

Im Auge der Partei

Autor(en): **Andersen, Ross**

Objektyp: **Article**

Zeitschrift: **Schweizer Monat : die Autorenzeitschrift für Politik, Wirtschaft und Kultur**

Band (Jahr): **100 (2020)**

Heft 1082

PDF erstellt am: **16.05.2024**

Persistenter Link: <https://doi.org/10.5169/seals-914692>

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Im Auge der Partei

Der Überwachungswahn der Kommunistischen Partei Chinas betrifft uns alle. Mittels künstlicher Intelligenz macht sie eine Dystopie zur Realität.

von Ross Andersen

Nördlich von Pekings Verbotener Stadt, ausserhalb der dritten Ringstrasse, baut die Chinesische Akademie der Wissenschaften seit 70 Jahren an einem Campus staatseigener Labore. Hier befindet sich das Institut für Automatisierung, ein glänzend silberblaues Gebäude, umgeben von kamerabestückten Stahlmasten. Das Institut betreibt Grundlagenforschung. Informatiker zerbrechen sich hier die Köpfe über die fundamentaltheoretischen Geheimnisse der künstlichen Intelligenz. Die eher praktischen Anwendungen dieser Technologie – Iriserkennung, cloudbasierte Spracherkennung – werden an chinesische Technologieriesen, KI-Start-ups und bisweilen auch an die Volksbefreiungsarmee ausgegliedert.

Ich besuchte das Institut an einem regnerischen Sommermorgen im Jahr 2019. Chinas Elite schlurfte herein, gerade erst den Pendlerzügen entstiegen, bequem gekleidet in Basketballshorts oder Yogahosen, AirPods in den Ohren. In meiner Tasche hatte ich ein Wegwerfhandy, in meinem Rucksack einen Computer, der – gemäss dem Standardprozedere für westliche Journalisten auf Reisen nach China – von allen Daten gereinigt worden war. Wer in sensibler Mission nach China kommt, riskiert, mit einem Sperrfeuer von Cyberangriffen und Malware bombardiert zu werden. 2019 etwa bemerkten Angehörige einer belgischen Handelsdelegation in Peking, dass ihre Mobildaten von vor dem Hotel aufgepflanzten Antennen abgefangen wurden.

Nachdem ich den Sicherheitscheck des Instituts überstanden hatte, schickte man mich weiter in einen kameraüberwachten Warteraum. An der Wand hingen Plakate der einflussreichsten

Nachkriegspolitiker. Mao Tse-tung prangte hier in seinem ikonischen Anzug mit den vier Taschen. Er sah heiter aus – zufrieden, China vom Joch des Westens befreit zu haben, konnte man meinen. Neben ihm hing ein unscharfes Schwarzweissfoto von Deng Xiaoping bei einem Besuch im Institut während seiner späteren Jahre, nachdem er Chinas Wirtschaft reformiert und das Land so auf den Weg gebracht hatte, seine angestammte Grossmachtrolle wieder einzufordern.

Das augenfälligste Plakat zeigte Xi Jinping im makellosen schwarzen Anzug. Chinas derzeitigem Präsidenten und Generalsekretär der Kommunistischen Partei Chinas liegt das Institut sehr am Herzen; es ist Teil einer grossangelegten KI-Strategie, die Xi in einer Reihe von Ansprachen dargelegt hat – ähnlich jenen, mit denen einst John F. Kennedy den Mond in den Fokus der amerikanischen Forschung rückte. Laut Xi sollte China bis Jahresende zu den führenden KI-Mächten der Welt aufschliessen. Dieses Ziel hat das Land wohl bereits heute schon erreicht. Bis 2030 soll China das KI-Rennen ganz für sich entschieden haben.

Xis Ankündigungen haben einen bedrohlichen Beiklang. Künstliche Intelligenz ist in fast allen Bereichen anwendbar, von der Echtzeitübersetzung gesprochener Sprache bis zur Früherkennung von Virusepidemien. Doch Xi will die Technologie mit ihrem enormen Analysevermögen auch dazu nutzen, in China einen futuristischen Überwachungsstaat zu errichten. Er will ein allsehendes soziales Kontrollsystem auf digitaler Basis schaffen, in dem vorausschauende Algorithmen mögliche Abweichler in Echtzeit ermitteln.

Die chinesische Regierung nutzt grosse, geschichtsträchtige Ereignisse, um den Ausbau der Überwachungsmassnahmen voranzutreiben. Im Vorfeld der Olympischen Spiele 2008 in Peking etwa bauten chinesische Sicherheitsbehörden die Überwachung des Internets in nie dagewesener Masse aus. Während des Coronaausbruchs bedrängte Xis Regierung private Unternehmen, die im Besitz sensibler Personendaten waren. Was auch immer dabei an Geheimvereinbarungen getroffen wurde: Es könnte über die Pandemie hinaus von Dauer sein.

Schon jetzt betreibt China Hunderte Millionen Überwachungskameras. Die Regierung hofft, wichtige Punkte im öffentlichen Raum bald vollständig im Blick zu haben. Algorithmen durchsuchen die Bilder nach Bedrohungen aller Art. Schon bald könnte jede Person im öffentlichen Raum augenblicklich identifiziert werden. KI würde ihr Bild mit einem Ozean persönlicher Daten abgleichen, etwa ihrer gesamten schriftlichen Kommunikation oder der unverwechselbaren Proteinstruktur ihres Körpers. Früher oder später werden Algorithmen in der Lage sein, Daten aus unterschiedlichsten Quellen zu integrieren – Bewegungsdaten, Freunde und Geschäftspartner, Lesegewohnheiten, Einkaufsverhalten –, um politischen Widerstand vorauszusagen, bevor er sich überhaupt manifestiert. Die chinesische Regierung könnte bald ein nie dagewesenes Mass an strengster politischer Kontrolle über 1 Milliarde Menschen ausüben.

In der Frühphase des Coronaausbruchs wurden die chinesischen Bürger einer Art Risikobewertung unterworfen. Ein Algorithmus wies den Menschen einen Farbcode zu – Grün, Gelb oder Rot –, von dem abhing, wie frei sie öffentliche Verkehrsmittel benutzen oder Gebäude in Chinas Megastädten betreten durften. In einem fortgeschrittenen digitalen Sozialkontrollsystem könnten solche Codes eingesetzt werden, um die Menschen nach ihrer politischen Fügsamkeit einzuteilen.

Die schlichte Version eines solchen Systems läuft bereits in Xinjiang, einer Region im Nordwesten Chinas. Hier sind mehr als 1 Million muslimische Uiguren inhaftiert – es ist die umfangreichste Internierung einer ethnisch-religiösen Minderheit seit dem Fall des Dritten Reiches. Sobald Xi dieses System in Xinjiang perfektioniert haben wird, gibt es keine technischen Beschränkungen mehr, die ihn davon abhalten könnten, die Überwachung per KI auf ganz China auszuweiten. Auch könnte er das System in andere Länder exportieren und damit einer ganzen Generation von Autokraten helfen, ihre Macht zu festigen.

Amerikanische Politiker aller Lager zeigen sich ob dieses Szenarios besorgt. Michael Kratsios, ein ehemaliger Gefolgsmann Peter Thiels, der später von Donald Trump zum Chief Technology Officer der US-Regierung gemacht wurde, erwähnte mir gegenüber, dass eine Technologieführerschaft demokratischer Staaten «noch nie so zukunftsentscheidend» gewesen sei – dass wir, «um sicherzustellen, dass die Technologien von morgen auf westlichen Werten aufbauen, hinsichtlich dieser Technologien führend sein müssen».

Trotz der beachtlichen Fortschritte Chinas gehen Experten davon aus, dass die USA ihren Vorsprung im Bereich KI noch 10 Jahre werden verteidigen können. Das ist aber ein schwacher Trost: Schon jetzt entwickelt China mächtige neue Überwachungstechnologien und exportiert diese in Dutzende bestehende oder potentielle Autokratien. In den nächsten Jahren werden diese Technologien verfeinert und in allumfassende Überwachungssysteme integriert werden; Diktatoren müssen sie dann nur noch anknipsen.

Das Aufkommen eines KI-gestützten autoritären Blocks unter chinesischer Führung könnte die Geopolitik unseres Jahrhunderts prägen. Er könnte Milliarden Menschen aus weiten Gebieten der Erde daran hindern, auch nur das kleinste bisschen politische Freiheit zu erlangen. Und entgegen allen Behauptungen amerikanischer Politiker sind nur Chinas Bürger in der Lage, diese Entwicklung aufzuhalten. Ich war nach Peking gekommen, um nach Anzeichen für ein solches Aufbegehren zu suchen.

Versuchslabor Xinjiang

Die Vorgeschichte des gegenwärtigen technopolitischen Augenblicks reicht weit zurück. China stand – mit Ausnahme einiger weniger Jahrhunderte – über die ganzen 5000 Jahre seiner Geschichte an der vordersten Front der Informationstechnologie. Neben Mesopotamien und Mittelamerika war China einer der drei Orte auf der Welt, wo unabhängig voneinander Schriftsysteme erfunden wurden. Im zweiten nachchristlichen Jahrhundert erfanden die Chinesen das Papier; dieses kostengünstige Speichermedium ermöglichte es, dass Informationen – etwa Handelsaufzeichnungen der Seidenstrasse, Heeresberichte oder höfische Korrespondenz – das Reich durchqueren konnten. Transportiert wurden sie von Pferden, die von Nomaden jenseits der Grossen Mauer auf grösstmögliche Schnelligkeit gezüchtet worden waren. Noch rasanter verbreiteten sich Informationen ein paar Jahrhunderte später, als Kunsthandwerker der Tang-Dynastie den Holztafeldruck perfektionierten. Der wurde zum Massenmedium und half, ein riesiges – und noch weiter anwachsendes – Staatswesen zu verwalten.

Als Herrscher über einige der weltweit grössten komplexen Gemeinwesen wussten die alten chinesischen Kaiser um den Zusammenhang zwischen Information und Macht sowie um den Nutzen von Überwachung. Während des 11. Jahrhunderts dämmerte es einem Kaiser der Song-Dynastie, dass Chinas elegante, von Mauern umgebene Städte zu zahlreich geworden waren, als dass sie noch von Peking aus beaufsichtigt werden konnten. Daher beauftragte er Einheimische damit, sie zu kontrollieren. Wenige Jahrzehnte vor Beginn des digitalen Zeitalters machte Chiang Kai-shek von dieser Tradition der Selbstkontrolle Gebrauch, indem er Bürger aufforderte, Dissidenten zu melden, damit kommunistische Aufstände im Keim erstickt werden konnten. Als Mao die Macht übernahm, teilte er Städte in Raster ein. In jedem Quadranten sollten ortsansässige Spione ihre «scharfen



In einem Showroom in Peking: Abbildung eines Bildschirms, auf dem die Gesichtserkennungssoftware von Megvii, einem der führenden chinesischen Technologieunternehmen, demonstriert wird. Bild: Gilles Sabrié.

Augen» nach konterrevolutionären Aktivitäten offenhalten – und seien sie noch so geringfügig. Während des ersten Coronaausbruchs warben chinesische Social-Media-Apps für Hotlines, über die man Mitbürger melden konnte, von denen man den Verdacht hatte, dass sie Symptome der Pandemie verheimlichten.

Die Rede von den «scharfen Augen» mit all ihren geschichtlichen Anklängen hat Xi sich angeeignet, um damit die KI-gestützten Kameras zu bezeichnen, die bald ganz China erfassen werden. Mithilfe von KI kann Xi den effektivsten autoritären Apparat der Menschheitsgeschichte aufbauen – ganz ohne Personal, wie Mao es noch benötigte, um Informationen über Abweichler zu einem zentralen Knotenpunkt zu befördern. In Chinas prominentesten Start-ups – SenseTime, CloudWalk, Megvii, Hikvision, iFlytek oder Meiya Pico – hat Xi kooperationswillige Partner gefunden. Und in der muslimischen Minderheit von Xinjiang eine Testbevölkerung.

Die Kommunistische Partei Chinas misstraut den Religionen schon lange – nicht erst seit dem marxistischen Einfluss. Im Einparteiensystem des heutigen Chinas ist eine Religion eine alternative Quelle höchster Autorität und muss daher entweder für die eigenen Zwecke eingespannt oder zerstört werden.

2009 hatten die chinesischen Uiguren nach Jahrzehnten von Diskriminierung und Landenteignungen genug: Es kam zu Massenprotesten und sogar einigen Selbstmordanschlägen gegen die chinesische Polizei. 2014 liess Xi die Proteste niederschlagen und wies die Provinzregierung von Xinjiang an, Moscheen zu zerstören und von Uiguren bevölkerte Wohngebiete dem Erdboden gleichzumachen. Mehr als 1 Million Uiguren verschwanden in Konzentrationslagern. Viele wurden gefoltert und zu Sklavenarbeit gezwungen.

Diejenigen Uiguren, denen das Lager erspart geblieben war, sind heute die am strengsten überwachte Bevölkerungsgruppe der Welt. Die Überwachung ist nicht ausschliesslich digital: Die Regierung hat Tausende Han-Chinesen – «Big Brothers» und «Big Sisters» – in den alten Seidenstrassenstädten Xinjiangs angesiedelt. Sie sollen die Zwangsassimilierung der Uiguren beaufsichtigen. Sie wohnen bei ihnen, essen mit ihnen, und so mancher «Big Brother» schläft im selben Bett wie die Ehefrau eines verschleppten Uiguren.

KI-gestützte Sensoren lauern überall, sogar in uigurischen Geldbeuteln und Hosentaschen. Laut dem Anthropologen Darren Byler vergruben auf dem Höhepunkt von Xis Feldzug der kulturel-

len Auslöschung einige Uiguren ihre Handys, auf denen sich islamische Inhalte befanden. Andere versteckten ihre Speicherkarten in tiefgefrorenen Teigtaschen. Doch inzwischen mussten sie auf polizeiliche Anordnung Kontrollsoftware auf ihren Handys installieren. Diese Apps nutzen Algorithmen, um rund um die Uhr nach «ideologischen Viren» zu suchen. Sie durchforsten Chatnachrichten nach Koranversen und spüren arabische Schriftzeichen in Memes und anderen Bilddateien auf.

Die üblichen Umgehungstricks kommen für Uiguren nicht infrage. Der Versuch, ein VPN zu installieren, würde Ermittlungen zur Folge haben. Uiguren können keine WhatsApp oder andere verbotene Chatprogramme mit Verschlüsselungsfunktion herunterladen. Auch Gebetsteppiche online zu bestellen, digitale Kopien muslimischer Bücher abzuspeichern oder die Predigten des Lieblingsimams herunterzuladen sind gefährliche Unterfangen. Würde ein Uigur die Bezahlungsfunktion von WeChat nutzen, um Geld an eine Moschee zu spenden, könnten die Behörden aufmerksam werden.

Die «Nanny Apps» arbeiten im Tandem mit der Polizei zusammen: An Kontrollpunkten nehmen Polizisten Stichproben vor, scrollen durch Anruflisten und Textnachrichten. Selbst harmlose digitale Verbindungen – etwa in derselben Chatgruppe zu sein wie jemand, der kürzlich eine Moschee besucht hat – können zu Verhaftungen führen. Völlige Social-Media-Enthaltung ist aber auch keine Lösung, sondern vielmehr ein weiterer Verdachtsgrund. Polizisten sind gehalten, jegliche Abweichung von bisherigen Verhaltensmustern zu melden. Ihre Datenbank will informiert werden, sobald Uiguren anfangen, ihr Haus durch die Hintertür statt durch die Vordertür zu verlassen. Sie will informiert werden, sobald Uiguren weniger Zeit als üblich damit verbringen, mit ihren Nachbarn zu reden. Ein Algorithmus überwacht den häuslichen Stromverbrauch, um unregistrierte Personen in den Haushalten aufzuspüren.

Ein Uigur kommt nur ein paar Strassenblöcke weit, bevor er auf einen Kontrollpunkt stösst, der mit einer der Hunderttausenden Überwachungskameras in Xinjiang ausgerüstet ist. Die Aufzeichnungen der Kamera werden von Algorithmen untersucht, die Aufnahmen von Gesichtern mit Fotos abgleichen, die Polizisten zuvor unter dem Deckmantel von Gesundheitschecks gemacht haben. Bei solchen Checks sammeln Polizisten so viele Körperdaten wie nur eben möglich, messen die Körpergrösse und nehmen Blutproben. Sie fertigen Stimmaufnahmen an und entnehmen DNA-Proben. Manche Uiguren wurden sogar zur Teilnahme an Experimenten gezwungen, bei denen ihre Erbinformation daraufhin untersucht wurde, wie sie die für Uiguren typischen Kinne und Ohren hervorbringt. Wahrscheinlich werden die Polizeibehörden sich die Pandemie zum Vorwand nehmen, noch mehr Körperdaten zu sammeln.

Uigurinnen müssen zudem Schwangerschaftstests über sich ergehen lassen. Einige werden zu Abtreibungen gezwungen oder bekommen Intrauterinpressare eingesetzt. Andere werden vom Staat sterilisiert. Es sind Fälle bekannt, wo Polizisten nicht geneh-

migte Kinder ihren Eltern weggenommen und diese anschliessend verhaftet haben. Solche Massnahmen haben die Geburtenrate in manchen Gegenden Xinjiangs innerhalb von 3 Jahren um mehr als 60 Prozent gesenkt.

Sobald ein Uigur sich der Grenze seines Wohnviertels nähert, wird das automatisch registriert. Dasselbe System folgt ihm auf seinem weiteren Weg durch kleinere Kontrollpunkte wie Banken, Parks oder Schulen. Wenn er sein Auto betankt, weiss das System, ob das Fahrzeug ihm gehört. An der Stadtgrenze muss er aussteigen, damit sein Gesicht und sein Ausweis nochmals gescannt werden können.

Uiguren, die das Glück haben, ins Ausland reisen zu dürfen – vielen Uiguren wurde der Reisepass weggenommen –, wird nahegelegt, rasch wieder zurückzukommen. Wo sie das nicht tun, steht bei ihren Freunden und Verwandten bald die Polizei vor der Tür. Dabei bieten Auslandsreisen oft gar nicht die erhofften Fluchtmöglichkeiten: Xis Diktatorenfreunde – selbst solche in mehrheitlich muslimischen Ländern wie Ägypten – sind gerne bereit, flüchtige Uiguren festzunehmen und in das Freiluftgefängnis Xinjiang zu deportieren.

Smart-City-Alpträume

Anscheinend nutzt Xi Xinjiang als Versuchsstätte zur Feinabstimmung der sensorischen und analytischen Fähigkeiten seines neuen digitalen Panoptikums, um dieses anschliessend über das restliche Land auszurollen. Das Staatsunternehmen CETC, das zum grossen Teil für den Bau des Überwachungssystems von Xinjiang verantwortlich war, präsentiert schon stolz Pilotprojekte in Zhejiang, Guangdong und Shenzhen. Diese Vorhaben sollen ein «belastbares Fundament für einen landesweiten Ausbau» legen, wie die Firma ankündigt. Dabei stellen sie nur ein einzelnes Element in Chinas geplantem Megaüberwachungsnetzwerk dar.

China ist der ideale Ort für einen Feldversuch zu totaler Überwachung. Die Bevölkerung ist höchst digitalaffin und online. Mehr als 1 Milliarde Mobiltelefone sind im Umlauf, jedes einzelne ist ausgerüstet mit hochentwickelten Sensoren. Die Handys zeichnen Internetsuchen auf, Webseitenaufrufe und mobile Bezahlvorgänge, die in China allgegenwärtig sind. Als ich im hippen Pekingerviertel Sanlitun meinen Kaffee mit einer chipbasierten Kreditkarte bezahlt, wurde ich angestarrt, als hätte ich einen Scheck ausgestellt.

All diese Daten können mit Zeitstempel und Geodaten versehen werden. Und seit ein neues Gesetz Telekomanbieter verpflichtet, die Gesichter ihrer Neukunden zu scannen, können Handydaten mit dem Gesicht einer Person verknüpft werden. Das Unternehmen SenseTime, das am Bau des Überwachungsstaats von Xinjiang beteiligt war, prahlte jüngst damit, dass seine Software sogar Personen mit Mund-Nase-Maske identifizieren könne. Eine andere Firma, Hanwang, behauptet, ihre Software könne Maskenträger in 95 von 100 Fällen identifizieren. Man findet auch Wege, an die Daten von Bürgern ohne Handy zu kommen: Auf

«Xis Diktatorenfreunde – selbst solche in muslimischen Ländern wie Ägypten – sind gerne bereit, flüchtige Uiguren festzunehmen und in das Freiluftgefängnis Xinjiang zu deportieren.»

Ross Andersen

dem Land stehen Dorfbewohner Schlange, um ihr Gesicht aus verschiedenen Winkeln scannen zu lassen – im Austausch für Kochgeschirr.

Bis vor kurzem wusste niemand so recht, wie China all diese Daten in ein einziges Überwachungssystem integrieren wollte. Das ist inzwischen klar. 2018 hackte sich ein Cybersicherheitsaktivist in ein Gesichtserkennungssystem ein, das mit der Regierung verbunden zu sein schien und das eine überraschende Kombination von Datenströmen zusammenführte. Das System konnte Uiguren an ihren Gesichtszügen erkennen, konnte erkennen, ob Augen und Münder geöffnet waren, ob jemand lächelte, einen Bart hatte oder eine Sonnenbrille trug. Von in der Nähe befindlichen Handys hielt das System Datum, Uhrzeit und Seriennummer fest – Daten, die auf einzelne Nutzer zurückgeführt werden können. Das System wurde von Alibaba gehostet und nahm auf die KI-gestützte Softwareplattform City Brain Bezug, die Alibaba im Auftrag der chinesischen Regierung baut.

Wie der Name schon andeutet, ist City Brain eine Art automatisiertes Nervenzentrum, das Datenströme aus einer Vielzahl im städtischen Raum verteilter Sensoren zusammenführen kann. Viele Funktionen sind nützlicher, technokratischer Art. Die Algorithmen von City Brain können etwa Passanten oder Autos zählen und Ampelschaltungen oder den U-Bahn-Verkehr koordinieren. Daten von sensorbestückten Abfalleimern können die Müllabfuhr optimieren.

Doch ebenso werden City Brain und seine Nachfolgetechnologien neue Formen integrierter Überwachung ermöglichen. Ei-

nige davon werden breite öffentliche Unterstützung genießen: City Brain könnte lernen, verlorengegangene Kinder ausfindig zu machen, oder auch Gepäck, das von Touristen oder Terroristen stehen gelassen wurde. Es könnte Herumlungerer, Obdachlose oder Krawallmacher markieren. Wer sich in Gefahr befände, könnte durch Handzeichen Hilfe herbeirufen, das stets wachsame Computerauge würde die Zeichen sofort erkennen. Polizisten mit Knopf im Ohr könnten von einem KI-Sprachassistenten zum Tatort geführt werden.

Besonders nützlich wäre City Brain während einer Pandemie: Ein Schwesterunternehmen von Alibaba hat eine App programmiert, die Nutzern per Farbcode die Wahrscheinlichkeit verrät, mit der sie sich angesteckt haben könnten. Im Hintergrund werden dabei Gesundheits- und Bewegungsdaten heimlich an die Polizei weitergeleitet. Als das Virus sich in Peking auszubreiten begann, fingen einige Läden und Restaurants an, die Handys potentieller Kunden zu scannen, indem sie Daten von den Mobilfunkbetreibern abriefen. Ziel war, herauszufinden, ob jemand kürzlich von einer Reise zurückgekommen war. Auch schickten Mobilfunkbetreiber Listen mit Besuchern aus Wuhan – dem Ort, wo das Virus erstmals nachgewiesen worden war – an die jeweiligen Lokalregierungen. Chinesische KI-Firmen stellen vernetzte Polizeihelme mit eingebauter Gesichtserkennungssoftware und Infrarotfiebersensoren her, die Daten an die Regierung übermitteln können. City Brain könnte diese Prozesse automatisieren und seine Datenströme integrieren.

Selbst die komplexesten chinesischen KI-Systeme sind immer noch lückenhaft. Noch hat City Brain nicht die ganze Bandbreite seiner Überwachungskapazitäten integriert, und Vorgängersysteme litten an etlichen peinlichen Leistungsproblemen: 2018 hielt eine KI-gestützte Kamera ein auf einen Bus gedrucktes Gesicht für einen unachtsamen Fussgänger. Doch die Software wird besser und besser, und es gibt keinen technischen Grund, warum sie nicht in massenhaftem Umfang eingesetzt werden könnte.

Datenströme könnten in beliebiger Grössenordnung in Systeme wie City Brain eingespeist werden. City Brain könnte Daten von an Laternenmasten oder Häuserecken angebrachten Kameras mit Aufnahmen der 1,9 Millionen Gesichtserkennungskameras kombinieren, die von der chinesischen Telekomfirma China Tower in Zusammenarbeit mit SenseTime angebracht werden. Es könnte die Kameras nutzen, die die chinesische Polizei in Verkehrshütchen versteckt, oder Bodycams der Polizei – egal ob uniformiert oder zivil. Der Staat könnte Läden zwingen, die Daten ihrer privaten Überwachungskameras zur Verfügung zu stellen, die inzwischen so weit entwickelt sind, dass sie erkennen, wohin im Regal ein Kunde schaut, und die bald schon um Ecken sehen können, indem sie Schatten analysieren. Kaum ein Fleckchen öffentlichen Raumes bliebe unüberwacht.

Die chinesische Regierung könnte Kameras in Taxis oder Mitfahrautos anzapfen – oder in selbstfahrenden Autos, die womöglich bald an deren Stelle treten werden: Automatisierte Fahrzeuge



Einheimische spielen in einem kleinen Dorf in Zhejiang Karten in einem Haus, an dem die Sozialkreditpunkte des Haushalts an der Wand angezeigt werden. Das seit 2018 in diesem Dorf implementierte Sozialkreditsystem basiert auf 5 Kriterien: Sauberkeit und Gepflegtheit des Hofes, Einhaltung von Gesetzen und Vorschriften, Bankkredit, Recycling und Familienwerte. Bild: Gilles Sabrié.

werden mit einer Unmenge Sensoren ausgestattet sein, von denen einige weit reichhaltigere Informationen ausgeben als 2-D-Video-kameras. Alle Daten einer riesigen Flotte solcher Fahrzeuge könnten zusammengeführt und mit anderen City-Brain-Datenströmen kombiniert werden, um ein sekundlich aktualisiertes 3-D-Modell der Stadt zu gewinnen. Ein solches System würde vor allem unbekannte Gesichter zu identifizieren suchen, etwa durch Aussendung von Drohnen.

Das Modell könnte mit Audiodaten von allerlei vernetzten und mit Mikrophon ausgestatteten Geräten synchronisiert werden: Smart Speaker, Smart Watches sowie weniger offensichtliche Geräte des Internets der Dinge wie digitalisierte Matratzen, Windeln oder Sexspielzeuge. All diese Quellen könnten zu einem vielspurigen, ortsspezifischen Audiomix verbunden und mithilfe polyglotter Algorithmen analysiert werden. Diese Kombination wäre nützlich für Sicherheitsdienste – besonders da, wo keine Kameras installiert sind: Die chinesische Firma iFlytek tüftelt an einem System, das Menschen an ihrem «Stimmabdruck» erkennt.

In wenigen Jahrzehnten können City Brain oder seine Nachfolger womöglich sogar unausgesprochene Gedanken lesen. Schon

jetzt lassen sich Drohnen mithilfe von Helmen steuern, indem sie neuronale Signale aufnehmen und übertragen. Auch entwerfen Forscher bereits Hirn-Computer-Schnittstellen, die es Nutzern erlauben, mit ihren Gedanken eine Tastatur zu bedienen. Eine Autokratie im Besitz der entsprechenden Rechenpower könnte die Hersteller einer solchen Software zwingen, jede neuronale Regung ihrer Bürger in eine regierungseigene Datenbank einzuspeisen. China drängt seine Bürger seit einiger Zeit dazu, eine Propaganda-App herunterzuladen und zu nutzen. Regierungen könnten Gefühls-Tracking-Software einsetzen, um die Reaktionen der Nutzer auf politische Inhalte einer solchen App zu überwachen. Eine schweigende, unterdrückte Reaktion auf ein Meme oder einen Ausschnitt aus einer Rede Xis wäre ein bedeutsamer Datenpunkt, den ein Vorhersagealgorithmus nutzen könnte.

Die synchronisierten Datenströme könnten weiter mit Luftaufnahmen angereichert werden, geliefert von Drohnen mit Giga-pixelkameras, die ganze Stadtlandschaften in solcher Detailgenauigkeit abbilden, dass Algorithmen Nummernschilder lesen und Menschen an ihrem Gang erkennen können. Vogelähnliche Drohnen («Spy Birds») bevölkern bereits heute den Himmel über

chinesischen Städten. Die City-Brain-Datenströme könnten mit Daten aus anderen städtischen Bereichen kombiniert werden, um fast alle menschlichen Aktivitäten innerhalb Chinas multidimensional und in Echtzeit abzubilden. Serverfarmen überall in China werden bald in der Lage sein, jeden Augenblick im Leben jedes einzelnen Bürgers aus mehreren Perspektiven in HD zu verarbeiten und abzuspeichern.

Es muss betont werden, dass Systeme solchen Umfangs erst in der Entwicklungsphase stehen. Die meisten Personendaten Chinas sind bislang noch nicht integriert, selbst innerhalb einzelner Firmen nicht. Auch verfügt die chinesische Regierung noch nicht über ein zentrales Datendepot – was zum Teil auf Konkurrenz zwischen den einzelnen Behörden zurückzuführen ist. Doch gibt es keine harten politischen Beschränkungen, die der Integration all dieser Daten im Wege stünden. Im Gegenteil – chinesische Privatunternehmen sind per Gesetz verpflichtet, mit den Geheimdiensten zusammenzuarbeiten.

Chinas Regierung könnte bald über detaillierte, sich selbst aktualisierende Datenprofile für jeden einzelnen seiner mehr als 1 Milliarde Bürger verfügen. Jedes dieser Profile würde Millionen Datenpunkte kombinieren – etwa über jede einzelne Anwesenheit des Bürgers an einem überwachten Ort sowie sämtliche Kommunikationsdaten und Bezahlvorgänge. Die Bedrohung, die von einem Bürger für die Herrschaft der Partei ausgeht, könnte permanent in Echtzeit kalkuliert werden. Die Bewertung wäre noch feinkörniger als die des bisherigen Sozialkreditsystems, das heute schon versucht, die gesellschaftliche Reputation einzelner Bürger anhand von Kontakten auf Social Media oder von Kaufverhalten zu bewerten. Algorithmen könnten diesen Wert ununterbrochen im Blick haben – ohne jegliche Ermüdungserscheinungen, wie sie wohl mancher Stasi-Offizier auf Nachtschicht empfunden haben mag.

Sobald die Risikobewertung eines Bürgers in den gelben Bereich kommt – ob aufgrund verdächtiger Bewegungsdaten, bestimmter Bekanntschaften, mangelnder Begeisterung für die Propaganda-App oder aufgrund irgendeiner Korrelation, deren Sinn nur dem Algorithmus zugänglich ist –, könnte seine Mobilität automatisch eingeschränkt werden. Er könnte daran gehindert werden, Flug- oder Zugtickets zu kaufen. Ihm könnte der Durchgang durch bestimmte Kontrollpunkte verwehrt werden. Oder das System könnte «Smart Locks» in öffentlichen oder privaten Räumen aktivieren, so dass die Person bis zum Eintreffen der Polizei festgehalten würde.

Alle Macht der Partei

In jüngerer Zeit haben sich in China einige Stimmen aus intellektuellen Kreisen erhoben und vor den Gefahren eines Missbrauchs von KI gewarnt – allen voran der Computerwissenschaftler Yi Zeng und der Philosoph Zhao Tingyang. Im Frühling 2019 veröffentlichte Yi «The Beijing AI Principles», ein Manifest, in dem er untersucht, wie KI mit Grundwerten wie Selbstbestimmung, Menschenwürde oder dem Recht auf Privatsphäre in Konflikt geraten könnte.

«Man findet auch Wege, an die Daten von Bürgern ohne Handy zu kommen: Auf dem Land stehen Dorfbewohner Schlange, um ihr Gesicht aus verschiedenen Winkeln scannen zu lassen – im Austausch für Kochgeschirr.»

Ross Andersen

Yi war es, den ich im Peking Institut für Automatisierung besuchte. Neben seinen Studien zum Thema KI-Ethik ist er hier als stellvertretender Leiter des Research Center for Brain-Inspired Intelligence tätig. Er holte mich in der Lobby ab. Für sein tatsächliches Alter von 37 Jahren sah Yi recht jung aus – mit freundlichen Augen und kräftig gebaut, aber schlanker wirkend in schwarzen Jogginghosen und Kapuzenpullover.

Auf dem Weg in Yis Büro kamen wir an einem seiner Labore vorbei, wo ein Assistent über ein Mikroskop gebeugt sass und elektrochemische Signale in Mäusehirngewebe beobachtete, die von Neuron zu Neuron blitzten. Wir liessen uns an einem langen Tisch in einem Konferenzraum neben seinem Büro nieder. Während ein Assistent Tee servierte, betrachteten wir die graue, neblige Stadtlandschaft.

Freimütig sprach Yi nun über das Missbrauchspotenzial von KI. Dabei erwähnte er ein Projekt, das an ausgewählten Schulen verwirklicht worden war. Im Rahmen dieses Projektes wurde nicht nur die Anwesenheit der Schüler verfolgt, sondern auch, wie aufmerksam einzelne Schüler im Unterricht waren. «Ich hasse diese Software», sagte Yi. «Ich kann es nicht anders sagen.»

Chinesische Start-ups haben da weit weniger Skrupel. Einige helfen Xi explizit dabei, KI für Überwachungszwecke zu entwickeln. Chinas Einparteienherrschaft in Kombination mit den ideologischen Resten der Planwirtschaft sichert die Macht der Parteielite in allen Bereichen. Doch während früher die Verbindungen zwischen Tech-Branche und Regierung diskreter Natur

waren, entsendet die Regierung seit einiger Zeit offizielle Vertreter in Tech-Unternehmen, die dort den Einfluss der Kommunistischen Partei stärken sollen.

Dem Staat Sicherheitsdienstleistungen zu verkaufen ist einer der schnellsten Wege, um als KI-Start-up in China Profit zu machen. Ein staatliches Telekomunternehmen ist der grösste Anteilseigner von iFlytek, dem chinesischen Spracherkennungsriesen. Die Synergien sind zahlreich: Wo die Polizei iFlytek-Software benutzt, um Anrufe abzuhören, berichten staatseigene Zeitungen darüber wohlwollend. Anfang dieses Jahres ging die Nachrichten-App Toutiao sogar so weit, die Unternehmensmission auf ein neues Ziel hin umzuschreiben: die öffentliche Meinung mit den Wünschen der Regierung in Einklang zu bringen. Xu Li, der CEO von SenseTime, nannte jüngst die Regierung als «bedeutendste Datenquelle» des Unternehmens.

Ob es in China überhaupt noch private, vor staatlichem Zugriff geschützte Daten geben wird, lässt sich angesichts der politischen Struktur des Landes nicht vorhersagen. Doch dank der digitalen Revolution sind Datenmonopole kaum vermeidbar: Selbst in den USA mit ihrer starken Tradition in puncto Kartellrechtsdurchsetzung haben die Bürger noch nicht den Willen aufgebracht, den wenigen Herrschenden die Kontrolle über die Daten abzurufen. Doch während private Datenmonopole immerhin der Hoheitsgewalt der Länder unterliegen, in denen sie Geschäfte betreiben, können nationalstaatliche Datenmonopole nur durch das Volk verhindert werden – und auch das nur, wenn dieses über genügend politische Macht verfügt.

Das chinesische Volk hat keine Möglichkeit, sich Xi Jinpings mithilfe von Wahlen zu entledigen. Und ohne eine unabhängige Justiz kann die Regierung nahezu nach Belieben das Recht beanspruchen, alle Datenströme auf mögliche Bedrohungen der «Stabilität» zu überwachen. Auch kann sie Unternehmen hinter verschlossenen Türen zur Herausgabe von Daten zwingen, wie es zu Beginn des Coronaausbruchs geschah. Eine unabhängige Presse, an die sich die Information über solche Forderungen durchstecken liesse, existiert nicht.

Globale Expansion

Yi und ich besprachen ein globales Szenario, über das sich KI-Ethiker und China-Experten zu sorgen begonnen haben. In diesem Szenario erkennt die Mehrheit der weltweiten KI-Forscher die Risiken der Technologie und entwickelt starke Normen rund um ihren Gebrauch. Doch ein einziges Land schert aus. Es bekennt sich zwar nach aussen zu jenen Normen, doch nur zum Schein; im Hintergrund entwickelt dieses Land schlüsselfertige Überwachungssysteme und verkauft sie an Länder, in denen die Demokratie entweder fragil oder inexistent ist. Autokraten werden meist durch Staatsstreiche oder Massenproteste zu Fall gebracht. Beides erfordert aber ein Mindestmass an politischer Organisation, wie sie sich in automatisch und vollständig überwachten Staaten als unmöglich erweisen könnte.

Yi zeigte sich ob dieses Szenarios besorgt, bezog es aber nicht explizit auf China. Das musste er auch nicht: Das Land ist inzwischen der grösste Exporteur KI-gestützter Überwachungssysteme. Die malaysische Regierung zum Beispiel kooperiert mit Yitu, einem chinesischen KI-Start-up, mit dem Ziel, die Polizei von Kuala Lumpur mit Gesichtserkennungstechnologie auszurüsten – als Pendant zu Alibabas City-Brain-Plattform. Chinesische Firmen bewerben sich zudem darum, jeden einzelnen der 110 000 Laternepfähle in Singapur mit Gesichtserkennungskameras auszustatten zu dürfen.

In Südasien hat die chinesische Regierung Überwachungssysteme an Sri Lanka geliefert. Entlang der alten Seidenstrasse hat die chinesische Firma Dahua die Strassen von Ulan-Bator, der Hauptstadt der Mongolei, mit KI-gestützten Überwachungskameras versehen. Weiter westlich, in Serbien, hilft Huawei beim Aufbau eines «Safe-City-Systems». Das Netzwerk kombiniert Gesichtserkennungskameras mit von serbischen und chinesischen Polizisten gemeinsam durchgeführten Patrouillen, deren Zweck es ist, dass sich chinesische Touristen sicher fühlen.

In den frühen Nullerjahren verkaufte der chinesische Telekomgigant ZTE der äthiopischen Regierung ein drahtloses Netzwerk mit eingebautem Backdoor-Zugriff. Bei einer späteren Razzia wurden Dissidenten zusammengetrieben und brutalen Verhören unterzogen. Dabei konfrontierte man sie mit Tonaufnahmen von Telefongesprächen, die sie zuletzt geführt hatten. Heute rüsten auch Kenia, Uganda und Mauritius grössere Städte mit Überwachungssystemen chinesischer Herkunft aus.

In Ägypten wollen chinesische Investoren den Bau einer neuen Hauptstadt finanzieren. Die Stadt soll mithilfe einer Smart-City-Plattform à la City Brain überwacht werden. Noch wurde aber nicht entschieden, wer den Auftrag dafür erhalten soll. Im südlichen Afrika hat Sambia eingewilligt, mehr als 1 Milliarde Dollar für Telekommunikationssysteme aus China auszugeben – darunter auch Technologie zur Überwachung des Internets. Die chinesische Firma Hikvision, der weltgrösste Hersteller KI-gestützter Überwachungskameras, unterhält ein Büro in Johannesburg.

China nutzt die Taktik «aggressiver Kreditverkäufe, um Telekommunikationstechnik zu erheblichen Preisnachlässen an Entwicklungsländer zu verkaufen, wodurch sich China in die Lage versetzt, diese Netzwerke und ihre Daten zu kontrollieren», erklärte Michael Kratsios, Chief Technology Officer der US-Regierung. Wo Länder die Kredite refinanzieren müssen, kann China als Bedingung Zugang zu den Netzwerken fordern. Ähnlich sichert sich Chinas Militär in von ihm finanzierten ausländischen Häfen das Recht, Militärstützpunkte einzurichten. «[China] unbeschränkten Zugang zu Datennetzwerken rund um die Welt zu geben, ist höchst problematisch», sagte Kratsios.

2018 unterschrieb CloudWalk Technology, ein in Guangzhou ansässiges Start-up, das aus der Chinesischen Akademie der Wissenschaften ausgegliedert worden war, einen Vertrag mit der Regierung von Simbabwe, in dessen Rahmen es ein Überwa-

«In Chinas prominentesten Start-ups hat Xi kooperationswillige Partner gefunden. Und in der muslimischen Minderheit von Xinjiang eine Testbevölkerung.»

Ross Andersen

chungsnetzwerk bauen sollte. Laut Vertrag sollte die Hauptstadt Harare Fotos ihrer Einwohner – ein reicher Datenschatz, wenn man bedenkt, dass Simbabwe Migranten aus dem gesamten subsaharischen Afrika beherbergt – an die CloudWalk-Büros in China schicken. Das Unternehmen wollte im Gegenzug mit den Fotos die Fähigkeit seiner Software perfektionieren, auch dunkelhäutige Gesichter zu erkennen. An dieser Aufgabe waren die Algorithmen bis dahin gescheitert.

Chinesische KI-Unternehmen haben Brückenköpfe in Asien, Europa und Afrika errichtet. Als nächstes nehmen sie Südamerika ins Visier – eine Region, die laut der chinesischen Regierung für das Land von «höchstem wirtschaftlichem Interesse» ist. So kaufte Ecuador mit chinesischem Geld ein Kameraüberwachungssystem für 240 Millionen Dollar. Auch Bolivien erwarb mithilfe chinesischer Kredite Überwachungstechnik. Und Venezuela führte jüngst ein neues Ausweissystem ein, das Informationen über die Parteizugehörigkeit einzelner Bürger in einer von ZTE konstruierten Datenbank speichert. Dass chinesische Firmen viele dieser Überwachungsprodukte über Jahre auf einer Messe der Sicherheitsbranche in Xinjiang verscherbelt hatten, der Heimatprovinz der Uiguren, stellt eine bittere Ironie dar.

Chinas Braindrain-Problem

Falls es China gelingt, die USA in Sachen KI zu überholen, wird das Land zu einer noch einflussreicheren geopolitischen Grösse – besonders als Bannerträger eines neuen autoritären Bündnisses.

Schon heute besitzt China einige der weltweit grössten Datensätze. Mit ihnen kann es seine KI-Systeme füttern und chinesischen Forschern so einen entscheidenden Vorteil verschaffen. In riesigen Megabüros in Städten überall in China sitzen Niedriglohnarbeiter stundenlang an langen Tischen und transkribieren Tonaufnahmen oder umreissen Gegenstände auf Bildern, um den Nutzen der von Chinas riesiger Bevölkerung generierten Daten zu steigern. Doch um das amerikanische KI-Ökosystem zu übertreffen, müssen diese Datenberge von Algorithmen analysiert werden, die Muster weit jenseits menschlicher Verstandeskräfte erkennen. Und selbst Topmanager des chinesischen Suchmaschinenriesen Baidu geben zu, dass die absoluten Spitzentalente im Westen arbeiten.

Schon immer tat sich China schwer damit, Topanalysten zu halten. Die meisten verlassen das Land, um in den USA zu studieren, deren computerwissenschaftliche Fachbereiche weltweit unübertroffen sind. Anschliessend heuern sie bei den interessanteren, finanziell besser ausgestatteten Unternehmen des Silicon Valley an. Doch das könnte sich bald ändern: Die Regierung Trump erschwert es chinesischen Studenten, in den USA zu studieren. Und wer es doch schafft, wird misstrauisch beäugt. Ein hochrangiger Google-Experte für maschinelles Lernen bezeichnete kürzlich Visa-Beschränkungen als «einen der bedeutendsten Engpässe für unsere kollektive Forschungsproduktivität».

Derweil setzen chinesische Informatikfachbereiche alles auf die KI-Karte: Drei der zehn weltweit bedeutendsten KI-Unis – gemessen am Umfang der Veröffentlichungen – befinden sich heute in China. Allerdings beinhaltet diese Zahl noch nicht die 50 neuen KI-Forschungszentren, die Xi im Rahmen seines «KI-Aktionsplans für höhere Bildungseinrichtungen» in Auftrag gegeben hat und die noch nicht fertiggebaut sind. 2017 zogen chinesische Firmen 36 Prozent der weltweiten Private-Equity-Investitionen an, 2015 waren es noch magere 3 Prozent gewesen. Talentierte chinesische Ingenieure haben jetzt die Möglichkeit, sich in der Heimat ausbilden zu lassen und nach dem Abschluss für weltweit attraktive Unternehmen wie TikTok zu arbeiten.

Mittelfristig wird China, was digitale Hardware betrifft, weiter die zweite Geige hinter den USA spielen. Ebenso wie Daten von Algorithmen verarbeitet werden müssen, um ihren Nutzen zu entfalten, sind Algorithmen auf physische Trägermedien angewiesen. Diese Rolle übernehmen Mikrochips. Deren Siliziumstrukturen sind so hauchzart, dass ein paar fehlende Atome dazu führen können, dass die durch den Chip laufenden elektrischen Impulse an den neuronartigen Verästelungen die falsche Abzweigung nehmen. Die Chips der neuesten Generation sind wohl die komplexesten Gegenstände, die je von Menschen gebaut wurden. Zu komplex jedenfalls, um von den legendären chinesischen Industriespionen einfach auseinandergenommen und rekonstruiert zu werden.

Chinesische Unternehmen sind noch nicht in der Lage, Chip-Produktionslabore auf höchstem Niveau zu bauen. Der Bau solcher Räumlichkeiten kostet Milliarden und bedarf über Jahrzehnte angesammelten institutionellen Wissens. Noch immer



Das vom chinesischen Start-up SenseTime entwickelte KI-System ermöglicht in Verbindung mit CCTV-Kameras grundlegende Beschreibungen von Personen und Fahrzeugen. Bild: Gilles Sabrié.

kann die US-Regierung die Lieferung von Hardware nach China beschränken – sehr zum Unmut der Kommunistischen Partei. Als die Regierung Trump im April 2018 den Verkauf von Mikrochips an ZTE verbot, erlebte China – nach Meinung von Frank Long, einem Experten für Chinas KI-Sektor – eine Art jähes Erwachen, demjenigen vergleichbar, das seinerzeit vom arabischen Öl-embargo in den USA ausgelöst wurde.

Doch die KI-Revolution hat China eine seltene Gelegenheit zum Überholen beschert: KI läuft am besten auf Spezialchips, wie sie Google einsetzt, um auf Tausenden Fotos im Nu das Gesicht einer bestimmten Person zu identifizieren. Da aber die Herstellung solcher Spezialchips allgemeines Neuland darstellt, liegt China hier nicht so weit zurück: Baidu und Alibaba bauen Spezialchips für Deep Learning. Und im August 2019 stellte Huawei einen mobilen Machine-Learning-Chip vor. Entwickelt worden war er von Cambricon, dem wahrscheinlich wertvollsten Start-up der weltweiten Chip-Branche, gegründet von Yis Kollegen an der Chinesischen Akademie der Wissenschaften.

Bis 2030 könnte China im Begriff sein, die KI-Vorherrschaft an sich zu reißen. Das Land wird bis dahin wahrscheinlich die grösste Volkswirtschaft der Welt haben – sowie neues Geld, das es

für militärische KI-Anwendungen ausgeben kann. Es wird womöglich die höchstentwickelten Drohenschwärme besitzen – sowie autonome Waffensysteme, die nach nur kurzer Beobachtung eines Kriegsschauplatzes die Handlungen des Gegners vorhersagen und taktische Entscheidungen weit schneller treffen können als der menschliche Verstand. Seine Raketenwarn-Algorithmen könnten den nuklearen Erstschlagvorteil der USA zunichtemachen. Kurz: KI könnte das globale Machtgleichgewicht auf den Kopf stellen.

Chinas Zukunft? Unsere Zukunft!

Auf meinem Weg aus dem Institut zeigte mir Yi noch sein Robotiklabor. In dem hohen Raum bastelten Doktoranden an einem riesigen Metallarm und einem kleinen humanoiden Roboter herum, den ein graues Exoskelett umgab. Yi erzählte mir von seinen Versuchen, ein Modell des Gehirns zu konstruieren. Nach seiner Überzeugung muss, wer das Wesen der Intelligenz ergründen will, zunächst die Struktur des menschlichen Gehirns verstehen.

Ich fragte Yi, wie sich KI wohl entwickeln werde. Er sagte, er könne sich vorstellen, dass eine dem Gehirn nachgebildete Software Schritt für Schritt bestimmte Fähigkeiten erlange. Sie könne



Eine Strassenkreuzung in Xinjiang: Überwachungskameras, die mit Gesichtserkennungstechnologie verbunden sind, zeigen auf einem Bildschirm Fotos von Fussgängern, die Verkehrsregeln missachten, mit Namen und I.D.-Nummer. Damit sollen Übeltäter in Verlegenheit gebracht werden. Bild: Gilles Sabrié.

womöglich so etwas wie Selbsterkenntnis erreichen und sich dann langsam der Vergangenheit und der Zukunft bewusst werden. Sie könne Motive und Werte entwickeln. Die letzte Stufe ihrer unterstützten Evolution wäre darin erreicht, dass sie andere Akteure als empathiewürdig begreift. Ich fragte ihn, wann es so weit sein könnte. «Ich glaube, so eine Maschine könnte bis 2030 gebaut werden», sagte Yi.

Bevor ich mich von Yi verabschiedete, fragte ich ihn nach einem Szenario, in dem sich die Dinge anders entwickeln: «Angenommen, Sie bauen Ihr digitales, hochauflösendes Modell des Gehirns», sagte ich. «Und angenommen, es erlangt eine rudimentäre Form von Bewusstsein. Und angenommen, es gelingt Ihnen, das Modell mit der Zeit zu verbessern, bis es den Menschen in allen kognitiven Aufgabenbereichen mit Ausnahme von Empathie übertrifft. Sie halten es unter Verschluss im Sicherheitsmodus, bis Sie jenes letzte Ziel erreicht haben. Doch dann treten eines Tages Sicherheitskräfte der Regierung Ihre Tür ein. Die Agenten wissen, dass Sie dieses KI-Modell auf Ihrem Computer haben. Sie wollen es als Software für eine neue Hardwareplattform nutzen, für die Erschaffung eines künstlichen, humanoiden Soldaten.

Eine Milliarde dieser Roboter wurde bereits produziert und die Regierung schert sich einen Dreck darum, ob sie empathiefähig sind. Die Agenten verlangen Ihr Passwort. Geben Sie es ihnen?» «Ich würde meinen Computer zerstören und gehen», sagte Yi. «Wirklich?», fragte ich. «Ja, wirklich», sagte er. «Dann wäre es für mich an der Zeit, meinen Job an den Nagel zu hängen und mich auf den Bau künstlerisch kreativer Roboter zu verlegen.»

Wer einen Philosophenkönig damit beauftragen wollte, einen ethischen Entwicklungspfad für KI zu entwerfen, könnte es schlechter treffen als mit Yi. Doch der Entwicklungspfad von KI wird durch sich überschneidende lokale, nationale und globale politische Systeme bestimmt werden, nicht durch einen weisen und wohlwollenden Philosophenkönig. Aus diesem Grund ist der Aufstieg Chinas zur KI-Supermacht ein solch bedrohliches Szenario: Die politische Struktur des Landes würde die schlimmsten Anwendungen dieser Technologie eher begünstigen als beschränken.

Selbst in den USA, einer Demokratie mit verfassungsmässig verbrieften Menschenrechten, verzweifeln die Menschen im Kampf gegen den aufkommenden öffentlich-privaten Überwa-

chungsstaat. Immerhin geben die politischen Strukturen der USA zu einiger Hoffnung Anlass. In China wird KI nur insoweit reguliert, wie es der Partei dient.

Es war fast Mittag, als ich das Institut endlich verliess. Yi bestellte mir ein Auto und begleitete mich dorthin, wo es eintreffen sollte. Dabei hielt er einen Regenschirm über mich. Ich schlug mich durch zur Verbotenen Stadt, dem alten Peking-Kaisersitz. Doch selbst diese kurze Fahrt brachte mich in Berührung mit dem chinesischen Überwachungsstaat: Bevor ich auf den Tiananmen-Platz einbog, wurden mein Pass und mein Gesicht gescannt. Dagegen war ich schon fast unempfindlich geworden.

Auf dem Platz marschierten Polizisten im Gänsemarsch, mannshohe kugelsichere Schilde haltend, durch Ansammlungen von Touristen. Die starke Polizei-Präsenz erinnerte mich an die protestierenden Studenten, die hier 1989 ermordet worden waren. Chinas KI-überwachte «Great Firewall» war unter anderem gebaut worden, um sicherzustellen, dass das Massaker niemals im chinesischen Internet diskutiert würde. Um der Ermordeten dennoch zu gedenken und dabei der Zensur durch Algorithmen zu entgehen, nutzen chinesische Aktivisten Memes – etwa eine Version des ikonischen «Tank-Man»-Fotos, in der statt Panzer vier riesige Badeenten auf einen jungen Mann zurollen, der sich ihnen in den Weg stellt.

Die KI-gestützte Zensur durch die Partei geht weit über Tiananmen hinaus. Zu Beginn dieses Jahres verhaftete die Regierung chinesische Programmierer, die versucht hatten, verschwundene Berichte zur Coronapandemie wiederherzustellen. Einige der Artikel in ihren Datenbanken waren aus dem Verkehr gezogen worden, weil sie Xi und die Partei kritisierten. Sie blieben nur deshalb erhalten, weil Internetnutzer sie auf Social Media weiterverbreitet hatten, verflochten durch Codesprache und Emojis, und so die Algorithmen der Zensur getäuscht wurden. Umgehungstaktiken dieser Art sind kurzlebig: Heimische Kritiker nutzten Bilder der Disney-Figur Winnie Puuh, um sich über Xi lustig zu machen – bis solche Bilder schliesslich ebenfalls verboten wurden. Die Fähigkeit der Partei, Geschichte und Kultur gewaltsam umzuschreiben, wird mit zunehmender Qualität der chinesischen KI umfassender und präziser werden.

Einer Regierung Macht abzuringen, die alle Information so gründlich kontrolliert, ist kein leichtes Unterfangen. Vielleicht braucht es dazu Millionen solcher Akte zivilen Ungehorsams, wie die Zerstörung eines Laptops, die Yi sich vorgestellt hatte. Chinas Bürger werden hinter ihren Studenten stehen müssen. Wer kann schon sagen, welches Leid sie dabei auf sich nehmen müssen?

Die Menschen in China scheinen noch nicht ausreichend empört zu sein. Womöglich führt die Pandemie sogar dazu, dass die Leute ihrer Privatsphäre weniger Wert beimessen – wie es eine Umfrage in den USA nahelegt. Bislang verkaufte Xi die Massnahmen seiner Regierung als triumphalen «Volkskrieg». Damit nutzte er einen weiteren alten Kampfbegriff Maos, der sich auf eine Generalmobilmachung zum Zweck der Vaterlandsverteidigung

bezieht. Es könnte sein, dass das chinesische Volk seit der Pandemie sogar noch fügsamer geworden ist als zuvor.

Es gibt jedoch Hinweise, dass junge Chinesen – zumindest einige von ihnen – der Regierung übelnehmen, wie sie den Ausbruch anfangs geheim zu halten versucht hatte. Nach allem, was wir wissen, könnte es sein, dass eine neue Jugendbewegung im Verborgenen heranreift und nur auf eine Gelegenheit wartet, um für mehr Demokratie aufzustehen. Die Menschen in Hongkong sind sich der Gefahr dieses technopolitischen Augenblicks jedenfalls wohl bewusst. In der Nacht vor meiner Ankunft in China waren dort mehr als 1 Million Demonstranten auf die Strasse gegangen. (Die kostenlose Staatszeitung in meinem Peking-Hotel beschrieb die Protestierer fälschlich als Unterstützer der Polizei.) Viele von ihnen hielten sich Regenschirme über den Kopf – in Solidarität mit protestierenden Studenten aus den Jahren zuvor, aber auch, um ihre Gesichter versteckt zu halten. Einige rissen einen Laternenpfahl nieder, an dem sie eine Gesichtserkennungskamera vermuteten. Seitdem hat Xi in der Region die Zügel angezogen und ein «nationales Sicherheitsgesetz» erlassen. Die Bürger Hongkongs sind nicht zahlreich genug, um etwas dagegen tun zu können. Jedenfalls nicht ohne Unterstützung durch eine Bewegung auf dem chinesischen Festland.

Während meines Besuches auf dem Tiananmen-Platz sah ich keine Demonstranten. Die Menschen liefen friedlich herum und machten Selfies mit dem riesigen Mao-Porträt. Sie hatten Schirme, aber nur, um sich damit gegen die Augustsonne zu schützen. Während ich in ihrer Mitte lief, dachte ich über die Zufälligkeit von Geschichte nach: Die politischen Systeme, die eine Technologie im Frühstadium regulieren, formen unsere gemeinsame globale Zukunft. So viel haben wir aus unseren Abenteuern mit dem Verbrennen von Kohlenstoff gelernt. Die politische Entwicklung unseres Planeten hängt womöglich zum grossen Teil davon ab, welche Gefahr das chinesische Volk in einer KI sieht, die von einer zentralen Macht kontrolliert wird. Und solange es sich nicht individuelle Freiheit erkämpft – wohl zu unvorstellbaren Kosten –, müssen freie Menschen auf der ganzen Welt gegen alle Wahrscheinlichkeit hoffen, dass die intelligentesten Maschinen der Welt woanders hergestellt werden. ◀

Aus dem Englischen übersetzt von Jan Meyer-Veden.

Dieser Artikel, der im September 2020 unter dem Titel «The Panopticon Is Already Here» publiziert wurde, erscheint hier zum ersten Mal in leicht gekürzter Version auf Deutsch. © 2020 The Atlantic Media Co., wie erstmalig in «The Atlantic Magazine» veröffentlicht. Alle Rechte vorbehalten. Zugestellt von «Tribune Content Agency».

Ross Andersen

ist Journalist und stellvertretender Herausgeber der amerikanischen Zeitschrift «The Atlantic».