Der Arabische Frühling:
Gefahren und Chancen der IT für die Demokratisierung

Christof Leng, Gesellschaft für Informatik e.V.
Kongress der Integrata-Stiftung 2012

Der Arabische Frühling ist vermutlich die bedeutendste politische Umwälzung der vergangenen Jahre. Und wie in keinem bisherigen Konflikt spielt das Internet dabei eine zentrale Rolle. Als Informatiker müssen wir diese Situation sehr genau analysieren und bewerten, welche Chancen und Gefahren durch Informationstechnologien in diesem Kontext ausgehen.

Lassen Sie mich kurz den Ablauf der Ereignisse rekapitulieren. Ausgelöst wurden die Proteste durch die Selbstverbrennung eines jungen Tunesiers am 17. Dezember 2010. Sehr schnell wurden über Facebook und ähnliche soziale Netzwerke Demonstrationen organisiert und diese dann mit Handy-Videos dokumentiert. Diese Videos landeten wiederum schnell auf Facebook und YouTube. Dieser Ablauf wiederholte sich in ähnlicher Form in Ägypten, Libyen, Bahrain und Syrien.

Den technischen Hilfsmittel (Handy, Internet, Social Media) kam dabei eine zentrale Rolle zu. Sie dienten nicht nur zur konkreten Organisation der Proteste und der Informierung der Weltöffentlichkeit. Auch im Vorfeld der Revolten tauschte sich die Bevölkerung über das Regime aus und schuf so eine Gegenöffentlichkeit zu den vom Staat zensierten Medien.

Selbstverständlich haben die Regimes Gegenmaßnahmen ergriffen.

- Dazu gehört die Abschaltung oder Einschränkung der Kommunikationsmöglichkeiten. Beispielsweise wurde in Ägypten am 27. Januar 2011 das Internet, SMS und weite Teile des Mobilfunknetzes abgeschaltet.
- Ebenfalls üblich ist die Abschaltung des Internetzugangs für bestimmte Personenkreise. Dies wurde zum Beispiel mehrfach vom syrischen Regime eingesetzt, um belagerte Viertel von der Außenwelt abzuschneiden.
- Auch der Zugriff auf bestimmte Websites oder Protokolle wurde vielfach verhindert. Facebook und Twitter wurden in Ägypten bereits vor der allgemeinen Internetabschaltung gesperrt, um die Organisation von weiteren Protesten zu erschweren.
- Darüber hinaus wurde beziehungsweise wird die Internetkommunikation in den betroffenen Ländern massiv überwacht. Immer wieder wird von Verhaftungen und Folter in Syrien berichtet, bei denen den Opfern detailliert ihre Onlinekommunikation vorgeworfen wird. Auch in Libyen wurde das Internet systematisch abgehört.
- Doch mit dem Abhören allein ist es nicht getan. Anhand der gewonnenen Daten können die Behörden präzise ermitteln, von welchem Anschluss die Kommunikation ausging. Massenverhaftungen, Folter und Hinrichtungen sind beispielsweise in Syrien an der Tagesordnung.

Wie konnten die Aufständischen trotz der massiven Maßnahmen der Regimes ihre elektronische Kommunikation aufrecht erhalten und ihre Risiken minimieren?

- Zunächst kann man Videos und Bilder auf Speicherkarten aus dem Land schmuggeln und dann im Ausland ins Internet einspeisen. Das ist allerdings ein mühsamer und langwieriger Prozess. Dennoch wurde diese Möglichkeit an der libysch-ägyptischen Grenze während des Aufstands gegen Gaddafi genutzt.
- Nach der Abschaltung des Internets in Ägypten boten die internationalen Netzaktivisten von Telecomix Modempools zur Einwahl über das Telefonnetz an. Die Rufnummern wurden per Telefax in Ägypten verbreitet.
- Da in Syrien das Internet nicht abgeschaltet wurde, aber Telefonnetz und Internet gleichermaßen überwacht werden, bietet Telecomix den Aufständischen dort spezielle Kommunikationskanäle an, um Daten unbemerkt über das Internet ins Ausland zu schleusen.
- Diese Daten werden dann von den Aktivisten aufwändig anonymisiert, indem zum Beispiel Metadaten und Geokoordi-

naten entfernt werden, um die Quellen vor Ort vor Verfolgung zu schützen.
- Auch nutzen die Menschen vor Ort zunehmend Live-Verbindungen wie Skype, um Videodaten in Echtzeit außer Landes zu bringen, denn eine temporäre Speicherung verursacht unnötige Risiken. Zudem ist Skype durch seine dezentrale Peer-to-Peer-Organisation und lückenhafte Dokumentation nicht ganz so leicht zu überwachen wie Webdienste.
- Letztlich haben Gruppen wie Telecomix in Syrien die Überwachungsinfrastruktur gehackt und öffentlich dokumentiert. Auch wenn das nur eine Momentaufnahme ist, kann das Verständnis der Überwachung den Aufständischen helfen und weltweite öffentliche Aufklärung bewirken.

Beide Konfliktparteien befinden sich inzwischen in einem klassischen Wettrüsten mit ungewissem Ausgang. Doch inwiefern betrifft uns diese Situation in fernen Ländern mit vollkommen anderen Verhältnissen? Nun, zunächst stammt die Überwachungsinfrastruktur von westlichen und insbesondere auch deutschen Unternehmen, und zum anderen wirft ein Vergleich mit den Gesetzesvorhaben in Deutschland spannende Fragen auf.

Natürlich ist die Situation hierzulande nicht im Geringsten mit den Regimes in der arabischen Welt zu vergleichen. Aber auch hier ist der Umgang mit der Kommunikation im Internet Gegenstand eines heftigen öffentlichen Diskurses.

- Sicher würde niemand in Europa ernsthaft eine Abschaltung des Internets in Betracht ziehen. Die gezielte Bevor- und Benachteiligung bestimmter Teilnehmer im Netz ist das Thema der heftig diskutierten Frage nach Netzneutralität.
- Auch die Sperrung einzelner Internetzugänge, zum Beispiel bereits bei Urheberrechtsverletzungen wird unter dem Stichwort „Three Strikes“ in Europa diskutiert. In Frankreich ist dieses Verfahren seit 2009 im Einsatz und auch im Rahmen von ACTA wurde es international diskutiert.
- Die Diskussion um die von Frau von der Leyen propagierten Websperren ist sicherlich allen noch lebhaft in Erinnerung. Aber auch darüber hinaus werden täglich in Unternehmensnetzwerken gezielt Websites blockiert, um „die Produktivität der Mitarbeiter zu steigern“.
- Die Vorratsdatenspeicherung und von Ermittlungsbehörden eingesetzte Trojanersoftware zur Quellen-TKÜ muss ich wohl nicht weiter erläutern.
- Ein weiterer Bereich ist die Anonymität im Internet. In den letzten Wochen haben sich mehrere Spitzenpolitiker öffentlich über die Tradition der Anonymität und Pseudonomisierung im Internet beschwert. Eine öffentliche Debatte sollte ihrer Meinung nach nur mit dem bürgerlichen Namen geführt werden.
- Ein anderer Bereich der aktiv gegen Anonymität kämpft, ist die Content-Industrie, welche die ursprünglichen Quellen von geleakten Medien aufdecken möchte. Hierzu werden zunehmend digitale Wasserzeichen eingesetzt, welche den Ursprung digitaler Daten enthüllen können.

Warum zähle ich all diese Dinge hier auf? Warum bringe ich sie in den Kontext von schrecklichen Verbrechen gegen die Menschlichkeit? Manche der Maßnahmen haben durchaus lobenswerte Ziele, zum Beispiel den Kampf gegen Kinderpornografie. Anderen liegen zumindest legitime unternehmerische Interessen zu Grunde. Ich halte es auch für undenkbar, dass auf absehbare Zeit eine deutsche Regierung eine solche Infrastruktur in einer ähnlichen Form missbraucht wie Diktatoren vom Schlag eines Muammar al-Gaddafi oder Baschar al-Assad. Warum also? Das Problem ist meiner Meinung, dass wir mit diesen Technologien die Büchse der Pandora öffnen könnten oder sogar bereits geöffnet haben. Um das zu verstehen, sollten wir uns die Herkunft der eingesetzten Technologie näher anschauen.

Die Werkzeuge stammen ausnahmslos aus dem Westen, viele auch aus Deutschland, teilweise von großen, renommierten Herstellern. Sie wurden aber wohl nicht primär für den Einsatz in Diktaturen entwickelt, sondern sind so genannte Dual-Use Technologien. Manche der Werkzeuge wurden für Jugendschutzfilterung, zum Netzwerkmanagement, zur Absicherung von Unternehmensnetzwerken oder Ähnliches entwickelt. Der Missbrauch ihrer Produkte wird von den Hersteller aber nicht oder nur sehr halbherzig unter-

sagt. Im Gegenteil: Man gewinnt den Eindruck, dass hier ein sehr lukrativer Markt bearbeitet wird.

Die Technologien fallen auch nicht oder nur sehr bedingt unter Exportkontrollgesetze, wie das Wassenaar-Abkommen von 1996 über Kriegswaffenexportkontrolle. Und selbst falls ihr Export verboten sein sollte, kann man sie hervorragend in Gesamtpaketen verstecken oder aufgrund ihrer Dual-Use-Eigenschaft als etwas vermeintlich Harmloses tarnen. Auch eine strikte Exportkontrolle ist insbesondere im Bereich Software hoffnungslos, weil sie sich über winzige Speichermedien oder Internetverbindungen einfach weitergeben und vervielfältigen lässt. Filesharing für Diktatoren sozusagen.

Nun haben wir es also mit einer Technologie zu tun, die sowohl legitim zivil als auch für massive Verbrechen gegen die Menschlichkeit genutzt werden kann. Das ruft Erinnerung an die Atomkraft oder den gesamten Bereich der ABC-Waffen wach. Es wäre eindeutig überzogen, Schnüffelsoftware als „digitale Massenvernichtungswaffe“ zu bezeichnen, aber ihr Missbrauchspotenzial ist ebenfalls hoch und ihre Verbreitung, wie schon gesagt, schwer zu kontrollieren.
Man könnte es also mit gefährlichen Krankheitserregern vergleichen, für die es auch legitime Einsatzbereiche gibt, zum Beispiel in der Erforschung neuer Impfstoffe. Die Nutzung solcher Gefahrenstoffe unterliegt allerdings aufwändigen Sicherheitsvorschriften. Wenn man aber den Einsatz von Überwachungstechnik derart extrem reglementieren würde, wären die meisten der legitimen Einsatzzwecke nicht mehr realisierbar.
Wenn ein legitimer Einsatz aus diesem Grund nicht mehr tragbar wäre, also vorwiegend der Missbrauch bliebe, müsste man dann nicht Herstellung und Verbreitung allgemein verbieten? Also so wie bei Landminen, deren mehr oder minder legitime militärische Einsatzzweck die Gefahren für die Zivilbevölkerung nicht rechtfertigt?
Kann man Content-Filtering, Wasserzeichen, Netzwerkmanagement und ähnliches wirklich ernsthaft mit Milzbrand und Landminen vergleichen? Erfüllen Jugendschutz und Unternehmenssicherheit nicht wichtige und lobenswerte Funktionen in unserer Gesellschaft? Wie kann man überhaupt den allgemeinen Nutzen einer Technologie gegenüber dem Schaden durch ihren potentiellen Missbrauch abwägen?
Welche ethische Verantwortung haben die Entwickler solcher Technologie in Unternehmen und Wissenschaft, die beispielsweise scheinbar harmlose Verfahren zum Netzwerkmanagement oder digitalen Wasserzeichen entwickeln? Welche Rolle kommt dabei dem Gesetzgeber zu, der immer weniger mit der rasanten Entwicklung Schritt halten kann?

Ich kann und will Ihnen diese Fragen nicht erschöpfend beantworten, lade Sie aber herzlich dazu ein, sie mit mir nach meinem Vortrag zu diskutieren. Bevor ich jetzt zum Ende komme, will ich den Blick noch einmal auf die andere Seite der Medaille lenken.
Der arabische Frühling lehrt uns, dass von der Informationstechnologie zwar erhebliche Gefahren für Demokratie und Menschenrechte ausgehen, aber er lehrt uns auch, dass ihr ein mindestens ebenso großes Potential zur Demokratisierung und Aufklärung inne wohnt.
Besonders bewegt hat mich bei den Geschichten aus Tunesien, Ägypten und Syrien wie viel Hoffnung das Internet für die Bürger in diesem Land bedeutet. Gerade Dienste wie Facebook, welche hierzulande oft Ängste und Bedenken auslösen, werden dort zur Keimzelle einer neuen und freien Gesellschaft.
Gerade deshalb müssen wir uns fragen, welche Verantwortung Zugangs- und Dienstanbieter im Internet in der Zukunft tragen werden. Durch soziale Netzwerke entsteht derzeit eine revolutionäre Möglichkeit zum politischen und kulturellen Austausch, die vor wirtschaftlichem und staatlichen Missbrauch gleichermaßen geschützt werden muss.
Wenn wir uns die Wahlen in Ländern wie Tunesien und Ägypten anschauen, stellen manche Kommentatoren die Frage, ob gewählte Islamisten wirklich eine Verbesserung gegenüber westlich-orientierten Diktatoren darstellen. Ich frage mich, ob man in Ländern, in denen jahrelang die Kommunikationsmöglichkeiten gefiltert wurden und nicht nur „staatsfeindliche“ sondern auch vermeintlich „unmoralische“ Inhalte gesperrt waren, wirklich ein hohes Maß an Aufklärung erwarten kann. Wenn wir etwas für Völkerverständigung, Frieden und langfristige Stabilität tun wollen, sollten wir uns für eine freie und ge-

schützte Kommunikation in den elektronischen Medien weltweit einsetzen. Ich glaube, dass sich daraus nicht nur gesellschaftliche Fragestellungen ableiten lassen, sondern auch die Informatik in Wissenschaft und Anwendung sich selbst weitreichende Fragen stellen muss. In diesem Sinne möchte ich mit meinen Vortrag mit einem Zitat von Stephan Urbach von Telecomix abschließen: „Freie Kommunikation ist der Schlüssel zu einem freien Menschen“.