Digitale Besatzung

In Israel werden Techniken der Cybersicherheit zur Überwachung der Palästinenser umfassend angewandt. Daraus ist ein profitabler Industriesektor entstanden

E-Mail, Handy, Facebook, Youtube, Twitter und Instagram sind für die Palästinenser in Israel, in der Westbank, im Gaza-Streifen und in Ostjerusalem als Mittel der Verständigung immer wichtiger geworden.

18. März 2019 · Sönke Hundt

E-Mail, Handy, Facebook, Youtube, Twitter und Instagram sind für die Palästinenser in Israel, in der Westbank, im Gaza-Streifen und in Ostjerusalem als Mittel der Verständigung immer wichtiger geworden – gerade weil die Bevölkerung so in ihrer Bewegungsfreiheit eingeschränkt ist. Aber ihre digitalisierte Form eröffnet auch ganz neue und komplexe Möglichkeiten der Überwachung. Israel unternimmt mit seinem riesigen Sicherheitsapparat aus Geheimdiensten, Militär, Polizei, Zivilverwaltung, Behörden und privaten Unternehmen nicht nur riesige Anstrengungen zur Kontrolle und Beherrschung der verschiedenen Kommunikationsnetze, sondern es hat daraus eine extrem profitable Exportindustrie mit extrem hohen Wachstumsraten gemacht. Ein Bewusstsein über die damit verbundenen ethischen und moralischen Probleme oder gar eine öffentliche Diskussion darüber sind in Israel kaum vorhanden. Im Gegenteil: *„Die in den letzten Jahren entstandene Cybersicherheits-Industrie ist Israels ganzer Stolz – und sie ist direkt aus der Praxis einer jahrzehntelangen Besatzung heraus entstanden. Die Veteranen aus den Geheimdiensten sind die neue Elite, die Helden unserer Zeit, gut aussehend und vielversprechend, sie sind die stolze Zukunft unserer High-Tech-Industrien. Wer möchte nicht, dass sein Sohn oder seine Tochter in der „8200“ (die Cy-*

bersicherheits-Einheit der Armee) dient? Wer ist nicht stolz auf die Arbeit des Mossad?“

[fn]Gideon Levy in Haaretz v. 16.02.2019 – *https://bit.ly/2UGqilR*[/fn]

1. Das „Palestinian Digital Acitivism Forum 2019“ in Ramallah

Das *Arab Center for Social Media Advancement* hat vom 16. – 18. Januar 2019 in Ramallah auf einem *„Palestinian Digital Acitivism Forum 2019“* über die Cyber-Kontroll- und Überwachungstechniken informiert und diskutiert. Das Forum wurde unterstützt von der *Association for Progressive Communication (APC), Amnesty International, Human Rights Watch* und – sehr verdienstvoll! – von der *Deutschen Welle*, die am 18. Januar 2019 auch als einziges der deutschen Mainstream-Medien ausführlich über das Forum berichtete.

[fn]Vgl. Deutsche Welle v. 18.01.2019 (“Sie haben Angst vor der Wahrheit“ – Palästinenser kritisieren Israels Internetzensur) – https://www.dw.com/de/sie-haben-angst-vor-der-wahrheit-pal%C3%A4stinenser-kritisieren-israels-internetzensur/a-47132086)[/fn]

Die internationalen Teilnehmer aus Universitäten, NGOs und anderen Organisationen diskutierten auf 14 Workshops über die Gefahren und die Folgen der israelischen Cyber-Sicherheitspolitik – und über die Möglichkeiten der Gegenwehr.

[fn]Ausführliche Informationen auf der Homepage der Konferenz – https://7amleh.org/2018/12/16/7amleh-center-launches-the-full-program-and-registration-for-the-palestinian-digital-activism-forum-2019/[/fn]

Dass und wie die neuen Cyber-Sicherheits-Techniken angewandt werden und wie sie arbeiten, hat der Fall der Dichterin *Dareen Tatour,* einer palästinensischen Israelin, die in Reineh lebt, deutlich gemacht. Ihr Fall erregte internationales Aufsehen und führte zu großen Protesten. *Gideon Levy* hat in der israelischen Tageszeitung Haaretz

[fn]Haaretz v. 21.05.2016 – https://www.haaretz.com/israel-news/.premium-in-2016-israel-a-palestinian-writer-is-in-custody-for-her-poetry-1.5385083)[/fn]

über die haarsträubenden Umstände ihrer Verhaftung und ihrer Verurteilung berichtet. Um vier Uhr morgens habe die Polizei das Haus ihrer Familie gestürmt. In Handschellen sei sie abgeführt und Computer und Mobiltelefon konfisziert worden. Während der nächsten sieben Monate sei sie in drei verschiedenen Gefängnissen inhaftiert und danach für eineinhalb Jahre bis zum Beginn ihres Prozesses unter Hausarrest mit elektronischer Fußfessel und ohne Zugang zum Internet gestellt worden. Sie bekam schließlich im Juni 2018 ihren Prozess und wurde vom Nazareth District Court zu fünf Monaten Gefängnis verurteilt (und im September 2018 freigelassen). Was hatte sie verbrochen? Sie wurde verurteilt wegen „Aufwiegelung zur Gewalt und Unterstützung einer terroristischen Organisation“ aufgrund von drei Einträgen bei Facebook und einem dreiminütigen Video auf Youtube, auf dem sie eines ihrer Gedichte rezitiert hatte.

Das Gedicht beginnt:
„Resist, my people, resist them.
In Jerusalem, I dressed my wounds and breathed my sorrows.
And carried the soul in my palm
For an Arabic Palestine.“

[fn]Das Gedicht ist vollständig abgedruckt in der Übersetzung von Tariq al Haydar in ArabLit – Arabic Literature and Translation – https://arablit.org/2016/04/27/the-poem-for-which-dareen-tatours-under-house-arrest-resist-my-people-resist-them/; der Youtube-Film hier:https://www.youtube.com/watch?v=R1qnlN1WUAA)[/fn]

Dareen Tatour war über die lange Haft und über das Urteil fassungslos. *„Ich hätte niemals geglaubt, dass ich wegen eines Gedichtes verhaftet werden könnte. […] Ich kann nicht leben ohne meine Gedichte. Ich weiß, dass sie mich jetzt nicht mehr allein lassen werden. Sie werden alles, was ich schreibe, überwachen und kontrollieren. Sie wollen, dass ich aufhöre zu schreiben. Aber ich kann nicht aufhören damit, um meine getöteten Schicksalsgenossen zu trauern. Ich will weiter Gedichte schreiben. Ich werde deshalb tun, was jeder Dichter, der frei sein will, tun würde: ich werde mein Land verlassen. Ich werde woanders leben müssen.“*

[fn]Vgl. zuletzt Haaretz v. 20.09.2018 – https://www.haaretz.com/israel-news/israeli-arab-poet-dareen-tatour-convicted-of-incitement-released-from-prison-1.6491021[/fn]

2. Die „digitale Besetzung“ Palästinas

Dareen Tatour ist kein Einzelfall, sie ist nur ein Beispiel für die Realität der *„digitalen Besatzung“*, wie es auf dem *Palestinian Digital Acitivism Forum 2019* in Ramallah formuliert wurde. Wenn es Israel es fordert, werden auf den großen Social-Media-Plattformen entweder einzelne Post oder ganze Accounts gelöscht. Israel prahlt regelrecht damit, wie *„gefügig Facebook sein kann, wenn es um israelische Zensurbefehle geht.“*

[fn]So Glenn Greenwald in The Intercept v. 30.12.2017 – https://theintercept.com/2017/12/30/facebook-says-it-is-deleting-accounts-at-the-direction-of-the-u-s-and-israeli-governments/[/fn]

Im März 2017 ist sogar der gesamte Facebook-Account der Partei Fatah mit Millionen Followern zeitweilig gesperrt worden. Dem Bericht in „The Intercept“ zufolge war auf einer Seite ein altes Foto von Jassir Arafat zu sehen, das ihn mit einem Gewehr in der Hand gezeigt habe. Die Begründungen, die von Israels Behörden für diese Art von Zensur genannt werden, sind immer ähnlich: es handele sich um „incitement“, also Aufwiegelung bzw. Anstiftung zum Terror. Der Vorwurf des „incitement“ wird asymmetrisch verwendet; sie geht nur von Palästinensern aus. Wenn radikale jüdische Siedler in den sozialen Medien zu direkter Gewalt mit Worten wie „töten“, „Mord“ oder „verbrennen“ aufrufen, wird das nicht beanstandet. Hier finde keinerlei Zensur statt.

[fn]Vgl. den Bericht auf Sputniknews v. 30.12.2017 – https://de.sputniknews.com/poli-

tik/20171230318903236-facebook-fuegt-sich-den-befehlen-israels-und-usa/)[/fn]

3. Predictive policing und proaktive Verhaftungen

Die rigide Durchführung von Zensurmaßnahmen ist der erste Schritt des Cyber-Sicherheitsnetzes, dem weitere folgen. 2015 wurde damit begonnen, ein geradezu Orwellsches Online-Überwachungssystem aufzubauen, das die gesamte private Kommunikation einbezieht, also Telefon- und Chatprotokolle, Log-Dateien, Profile in sozialen Medien, Freundschafts- und Likes-Netze, Bewegungsprofile über GPS-Tracking, online-Bestellungen und online-Zahlungsverkehr usw. usf. Dank Big-Data und Künstlicher-Intelligenz-Techniken wird all das verbunden mit den Daten der israelischen Behörden (Polizei, Geheimdienste, Militär) und mit Hilfe algorithmischer Verfahren zu Vorhersagen künftiger Straftaten verdichtet und damit das berüchtigte „predictive policing" praktiziert. Wie auf dem *„Palestinian Digitial Activism Forum 2019"* berichtet, sind aufgrund dieses Systems allein im Jahr 2018 *vorbeugend*, also ohne dass eine Straftat oder ein auch nach israelischer Auffassung strafbares Vergehen vorlag, über 350 „proaktive Verhaftungen" vorgenommen worden. Genaue Zahlen werden von den israelischen Behörden nicht bekannt gegeben.

[fn]So die Deutsche Welle in ihrem Bericht. v. 18.01.2019 – https://www.dw.com/de/sie-haben-angst-vor-der-wahrheit-pal%C3%A4stinenser-kritisieren-israels-internetzensur/a-47132086[/fn]

„Predictive policing" wird in Israel nicht weiter problematisiert. Im Gegenteil, die israelischen Behörden sind durchweg stolz auf ihre Praxis, und sie verweisen auf Erfolge. Nach *Gilad Erdan,*Israels Minister für Sicherheit, sei die Zahl der Terroranschläge seit Beginn des „predictive policing"-Programms um 80 Prozent zurückgegangen. Der Algorithmus, der die Vorhersagen aus dem vorliegenden Big-Data-Material generiere, sei nach den vielen Jahren des Terrors immer treffsicherer geworden, so *Roni Alsheich*, Israels oberster Polizeichef (police commissioner). Auch Premierminister Benjamin Netanyahu war des Lobes voll über diesen „wunderbaren Algorithmus". Man müsse eben, meinte er, die Balance halten zwischen den Sicherheitsanforderungen einerseits und einem „Abgleiten in die Diktatur" andererseits.

Die Washington Post hat in Bezug auf diese Balance so ihre Zweifel. Die israelische Praxis werfe doch ernsthafte Fragen in Bezug auf solche traditionellen westlichen Werte auf wie Völkerrecht, Schutz der Privatsphäre, Freiheit der Meinungsäußerung und überhaupt den Menschenrechten. Viele Menschenrechtsgruppen würden kritisieren, dass Palästinenser wegen unbestimmt bleibender und von Algorithmen generierter „Incitement"-Anschuldigungen verfolgt würden.

[fn]Vgl. den ausführlichen Bericht in der Washington Post v. 09.07.2018 – https://www.washingtonpost.com/world/middle_east/israel-says-that-monitoring-social-media-has-cut-lone-wolf-attacks-palestinians-are-crying-foul/2018/07/08/bfe9ece2-7491-11e8-bda1-18e53a448a14_story.html?utm_term=.1d6845f6b812)[/fn]

4. Die israelische Cybersicherheitsindustrie: „moralfreie Disruption“

Israel ist schon lange der Meinung, dass es in seiner Besatzungspraxis an Völkerrecht und Menschenrechte nicht gebunden ist. Mehr noch: aus den Techniken der Kontrolle, Beherrschung und Unterdrückung der Millionen Palästinenser hat sich eine blühende Rüstungs- und Sicherheitsindustrie entwickelt, die heute einen der wichtgsten Industriezweige des Landes darstellt. In dem Film „The Lab“ von *Yotam Feldman* aus dem Jahr 2013 wurde die Hardwareseite des Waffenarsenals eindrucksvoll mit Gewehren, die um die Ecke schießen, mit ferngesteuerten Aufklärungs- und Kampfrobotern, Killerdrohnen, Raketenabwehrsystemen („iron dome“) und anderem Aufstandsbekämpfungs- und Tötungswerkzeug präsentiert. Inzwischen sind die Cyber-Techniken zum neuen Exportschlager und Israel zur „digitalen Supermacht“, zum „Global Hotspot“ der digitalen Sicherheitstechnik geworden. *„In wenigen Jahren ist die israelische Cyberindustrie zur Speerspitze des internationalen Handels mit Produkten der Überwachungs- und Abhörtechniken aufgestiegen. Heute ist jeder Dienst, der etwas auf sich hält und keinen übertriebenen Respekt vor solchen Dingen wie Privatsphäre hat, ausgerüstet mit den Spionage-Werkzeugen, die in Herzliya Pituach entwickelt wurden.“*

[fn]*Vgl. Haaretz v. 20.10.2018 – https://www.haaretz.com/misc/article-print-page/.premium.MAGAZINE-israel-s-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays-1.6573027)*[/fn]

Werner Rügemer bestätigt dieses Ergebnis: Israel ist *„das höchstentwickelte Digitallabor der westlichen Welt für die Bekämpfung von Aufständen und die Tötung von Menschen, die von Geheimdiensten ohne Gerichtsurteil als Terroristen bezeichnet werden. […] Mit bisher 5.000 Start-ups, die mehrheitlich von US- und anderen Weltkonzernen gekauft wurden, hat Israel die höchste Start-up-Dichte pro Einwohner. […] Die völkerrechts- und menschenrechtswidrige Praxis des jahrzehntelangen Besatzungsregimes ist ein Trainingscampus der moralfreien Disruption.„*

[fn]*Werner Rügemer: Die Kapitalisten des 21. Jahrhunderts, Köln 2018, S. 186)*[/fn]

Diese neue Industrie, ihre Produkte, das dazugehörende Consulting und Marketing, die begleitenden Dienstleistung und schließlich ihre Anwendungspraxis sind unauflöslich mit den nationalen und internationalen Geheimdiensten verwoben – und dementsprechend unter einem dichten Schleier der Geheimhaltung verborgen. Über die Kunden in vieler Herren Länder wird nicht einmal der zuständige Ausschuss der Knesset (Foreign Affairs and Defense Committee) informiert. Das israelische Verteidigungsministerium weigert sich beharrlich, die Länder zu bennen, in die Cyber-Sicherheit-Produkte exportiert werden. Aber eine ganze Menge ist inzwischen dennoch bekannt geworden. Am 20.10.2018 hat die israelischen Tageszeitung Haaretz in einer umfangreiche Recherche diesen ganzen Komplex untersucht und unter dem Titel „Revealed: Israel’s cyber-spy industry helps world dictators hunt dissidents and gays“ veröffentlicht.

[fn]*Vg. Haaretz v. 20.10.2018. (https://www.haaretz.com/misc/article-print-page/.premium.MAGAZINE-israel-s-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays-1.6573027*[/fn]

Das Haaretz-Team befragte 100 fachkundige Personen aus 15 Ländern, um den Schleier wenigstens etwas zu lüften. Was vermutet wurde, konnte bestätigt werden. Die Cyber-Sicherheits-Industrie hat nicht gezögert, ihre Produkte und Dienstleistungen auch an solche Länder zu verkaufen, „die nicht eben über eine besonders starke demokratische Tradition verfügen". Verkauft wurde an jeden, der zahlte: Bahrain, Indonesia, Angola, Mozambique, the Dominican Republic, Azerbaijan, Swaziland, Botswana, Bangladesh, El Salvador, Panama, Nicaragua, Malaysia, Vietnam, Mexico, Uzbekistan, Kazakhstan, Ethiopia, South Sudan, Honduras, Trinidad and Tobago, Peru, Colombia, Uganda, Nigeria, Ecuador and United Arab Emirates. Die Zeugenaussagen haben deutlich gemacht, „dass israelische Produkte in vielen Fällen dazu benutzt wurden, Menschenrechtsaktivisten zu lokalisieren und festzunehmen, Mitglieder der LGBT-Community zu verfolgen und Bürger, die ihrer Regierung gegenüber kritisch eingestellt sind, zum Schweigen zu bringen. Israelische Unternehmen verkauften ihre Spionage-Produkte, auch wenn öffentlich geworden war, für welche bösartigen Zwecke (malicious purposes) sie eingesetzt wurden." Die Rechtfertigung für diese Praxis sei immer ähnlich gestrickt gewesen: die Exporte dienten der Verbrechens- und der Terrorbekämpfung und seien vom Verteidigungsministerium autorisiert worden.

Genaue Zahlen über Umsatz, Marktanteil, Marktwachstum, Kapitalausstattung und Profite von Unternehmen der neuen Cyberindustrie sind aus Geheimhaltungsgründen nicht bekannt. Aber der finanzielle Erfolg dieser Industrie muss wohl schwindelerregend (dizzying) sein, so die Haaretz-Recherche, und sie lockt jede Menge Risikokapital aus aller Welt an. Die 27 größten Cyber-Sicherheits-Unternehmen aus Israel würden heute über einen Marktanteil von weltweit 10 bis 20 Prozent in dieser Branche verfügen; im Jahr 2016 seien 20 Prozent aller Investitionen im Cyber-Sicherheitssektor in israelische Start-ups geflossen.

5. Die NSO-Group Technologies, Tel Aviv

Ein gutes Beispiel für die Goldgräberstimmung in dieser Industrie ist die NSO Group Technologies (Hauptsitz in Herzliya bei Tel Aviv, 500 Mitarbeiter). NSO wurde 2010 als Start-up gegründet von einer Gruppe „Alumni" aus der Armeeeinheit 8200 unter Führung des pensionierten Generals Avigdor Ben-Gal, der vorher Chef der israelischen Luftfahrtindustrie war. 2014 wurde das Unternehmen von den Gründern an die Private-Equity-Firma Francisco Partners für 130 Millionen Dollar verkauft, die es schon ein Jahr später für 1 Milliarde Dollar weiterverkaufen konnte. Der meiste Umsatz und der höchste Profit werden von der inzwischen berühmt und berüchtigt gewordene Mobiltelefonspionagesoftware „Pegasus" generiert. Sie soll es ermöglichen, die GPS-Daten und die komplette Kommunikation eines Handys (iMessage, Gmail, Viber, Facebook, Whatsapp, Telegram und Skype sowie Wifi-Passwords auszulesen und Kamera sowie Mikrofon ein- auszuschalten.

[fn]*Angaben nach Wikipedia – https://en.wikipedia.org/wiki/NSO_Group*[/fn]

Die New York Times berichtete am 02.09.2015

[fn]*The New York Times v. 02.09.2015*

– *https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html*[/fn]

auch über Preise für diese Wunderwaffe. Für das Ausspionieren von zehn iPhones würde NSO 650.000 Dollar plus einer einmaligen Einrichtungsgebühr von 500.000 Dollar berechnen. Geliefert worden seien die Spionagetools an die Regierungen von Israel, Türkei, Thailand, Qatar, Kenia, Uzbekistan, Mozambique, Marokko, Yemen, Ungarn, Saudi Arabien, Nigerien und Bahrain. Besonders bekannt wurde die Software, da sie das tracing des arabischen Washington-Post-Korrespondenten Jamal Khashoggi, der am 2. Oktober 2018 in der Saudi-arabischen Botschaft in Istanbul ermordert wurde, ermöglicht habe.

6. Die Erfahrungen aus 50 Jahren Besatzung werden kapitalisiert

Die Entstehung der israelischen Cyber-Sicherheits-Industrie, ihre spektakulären Erfolge und riesigen Profite, sind ohne die Erfahrungen aus der Besatzung nicht denkbar. Aus den Karrierewegen vieler führender Manager ist dieser Prozess gut rekonstrierbar. Viele von ihnen hatten vorher Führungspositionen in der IDF bzw. in den Geheimdiensten inne; sie wurden früh pensioniert (in der Regel mit 46 Jahren) und gingen dann in die hoch bezahlten Jobs der Sicherheitsindustrie bzw. gründeten selber Start-ups. Auch die jungen Rekruten der IDF spielen eine wichtige Rolle. „Jedes Jahr hängen zwischen 1.500 und 2.000 topgeschulte Computerfreaks ihre Uniform an den Nagel, hungrig danach, ihre Erfahrungen zu Geld zu machen. Besonders begehrt sind die Alumni der legendären Spionageeinheit 8200, der heute größten Militäreinheit Israels. Vorbei die Zeiten der muskelstrotzenden Nahkampfmaschinen, hoch lebe der Mathe-Nerd.“, so die Taz voller Bewunderung in einem ausführlichen Bericht v. 10.01.2017

[fn]*Vgl. Taz v. 10.01.2017 (15)– http://www.taz.de/!5369118/*[/fn]

.

Israels Besatzungpraxis wird gewissermaßen globalisiert („has gone global“), so der jüdisch-australischer Journalist Antony Loewenstein in einem informativen Bericht („Israel selling decades of occupation knowledge to any bidder“ in der renommierten The New York Review of Books v. 06.01.2019. Das Know-how aus der Besatzungspraxis würde in Produkte verpackt und verkauft an Regierungen, Unternehmen und Privatpersonen, die eben dieses Know-how bewundern und selber nutzen wollen. Saar Korush von der Firma Magal Security Systems (sie produziert die Hard- und Software für Sicherheitszäune bzw. -mauern aller Art und bewirbt sich gerade für Trumps Absperrungen an der mexikanischen Grenze), hat das völlig ungeniert so formuliert: „Gaza war ein showroom für unsere Produkte. Kunden schätzen es, wenn das, was sie kaufen, schon im Kampf getestet und erprobt wurde.“

[fn]*Antony Loewenstein: Israel selling decades of occupation knowledge to any bidder. In: The New York Review of Books v. 06.01.2019 – http://antonyloewenstein.com/2019/01/06/israel-selling-decades-of-occupation-knowledge-t*

o-any-bidder/[/fn]

Die Technik der Besatzung ist nur systemisch zu begreifen. Es ist der Versuch, rund sechs Millionen Palästinenser zu kontrollieren, zu beherrschen und die Kontrolle soweit wie möglich auf technische Systeme zu übertragen. Jeff Halper hat dafür den treffenden Begriff der „Matrix of Control" geprägt. Entstanden sei so ein komplexes Hightech-System aus Mauern, Zäunen, Checkpoints, Patrouillen, Drohnenüberwachung, Internet- und Telefonspionage usw. usf. Die „Matrix" werde abgesichert und perfektioniert durch ihre Legalisierung innerhalb eines kafkaesken Geflechts aus Gesetzen, Erlassen, bürokratischen Regulierungen und der entsprechenden Rechtssprechung.

[fn]*Vgl. ausführlich Shir Hever: The Privatization of Israeli Security, London 2018, S. 52 ff. und Jeff Halper: The Palestinians. Warehousing a ‚Surplus People,. In: palestine chronicle v. 11.09.2008 –http://www.palestinechronicle.com/warehousing-a-surplus-people/*[/fn]

Wie gesagt, über ethische und moralischer Probleme dieser Industrie wird in Israel kaum diskutiert. Die Produktion und der Export von Waffen und Waffensystemen aller Art entspricht der israelischen Staatsraison. Was zähle in der internationalen Politik sei allein militärische Stärke, nur sie könne Israel in einem Meer von Feinden Schutz bieten. Israels Ministerpräsident Benjamin Netanyah hat das mal so auf den Punkt gebracht: „Stärke und Macht sind die wichtigsten Komponenten in der internationalen Politik. Es gibt Länder, die ganze Bevölkerungen erobert und vertrieben haben – und die Welt schwieg dazu. Stärke ist der Schlüssel, sie macht den Unterschied aus zwischen uns und der Welt der Araber."

[fn]*Zitiert von Antony Loewenstein in seinem schon genannten Artikel*[/fn]

Und andererseits zählt das Geld. Gideon Levy beschreibt scharfzüngig und voller Verachtung die Szene der jungen High-Tech-Cyber-Krieger in Tel Aviv. „Es gibt viele Erfolgsgeschichten jetzt. Und das Spiel geht so: gründe ein Start-up und verkaufe es schnell wieder für viel Geld. In ihren T-shirts, Sneakers und Jeans machen die jungen Leute im Handumdrehen viel Geld. In ihren Pausen am Nachmittag bestellen sie Sushi und spielen die Video-Spiele ‚FIFA 17' und ‚Mortal Combat'. Die meisten kommen aus der ‚8200'. Aber unter ihren eindrucksvollen Erfolgen ist Verwesung (beneath their impressive successes, there is rot)… Es gibt nichts, was sie nicht für Geld tun würden."

[fn]Gideon Levy in Haaretz v. 16.02.2019 https://bit.ly/2UGqiIR[/fn]

Nicht auszuschließen ist, dass Israel an seiner unglaublichen Hybris auch scheitern kann. Für Shir Hever, Autor von „The Privatization of Israel Security" (London 2018), ist es schon ausgemacht, dass die jahrzehntelange Besatzung für Israel zunehmend zur Belastung wird und als Verkaufsargument an Wert verliert – eben weil es offentsichtlich ist, dass letztendlich der palästinensischen Widerstand nicht gebrochen werden konnte. Autoritäre Regime in aller Welt seien zwar immer noch daran interessiert, von Israels Methoden der Unterdrückung und Aufstandsbekämpfung zu lernen. „Aber", so Hever, „ich befürchte, dass Israel immer mehr für seinenRassismus, seine Methoden des racial profiling und seinen Nationalismus bewundert wird und die Überzeugung schwindet, dass es über das 'stärkste Militär der Welt' verfügt." Antony Loewenstein malt schließlich in seinem Artikel das Beispiel Südafrika als

Menetekel an die Wand. Und Israel sollte diese Warnung der Geschichte nicht überhören! „Auf seinem Höhepunkt war Südafrika einer der größten Waffenhändler weltweit. Trotz des Waffenembargos, das damals von den Vereinten Nationen verhängt wurde, betrugen in den späten 1980er Jahren die Rüstungsausgaben Südafrikas 28 Prozent des Staatshaushalts. Eine Ökonomie, die ihren Erfolg auf militärisches Know-how und auf der Expertise in Techniken der inneren Repression gründet , mag stark erscheinen. Aber die Apartheid war fünf Jahre später am Ende.“ [fn]Zitate auch von Hever in dem Artikel von Antony Loewenstein[/fn]

7. Israel als Vorbild für Europa?

Die enge Zusammenarbeit von Staat, Militär, Polizei, Geheimdiensten und Besatzungsbehörden, verbunden mit einer nur geringen Rücksichtnahme auf Dinge wie Privatsphäre, Datenschutz, Menschenrechte und Völkerrecht ist in der Bundesrepublik Deutschland nicht möglich. Aber diskutiert wird schon darüber. „Die israelischen Ansätze können und wollen wir in Europa nicht übernehmen. Weder wollen wir die Bevölkerung bewaffnen noch grundlegende Bestandteile des Datenschutzes aushebeln oder ganze Bevölkerungsgruppen wegen einiger potenzieller Täter überwachen und schärfer kontrollieren.“ Aber: „Deutschland und Europa kommen nicht umhin, eigene Antworten auf die veränderte Bedrohungslage zu finden. Eine wichtige Komponente sind starke Sicherheitsbehörden, die nicht nur ermitteln, wenn bereits ein Anschlag verübt wurde, sondern deren Ziel es ist, Anschläge zu verhindern.“

[fn]*So wurde es mal formuliert im im Blog Sicherheit.info v. 26.09.2017 –https://www.sicherheit.info/mit-technologien-gegen-kriminalitaet-und-terror*[/fn]

Seit den Anschlägen vom 9. September 2001 und vermehrt nach dem LKW-Attentat Weihnachten 2016 auf dem Breitscheidplatz in Berlin ist die „innere Sicherheit“ das große Thema für die Politik, die Medien, die Sicherheitsbehörden aller Art und die einschlägige Industrie. „Sicherheit besser vernetzen – Information – Prävention – Repression“ – das war das Thema des Europäischen Polizeikongresses in Berlin (v. 6. – 7. Februar 2018), auf dem etwa 1800 Entscheider auf über 25 Fachforen die faszinierenden Möglichkeiten und Probleme der neuen Cyber-Sicherheits-Techniken erörterten. Ein Vertreter des Bundesinnenministeriums stellte auf dem Kongress die Pläne für ein „Digitales Haus der Polizei“ vor und BKA-Präsident Holger Münch referierte über die geplanten technischen Modernisierungen und Zentralisierungen bei der Polizei unter dem Kürzel „Polizei 2020“.

[fn]*Ausführliche Informationen über den Polizeikongress auf heise.de v. 06.02.2018 –https://www.heise.de/newsticker/meldung/Europaeischer-Polizeikongress-Regierungskoalition-baut-Digitales-Haus-der-Polizei-3961405.html und auf der sehr informativen polizeikritische Plattform police-it.org mit dem großen neunteiligen „Palantir-Dossier – https://police-it.org/das-palantir-dossier.Auf dem Europäischen Polizeikongress 2019 (v. 19. – 20.02.2019) werden die einschlägigen Themen weiter präsentiert und diskutiert. Das Motto heißt dieses Jahr „Europa – Migration – Integration – Sicherheit“. Vgl. die Homepage des Kongresses – https://www.europaeischer-polizeikongress.de/*[/fn]

Glaubt man den Versprechen der einschlägigen IT-Industrie, die natürlich ihre Systeme auf

den Polizeikongressen präsentieren konnte, sind die technischen Möglichkeiten schier unbegrenzt. Besonders das us-amerikanische Unternehmen Palantir mit seinen Produkten „Palantir Gotham“ und „Palantir Metropolis“ (Namen in Anlehnung an J.R.R. Tolkiens Roman „Herr der Ringe“) übt zur Zeit auf alle Sicherheits-Experten eine düstere Faszination aus, verspricht es doch nichts weniger als eine total gewordene Überwachung in Gegenwart, Vergangenheit und in die Zukunft hinein. Palantir hat vor kurzem den ersten Schritt in den großen deutschen und europäischen Markt der inneren Sicherheit geschafft, nämlich in das Bundesland Hessen. Das Palantir-Produkt heißt hier „Hessendata“ und kann viele Quellen nutzen: drei Polizeidatenbanken für Kriminalfälle und Fahndungen, die Verbindungsdaten aus der Telefonüberwachung, Daten aus ausgelesenen Handys und vor allem Daten aus den sozialen Medien. Glaubt man den Berichten, kann die hessische Polizei z.B. alle Informationen aus bestimmten Facebook-Profilen von Verdächtigen erhalten, nachdem sie ein Rechtshilfeersuchen an US-Behörden zur Bereitstellung der Datensätze gestellt hat.

Im Oktober 2018 wurde das System der Presse vorgestellt, und der Reporter der Süddeutschen Zeitung war fasziniert: „Verborgenes wird sichtbar, wenn Kriminalhauptkommissar Otto an seinem Laptop ‚Gotham‘ aktiviert. Zum Beispiel Linien zwischen Portraitfotos mürrisch dreinblickender Salafinsten, ihren Kontaktpersonen und Handyicons, unter denen Telefonnummern stehen, die zu weiteren Personen führen. Otto zieht einen Namen mit der Maus auf ein Feld namens ‚Graph‘ – und die Gotham-Software baut ein weiteres Spinnennetz aus Informationen auf dem Bildschirm auf. Wann die Überwachten mit wem telefonierten, zu welcher Islamisten-Gruppe sie gehören, welche Waffe und welches Auto zu welcher Person gehören. Die Software ist wie ein zweites Gehirn für Polizisten, ein Gehirn mit Röntgenblick, das in einer Sekunde Dutzende Verbindungen erkennt. ‚Das hätten wir früher nie und nimmer gefunden‘, sagt Otto, und meint die Zeit, als sich Polizisten stunden- oder gar tagelang durch viele Datenbanken klicken mussten. Hauptkommissar Otto […] sitzt tief im Bauch des Frankfurter Polizeipräsidiums, wo ein Aufkleber an einer Tür auf Hessisch verkündet ‚Mir basse uff!‘ Otto ist Teil eines kleinen Teams, das seit 2017 für das Land Hessen die Zukunft der Polizeiarbeit testet – oder, aus Sicht der Skeptiker: die Zukunft des Überwachungsstaates. 200 Staatsschützer sind im Umgang mit Gotham, das nach Batmans Heimatstadt benannt ist, schon geschult.“

[fn]*Süddeutsche Zeitung v. 18.10.2018: Palantir in Deutschland. Wo die Polizei alles sieht –https://www.sueddeutsche.de/digital/palantir-in-deutschland-wo-die-polizei-alles-sieht-1.4173809*[/fn]

Ein erster Erfolg konnte auch schon präsentiert werden. Nach der Auswertung von Chats hätten die Ermittler im Februar 2018 einen 17-Jährigen festnehmen können, der dabei war, eine Bombe zu bauen. Frankfurts Polizeipräsident Gerhard Bereswill war begeistert; man realisiere mit „Hessendata“ einen Quantensprung in der Polizeiarbeit.

Nachprüfen lässt sich das selbstverständlich nicht – und offene Fragen gibt es natürlich reichlich. Was ist mit dem verfassungsrechtlich gebotenen Trennungsverbot von Polizei und Geheimdiensten, was mit Datensicherheit, Datenschutz, Persönlichkeitsschutz, Informationsfreiheit und überhaupt den Menschenrechten? Aus welchen Datenquellen wird geschöpft, mit welchen Geheimdiensten wird wie zusammengearbeitet, welche vertraglichen Verpflichtun-

gen geht das Land Hessen ein? Nach intensiven Diskussionen über Palantir im Hessischen Landtag hat es die Opposition (SPD und FDP) zwar geschafft, einen parlamentarischen Untersuchungsausschuss einzusetzen, dessen Ergebnisse auch schon vorliegen. Aber leider hat sich der Untersuchungsausschuss nur um das Preismodell von Palantir und um die Modalitäten der Auftragsvergabe gekümmert, die viel interessanteren bürgerrechtlichen Fragen jedoch leider nicht untersucht.

[fn]*Nähere Informationen hier: Palantir-Untersuchungsausschuss in Hessen. police-it.org v. 22.01.2019 –https://police-it.org/palantir-untersuchungsausschuss-in-hessen-was-rausgekommen-ist*[/fn]

Seit 2014 werden im Bund und in allen Bundesländern die Polizeigesetze und teilweise die Verfassungsschutzgesetze der Länder auf breiter Front modernisiert und vereinheitlicht. Die deutschen Polizeibehörden und Geheimdienste erhalten gegenwärtig Eingriffsbefugnisse und digitale Cyber-Sicherheits-Techniken, die noch vor wenigen Jahren unvorstellbar waren. Geradezu einen Paradigmenwechsel in Richtung „predictive policing" stellt die Unterscheidung von „konkreter" und „drohender" Gefahr. Bis jetzt durfte die Polizei nur bei „konkreter Gefahr", die unmittelbar bevorsteht, tätig werden. Künftig soll für Verhaftungen die „drohende Gefahr", also „die Wahrscheinlichkeit einer Straftat in einer überschaubaren Zukunft", reichen. Es ist der „krasseste Ausdruck der präventiven Orientierung" und stellt eine echte Innovation im bundesdeutschen Polizeirecht dar. Was ist unter einer „drohenden Gefahr zu verstehen?" fragt Maria Scharlau, Expertin für Polizei und Menschenrecht bei Amnesty International. „Wochen? Monate? Jahre? Das Problem ist, dass die vagen Voraussetzungen für solche Annahmen wirklich mit allem und nichts gefüllt werden können. […] Diese Vorverlagerung der Befugnisse für sehr einschneidende polizeiliche Maßnahmen ist eins der Hauptprobleme. Das öffnet der subjektiven Auslegung durch die Polizei Tür und Tor."

[fn]*Dazu ausführlich Matthias Becker: Predictive Staatsschutz. in: Telepolis v. 06.07.2018 –https://www.heise.de/tp/features/Predictive-Staatsschutz-4096468.html und ders.: Datenkrake Polizei? Palantir als die Spitze des Eisberges. in: Telepolis v. 22.06.2018 –https://www.heise.de/tp/features/Datenkrake-Polizei-Palantir-als-die-Spitze-des-Eisberges-4090056.html?seite=all*
Das Gespräch mit Maria Scharlau auf netzpolitik.org v. 25.01.2019 – https://netzpolitik.org/2019/amnesty-zu-neuen-polizeigesetzen-diese-entwicklung-nicht-einfach-hinnehmen/[/fn]

Das Land Bayern hat die „drohende" Gefahr in seinem neuen Polizeigesetz schon beschlossen. Andere sollen folgen. Der Modernisierungsprozess der Polizei und der Geheimdienste wird kritisch begleitet von vielen Diskussionen, Protesten und Demonstrationen. Im Mai 2018 demonstrierten in München 30.000 Menschen; in Dresden gingen zuletzt am 26. Januar 2019 5.000 Menschen aus Protest auf die Straße.

Anmerkungen