ASIEN 16.05.2019 | Janjira Sombatpoonsiri

Das Arsenal der Cyber-Waffen

Autokratische Regierungen nutzen zunehmend Gesetze zur Regulierung des Internets, um ihre Gegner zu unterdrücken.

Lesen Sie diesen Text auch auf Englisch.

In den letzten Jahren mussten die Autokraten dieser Welt beobachten, wie Proteste der Bevölkerung - von den Farbrevolutionen in der ehemaligen Sowjetunion bis zum Arabischen Frühling - die Macht ihrer Amtskollegen in Frage stellen. Sie reagieren darauf mit rechtlichen Maßnahmen, um zivile Gruppen, einschließlich prodemokratischer Bewegungen und nichtstaatlicher Menschenrechtsorganisationen, außer Gefecht zu setzen. Zu den einschneidendsten Maßnahmen gehören solche, die es Behördenvertretern ermöglichen, die Online-Aktivitäten von Aktivisten zu überwachen und zu ahnden.

Zwar stellen Durchgriffe von Sicherheitskräften in der Öffentlichkeit nach wie vor ein ernstes Problem dar. Doch haben autokratische Regime in den letzten Jahren zunehmend auf rechtliche und bürokratische Instrumente gesetzt, um ihren Gegnern das Leben schwer zu machen. So haben viele Länder – darunter Kambodscha, China, Ägypten, Äthiopien, Jordanien, Russland, Tansania, Thailand, Usbekistan und Venezuela – die Vorschriften für die Registrierung von Organisationen, für Finanzierungen aus dem Ausland und öffentliche Versammlungen verschärft.

Autokratische Regierungen haben zudem umfassend von bestehenden Gesetzen Gebrauch gemacht, die vage definierte Straftaten wie Diffamierung und Aufwiegelung verbieten, und auch von der Anti-Terror-Gesetzgebung. Und jetzt ergänzen sie ihr Unterdrückungsinstrumentarium um Internet-Gesetze. Natürlich haben die meisten Länder Gesetze erlassen, die Cyberkriminalität, Datenschutz und finanzielle Transparenz im Internet betreffen, und das aus gutem Grund. Aber autokratische Regime entwickeln solche Gesetze oft, um ihre Gegner in Schach zu halten – insbesondere mithilfe von mehrdeutigen Formulierungen.

Zunehmend werden Gesetze, mit denen vorgeblich die Verbreitung von Falschinformationen verhindert werden soll, gegen politische Gegner eingesetzt.

Bei der Identifizierung, wer eine Bedrohung im Cyberspace darstellt, können sich solche Gesetze etwa auf Gruppen oder Einzelpersonen mit „böswilliger Absicht“ beziehen oder auf solche, die „sich dem Staat widersetzen“, „die nationale Sicherheit oder Ideologie gefährden“, „Informationen verzerren, die Panik in der Bevölkerung auslösen“, „Homosexualität oder Lesbianismus befürworten“ oder „staatsfeindliche soziale Bewegungen bilden“. Derart weit gefasste Definitionen ermöglichen es Autokraten, praktisch jeden Dissidenten als Sicherheitsbedrohung darzustellen und damit einen Vorwand für Repressionen zu liefern – und sogar die Unterstützung der Öffentlichkeit zu gewinnen.

In Südostasien gibt es zahlreiche Beispiele für diese Entwicklung. In sieben der zehn Mitgliedsländer des Verbandes Südostasiatischer Nationen existieren verschiedene autokratische Herrschaftsformen: kompetitiver Autoritarismus (Kambodscha, Singapur und Myanmar), Einparteienherrschaft (Laos, Vietnam), absolute Monarchie (Brunei) und Militärregierung (Thailand). Bis 2018 befand sich Malaysia in der Kategorie der kompetitiven autoritären Systeme, die sich Wahlen stellen.

In den letzten zehn Jahren haben diese Länder ihre Gesetzgebung zur Unterdrückung abweichender Meinungen durch Gesetze zur Computer- und Netzsicherheit ergänzt, die alle ähnlich ausgestaltet sind. Kambodschas Internetgesetz, das von einer neuen Cyberkriminalitätseinheit durchgesetzt wird, ist vage formuliert, um die Unterdrückung der freien Meinungsäußerung zu erleichtern. In Singapur gibt es zu diesem Zweck einen Verhaltenskodex im Internet und seit neuestem ein Gesetz zum Schutz vor Online-Fälschungen und Manipulationen. In Myanmar wird dies mit den Internetregeln aus dem Jahr 2000 erreicht, die einschränken, was online veröffentlicht werden darf; dem Telekommunikationsgesetz von 2013, das Online-Verleumdungen kriminalisiert, und dem Gesetz über elektronische Transaktionen von 2004 (geändert 2013), das schwere Strafen für eine lange Liste von nebulösen Straftaten vorsieht.

Ebenso wurden Gesetze, mit denen vorgeblich die Verbreitung von Falschinformationen verhindert werden soll – wie Artikel 65 des Strafgesetzbuches von Laos – gegen Gegner eingesetzt. Während des Wahlkampfes 2018 in Malaysia verabschiedete die Regierungspartei ein Anti-Fake-News-Gesetz, um die Opposition zu schwächen, die trotzdem

den Wahlsieg errungen hat.

Für Aktivisten wird es nicht einfach sein, gegen drakonische Cybergesetze und andere Formen der digitalen Unterdrückung vorzugehen.

Eine zentrale Komponente dieser repressiven Cyber-Strategien ist umfassende Überwachung. Thailands kürzlich verabschiedetes Gesetz zur IT-Sicherheit – das das 2007 verabschiedete und 2016 überarbeitete Gesetz gegen Computerkriminalität ergänzt – ermächtigt den Staat zur Ausweitung der Überwachung und stärkt seine Handhabe gegen vage definierte Cyberangriffe. Die thailändische Regierung – wie auch die Regierungen in Aserbaidschan, Malaysia, Marokko und Katar – hat Berichten zufolge Spyware von Unternehmen gekauft, darunter das in Italien ansässige Hacking Team, die es ihnen ermöglichen würde, sich in die Computer, Mobiltelefone und sogar GPS-Systeme der Bürger einzuhacken.

Anforderungen an die Datenlokalisierung – die Technologieunternehmen zwingen, die Daten der Bürger auf lokalen Servern zu speichern – erleichtern diese Bemühungen. Zusammen mit China, Nigeria, Pakistan und Russland hat Vietnam unlängst solche Anforderungen eingeführt, angeblich um Datendiebstahl zu verhindern. Doch die Speicherung von Daten innerhalb eines Landes ermöglicht es Regierungen auch, Kontrolle darüber auszuüben.

Das im Januar in Vietnam in Kraft getretene Gesetz zur IT-Sicherheit erlaubt es der Regierung, auf lokal gespeicherte Social-Media-Daten zuzugreifen und Inhalte zu entfernen, die als gegen den Staat gerichtet gelten. China geht noch einen Schritt weiter: Mit seinen riesigen Ressourcen ist es in der Lage, fortschrittliche künstliche Intelligenz einzusetzen, um den Datenverkehr zu analysieren und seine Bürger auf diese Weise zu überwachen. Neben Unterdrückung auf Grundlage von Gesetzen hilft die Verwendung von gefälschten Videos („Deepfakes“) und Troll-Armeen Regierungen, ihre Agenda zu propagieren und Aktivisten zu diskreditieren. Cyber-Trolle in Thailand, auf den Philippinen und in Vietnam sollen Berichten zufolge systematisch Mobbing gegen Online-Dissidenten betreiben.

Aktivisten in ganz Südostasien und in Autokratien auf der ganzen Welt bekommen die Folgen dieser Initiativen zu spüren. Malaysias Kommunikations- und Multimediengesetz wurde 2017 in mindestens 38 Fällen zur strafrechtlichen Verfolgung von Personen wegen Kritik an den

Behörden oder der Monarchie herangezogen. In Myanmar wurden seit 2013 mehr als hundert Fälle nach dem Telekommunikationsgesetz verhandelt, und allein 2016 wurden 54 Personen strafrechtlich verfolgt und acht wegen der Äußerung abweichender Meinungen in sozialen Netzwerken inhaftiert.

Es besteht Bedarf an einer koordinierten globalen Reaktion, um den Raum für zivilgesellschaftliches Handeln zu schützen.

Die thailändische Junta hat mehrere Dutzend Bürger inhaftiert, weil sie „sensible" Informationen auf sozialen Netzwerkseiten geteilt haben. Angesichts der bevorstehenden Wahlen 2019 hat die Militärregierung das Gesetz gegen Computerkriminalität genutzt, um unbegründete Anschuldigungen gegen Oppositionsparteien zu erheben und gleichzeitig über die Fake News ihrer eigenen Trolle hinweggesehen. In Vietnam, wo in den Jahren 2017-18 Hunderte von Dissidenten wegen angeblich staatsfeindlichem Aktivismus - sowohl online als auch offline - angeklagt wurden, wird das neue Internetsicherheitsgesetz die Situation nur noch verschlimmern.

Für Aktivisten wird es nicht einfach sein, gegen drakonische Cybergesetze und andere Formen der digitalen Unterdrückung vorzugehen, nicht zuletzt, weil es sich dabei immer noch um Neuland handelt. Aber das hat einige nicht davon abgehalten, es zu versuchen. Und schon jetzt haben Proteste wie in Südkorea mit gewissem Erfolg eine verstärkte rechtliche Aufsicht bewirkt. Viele Gruppen, die sich für politische Bildung engagieren, setzen zudem auf mehr digitale Kompetenz, damit Bürger dazu beitragen können, den Missbrauch von Internetgesetzen zu erkennen.

Auf internationaler Ebene haben Netzwerke von Interessengruppen demokratische Regierungen und internationale Organisationen dazu veranlasst, Druck auf autokratische Regime auszuüben. Aber es besteht auch Bedarf an einer koordinierten globalen Reaktion, um den Raum für zivilgesellschaftliches Handeln zu schützen. Nur durch anhaltenden öffentlichen Druck können wir hoffen, autokratische Regime davon zu überzeugen, ihre Netzpolitik zu überarbeiten oder rückgängig zu machen.

Aus dem Englischen von Sandra Pontow.

(c) Project Syndicate



Janjira Sombatpoonsiri
Berlin

Janjira Sombatpoonsiri lehrt als Assistenzprofessorin für Politikwissenschaft an der *Thammasat*-Universität und Mitarbeiterin am *German Institute of Global and Area Studies*.