

Auch in Afrika sind wir nicht sicher vor High-Tech-Überwachung



Überwachungskamera in Flic-en-Flac, Mauritius ¹

* * *

Günther Lanier, Ouagadougou 8. November 2023²

* * *

Dass es illegal ist, hält Mächtige selten davon ab, etwas zu tun, was ihnen beim Erhalt der Macht hilft. Da werden auch keine Kosten gescheut.

Das *Institute of Development Studies/IDS* (Institut für Entwicklungsstudien)³ hat im September 2023 eine Studie⁴ herausgegeben, die sich mit der Frage der Überwachung in Afrika befasst, genauer gesagt in fünf afrikanischen Staaten: Nigeria, Ghana, Marokko, Malawi und Sambia. Geplant waren zehn Länder, doch in Ägypten, Algerien, Äthiopien und Tunesien erwies sich das Unterfangen als zu gefährlich für die ForscherInnen, musste abgebrochen werden. In der Côte d'Ivoire hinderten persönliche (gesundheitliche) Gründe den Forscher/die Forscherin an der Realisierung einer Länderstudie⁵.

Hier ein Kurzüberblick über die Ergebnisse:

	Sambia	Malawi	Marokko	Ghana	Nigeria
Internet-Überwachung					
Überwachung der mobilen Telefonie					
Monitoring der sozialen Medien					
Sichere Stadt/Smarte Stadt					
Biometrische Erkennung					
		über 100 Mio USD jährlich			
		10-100 Mio USD jährlich			
		unter 10 Mio USD jährlich			
		kein Beleg für Überwachung			

6

¹ Foto Benoît Prieur 4.3.2020, leicht zugeschnitten GL,

https://commons.wikimedia.org/wiki/File:Cam%C3%A9ra_de_surveillance_dans_une_rue_de_Flic-en-Flac.jpg.

² Petra Radeschnig gilt – wie stets – mein herzlicher Dank fürs Lektorieren!

³ Das der University of Sussex in Brighton (südlich von London) angeschlossene IDS dient der Forschung und der Ausbildung.

⁴ Tony Roberts et al., *Mapping the supply of surveillance technologies to Africa: case studies from Nigeria, Ghana, Morocco, Malawi, and Zambia*, Brighton (Institute of Development Studies) September 2023 (ab sofort "Tony Roberts et al."), DOI: 10.19088/IDS.2023.027. Herunterladbar auf <https://opendocs.ids.ac.uk/opendocs/handle/20.500.12413/18120>.

⁵ Ebd., p.14.

⁶ Angelehnt an die Tab.1.1 ebd., p.7.

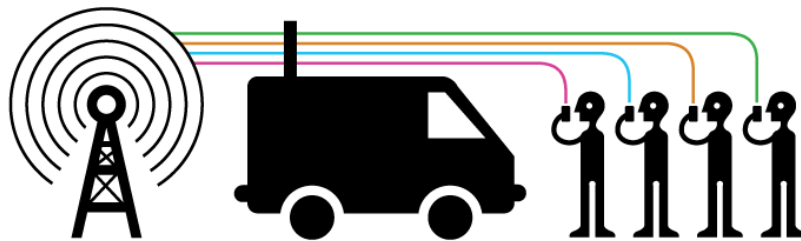
Theoretisch sind Freiheits- und Privatsphäre der Menschen umfassend geschützt, angefangen von der Allgemeinen Erklärung der Menschenrechte von 1948 bis zu den nationalen Verfassungen. Die Überwachung, um die es in dieser Studie geht, ist illegal. War Überwachung früher extrem aufwendig, so hat die Digitalisierung Massenüberwachung von Kommunikation ermöglicht. Seit den Enthüllungen von Edward Snowden 2013 wird dem Thema im Globalen Norden erhöhte Aufmerksamkeit geschenkt.

Doch auch afrikanische Länder sind betroffen.

Trotz Menschenrechtsschutzes auf nationaler, kontinentaler und globaler Ebene verletzen auch afrikanische Staaten routinemäßig die in den Verfassungen garantierten Rechte ihrer BürgerInnen auf Freiheits- und Privatsphäre.

Damit etwas dagegen getan werden kann, muss zuerst bekannt sein, was überhaupt Sache ist. Dem soll dieses *Mapping*, diese Bestandsaufnahme dienen. Da es sich vielfach um Geheiminformationen handelt, ist von vornherein klar, dass die gebotenen Infos nicht vollständig sein können – sie sind zu lesen als Mindestwerte: was nachgewiesen werden konnte⁷.

Wie aus der Tabelle hervorgeht, befasste sich die Studie mit fünf Sorten von Überwachung: Internet-Überwachung betrifft E-Mails, Sofortnachrichten, Internetsurfen und Browserverlauf. Legal ist eine solche Überwachung nur, wenn eine richterliche Genehmigung ausgestellt wurde. Bei der Überwachung der mobilen Telefonie geht es um das Ausspionieren von Anrufen, Textbotschaften, Sofortnachrichten und Internetkommunikation unter Verwendung eines Mobiltelefons. Um legal zu sein, braucht solche Überwachung abermals einer richterlichen Erlaubnis. Jenseits der Legalität gibt es Handy-Malware (ein bekanntes Beispiel solcher Schad-Software war das Pegasus-Spionage-Programm) oder Handy-Masten-Simulatoren (auch IMSI Catcher oder Stingray genannt), wo sich Geräte als Handy-Masten gerieren, Handys sich mit ihnen verbinden und so Kommunikation ausspioniert wird.



links der eigentliche Handy-Mast; ein *Cell-site simulator* = *Stingray* = *IMSI catcher* schaltet sich zwischen diesen und die Handy-NutzerInnen⁸

Beim Monitoring der sozialen Medien werden auf der Basis von Überwachung gezielt Botschaften an Individuen gerichtet, die Ansichten und Verhalten beeinflussen sollen. Google, Facebook et al. haben überwachungs-basiertes Werben (*surveillance advertising*) als Geschäftsmodell. Da passt es gut dazu, wenn britische und US-amerikanische politische Marketing-Unternehmen afrikanische Regierungen mit Wahl-Beratung zur Seite stehen, z.B. Cambridge Analytica in Nigeria und Kenia und Bell Pottinger, ebenfalls eine britische Firma, in Südafrika⁹.



Überwachungskamera unweit des Bahnhofs in Thiès, Senegal¹⁰

⁷ Siehe ebd., p.12.

⁸ Bild Electronic Frontier Foundation (EFF), <https://www.eff.org/de/pages/cell-site-simulatorsimsi-catchers>.

⁹ In Tony Roberts et al., p.16.

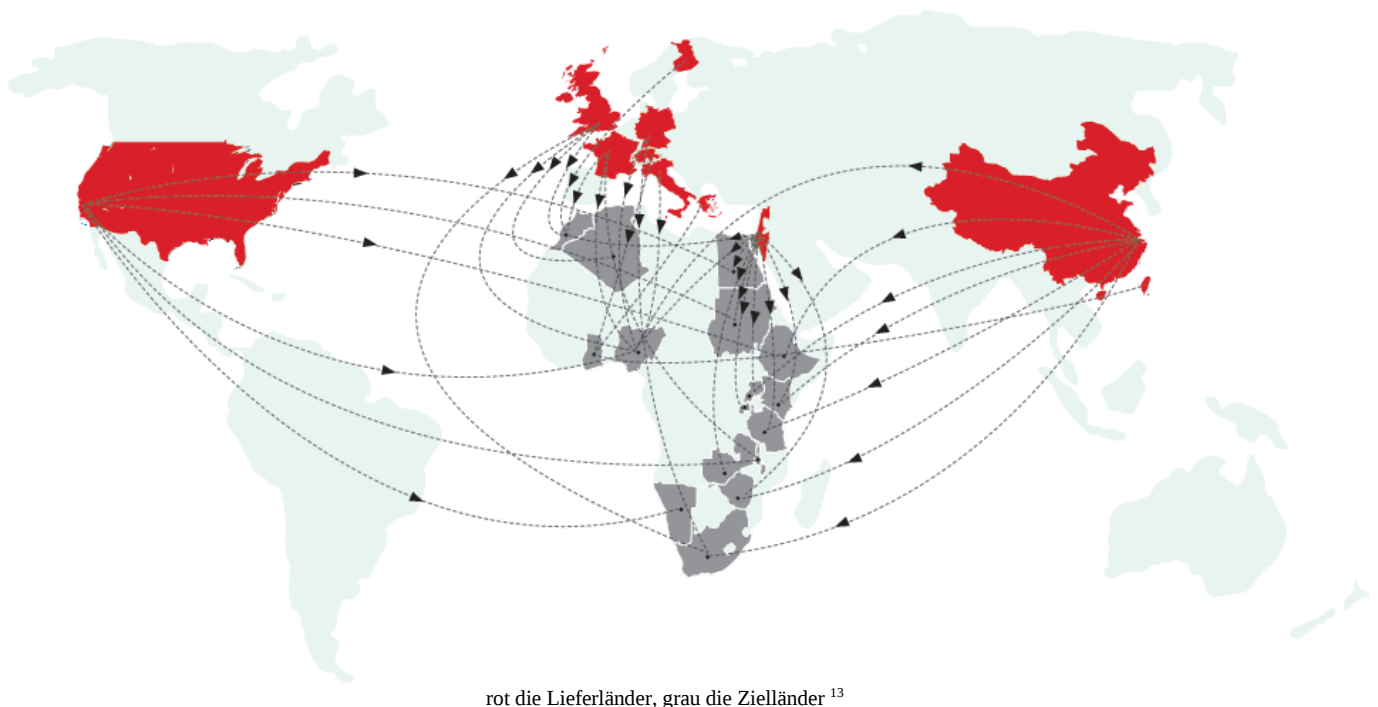
¹⁰ Foto Babacar Dioum 7.4.2020, leicht überarbeitet GL, https://commons.wikimedia.org/wiki/File:Surveillance_camera_in_public_roads.jpg.

Im Bereich “Sichere Stadt/Smarte Stadt“ ist China besonders aktiv. Kreditbasiert werden im Rahmen von Huawei- und ZTE-Video-Überwachungspaketen tausende Kameras mit Gesichts- und Kfz-Kennzeichenerkennungsfähigkeit installiert. Meist werden die Daten von den Sicherheitskräften in einem gleichzeitig eingerichteten Kommando- und Kontrollzentrum ausgewertet. Auch die US-amerikanische Firma Honeywell bietet solche Technologie an und hat sie z.B. nach Ägypten geliefert¹¹. Es gibt verschiedene Arten von Überwachungskameras – auf dem Foto zu Beginn des Artikels aus Mauritius und auf dem soeben gezeigten vom Senegal handelt es sich um PTZ (*Pan Tilt Zoom*)-Kameras, die ein ferngesteuertes Drehen, Kippen und Zoomen erlauben¹².

In der Biometrie geht es um Fingerabdrücke, Iris- oder Gesichtserkennung. Systeme, die auf solch biometrischer Erkennung basieren, werden von vielen afrikanische Regierungen implementiert, oft an die Handy-Verwendung und mobile Geld- oder Bankoperation gebunden oder nötig zum Erhalt von Pässen, Führerscheinen, zum Bezug von Leistungen von Gesundheitsdiensten, Sozialleistungen und anderen staatlichen Diensten.

Da viele rund um die Uhr ihre Handys bei aktivem GPS eingeschaltet lassen, eröffnet das ungeahnte Möglichkeiten der Überwachung in Sachen Geolokalisation, Kommunikation, Finanztransaktionen, Internet-Surfen, Posts und Likes in sozialen Netzwerken usw.

Hier eine kartographische Darstellung der Lieferländer von Überwachungstechnologie an ausgewählte afrikanische Länder:



Unter den fünf behandelten Ländern konsumiert Nigeria bei weitem am meisten Überwachungstechnologie. Zwischen 2013 und 2022 wurden dafür mindesten 2,7 Mrd. USD ausgegeben. Oppositionelle, JournalistInnen und die Zivilgesellschaft haben das zu spüren bekommen¹⁴.

Was die Internet-Überwachung betrifft, hat Abuja sich insbesondere bei Elbit (einem israelischen Unternehmen, das Waffen-, Kommunikations- und Aufklärungssysteme liefert; 40 Mio USD), Romix (Zypern), Packets Technology (Bulgarien) und Hacking Team (Italien) eingedeckt.

Bei der Spionage qua Mobiltelefon half und hilft Ware für insgesamt mindestens 18 Mio USD von FinFisher (GB/Deutschland), Mi Marathon (Australien), Cellebrite (Israel), Circles (Bulgarien/Israel), MPD Systems (USA) und Nice Security (GB).

Das britische Cambridge Analytica hat bei den 2015er Wahlen für 2,8 Mio USD Facebook-Daten ausgewertet, um das Wahlverhalten zu beeinflussen. Seither sind an zwei andere nicht genannte Firmen deutlich größere Beträge gezahlt worden – insgesamt über die untersuchten zehn Jahre 20 Mio USD oder mehr.

2008 hat Nigeria dem chinesischen Unternehmen ZTE 470 Mio USD gezahlt, um die beiden wichtigsten Städte des Landes (Lagos und Abuja) mittels Videoüberwachung “sicher & smart“ zu machen. Huawei (China) erhielt 113 Mio

¹¹ In Tony Roberts et al., pp.16f.

¹² Zu den verschiedenen Kamera-Arten siehe Electronic Frontier Foundation (EFF), *Surveillance Cameras*, <https://www.eff.org/de/pages/surveillance-cameras#main-content>.

¹³ Abb.5.6 in Tony Roberts et al., p.34.

¹⁴ Siehe dazu die *Surveillance Stories* ebd., p.61.

USD für ein elektronisches Grenz-Projekt. Betrieben werden die Systeme von lokalen Unternehmen unter Beistand von Firmen aus den Vereinigten Arabischen Emiraten und Südkorea.

Die Singapur-Filiale des französischen Rüstungskonzerns Thales erhielt 2012 für ein biometrischen Erkennungssystem 430 Millionen USD. Zusätzliche Technologie kam von Dermalog (Deutschland/50 Mio USD), BIO-key (USA/45 Mio USD) und Chongqing Huifan (China/Betrag unbekannt).

Im Nigeria-Teil der Studie findet sich eine zweiseitige Liste der Lieferfirmen in den fünf Kategorien mit den gelieferten Produkten und den bezahlten Unsummen¹⁵. Vergessen wir nicht, dass des Landes Reichtum an Erdöl und auch Erdgas nur wenigen zugutegekommen ist und dass die zwischen 2013 und 2022 für Überwachungstechnologie ausgegebenen mindesten 2,7 Mrd. USD anderweitig sehr viel besser hätten verwendet werden können.

* * *

Ghana hat, was Demokratie betrifft, einen guten Ruf, auch wenn er – insbesondere, was JournalistInnen betrifft – zuletzt etwas gelitten hat. Parallel dazu hat das Land in Überwachungstechnologie investiert. Insbesondere für die “sichere und smarte Stadt“ wurden an Huawei (China) und ArisCel (Ghana/China) insgesamt 701 Mio USD gezahlt¹⁶.

* * *

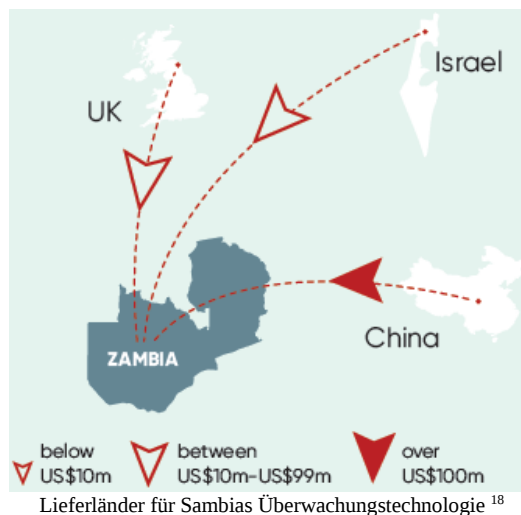
Marokko mangelt es insbesondere an einer unabhängigen Gerichtsbarkeit, um die Rechte seiner BürgerInnen auf ihre Freiheits- und Privatsphäre durchzusetzen. JournalistInnen und AktivistInnen sind immer wieder Ziel illegaler staatlicher Repression. Wie Nigeria, Ghana und Sambia, hat auch Rabat in die “sichere und smarte Stadt“ investiert, auch andere Kategorien von Überwachungstechnologie sind abgedeckt. Bizzarrerweise wurde Pegasus-Spionage-Technologie auch zum Überwachen des marokkanischen Königs Mohammed VI eingesetzt.¹⁷

* * *

Malawi hat unter den fünf beforschten Ländern am wenigsten in Überwachungstechnologie investiert und als einziges gar nicht in die “sichere und smarte Stadt“. Die mobile Telefonie wird allerdings überwacht und im Bereich der biometrischen Erkennung ist Fingerabdruck- und Gesichtserkennungstechnologie angeschafft worden.

* * *

Sambia hat in erster Linie in die “safe/smart city“ investiert (Huawei und ZTE/China/210 Mio USD). Das Land ist zudem bei der Internet Überwachung aktiv (Cyberbit/Israel) und in der biometrischen Erkennung (GB/54,8 Mio USD). Hier dieselben Infos in einer kartographischen Darstellung:



* * *

Was ist zu tun?

Die IDS-Studie verlangt, dass sowohl angebots-, als auch nachfrageseitig nachgebessert wird. In den Lieferländern braucht es klare Regeln für den Verkauf von Überwachungstechnologie, in den Zielländern braucht es klare Regeln für ihre Verwendung. Verpflichtende Exportgenehmigungen sollten nur unter Voraussetzung einer Prüfung der Auswirkungen auf die Menschenrechte in den Zielländern erteilt werden. Und in den Zielländern gilt es, Bewusstsein zu schaffen und die Fähigkeiten der Zivilgesellschaft, als Kontrollorgan für die Einhaltung der Regeln zu fungieren.

¹⁵ Siehe Tony Roberts et al., pp.56f.

¹⁶ Der Ghana-Länderbericht findet sich ebd., pp.66-82.

¹⁷ Ebd., p.87. Marokko-Länderbericht: ebd., pp.83-103.

¹⁸ Solche kartographischen Darstellungen gibt es für die anderen vier Länder auch. Die für Sambia findet sich ebd., p.32. Sambia-Länderbericht: ebd., pp.120-135.

Fast wichtiger noch als die Regeln ist, dass sie angewendet werden.

Unser aller Menschenrechte würden davon profitieren.

Der Trend geht allerdings in die Gegenrichtung – nicht nur, aber auch in Afrika.

* * *

Zum Abschluss hier das Cover der IDS-Studie. Dem Institut, Tony Roberts und seinen Co-AutorInnen herzlichen Dank für die umfassenden, augenöffnenden Informationen.

