Körber-STIFTUNG
Forum für Impulse

Deutscher Studienpreis
Der Wettbewerb für junge Forschung

Dr. Anita Gohdes

»Repression 2.0: Das Internet im Kriegsarsenal moderner Diktatoren?«

Der vorliegende Beitrag wurde beim Deutschen Studienpreis 2015 mit einem 1. Preis in der Sektion Sozialwissenschaften ausgezeichnet. Er beruht auf der 2014 an der Universität Mannheim eingereichten Dissertation »Repression in the Digital Age: Communication Technology and the Politics of State Violence« von Dr. Anita Gohdes.

Repression 2.0: Das Internet im Kriegsarsenal moderner Diktatoren?

Dr. Anita Gohdes

Einleitung

Wenige Wochen bevor sich im März 2011 politische Massenproteste über ganz Syrien erstreckten, entschied sich das von Präsident Bashar Al-Assad geführte Regime dazu, eine große Anzahl von bis dato gesperrten digitalen Sozialen Netzwerkplattformen wie Facebook und YouTube für seine Bürger_innen zugänglich zu machen. Bis zu diesem Zeitpunkt hatte das Assad-Regime die mit Abstand prohibitivste Medien- und Telekommunikationspolitik des Nahen Ostens verfolgt. Die Aufhebung einer solchen Beschränkung war die Wahl einer politischen Option, die andere repressive Staaten, darunter China, bis heute strikt ablehnen und aktiv unterbinden. Plötzlich sah sich die syrische Bevölkerung mit neuen, digitalen Formen politischer Meinungsäußerung konfrontiert, in denen sie ihrer Wut gegenüber der despotischen Herrschaft Ausdruck verleihen konnte. Die Proteste wurden von Beginn an von der Hoffnung begleitet, dass eine neue Öffentlichkeit auch eine neue Politik entstehen lassen könnte. Warum aber sollte diese Veränderung nicht auch für das autokratische Regime selbst gelten? Ist es nicht abwegig, dass machthungrige Staaten, mit De-facto-Kontrolle über den Zugang zu sozialen Medien, teilnahmslos zusehen, wie Bürger_innen sich dieser neuen Werkzeuge bedienen, um ihre politische Autorität zu untergraben?

Die vorliegende Dissertation untersucht erstmalig theoretisch und empirisch den Zusammenhang zwischen staatlich implementierten Internetkontrollen und staatlich gewaltsamer Unterdrückung. Sie liefert einen entscheidenden Beitrag zum Verständnis der heutigen und zukünftigen Dynamik von Protest und Repression im digitalen Zeitalter. Hierbei legt sie den Fokus auf das Zusammenspiel zwischen staatlich implementierten Kontrolltechniken des Internets einerseits und staatlicher Gewalt gegenüber der Zivilbevölkerung andererseits. Die zentrale These dieser Arbeit besagt, dass die Art der gewählten Internetkontrolle die *Höhe und Form* der staatlichen Gewaltausübung beeinflusst. Sie zeigt somit, dass die scheinbare politische Öffnung eines autokratisch geführten Staates mit veränderten Formen der Gewaltausübung gegen die beherrschte Bevölkerung einhergeht. Im ersten Schritt veranschaulicht sie in einer global

vergleichenden Analyse, dass Regierungen, die Internetkontrollen mit umfassender Zensur betreiben, in einem höheren Maß Menschenrechte (Tötungen, Folter, politische Inhaftierung) verletzen als Regierungen, die keine politisch motivierten Netzwerkunterbrechungen veranlassen. Im zweiten Schritt widmet sie sich zwei detaillierten quantitativen Untersuchungen des immer noch andauernden syrischen Bürgerkriegs. Diese zielen auf Erkenntnisse über die Mechanismen ab, mit denen das Assad-Regime Zensur und Überwachung als Kriegswaffe einsetzt. Dazu stellt sie eine völlig neu erarbeitete Datenbank vor, die die Opfer des syrischen Regimes dokumentiert. Teile dieser Datenbank wurden im Auftrag des *UNO-Hochkommissariats für Menschenrechte* erstellt und in einer Reihe von Reporten veröffentlicht.[1]

Die Ergebnisse stellen die vorwiegend positiven Narrative zur digitalen Revolution kritisch in Frage. Sie tragen somit wesentlich zu unserem Verständnis von staatlicher Repression im 21. Jahrhundert bei. Schon die weitreichenden Enthüllungen durch den Ex-NSA-Mitarbeiter Edward Snowden haben demonstriert, in welchem Maße staatliche Institutionen in der Lage sind, digitale Kommunikation unerkannt einzusehen und zu speichern. Es ist bisher jedoch nicht klar gewesen, in welcher Weise Kontrolltechniken des Internets von großem Wert für despotische Staaten sein können, insofern sie diese als Instrument der Unterdrückung der eigenen Bevölkerung zu nutzen wissen. Die Bedeutung dieser Arbeit spiegelt sich in ihrer öffentlichen und wissenschaftlichen Resonanz wider. Auf Einladung wurden Teile dieser Ergebnisse an der Yale University (USA) und beim 31. Kongress des Chaos Computer Clubs in Hamburg vorgestellt sowie in einer international hochrangigen Fachzeitschrift veröffentlicht. Unter dem Aspekt „Das Internet als Kriegswaffe“ haben auch die „Süddeutsche Zeitung“ sowie die „Washington Post“ über die Ergebnisse berichtet.

Der trügerische Diskurs zu sozialen Medien und Demokratisierung

Bis heute wird die Möglichkeit der Vernetzung auf digitalen Plattformen von Sozialwissenschaftler_innen, Politiker_innen und Menschenrechtsgruppen auf der ganzen Welt als Erfolgsgeschichte der Demokratisierung, Befreiung und Mobilisierung gefeiert. Die digitale Vernetzung, so die wiederkehrende Einschätzung, sei ein wirksames Instrument zur Beschleunigung und Stärkung des politischen Wandels hin zum effektiven Kampf gegen repressive Herrschaftsformen aller Art. Unterdrückten Gruppen ermögliche sie, sich endlich ohne große

[1] Price, Megan, Anita R. Gohdes and Patrick Ball. 2014. „Updated Statistical Analysis of Documentation of Killings in the Syrian Arab Republic.“ *Report commissioned by the Office of the UN High Commissioner for Human Rights.*

finanzielle Ressourcen zu organisieren und zu wehren. Diese Hoffnung teilte auch die amerikanische Regierung: Das US-Außenministerium erachtete die Rolle von sozialen Medien im Kampf für die Demokratisierung autokratischer Staaten als so essenziell, dass es 2009 Twitter offiziell bat, geplante Wartungsarbeiten zu verschieben, um Aktivist_innen während der Proteste im Iran vollen Zugang zu allen Kommunikationskanälen zu ermöglichen. Ein ehemaliger stellvertretender Berater des Nationalen Sicherheitsrats des Weißen Hauses ging so weit zu behaupten, dass Twitter als „weiche Waffe" der Demokratie einen Friedensnobelpreis erhalten sollte.[2] Zwei Jahre später, als zivile Aufstände sich wie ein Lauffeuer im gesamten Nahen Osten sowie im arabischen Maghreb verbreiteten, wurden soziale Medien zur wirksamsten Waffe der neuen Protestbewegung erklärt. Journalist_innen und Wissenschaftler_innen verkündeten, dass im 21. Jahrhundert die Revolution *getweeted* wird – eine Anspielung auf die in den 1970er Jahren entstandene Version, dass die Revolution nicht im Fernsehen übertragen werde.

Die vorliegende Dissertation zeigt, dass diese Perspektive auf die *digitale Revolution* über die Widersprüche und Gefahren hinwegtäuscht, die sich für die protestierenden Bevölkerungen ergeben. Während sich die öffentliche Aufmerksamkeit auf die demokratisierenden Elemente der sozialen Medien konzentriert, haben in den letzten zwei Jahrzehnten Regierungen auf der ganzen Welt kontinuierlich ein Arsenal an Techniken entwickelt, das die Überwachung, Manipulation und Zensur des digitalen Informationsflusses auf vielfältige Weise ermöglicht. Autokratische Mächte unterliegen nicht einfach einem einseitig wirksamen Wandel der demokratischen Öffnung, der durch die sozialen Medien angetrieben wird. Gleichzeitig nutzen sie die neuen Möglichkeiten des Internets für ihre eigenen Zwecke, um mit gezielten Maßnahmen oppositionelle Kräfte zu kontrollieren oder gar aktiv zu bekämpfen.

Diese Arbeit beschäftigt sich folglich mit der Annahme, dass sich die Gewalt autokratischer Regime durch die digitale Revolution nicht einfach verringert, sondern vielmehr transformiert hat. Um ein paar Beispiele zu nennen: Regierungen von Bahrain bis Vietnam investieren in die Zensur und das Verhaften von digitalen Aktivist_innen und oppositionellen Blogger_innen. Europäische Firmen, die digitale Spähsoftware anbieten, finden in Regierungen von Kuwait bis Mexiko begeisterte Abnehmer, die diese dann zur Überwachung von echten und angeblichen Dissidenten anwenden. Als im September 2014 Proteste im Zentrum von Hongkong ausbrachen, wurde der Zugang zur Bilder-Plattform Instagram blitzschnell von chinesischen Behörden gesperrt, um das Verbreiten

[2] Pfeifle, Mark. 2009. „A Nobel Peace Prize for Twitter?" *The Christian Science Monitor* 6 July.

von Bildern zu unterbinden. Im Mai 2014 erzielte die türkische Regierung kurzzeitig ein Verbot von Twitter, nachdem die Plattform im Zuge der Gezi-Park-Proteste zur populären Nachrichtenquelle geworden war. Staatliche Behörden in Ägypten, im Sudan, in der Demokratischen Republik Kongo und im Iran haben zu verschiedenen Zeitpunkten ihre Internetdienste als Reaktion auf innere Unruhen kurzzeitig eingestellt. Offensichtlich verstehen unter Druck geratene Regierungen die gleichzeitige Brisanz und Opportunität des digitalen Austausches ihrer Bevölkerung. Es ist jedoch nicht klar, wie sich ihre Wahl der Internetkontrolle – von Zensur bis Überwachung – in tatsächlichen staatlichen Gewalttaten widerspiegelt.

Das Dilemma der Diktatur im 21. Jahrhundert

Das historische Aufkommen mehrerer Demokratisierungswellen hat die These gestärkt, dass die globale Ausweitung politischer Öffentlichkeit nach und nach auch zum Verschwinden repressiver Staaten führen wird. Vor dem Hintergrund dieser Erzählung wurden auch die Diktaturen des 20. Jahrhunderts, vom „Dritten Reich" bis zu den Militärjuntas Argentiniens, als bloße Ausrutscher fast schon weltgeschichtlich vorbestimmter Entwicklungstendenzen interpretiert. Obwohl diese Diktaturen Meister der medialen Manipulation waren, hat das Narrativ der unvermeidlichen historischen Kraft von Freiheit und Demokratie bis heute nur phasenweise an Bedeutung eingebüßt. Dabei hätte man schon von den Diktaturen des vergangenen Jahrhunderts lernen können, wie die Manipulation der Medien zum Kerninstrument konzertierter Repressionsstrategien genutzt wird. Erst Zensur und Manipulation der Medien ermöglichen aber die Rechtfertigung und den Einsatz von zielgerichteten Formen staatlicher Gewalt in Zeiten der massenmedialen Vernetzung und Versammlung.

Die digitale Revolution hat die Handlungslogiken und Möglichkeiten der Informationskontrolle und die Rolle, die sie in den Strategien staatlicher Repression spielt, grundlegend verändert. Ein ehemaliger Abteilungsleiter im Ministerium für Staatssicherheit der DDR hat vor Kurzem in einem Interview behauptet, die Überwachungsmethoden der US-amerikanischen NSA wären für den Geheimdienst der DDR „ein wahr gewordener Traum" gewesen.[3] Zu DDR-Zeiten war die Anzahl der abgehörten Telefone aufgrund der begrenzten technischen Kapazitäten limitiert. Das digitale Zeitalter hat diese Überwachungsmöglichkeiten nun vervielfältigt und aus Sicht der autokratischen Staaten die Suche nach neuartigen Lösungsstrategien auf die Agenda gebracht. Es würde heutzutage nicht mehr ausreichen, nationale Print- und Funkmedien zu kontrollieren, um den

[3] Schofield, Matthew. 2013. „Memories of Stasi color Germans' view of U.S. surveillance programs." *McClatchy, Washington D.C.*

Informationsaustausch zwischen potenziellen Dissidenten zu überwachen und zu unterbinden. Vielmehr müssen sich die teilweise überaus persistenten autokratischen Regime des 21. Jahrhunderts den Herausforderungen der digitalen Revolution in einer Art und Weise stellen, die auf die neuen Entwicklungen nicht nur reagiert, sondern von diesen aktiv profitiert.

Das digitale Zeitalter stellt somit Regierungen, die Angst um ihr politisches Überleben haben, vor ein schwieriges Dilemma. Einerseits wird den Dissidenten und Oppositionsgruppen durch den Einsatz von sozialen Medien das Vernetzen, Organisieren und Protestieren erleichtert; andererseits bieten diese Plattformen ein bisher ungeahntes Potenzial an Formen der Überwachung und Manipulation. Ganz allgemein gesprochen hat eine autokratische Regierung des 21. Jahrhunderts somit zwei Handlungsoptionen: Einerseits kann sie Kommunikationsströme über das Internet sperren, um der Opposition die Möglichkeit zu verwehren, Mitglieder anzuwerben und gemeinsame Aktionen zu planen. Damit beschränkt die Regierung jedoch ihre Fähigkeit, diesen digitalen Informationsaustausch zu überwachen, um die zentralen Figuren und Handlungen der Opposition präventiv und effektiv zu identifizieren und zu eliminieren. Andererseits, und das ist die zweite Option, kann die Regierung die Kommunikation über das Internet und in den sozialen Medien weitestgehend zulassen, um diese unerkannt mitzuverfolgen und zum eigenen Vorteil zu nutzen. Beide Strategien der Internetkontrolle – Zensur und Überwachung – können jedoch grundsätzlich nicht zur gleichen Zeit durchgeführt werden, da die Zensur das Anzapfen der Informationen verhindert, die für eine umfassende Überwachung der oppositionellen Entwicklungen nötig wäre. Die Autokratie der digitalen Revolution bewegt sich so auf einem schmalen Grat zwischen Öffnung und Repression, um ebenfalls die neuen Informationsquellen des Internetzeitalters für sich nutzen zu können.

These

Die zentrale These dieser Arbeit besagt, dass die Entscheidung zwischen den eben genannten Handlungsoptionen – Zensur oder Überwachung – über die Form und Höhe der staatlich ausgeübten Gewalt informiert. Die Art der Internetkontrolle beeinflusst die Handlungsmöglichkeiten im Bereich der staatlichen Gewaltausübung. Die Arbeit vertritt somit eine zweifache These. Wenn autokratische Regierungen beschlossen haben, sichtbar und direkt mit umfänglicher Zensur des Internets auf kritische Proteste oder Oppositionsbewegungen zu reagieren, werden sie auch eher bereit sein, ihre Autorität durch ein hohes Ausmaß an Gewalt zu demonstrieren. Umfängliche Zensur – meist verdeutlicht durch das völlige Versperren des

Zugangs zum Internet – führt jedoch auch zum Fehlen von wichtigen lokalen Informationen und limitiert die Möglichkeiten präziser und gezielter Attacken gegen einzelne Oppositionsmitglieder. Ein erhöhtes Aufkommen von *nicht zielgerichteter* Gewalt gegen die Zivilbevölkerung sollte daher mit umfassender Internetzensur einhergehen.

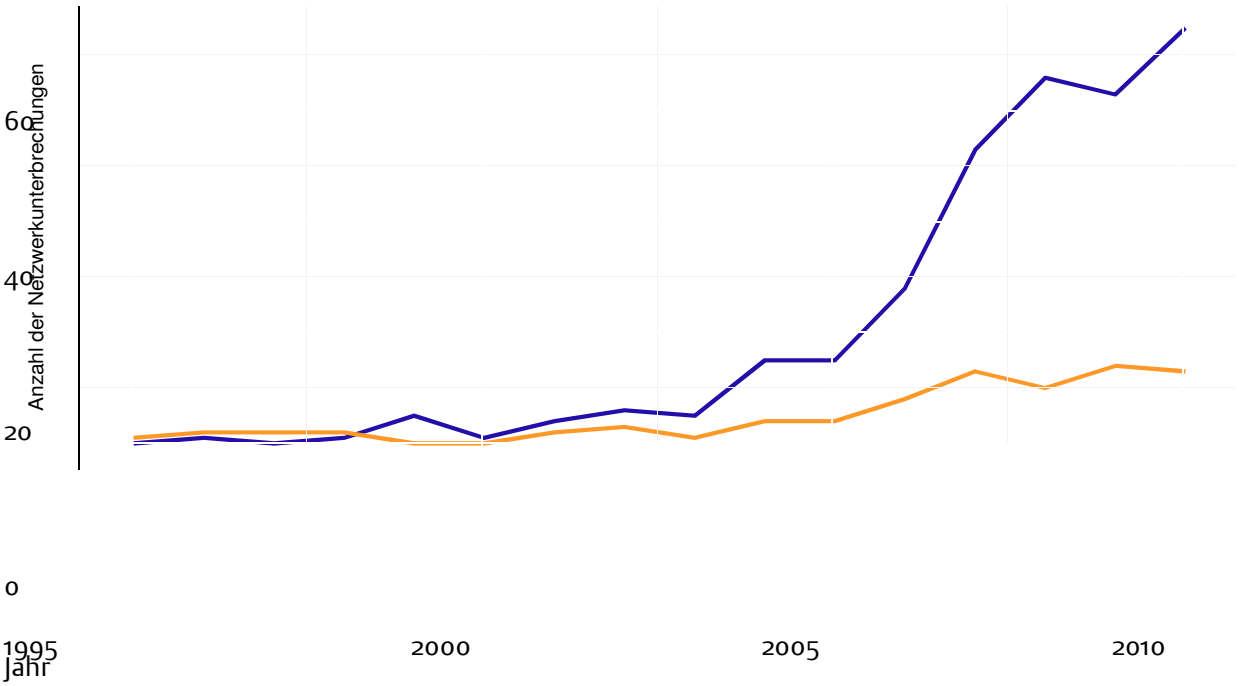
Die Option der Überwachung führt zu anderen Handlungsformen. Wenn autokratische Regierungen versuchen, durch das gezielte Ausspähen von digitaler Kommunikation Informationen über Organisationsstrukturen der zivilen Bevölkerung zu erlangen, um präventiv gegen größere Oppositionsbewegungen vorzugehen, ist ein höheres Aufkommen von *zielgerichteten* und *individualisierten* Gewalttaten zu beobachten. Während autokratische Regierungen mit den Mitteln der Zensur als weniger präzises Mittel gegen mögliche oppositionelle Bedrohungen in der Bevölkerung vorgehen, verfügen sie mit den Mitteln der geheimen Überwachung von Internetkommunikation zusätzlich über die Möglichkeiten zielgerichteter, selektiver Gewalt.

Globale Untersuchung: Netzwerk-Unterbrechungen und Gewalt

Im Rahmen der Fallstudie zum Zusammenhang von neuen Medien und staatlicher Gewalt stellt sich zunächst die global ausgerichtete Frage, ob Regierungen mit einer repressiven Haltung gegenüber der Nutzung des Internets auch darüber hinaus durch Repressionen gegenüber der eigenen Bevölkerung auffallen. Sind Regierungen, die aus politischen Gründen ihren Bürger_innen den Zugang zum Internet versperren, auch in anderen Fragen repressiver? Die globale Analyse, welche die Menschenrechtsbilanz von 171 Ländern im Zeitraum von 1995 bis2010 vergleicht, liefert hierfür empirische Unterstützung. Unter Berücksichtigung der wichtigsten Erklärungsfaktoren für gewalttätige staatliche Repression zeigt die Untersuchung, dass die Umsetzung von Netzwerkunterbrechungen signifikant mit einem häufigeren Verüben von staatlich durchgeführten Tötungen, Folter und politischen Inhaftierungen einhergeht.

Zur Veranschaulichung zeigt die unten stehende Abbildung den globalen Trend von politisch motivierten Netzwerkunterbrechungen zwischen 1995 und 2010. Hierbei zeigt die blaue Linie die Anzahl der jährlichen Unterbrechungen in Ländern mit unterdurchschnittlicher Menschenrechtsbilanz, während die gelbe Linie Sperrungen in Ländern mit überdurchschnittlichem Respekt für Menschenrechte verfolgt. Weltweit steigt die Zahl der Netzwerkunterbrechungen stark an, jedoch ist deutlich zu erkennen, dass zwischen 2003 und 2010 die Anzahl der Unterbrechungen in Ländern mit politischen Tötungen, Folter und Inhaftierungen

um mehr als das Dreifache zunimmt im Vergleich zu anderen Ländern.



Politisch motivierte Netzwerkunterbrechungen und staatliche Repression, 1995-2010.

In vier kurzen Fallstudien wird das Zusammenspiel zwischen Internetkontrolle und Repression näher erörtert. Ägypten, Bahrain, Äthiopien und China liefern hierbei ein breites Spektrum von Regierungstypen und beleuchten, wie die Nutzung von digitaler Zensur und Überwachung unterschiedlich erfolgreich zur Sicherung der politischen Stabilität beigetragen hat. Ägyptens Regierung unter Mubarak wurde im Zuge der Proteste Anfang 2011, welche zum großen Teil über soziale Netzwerke verbreitet wurden, gestürzt. Das Bahrain-Regime sah sich ebenfalls weitreichenden Protesten ausgesetzt, schaffte es jedoch, seine Macht nicht zuletzt durch die Überwachung von Online-Aktivitäten seiner Dissidenten zu erhalten. In Äthiopien, welches zu den am wenigsten digital vernetzten Ländern der Welt gehört, hat die Regierung erhebliche Ressourcen in die Kontrolle des Internets investiert, um potenzielle Revolutionsbewegungen in der kleinen, aber sehr vernetzten Elite des Landes überwachen zu können. Zu guter Letzt stellt Chinas Online-Infrastruktur eines der engmaschigsten und teuersten Systeme zur Verknüpfung von digitaler Zensur und Überwachung dar; die Stabilität des chinesischen Regimes wird nicht zuletzt auf ihre überaus anspruchsvolle digitale Kontrolle zurückgeführt.

Das Internet als Kriegswaffe im syrischen Konflikt

Die zentrale Studie dieser Dissertation beschäftigt sich mit der fortlaufenden Entwicklung des syrischen Bügerkrieges. Noch nie zuvor ist ein Konflikt solchen Ausmaßes so stark durch die sozialen Medien begleitet und dokumentiert worden. Täglich werden Hunderte Ereignisse akribisch erfasst, dokumentiert und via verschiedenster Internetplattformen kommuniziert. Tausende von YouTube-Videos halten Bilder der Toten und Verletzten in Leichenhallen, Krankenhäusern und auf Marktplätzen fest. Aktivist_innen nutzen Twitter und Facebook-Konten, um sich gegenseitig über die militärischen Operationen und Massaker zu informieren und eigene Aktionen zu organisieren und zu koordinieren.

Im Februar 2011, nach Jahrzehnten restriktiver Medienzensur, erkannte das syrische Regime, dass es sich im Verhältnis zum globalen Geschehen in ein Informationsvakuum manövriert hatte. Die syrische Regierung war zunehmend mit dem Problem einer realistischen Einschätzung der eigenen Reichweite und Akzeptanz konfrontiert. Das wirkliche Ausmaß einer möglicherweise anschwellenden Unzufriedenheit innerhalb öffentlich kaum repräsentierter Bevölkerungsteile wurde für die Regierung nur schwer greifbar. Der Assad-Clan benötigte somit dringend neue Strategien, um potenzielle Oppositionskräfte, deren aktuelle Standorte sowie geplantes Protestverhalten zu identifizieren, um Gefahren für das eigene politische Überleben effektiv zu bekämpfen. Ein Teil des Lösungsansatzes eröffnete sich durch die Möglichkeit der Bevölkerung, an überwachbaren sozialen Medien teilnehmen zu können. Das syrische Regime hat seine virtuelle Präsenz konsequent ausgebaut, nicht zuletzt durch seine berüchtigte „Electronic Army“ von Hackern, um mit einer Reihe von Überwachungsprogrammen (sogenannter *Spyware*) gegen die eigene Bevölkerung vorzugehen. Syrische Behörden nutzen dazu unterschiedlichste Tricks. So senden sie beispielsweise unechte Sicherheitszertifikate an Facebook-Nutzer, um deren Passwörter abfangen zu können und um Zugriff auf die soziale Medienpräsenz potenzieller Ziele zu erlangen. Berichten zufolge wurden Zivilisten in Verhören sogar gefoltert, um an Facebook-Passwörter zu kommen. In den letzten vier Jahren hat das Regime aber vor allem in regelmäßigen Abständen den gesamten Zugang zum Netz gesperrt.

Empirischer Ansatz

Um die theoretischen Erwartungen zu überprüfen, nimmt diese Arbeit eine Reihe von empirischen Untersuchungen vor, darunter eine globale, vergleichende Studie, vier kurze Fallstudien sowie zwei

detaillierte quantitative Untersuchungen des aktuellen syrischen Bürgerkriegs. Die Messung von Internetkontrollen und verschiedenen Formen staatlicher Gewalt bringt eine Menge methodischer und empirischer Herausforderungen mit sich. Im Gegensatz zu anderen sozialwissenschaftlichen Feldern mit umfangreichem und präzise erfassbarem empirischem Material bedarf es in diesen beiden Fällen eines passenden methodischen Zugangs, um eine hinreichende Datenbasis zu gewährleisten. Politisch motivierte Gewalt wird teilweise öffentlich und teilweise im Verborgenen ausgeführt. Ebenso sind manche Formen der digitalen Kontrolle sichtbar (wenn z.B. das ganze Netz ausgeschaltet wird), und andere Formen der nuancierten Überwachung (durch spezialisierte Computerprogramme) bleiben geheim. Die vorliegende Arbeit bedient sich einer Reihe innovativer Schätzmethoden sowie der Zusammenstellung eines neuen Datensatzes zu Kriegstoten in Syrien, um diese Probleme zu lösen.

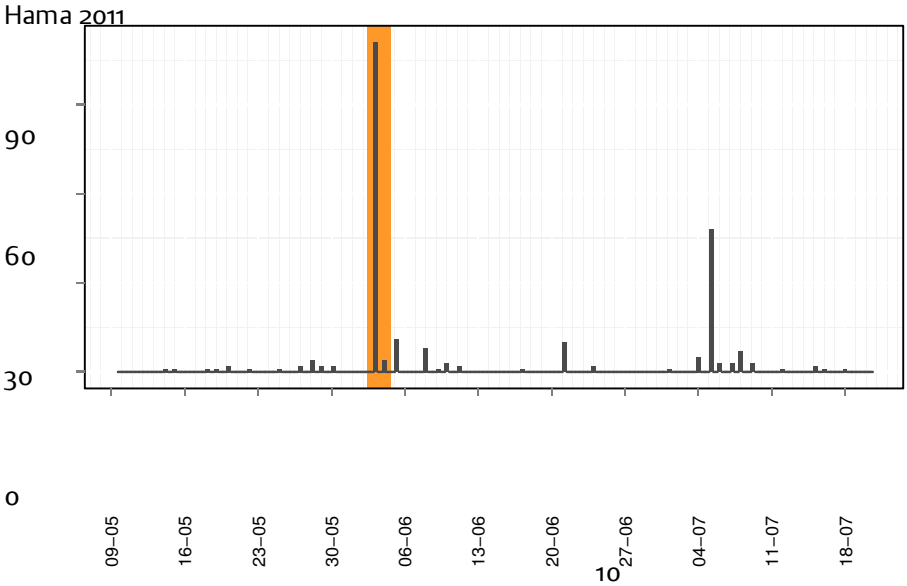
Um den Zusammenhang zwischen Internetzensur und staatlicher Repression zu untersuchen, präsentiert diese Doktorarbeit eine völlig neu erarbeitete Datenbank. Sie greift folglich auf empirisches Material zurück, das in diesem Umfang bisher nicht vorgelegen hat oder gar entsprechend ausgewertet wurde. Die Datenbank vereint alle dokumentierten Tötungen des syrischen Regimes, die zwischen März 2011 und April 2014 von den fünf wichtigsten in Syrien agierenden Menschenrechtsgruppen erfasst wurden, darunter das *Syrian Center for Statistics and Research (SCSR)*, das *Syrian Network for Human Rights (SNHR)*, das *Syrian Observatory for Human Rights (SOHR)*, die Internetseite *Syria Shuhada (SS)* und das *Violations Documentation Centre (VDC)*. Teile dieser Datenbank wurden im Auftrag des *UNO-Hochkommissariats für Menschenrechte* erstellt und in einer Reihe von Reporten veröffentlicht. Die internationale Presse berichtete im August 2014 über den zuletzt veröffentlichten Report, welcher errechnet hat, dass zwischen März 2011 und April 2014 über 191.000 Tote im andauernden Bürgerkrieg dokumentiert worden sind.

Da selbstverständlich nicht alle Gewalttaten beobachtet oder gar dokumentiert werden können, bedient sich die Arbeit einer innovativen statistischen Methode, um die schwankende Dunkelziffer der nicht gemeldeten Tötungen zu schätzen. Hierbei werden die Überschneidungen zwischen den verschiedenen Quellen verwendet, um den Dokumentationsprozess statistisch zu modellieren und für jede Region in Syrien sowie jeden Zeitpunkt die Zahl der nicht dokumentierten Todesfälle akkurat vorherzusagen. Diese Doktorarbeit gehört dabei zu den ersten sozialwissenschaftlichen Arbeiten, die sich dieser Methode bedienen und damit das zentrale Problem lückenhafter Gewaltdaten wissenschaftlich angehen.

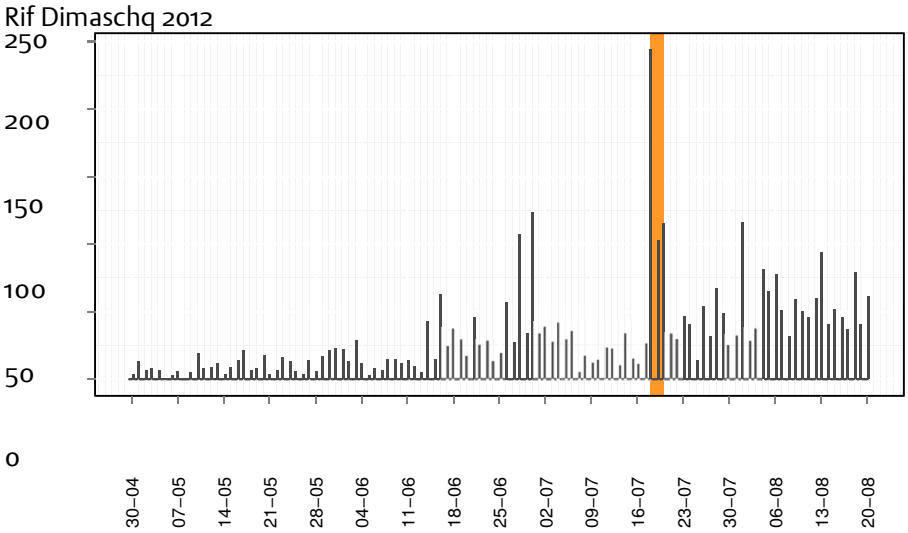
Internetzensur als Militärstrategie

Die erste quantitative Untersuchung zum syrischen Konflikt widmet sich der Frage, ob Internetausfälle mit einer gleichzeitig *höheren Anzahl von Gewalttaten* auftreten. Die theoretische Erwartung ist, dass eine autokratische Regierung einen strategischen Anreiz hat, Internetausfälle in Verbindung mit größeren repressiven Operationen gegen die Oppositionsgruppen einzusetzen. Das zeitweilige Abschalten des Internets führt zu Kommunikationsbrüchen auf Seiten der Opposition und kann so die Koordination von Gegenangriffen erschweren, womit die Position des Regimes gestärkt wird.

Die empirische Untersuchung fragt also, ob die syrische Regierung Internetausfälle mit einem höheren Aufkommen von Gewalttaten verbindet. Die zwei Abbildungen zeigen deskriptive Zeitreihen zur Gewalt in Syrien im Gouvernement Hama Mitte 2011 und im Gouvernement Rif Dimaschq (im Umland von Damaskus) Mitte 2012. In Gelb gekennzeichnet sind die Tage, an denen das Internet von der Regierung unterbrochen wurde. Hier und in einer Reihe weiterer umfangreicher statistischer Untersuchungen zeigt die Arbeit, dass an Tagen, an denen das Internet unterbrochen war, signifikant mehr Regierungsgewalt ausgeübt wurde. Genau genommen sagt das statistische Modell voraus, dass in Syrien an Tagen, an denen das Internet blockiert war, im Schnitt 9% mehr Menschen durch das Regime getötet wurden als an Tagen mit normaler Internetverbindung. Etwas konkreter zeigen die Analysen, dass das Regime im Umland von Damaskus sowie in Aleppo und Homs bei Netzwerkunterbrechungen im Schnitt für fünf zusätzliche Tote pro Tag verantwortlich ist. Diese Berechnungen zeigen deutlich das Ausmaß der Grausamkeiten, die das Assad-Regime höchstwahrscheinlich noch heute täglich begeht.



Gewalt und Netzwerkunterbrechungen, Hama 2011 (Unterbrechung in Gelb).



Gewalt und Netzwerkunterbrechungen, Rif Dimaschq 2012 (Unterbrechung in Gelb).

Eine Analyse der Dunkelziffer der Gewalt vor den und während der Netzwerkstörungen zeigt außerdem, dass es sich hierbei nicht um Verdeckungsstrategien handelte – das Regime also nicht versuchte, seine Gräueltaten durch Internetausschaltung zu verbergen. Vielmehr handelt es sich um militärische Aktionen, die ohne Rücksicht auf Verluste nach dem Verdunkeln der Kommunikationskanäle schonungslos gegen die Bevölkerung durchgeführt wurden.

Internetkontrolle und Gewaltstrategien gehen Hand in Hand

Im zweiten Teil der Analyse zu Syrien beschäftigt sich die vorliegende Arbeit mit der Frage, inwiefern sich neben der *Höhe* der Gewalt auch die *Art* der Gewalt in Zeiten der extremen Internetzensur verändert. Die wichtigste Unterscheidung, die hierbei in der Konfliktforschungsliteratur angeführt wird, ist die Differenzierung zwischen zielgerichteter bzw. *selektiver* sowie nicht zielgerichteter bzw. *willkürlicher* Gewalt. Die konzeptionelle Unterscheidung

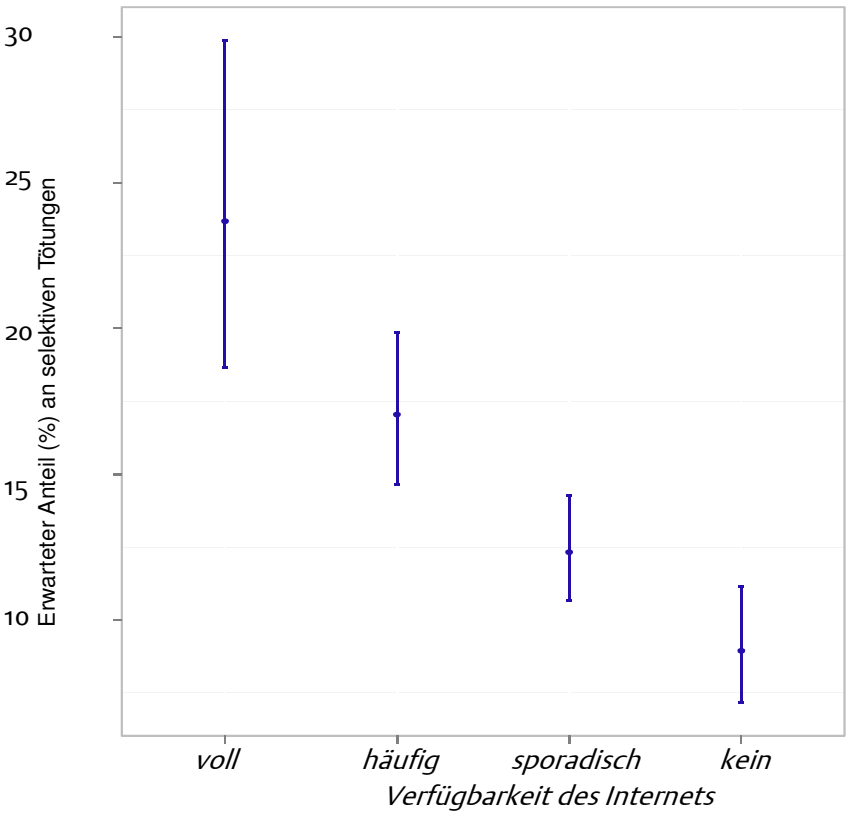
zwischen einerseits selektiver und andererseits willkürlicher Gewalt ist eine etablierte theoretische Kategorisierung. Die empirische Messung und Unterscheidbarkeit beider Phänomene ist jedoch nur sehr schwer nachvollziehbar, da die Intentionen und Motive der Gewaltausübenden in Ex-post-Untersuchungen kaum überprüfbar sind. Die neu erfasste Datenbank zu Kriegstoten in Syrien ermöglicht es, eine nicht nur alternative, sondern adäquatere Messung zur Art der Gewalt vorzunehmen. Zu jedem dokumentierten Opfer stellt die Datenbank eine kurze qualitative Beschreibung der Todesumstände bereit, welche auf die Art der Gewalt schließen lässt. Menschen, die vor ihrem Tod gefoltert wurden, die hingericht oder als Deserteure exekutiert wurden, werden beispielsweise als Opfer selektiver Gewalt klassifiziert. Menschen, die im Zuge von großflächigen Bombardierungen oder Bränden umgekommen sind, werden als Opfer willkürlicher Gewalt klassifiziert.

Um die enorme Anzahl von Fällen im syrischen Bürgerkrieg einzuordnen, bedient sich diese Arbeit der automatischen Textklassifizierung für alle dokumentierten Tötungen. Automatische Textklassifizierung ist eine Form der überwachten, maschinengestützten Lernmethode, bei der ein Algorithmus anhand einer kleinen, handklassifizierten Stichprobe (in dieser Arbeit 2000 Fälle) erlernt, welche Worte im Text auf eine selektive Tötung hindeuten und welche auf eine willkürliche Tötung verweisen. Mit Hilfe der erlernten Funktionen sortiert der Algorithmus die übrigen Fälle in die zwei Klassen „selektive“ bzw. „willkürliche“ Ereignisse ein. Diese neuartige und sehr innovative Art der Gewaltklassifizierung erlaubt es, systematisch und genau zu untersuchen, in welchem Zusammenhang Internetkontrollen und Kriegsstrategien stehen, ohne Rückschlüsse auf die überaus unsicheren Erkenntnisse über Intentionen oder Motivlagen der Gewalt ausübenden Akteure zu ziehen.

Um die Internetkontrollen in Syrien zu messen, wurden Umfragedaten des Syria Digital Security Monitor (SDSM), einem Projekt der kanadischen SecDev Stiftung, verwendet. SDSM interviewt alle zwei Wochen in allen 65 syrischen Distrikten eine feste Anzahl von Befragten nach dem Grad der digitalen Erreichbarkeit in ihrer Umgebung. Die Umfrage bittet die Befragten, ihre digitale Erreichbarkeit (mobil sowie durch DSL) auf einer Skala von 1 bis 4 einzuordnen. Die Skala reicht von „1 = allgemeine Verfügbarkeit“ über „2 = häufige Verfügbarkeit“ und „3 = sporadische Verfügbarkeit“ bis zu „4 = keine Verfügbarkeit“.

Die Abbildung zeigt die statistisch simulierte Erwartung des Anteils (in Prozent) von gezielten Tötungen in Relation zu verschiedenen Graden der Verfügbarkeit des Internets (mit 95% Konfidenzintervall). Die Ergebnisse zeigen, dass ein besserer Internetzugang konsequent zu einer

Erhöhung des Anteils von gezielten Tötungen führt. Umgekehrt ist mit wenig oder keinem Zugang zum Internet ein signifikant höherer Anteil willkürlich ausgeführter Gewalt verbunden. Wo ein freier Internetzugang besteht, ist der erwartete Anteil an selektiven Tötungen durch die Regierung demnach bei mehr als 20% (mit einem Konfidenzintervall von 16,5% bis 26,9%). Nach diesem Modell wird in Regionen, in denen das Internet verfügbar ist und die Regierung über die Möglichkeit verfügt, digitale Kommunikationen auszuspähen, jedes fünfte Opfer selektiv getötet. Mit abnehmender Vernetzung sinkt dieser Anteil deutlich. Ist der Zugang zum Internet in vollem Umfang zensiert, sagt das Modell voraus, dass nur etwa 8% (mit einem Konfidenzintervall von 7,2% bis 10,6%) aller Opfer auf der Grundlage individueller oder kollektiver Eigenschaften gezielt getötet werden. Dies bedeutet, dass 9 von 10 Individuen das Opfer willkürlicher Gewalt sind. Dieser große und signifikante Unterschied in den Gewaltstrategien bietet empirische Unterstützung für die leitende Vermutung und These der vorliegenden Doktorarbeit: Die Wahl der Internetkontrolle geht Hand in Hand mit der Wahl einer geeigneten Gewaltstrategie; je nachdem, ob eine Regierung repressive Strategien der Zensur oder der Überwachung verfolgt, wird sie auf eher willkürliche oder selektive Arten der Gewaltausübung zurückgreifen.



Internetverfügbarkeit und selektive Tötung gehen Hand in Hand.

Fazit

Mit der wachsenden Rolle der neuen digitalen Medien in Protest und Oppositionsbewegungen in der ganzen Welt ist es für bürgergeleitete Demokratisierungsbewegungen von wesentlicher Bedeutung, die Handlungsoptionen und das Kalkül von in Bedrängnis geratenen autokratischen Regierungen zu verstehen und zu antizipieren. Die wachsende Bedeutung von Internetkontrollen im Bereich der staatlichen Repression ist jedoch ein bis dato vollkommen unterentwickelter Forschungsbereich. Die Ergebnisse zeigen eindrücklich, dass eine durchgehend optimistische Perspektive auf die *digitale Revolution* über die Widersprüche und Gefahren hinwegtäuscht, die sich für die protestierenden Bevölkerungen ergeben. Die Arbeit bedient sich zu diesem Zweck einer Reihe innovativer Methoden und neuer Datenquellen, um zu veranschaulichen, wie Zensur und Überwachung Bestandteile des staatlichen Repressionsapparates werden und Hand in Hand mit bestimmten Formen der Gewaltausübungen verwendet werden.

Die digitale Revolution stellt Regierungen, die um ihr politisches Überleben fürchten, vor ein schwieriges Dilemma. Auf der einen Seite bietet die exponentielle Zunahme von privaten, nutzergenerierten digitalen Informationen schier endlose Möglichkeiten für eine neuartige und effektive Überwachung, sodass Spionage, Tracking, Profiling und letztendlich das selektive Eliminieren von als bedrohlich eingestuften Individuen für das Regime plötzlich günstig und effizient wird. Auf der anderen Seite haben Zivilaufstände von Damaskus nach Kairo gezeigt, dass soziale Medien das Potenzial haben, die kollektive Mobilisierung von Demonstrierenden in einer Art und Weise zu vereinfachen und zu verbreiten, wie sie bisher für unmöglich gehalten wurde. Jede Öffnung von digitalen Kommunikationsplattformen birgt somit auch Gefahren für die Stabilität autokratischer Regierungssysteme.

Die Ergebnisse dieser Arbeit zeigen deutlich, dass verschiedene Formen der Internetkontrolle unweigerlich mit bestimmten staatlichen Repressionsstrategien verknüpft sind. Die globale Analyse veranschaulicht, dass Regierungen, die umfassende Internetzensur betreiben, repressiver als andere Staaten sind. Die syrischen Fallstudien legen nahe, dass die Assad-Regierung Internetunterbrechungen generell in Verbindung mit größeren Militäroffensiven einsetzt und in Zeiten solcher extremer Zensur zu härteren Gewalttaten neigt. Die zweite Studie zu Syrien zeigt, dass die Art der staatlichen Gewalt - welche selektiv oder willkürlich ausgeübt werden kann – unweigerlich mit der Art der Netzwerkkontrolle zusammenhängt.

Regierungen in die Verantwortung nehmen

Die hier vorgestellten Ergebnisse zeigen deutlich, dass autokratische Regierungen Internetkontrollen als Teil ihrer Repressionsstrategie gegen die eigene Bevölkerung nutzen. Dies hat wichtige Konsequenzen für den politischen Schutz der Menschrechte und die Gewährleistung der Rechenschaftspflicht für diejenigen, die sie missbrauchen. Ausländische Regierungen und die internationale Gemeinschaft sollten damit beginnen, politisch implementierte Sperrungen des Internets als ernsthaftes Signal zu verstehen; sie sollten dieses Verhalten stark und schnell verurteilen.

Der Handel und Gebrauch von kommerzieller Überwachungssoftware, welche Regierungen unter dem Deckmantel der nationalen Sicherheit zur Identifizierung von möglichen Dissidenten missbrauchen, ist dramatisch angestiegen. Ein Großteil dieser Überwachungssoftware wird hierbei von US-amerikanischen Unternehmen und Firmen mit Sitz innerhalb der Europäischen Union exportiert. Beispiele hierfür sind die italienische Firma *Hacking Team* und das britisch-deutsche Unternehmen *Gamma,* welches die erfolgreiche Software *FinFisher* vermarktet. *FinFisher* ist eine Überwachungssoftware, die in den Rechnern vieler Oppositioneller von Ägypten bis Bahrain gefunden wurde. Die Europäische Union sollte sich einer sorgfältigen und genau regulierten Exportpolitik dieser digitalen Überwachungssoftware annehmen. Analog zu politisch motivierten Exportbeschränkungen bei der Ausfuhr von Waffen an despotische Regime sind politische Reformen im Bereich der Exporte von Überwachungssoftware dringend notwendig.

Praktische Implikationen für Bürger_innen und Aktivist_innen

Einfachen Bürger_innen wie auch marginalisierten Gruppen ermöglicht das Internet, sich ohne große finanzielle Ressourcen zu organisieren, um beispielsweise Kampagnen und Widerstandsbewegungen gegen autokratische Herrscher zu planen. Die Ergebnisse dieser Arbeit demonstrieren jedoch, dass diese neu gewonnene Freiheit ein zweischneidiges Schwert ist: Digitale Fingerabdrücke wie E-Mails, Kreditkartenabrechnungen, Facebook-Einträge und Newsletter-Abonnements können Aktivist_innen auf den Radar despotischer Regierungen setzen, bevor überhaupt sichtbare Demonstrationen stattgefunden haben. Das Erlernen von sicherer digitaler Kommunikation und das Abtauchen in Bereiche außerhalb der Überwachung dieser Regierungen werden für einfache Bürger_innen genauso wichtig, wie es in der Vergangenheit nur für sogenannte „Staatsfeinde“ der Fall war.

Die Ergebnisse dieser Arbeit demonstrieren, dass Regierungen dort, wo das Internet scheinbar frei

nutzbar ist, selektive Formen der Gewalt einsetzen, um potenzielle Gegner_innen auszuschalten. Die Kehrseite der *digitalen Revolution* liegt in der Zunahme zielgerichteter, selektiver Formen der Gewaltausübung von Seiten autokratischer Regime. Das Stärken der digitalen Privatsphäre als Grundrecht jedes Individuums ist somit im Umkehrschluss noch nie wichtiger gewesen als im gegenwärtigen digitalen Zeitalter. Wer die Menschenrechte schützen will, muss daher das Recht auf vertrauliche Kommunikation in digitalen Öffentlichkeiten umso entschiedener verteidigen.