gehen davon aus, dass mehr als ein Viertel der Erwachsenen im erwerbsfähigen Alter Stasi-Informanten waren. Der Aktenberg der Stasi wird auf 20 Milliarden Seiten[2] geschätzt. Schon bald überstieg es das Vermögen jeder menschlichen Organisation, diese gewaltigen Informationsflüsse auszuwerten und darauf zu reagieren.

Kein Wunder also, dass die Geheimdienste dieser Welt großes Potenzial in der KI sehen. Viele Jahre lang setzte man dort auf einfache Spielarten der künstlichen Intelligenz, darunter Spracherkennung und die Suche nach Schlüsselbegriffen im gesprochenen und geschriebenen Wort. Immer häufiger sind KI-Systeme nun in der Lage, den *Inhalt* von Gesprächen und Handlungen zu verstehen: mithilfe von Sprachaufzeichnungen, Texten und Videoüberwachung. Setzen Regime diese Technologien zum Machterhalt und zur Kontrolle ein, wird quasi jeder Bürger von einem für ihn abgestellten Stasi-Offizier überwacht – tagein, tagaus, rund um die Uhr.[3]

Selbst in relativ freien Staaten sind Bürger einer immer umfassenderen und wirksameren Überwachung ausgesetzt. Konzerne sammeln und verkaufen Daten über unsere Einkäufe, unsere Nutzung des Internets und sozialer Medien, unseren Einsatz elektrischer Geräte, unsere Telefonate und Textnachrichten, unsere Arbeit und unsere Gesundheit. Unsere Bewegungen können anhand unserer Smartphones und unserer vernetzten Autos verfolgt werden. Kameras auf öffentlichen Straßen und Plätzen erkennen unsere Gesichter. All diese Daten und noch viele mehr lassen sich durch intelligente Informationsintegrationssysteme verknüpfen und ergeben ein ziemlich umfassendes Bild all unserer Handlungen. Sie zeigen, wie wir unser Leben leben, wen wir mögen und wen nicht oder wie wir bei der nächsten Wahl abstimmen werden.[4] Im Gegensatz dazu ist die Stasi geradezu stümperhaft vorgegangen.

Verhaltenskontrolle

Sobald Überwachungskameras installiert sind, folgt der nächste Schritt: Unser Verhalten wird von denen, die diese Technologie einsetzen, nach ihrem Ermessen gesteuert. Eine recht plumpe Methode ist die automatisierte und personalisierte Erpressung. Ein System, das versteht, was Sie tun – ob durch Zuhören, Mitlesen oder Zusehen –, kann auch schnell feststellen, ob Sie etwas Verbotenes tun. Sobald es einen Verstoß entdeckt hat, nimmt es Kontakt auf. Je nach Absicht der Person oder Organisation hinter dem System wird es entweder möglichst viel Geld fordern oder aber versuchen, Ihr Verhalten auf die gewünschte Weise zu beeinflussen. Geldforderungen sind ein perfektes Belohnungssignal für einen Reinforcement-Learning-Algorithmus. Wir können daher davon ausgehen, dass KI-Systeme sehr schnell lernen werden, Fehlverhalten zu erkennen und davon zu profitieren. Anfang 2015 sagte ich gegenüber einem Experten für Computersicherheit, dass automatisierte Erpressungssysteme mit Reinforcement-Learning-Algorithmen schon bald Realität werden könnten. Er lachte darüber und sagte, es gäbe sie längst. Der erste Erpressungsbot, der weithin bekannt wurde, war Delilah. Das war im Juli 2016.[5]

Eine subtilere Möglichkeit, das Verhalten von Menschen zu beeinflussen, besteht darin, ihr Informationsumfeld zu verändern, damit sie andere Dinge glauben und andere Entscheidungen treffen. Werbetreibende nutzen solche Techniken schon seit Jahrhunderten, um das Kaufverhalten von Einzelpersonen zu beeinflussen. Propaganda als Werkzeug zur Meinungsmache in Krieg und Politik existiert schon sehr viel länger.

Was hat sich also geändert? Nun, KI-Systeme können unsere Onlinelesegewohnheiten, unsere Vorlieben und unseren vermuteten Wissensstand erfassen und verfolgen. Auf dieser Grundlage können sie zielgerichtete Nachrichten erzeugen, die maximalen Einfluss auf jede Einzelperson haben und gleichzeitig das Risiko für Zweifel an diesen Botschaften minimieren. Außerdem weiß ein solches KI-System, ob die Nachricht vom Empfänger gelesen wurde, wie viel Zeit er mit dem Lesen verbracht hat und ob er auf Links in der Nachricht geklickt hat. Diese Signale nutzt das System als unmittelbares Feedback über Erfolg oder Misserfolg des Versuchs, das jeweilige Individuum zu beeinflussen. So lernt es sehr schnell, seine Strategie zu optimieren. Auf dieselbe Weise nehmen Content-Algorithmen in sozialen Medien Einfluss auf die politische Meinungsbildung.

Eine weitere Neuerung in unserer Zeit sind *Deepfakes*: Mithilfe von KI, Computergrafiken und Sprachsynthese können realistische Videos und Audioinhalte erzeugt werden, in denen man praktisch jede Person jede beliebige Aussage machen oder Handlung ausführen lassen kann. Dazu benötigt man kaum mehr als eine mündliche Beschreibung des gewünschten Ereignisses, sodass nahezu jeder solche Deepfakes generieren kann. Sie möchten ein Handyvideo, in dem Politiker X sich

4

MISSBRAUCH DER KI

Eine barmherzige und triumphale Nutzung unseres kosmischen Erbes klingt wunderbar, aber wir müssen auch mit einer rasanten Innovationsrate im Bereich der Missbrauchsfälle rechnen. Böswillige Menschen suchen ständig nach Möglichkeiten, die KI zu ihrem Vorteil und zum Nachteil aller anderen zu missbrauchen. Daher wird dieses Kapitel vermutlich noch vor der Veröffentlichung dieses Buchs überholt sein. Lassen Sie sich von den angeführten Beispielen bitte nicht entmutigen, sondern fassen Sie sie als einen Weckruf auf – einen Weckruf zum Handeln, bevor es zu spät ist.

Überwachung, Beeinflussung und Kontrolle

Die automatisierte Stasi

Das Ministerium für Staatssicherheit der Deutschen Demokratischen Republik, kurz Stasi, gilt weithin als »einer der effektivsten und repressivsten Geheimdienste bzw. Geheimpolizeiapparate, die es jemals gab«.[1] Sie führte Akten über den Großteil der ostdeutschen Haushalte, überwachte Telefonate, las Briefe und brachte versteckte Kameras in Wohnungen und Hotels an. Sie war skrupellos effektiv dabei, Aktivitäten von Dissidenten aufzuspüren und zu eliminieren. Anstelle von Gefängnis oder Hinrichtung setzte sie bevorzugt auf psychologische Zersetzung. Für eine solch umfassende Kontrolle war man bereit, extrem viele Ressourcen zu binden. Einige Schätzungen