Wo die digitale Gefahr wächst

… wächst das Rettende auch: Der böswillige Einsatz von Technologie besonders durch Autokratien bedroht den Frieden. Doch lassen sich Plattformen und innovative Anwendungen ebenso nutzen, um Konflikten vorzubeugen und sie zu bewältigen.

Von Tyson Barker

Es geschah an der ukrainisch-rumänischen Grenze, kurz nach dem russischen Überfall am 24. Februar: Tausende ukrainischer Flüchtlinge hatten sich am Grenzübergang versammelt, als die dortigen Grenzbehörden von einer massiven Cyberattacke heimgesucht wurden. Die Grenzabfertigung kam fast zum Erliegen, und die Beamten mussten auf Stift und Papier zurückgreifen, um Zehntausende ukrainischer Flüchtlinge zu registrieren, die vor der russischen Invasion flohen. Glück im Unglück: Innerhalb weniger Stunden hatte eine Gruppe von IT-Spezialisten Programme zur Verarbeitung und Authentifizierung entwickelt, die es den rumänischen und ukrainischen Behörden erlaubten, Migrationsdaten in Echtzeit auszutauschen.

Von Beginn des russischen Angriffskriegs gegen die Ukraine an hat die globale IT-Gemeinschaft zusammen mit westlichen Technologieunternehmen kreative Maßnahmen entwickelt, um die Ukraine gegen russische Informations- und Cyberattacken zu schützen. Damit ist der Krieg zu einem Echtzeitlabor für umkämpfte Räume geworden, in denen Autoritarismus und Demokratie, digitaler Extremismus und digitales Krisenmanagement aufeinanderprallen. Die Nutzung von Online-Instrumenten zur Erhaltung und Förderung der demokratischen Ordnung verdient deshalb größere Aufmerksamkeit.

Gute Digitalisierung, schlechte Digitalisierung

Nicht nur digital, auch mit klassischer Kriegsführung versucht Russland, Telekommunikationsinfrastruktur im Kriegsgebiet zu zerstören. Die ukrainischen Regionen, die unter seiner Kontrolle stehen, annektiert Moskau digital, indem es den Internetverkehr umleitet und die Telefonvorwahl auf die russische +7 umstellt.

Aufgrund der weltweiten Verflechtung der Informations- und Kommunikationstechnik, der digitalen Konnektivität, wirken sich all diese Maßnahmen auch in Ländern aus, die nicht direkt das Ziel der Attacken waren. So führten russische Cyberangriffe

auf das Satellitenkommunikationssystem Viasat zwischenzeitlich zur Störung von 5800 Windturbinen in Deutschland.

Auf der anderen Seite können neue Technologien in Konfliktgebieten zur Stabilisierung der Konnektivität beitragen. Das amerikanische Raumfahrt- und Telekommunikationsunternehmen SpaceX hat die Ukraine mit gut 15 000 Hardware-Elementen ausgerüstet – hauptsächlich Satellitenschüsseln, um die Breitbandkonnektivität aufrechtzuerhalten und Hunderttausende von Ukrainern, mehr als 600 Krankenhäuser und medizinische Einrichtungen sowie die ukrainischen Truppen an der Front im Osten mit Internet zu versorgen. Das von SpaceX betriebene Netzwerk Starlink hat derzeit 2404 Satelliten in der Erdumlaufbahn, das britisch-amerikanische Unternehmen OneWeb kommt auf 427; Starlink und OneWeb stimmen sich hier bereits ab. Zudem entwickelt die EU Internet-Konnektivitätskapazitäten in einer niedrigen Erdumlaufbahn (LEO). Ziel der Initiative ist es, auf der Grundlage des Satellitennavigationssystems Galileo und des Copernicus-Dienstes eine sichere weltraumgestützte Konnektivität aufzubauen.

Dass die Kosten für die Montage und den Start von Satelliten sinken, macht die Technologie immer leichter zugänglich. Die EU, die NATO und andere könnten sich dafür stark machen, ungehinderte Konnektivität als universelles Grundrecht anzuerkennen und die Mittel für Informations- und Kommunikationstechnologie in Regionen bereitstellen, die von Konflikten oder Internetsperren bedroht sind. Damit würde man quasi dem Beispiel des Kurzwellenfunks im Kalten Krieg folgen.

China hat das Thema Konnektivität bereits als Areal der digitalen Auseinandersetzung erkannt. Peking plant nicht nur, 13 000 eigene LEO-Satelliten zu starten, es erforscht auch regulatorische und technische Mittel zur Unterbrechung der LEO-Satelliten-Konnektivität.

Das Unternehmen SpaceX hat die Ukraine mit Tausenden von Satellitenschüsseln ausgerüstet

Abspalten und abschotten

Ein Internetzugang ist heute die grundlegende Voraussetzung für ein offenes, friedliches und stabiles gesellschaftliches Umfeld und damit auch für die Ermächtigung von Bürgerinnen und Bürgern. Kein Wunder, dass in Ländern wie dem Iran, dem Sudan, Weißrussland, Indien oder Kasachstan zuletzt stets eine Sperrung von Internetinhalten erfolgte, bevor massenhafte Kontrollen und sonstige Unterdrückungsmaßnahmen gegen vermeintliche Regimegegner gestartet wurden.

Autokratien fahnden ständig nach Möglichkeiten, die digitale Kommunikation zu gestalten und gegebenenfalls aufzuspalten – und sie versuchen, den Zugang zum globalen Netz zu kontrollieren. So geschieht es etwa in China mit der Great Firewall, im Halal Internet des Iran und im wachsenden RuNet des Kremls. Überall werden digitale Grenzen entlang geografischer Parameter geschaffen.

Auch innerhalb ihres Territoriums sorgen autoritäre Staaten dafür, das Netz auf Plattformebene aufzuspalten. So wollen russische Behörden die Arbeit globaler Unternehmen mit Gesetzen erschweren, die Konzerne wie Google dazu verpflichten, physische Niederlassungen in Russland zu unterhalten, ihren Datenfluss zu beschränken und Auflagen zuzustimmen, die eine Grundlage für Erpressung und alle Arten illegaler Einflussnahme bilden können.

Tyson Barker
ist Leiter des Programms Technologie und Außenpolitik bei der Deutschen Gesellschaft für Auswärtige Politik.

Solche Maßnahmen sind jedoch längst nicht nur auf postsowjetische Staaten beschränkt. Auch Indien tut einiges dafür, den Aufstieg globaler Plattformen durch staatliche Regulierung zu beschränken und nationale Plattformen zu stärken. Zudem ist der Einsatz von staatlichen DDoS-Angriffen weit verbreitet (einer Form der Cyberattacke, bei der eine Website oder Netzwerkressource durch Überflutung mit schädlichem Traffic so überlastet werden soll, dass sie nicht mehr betrieben werden kann), nicht nur in postsowjetischen Ländern wie Kirgisistan, sondern auch in Indien und Nigeria. China setzt seine große DDoS-Kanone – eine Art digitalen Todesstern – derweil ein, um jede gegen die Kommunistische Partei gerichtete Internetaktivität zu pulverisieren.

Russlands Krieg hat die Bemühungen, den russischen digitalen Raum nach chinesischem Vorbild vom Rest der Welt abzuschotten, nochmals beschleunigt. Die Digitalaufsichtsbehörde Roskomnadzor hat Facebook und Instagram verboten und macht auch ansonsten den Betrieb global operierender Plattformen praktisch unmöglich. An ihre Stelle treten verdächtig ähnliche Plattformen, die dem Kreml gefügiger und weniger global vernetzt sind. So ist die YouTube-Alternative RuTube im Besitz von Gazprom, Yappy ist die 2021 gestartete TikTok-Alternative und Fiesta seit November 2021 das Instagram-Pendant, das nach dem Verbot des Originals schnell auf Platz eins der Downloads landete.

China und Russland waren bei der Schaffung paralleler Plattform-Ökosysteme am erfolgreichsten. Doch nur Peking hat sich bislang erfolgreich der kompletten digitalen Abschottung angenähert. Die russische Behauptung, man verfüge über die technischen Mittel, um das RuNet – mitsamt aller beteiligten Internetanbieter, Telekommunikationsunternehmen und dem russischen Root-Domain-Names-System (DNS) – vom globalen Internet zu trennen, bleibt zumindest fragwürdig.

Bild nur in Printausgabe verfügbar

Freiheit für Facebook: Noch 2017 konnte man in Moskau gegen die Strategie des Kremls, Russland digital abzuschotten, demonstrieren.

Tatsächlich explodiert nämlich gerade im postsowjetischen Raum die Nutzung virtueller privater Netzwerke (VPNs), mit deren Hilfe sich Bürgerinnen und Bürger Tunnel zum freien Netz graben. So lagen die täglichen VPN-Downloads in Russland am 23. Februar 2022 bei rund 14 000, bevor sie bis Ende März auf 475 000 anstiegen und sich später bei etwa 300 000 täglichen Downloads einpendelten. Globale VPNs wurden dabei von VPNs flankiert, die von zivilgesellschaftlichen Akteuren wie der mit Alexej Nawalny verbundenen

„Internet Protection Society“ entwickelt wurden. Immer mehr Russinnen und Russen wählen sich per VPN in andere Länder ein, um auf daheim gebannte Inhalte zuzugreifen. Zuletzt gab sogar Kremlsprecher Dmitri Peskow zu, ein VPN zu nutzen. Dabei gibt es in Russland bereits seit 2017 ein Anti-VPN-Gesetz.

Hieran können demokratische Staaten und Institutionen anknüpfen. So fördert der amerikanische Open Technology Fund (OTF) Technologien zur Umgehung von Überwachung, Zensur und anderen digitalen Rechtsverletzungen. Unter anderem hat der OTF sich an der Finanzierung des „Tor-Projekts“ beteiligt, einem auf Anonymität ausgerichteten Netzwerk. Derzeit werden vom OTF geförderte Technologien täglich von mehr als zwei Milliarden Menschen weltweit genutzt. Deutschland unterstützt diese Bemühungen, indem es einen Sovereign Tech Fund eingerichtet hat. Auch die EU könnte sich an diesem Fonds beteiligen. Die Erleichterung des Schutzes der Privatsphäre und des Zugangs zu Technologien ist ein wichtiger Schritt, um den digitalen Raum in Richtung Demokratie, Offenheit und Gerechtigkeit zu lenken.

Ausgeklügeltes Getrolle

Ein weiteres digitales Phänomen, mit dem sich Demokratien auseinandersetzen müssen, sind informelle Desinformationsnetzwerke, die mittlerweile deutlich ausgeklügelter und globaler aufgestellt sind als die bekannten Sankt Petersburger Trollfarmen. Zu ihnen zählt die in Kanada ansässige Corona-Verschwörungsplattform Global Research, die von der Strategic Culture Foundation finanziert wird, einer Vertretung des russischen Auslandsgeheimdiensts (SVR). Oder SouthFront, eine Plattform, die nach Ansicht des US-Justizministeriums mit Russlands Inlandsgeheimdienst FSB verbunden ist.

Formen des digitalen „Astroturfing“ sind von Brasilien über Indien bis Vietnam auf dem Vormarsch. Der Begriff ist von der US-Firma AstroTurf abgeleitet, die Kunstrasen herstellt, der täuschend echt aussehen soll. Klassisches Astroturfing will Graswurzelbewegungen vortäuschen, also so tun, als gehe eine fabrizierte Meinungsströmung tatsächlich von der Basis der Gesellschaft aus. Die chinesische United Front geht noch einen Schritt weiter und transportiert digitales Astroturfing in die analoge Welt. Das geschieht über Kultureinrichtungen, Unternehmen und die chinesische Diaspora, besonders in den kaum geschützten Informationsökosystemen des globalen Südens.

Es geht darum, die Illusion zu schaffen, eine fabrizierte Meinung komme von der Basis der Gesellschaft

Oft verstärken die Macher dieser informellen Netzwerke Narrative, indem sie eine passende Desinformationsinfrastruktur nutzen. So speisen sich Chinas Staatsmedien in ihrer Berichterstattung zu Themen wie Nahrungsmittelknappheit, Inflation und den angeblichen NATO-Kolonialismus in der Ukraine immer wieder aus russischen Falschinformationen, wie Moskau sie auch in Afrika, Lateinamerika oder Indien streut.

Um hier etwas entgegenzusetzen, hat man auf Seiten der Demokratien unter anderem digitale Verhaltenskodizes geschaffen. So soll der Digital Services Act (DSA) der EU einheitliche Regeln für die Behandlung von rechtswidrigen Inhalten festlegen. Hinzu kommen Influencer, die ihre Netzwerke für die Bekämpfung von

Desinformation nutzen, und sogenannte Open-Source-Intelligence-Infrastrukturen (OSINT), die in Konfliktzonen und in autoritär gelenkten Informationsräumen ihre Wirkung entfalten sollen. So wurde OSINT eingesetzt, um das Ausmaß der Zerstörung in Syrien zu dokumentieren und die dort bei Luftangriffen eingesetzten Munitionsarten zu ermitteln – auch, um Kriegsverbrechen und Menschenrechtsverletzungen für mögliche Verfahren vor dem Internationalen Strafgerichtshof zu dokumentieren.

Derzeit stellt die in Berlin ansässige Nichtregierungsorganisation Mnemonic der ukrainischen Regierung und anderen Unterstützerstaaten Datenmaterial zu den Gräueln russischer Truppen in Orten wie Butscha zur Verfügung, damit diese später vom Internationalen Strafgerichtshof verfolgt werden können. Die ukrainische Regierung nutzt OSINT, indem sie eine neue Funktion zur Übermittlung von Beweisen für russische Kriegsverbrechen in ihre Verwaltungs-App Diia integriert hat.

Das bekannteste Recherchenetzwerk ist derzeit Bellingcat. Es hat nicht nur die beim MH17-Abschuss genutzten Raketen identifiziert, sondern auch IS-Ausbildungslager in Syrien, den Einsatz von Chemiewaffen durch das Assad-Regime und die Identitäten der Auftragskiller hinter dem Anschlag auf Alexej Nawalny im Jahr 2020 aufgedeckt. Netzwerke wie Bellingcat können aus einem globalen Pool technisch versierter Forscher schöpfen, brauchen aber jede Menge Daten. Die EU, die USA und andere sollten die Katalogisierung von Menschenrechtsverletzungen und Kriegsverbrechen finanziell unterstützen.

Digitales Panoptikum

Die Grenzen umkämpfter digitaler Räume werden in Zukunft vor allem durch Überwachungs- und Frühwarntechnologien definiert werden, also durch zwei Faktoren, die zwangsläufig mit den Fähigkeiten eines Staates und der Qualität seiner Regierungsführung zusammenhängen. Funktionieren ein Staat und seine Institutionen gut, dann sind hier in der Regel auch gute Ergebnisse zu erwarten. So haben IBM und zivilgesellschaftliche Gruppen wie Moonshot CVE nach dem Terroranschlag im neuseeländischen Christchurch 2019 damit begonnen, Muster im gewalttätigen Extremismus zu identifizieren. Andere Systeme nutzen Künstliche Intelligenz, um Frühwarninstrumente zu entwerfen, mit deren Hilfe sich polizeiliche Einsatzkräfte in Städten optimal zuweisen lassen.

Dass die Attraktivität von Frühwarn- und Überwachungsinstrumenten immer größer wird, hat viel mit der ständigen Verfeinerung der Technologie zu tun. Heute ist es möglich, Informationen zu sammeln, ohne dass Nutzer auf einen Link klicken oder eine Datei herunterladen müssen. Dabei ist der Einsatz von Spionageprogrammen zur Überwachung der Opposition nicht auf autoritäre Staaten beschränkt. Mithilfe ähnlicher Technologien wird derzeit auch in Ländern wie Polen, Ungarn und Ruanda die Demokratie untergraben – und selbst für konsolidierte Demokratien ist die Verlockung mitunter groß, derartige Software zu nutzen. Zuletzt zeigte das etwa die Bespitzelung von Vertretern der katalanischen Regierung und Zivilgesellschaft durch den spanischen Geheimdienst.

Die Corona-Krise hat den Ausbau der Überwachungsinfrastruktur noch einmal beschleunigt. Seien es digitale Impfpässe oder Corona-Apps mit Geo-Tracking- und Kommunikationsfunktionen: In der Krise haben Regierungen die Grenzen akzeptabler staatlicher Eingriffe ausgetestet. Einige demokratische Staaten haben strenge Leitplanken für die Datenverarbeitung und -nutzung aufgestellt. Anderswo aber – und selbst in funktionierenden Demokratien

So klein und schon ein Staatsgefährder? Der mobile Überwachungsroboter nimmt sicherheitshalber alles auf, was ihm in Peking vor die Linse kommt.

wie in Ostasien – waren die Erhebung, Verarbeitung und Nutzung von Daten viel weitreichender und umfassten nicht selten gezielte Angriffe auf Gruppen und Einzelne. In Ländern wie China, Russland und den Golfstaaten wurde geradezu ein digitales Panoptikum aufgebaut. Moskau nahm die Corona-Pandemie zum Anlass, um 100 000 neue Gesichtserkennungskameras zu installieren. Ein Instrument, das die Regierung heute skrupellos anwendet, um den Widerstand gegen die Invasion der Ukraine zu brechen. Und auch in Zentralasien, Indien und Lateinamerika werden KI-gestützte Gesichtserkennungskameras in wachsendem Maße genutzt.

Antizipieren und stabilisieren

Auf der anderen Seite könnte Frühwarntechnologie dazu beitragen, Konflikte zu antizipieren und zu verhindern, politische Gemeinschaften zu stabilisieren und gute Regierungsführung zu fördern. Das gilt besonders für Gebiete mit fragilen Staats- und Regierungssystemen.

In dieser Hinsicht haben erste Bemühungen der internationalen Gemeinschaft die Erwartungen bislang jedoch nicht erfüllt. So war etwa das Frühwarnsystem CEWARN (Conflict Early Warning and Response Framework) in Zentralafrika nicht in der Lage, breite Datenanalysen mit sinnvollen politischen Maßnahmen zu verbinden. Und so besteht weiterhin eine Diskrepanz zwischen KI-Analytik und Krisenprävention, was viel mit einem übermäßigen Vertrauen in technologische Lösungen und einer schlechten Integration der Software in den jeweiligen politischen, geografischen, kulturellen und wirtschaftlichen Kontext zu tun hat.

Auch andere Maßnahmen haben bislang nur bescheidene Ergebnisse erzielt. So entwickelten IT-Spezialisten in Kenia im Zuge der politischen Gewalt nach den Wahlen die Software Ushahdi, um derartige Ausschreitungen vorhersehen und verhindern zu können.

Das sogenannte ViEWS-System wiederum stützt sich auf Formen der Künstlichen Intelligenz, die Sprache und Bildverarbeitung, soziale Medien und Nachrichtentexte, Open-Source-Klimadaten und andere wirtschaftliche und politische Daten heranziehen, um integrierte Modelle zu erstellen, mit deren Hilfe sich Klima-, Politik- und Ernährungssicherheitsrisiken abschätzen lassen. All diese Systeme stützen sich auch auf Migrationsdaten, Dichtemuster aus dem Handy- und IP-Traffic sowie Geodaten, die vom ständigen Ausbau der Satellitensysteme profitieren.

Europa beteiligt sich am sogenannten Global Conflict Risk Index (GCRI), der maschinelle Sprachverarbeitung einsetzt, um Frühwarn- beziehungsweise Frühaktionssysteme einzurichten. Die deutsche Regierung leistet dabei einen Beitrag mit ihren PREVIEW-KI-Analysetools, die eine Visualisierung von Klima-, Migrations- und Politiktrends ermöglichen. PREVIEW wurde für die Krisenanalyse und -vorhersage in der Tschadsee-Region erprobt und findet mittlerweile auch anderswo Anwendung.

Der Kampf in digitalen Räumen wird durch Geld, Technologie und Innovation entschieden

Technologische Anwendungen im Dienste guter Regierungsführung und des Krisenmanagements werden künftig wichtige Instrumente für den Aufbau staatlicher Kapazitäten sein. Die EU, die USA und internationale Organisationen müssen aber klare Leitplanken für Überwachungs- und Frühwarntechnologien schaffen – insbesondere in Krisengebieten und Regionen mit fragiler Staatlichkeit.

Peking versucht derweil aggressiv, sein Modell des Techno-Autoritarismus zu exportieren. Ein Modell, das alle Technologieebenen zur Regulierung des Internetverkehrs, digitale Dienste sowie intelligente Stadt- und Frühwarntechnologien einschließt. Dieser Ansatz geht zurück auf Chinas Streben nach staatlicher Kontrolle, seine technologiegestützten sozialen Beziehungen im Inland sowie sein umfassendes technologisches Netzwerk im Ausland – unter anderem durch die Neue und die Digitale Seidenstraße.

Alle der genannten Konfliktfelder gehören zu einem sich ständig weiterentwickelnden Kaleidoskop umkämpfter digitaler Räume. Ein Kampf, in dem letztlich technologischer Vorsprung und die finanziellen Mittel für Innovationen entscheidend sein können. Und in gewisser Weise wurde das Internet, vielleicht versehentlich, genau so konzipiert, dass es diese Spannungen noch weiter verstärkt. Denn bereits die frühsten Silicon-Valley-Utopisten brüsteten sich damit, dass die digitale Technologie den Nutzern die Möglichkeit geben würde, sich von der allumfassenden Macht der Staaten und der Industrie zu emanzipieren. John Perry Barlows Manifest „A Declaration of the Independence of Cyberspace“ aus dem Jahr 1996 umriss diesen Gedanken wie folgt: „Regierungen der industriellen Welt, ihr müden Giganten aus Fleisch und Stahl, ich komme aus dem Cyberspace, der neuen Heimat des Verstands. Im Namen der Zukunft bitte ich euch Vergangene, uns in Ruhe zu lassen. Ihr seid bei uns nicht willkommen. Wo wir uns versammeln, habt ihr nicht viel zu sagen.“

Doch der fruchtbare Boden für Technoliberale wurde tatsächlich erst durch die Finanzierung des ARPANET (Advanced Research Projects Agency Network) durch das US-Militär und durch CERN, die Europäische Organisation für Kernforschung, bereitet. Maßgeblich war hier die Entwicklung von Software-Schnittstellen in Form von HTTP und HTM. Der Konflikt um den digitalen Raum war programmiert.

Diese Reibung ist und bleibt ein zentrales Paradox der digitalen Welt. Einerseits ist sie das dezentralisierende, demokratisierende Instrument der Offenheit und der Widerstandsfähigkeit, andererseits ein Einfallstor für potenziell grenzenlose staatliche, militärische und unternehmerische Kontrolle. Hier verläuft vielleicht eine der wichtigsten geopolitischen Bruchlinien des digitalen Zeitalters. IP

Aus dem Amerikanischen von Kai Schnier