Spionieren, kontrollieren, desinformieren

Einst als „Befreiungstechnologien“ gefeiert, dienen digitale Techniken heute Autokratien wie China und Russland als nützliche Tools zur Unterdrückung und im Konflikt mit dem Westen. Ein Überblick.

Von Alena Epifanova und Valentin Weber

Es war Ende März 2023, als sich Wladimir Putin und Xi Jinping in Moskau trafen und eine gemeinsame Erklärung verabschiedeten, in der sie eine „Vertiefung der strategischen Zusammenarbeit in einer neuen Ära“ ankündigten. Nicht die erste Ankündigung dieser Art von zwei Autokraten, jedoch ein bemerkenswertes Zeichen in Zeiten des Ukraine-Krieges und des angespannten Verhältnisses zum Westen. Mehr Koordinierung und Austausch besonders zu digitalen Überwachungstechnologien, zu Cyberoperationen und Desinformation können für Putin und Xi von Nutzen sein, wenn sie ihre Macht zuhause konsolidieren und ihren Einfluss im Ausland ausbauen wollen.

Schon seit einiger Zeit unternehmen beide Länder erhebliche Anstrengungen, um sogenannte „Befreiungstechnologien“, das heißt Informations- und Kommunikationstechnologien, die unabhängiges kollektives Handeln ermöglichen und die Zivilgesellschaft stärken können, in die eigenen Dienste zu stellen. Auch wenn von einer grenzüberschreitenden Allianz im eigentlichen Sinne zwischen China und Russland noch keine Rede sein kann, sehen die beiden Regime den Westen als gemeinsamen Gegner in einer multipolaren Weltordnung. Zudem stehen beide für eine starke staatliche Informationskontrolle zuhause und das Setzen eigener Narrative im Ausland.

Exportschlager Überwachung

Über die Jahre hat Wladimir Putins Regime ein robustes System aufgebaut, um das Internet zu kontrollieren, die Kommunikation zu überwachen und die Opposition im Land zu verfolgen. Die russischen

Behörden verfügen über neueste digitale Technologien, mit deren Hilfe sie Webseiten mit kritischen und unerwünschten Inhalten aus dem Internet in Russland verschwinden lassen können. So unterliegen seit Beginn des Krieges in der Ukraine am 24. Februar 2022 mehrere tausend Internetseiten der militärischen Zensur, weil der Staat sie als „Fake" bezeichnet oder der Diskreditierung der russischen Armee beschuldigt. Das schränkt die freie Meinungsäußerung massiv ein, und es wird dadurch nicht besser, dass gleichzeitig die Staatspropaganda alle Kanäle beherrscht.

Zudem nutzt der Inlandsgeheimdienst FSB ein mittlerweile berühmt-berüchtigtes technisches System namens SORM, um Informationen aus dem Mobilfunk-, Internet- und Telefonverkehr in Russland zu überwachen, zu speichern und zu filtern. SORM, auch als „Hintertür" des FSB zum russischen Internet bezeichnet, ist allerdings nicht nur in Russland verbreitet: Der Kreml setzt auf die Stärkung von autoritären Kräften in seinen Nachbarländern und versucht, demokratische Bewegungen in ehemaligen Sowjetrepubliken zu untergraben.

So wurde Russland zu einem wichtigen Exporteur von SORM-Technologien nach Kasachstan, Belarus oder Kirgisistan. Diese Länder implementieren zudem aktiv Videoüberwachungssysteme mit Gesichtserkennungsfunktionen, die eine Verringerung der Kriminalitätsrate versprechen, tatsächlich jedoch zu mehr Festnahmen von friedlichen Demonstranten führen. Russische Tech-Unternehmen, die vom Staat kontrolliert sind, konkurrieren in Zentralasien mit chinesischen Firmen, die ebenfalls über hochentwickelte Überwachungssysteme verfügen, mit deren Hilfe sich die Opposition unterdrücken lässt.

Durch Exporte von Überwachungstechnologie stärkt China wiederum autoritäre Staaten in Südostasien und Afrika. In Burundi wurde Huawei-Technik genutzt, um Medien generell zu zensieren, in Nigeria, um oppositionelle Politikströmungen zu unterbinden, und in Kuba, um Inhalte zu unterdrücken, die sich mit den Rechten von lesbischen, schwulen, queeren, bisexuellen, trans- und intersexuellen Menschen beschäftigen.

Peking fördert zudem die Ausbildung von Journalistinnen und Journalisten aus Dutzenden Ländern im Umgang mit digitalen Medien. Dass diese in China einer autoritären Medienumgebung ausgesetzt werden und dieses Gedankengut in ihre Heimatländer mitnehmen, ist durchaus gewollt. Die autoritären Führungskräfte in etlichen afrikanischen Staaten orientieren sich ohnehin stark in Richtung China. Indem Peking diese Kräfte unterstützt, stärkt es seine Position in der Welt.

Cyberkrieg und schmutzige Geschäfte

Russland konzentriert sich in seiner Cyberstrategie anders als China auf disruptive, zerstörerische Eingriffe, oft in Ländern, die man gleichzeitig militärisch attackiert. Russlands Cyberoperationen etwa in der Ukraine waren allerdings nicht so erfolgreich wie erwartet; der große Internetblackout im Land blieb aus. Das ist mindestens zum Teil der Unterstützung der Ukraine durch amerikanische Unternehmen und Behörden zu verdanken; neben Geheimdienstinformationen ist hier die Migration der ukrainischen öffentlichen digitalen Dienste ins Ausland zu nennen.

Eine nicht weniger große Gefahr geht von russischen cyberkriminellen Aktivitäten aus, die vom Kreml toleriert und zuweilen sogar aktiv unterstützt werden. Kriminelle dürfen tun, was sie wollen, solange sie keine Systeme in Russland oder in ehemaligen Sowjetrepubliken

Alena Epifanova
ist Research Fellow am Zentrum für Ordnung und Governance in Osteuropa, Russland und Zentralasien der DGAP.

Dr. Valentin Weber
ist Research Fellow am Zentrum für Geopolitik, Geoökonomie und Technologie der DGAP.

angreifen. Um die 70 Prozent aller Gelder, die mittels Ransomware erbeutet werden – also durch Schadprogramme, die den Computer sperren oder darauf befindliche Daten verschlüsseln –, lassen sich Russland zuordnen; in den vergangenen Jahren handelte es sich dabei um Summen im mittleren dreistelligen Millionenbereich.

Bild nur in Printausgabe verfügbar

Spätestens mit den Angriffen auf Costa Rica 2022, wo der nationale Katastrophenfall ausgerufen wurde, haben Dutzende UN-Staaten Ransomware zur Bedrohung der internationalen Sicherheit erklärt. Tiefere Einblicke in die russische Cyberangriffsmaschinerie erlaubten die vor Kurzem veröffentlichten Vulkan-Files. Sie zeigen, wie stark die russische Privatwirtschaft mit dem nachrichtendienstlichen und militärischen Apparat verzahnt ist.

Derweil nutzt China die internationale Verbreitung chinesischer Technologien für Cyberspionage. So wurde das Hauptquartier der Afrikanischen Union (AU) in Addis Abeba, Äthiopien, gleich zwei Mal Opfer von entsprechenden Angriffen. Ist es ein Zufall, dass dieses Hauptquartier von chinesischen Unternehmen gebaut und digital ausgestattet wurde? Zwischen 2013 und 2018 flossen täglich verdeckt Daten Richtung China, und als das zwei Jahre später erneut geschah, handelte es sich um Aufnahmen von Überwachungskameras auf dem AU-Gelände.

Peking hat sich über die Jahre eine Struktur aufgebaut, die gemeinhin als „Sharp Power“ bezeichnet wird: Die Technologie, die man weltweit verbaut, kann China gegebenenfalls privilegierten Zutritt zu diesen Systemen verschaffen und somit Spionage- oder Sabotageoperationen erleichtern. Sharp Power ist vielleicht nicht so sichtbar wie militärische Macht (Hard Power) oder die Anziehungskraft eines Staates (Soft Power), aber sie kann, verdeckt und im richtigen Moment eingesetzt, erhebliche Wirkung entfalten.

Schuld sind immer die anderen

Während die Regierungen Russlands und Chinas in ihren Ländern das Internet und den generellen Diskurs einer umfassenden Kontrolle unterworfen und demokratische Kräfte weitgehend aus der Politik ausgeschaltet haben, nutzen sie digitale Technologien auch für Desinformationskampagnen. Es geht darum, regierungsnahe Narrative über das Weltgeschehen online zu verbreiten, die Politik von Autokratien zu legitimieren und Zweifel an liberalen Demokratien zu säen. Beide Länder isolieren die eigene Bevölkerung in wachsendem Maße vom globalen Internet – und versorgen sie quasi im Gegenzug mit reichlich Fake News und Propaganda.

Auch international wird China aktiver in Sachen Desinformation und orientiert sich dabei am russischen Vorbild. So erinnerte die Verbreitung mehrerer widersprüchlicher Verschwörungstheorien zu den Ursprüngen des Coronavirus über Social-Media-Accounts von chinesischen Diplomaten und Botschaften an entsprechende Kampagnen Moskaus. Und

Pekings „prorussische Neutralität“ im Ukraine-Krieg spiegelt sich in der Berichterstattung der chinesischen Medien wider. Hier wird das Kreml-Narrativ verbreitet, wonach Moskau notwendige Sicherheitsmaßnahmen als Reaktion auf eine Osterweiterung der NATO und eine aggressive Politik der USA durchführe.

Für die Strategie der russischen und chinesischen Propagandisten, die Aufmerksamkeit auf andere zu lenken oder die Schuld zu verlagern, ist „der Westen“ das ideale Ziel. Wenn er für unterschiedlichste Probleme verantwortlich gemacht wird, findet das Widerhall im Globalen Süden, aber auch bei antiamerikanischen und linken Bewegungen in Westeuropa. Und wenn in der jüngsten gemeinsamen chinesisch-russischen Erklärung zu lesen ist, dass man beabsichtige, „die Zusammenarbeit und den gegenseitigen Informationsaustausch über die Politik in den Bereichen Rundfunk, Fernsehen und audiovisuelle Inhalte im Internet auszubauen“, dann zeigt das, dass Peking und Moskau die Zeichen der Zeit in Sachen Desinformation erkannt haben. Denn nach Angaben des Europäischen Auswärtigen Dienstes basieren Manipulationen mit Informationen im Internet hauptsächlich auf der Verbreitung von Bildern und Videos.

Digitale Seidenstraße

Bei all diesen Aktivitäten spielt es Russland und China immer wieder in die Karten, dass es ihnen gelungen ist, ihre Technologien weit über ihre Grenzen hinaus zu verbreiten. Russische Technologien werden vor allem in postsowjetischen Staaten genutzt, chinesische global. Die aktive Unterstützung beim Aufbau von Überwachungsinfrastrukturen durch Moskau und Peking hilft bei der Verbreitung und Festigung von autoritären Strukturen sowie der Unterdrückung der Opposition. Durch Cyberoperationen verschaffen sich Russland und China einen weiteren Vorteil: Sie nutzen die Asymmetrien des Cyberraums aus, weil sie wissen, dass die Zurechnung von Operationen hier schwierig ist.

China und Russland ist es gelungen, ihre Technologien weit über ihre Grenzen hinaus zu verbreiten

Auch im Informationsraum machen Peking und Moskau Gebrauch von kaum regulierten digitalen Plattformen. Sie nutzen geschickt die Grundelemente der Demokratie wie das Recht zur freien Meinungsäußerung zu ihren Gunsten. Während sie demokratische Strukturen unterwandern, bauen China und Russland ihre eigenen Strukturen im Ausland auf. China insbesondere prescht mit seiner digitalen Seidenstraße vor, die der Verbreitung von chinesischen technologischen Standards und Technologien dienen soll. So wird beispielsweise die Einführung des chinesischen Satellitennavigationssystems Beidou entlang der Seidenstraße gefördert. Auf russischer Seite hat der Angriffskrieg gegen die Ukraine die Entstehung eines russischsprachigen, staatlich kontrollierten Internets beschleunigt.

Das Aufkommen russischer und chinesischer Alternativen zu westlichen technologischen Strukturen ist ein Merkmal der entstehenden multipolaren Weltordnung – einer Ordnung, in der Technologien nicht nur im Dienste der Demokratien stehen, sondern auch von Autokratien für die Durchsetzung ihrer Interessen genutzt werden. IP