Tech gegen Taten

Von Algorithmen für die Jagd auf Kriegsverbrecher, Bildern vorgetäuschter Massengräber und Apps für Zeugen von Verbrechen gegen die Menschlichkeit: Wie Deutschland mit dem Einsatz digitaler Technologie bei der Verfolgung internationaler Verbrechen zu einer intelligenten Außenpolitik kommen kann.

Von Alicja Polakiewicz

Würde man sämtliche Videos auf YouTube, die über den Krieg in Syrien aufgezeichnet wurden, hintereinanderweg schauen, bräuchte man länger als der Krieg selbst andauert. Einerseits ist dieser Vergleich eindrucksvoll; andererseits ist bekannt, dass der Syrien-Krieg minutiös dokumentiert wurde. Weniger klar ist, ob die Außenpolitik den Technologien, die diesen Konflikt zu dem vielleicht bestdokumentierten Krieg der Geschichte machten, mit Begeisterung entgegensehen sollte – oder mit Angst.

In diesem Essay befasse ich mich mit den Auswirkungen des technologischen und speziell des digitalen Fortschritts auf die Außen- und Sicherheitspolitik. Ich konzentriere mich dabei auf ein außenpolitisches Ziel, das im Vergleich zu anderen ein Nischendasein führt: den Kampf gegen die Straflosigkeit internationaler Verbrechen, also dagegen, dass schwerste Verbrechen wie Völkermord, Kriegsverbrechen und Verbrechen gegen die Menschlichkeit ungeahndet bleiben. Meine Entscheidung ist dadurch begründet, dass die Digitalisierung die Verfolgung internationaler Verbrechen tatsächlich revolutioniert. Deswegen eignet sich dieses Thema für eine Fallstudie, auf deren Basis sich viele Fragen über die Folgen von digitalen Technologien und Interaktionsformen auf die Außen- und Sicherheitspolitik produktiv diskutieren lassen.

„Gerechtigkeit" zu schaffen, ist ein hoher moralischer Wert – und doch ganz und gar unerreichbar. Gute Außenpolitik erfordert trotzdem den Einsatz dafür, schwerste internationale Verbrechen nicht ungeahndet zu lassen, hat doch eine solche Politik segensreiche Nebenwirkungen. In anderen Worten: Damit sich die Bemühungen im Kampf gegen die Straflosigkeit aus außenpolitischer Perspektive lohnen, müssen sie nicht unbedingt dazu führen, dass wirklich jeder Täter zur Verantwortung gezogen wird.

Gerade für Deutschland kann es sich wirklich lohnen, die Verfolgung von Kriegsverbrechen und Verbrechen gegen die Menschlichkeit (in weniger abstrakten Begriffen ist es das, was ich mit der Beendigung der Straflosigkeit meine) voranzutreiben. Ziele, die die deutsche Außenpolitik ausdrücklich verfolgt (Sicherheit, Stabilität, Menschenrechte) profitieren unmittelbar von Investitionen in den Kampf

gegen die Straflosigkeit. Das liegt daran, dass die Verfolgung dieser Straftaten ihrer Definition nach ein Akt der Durchsetzung internationalen Rechts ist. Das internationale Recht durchzusetzen, bedeutet die Werte der internationalen Gemeinschaft zu verteidigen. Dies wiederum ist gleichbedeutend damit, einen Beitrag zur Stabilität des Systems zu leisten. Da einer dieser Werte der Gewaltverzicht ist, gibt es zudem einen starken sicherheitspolitischen Anreiz, diese Normen zu festigen.

Ein weiterer Wert und ein Ziel deutscher Außenpolitik ist die Achtung der Menschenrechte. Mehr noch: Wer gegen Straflosigkeit kämpft, arbeitet für und mit denjenigen Teilen unterdrückter Gesellschaften, die für eine demokratische und rechtsstaatliche Zukunft ihres Landes kämpfen und sich schon deswegen als strategische Partner für Deutschland eignen. Deutschland, das sich dank der jüngst nach dem Weltrechtsprinzip geführten Strafverfahren einen Ruf als Vorreiter in der Strafjustiz erwirbt, sollte daraus nicht nur bei Menschenrechtsaktivisten und Strafrechtlern Nutzen ziehen, sondern auch in außenpolitischen Kreisen.

Das Syrian Archive, das in der Organisation Mnemonic aufgegangen ist, wurde ad hoc gegründet, um Beweise für Straftaten zu sichern, die im Zusammenhang mit dem Krieg in Syrien verübt wurden. Laut seiner Webseite verfügt das Syrian Archive über mehr als drei Millionen Aufnahmen und Dokumente. Es ist zu hoffen, dass zumindest ein Teil davon als Beweismittel in Ermittlungsverfahren Eingang findet. Viele dieser Beweise stammen aus offenen Quellen. Das sind Dokumente jeglicher Art – Videos, Fotografien, Audioaufnahmen, eingescannte Papiere –, die frei im Internet verfügbar sind oder waren.

Die Dokumentation und der Zugang zu Beweisen für internationale Verbrechen sind durch die Verbreitung von digitalen Technologien demokratisiert worden. Das gilt besonders für persönliche Geräte wie Handys und für das Internet. In vielen Fällen verfügen Zeugen, Opfer und sogar Täter über Mittel, Straftaten zu dokumentieren, bei denen sie zugegen sind. Der Syrien-Krieg zeigt, wie intensiv diese Möglichkeit genutzt wird. Immer häufiger kommen zudem sekundäre Hilfsmittel zum Einsatz, die den Prozess weiter unterstützen.

Eines dieser Tools ist die App „eyeWitness to Atrocities“ (auf Deutsch: Zeuge von Gräueltaten). Sie ermöglicht es, Videos von Zeugen so aufzuzeichnen, zu übertragen und zu speichern, dass sie als Beweise vor Gericht verwertbar sind. Die Vorteile für die internationale Strafverfolgung liegen auf der Hand: Solche Beweise sind vor allem in Fällen wichtig, in denen die Ermittler nur schwer Zugang zu Gegenden bekommen, wo Regierungskräfte nicht nur Straftaten verüben, sondern auch den Zugang kontrollieren. Darauf weist die Wissenschaftlerin Konstantina Stavrou vom Ludwig Boltzmann Institute of Fundamental and Human Rights hin, die auf internationales Strafrecht und elektronische Beweismittel spezialisiert ist. Die Beweismittel, die von Einzelnen am Ort dokumentiert und von Organisationen wie Mnemonic archiviert werden, eröffnen dringend benötigte Alternativwege, um Straftaten einwandfrei dokumentieren zu können.

Es hieße allerdings, die heutige Realität zu verklären, würde man die Dokumentation von Verbrechen und den Zugang zu Beweismitteln als einen ganz und gar demokratischen Prozess darstellen. Um diesen Punkt zu veranschaulichen, möchte ich bitten, ein kleines Gedankenexperiment anzustellen: Wenn Sie über die Dokumentation des Krieges gegen die Ukraine auf den sozialen Medien nachdenken, welche Inhalte fallen Ihnen ein? Ich selbst denke an Selensky und seine Mitarbeiter, die mit Kaffeebechern in der Hand durch die Geisterstadt Kiew laufen, an ukrainische Traktorfahrer, die russische Panzer abschleppen, an Tee trinkende Kriegsgefangene und an Audioaufzeichnungen von der Schlangeninsel. Natürlich gibt es jede Menge Bilder von ausgebombten Gebäuden, aber wo sind die Videos von in diesem Moment verübten Kriegsverbrechen, die die Identifizierung einzelner Täter ermöglichen?

Was wir in den sozialen Medien erleben, wird von gewinnorientierten Unternehmen gefiltert, die Plattformen wie Twitter, Facebook oder TikTok besitzen. Brutale Inhalte, darunter auch Videos, die terroristische Aktivitäten oder

andere Arten extremer Gewalt darstellen, werden zwar auf diesen Plattformen gepostet, aber so schnell wieder entfernt, dass die meisten Nutzer sie nie zu sehen bekommen. Ohne Zweifel ist es richtig, diese Videos zu entfernen, zum Beispiel aus Respekt vor den Opfern oder zum Schutz gefährdeter Nutzer. Allerdings birgt die rasche Löschung das Risiko, die Vorteile zunichtezumachen, die daraus erwachsen, dass Beweise für internationale Verbrechen leicht dokumentiert und geteilt werden können. Für Jay D. Aronson und Enrique Piracés, beide Mitarbeiter des Carnegie Mellon University Center for Human Rights Science, ist dies eine der zentralen Herausforderungen, vor denen Staatsanwälte stehen, die wegen Völkermord, Kriegsverbrechen oder Verbrechen gegen die Menschlichkeit ermitteln.

Aber auch dieses Problem ist nicht unüberwindbar – und digitale Technologien, vor allem künstliche Intelligenz, spielen bei der Lösung womöglich eine zentrale Rolle. Es gibt einen Mittelweg zwischen der viralen Verbreitung brutaler Inhalte und ihrer Löschung für alle Zeiten: Daten, die für die Strafverfolgung hilfreich sein könnten, aber nicht geeignet sind, breit geteilt zu werden, sollten aus den sozialen Medien entfernt, aber zweckgebunden gespeichert werden. Dafür sollte es digitale Tresore wie das Syrian Archive geben. Schon heute wird ein großer Teil der fraglichen Inhalte nicht von Mitarbeitern von YouTube persönlich gelöscht. Vielmehr übernehmen maschinelle Lernalgorithmen einen großen Teil der Sucharbeit. Das bedeutet, dass Verfahren, um zumindest einen Teil der Beweissuche zu automatisieren – das Auffinden von potenziell relevanten, aber brutalen Inhalten –, bereits verfügbar sind.

Im größten Potenzial für den digitalen Fortschritt bei der Verfolgung internationaler Verbrechen liegt zugleich das größte Problem: Die Datenmenge ist nun so groß, dass es schwierig geworden ist, Beweismittel herauszufiltern, die für spezifische Ermittlungsverfahren relevant sind. Wo Ermittler früher mit einem Mangel an Daten zu kämpfen hatten, ist heute die Datenflut das größte Problem, sagt Lindsay Freeman, Direktorin für Technologie, Recht und Politik am Human Rights Center der UC Berkeley School of Law.

Massaker, Folter, Kriegsverbrechen: Im Zusammenhang mit Russlands Krieg gegen die Ukraine hat vielerorts die Beweissicherung begonnen.

Mit der riesigen Menge von Daten hängt ein weiteres Problem zusammen: die Gefahr, dass wichtige Informationen von der Masse an Unwichtigem überdeckt werden. Hieraus erwächst ein besonderes Problem, wie Sam Gregory erklärt, Programmdirektor der Menschenrechtsorganisation Witness: Zwar ist die Gefahr nicht geringer geworden, der sich Zeugen im echten Leben durch die Dokumentation von Menschenrechtsverletzungen aussetzen, wohl aber die Wahrscheinlichkeit, dass ihre Berichte Aufmerksamkeit erregen. Aus der Perspektive der Strafverfolger ist das Problem weit komplexer als das Bild

von Nadel und Heuhaufen. Das zutreffendste Bild für diese Ermittlungen, vor allem für Strukturermittlungsverfahren nach deutschem Vorbild: Erst muss man einen Heuhaufen aufhäufen, bevor man im zweiten Schritt versuchen kann, die Nadel zu finden, die hoffentlich darin versteckt ist. Strukturermittlungsverfahren zeichnen sich ja gerade dadurch aus, dass sie eingeleitet werden, ohne dass es bereits konkrete Verdächtige gibt. Das Ziel ist, zunächst so viele Informationen wie möglich zu sammeln, um dann später zu schauen, welche davon nützlich sind.

Dieses Problem hat noch eine weitere Ebene: In der Realität gibt es mehr als nur einen Heuhaufen. Gerade im Zusammenhang mit dem Ukraine-Krieg haben zahlreiche Akteure und Organisationen, einschließlich staatlicher Strafverfolgungsbehörden, internationaler Gerichte und zivilgesellschaftlicher Organisationen, mit der Sicherung von Beweisen begonnen. Zwar gibt es Versuche, diese Bemühungen zu bündeln, vor allem in der Form des von Polen und Litauen initiierten gemeinsamen Ermittlerteams. Aber noch existiert keine zentrale Informationsbasis, durch die sich der Ermittler, der die Nadel finden soll, durchgraben könnte.

Als ob dies alles noch nicht entmutigend genug wäre, ist die Arbeit der Ermittler, wenn sie die Nadel endlich gefunden haben, noch immer nicht beendet. Sie müssen erst noch prüfen, ob es sich bei dem, was sie in der Hand halten, tatsächlich um eine Nadel handelt. Manche Staaten bezahlen Trolle, damit sie bei jeder Gelegenheit das Internet mit gefälschten Beweisen oder manipulierten Aufnahmen überschwemmen. Menschen, die der staatlichen Propaganda auf den Leim gegangen sind, tragen zu deren weiterer Verbreitung bei. Auf diese Weise wird die Arbeit der Ermittler und Strafverfolger bei internationalen Verbrechen stark behindert. Die Anfälligkeit für bösartige Desinformation ist nach Einschätzung von Giancarlo Fiorella, Charlotte Godart und Nick Waters – investigative Reporter beim Recherchenetzwerk Bellingcat – denn auch eine der größten Schwächen der digitalen Beweismittel. Welche Gefahren bestehen, zeigte sich vor Kurzem in Mali, wo es Versuche offenbar russischen Ursprungs gab, französischen Soldaten Verbrechen gegen die Menschlichkeit anzudichten. Wahrscheinlich waren russische Söldner in einen kurz zuvor von den Franzosen verlassenen Militärstützpunkt eingedrungen. Die Russen legten ein falsches Massengrab an, machten Fotos und verbreiteten sie über die sozialen Medien. Über den genauen Hergang wird noch gestritten, aber die Franzosen haben Drohnenaufnahmen veröffentlicht, die ihre Darstellung der Ereignisse stützen.

Wie soll man mit diesen Chancen und Herausforderungen umgehen? Meine These ist, dass die digitalen Technologien und Interaktionsformen an sich weder gut noch schlecht für die Außenpolitik sind. Es hängt immer davon ab, wie jene, die die Außenpolitik gestalten, ihr Potenzial nutzen und mit den damit einhergehenden Problemen umgehen. Im Folgenden möchte ich vier Vorschläge machen, um zu skizzieren, wie intelligente Außenpolitik aussehen könnte.

Erstens: Akzeptieren Sie die Realität des Digitalen und erkennen Sie seine Grenzen. Auch wenn die Folgen des digitalen und technologischen Fortschritts für die Außenpolitik weder ausschließlich gut noch ausschließlich schlecht sind, real sind sie allemal. Zu akzeptieren, dass diese Realität unausweichlich ist – und dass es sinnlos ist, ihr entkommen zu wollen –, ist der erste Schritt zu einer intelligenten Reflexion über Außenpolitik. Angela Merkels weithin belächelte Äußerung vom Internet als „Neuland“ fiel zwei Jahre nach Ausbruch des Krieges in Syrien. Dieser Krieg brachte den Durchbruch für Ermittlungsverfahren auf der Basis offener Quellen und künstlicher Intelligenz. Die Akklimatisierungsphase ist also vorbei.

Die Realität des Digitalen zu akzeptieren, bedeutet zugleich, sich seiner Grenzen bewusst zu sein. Anders ausgedrückt: Man wird auch in Zukunft noch selbst anpacken und sich die Hände schmutzig machen müssen, um Beweise zur Verfolgung internationaler Verbrechen zu sammeln. Der Podcast „Nowhere to Hide“ des Global Public Policy Institute beschreibt sehr eindrücklich, wie französische

Journalisten einen Fußmarsch durch die Wüste auf sich nahmen, um über die Grenze auf jordanisches Hoheitsgebiet zu kommen. Auf diese Weise gelang es ihnen, Proben zu sichern, die beweisen, dass das Assad-Regime chemische Waffen gegen seine eigene Bevölkerung eingesetzt hatte. Diese Art von harten Beweisen lässt sich auch durch die gründlichste Suche in den sozialen Medien nicht ersetzen.

Zweitens: Verabschieden Sie sich vom Elitismus der Außenpolitik und weltweiten Justiz und binden Sie die Öffentlichkeit ein. Kurz nach Ausbruch des Ukraine-Krieges richtete die ukrainische Strafverfolgungsbehörde eine Webseite ein, über die ganz normale Bürger Beweise für Kriegsverbrechen einreichen können. Inzwischen ist sie auch als App verfügbar. So können Zeugen es vermeiden, Inhalte in den sozialen Medien zu posten, die aus weiter Ferne von gewinnorientierten und schwer zu kontrollierenden Unternehmen verwaltet werden. Die Webseite ermöglicht es auch, die Beweismittelkette zu wahren, das heißt lückenlos zu dokumentieren, welchen Ursprung ein Beweismittel hat, wie es weitergegeben wurde, und wer darauf Zugriff hatte.

Die Wahrung der Beweiskette ist von zentraler Bedeutung, weil viele Gerichte Beweise nur dann als gültig akzeptieren, wenn ihre Herkunft vollständig dokumentiert ist. Die Tatsache, dass ich – eine Twitter-Nutzerin, die mit diesen Fragen nicht unmittelbar etwas zu tun hat – über diese Webseite gestolpert bin, zeigt, dass sie weite Verbreitung gefunden hat und nützlich ist. Der ukrainische Generalstaatsanwalt hat offensichtlich begriffen, welches Potenzial in der Beteiligung der Öffentlichkeit liegt. Davon kann Deutschland lernen.

Ironischerweise ermöglichen es digitale Interaktionsformen nicht nur jedem, der über eine Internetverbindung verfügt, vom Wohnzimmer aus wegen internationaler Verbrechen zu ermitteln. Sie machen es auch einfacher, vom Sofa aus Kriegsverbrechen zu begehen. Wenn ich an den oben erwähnten Tee trinkenden Kriegsgefangenen zurückdenke, war der Grund, warum ich mir diesen Inhalt angeschaut habe, dass er in sozialen Medien gepostet und geteilt worden war. Die Genfer Konventionen verlangen jedoch, Kriegsgefangene vor „Beleidigung oder öffentlicher Neugier“ zu schützen. Das Internationale Komitee vom Roten Kreuz ebenso wie andere Organisationen interpretieren diese Vorgabe so, dass die Verbreitung der Fotos von Kriegsgefangenen verboten ist. Die Öffentlichkeit einzubeziehen, bringt also Verantwortung mit sich. Es ist entscheidend, nicht nur hochrangige Vertreter des Staates, sondern alle Bürgerinnen und Bürger darüber aufzuklären, was ihre zufälligen Handlungen im Internet für außenpolitische und völkerrechtliche Folgen haben können.

Drittens: Investieren Sie in Technologien und statten Sie strategische Partner aus. Deutschland ist heute das Land mit den besten Voraussetzungen, weil hier die intellektuellen Fähigkeiten und Fachkenntnisse im Systemdesign auf Flüchtlingspopulationen treffen, die sich für internationale Gerechtigkeit einsetzen. In Berlin sind einige der spannendsten und innovativsten Organisationen ansässig, die digitale Tools für die internationale Strafjustiz einsetzen, so wie Mnemonic und VFRAME. Im Gegensatz zu angelsächsischen Justizsystemen, in denen die Zulassung von Beweisen strikt geregelt ist, ist Deutschland für Menschenrechtsaktivisten attraktiv, weil die Zulassung von offenen Quellen ihnen hier vergleichsweise weniger Sorgen bereiten wird. Hinzu kommt, dass Deutschland eine große Zahl von Flüchtlingen beherbergt, von denen viele sich leidenschaftlich engagieren, um die Verfolgung von Kriegsverbrechen und anderen internationalen Verbrechen zu ermöglichen. Die Voraussetzungen sind also da, dass Deutschland ein wirkliches Zentrum für die internationale, auf technologische Tools und digitale Interaktionsformate gestützte Strafjustiz wird. Nun sind die außenpolitischen Akteure gefordert, diese Voraussetzungen zu nutzen.

Ein Beispiel aus dem *Wall Street Journal* verdeutlicht, wie: In Zusammenarbeit mit dem Syrian Archive gelang es VFRAME, das Problem zu lösen, dass sein KI-Algorithmus Streumunition nicht zuverlässig auf Fotos und in Videos

identifizieren konnte. Die Organisation verwendete existierende Fotos von Streumunition, um 3D-Modelle zu konstruieren. Diese Modelle wiederum dienten dazu, weitere Fotos zu erstellen. Außerdem druckte VFRAME Modelle von Streumunition auf dem 3D-Drucker und platzierte sie in einer natürlichen Umgebung, um Fotos zu machen. Das so generierte Material wurde in den Algorithmus eingespeist. KI-Algorithmen benötigen riesige Datenmengen, um zu lernen. Als VFRAME erkannte, dass das Problem am Datenmangel lag, produzierte die Organisation die benötigten Daten einfach selbst.

Auf der Grundlage dieses Beispiels möchte ich einen etwas unorthodoxen Vorschlag machen. Wenn es um die Strafverfolgung im Zusammenhang mit dem Ukraine-Krieg geht, können wir von fünf Faktoren ausgehen: Erstens sind riesige Mengen von Daten zu analysieren. Zweitens wird man zur Analyse dieser Daten künstliche Intelligenz brauchen. Drittens gibt es Algorithmen, die Texte und mit Einschränkungen auch Audiodateien durchsuchen können. Viertens funktioniert die auf KI basierende Technologie zwar gut für Dokumente in englischer Sprache. Bei anderen Sprachen ist sie aber weniger zuverlässig, vor allem wenn es um Sprachen wie Ukrainisch oder Russisch geht, die nicht die lateinische Schrift verwenden. Und fünftens hat Deutschland eine große Zahl von Russisch oder Ukrainisch sprechenden Flüchtlingen aufgenommen, von denen einige nur zu gerne einen Beitrag zur Verfolgung von Kriegsverbrechen leisten würden. In Technologien und die Ausrüstung strategischer Partner zu investieren, könnte beispielsweise bedeuten, mithilfe staatlicher Gelder ein Projekt, eventuell auch mit Hilfe von Mnemonic oder VFRAME, für ukrainische und russische Muttersprachler zu initiieren. Man würde sie bitten, kurze Texte oder Audioaufnahmen einzureichen, um einen KI-Algorithmus zu füttern. Aller Voraussicht nach könnte ein solches Tool schon sehr bald dazu beitragen, die Arbeit der internationalen Strafverfolger zu erleichtern.

Viertens: Machen Sie sich auf Veränderungen gefasst. Zwar wissen wir nicht, welche Form Beweise in Zukunft haben werden, aber wir wissen, dass sie anders aussehen werden als heute. Daher können wir uns zwar nicht auf eine spezifische Art von Beweismitteln vorbereiten, aber wir können unsere Strukturen so verändern, dass sie anpassungsfähiger werden. Agilität, in Verbindung mit der nötigen Gründlichkeit, die alle außenpolitischen und juristischen Prozesse begleiten sollte, ist von größter Bedeutung. Wir brauchen eine enge Zusammenarbeit zwischen Außenpolitikern und Juristen, um unsere Institutionen auf den neuesten Stand der digitalen Entwicklung zu bringen. Denn das ist, wie Kaan Sahin, heute Beauftragter für Cyber- und Hybridpolitik bei der NATO, sagte, eine „interministerielle Aufgabe“. Notwendig ist außerdem eine allgemeine Haltung, die Abweichungen vom üblichen Vorgehen – wenn auch immer auf kühl durchdachte Weise – billigt, um Kreativität und Innovation zu ermöglichen. Fakt ist, dass der technische Fortschritt und digitale Interaktionsformen die außen- und sicherheitspolitische Landschaft auch in Zukunft rasant verändern werden. Die Frage ist, ob wir unsere Strukturen so anpassen, dass wir diese Transformation aktiv gestalten können.

Fassen wir zusammen: Dafür zu sorgen, dass internationale Verbrechen nicht straflos bleiben, ist gute Außenpolitik. Technologische Tools und digitale Interaktionsformen können helfen, dass daraus gute und zugleich intelligente Außenpolitik wird. Deutschland ist in einer einzigartigen Position, um die Chancen der digitalen Werkzeuge zu nutzen, die Herausforderungen zu bewältigen und eine wirkliche Führungsrolle für die digital unterstützte internationale Strafjustiz zu spielen. Die Zeit ist reif, dieser Aufgabe gerecht zu werden.

Aus dem Englischen von Bettina Vestring

Alicja Polakiewicz
ist Doktorandin an der Friedrich-Alexander-Universität Erlangen-Nürnberg. Mit diesem Text hat sie den Sylke-Tempel-Essaypreis 2022 gewonnen.