Feinde des Internets 2020

Zum Welttag gegen Internetzensur am 12. März 2020 veröffentlicht Reporter ohne Grenzen (RSF) eine Liste der 20 größten Feinde des Internets. Sie umfasst Behörden, Unternehmen und informelle Netzwerke, die Journalistinnen und Journalisten mit Hilfe digitaler Technologien einschüchtern, bedrohen, überwachen oder zensieren und damit die Informationsfreiheit im Internet gravierend beeinträchtigen.

Die Feinde des Internets bedrohen die Medienfreiheit im digitalen Raum auf viele verschiedene Arten: Sie identifizieren, lokalisieren und überwachen Journalistinnen und Journalisten, die den Mächtigen lästig sind. Sie schüchtern unliebsame Medienschaffende durch systematische Online-Belästigung, Verleumdung und Drohungen ein. Sie bringen kritische Medien durch vielerlei Arten von Zensur zum Schweigen. Und manche Feinde des Internets versuchen, demokratische Staaten zu destabilisieren, indem sie absichtlich Desinformation verbreiten.

Die Liste ist nicht erschöpfend, aber diese 20 Feinde des Internets stehen stellvertretend für die größten aktuellen Bedrohungen der Meinungs- und Pressefreiheit im digitalen Raum: Online-Belästigung, staatliche Zensur, Desinformation und Überwachung. Unter den Feinden des Internets sind neben staatlichen Stellen auch privatwirtschaftliche Unternehmen und informelle Netzwerke wie „Troll-Armeen“ von bezahlten oder freiwilligen Helferinnen und Helfern despotischer Regime. Sie alle stehen für die traurige Realität, dass unabhängig recherchierende oder auf andere Weise unbequeme Journalistinnen und Journalisten im Jahr 2020 Anfeindungen und Angriffen von vielen, oft verdeckt arbeitenden Seiten ausgesetzt sind.

Feinde des Internets auch in demokratischen Staaten

Einige Feinde des Internets arbeiten von repressiven Staaten aus, deren Regierungen ohnehin als Feinde der Pressefreiheit bekannt sind. Andere sind Unternehmen aus demokratisch regierten Ländern wie Deutschland, Spanien, den USA oder Israel, die ihr Geld mit hochspezialisierter digitaler Überwachungstechnologie verdienen.

„Autoritäre Regierungen kennen keine Skrupel, wenn es darum geht, die Möglichkeiten der digitalen Welt zur Sicherung ihrer Macht zu nutzen“, sagte der Geschäftsführer von Reporter ohne Grenzen, Christian Mihr. „Aber zur Wahrheit gehört auch: Die Feinde des Internets haben viele Komplizinnen und Komplizen, und einige davon arbeiten mitten in demokratischen Staaten. Wer sich glaubhaft gegen despotische Regime stellen will, muss auch dafür sorgen, dass diese nicht aus Deutschland und anderen westlichen Staaten mit Instrumenten zur Überwachung und Zensur versorgt werden.“

Die 20 größten Feinde des Internets im Jahr 2020

Online-Belästigung

Modis „Krieger“

LAND: Indien

METHODE: Beleidigungen, Aufrufe zu Vergewaltigungen, Todesdrohungen in sozialen Netzwerken

ZIELE: Millionen **„Yoddhas“** (Krieger) des indischen Ministerpräsidenten Narendra Modi hetzen in sozialen Netzwerken gezielt gegen Kritikerinnen und Kritiker von dessen hindu-nationalistischer Regierung. Einige der Trolle tun dies aus eigenem Antrieb, viele werden von Modis Bharatiya Janata-Partei (BJP) dafür bezahlt. Die Journalistin **Rana Ayyub** schrieb ein Buch über den Aufstieg des indischen Premiers und wurde damit zu einem bevorzugten Gegenstand von Hetze und Belästigung. Ein häufiges Ziel solcher Angriffe ist auch die Journalistin **Swati Chaturvedi**, die ein investigatives Buch über die digitale Troll-Armee im Dienste der Regierung Modi veröffentlicht hat.

Troll-Armeen des Kremls

LAND: Russland

METHODE: Verbreitung falscher Informationen und gefälschter Videos, Veröffentlichung persönlicher Informationen („Doxing“), Verleumdung

ZIELE: Die finnische Investigativjournalistin **Jessikka Aro** wurde selbst zur Zielscheibe der russischen Troll-Armeen, nachdem sie ein Enthüllungsbuch über die Trolle von Präsident Wladimir Putin veröffentlichte. Darin zeigt sie die Mechanismen der Propaganda gegen diejenigen auf, die es wagen, sich kritisch über diese Methoden zu äußern. Professionelle Journalistinnen und Journalisten gehören zu den bevorzugten Zielen der Troll-Armeen. Beispiele dafür sind der russische Journalist **Igor Jakowenko** sowie die in Moskau lebenden ausländischen Journalisten **Isabelle Mandraud**, (ehemalige Korrespondentin von *Le Monde*) und **Shaun Walker** (Korrespondent des *Guardian*).

Jair Bolsonaros „Hasskabinett“

LAND: Brasilien

METHODE: Beleidigungs- und Drohkampagnen in sozialen Netzwerken

ZIELE: Im Dezember 2019 enthüllte eine brasilianische Abgeordnete und ehemalige Mitstreiterin von Präsident Jair Bolsonaro vor einem parlamentarischen Untersuchungsausschuss die Existenz eines "Hasskabinetts". Dabei handelt es sich um eine Gruppe von engen Beratern des Präsidenten, die von dessen Sohn Carlos koordiniert wird und die in den sozialen Medien in großem Stil Hass gegen Journalistinnen und Journalisten schürt. Zu den häufigsten Zielen dieser Kampagnen gehören die Journalistinnen **Patricia Campos Mello** und **Constança Rezende** sowie der Journalist **Glenn Greenwald**, die immer wieder unbequeme Recherchen über die Regierung Bolsonaro veröffentlicht haben.

„Elektronische Fliegen“

LAND: Algerien

METHODE: Die „mouches électroniques“ („elektronischen Fliegen“) des algerischen Regimes melden den Betreibern sozialer Netzwerke massenhaft vermeintliche Verstöße gegen deren Richtlinien, um missliebige Beiträge oder ganze Profile löschen zu lassen. Sie veröffentlichen persönliche Informationen über Journalistinnen und Journalisten („Doxing“), ziehen deren Berichte in Zweifel, überhäufen sie mit feindseligen Kommentaren, persönlichen Angriffen und ehrverletzenden Behauptungen.

ZIELE: Diese von der algerischen Regierung bezahlte Troll-Armee versucht, alle regierungskritischen Journalistinnen und Journalisten zu diskreditieren. Zu den ständigen Zielen ihrer Angriffe gehören Journalisten, die wie **Lamine Maghnine**, **Redouane Boussag** und RSF-Korrespondent **Khaled Drareni** über die seit Monaten andauernden regierungskritischen Hirak-Proteste berichten. Maghnine und Boussag wurden offenbar infolge solcher Angriffe von ihren Facebook-Profilen ausgesperrt.

Troll-Banden

LAND: Mexiko

METHODE: Verunglimpfung, Drohungen und Beleidigungen in sozialen Netzwerken

ZIELE: Mehrere Journalistinnen und Journalisten wurden tagelang zum Ziel von Troll-Angriffen in den sozialen Netzwerken, nachdem sie Präsident Andrés Manuel López Obrador Ende Oktober 2019 in einer Pressekonferenz kritische Fragen zur misslungenen Festnahme eines Sohns des Drogenbosses Joaquín „El Chapo“ Guzmán gestellt hatten. Heftig angefeindet wurde unter anderem **Irving Pineda** vom Fernsehsender *TV Azteca*. Solche Kampagnen werden in Mexiko immer häufiger; oft zielen sie auf Frauen. Im November 2019 geriet zum Beispiel die Journalistin **Silvia Chocarro** ins Visier der Trolle. Sie repräsentierte zu dieser Zeit ein Bündnis von Nichtregierungsorganisationen einschließlich RSF, die sich für Meinungs- und Pressefreiheit einsetzen. Die Trolle verwenden für ihre Angriffe Hashtags wie #PrensaCorupta, #PrensaSicaria und #PrensaProstituida – „korrupte Presse“, „Killer-Presse“ und „Hurenpresse“.

Staatliche Zensur

Roskomnadsor

LAND: Russland

METHODE: Sperrung von Webseiten und Internetdiensten

ZIELE: Die russische Medienaufsichtsbehörde Roskomnadsor hat seit 2012 Hunderttausende Webseiten blockiert. Sie führt eine schwarze Liste verbotener Webseiten, die sie jedoch nicht veröffentlicht. Die Behörde sperrt Nachrichtenagenturen wie *Ferghana News*, investigative Webseiten wie *RussianGate* und politische Online-Magazine wie *Grani.ru, ej.ru* oder *mbk.news*. Roskomnadsor blockiert auch ausländische Online-Plattformen und internetbasierte Dienste, die sich weigern, ihre

Daten auf Servern in Russland zu speichern oder den russischen Behörden Zugriff auf verschlüsselte Nachrichten zu gewähren. So wurden Anfang 2020 mehrere Anbieter verschlüsselter E-Mail-Dienste blockiert.

Hoher Rat für den Cyberspace

LAND: Iran

METHODE: Selektiver Zugang zum Internet; Sperrung von Webseiten, Plattformen und Apps wie Facebook, WhatsApp, Twitter, Telegram und Signal

ZIELE: Der 2012 gegründete Hohe Rat für den Cyberspace setzt sich aus hochrangigen Militärs und Politikern zusammen. Er ist der Architekt des „halalen Internets", eines so weit wie möglich vom Rest der Welt abgeschotteten nationalen Datennetzes. Das weltweite Netz lässt der Rat mit einer Art staatlicher Firewall stark filtern. Immer öfter greift der Hohe Rat für den Cyberspace zu kürzeren oder längeren Internet-Abschaltungen, um Proteste zu unterdrücken und die Verbreitung unabhängiger, vom Regime als subversiv oder konterrevolutionär eingestufter Informationen zu verhindern.

Innenministerium

LAND: Indien

METHODE: Abschaltung des Internets

ZIELE: Am 5. August 2019 ließ das indische Innenministerium die Telefon- und Internetkommunikation in der Provinz Jammu und Kaschmir vollständig abschalten. Mit diesem extremen Schritt hinderte die Regierung Journalistinnen und Journalisten daran, frei zu recherchieren und zu berichten. Zugleich schnitt sie alle Bürgerinnen und Bürger in der Region von unabhängigen Nachrichten und Informationen ab. Erst nach sechs Monaten stellten die Behörden den Zugang zum Breitband-Internet teilweise wieder her. Der Zugang zu vielen Webseiten blieb auch danach noch sehr problematisch. Indien schaltet das Internet so oft wie kein anderes Land komplett ab: allein im Jahr 2019 geschah dies 121 Mal.

Conatel

LAND: Venezuela

METHODE: Sperrung von Webseiten, Plattformen und Apps

ZIELE: Venezuelas Nationale Kommission für Telekommunikation (Conatel) wird indirekt von der Regierung kontrolliert und kann die Sperrung von Webseiten, Online-Plattformen und Apps anordnen, die den Behörden ein Dorn im Auge sind. Viele Nachrichtenseiten wie *infobae.com*, *elpitazo.com*, *dolartoday.com* und *armando.info* wurden dauerhaft geschlossen, ohne dass eine Berufung möglich wäre. Immer wieder sperrt Conatel vorübergehend soziale Netzwerke wie Facebook – besonders dann, wenn dort Reden von Oppositionsführer Juan Guaidó live übertragen werden.

Chinesische Cyberspace-Verwaltung

LAND: China

METHODE: Internetzensur, Überwachung privater Plattformen wie Baidu, WeChat, Weibo und TikTok; Sperrung und Löschung von Inhalten und Anwendungen

ZIELE: Seit dem Beginn der Coronavirus-Epidemie Ende 2019 hat Chinas Internet-Kontrollbehörde ihren Kampf gegen die Verbreitung tatsächlicher und vermeintlicher Gerüchte weiter verschärft. Social-Media-Profile von Medien, Bloggerinnen und Bloggern wurden gesperrt. Mehrere Medien wurden zensiert, darunter *Caijing*, eine in Peking ansässige Zeitschrift, die über offiziell nicht gemeldete Infektionsfälle berichtet hatte.

Hoher Rat für die Medienaufsicht

LAND: Ägypten

METHODE: Sperrung von Nachrichten-Webseiten und Messenger-Diensten

ZIELE: Mit Verweis auf die Verbreitung vermeintlicher Falschmeldungen lässt Ägyptens Hoher Rat für die Medienaufsicht die Webseiten zahlreicher Medien sperren. Unter den mehr als 500 blockierten Seiten sind zum Beispiel Angebote der *BBC*, des arabischsprachigen US-Auslandssenders *Al-Hurra* und von Reporter ohne Grenzen. Ende September 2019 ließ der Rat elf Messenger-Dienste sperren, darunter die verschlüsselten Dienste Wickr und Signal. Der Rat hat auch versucht, den Zugang zur Messenger-App Wire und zum Facebook Messenger zu blockieren.

Desinformation

Force 47

LAND: Vietnam

METHODE: Desinformationskampagnen in sozialen Netzwerken

ZIELE: Die rund 10.000 Personen starke „Cyber-Armee“ unter dem Kommando des Ministeriums für öffentliche Sicherheit spürt „Verstöße“ und „reaktionäre Kräfte“ in den sozialen Netzwerken auf – also alle Kräfte, die in Opposition zur vietnamesischen Regierung stehen. Ein Beispiel ist das Vorgehen der Gruppe nach einer tödlichen Razzia in dem Dorf Dong Tam am 9. Januar 2020, die scharfe Kritik an den Behörden auslöste. Die Force 47 überflutete die sozialen Netzwerke daraufhin mit erzwungenen Geständnissen, in denen Menschen gezeigt wurden, die zugaben, sie hätten Benzinbomben und andere Waffen gebaut, um die Polizei damit anzugreifen.

Callcenter-Kampagnen

LAND: Philippinen

METHODE: Verbreitung falscher oder vorsätzlich irreführender Informationen und Internet-Meme, Online-Einschüchterungskampagnen

ZIELE: Unterstützerinnen und Unterstützer von Präsident Rodrigo Duterte versuchen mit einer Verleumdungs- und Boykottkampagne, eine Lizenzerneuerung für die Fernseh- und Radiosendergruppe *ABS-CBN* zu hintertreiben. Dazu haben sie sogar eine imaginäre Verschwörung unabhängiger Medien angeprangert, die darauf ziele, den Präsidenten zu stürzen. Seit Dutertes Wahlkampf 2016 sind Troll-Armeen auf den Philippinen ein lukratives Geschäft geworden. Sie unterstützen und verstärken die politischen Botschaften von Regierungsmitgliedern, verunglimpfen unabhängige Medien und versuchen, die öffentliche Meinung zu manipulieren.

Troll-Armee

LAND: Saudi-Arabien

METHODE: Verbreitung von Desinformation und Hassbotschaften

ZIELE: Ein Netzwerk regimetreuer Trolle und Bots produziert mehr als 2500 Tweets pro Tag, die derzeit vor allem für die Inhalte des konservativen Satellitenfernsehsenders *Saudi 24* werben. Das Netzwerk wurde auch schon für die Verbreitung religiös motivierter und antisemitischer Hassbotschaften sowie von Verschwörungstheorien über den 2018 ermordeten Exil-Journalisten **Jamal Khashoggi** eingesetzt. Geschaffen wurde diese Troll-Armee von Saud al-Kahtani, dem damaligen engen Berater von Kronprinz Mohammed bin Salman. Al-Kahtani gilt auch als einer der Drahtzieher des Mordes an Khashoggi.

Einheit für den Cyber-Dschihad

LAND: Sudan

METHODE: Spionage in sozialen Netzwerken, Produktion und Verbreitung falscher Informationen

ZIELE: Diese kurz nach dem Beginn des Arabischen Frühlings 2011 gegründete Troll-Armee des sudanesischen Geheimdienstes spioniert in sozialen Netzwerken Aktivistinnen, Politiker, Journalistinnen und Journalisten aus. Außerdem verbreitet sie vor allem über soziale Netzwerke und Messenger-Dienste Nachrichten und Artikel mit falschen Informationen, die darauf abzielen, die Mitglieder der aktuellen Übergangsregierung zu diskreditieren und führende Persönlichkeiten des 2019 gestürzten alten Regimes zu verteidigen.

Überwachung

NSO Group (auch Q Cyber Technologies)

LAND: Israel

METHODE: Die NSO-Überwachungssoftware nutzt eine Sicherheitslücke des Messengers WhatsApp, um sich auf den Smartphones der Zielpersonen zu installieren und diese umfassend auszuspähen

ZIELE: Den Recherchen zweier UN-Sonderberichterstatter zufolge wurde die Software der NSO Group wahrscheinlich von Saudi-Arabien eingesetzt, um den Journalisten **Jamal Khashoggi** mehrere Monate vor seiner Ermordung auszuspähen. Dazu wurden die Smartphones von drei seiner Vertrauten mit dem Überwachungsprogramm infiziert. Auch viele weitere Journalistinnen und Journalisten sind auf diese Weise überwacht worden, darunter **Ben Hubbard** von der *New York Times*, **Griselda Triana**, die Frau des ermordeten mexikanischen Journalisten **Javier Valdez Cárdenas**, sowie mehrere seiner Kolleginnen und Kollegen. Insgesamt sollen 1400 Geräte auf der ganzen Welt über eine WhatsApp-Sicherheitslücke mit Spyware der NSO Group infiziert worden sein, darunter auch das des RSF-Korrespondenten in Indien sowie die Smartphones mehrerer anderer indischer Journalistinnen und Journalisten.

Memento Labs (ehemals Hacking Team)

LAND: Schweiz, Italien, Saudi-Arabien

METHODE: Die Überwachungssoftware von Memento Labs kann von einem Zielgerät Dateien kopieren, E-Mails und Messenger-Nachrichten abfangen sowie Webcam und Mikrofon des Geräts einschalten.

ZIELE: Memento Labs hat eines der beiden Überwachungsprogramme entwickelt, mit denen das Smartphone des *Washington Post*-Eigentümers **Jeff Bezos** ausgeforscht worden sein könnte. Das Unternehmen, das seine Produkte ausschließlich an Regierungen verkauft, hat sich in jüngerer Zeit weitgehend aus den Schlagzeilen herausgehalten. In der Vergangenheit wurden mit einem seiner Spähprogramme Journalistinnen und Journalisten der marokkanische Bürgerplattform *Mamfakinch* sowie des unabhängigen äthiopischen Exil-Fernsehsenders *ESAT* ausgeforscht.

Zerodium (ehemals Vupen)

LAND: USA

METHODE: Aufspüren unbekannter Sicherheitslücken (Zero-Day-Exploits) in verbreiteter Software und Verkauf dieses Wissens an interessierte Dritte

ZIELE: Um bislang unbekannte IT-Sicherheitslücken aufzuspüren, zahlt Zerodium Belohnungen an Hacker und Sicherheitsfachleute, die das Unternehmen exklusiv über solche Funde informieren. Zelodium verkauft dieses Wissen dann nach eigener Darstellung „vor allem an europäische und nordamerikanische Regierungen“ weiter, deren Geheimdienste und Sicherheitsbehörden die Schwachstellen nutzen können, um zum Beispiel in Computer und Smartphones von Terrorverdächtigen einzudringen. Eine solche Sicherheitslücke wurde eingesetzt, um den Blogger **Ahmed Mansur** auszuspähen, der in den Vereinigten Arabischen Emiraten eine der wenigen Quellen für unabhängige Informationen über Menschenrechtsverletzungen war. Nun verbüßt Mansur eine zehnjährige Haftstrafe – unter anderem wegen des Vorwurfs, er habe falsche Informationen veröffentlicht, um dem Ruf des Landes zu schaden.

Mollitiam Industries

Spanien

METHODE: Technologie zum Abhören von Telefongesprächen und E-Mails

ZIELE: Zu den Kunden von Mollitiam Industries gehört unter anderem die kolumbianische Armee. Sie hat die Überwachungstechnologie des Unternehmens genutzt, um Verfassungsrichter, Politikerinnen und Politiker sowie Medienschaffende und deren Informanten auszuspähen. Ziele dieser Überwachung waren zum Beispiel Journalistinnen und Journalisten des Nachrichtenmagazins *Semana*, darunter dessen Chefredakteur **Alejandro Santos**. Das Magazin hatte über Ermittlungen zu Verbrechen und Verfehlungen von Militärangehörigen berichtet.

FinFisher

LAND: Deutschland

METHODE: Überwachungssoftware und „Staatstrojaner", die Zugriff auf Anwendungen und persönliche Daten auf Smartphones ermöglichen, darunter Chatverläufe, Fotos und Ortungsdaten

ZIELE: Das Unternehmen wird verdächtigt, sein Spionageprogramm FinSpy illegal an die Türkei verkauft zu haben, die damit Medienschaffende sowie Aktivistinnen und Aktivisten ausspioniert hat. Die Software wurde auf einer gefälschten Version der türkischen Oppositionswebseite Adalet gefunden, mit der Aktivistinnen und Aktivisten ihre Proteste gegen den türkischen Präsidenten Recep Tayyip Erdogan im Sommer 2017 koordinierten. Reporter ohne Grenzen und drei weitere Organisationen haben deshalb Strafanzeige gegen das Unternehmen gestellt, das die Vorwürfe bestreitet. Die Ermittlungen sind noch nicht abgeschlossen.