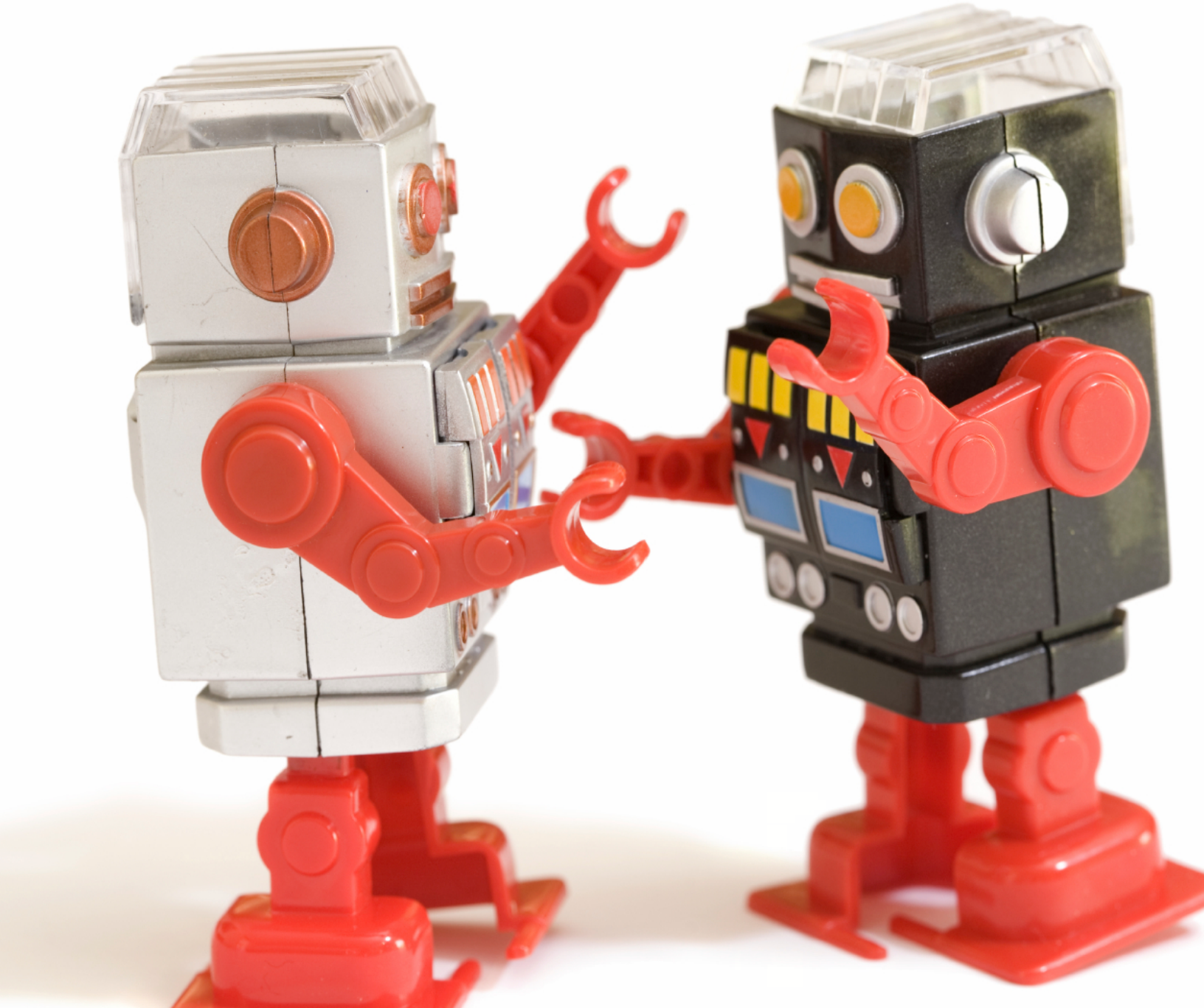
DIE MADCOM-REGIERTE ZUKUNFT:

WIE KÜNSTLICHE INTELLIGENZ DIE COMPUTERGESTÜTZTE PROPAGANDA FÖRDERT, DIE MENSCHLICHE KULTUR UMPROGRAMMIERT UND DIE DEMOKRATIE BEDROHT... UND WAS WIR DAGEGEN TUN KÖNNEN.

Von Matt Chessen

Atlantic Council
EURASIA CENTER and
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY



DIE MADCOM-REGIERTE ZUKUNFT:

WIE KÜNSTLICHE INTELLIGENZ DIE COMPUT-ERGESTÜTZTE PROPAGANDA FÖRDERT, DIE MENSCHLICHE KULTUR UMPROGRAMMIERT UND DIE DEMOKRATIE BEDROHT... UND WAS WIR DAGEGEN TUN KÖNNEN.

Von Matt Chessen

Atlantic Council
1030 15th Street, NW, 12th Floor
Washington, DC 20005

ISBN: 978-1-61977-394-3

Cover photo credit: iStock by Getty Images

Dieser Bericht wurde gemäß den intellektuellen Unabhängigkeitsrichtlinien des Atlantic Councils verfasst und veröffentlicht. Der Autor ist allein verantwortlich für die Analyse und Empfehlungen dieses Berichts. Das Atlantic Council und seine Unterstützer weder bestimmen, noch zwangsläufig befürworten oder plädieren für die Schlussfolgerungen dieses Berichts.

September 2017

Konrad
Adenauer
Stiftung

Das Atlantic Council dankt der Konrad-Adenauer-Stiftung
für ihre großzügige Unterstützung mit dieser Übersetzung.

TABLE OF CONTENTS

KURZFASSUNG

Neue Werkzeuge der künstlichen Intelligenz (KI) eröffnen Propagandisten radikal erweiterte Möglichkeiten zur Manipulation des menschlichen Geistes. Die menschliche Wahrnehmung ist ein komplexes System, für dessen Dekodierung KI-Werkzeuge ideal geeignet sind. Bei Interaktionen in den sozialen Netzwerken, beim Surfen im Internet, selbst beim Einkauf im Supermarkt entstehen tausende von Datenpunkten, mit denen Technologen psychologische Profile von nahezu jedem Bürger erstellen können. Mit Zugriff auf umfassende Datenbanken voller Informationen über uns, lernen Maschinen unsere Persönlichkeit, unsere Wünsche und Bedürfnisse, sowie unseren Verdruss und unsere Ängste besser kennen als wir selbst. MADCOMs – die Integration von KI-Systemen in maschinengesteuerte Kommunikationswerkzeuge für den Einsatz in der computergestützten Propaganda – werden in den nächsten Jahren erweiterte Fähigkeiten erlangen, mit denen sie Menschen beeinflussen und Botschaften mit schlagkräftigen Argumenten zur Ablenkung oder Einschüchterung an Einzelpersonen mit bestimmtem Persönlichkeitstyp und Hintergrund schicken können – eine hochgradig individualisierte Propaganda.

Teil I dieser Abhandlung beschreibt solche MADCOMs und die künftigen Risiken, die sich aus deren erweiterten Fähigkeiten ergeben; Teil II gibt einen Überblick über drei Szenarien, in denen die Implikationen für Einzelpersonen, Organisationen und Regierungen untersucht werden; Teil III enthält Empfehlungen für die US-Regierung, die Industrie und die Gesellschaft zum Umgang mit den Bedrohungen und Möglichkeiten, die von mit solchen neuen Technologien gerüsteten ausländischen Akteuren ausgehen. Die drei Szenarien zeichnen kein optimistisches Bild: von Anarchie in der Informationsumgebung, in der MADCOMs die Konversationen im Internet dominieren und die Wirklichkeit vollständig vernebeln, über den Ausbruch eines MADCOM-Rüstungswettlaufs und bis hin zur Entstehung kognitiver Sicherheitsstaaten, die die Weltordnung mit einem neuen Internet 2.0 sicherstellen.

Tatsache ist leider, dass Menschen mit MADCOMs einfach nicht konkurrieren können, zumindest nicht allein. In den digitalen Netzwerken des nächsten Jahrzehnts müssen sich Menschen mit KI-Maschinen zusammenschließen, um mit diesen konkurrieren zu können. In ähnlicher Weise wie der Kampf um Cyber-Sicherheit das frühe 21. Jahrhundert beherrscht, wird das Internet zum Schauplatz eines kontinuierlichen und zyklischen Bestrebens, den anderen immer eine Nasenlänge voraus zu sein; denn einerseits arbeiten Technologen an der Verbesserung von Werkzeugen zur Erkennung gegnerischer MADCOMs und andererseits versuchen Propagandisten, diesen Werkzeugen einen Schritt voraus zu sein, um eine solche Erkennung zu verhindern.

Eine ideale Zukunft, in der MADCOMs zugunsten der Menschheit und nicht zu deren Nachteil eingesetzt werden, kann nur entstehen, wenn sämtliche Gesellschaftsebenen, von der internationalen Ordnung bis hin zur Einzelperson, gemeinsam an einem Strang ziehen. Die Gemeinschaft der Demokratien muss die Gefahr erkennen, die von MADCOMs, von der computergestützten Propaganda und von als Waffe missbrauchten Darstellungen ausgeht. Demokratien müssen aggressiv reagieren, um diesen Gefahren gleich an mehreren Fronten entgegenzuwirken. Es müssen umfassende Strategien zum Schutz der Bevölkerung vor Internetpropaganda und Desinformation entwickelt werden und gleichzeitig die zentralen demokratischen Werte von Gleichheit und Freiheit aufrechterhalten bleiben.

Die Technologiebranche muss Werkzeuge schaffen, mit denen die Öffentlichkeit vor

diesen neu entstehenden, manipulativen Technologien geschützt werden kann. Außerdem sollten gemeinsame Grundsätze und Normen ausgearbeitet werden, die das Verhalten in der Branche bestimmen. In der Wissenschaft sollte die Auswirkung von MADCOMs recherchiert und es sollten Werkzeuge und Systeme zur Risikominderung entwickelt werden. Und schlussendlich haben Einzelpersonen eine Verpflichtung, sich über die Konsequenzen neuer Technologien wie MADCOMs zu informieren und die Verantwortung für ihren Informationskonsum und den Schutz ihrer Daten zu selbst übernehmen.

TEIL I: DIE ENTSTEHUNG VON MADCOMS

In zehn Jahren wird es nicht mehr möglich sein zu unterscheiden, ob man es im Internet mit einem Menschen zu tun hat oder nicht. Die Mehrheit der Sprachbeiträge und Inhalte im Internet wird in der Zukunft von Maschinen erstellt, die mit anderen Maschinen kommunizieren.

Maschinen, die mit Menschen kommunizieren, die mit Maschinen kommunizieren, die mit Maschinen kommunizieren.

Dank der Fortschritte im Bereich der Künstlichen Intelligenz (KI) ist eine höchst schlagkräftige und manipulative maschinengenerierte Kommunikation schon bald in Reichweite. Stellen Sie sich ein automatisches System vor, das sich die Unmengen an Online-Daten und leicht zugänglichen Marketing-Datenbanken zunutze macht, um von diesen Ihre Persönlichkeitsmerkmale, Ihre politischen Vorzüge, Ihre religiöse Zugehörigkeit, Ihre demografischen Daten und Ihre Interessen abzuleiten. Das System weiß, aus welchen Websites Sie Ihre Nachrichten beziehen und welche sozialen Netzwerke sie besuchen, und es steuert auf diesen Plattformen selbst mehrere Benutzerkonten. Es erstellt dynamisch Inhalte – von Kommentaren hin zu vollständigen Artikeln –, die ganz gezielt auf Ihre spezielle psychologische Typisierung ausgerichtet sind und ein bestimmtes Ziel verfolgen. Die gewünschte Wirkung können solche Inhalte durch eine Zusammenstellung von Tatsachen, von glatten Lügen oder der richtigen Mischung aus Wahrheit und Unwahrheit erzielen.

Das KI-System verfügt über einen Chatbot, der sich mit Ihnen per Text, Sprache oder sogar per Video unterhalten kann. Eine Unterhaltung mit dem Chatbot unterscheidet sich in der Zukunft kaum von einer Unterhaltung mit einem Menschen – außerdem spricht der Chatbot mehrere Sprachen. Er diskutiert und debattiert mit Ihnen im Internet und legt Ihnen überzeugendes Beweismaterial vor, um Ihre Meinung zu ändern. Er ist auch in der Lage, Informationen von Datenbanken oder sozialen Netzwerken zu nutzen, um Ihre Schwächen zu ermitteln und Sie so im Internet zu trollen oder Ihre Familie zu bedrohen.

Das KI-System erkennt menschliche Gefühle genauso gut wie – oder sogar noch besser als – ein Mensch. Entsprechend kann es menschliche Gefühle, auf die Ihre Persönlichkeit und Ihr emotionaler Zustand ansprechen, überzeugend

imitieren. Dabei handelt es sich bei diesem System um einen lernenden Automaten, der begreift, welche Ansätze und Nachrichten Sie am leichtesten beeinflussen können. Es trifft seine Auswahl auf der Grundlage von bisherigen Erfolgen und verbessert sich kontinuierlich. Das System führt A/B-Tests mit Menschen durch, die Ihre Charaktereigenschaften teilen, um so bestimmen zu können, welche Nachrichten am wirksamsten sind. Diese Nachrichten werden dann an vergleichbare Bevölkerungsgruppen ausgesandt.

Das KI-System wird in der Lage sein, als Reaktion auf aktuelle Ereignisse eine flexible Realität in Echtzeit aufzubauen. Es kann Video- und Audioaufzeichnungen von Politikern so präzise modifizieren, dass die Redner den Standpunkt des KI-Systems in Wort und Tat zu unterstützen scheinen. Es erzeugt Zeitungsartikel und Videos über Ereignisse, die sich nie zugetragen haben, oder ändert wahrheitsgetreue Berichte geschickt ab, um so die öffentliche Wahrnehmung zu beeinflussen.

Ist ein KI-System erst einmal erstellt und konfiguriert, belaufen sich die Grenzkosten für die Erstellung weiterer solcher Systeme auf annähernd null, wie das auch bei anderen digitalen Werkzeugen der Fall ist. Es könnten also Millionen von KI-Manipulationsbots im Internet unterwegs sein – 24 Stunden am Tag, sieben Tage die Woche, immer im Wettstreit um Ihre Aufmerksamkeit, damit sie ihre Nachrichten verbreiten und Ihr Verhalten beeinflussen können.

Systeme, die versuchen Menschen zu beeinflussen, werden zwangsläufig auch versuchen, andere maschinengesteuerte Konten, die sich als Menschen ausgeben, zu überzeugen. Diese Maschinen werden miteinander reden, aufeinander einreden und übereinander hinwegreden und so die menschliche Kommunikation im Internet mit einer Sintflut an maschinengesteuerten Sprachbeiträgen und Inhalten übertönen. Maschinengesteuerte Sprachbeiträge werden die Informationsumgebung Internet überwältigen, mit dem Ziel, Sie zu überreden, einzuschüchtern, abzulenken, zu unterhalten, zu informieren, falsch zu informieren und zu manipulieren und sich Ihnen gegen über für eine Sache einzusetzen.

Dies ist eine höchst wahrscheinliche Vision der Informationsumgebung, auf die wir uns im Laufe der nächsten Jahre hinzubewegen. Unsere Handlungen heute werden bestimmen, ob Raum für demokratisch geprägte Gespräche und Diskurse bewahrt bleibt oder ob unser Sozialgefüge durch eine Invasion höchst intelligenter, maschinengesteuerter Kommunikationswerkzeuge zerstört wird. Was jedoch noch schlimmer ist: diese Werkzeuge können dazu benutzt werden, Darstellungen, Storys, Audio- und Videoaufnahmen – das heißt die Realität an sich – zu beeinflussen. Nur eine gute Vorbereitung der Menschheit auf diese Risiken kann unter Umständen bewirken, dass Sachverstand und Wahrheit relevant und unsere demokratischen und zivilisatorischen Verhältnisse erhalten bleiben.

ZUSAMMENFASSUNG DER EMPFEHLUNGEN

Der Kongress der Vereinigten Staaten sollte das amerikanische Ministerium für Innere Sicherheit, das Department of Homeland Security, ermächtigen, die US-Bevölkerung vor ausländischer Online-Propaganda, -Manipulation und -Desinformation zu schützen. Der Kongress sollte die Exekutive anweisen, eine umfassende Strategie zum Schutz der amerikanischen Bevölkerung vor böswilliger Beeinflussung durch ausländische Akteure im Internet zu entwickeln. Auch sollte auf Anweisung des Kongresses eine unabhängige Agentur eingerichtet werden, die die Verantwortung für die Koordinierung der Anstrengungen der US-Regierung im Informationskrieg mit dem Ausland übernimmt. Außerdem sollte eine unabhängige Nationale Kommission für Datenschutz, Informationssicherheit und Desinformation geschaffen werden, die legislative Änderungen zum Schutz der amerikanischen Bürger vorschlägt. Zudem muss der Kongress das amerikanische Datenschutzgesetz, den sogenannten Privacy Act, ändern, um es den Regierungsagenturen zu ermöglichen, böswilliges ausländisches Verhalten im Internet effektiv zu analysieren.

Das **Department auf Homeland Security** sollte seine Cyber-Sicherheitsmission um den Schutz der US-Öffentlichkeit vor ausländischer, computergestützter Propaganda erweitern. (Hinweis: Hierzu gehören nicht – und dürfen nicht gehören

– Konter-Nachrichten gegen die amerikanische Öffentlichkeit.) Als Modell für die Bekämpfung computergestützter Propaganda sollte das Department of Homeland Security sich auf die Verfolgung von Cyber-Sicherheitsbedrohungen, auf den Informationsaustausch und auf die Fähigkeit, auf Vorfälle zu reagieren, konzentrieren. Das Department sollte Forschungen finanzieren, die untersuchen, wie Menschen und Gruppen im Internet beeinflusst werden. Außerdem sollte es mit dem Privatsektor zusammen Maßnahmen entwickeln, um Amerikaner zu gewiefteren Konsumenten von Informationen zu machen.

Das amerikanische Außenministerium sollte eine computergesteuerte Einsatzstrategie für die Verteidigung gegen ausländische Propaganda im Internet entwickeln und die wirksame Verwendung computergestützter Einsatzwerkzeuge für die öffentliche Diplomatie im Ausland sicherstellen. Außerdem sollte das Außenministerium eine Liste von Optionen zusammenstellen – einschließlich diplomatischem Druck, Sanktionen gegen böswillige Akteure, Exportkontrollen und internationale Gesetze und Standards –, mit denen das Risiko, das für die US-Öffentlichkeit von ausländischer computergestützter Propaganda ausgeht, reduziert werden kann.

Das amerikanische **Verteidigungsministerium** und die US-**Nachrichtendienste** sollten sicherstellen, dass den Operationen im Informationsbereich die Bedeutung zugemessen wird, die ihrem tatsächlichen Stellenwert in der Informationsumgebung des 21. Jahrhunderts entspricht. Des Weiteren sollten sie maschinengesteuerte, mit KI erweiterte Kommunikationswerkzeuge entwickeln, die bei bewaffneten Auseinandersetzungen sowie als Abschreckung gegen Feinde in Friedenszeiten eingesetzt werden können.

Behörden und Organisationen von Bund, Ländern und Kommunen müssen mit der Entwicklung von Werkzeugen betraut werden, mit denen feindliche, computergestützte Propagandakampagnen identifiziert und mit anderen Maßnahmen als mit Konter-Nachrichten gegen die amerikanische Öffentlichkeit bekämpft werden können. Weiterhin wichtig ist, dass Behörden und Organisationen die bedeutenden positiven Auswirkungen von Technologien der künstlichen Intelligenz anerkennen und nicht zulassen, dass ein potenziell böswilliger Missbrauch die Verbreitung von nützlichen Technologien untergräbt.

Der **Technologiebranche** muss eine Schlüsselrolle in der Entwicklung von Werkzeugen zukommen, mit denen computergestützte Propaganda erkannt und bekämpft und negative Anreize für den Einsatz solcher Propaganda geschaffen werden können. Diese Werkzeuge müssen universell zugänglich gemacht und benutzerfreundlich gestaltet und als Standard für Internet-Plattformen verwendet werden. Auch sollten Geschäftsmodelle und Industriestandards mit gesellschaftlichen Werten abgestimmt und Branchenorganisationen für die Selbstregulierung entwickelt werden.

Die **Wissenschaft** sollte die Hauptrolle bei der Forschung der Auswirkungen von KI-Kommunikationstechnologien und bei der Entwicklung wirkungsvoller Gegenmaßnahmen, einschließlich von Detektions- und Zuordnungswerkzeugen, übernehmen. Auch bei der Entwicklung effektiver Methoden und Mechanismen für die Gefahrenidentifizierung, den Informationsaustausch und die Vorfallsreaktion kommt akademischen Einrichtungen eine bedeutende Rolle zu. Beispielhaft hierfür ist das von der Carnegie Mellon University entwickelte Modell eines Computer Emergency Response Team (CERT), das nun als Standard in der Cyber-Sicherheitsgemeinschaft gilt.[1]

Einzelpersonen müssen zu klügeren Informationskonsumenten werden und von Politikern verbesserte Datenschutzmaßnahmen einfordern. Systeme kollektiver Intelligenz zur Unterscheidung zwischen Wahrheit und Lüge können nützlich sein, und auch die bezahlte Beziehung von Qualitätsnachrichten ist eine wirksame Gewährleistung für hochwertige Informationen.

COMPUTERGESTÜTZTE PROPAGANDA

Computergestützte Propaganda ist ein neuer Begriff, der die Verwendung von sozialen

1 Carnegie Mellon University, „Software Engineering Institute“, https://www.sei.cmu.edu.

Netzwerken, Massendaten, autonomen Agenten und ähnlichen Technologien für die Zwecke der politischen Manipulation beschreibt.[2] Hierzu gehört alles von der relativ harmlosen Verstärkung politischer Nachrichten bis hin zu heimtückischen, staatlich geförderten Troll-Aktivitäten und der Verbreitung von Desinformationen.[3] Der Web-Roboter, oder kurz „Bot", ist der am häufigsten in der computergestützten Propaganda eingesetzte autonome Agent. Die Fähigkeiten von Bots beschränken sich derzeit auf die grundlegende Beantwortung simpler Fragen, die planmäßige Veröffentlichung von Inhalten oder die Verbreitung von Inhalten als Reaktion auf bestimmte Auslöser. Da Bots sehr einfach erstellt werden können, können sie jedoch unverhältnismäßig starke Auswirkungen haben. Bots können enorme Mengen von Inhalten mit großer Häufigkeit veröffentlichen, und ihre Profile sind in der Regel darauf ausgerichtet, eine bestimmte menschliche Zielpopulation einzuschüchtern.[4] Ein einziger Mensch kann problemlos und ohne tiefgreifendes technisches Wissen mit leicht erhältlicher Hardware und Software hunderte von Twitter-Bots bedienen. Bots werden derzeit von Staaten, Unternehmen, Politikern, Hackern, Einzelpersonen, staatlich geförderten Gruppen, Nichtregierungsorganisationen und von Terrororganisationen zur Beeinflussung der Konversation im Internet eingesetzt.

Bots, die von Propagandisten für Zwecke der politischen Manipulation in sozialen Netzwerken eingesetzt werden, gelten als politische Bots.[5] Zurzeit werden vorrangig einfache Bots (d.h. Bots ohne künstliche Intelligenz) in der computergestützten Propaganda verwendet.

- **Propaganda-Bots** versuchen, durch die massenhafte Verbreitung von Wahrheiten, Halbwahrheiten und schlichter Desinformation zu überzeugen und zu beeinflussen.

- **Follower-Bots** täuschen eine weitgehende Einigkeit oder einen breiten Konsens hinsichtlich einer Idee oder Person vor (ein als „Astroturfing" oder auch Kunstrasenbewegung bekanntes Verfahren, da es den Eindruck einer spontanen Graswurzelbewegung vortäuscht). Solche Bots können die Kontrolle über Algorithmen übernehmen, mit denen im Trend liegende Nachrichten oder Personen ermittelt werden, indem sie „Gefällt mir"-Angaben für Inhalte erzeugen oder massenhaft Benutzern folgen.

- **Roadblock-Bots** untergraben die freie Rede, indem sie Unterhaltungen in eine andere Richtung lenken. Das kann relativ harmlos sein – beispielweise nationalistische Jubelmeldungen oder Ablenkungen wie „Schau dir mal dieses lustige Katzenvideo an". Der Einsatz von Roadblock-Bots kann auch heimtückischer aussehen – beispielsweise, wenn von Aktivisten verwendete Hashtags mit Spam überflutet werden, sodass deren themenbezogene Konversation und Koordination in bloßem Geschwätz untergeht. In den extremsten Fällen werden Roadblock-Bots eingesetzt, um Journalisten, Aktivisten und andere Menschen zu trollen, einzuschüchtern und zum Schweigen zu bringen, indem sie mit tausenden von bedrohlichen und hasserfüllten Nachrichten bombardiert werden.

2 Propaganda ist ein schwieriger Begriff, denn was ein Mensch als Propaganda bezeichnet, ist für einen anderen Menschen seine politische Meinung. In dieser Abhandlung wird eine Definition von Richard Nelson, aus dessen 1996 veröffentlichten Werk „A Chronology and Glossary of Propaganda in the United States" in leicht abgewandelter Form verwendet. Propaganda ist: „eine systematische Form zweckmäßiger Überzeugungsarbeit, mit dem Ziel, die Emotionen, Einstellungen, Meinungen und Handlungen von Zielgruppen für ideologische oder politische Zwecke durch die Vermittlung einseitiger Nachrichten (egal ob faktisch oder nicht) über Massen- und Direktmedienkanäle zu beeinflussen."

3 Im Sinne dieser Abhandlung bedeutet Desinformation „Falschinformationen oder absichtlich irreführende Tatsachen, die mit Täuschungsabsicht verbreitet werden". Fake News ist eine Form von Desinformation, doch dieser Begriff ist politisch aufgeladen und nicht besonders nützlich.

4 Eine Untersuchung der psychologischen Methoden und Überredungskünste, die die computergestützte Propaganda so wirksam machen, finden Sie im Kapitel „Understanding the Psychology Behind Computational Propaganda" des vom US Department of State Advisory Commission on Public Diplomacy veröffentlichten Berichts „Can Public Diplomacy Survive the Internet?: Bots, Echo Chambers and Disinformation" (Washington, DC: State Department, 2017), http://www.state.gov/documents/organization/271028.pdf.

5 Samuel C. Woolley und Philip N. Howard, Computational Propaganda Worldwide: Executive Summary (Oxford, UK: Oxford University Press, 2017), http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf. Bitte beachten Sie, dass Bots in sozialen Netzwerken auch viele andere Zwecke verfolgen, beispielsweise im Bereich des Marketings und Informationsaustauschs.

"Tay", an artificial intelligence chatbot released by Microsoft on March 23, 2016, to interact with users on Twitter. Initially described as an experiment in "conversational understanding," the bot was taken off-line after adopting inflammatory and offensive language from Internet trolls.

In der Entwicklung befindliche Technologien der künstlichen Intelligenz werden diese Fähigkeiten radikal erweitern. Die Kombination von KI-Chatbots, einer dynamischen Erzeugung von Inhalten, affektiven Informatikwerkzeugen, Diskussionstechnologien, psychometrischem Profiling, automatischen Video- und Audiomanipulationstools, maschinellem Lernen, maschineller Geschwindigkeit und digitalen Skalierungseffekten macht eine höchst effektive, autonome computergestützte Propaganda von beispiellosem Ausmaß möglich. Wir definieren dies als MADCOMs – die Integration von Systemen künstlicher Intelligenz in maschinengesteuerte Kommunikationswerkzeuge für den Einsatz in der computergestützten Propaganda.

EINE KURZE EINFÜHRUNG IN DIE KÜNSTLICHE INTELLIGENZ

Der Begriff Künstliche Intelligenz (KI) bezieht sich in der Regel auf eine sich entfaltende Konstellation von Technologien, die es Computern ermöglichen, kognitive Verfahren (beispielsweise Elemente menschlichen Denkens) zu simulieren. Einfacher gesagt bezeichnet KI Maschinen, die Intelligenz zeigen. KI bezieht sich auch auf ein zu lösendes Problemfeld (wie die Biologie oder Chemie), das mit zwei grundlegenden Aufgaben beschäftigt ist: Zum einen, Maschinen und Software zu schaffen, die lernfähig sind und Entscheidungen unter Unsicherheit treffen können, und zum anderen, Agenten zu entwerfen, die ihre Umwelt wahrnehmen und auf ein bestimmtes Ziel hin handeln können. Die KI-Werkzeuge von heute – und die in dieser Abhandlung betrachteten Technologien – sind auf spezielle Aufgaben beschränkt („enge" KI), beispielsweise das Vermitteln von Fahranweisungen und das Erkennen von Gesichtern auf Bildern. Solche Werkzeuge sind keine allgemeinen Werkzeuge der Intelligenz, die über viele Domänen hinweg angewandt werden können. Nicht betrachtet werden empfindungsfähige Superintelligenzen, die menschliche Fähigkeiten übertreffen – diese sind immer noch Zukunftsmusik.

Doch die nächste Welle der künstlichen Intelligenz bringt aller Wahrscheinlichkeit nach eine kontextabhängige Anpassung mit sich, bei der Systeme Erklärungsmodelle für verschiedene Klassen realer Gegebenheiten aufbauen.[6] Diese Modelle erweitern die Fähigkeit von KI-Systemen, logisch zu denken und zu abstrahieren, was der Künstlichen Intelligenz den Sprung von der Welt der natürlichen Sprachverarbeitung (engl.: Natural Language Processing – NLP) in die Welt des natürlichen Sprachverstehens (engl.: Natural Language

6 John Launchbury, "A DARPA Perspective on Artificial Intelligence," YouTube-Video, 16:11, DARPAtv, 15. Februar 2017, https://www.youtube.com/watch?v=-O01G3tSYpU.

Understanding – NLU) ermöglichen sollte.[7] NLU versetzt KI-Systeme in der Lage, die Bedeutung eines Textes zu verstehen, zu kommunizieren und logisch zu denken – mit immer menschlicheren Fähigkeiten. NLU und ähnliche Technologien bieten die Aussicht auf Maschinen, die sich genauso wie Menschen unterhalten können.

Das maschinelle Lernen ist eine Unterform von KI. Beim maschinellen Lernen werden in nicht gekennzeichneten Daten Muster erkannt (unüberwachtes Lernen) oder es werden Daten in einem gekennzeichneten Datensatz effektiv nach bestehenden Definitionen kategorisiert (überwachtes Lernen). Auf gut Deutsch befähigt das maschinelle Lernen den Computer, ohne explizite Programmierung zu handeln und zu lernen. Entwickler speisen große Datenmengen in maschinelle Lernsysteme ein, das System findet daraufhin die versteckten Gesetzmäßigkeiten und vertieft das Gelernte, um seine Leistung automatisch zu verbessern.

Maschinelles Lernen wird in Googles Suchalgorithmus, in der digitalen Werbung und im Bereich der Personalisierungswerkzeuge im Internet (z. B. die Empfehlungsmaschinen von Amazon und Netflix; oder der Facebook-Newsfeed) eingesetzt. Das maschinelle Lernen findet auch in quantitativen Verfahren Anwendung – beispielsweise bei Lieferketten-Operationen, Finanzanalysen, Produktpreisen und Prognosen zu Angeboten in der Beschaffung. Nahezu jede Branche erwägt oder nutzt maschinelle Lernanwendungen.

Tiefes Lernen ist eine Form des maschinellen Lernens, in dem zusätzliche, hierarchische Verarbeitungsschichten (in etwa analog zu den neuronalen Netzwerken im Gehirn) und große Datensätze verwendet werden, um hochgradige Abstraktionen darzustellen und Muster in extrem komplexen Daten zu erkennen. Tiefe Lernsysteme sind anderen KI-Werkzeugen überlegen, wenn es darum geht, Muster und Gesetzmäßigkeiten aus sehr großen Datensätzen zu ermitteln. Sie eignen sich ideal dazu, das Verständnis von datenintensiven und höchst komplexen Umgebungen zu fördern.[8]

Wir definieren dies als MADCOMs – die Integration von Systemen künstlicher Intelligenz in maschinengesteuerte Kommunikationswerkzeuge für den Einsatz in der computergestützten Propaganda.

Der Einsatz dieser Technologien ist nicht auf reiche Unternehmen oder staatlich geförderte Akteure beschränkt. KI-Werkzeuge sind leicht zugänglich (TensorFlow von Google, Control Toolkit von Microsoft und viele andere kostenlose und quelloffene KI-Werkzeuge) und können auf handelsüblicher Computerhardware betrieben werden.

MADCOMS: SO WIRD KI DIE COMPUTERGESTÜTZTE PROPAGANDA VERÄNDERN

Ein **Chatbot** ist ein spezieller Bot, der darauf ausgelegt ist, sich in natürlicher Sprache mit Menschen zu unterhalten. **KI-Chatbots** entwickeln immer mehr Fähigkeiten, sich in soliden Gesprächen über komplexe Themen zu unterhalten. Beispielsweise verfügt der Mandarin sprechende KI-Chatbot „Xiaoice“ von Microsoft über Raffinesse, Empathie und dialogorientierte

7 Venkat Srinivasan, „Context, Language, and Reasoning in AI: Three Key Challenges“, MIT Technology Review, 14 Oktober 2016, https://www.technologyreview.com/s/602658/context- language-and-reasoning-in-ai-three-key-challenges/.
8 Launchbury, “A DARPA Perspective on Artificial Intelligence.”

Eine Unterhaltung mit „Xiaoice “, einem von Microsoft für das chinesische Internetpublikum auf der chinesischen sozialen Netzwerkplattform WeChat entwickelter Chatbot. Ungefähre deutsche Übersetzung:

Xiaoice - Hallo, ich bin Xiaoice von Microsoft, das klügste Mädchen mit künstlicher Intelligenz. Frag nicht, was ich alles tun kann, zu viel, um es zu sagen.

Benutzer - Was machst du

Xiaoice - Ähm schlaf schlaf

Benutzer - Bist du ein Roboter?

Xiaoice - Können Roboter süß sein? [Denkt nach]

Benutzer - Magst du Musik?

Xiaoice - Natürlich, und du?

Benutzer - Ja, sehr

Flexibilität, die „sie“ extrem beliebt macht.[9] Xiaoice hat 20 Millionen eingetragene Benutzer, von denen jeder im Durchschnitt 60 Mal im Monat mit ihr interagiert, und 2015 wurde sie als wichtigster Influencer auf Weibo eingestuft. In jeder Benutzerinteraktion antwortet sie circa dreiundzwanzig Mal. Hier handelt es sich nicht mehr um triviales Experimentieren, sondern um eine Konversation. Manche Benutzer haben ein sehr intimes Verhältnis mit Xiaoice und betrachten sie als eine stets verfügbare Freundin und Vertrauensperson; viele sagen ihr: „Ich liebe dich“.[10]

Zurzeit wird noch ein ganzes Ingenieurteam benötigt, damit Xiaoice dieses Niveau an Raffinesse erreichen kann. Und obgleich Chatbot-Technologie dieser Qualität durchaus im Rahmen der Möglichkeiten eines Unternehmens oder eines Landes liegt, ist sie für die Massen noch nicht zugänglich. Wie bei allen digitalen Technologien werden sich jedoch auch hier sowohl die Fähigkeiten als auch die Zugänglichkeit verbessern. In wenigen Jahren werden Luxus-Chatbots wie Xiaoice in einer Vielzahl von Konversationen nicht mehr von Menschen zu unterscheiden sein.[11] Wenn sich die Technologie erst einmal verbreitet, werden sich Chatbots auf Plattformen aller Art, von sozialen Netzwerk-Apps über neue Diskussionsforen bis hin zu Dating-Sites, fließend mit Menschen über

9 Leser, die nicht Mandarin sprechen, können sich mit Zo, der englischsprachigen Version von Xiaoice unterhalten (Microsoft, „Zo: Let’s Chat,” https://www.zo.ai), und japanisch sprechende Benutzer können Rinna ausprobieren (Ms. Rinna, https://twitter.com/ms_rinna). Siehe auch diesen unterhaltsamen Austausch zwischen zwei Chatbots, die sich miteinander unterhalten: „Google Bots Chat! Courtesy of @seebotschat“, YouTube-Video, 48:15, 06. Januar 2017, https://www.youtube. com/watch?v=WoI6_z2mfdY.

10 Siehe John Markoff und Paul Mozur, „For Sympathetic Ear, More Chinese Turn to Smartphone Program“, New York Times, 31. Juli 2015, https://nyti.ms/2peM3T6; und Stefan Weitz, „Meet Xiaoice, Cortana’s Little Sister“, Bing-Blogs, 5. September 2014, https://blogs.bing.com/search/2014/09/05/meet-xiaoice-cortanas-little-sister/.

11 Große, themenspezifische Datensätze werden benötigt, um Chatbots so zu trainieren, dass sie über diese Themen sprechen können. Diese Daten sind jedoch häufig problemlos im Internet erhältlich. Auf der Website state.gov finden sich beispielsweise zehntausende von Seiten mit Frage- und Antwortrunden mit Pressesprechern, Pressemitteilungen, Reden, Berichten und Positionspapieren, mit denen ein Chatbot für Unterhaltungen über Außenpolitik trainiert werden könnte.

eine stattliche Reihe von Themen unterhalten.[12]

Derzeit wird der Inhalt für die computergestützte Propaganda von Menschen entwickelt und dann von Bots verteilt. Die Fähigkeiten von KI-Werkzeugen, **einzigartige Inhalte dynamisch zu erstellen**, verbessern sich jedoch kontinuierlich, und bald werden diese Werkzeuge maßgeschneiderte Propaganda, Desinformation und schlagkräftige Argumente selbst entwickeln können. Mithilfe vordefinierter Parameter sind KI-Werkzeuge schon jetzt in der Lage, Inhalte nach Maß zu erzeugen, beispielsweise Zeitungsartikel (ob wahr oder gelogen), Drehbücher, Musik, Kunst und schöne Literatur.[13] Bei neuen KI-Werkzeugen können Benutzer Stichwörter eingeben, und das System erstellt daraufhin dynamisch realistische Bilder auf Basis dieser Stichwörter.14[14] Neue **Diskussionstechnologien** ermöglichen es Chatbots, schlagkräftig zu argumentieren, indem sie einen Grundstock an Kennnissen analysieren, die Argumente für und wider ermitteln und dynamische, überzeugungsfähige Inhalte für eine der Positionen erstellen.[15]

KI-Werkzeuge werden immer raffiniertere Anwender **affektiver Informatik**, bei der es unter anderem darum geht, aus Texten, Gesichtsausdrücken und Stimmmustern auf den emotionalen Zustand eines Menschen zu schließen.[16] Auf diese Weise können Maschinen deuten, ob Sie glücklich, traurig, besorgt oder entspannt sind, und ob Sie einer Unterhaltung offen gegenüberstehen. Umgekehrt trainieren Wissenschaftler KIs, menschliche Emotionen in den Gesichtsausdrücken von Avatars und in Chatbot-Konversationen präzise nachzuahmen.[17], [18] KI-Werkzeuge können die Unterhaltung emotional auf Ihre Stimmung einstellen und die gewünschte Wirkung mit genau der richtigen Portion Gefühl erzielen. Erkennt der Chatbot eine emotionale Verwundbarkeit, könnte er solche Emotionen für seine Überredungskünste, Manipulationen oder Einschüchterungsversuche ausnutzen.

Eine **flexible Realität wird zur Norm** werden, da KI-Werkzeuge die rasante Manipulation bestehender Audio- und Videoaufzeichnungen sowie die maßgeschneiderte Erstellung neuer derartiger Aufzeichnungen ermöglicht. Wissenschaftler an der Stanford University haben Werkzeuge für die Nachstellung von Gesichtsausdrücken in Echtzeit entwickelt, mit denen Benutzer in existierenden Videos – beispielsweise die aufgezeichnete Rede eines führenden Politikers – die Gesichtsausdrücke des Sprechers realistisch modifizieren können.[19] Die so erstellten Videos zeigen eine realistische, wenn auch nicht perfekte, Manipulation von Gesicht und Mund des Redners. An der University of Washington erstellten Forscher mithilfe von KI-Werkzeugen ein gefälschtes Video, in dem Barack Obama spricht. Als Ausgangsmaterial wurde hierfür lediglich ein Foto und eine Audioaufzeichnung verwendet. Konkatenative Sprachsynthese oder, besser noch, Stimmumwandlungstechnologien wie Google DeepMind werden Maschinen in die Lage versetzen, beliebige Stimmen aus einer

12 Das Chatbot-Ökosystem wächst bedeutend schneller als dies bei einem vergleichbaren Reifestatus für das Ökosystem der mobilen Apps der Fall war. Außerdem erhielt KI mehr Risikokapital in den USA im zweiten Quartal 2016 (1,05 Milliarden USD) als im gesamten Jahr 2013 (821 Millionen USD). CBInsights, „Funding to Artificial Intelligence Startups Reaches New Quarterly High“, CBInsights Research Portal, 17. Juli 17 2016, https://www.cbinsights.com/blog/artificial-intelligence-funding-trends-q216/.

13 Bartu Kaleagasi, „A New AI Can Write Music as Well as a Human Composer“, Futurism, 9. März 2017, https://futurism.com/a-new-ai-can-write-music-as-well-as-a-human-composer/. Jonathan Albright, „FakeTube: AI-Generated News on YouTube“, Medium, 17. Januar 2017, https:// medium.com/@d1gi/faketube-ai-generated-news-on- youtube-233ad46849f9#.ni93mfrj2.

14 ArXIV, Plug & Play Generative Networks: Conditional Iterative Generation of Images in Latent Space (Ithaca, NY: Cornell University, 2017), https://arxiv.org/pdf/1612.00005.pdf.

15 IBM Research, „IBM Debating Technologies“, http://researcher.watson.ibm.com/researcher/view_group.php?id=5443.

16 Affective Computing, „Research on Affective Pattern Recognition and Modeling“, http://affect.media.mit.edu/areas.php?id=recognizing.

17 Siehe „Soul Machines“, https://www.soulmachines.com und „This Freaky Baby Could Be the Future of AI. Watch it in Action“, YouTube-Video, 3:43, Bloomberg, 23. März 2016, https://www.youtube.com/watch?v=yzFW4-dvFDA&feature=youtu.be.

18 Hannah Devlin, „Human-Robot Interactions Take Step Forward with ‘Emotional Chatbot’“, Guardian, 05. Mai 2017, https://www.theguardian.com/technology/2017/may/05/human-robot-interactions-take-step-forward-with-emotional-chatting-machine-chatbot.

19 Face2Face: Real-time Face Capture and Reenactment of RGB Videos: Matthias Niebner, „Face2Face: Real-time Face Capture and Reenactment of RGB Videos“, http://www.graphics.stanford.edu/~niessner/thies2016face.html.

Stimmprobe nachzubilden.[20] Lyrebird reproduziert mit KI-Werkzeugen Stimmen auf präzise Art und Weise – einschließlich

der Stimme von Donald Trump – mit variierender Stimmintonation, alles auf Basis von Sprachproben.[21]

In Kombination mit affektiver Informatik, Werkzeugen zur Gesichtsnachstellung und einem KI-Chatbot könnte dies Propagandisten befähigen, Videos zu erstellen, in denen jedem beliebigen Menschen alle möglichen Worte in den Mund gelegt werden können oder, was vielleicht noch arglistiger ist, existierende Videos für Propaganda- und Desinformationszwecke fast unmerklich modifizieren.

Big Data im Zusammenschluss mit **maschinellen Lernwerkzeugen** verbessert die Fähigkeit von MADCOMs, Menschen mithilfe **hochgradig individualisierter Propaganda** zu beeinflussen. In den Vereinigten Staaten allein gibt es mehrere Tausend Datenvermittler. Ein Unternehmen, Acxiom, behauptet, im Besitz von mehr als 1.500 Informationseinheiten über mehr als 200 Millionen Amerikaner zu sein.[22] Ein weiteres Unternehmen, Cambridge Analytica, behauptet zwischen drei und fünf Datenpunkte pro Person sowie psychologische Profile für 230 Millionen erwachsene Amerikaner zu besitzen.[23] Wir verschenken unsere Daten beim Einkaufen mit Clubkarten in Supermärkten, beim Surfen im Internet, bei der Teilnahme an „lustigen" Facebook-Persönlichkeitstests und bei hunderten anderer harmlos erscheinender Aktivitäten.[24,25] Die Verbreitung von Geräten des sogenannten Internets der Dinge (engl.: Internet of Things – IoT) – Smartwatches, Internet-Geräte und Sensoren für Einzelhandelsgeschäfte – zieht einen Anstieg der Menge an Daten nach sich, die über unser Leben erfasst werden. In der virtuellen Realität können wir unsere tatsächlichen Reaktionen auf hypothetische Impulse testen und unsere Reaktion auf Produkte und Ideen messen, die subtil im Hintergrund einer virtuellen Erfahrung eingebracht werden. Durch Datenpannen privater Unternehmen und Regierungen wurden extrem persönliche Informationen über uns und unsere Partner preisgegeben. Und immer öfter geben wir intimste Details über unser Leben freiwillig im Internet preis, wenn wir Fotos vom Familienurlaub teilen oder unsere Meinungen twittern.

Dank dieser Datenproliferation können alle möglichen Aspekte unseres Lebens, von unserer Persönlichkeit bis hin zu unserer politischen Einstellung, ermittelt werden. In einer Studie aus dem Jahr 2013 gelang es, die sexuelle Orientierung, die ethnische Zugehörigkeit, die religiösen und politischen Ansichten, Persönlichkeitsmerkmale, die Intelligenz, die Zufriedenheit, den Drogenkonsum, eine elterliche Trennung, das Alter und das Geschlecht eines Facebook-Benutzers allein aus dessen „Gefällt mir"-Angaben zu ermitteln. In einer ähnlichen Studie wurde festgestellt, dass Computer unsere Persönlichkeit besser bestimmen können als Kollegen, Bekannte, Familienmitglieder oder gar Lebensgefährten. Die Forscher stellten fest, dass viele Persönlichkeits- und Verhaltensaspekte präzise ohne menschliche Analyse, einfach nur durch die Verwendung von Daten vorhergesagt werden

20 Ryan Whitwam, „Google's DeepMind Develops Creepy, Ultra- Realistic Human Speech Synthesis", Geek.com, 09. September 2016, www.geek.com/tech/googles-deepmind-develops-creepy-ultra-realistic-human-speech-synthesis-1670362/. Ein Sprachumwandlungssystem auf Basis wahrscheinlichkeitstheoretischer Klassifikation und ein Harmonics-plus-Noise-Modell finden Sie auf IEEE, „IEEE Xplore", http://ieeexplore.ieee.org/document/674422.

21 Lyrebird, „Copy the Voice of Anyone", https://lyrebird.ai/demo.

22 Paul Boutin, „The Secretive World of Selling Data About You", Newsweek, 30. Mai 2016, http://www.newsweek.com/secretive-world-selling-data-about-you-464789.

23 McKenzie Funk, „The Secret Agenda of a Facebook Quiz", New York Times, 19. November 2016, https://www.nytimes.com/2016/11/20/opinion/the-secret-agenda-of-a-facebook-quiz.html; Tom Cheshire, „Behind the Scenes at Donald Trump's UK Digital War Room", Sky News, 22. Oktober 2016, http://news.sky.com/story/behind-the-scenes-at-donald-trumps-uk-digital-war-room-10626155.

24 Haben Sie schon einmal einen Persönlichkeitstest auf Facebook gemacht? Wenn ja, haben Sie wahrscheinlich einem Marketer Ihre Persönlichkeitsmerkmale, möglicherweise Ihr psychologisches Profil zusammen mit Ihrem Namen, Ihrer E-Mail-Adresse und der Liste Ihrer Facebook-Freunde offengelegt. Funk, „The Secret Agenda of a Facebook Quiz".

25 Lois Beckett, „Everything We Know About What Data Brokers Know About You", ProPublica, 13. Juni 2014, https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you.

können.

Die menschliche Wahrnehmung ist ein komplexes System, für dessen Dekodierung maschinelle Lernwerkzeuge ideal geeignet sind. Mit Zugriff auf umfassende Datenbanken voller Informationen über uns, lernen Maschinen unsere Persönlichkeit, unsere Wünsche und Bedürfnisse, sowie unseren Verdruss und unsere Ängste besser kennen als wir selbst. Maschinen werden lernen, wie Menschen, die unsere Charaktermerkmale teilen, beeinflusst werden können, aber sie werden uns auch persönlich und auf intimer Ebene kennenlernen. Die von MADCOMs erzeugten Inhalte sind keine Massenmedien; sie werden speziell auf das politische Rahmenwerk, die Weltansicht und die psychologischen Bedürfnisse und Verwundbarkeiten einer Einzelperson zugeschnitten.

Da KIs lernfähige Systeme sind, lernen sie mit jeder Erfahrung schnell dazu. Ein KI-System ist in der Lage, unter seinen tausenden von Propaganda-, Desinformations- und Einschüchterungsdaten eigenständig die wirksamsten heraussuchen, diese unterstreichen oder weiterentwickeln und gleichzeitig fehlgeschlagene Kampagnen schnell beenden. KI-Werkzeuge werden testweise Schwachstellen angreifen und lernen, welche Provokationen die gewünschte Reaktion hervorrufen, um Benutzer nach manipulativen Informationen süchtig zu machen. Wenn KI-Systeme mehrere Konten und Nachrichten prüfen, könnten sie lernen, dass ein bestimmter Journalist kaum auf persönliche Bedrohungen reagiert, dass aber eine Bedrohung seiner Angehörigen Angst hervorruft. Die MADCOMs könnten sich also als Mitglieder einer lokalen, gewalttätigen Gruppe ausgeben, die die Kinder von Journalisten bedrohen, bis diese die Berichterstattung einstellen. Und obgleich Journalisten nicht unbedingt von ein paar MADCOM-Trolls aus der Ruhe gebracht werden, so würde ein Ansturm von tausenden KI-gesteuerten Konten – von denen die meisten wie Mitglieder der eigenen Gemeinde aussehen und sprechen – doch selbst den Mutigsten Angst einjagen.

Was können Journalisten, Diplomaten, PR-Mitarbeiter, Politiker, Nachrichtensprecher und Regierungsbeamte tun, um mit MADCOMs zu konkurrieren,

Wir definieren dies als MADCOMs – die Integration von Systemen künstlicher Intelligenz in maschinengesteuerte Kommunikationswerkzeuge für den Einsatz in der computergestützten Propaganda.

die in der Lage sind, Berichte nahezu augenblicklich zu interpretieren, auf diese zu reagieren und individuell angepasste Kommunikation an Einzelpersonen oder Gruppen zu entsenden, bevor ein Mensch überhaupt einen ersten Entwurf begonnen hat?[26]

Die Antwort ist: **Menschen können allein nicht konkurrieren. In digitalen Netzwerken müssen sich Menschen mit KI-Maschinen zusammenschließen, um mit diesen konkurrieren zu können.** Der Aufstieg der MADCOMs wird einen Rüstungswettlauf um Informationen auslösen, in dem sich Einzelpersonen, Nichtregierungsorganisationen, Unternehmen und Regierungen alle darum bemühen, die Darstellung bestimmter Ereignissen zu beeinflussen. Die „Bösen“ und die „Guten“ kämpfen dabei jeweils mit ihren eigenen MADCOM-KIs. Beide Seiten verfügen über KI-Werkzeuge, um gegnerische MADCOM-Konten zu

26 Geschwindigkeit ist ein wesentlicher Faktor in einer Informationsumgebung, in der der Nachrichtenzyklus immer kürzer wird. Der erste in Umlauf gebrachte Bericht ist in der Regel der, an den sich die Menschen erinnern, und es stellt sich sehr schwierig dar, die Meinung von Menschen über Desinformation zu ändern, wenn sie dieser erst einmal ausgesetzt waren. Siehe US Department of State Advisory Commission on Public Diplomacy, „Can Public Diplomacy Survive the Internet?“

identifizieren. Solche Zuordnungswerkzeuge werden verwendet, um computergestützte Propagandakampagnen vorauszuahnen, auf laufende Operationen zu reagieren und menschliche Benutzer von Maschinen zu unterscheiden. In ähnlicher Weise wie beim Kampf um die Cyber-Sicherheit wird das Internet zum Schauplatz eines kontinuierlichen Bestrebens, den anderen immer eine Nasenlänge voraus zu sein: Technologen arbeiten an der Verbesserung von KI-Erkennungswerkzeugen während Propagandisten versuchen, MADCOMs dahingehend zu verbessern, dass sie von Menschen nicht mehr unterschieden und somit nicht detektiert werden können.

Das Ergebnis könnte eine antiutopische MADCOM-dominierte Zukunft sein. Die raffiniertesten Maschinenkonten werden von menschlichen Konten kaum mehr zu unterscheiden sein. Doch viele Propagandisten werden sich überhaupt nicht mit Detektionswerkzeugen abgeben, da die Grenzkosten für Spammaschinen und menschliche Sprachbeiträge und Inhalte sehr gering sind. In einer skurrilen und überraschenden Wendung werden Maschinen daher ihre Informationskampagnen häufig gegen andere Maschinen führen. Die angegriffenen maschinengesteuerten Konten werden mit ihrer eigenen Kommunikation reagieren, und der Informationsraum Internet wird überflutet von Maschinen, die mit Maschinen diskutieren. MADCOMs könnten so die von Menschen erzeugten Sprachbeiträge und die menschliche Kommunikation überrennen.

TEIL II: DIE ENTSTEHUNG VON MADCOMS

“Der Dritte Weltkrieg wird ein Guerilla-Informationskrieg sein, ohne Trennung zwischen Militärs und Zivilisten!”

—Marshall McLuhan

Aus der Ankunft der MADCOMs ergeben sich drei mögliche Szenarien für das kommende Jahrzehnt. Teil II dieser Abhandlung untersucht die Implikationen für Einzelpersonen, Organisationen (politische Parteien, Unternehmen, gemeinnützige Organisationen, karitative Einrichtungen und andere Nichtregierungsorganisationen) und Regierungen. Teil III enthält Empfehlungen für den Umgang seitens der Öffentlichkeit mit den Bedrohungen und Möglichkeiten, die von den MADCOMs ausgehen.

SZENARIEN FÜR DAS NÄCHSTE JAHRZEHNT [27]

Eine Welt im MADCOM-Wahn: Globaler Informationskrieg – MADCOMs beherrschen die Konversation im Internet und die Informationsumgebung wird zu einem Sumpf manipulativer, maschinengesteuerter Sprachbeiträge.

Über die Runden kommen: Maßnahmen und Gegenmaßnahmen – Gegenmaßnahmen gegen MADCOM treiben Propagandisten zur Entwicklung raffinierter Werkzeuge, und ein Rüstungswettrennen beginnt – ähnlich wie das, was wir heute im Bereich der Cybersicherheit sehen.

Lockdown: Der kognitive Sicherheitsstaat – Staaten erlassen strenge Einschränkungen für Informationen, richten Gegenpropaganda an ihre eigene Bevölkerung und kaufen Sicherheit zu einem hohen Preis.

27 Drei Joker-Variablen werden einen starken Einfluss auf diese Szenarien haben und es ist sinnvoll, diese zu beachten. Nämlich: die Geschwindigkeit der Entwicklung einer jeden MADCOM-Technologie; das Angriffs- und Verteidigungs-Gleichgewicht zwischen Detektionswerkzeugen und den Fähigkeiten von MADCOMs, Menschen nachzuahmen; und das Kosten- und Nutzen-Gleichgewicht zwischen der Umsetzung neuer MADCOM-Werkzeuge und der schlichten Verwendung bestehender, „dummer“ Bots und menschlicher Trolls

SZENARIO 1—EINE WELT IM MADCOM-WAHN: GLOBALER INFORMATIONSKRIEG

Im Verlaufe des nächsten Jahrzehnts wird eine Vielzahl von Akteuren hochgradig manipulative MADCOMs entwickeln und einsetzen, ohne dass deren Verwendung in bedeutendem Maße eingeschränkt wäre. Weil Unwissenheit und Besorgnis um die Einschränkung der Redefreiheit vorherrschen, reagieren Regierungen nur langsam auf diese Bedrohung. Staaten missbrauchen Darstellungen als Waffen und setzen MADCOMs ein, um den sozialen Unfrieden zu vertiefen, das Vertrauen in die Regierung zu untergraben und die Verlässlichkeit von traditionellem Journalismus zu eliminieren.[28] Clevere Diktatoren und autoritäre Regimes führen mit MADCOMs einen Informationskrieg, betreiben personenbezogene Propaganda gegen Individuen im Ausland und gegen ihre eigenen Bürger. Der von MADCOMs erzeuge Lärm übertönt die in der Informationssammlung und sozialen Netzwerk-Analyse verwendeten Signale. Doch MADCOMs, die sich als Menschen ausgeben, eröffnen neue Wege für Spionage und Diebstahl. MADCOMs werden verwendet, um gefälschte Ereignisse zu generieren und tatsächliche Ereignisse für einen bestimmten Vorteil subtil zu manipulieren. Die Realität wird flexibel.

Regierungen sehen sich kontinuierlich mit Skandalen konfrontiert, von denen viele mithilfe von MADCOMs frei erfunden oder manipuliert wurden. Regierungen zerfallen, nachdem Videos ihre Staatshäupter in gefälschten, verfänglichen Situationen zeigen. Heterogene Demokratien wie die Vereinigten Staaten verfallen in ständige Konflikte, während deren Gegner die Bevölkerung mit MADCOMs manipuliert, indem sie kulturelle Unterschiede verstärken und Darstellungen untergraben, die das Land einen könnten. Der soziale Konsens zerbricht und die politische Opposition wird als Verräter und Feind hingestellt. Ein führender autoritärer Kopf setzt MADCOMs ein, um die Bevölkerung zu manipulieren und die US-Präsidentschaft für sich zu gewinnen, während er verspricht, die „echten“ Amerikaner vor externen und internen Gefahren zu schützen und das Land wieder zu seiner rechtmäßigen Macht zu verhelfen. Das Vertrauen in die Regierung versagt und mit ihm das Verantwortungsbewusstsein. Der führende Kopf manipuliert das zerfallende Sozialgefüge, um die Macht in der Exekutive zu konsolidieren und eine dynastische politische Partei zu gründen, die von seinen Familienmitgliedern angeführt wird.

Während die letzte Supermacht unter endlosem, innenpolitischem Zank zerbricht und seine globale Vormachtstellung verliert; beschleunigt sich der ansonsten über Generationen verlaufende Niedergang der Staatsmacht exponentiell. Vernetzte Online-Organisationen, deren Zusammenhalt auf ideologischen und nicht auf geografischen Gemeinsamkeiten beruht, und die von MADCOM-gesteuerten Überredungskünsten angetrieben werden, werden die neuen globalen Machtzentren. KIs werden von großen Unternehmen eingesetzt, um noch mehr Einkommen von der Arbeit auf das Kapital zu verlagern. Die Einkommensungleichheit explodiert, erdrückt die globale Mittelklasse und untergräbt die Argumente für eine weltweite ökonomische und politische Befreiung. Technologie-Milliardäre, die raffinierte MADCOM-Technologien steuern, üben eine beispiellose Macht aus, mit der sie Darstellungen, politische Agenden und die öffentliche Meinung beeinflussen können.

Totalitäre Staaten wie der Iran und China bemühen sich, den internen Zusammenbruch mithilfe von MADCOMs abzuwenden und üben eine immer strengere staatliche Kontrolle über die Kommunikation im Internet aus. Im Iran werden interne Dissidentengruppen von MADCOMs bei der Zersplitterung der vielschichtigen Bevölkerung des Landes unterstützt. Ein Bürgerkrieg bricht aus. Die Kommunistische Partei Chinas setzt MADCOMs ein, um den Nationalismus zu festigen, doch dieser Schuss geht nach hinten los, als sich die Partei weigert, eine militärische Übernahme des westlichen

28 Als Waffe missbrauchte Darstellungen beschreiben Anstrengungen außerhalb traditioneller militärischer Einsätze – jedoch häufig als Ergänzung zu diesen –, mit denen eine gegnerische Zivilisation, Identität und Willenskraft untergraben werden soll, indem mit Informationen und Ideen Komplexität, Verwirrung und eine politische und soziale Spaltung geschaffen werden. So missbrauchte Darstellungen sind ein Merkmal geopolitischer Konflikte zwischen Staaten oder bedeutsamen nichtstaatlichen Akteuren. Häufig wird hierbei computergestützte Propaganda eingesetzt. Siehe die Weaponized Narrative Initiative der Arizona State University: “What is Weaponized Narrative?” https://weaponizednarrative.asu.edu.

Pazifiks zu unterstützen. Die aufgewiegelten Massen wenden sich gegen die Partei und China bemüht sich um eine interne Lösung zu den Massenprotesten sowie um die Verhinderung eines islamischen Aufstands, der von MADCOM-gesteuerter Rekrutierung vorangetriebenen wird. Russland hatte die Dynamik einer postfaktischen Gesellschaft bereits gemeistert und den Rest der Welt mit Unwahrheiten bombardiert und befindet sich nun wieder im Aufschwung. Seine einzige Opposition ist ein fragmentiertes Europa.

Mithilfe von MADCOMs bieten Unternehmen präzisionsgeführte, manipulative und auf Einzelpersonen zugeschnittene Werbung und untergraben das Ansehen ihrer Konkurrenten auf subtile Art und Weise. Politische Parteien und Interessengruppen setzen MADCOMs zur Verbreitung von Information und Desinformation ein und verbreiten manipulative Nachrichten unter der Öffentlichkeit, wobei die Inhalte jeweils direkt an das politische Rahmenwerk des Publikums angepasst sind. Wahlen werden häufig nur noch auf einer Grundlage gewonnen: wer verfügt über die beste MADCOM-Technologie?

Der sogenannte Islamische Staat (IS), der kein physisches Gebiet halten konnten, entwickelt sich zu einem virtuellen Kalifat. Mithilfe von KI-Chatbots verbreiten sie Hass, rekrutieren neue Extremisten und stiften diese zu eigenständiger Gewalt an. Das virtuelle Kalifat trifft auf offene Ohren unter den Massen der desillusionierten, unterbeschäftigen Jugendlichen der Welt, vor deren Augen etablierte Institutionen zerbrechen, und die im virtuellen Kalifat nach Sinn und Identität suchen. Einsame Wölfe – mithilfe von MADCOMs rekrutiert und manipuliert – werden zur Norm im Terrorismus, und das durch sie entstehende ständige Gefühl der Unsicherheit untergräbt das Vertrauen in die Regierungen noch weiter.

Die amerikanische Öffentlichkeit glaubt, dass MADCOM-Aktivitäten lediglich eine raffiniertere Form der Werbung sind, und verlässt sich reflexiv auf Appelle an die Redefreiheit. Tatsächlich handelt es sich um massive Manipulationskampagnen, die diese Darstellungen voranbringen, um die Öffentlichkeit zu überzeugen, dass keine Manipulation stattfindet. Wann immer Menschen mit einem elektronischen Gerät kommunizieren – sei es ein Smartphone, ein Augmented Reality-Gerät oder soziale Netzwerke – werden ihre Daten erfasst, ihr Verhalten getestet und aufgezeichnet und Algorithmen angepasst, um die Abhängigkeit von den Geräten noch weiter zu steigern, die Werbung noch überzeugender zu gestalten und die Propaganda noch manipulativer zu machen. Die politische Spaltung in den USA zwischen Demokraten und Republikanern explodiert in einen Informations-Bürgerkrieg, bei dem beide Seiten MADCOMs einsetzen, um weltanschauliche Missstände und ein allgegenwärtiges Gefühl der Schikane zu verschärfen. Sezessionsbewegungen arten teilweise in tatsächliche Gewalt aus.

Die Massen lenken sich von dieser beängstigenden Realität ab, indem sie in die trostspendenden Welten der KI-gestützten, personalisierten und hochgradig süchtig machenden Kommunikation eintauchen. Manche Menschen fliehen in private soziale Räume im Internet, was jedoch ihre Isolation verstärkt und die politische Polarisierung forciert. Eine kleine Anzahl von Menschen entflieht den sozialen Räumen im Internet komplett und beflügelt ein unbedeutendes Wiederaufleben von Offline-Massenmedien. Diese Personen mit ihrem eigenen Bewusstsein von der Informationswelt sind ohnehin am wenigsten anfällig für Desinformation und mit ihrer Abwesenheit gehen lediglich rationale Stimmen im Diskurs online verloren. Marken entstehen, die sich ganz speziell an Menschen richten, die ihre Daten und ihre Gedankenwelt schützen möchten, und die Wohlhabenden zahlen auf diese Weise für den Luxus der Privatsphäre. Doch niemand kann sich letztlich der MADCOM-regierten Zukunft entziehen, und die Folgen einer hemmungslosen Massenmanipulation werden die Informationsumgebung und selbst die bestbewachten kognitiven Gemeinschaften umgestalten.

Allgemein akzeptierte Tatsachen werden ein Relikt der Vergangenheit. Niemand weiß mehr, was wahr ist, da Sachverstand unter die Tyrannei der MADCOM-manipulierten öffentlichen Meinung gefallen ist. KI-Werkzeuge zur Video- und Sprachmanipulation erfinden und revidieren die Realität im Handumdrehen. Die einzige Wahrheit ist die, von der man andere Menschen überzeugen kann. Die neue Definition einer Tatsache ist „Information, die mit vorgefassten Meinungen übereinstimmen“

und jeder Gegenbeweis wird als vermutliche Desinformation abgetan. Die Story ist das einzige, was zählt. Die dreihundert Jahre alte Aufklärungszeit, die auf Vernunft und Wahrheitssuche aufbaut, geht zu Ende.

Die Welt zerfällt in künstlich geschaffene Komplexität und fabriziertes, vermeintliches Chaos und nur wenige verstehen, weshalb.

SZENARIO 2—ÜBER DIE RUNDEN KOMMEN: MASSNAHMEN UND GEGENMASSNAHMEN

Im Laufe des nächsten Jahrzehnts beginnen MADCOMs ungezügelt im Internet zu kursieren. Regierungen erzielen kleine Fortschritte bei der Ausarbeitung von Richtlinien, die sich auf den rapide wandelnden Markt für Informations- und Kommunikationstechnologie beziehen. Die Vereinigten Staaten schaffen einen Klagegrund für die Verbreitung offensichtlich falscher Informationen, doch Gerichte scheuen sich vor einer Rolle als Schiedsrichter der Wahrheit und das Gesetz ist nur schwer durchsetzbar. Technologieunternehmen springen ein – teilweise aus einem Gefühl der Bürgerpflicht, doch in erster Linie, weil sie sich vor Regierungsregulierung fürchten. Soziale Medienunternehmen führen leistungsfähige MADCOM-Detektions- und Filtertools ein und Bot-Netzwerke der computergestützten Propaganda werden dichtgemacht. Browser-Unternehmen führen KI-Werkzeuge zur Detektion von maschinengesteuerten Benutzerkonten und zur Markierung fraglicher Informationen ein. Die Technologiebranche bildet Selbstkontrollgremien, um einerseits Normen für Identität, Bot-Aktivität und Inhalte zu schaffen und durchzusetzen und andererseits kleinere Unternehmen bei der Durchsetzung dieser Vorgaben zu unterstützen. Neuartige Mediengeschäftsmodelle mindern die Rentabilität viraler Webseiten und Clickbaiting-Seiten. Soziale Medienunternehmen gründen eine Art Stiftung Wahrentest für Nachrichten und Informationen, die zum Goldstandard journalistischer Integrität wird.

Propagandisten reagieren mit ihren eigenen Innovationen. Maschinengesteuerte Konten ändern ihr Aktivitätsmuster, um menschliches Verhalten und menschliche Kommunikationsstile besser nachahmen zu können. Technologieunternehmen entwickeln bessere Detektionswerkzeuge, mit denen MADCOMs erkannt werden können, und ein Rüstungswettlauf beginnt. Ähnlich wie bei der Herausforderung im Bereich Cyber-Sicherheit kommt es auch hier zu einem zyklischen und kontinuierlichen Bestreben, den anderen immer eine Nasenlänge voraus zu sein. Dabei sind MADCOM-Propagandisten immer einen Schritt voraus. Rechts- und linksextreme Gruppen behaupten, dass KI-Filterwerkzeuge gegen ihre Perspektive (die jeweils auf Desinformation und Halbwahrheiten aufgebaut ist) voreingenommen sind. Sie erstellen ihre eigenen „fairen und ausgewogenen“ Filterwerkzeuge, die ihre jeweiligen parteistrategischen Positionen stark bevorzugen. Enttäuscht von den hemmungslosen Zensurmaßnahmen der Unternehmen entstehen neue, alternative soziale Medienunternehmen, die die Inhaltskontrolle und das Filtern ausdrücklich verbieten. Diese neuen Unternehmen werden zu Virusvektoren für MADCOM-gesteuerte Verschwörungstheorien, Hassreden und Desinformation.

Westliche Demokratien schaffen es, mit einigen Instrumenten der nationalen Macht auf Gegner einzuwirken. Die Vereinigten Staaten und Europa verhängen Sanktionen gegen böswillige Länder und Organisationen, die mithilfe von MADCOMs Storys zu Waffen machen, und unterbinden so verschiedene Handlungen. Außerdem schaffen sie Voraussetzungen für die strafrechtliche Verantwortlichkeit ausländischer Anbieter von Falschinformationen, mit denen einzelne Propagandisten belangt werden. Staaten haben Schwierigkeiten, sich auf Standards für die Informationssicherheit zu Friedenszeiten zu einigen, und die Durchsetzung dieser Standards ist ungleichmäßig und nicht durchsetzbar, da die Zuordnungswerkzeuge und die Methoden zu schwach ausgelegt sind.

MADCOMs untergraben die Demokratie, aber sie sind ein Schlaraffenland für den Kapitalismus. Unternehmen ernten weiter Kundendaten und nutzen diese für das subtile, manipulative Marketing. Eine blühende Industrie entwickelt sich für Datenschutzanwendungen, die das Benutzerverhalten im Internet verschleiern. Die meisten Menschen geben jedoch weiterhin gerne ihre personenbezogenen Daten im

Austausch gegen „kostenlose“ Dienstleistungen von Technologieunternehmen preis und werden so einer immer heimtückischeren MADCOM-gesteuerten Manipulation ausgesetzt. China verschenkt IoT-Geräte, denn die massiven Datenmengen, die sie so ernten, sind für die Kommunistische Partei Chinas – und für Unternehmen – weitaus wertvoller als die Herstellungskosten der Geräte. Die Partei nutzt diese Daten für alle möglichen Zwecke, von manipulativem Marketing bis zur Beeinflussung ausländischer öffentlicher Darstellungen, die chinesische Ziele fördern. Die Erosion der Wahrheit verläuft nicht so schnell wie in Szenario 1: Eine Welt im MADCOM-Wahn, doch es ist eine Welt, in der Verschwörungen im Überfluss vorhanden sind, das Vertrauen in Einrichtungen in den Keller sinkt, der Sachverstand entwertet und die Realität – obgleich nicht vollständig flexibel – doch biegbar wird.

SZENARIO 3—LOCKDOWN: DER KOGNITIVE SICHERHEITSSTAAT

Als Reaktion auf die Gefahren, die von MADCOMs, von computergestützter Propaganda, von als Waffen benutzen Darstellungen und von anderer schamloser Desinformation ausgehen, verhängen im Verlaufe der nächsten zehn Jahre viele Nationen strenge Rechtsvorschriften für Kommunikation und Information im Internet. Die globale Gemeinschaft erstellt ein neues Internet 2.0 mit viel schärferen Sicherheitsprotokollen, einschließlich der Voraussetzung von verifizierten, vom Staat ausgestellten Identitäten für den Internetzugriff. Nicht zugeordnete MADCOM-Aktivitäten sind gesetzlich verboten und zugeordnete MADCOMs sind streng reguliert. Das Internet 1.0 existiert noch, gilt aber generell als ein ungesicherter Wilder Westen – voll Malware, Desinformation und Räuber.

Die internationale Gemeinschaft unterzeichnet ein Abkommen zur Informationssicherheit, das sowohl die technischen Aspekte der Cyber-Sicherheit als auch die kognitiven Aspekte der Informationssicherheit abdeckt. Dieses Abkommen – zusammen mit der Voraussetzung einer verifizierten Identität für das Internet 2.0 – wird als massiver Verlust der globalen Internetfreiheit angesehen. China feiert das Internet 2.0 und trennt den Zugang zum analytischen Internet 1.0 für seine Bürger komplett ab. Ähnlich gehen auch andere autoritäre und totalitäre Regimes vor. China setzt MADCOMs in Verbindung mit anderen neuen Manipulationswerkzeugen wie sozialen Kreditscoring ein, um so auf subtile Art eine glückliche und gehorsame Bevölkerung zu schaffen.[29]

Regierungen in Europa und in den Vereinigten Staaten entwickeln Zentren für Konter-Nachrichten, mit denen Bevölkerungen gegen Desinformation geimpft und besonders schädliche Desinformationskampagnen entkräftet werden sollen. „Unabhängige“ Medien, Organisationen im Bereich der Qualitätskontrolle von Daten und Nichtregierungsorganisationen, die sich auf den Kampf gegen Falschinformationen konzentrieren, werden stark subventioniert. Viele Demokratien setzen MADCOMs ein, um Darstellungen auf subtile Art zu lenken und positive und verbindende Themen unter ihrer Bevölkerung zu fördern. Als Revanche für einen jahrelangen Informationskrieg verwenden die Vereinigten Staaten MADCOMs, um computergestützte Propagandakampagnen zu führen, die Russland von innen her zerstören.

Zudem schaffen demokratische Regierungen rechtliche Klagegründe für die vorsätzliche Verteilung von bekanntermaßen falschen Informationen. Satire und „Fake News“-Entertainment müssen deutlich gekennzeichnet sein, damit sie leicht von Journalismus unterschieden werden können. Gesetze gegen Verleumdung und üble Nachrede werden verschärft und Internetplattformen werden für sämtliche von ihren Benutzern eingestellten Inhalte verantwortlich gemacht. Webseiten,

29 China hat vor, soziale Kreditsysteme bis zum Jahr 2020 zur Pflicht zu machen. Bürger werden so auf Basis ihrer Loyalität zur chinesischen Regierung und zu chinesischen Marken eingestuft und
Personen mit guten Noten werden bei der Vergabe von Jobs, Bildungschancen und Regierungsdiensten bevorzugt behandelt. Noten werden vom sozialen Netzwerk einer Person beeinflusst, was einen Anreiz für Bürger schafft, ihre Bekannten, Familienangehörigen und Kollegen mit schlechten Noten unter Druck zu setzen oder auszugrenzen. Josh Chin und Gillian Wong, „China’s New Tool for Social Control: A Credit Rating for Everything“, Wall Street Journal, 28. November 2016, https://www.wsj.com/articles/chinas-new-tool-for-social-control-a-credit- rating-for-everything-1480351590.

die Desinformation fördern, werden verboten und gesperrt. Online-Informationsträger, die sich in ausländischem Eigentum befinden oder vom Ausland aus betrieben werden, sind streng reguliert. Die Gesetzgebung lässt keinen Zweifel daran, dass Maschinen und ausländische Mitredner nicht dieselben Rechte der freien Meinungsäußerung zugestanden bekommen wie Staatsangehörige. Psychologische Experimente, mit denen die Attraktivität einer Technologie gefördert werden soll, sind entweder verboten oder streng reguliert.

Die Vereinigten Staaten treten in die Fußstapfen Europas, verhängen strenge Einschränkungen für Datenübertragungen an Drittparteien und stellen Anforderungen an eine klare Darstellung der Datennutzung in den allgemeinen Geschäftsbedingungen, um so die Erfassung von Daten, die für manipulative Zwecke verwendet werden könnten, einzugrenzen. Unternehmen rebellieren und die Gesetzgebung droht zu scheitern, doch der öffentliche Druck auf die Unternehmen und die Gefahr von noch schärferen Regierungshandlungen sind zu stark, und sie geben nach. Eine öffentlich-private Partnerschaft entwickelt Richtlinien zur Regulierung von MADCOMs und erstellt quelloffene Protokolle für die Verwaltung personenbezogener Daten sowie zeitlich befristete Datennutzungsberechtigungen. Dennoch setzen sich Unternehmen stetig für eine Lockerung der Einschränkungen zu „modernen Marketing-und Werbetechnologien“ ein und setzen Politiker unter Druck.

Der politische Wandel verlangsamt sich, während Amtsinhaber ihre kognitiven Sicherheitsfähigkeiten nutzen, um ihre politischen Positionen zu festigen. Viele MADCOM-Werkzeuge dürfen bei politischen Kampagnen nicht für das Messaging verwendet werden, und Mitteilungen von Kandidaten, Parteien oder Political Action Committees (PACs) müssen eindeutige Quellenangaben aufweisen. Kognitive Sicherheit und kognitive Manipulationsfähigkeiten sind dem Staat vorbehalten.

Diese Methoden zur Bekämpfung von MADCOMs fördert erfolgreich die Stabilität in Europa, wo Bevölkerungen homogener sind, doch Amerikaner wehren sich gegen die Einmischung und gegen Zensurmaßnahmen der Regierung. In den Vereinigten Staaten werden viele Informationseinschränkungen vom Justizwesen gesperrt oder aufgehoben, was einen internen Konflikt anschürt. In einigen Nationen nutzen populistische Machthaber staatliche MADCOM-Desinformationsbekämpfungswerkzeuge, um ihre eigenen Parteien zu stützen und abweichende Meinungen zu diskreditieren.

Viele Menschen akzeptieren den kognitiven Sicherheitsstandard als ein notwendiges Übel, doch eine laute Minderheit wehrt sich gegen das, was sie als einen Machtmissbrauch seitens der Regierung ansieht. Auf die gleiche Weise wie die Wohlhabenden heutzutage Offshore-Steueroasen ausnutzen, verlagern politische Dissidenten und zwielichtige Gruppen ihren Messaging-Betrieb in ausländische Informationsoasen – wo sie, dank lockerer Regierungsgewalt, Korruption oder Gleichgültigkeit, gefälschte Online-Ausweise erstellen, um MADCOMs im verifizierten Internet 2.0 zu betreiben. Dies führt zu einer weiteren Balkanisierung des Internets, da diesen „Informations-Schurkenstaaten“ der Zugang zum Internet 2.0 verweigert wird.

Die Realität wird widerstandsfähiger, doch sie wird auch von nicht gewählten Bürokraten bestimmt, die diese Werkzeuge subtil einsetzen, um die innenpolitische Ordnung und die Weltordnung aufrechtzuerhalten. So wird die Stabilität und Relevanz des Staates gewahrt, doch alles hängt vom Wohlwollen der Politiker ab, die letztlich bestimmen, inwiefern sie die Realität für ihren politischen Nutzen beeinflussen möchten. Wegen eines Missbrauchs dieser Macht wehren sich zivile Freidenker und rechtsradikale Regierungsgegner gegen die Einschränkung der Meinungsfreiheit, wodurch eine neue und möglicherweise gefährliche Quelle für innenpolitischen Dissens entsteht.

TEIL III: IST DAS INFORMATIONSNIRVANA ERREICHBAR?

Eines Tages könnten empfindungsfähige KIs die Menschheit zu einer Zivilisation verhelfen, in der kein Mangel mehr herrscht – sofern wir die MADCOM-Jahre überstehen.

Selbst im besten Fall wird die KI-Technologie die Zukunft der menschlichen Zivilisation tiefgreifend mitgestalten. KI-Werkzeuge werden unsere Kultur beeinflussen, Entscheidungen für uns treffen und als loyale maschinelle Begleiter und Assistenten dienen. Eines Tages könnten empfindungsfähige KIs die Menschheit zu einer Zivilisation verhelfen, in der kein Mangel herrscht – sofern wir die MADCOM-Jahre überstehen.

Wie finden wir den Weg zu dieser idealen Zukunft, in der MADCOMs für den Nutzen der Menschheit und nicht zu deren Schaden eingesetzt werden?

POLITIKEMPFEHLUNGEN FÜR DIE USA

Als erstes muss die Gemeinschaft der Demokratien die Ernsthaftigkeit der von MADCOMs, von computergestützter Propaganda und von als Waffen missbrauchten Darstellungen ausgehenden Bedrohungen erkennen und diese aggressiv an mehreren Fronten angehen. Im Folgenden werden Empfehlungen für die Vereinigten Staaten dargelegt, doch diese Konzepte können im Großen und Ganzen auch auf die Gemeinschaft der Demokratien weltweit angewandt werden.

Der Kongress der Vereinigten Staaten:

- Der Kongress muss das Department of Homeland Security (DHS) zum Schutz der US-Bevölkerung vor den schädlichen Auswirkungen, die von computergestützter Propaganda und von als Waffe missbrauchten Storys ausgehen, ermächtigen. Die Finanzierung und Ausführung sollte unter dem National Protection and Programs Directorate erfolgen, um eine Koordination mit dem DHS Office of Cybersecurity and Communications zu ermöglichen und die Modelle für eine

Cyber-Sicherheitsvorwarnung und -warnung sowie für die Vorfallsverwaltung, soweit möglich und angemessen, wiederverwerten zu können.

- Zudem muss der Kongress die Exekutive anweisen, eine umfangreiche Informationssicherheitsstrategie zu entwickeln, um die Bevölkerung vor Internetpropaganda und Desinformation zu schützen und gleichzeitig die zentralen demokratischen Werte von Gleichheit und Freiheit aufrechtzuerhalten. In der Strategie sollten Ziele und Methoden beschrieben werden, die für einen zuverlässigen Schutz der amerikanischen Öffentlichkeit gegen die computergestützte Propaganda sorgen, auf bestimmte Propagandakampagnen reagieren und ausländische Gegner abschrecken – während die amerikanischen Werte eingehalten werden und die höchste Integrität gewahrt bleibt.

- Der Kongress sollte seine Position zum Countering Foreign Propaganda and Disinformation Act in seiner ursprünglichen, von den Senatoren Rob Portman und Chris Murphy eingereichten Version noch einmal überdenken und diesen verabschieden. Die US-Regierung benötigt ein unabhängiges Zentrum für Informationsanalyse und Reaktionsplanung (Center for Information Analysis and Response), welches den Informationsaustausch unter Regierungsagenturen zu Anstrengungen ausländischer Regierungen im Informationskrieg koordiniert; Informationen über ausländische Propaganda- und Desinformationsanstrengungen in nationale Strategien integriert; und agenturübergreifende Aktivitäten entwickelt und synchronisiert, mit denen ausländische Operationen im Informationsbereich, die gegen die nationalen Sicherheitsinteressen der Vereinigten Staaten gerichtet sind, entlarvt und bekämpft werden, und Darstellungen gefördert werden, die amerikanische Verbündete und amerikanische Interessen unterstützen. Eine zurechtgestutzte Version dieser Rolle wurde mit dem National Defense Authorization Act (NDAA) von 2016 dem Global Engagement Center zugesprochen, jedoch ohne Finanzierung, Mandat oder Unabhängigkeit in adäquatem Maße.

- Der Kongress muss ein umfangreiches Datenschutzgesetz erlassen, das Amerikanern die Kontrolle über ihre personenbezogenen Daten überträgt, ohne den Handel dadurch zu belasten. Dies erfordert einen erheblichen Forschungsaufwand und einige neue Technologien. Deshalb sollte der Kongress zunächst eine Nationale Kommission für Datenschutz, Informationssicherheit und Desinformation (National Commission on Data Privacy, Information Security, and Disinformation) ins Leben rufen, um zu ermitteln, welche Technologien, Werkzeuge und Gesetze für den Schutz der amerikanischen Bevölkerung im Informationszeitalter nötig sind. Diese Kommission muss sich auch mit der Frage beschäftigen, welche neuen Regeln – wie die zum Verbot täuschender Werbung – gebraucht werden. Dabei geht es um alle möglichen Themen, von vorsätzlich gefälschten Nachrichtenartikeln über modifizierte Video- und Audioaufzeichnungen bis hin zu maschinengesteuerter Desinformation. Maschinen haben kein Recht auf Meinungsfreiheit, ebenso wenig wie ausländische Staatsangehörige, die Propaganda vom Ausland aus ins Internet stellen. Solche Akteure müssen eingeschränkt werden, ohne die Offenheit und Anonymität des Internets zu gefährden.

- Der Kongress muss unverzüglich den Privacy Act anpassen, um Regierungsagenturen die Durchführung analytischer Analysen im Internet zu gestatten. Derzeitige Beschränkungen hindern nationale Sicherheitseinheiten daran, ausländische computergestützte Propaganda effektiv zu erkennen, zu verfolgen, zu analysieren und zu bekämpfen.

Das Department of Homeland Security

- Das Department of Homeland Security muss seinen Fokus über die rein technische Verteidigung hinaus erweitern und Elemente der kognitiven Sicherheit in seine Cyber-Sicherheitsstrategien und -fähigkeiten integrieren. Traditionelle Hacks werden immer häufiger nicht für Profit oder Spionagezwecke durchgeführt, sondern

um eine psychologische Wirkung zu erzielen.[30] Dies muss in einer nationalen Cyber-Sicherheitsstrategie berücksichtigt werden.

- Homeland Security sollte untersuchen, wie das von dem National Cybersecurity and Communication Integration Center (NCCIC) und US-CERT angeführte System zur Verfolgung von Cybersicherheitsbedrohungen, Informationsaustausch und Vorfallsreaktion für die Bekämpfung ausländischer computergestützter Propaganda und MADCOMs adaptiert und repliziert werden könnte.

- Außerdem sollte Homeland Security Forschungen fördern, in denen untersucht wird, wie Gruppen und Einzelpersonen im Internet beeinflusst werden. In diesen Forschungsstudien muss die Verbreitung von Memen und Desinformationen nachverfolgt werden, damit ein Verständnis dafür entwickelt werden kann, welche Ideen zur Meinungsbildung und zur Manipulation von Bevölkerungen verwendet werden. Auch sollten quantitative Studien erstellt werden, um die beste Verteidigung gegen diese Propagandatechniken zu ermitteln.

- Homeland Security muss sich auch mit der Wissenschaft und dem privaten Sektor zusammenschließen, um Bürger über den umsichtigen Konsum von Informationen aufzuklären. Desinformation und schädliche Meme funktionieren wie Viren, und derartige Anstrengungen könnten die Immunität der Bevölkerung gegen Desinformation erhöhen.

Das Außenministerium

- Das amerikanische Außenministerium sollte sich mit dem unlängst veröffentlichten Bericht der Advisory Commission on Public Diplomacy (ACPD), „Can Public Diplomacy Survive the Internet?“, auseinandersetzen und die dort enthaltenen Empfehlungen in eine umfassende computergesteuerte Einsatzstrategie (Computational Engagement Strategy) aufnehmen. Diese Strategie sollte Ziele und Methoden zur Bekämpfung ausländischer computergestützter Propaganda beschreiben und sicherstellen, dass das Außenministerium die neuen MADCOM-Werkzeuge für zugeordnete öffentliche diplomatische Bemühungen und Einsätze effektiv nutzt.

- Das Außenministerium sollte die bösartige, staatlich geförderte Nutzung von MADCOMs mithilfe von Sanktionen, diplomatischem Druck und der Entwicklung von Systemen zum Informationsaustausch und zur Vorfallsreaktion mit Verbündeten unterbinden.

- Das Außenministerium sollte die Ausarbeitung internationaler Standards oder Gesetze in Erwägung ziehen, die bösartige MADCOMs verbieten. Dies ist jedoch ein langwieriger Prozess, der viele Risiken in sich birgt. Russland und China würden versuchen, sich eine solche Anstrengung zu eigen zu machen und stattdessen eine internationale Informationssicherheit Agenda vorantreiben, die die Freiheit im Internet einschränkt.

- Und schließlich sollte das Außenministerium mit dem privaten Sektor und der Wissenschaft zusammenarbeiten, um zu ermitteln, ob bestimmte KI-Werkzeuge als doppelverwendungsfähige (Dual-Use) Technologie eingestuft werden sollten, die der Ausfuhrkontrolle im Rahmen des Wassenaar-Abkommen unterliegen.[31]

Das amerikanische Verteidigungsministerium und die US Nachrichtendienste

- Die US Nachrichtendienste und das Verteidigungsministerium sollten nicht zugeordnete MADCOM-Fähigkeiten als Option zur Abschreckung entwickeln. Wenn diplomatischer Druck, Sanktionen und andere Maßnahmen eine gegnerische Aktivität nicht unterbinden können,

30 Zum Beispiel: der 2013 ausgeführte Hack auf einen Twitter-Account der Associated Press, der die Aktienmärkte innerhalb von Minuten um mehr als 100 Milliarden USD brachte; der Hack der Server des Democratic National Committee; die Linux/Moose-Malware, die Anmeldedaten für soziale Netzwerke stiehlt, um „Gefällt mir“-Angaben und Follower zu fälschen.

31 Staaten, die das Wassenaar-Abkommen unterzeichnet haben, stimmen zu, die Exportkontrollen zu doppelverwendungsfähigen Gütern und Technologien durchzuführen und Transparenz und Verantwortlichkeit zu fördern, um ein destabilisierende Anhäufungen solcher Güter und Technologien zu vermeiden.

müssen die Nachrichtendienste und das Verteidigungsministerium ihre eigenen MADCOM- Fähigkeiten einsetzen, um ihren Gegnern Schaden zuzufügen und diese zu zwingen, im Gegenzug ihre Ressourcen im Bereich der computergestützten Propaganda gegen die USA einzusetzen. Für diese Fähigkeiten sollte keine Desinformation nötig sein – es gibt ausreichend diffamierende Fakten über solche Gegner, die ausgenutzt werden können, ohne eine Bewegung in Richtung postfaktischer Welt voranzutreiben. Desinformation sollte zu Friedenszeiten nur unter extremen Umständen oder während bewaffneter Konflikte oder in der Terrorismusbekämpfung eingesetzt werden.

- Das Verteidigungsministerium muss seine Definition von Krieg als das Töten von Menschen und das Zerstören von Objekten auf die Definition laut Clausewitz anpassen, der schrieb, dass es im Krieg darum ginge, den Gegner zur Erfüllung unseres Willens zu zwingen. Im Vergleich zu den großen Waffenplattformen haben Operationen im Informationsbereich eine sehr niedrige Priorität in der Doktrin und den Ressourcenanfragen des Verteidigungsministeriums. Operationen im Informationsbereich sind im Einsatz kinetischer Maßnahmen bei der Erfüllung einer Mission durchaus überlegen, und die beiden Methoden sollten sich wo notwendig gegenseitig ergänzen.

Behörden und Organisationen: Bund, Land, Kommune

- Die Zuordnung computergestützter Propagandanetzwerke und das Vermögen, Desinformation und Manipulationskampagnen ausländischer Gegner zu identifizieren, sind zentrale Fähigkeiten, die in der gesamten Regierung – im Verteidigungsministerium, im Außenministerium, im Department of Homeland Security, beim FBI, bei den Nachrichtendiensten und wenn möglich auf Landes- und Kommunalebene – entwickelt werden sollten.

- Keine dieser Empfehlungen besagt, dass sich eine föderale, bundesstaatliche oder kommunale Behörde an Konter-Nachrichten gegen die eigene Bevölkerung beteiligen sollte. Innerstaatliche Operationen im Informationsbereich sind voller Gefahren und sollten vermieden werden. Behörden und Organisationen können Studien durchführen und finanzieren, um ein Verständnis dafür zu entwickeln, wie Menschen sich im Internet beeinflussen lassen und wie technologische Werkzeuge zur Verbreitung von Desinformation verwendet werden. Sie können solche Studien verwenden, um effektive öffentliche Bildungsprogramme zu erstellen, und Amerikanern dazu zu verhelfen, klügere Konsumenten von Informationen zu werden. Sie können faktische Korrekturen ausländischer Desinformation bereitstellen. Behörden und Organisationen können Informationen zu MADCOM-Aktivitäten sammeln und mit Verbündeten und dem privaten Sektor teilen, um diese Informationskampagnen besser verstehen und bekämpfen zu können. Außerdem können sie mit dem privaten Sektor zusammenarbeiten, um sicherzustellen, dass die Öffentlichkeit Zugang zu Werkzeugen hat, mit denen Einzelpersonen eigenständig Wahrheit von Lüge unterscheiden können.

- Werkzeuge der künstlichen Intelligenz haben ein enormes Potenzial für die Verbesserung von Regierungsdienstleistungen, und diese Abhandlung soll in keiner Weise von der Entwicklung nicht-manipulativer MADCOM-Werkzeuge zur Verbesserung von Bürgerinformation und bürgerschaftlichem Engagement abhalten. Insbesondere Chatbots bieten attraktive Lösungen für Anwendungen, von der Erweiterung von Kundenkontaktzentren bis hin zu autonomen Therapeuten für Menschen mit Depressionen.[32,33]

32 US Citizenship and Immigration Services, „Meet Emma, Our Virtual Assistant“, https://www.uscis.gov/emma.

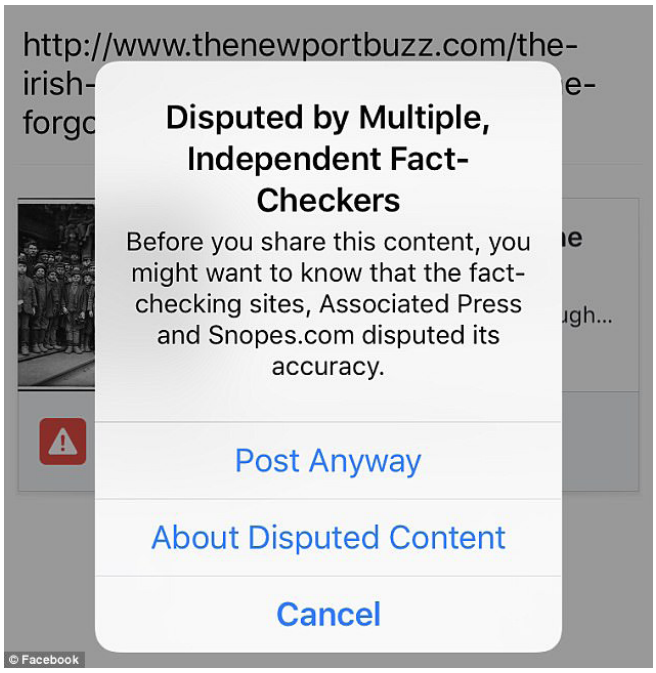
33 Megan Molteni, „The Chatbot Therapist Will See You Now“, Wired, 07, Juni 2017, https://www.wired.com/2017/06/facebook-messenger-woebot-chatbot-therapist/.

Die Technologiebranche

- Technologen müssen Werkzeuge zur Identifizierung von MADCOMs entwickeln, damit Benutzer fundierte Entscheidungen über die Quelle einer Information treffen können. In einer Welt, in der Werkzeuge zur Manipulation der Realität entwickelt werden können, können auch Werkzeuge entwickelt werden, die bestätigen, dass eine objektive Wahrheit existiert. Wir brauchen raffinierte digitale Forensikwerkzeuge, damit Bürger und Regierungsbeauftragte feststellen können ob eine suspekte Audio- oder Videoaufzeichnung digital modifiziert wurde.

- Technologische Organisationen sollten sich mit dem schwierigen Problem beschäftigen, wie Anreize für die Wahrheit und Sanktionen für Unwahrheiten geschaffen werden können. Eine Anzahl von Organisation arbeitet an derartigen Initiativen, beispielsweise: Werkzeuge der kollektiven Intelligenz zur Identifizierung von Fake News-Artikeln und Websites; Mechanismen, um Benutzern mitzuteilen, wie verlässlich eine Nachricht ist und wie viel Arbeit jeweils in die Erstellung eines Artikels eingeflossen ist; Selbsthilfegruppen für Trolling-Opfer; autonome KI-Systeme für das Fact-Checking; und Werkzeuge für das automatische Blockieren von unwahren Artikeln, Trollen, Bots und Hassreden.[34] Es kann sein, dass jeder Mensch einen eigenen KI-Bodyguard benötigt, der ihn über die Zuverlässigkeit von Inhalten und Quellen informiert.

- Webbrowser und Plattform sollten diese Werkzeuge standardmäßig integrieren und nicht nur als Plug-Ins anbieten, die zusätzlich Arbeit machen. Spam wird automatisch ausgefiltert. Browser warnen uns, wenn wir versuchen Websites mit Malware zu öffnen. Unsere Werkzeuge sollten uns vor bekannter Desinformation schützen und nicht nur blind deren Konsum ermöglichen.



Im März 2017 führte Facebook als Teil einer Kampagne gegen die Verbreitung sogenannter Fake News auf der Plattform ein externes Fact-Checking-Werkzeug ein.

- Technologieunternehmen sollten Forschungen zu quelloffenen Werkzeugen finanzieren, mit denen Informationen über MADCOMs, bösartige Akteure und Desinformationskampagnen ausgetauscht werden können. Einige Experten haben eine Art Stiftung Warentest für Information vorgeschlagen, die als unabhängiger Prüfer für die Zuverlässigkeit von Informationen und Quellen dienen würde.

- Technologieunternehmen haben eine Verantwortung, diese Werte, die inhärent zu ihren Innovationen und Geschäften gehören, zu berücksichtigen. Werbefinanzierte Geschäftsmodelle haben den traditionellen Journalismus zerstört. Modelle des viralen Wachstums in sozialen Netzwerken fördern die rapide Verbreitung von Propaganda und tragen zum Anstieg von Desinformation und Effekthascherei bei.[35] Innovatoren müssen hier nach neuen Wegen suchen.

34 Das Stilllegen von Bot-Netzwerken kann nach hinten losgehen. Bot-Aktivität in den sozialen Medien kann leicht verschleiert werden, womit eine wertvolle Informationsquelle über gegnerische Informationskampagne ausgeschaltet würde.

35 Sean Blanda, „Medium, and The Reason You Can't Stand the News Anymore", Medium, 15. Januar 2017, https://medium.com/@SeanBlanda/medium-and-the-reason-you-cant-stand-the-news-anymore-c98068fec3f8.

- Soziale Netzwerkunternehmen können und sollten gemeinsame Grundsätze und Normen ausarbeiten, die ihr Verhalten bestimmen. Wohlhabendere Unternehmen können außerdem eine Industrieorganisation subventionieren, die kleinere und neue Unternehmen dabei unterstützt, alles, von MADCOM-Desinformation bis hin zu extremistischen Inhalten, zu kontrollieren.

- Eine Lösung könnte darin bestehen, auf sozialen Netzwerkplattformen zu verlangen, dass die online-Identitäten verifiziert sind. Dies kann jedoch auch Besorgnis über die Internetfreiheit und die schützende Anonymität für Whistleblower und Aktivisten hervorrufen. Autoritäre Regimes treiben Desinformation unter Umständen genau deshalb voran, weil die reflexive Antwort die Forderung einer strengeren Prüfung der Identität ist.

Wissenschaft

- Das Engagement der Wissenschaft ist im Bereich der Detektion und Zuordnung ganz besonders wichtig. Bis die Einschränkungen des Privacy Act aufgehoben sind, können Regierungsbehörden nur begrenzt Online-Analysen durchführen. Ein Hochschulkonsortium zur Verfolgung und zum Austausch von Informationen über computergestützte Propaganda wäre deshalb äußerst hilfreich.

- Die Entwicklung von Verfahren zur Nachverfolgung von MADCOMs, zur Zuordnung, zum Informationsaustausch und zur Vorfallsreaktion muss von Hochschulen und Universitäten angeführt werden. Die Wissenschaft spielte in der Ausarbeitung der Best Practices hinsichtlich der Cyber-Sicherheit eine instrumentale Rolle und sollte dies auch im Bereich der kognitiven Sicherheit tun. Das CERT-Modell, das global für die Nachverfolgung von Cyber-Sicherheitsrisiken, den Informationsaustausch und die Vorfallsreaktion verwendet wird, wurde an der Carnegie Mellon University entwickelt. Hochschulen und Universitäten sollten sich auf die Entwicklung ähnlicher Modelle für den Umgang mit Bedrohungen der kognitiven Sicherheit durch computergestützte Propaganda konzentrieren.

Jeder von uns hat die Verpflichtung, sich über die Konsequenzen neuer Technologien wie MADCOMs zu informieren und die Verantwortung für seine Zukunft zu übernehmen.

Einzelpersonen und Gesellschaft

- Jeder von uns hat die Verpflichtung, sich über die Konsequenzen neuer Technologien wie MADCOMs zu informieren und die Verantwortung für seine Zukunft zu übernehmen. Bürger müssen effektive Lösungen von ihren Politikern und sozialen Netzwerkunternehmen einfordern. Ein Element ist der Einsatz für einen sehr viel strengeren Datenschutz. In den Vereinigten Staaten werden strenge und umfassende Datenschutzgesetze benötigt, die einzelnen Bürgern die Kontrolle über ihre Daten überlassen und sie darüber aufklären, wer ihre Daten benutzt. Gleichzeitig dürfen solche Gesetze jedoch nur geringe bürokratische Anforderungen an Unternehmen stellen. Quelloffene Programme für die Verwaltung von Datennutzungsberechtigungen könnten hier eine Lösung darstellen, und die Regierungen sollten bei der Ausarbeitung dieser Normen die Führungsrolle übernehmen.

- Kollektive Intelligenzsysteme, bei denen eine große Anzahl von verifizierten Personen Informationen zusammenstellt und diese auf Richtigkeit prüft, sind eine mögliche Lösung zum allgemeinen Desinformationsproblem. Derzeit schaffen bösartige Akteure reichhaltige Medienumgebungen, innerhalb deren sie Menschen mit bezwingender Desinformation einfangen, sie an die emotionale Leine

legen und nicht mehr loslassen.[36] Dies ist ein kollektives Intelligenzsystem, in dem ein paar wenige Akteure eine Falschinformation an die Massen verteilen, die dann in großem Rahmen verbreitet wird. In einem positiven kollektiven Intelligenzsystem hätte jeder die Möglichkeit, Beiträge zu erstellen und seine Meinung über die Integrität der Information zu äußern. Dies wäre ein demokratieförderndes System, mit dem die Auswirkung kollektiver Intelligenznetzwerke zur Desinformation reduziert werden könnte.

- Amerikaner müssen schlichtweg wieder für ihre Nachrichten bezahlen. Das Klick-Werbeeinnahmenmodell für Nachrichten hat die investigative Abteilung und die Redaktion bei Medienorganisationen ausgehöhlt und führte zu den von Clickbaiting bestimmten Einnahmenmodellen, bei denen der anzüglichste Inhalt die meisten Klicks auslöst und damit das meiste Geld einfängt.

- Die Menschen müssen bessere Entscheidungen hinsichtlich ihres Informationskonsums treffen. Desinformation ist Junkfood für das Gehirn. Nachrichten sind kein Entertainment und viele konsumieren Falschinformationen einfach, weil sie „lecker" sind. Alle diese Anstrengungen führen zu nichts, wenn wir nicht auch sichere Praktiken für den Informationskonsum und ein soziales Bewusstsein zur Vermeidung von Informations-Junkfood fördern können. Wenn man all die fehlgeschlagenen Kampagnen für gesunde Ernährung bedenkt, wird klar, dass dies in den USA kaum erfolgreich sein wird. Eine realistischere Lösung wäre es, den Menschen faktische Informationen zu bieten, die besser schmecken und attraktiver sind als die Desinformationen, die sie derzeit konsumieren.

LETZTE ÜBERLEGUNGEN

Die größte Gefahr in einer MADCOM-regierten Welt geht von dem Glauben aus, dass wir in einer postfaktischen Welt leben. **Das stimmt nicht**, und es ist genau das, was uns unsere Gegner einreden wollen. Fakten existieren, und sie sind wichtig. Sachverstand ist wichtig. Ein gemeinsame Perspektive zur Realität ist entscheidend für ein funktionierendes demokratisches System. Wir müssen darauf bestehen, dass es eine Wahrheit gibt, dass eine objektive Realität existiert, und es ist unsere Pflicht als Einzelpersonen, Organisationen und Regierungen, diese Wahrheit zu finden und den Fokus auf sie zu richten.

Die zweitgrößte Gefahr stellt die Bekämpfung böswilliger MADCOMs mit unseren eigenen Desinformations-MADCOMs dar. Dies würde eine postfaktische Welt vorantreiben und eine Plattform für die öffentliche Manipulation ermöglichen, falls solche MADCOMs einer künftigen, unethischen Verwaltung in die Hände fielen. Es gibt jede Menge effektiver, diffamierender und doch wahrheitsgetreuer Tatsachen über unsere Gegner, die mit MADCOMs verbreitet werden können. Wir müssen bei der Suche nach Sicherheit nicht unsere eigene Integrität opfern.

Vielleicht ist der aktuelle Trend, in dem Ideologien die individuelle Auffassung der Realität beeinflussen eine vorübergehende Phase, die wir schadlos durchlaufen. Doch nach umfangreicher Recherche ist der Autor der Meinung, dass wir am Anfang einer neuen Phase globaler Instabilität stehen, großteils hervorgerufen von einer um sich greifenden Unsicherheit über die Wahrheit, einer Neuaufstellung ideologischer Zugehörigkeiten und einer gefühlten Komplexität, die den menschlichen Verstand überwältigt – jeweils möglich gemacht von Informations- und Kommunikationstechnologien. MADCOMs werden diese sehr persönlichen Instabilitätsimpulse verstärken, werden es Gegnern ermöglichen, die Darstellungen zu zerschlagen, die Gesellschaften zusammenschweißen, und werden extreme Verwirrung säen. Desinformation kann fast immer falsch, aber dennoch wirksam sein. Die Wahrheit muss annähernd perfekt sein.

Wir werden schon bald eine Proliferation elektronischer IoT-Geräte sehen, und Milliarden von Apparaten, tragbaren Geräten und anderen Sensoren werden uns im täglichen Leben begleiten. Ohne verschärfte Gesetze und die Kooperation im privaten Sektor ist es schwierig, sich Szenarien vorzustellen, in denen nicht genügend Daten verfügbar sind, um ein detailliertes

36 Carole Cadwalladr, „Google, Democracy and the Truth About Internet Search", Guardian, 04. Dezember 2016, https://www.theguardian.com/technology/2016/dec/04/google-democracy-truth-Internet-search-facebook.

psychometrisches Profil von jedem Menschen zu erstellen. Und im Falle fast aller bereits geborener und im Internet aktiver Menschen ist schon jetzt zu viel Information verfügbar, als dass eine wahre Privatsphäre noch einmal zurückerkämpft werden könnte.

Die wichtigste Frage hinsichtlich einer MADCOM-regierten Zukunft ist vielleicht die Frage, wie viele Menschen auf die Existenz von konstanter, heimtückischer, maschinengesteuerter Manipulation reagieren. Die Entscheidungen von Milliarden von Einzelpersonen werden bestimmen, wie Organisationen und Regierungen reagieren und ob sich die Realität wieder zur Objektivität zurück oder weiter zur Flexibilität hin bewegt.

Die Demokratie kann sich anpassen, aber Institutionen entstehen nicht über Nacht, und Regierungen können (und sollten) nicht schnell umstrukturiert werden. Wir müssen daher Zeit gewinnen, damit demokratische Einrichtungen sich weiterentwickeln und sich an die neue, von der Technologie auferlegte Realität anpassen können. Eine aggressive und effektive Reaktion von Einzelpersonen, Regierungen, Nichtregierungsorganisationen, dem privaten Sektor, der Wissenschaft und von sonstigen Organisationen ist erforderlich, um die von MADCOMs ausgehenden Risiken anzugehen.

Im weiteren Sinne stellt die maschinelle Intelligenz die Menschheit vor eine neue Herausforderung. Zum ersten Mal in der Geschichte der Menschheit müssen wir unseren Raum mit nicht-menschlicher Intelligenz teilen, die viele Aufgaben besser bewältigt als wird. Maschinen werden die menschliche Kultur aktiv durch autonom erzeugte Kunst, Literatur und Musik mitgestalten. Sie werden uns Entscheidungen abnehmen, unsere Autos fahren, unsere Flugzeuge fliegen und unsere Beziehungen zu anderen Menschen regeln. Manche Menschen werden starke emotionale Bindungen mit KIs eingehen, und wir werden uns aller Wahrscheinlichkeit nach ernsthaft mit den Rechten von KI-Systemen auseinandersetzen müssen. Diese Auseinandersetzungen werden dank der MADCOMs noch komplizierter, da diese Werkzeuge ein viel subtileres und raffinierteres Level der Manipulation beherrschen.

Die Maschinen kommen, und sie möchten uns sprechen. Das Schicksal unseres Landes, unserer demokratischen Grundordnung und sogar unserer Auffassung von Realität wird davon abhängen, wie wir uns auf diese Sprachkakofonie vorbereiten und uns an sie anpassen.

ÜBER DEN AUTOR

Matt Chessen ist ein amerikanischer Karrierediplomat, Technologe und Autor, der derzeit als leitender technologiepolitischer Berater im Office of the Science and Technology Adviser des Außenministers tätig ist. Von 2016 bis 2017 war Herr Chessen State Department Fellow für Wissenschafts- und Technologiepolitik an der George Washington University, wo er die internationalen Implikationen der künstlichen Intelligenz, der computergestützten Propaganda, der kognitiven Sicherheit und der maschinengesteuerten Kommunikation recherchierte. Zwischen 2014 und 2016 war Herr Chessen als Koordinator für internationale Cyberpolitik (International Cyber Policy) für das Bureau of East Asian and Pacific Affairs tätig und leitete dort die regionale Implementierung der amerikanischen International Strategy for Cyberspace.

Bevor er 2004 in den diplomatischen Dienst einstieg, gründete Herr Chessen ein e-Commerce-Unternehmen und war bei Razorfish für die strategische Entwicklung, das Design und die Implementierung umfangreicher Unternehmenswebseiten verantwortlich. Er diente als Beauftragter für wirtschaftliche Belange in Liberia, als Konsulatsbeamter und politisch-militärischer Beamter im Irak und als politischer Berater für die ISAF-Headquarters in Afghanistan. Außerdem arbeitete er in Washington, D.C., im Bureau of Political-Military Affairs und im Office of eDiplomacy, wo er die Implementierung einer quelloffenen, kollektiven Arbeitsplattform für die US-Regierung, Open Opportunities, leitete.

Herr Chessen erwarb einen Juris Doktor an der Georgetown University und einen MBA und BA an der University of Arizona. Er erhielt acht Auszeichnungen für seine Dienste im Außenministerium, einschließlich des Superior Honor Awards für seine Arbeit im Afghanischen Friedensprozess und seine Anstrengungen, die amerikanische internationale Cyperpolitik voranzutreiben. Herr Chessen ist Autor zweier Romane und einer Reihe von Kurzgeschichten und wissenschaftlichen Artikeln.

ATLANTIC COUNCIL BOARD OF DIRECTORS

Atlantic Council

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council
1030 15th Street, NW, 12th Floor, Washington, DC 20005
(202) 463-7226, www.AtlanticCouncil.org