausnahmezustand und Menschenrecht. Unter Berücksichtigung des Falls Guantanamo, Zürich.