67. Jahrgang, 46–47/2017, 13. November 2017

bpb:

AUS POLITIK UND ZEITGESCHICHTE

Darknet

APuZ

ZEITSCHRIFT DER BUNDESZENTRALE FÜR POLITISCHE BILDUNG

Beilage zur Wochenzeitung Das **Parlament**

Darknet
APuZ 46–47/2017

EDITORIAL

Spätestens nachdem im Juli 2016 ein 18-jähriger Schüler am Münchner Olympia-Einkaufszentrum neun Menschen erschoss, ist auch der deutschen Öffentlichkeit das Phänomen „Darknet“ bekannt. Hier soll der Attentäter den Kauf der Tatwaffe angebahnt haben. In den Schlagzeilen erschien das Darknet entsprechend als anrüchige, „dunkle“ Seite des Internets: In seinen undurchsichtigen Weiten tummeln sich Kriminelle, die mithilfe von Verschlüsselungstechnologie Drogen, Waffen und kinderpornografisches Material kaufen und verkaufen. Gezahlt wird anonym mit sogenannten Kryptowährungen wie dem Bitcoin, der inzwischen das Image einer Schurkenwährung hinter sich gelassen hat.

In der Berichterstattung über das Darknet wird aber auch seine „helle“ Seite betont: Die absolute Anonymität bietet Menschenrechtlern, Journalistinnen und Whistleblowern in repressiven Staaten Schutz vor politischer Verfolgung. Für sie ist das Darknet oft die einzige Möglichkeit, sich politisch zu engagieren und der staatlichen Überwachung zu entkommen. Dank derselben Verschlüsselungstechnologie, die digitale Drogen- und Waffenmärkte absichert, können Oppositionelle in Staaten wie Syrien, Iran und China im Verborgenen über Missstände berichten.

Auch in liberalen Demokratien ist Verschlüsselung existenziell. Entscheidend sind die Fragen, was „gute“ von „schlechter“ Verschlüsselung unterscheidet und wie viel Kryptografie für das Funktionieren einer offenen Gesellschaft notwendig ist. Starke Verschlüsselung schützt Bürgerinnen und Bürger vor Cyberkriminalität, aber ebenso Terroristen und Waffenhändler vor Ermittlungsbehörden. Absichtlich geschwächte Verschlüsselung erleichtert dem Staat die Strafverfolgung, aber zugleich weltweit agierenden Hackern Phishing und Diebstahl. Damit stehen im Kampf gegen Internetkriminalität nicht nur Freiheit und Sicherheit in einem Spannungsverhältnis, sondern auch zwei unterschiedliche Aspekte von Sicherheit: die innere Sicherheit und die moderne Cybersicherheit.

Lorenz Abu Ayyash

„TOR" IN EINE ANDERE WELT?

Begriffe, Technologien und Widersprüche des Darknets

Stefan Mey

Das Darknet gilt als Gegenentwurf zum World Wide Web und will eine völlig unzensierte Kommunikation ermöglichen, die vor Überwachung geschützt ist. Wie zu erwarten, wird die dort gebotene Anonymität auf gesellschaftlich erwünschte wie ethisch unerwünschte Weise genutzt. Und auch sonst lassen sich verschiedenste Widersprüche beobachten.

Immer wieder geistert es durch die Medien, dieses rätselhafte, irgendwie mythische Darknet, in dem das Böse wie das Gute im Menschen potenziert zu sein scheint. Auf der einen Seite, so heißt es, werden dort ungestört Bilder missbrauchter Kinder getauscht und Waffen gehandelt. Auf der anderen Seite biete dieser Ort den Aktivisten und Whistleblowern dieser Welt Schutz vor staatlicher Verfolgung.

DARKNET, CLEARNET UND DEEP WEB

Versuchen wir uns an einer Definition: Ein Darknet ist ein digitales Netz, das sich vom sonstigen Internet abschirmt und mit technologischen Mitteln die Anonymität seiner Nutzer herstellt. Wer Inhalte anbietet, wer mit wem kommuniziert und worüber, das alles wird mithilfe von Verschlüsselungstechnologien verschleiert.

Als Gegenkonzept gilt das restliche, offene World Wide Web, das mitunter auch als „Clearnet" oder „Surface Web" (Oberflächennetz) bezeichnet wird. Dessen Inhalte sind unter Endungen wie .de oder .com zu finden. Sie lassen sich mit gängigen Internetbrowsern wie Google Chrome, Firefox oder Internet Explorer aufrufen und werden von verbreiteten Suchmaschinen wie Google erfasst.

Relevant in der Diskussion ist auch der Begriff „Deep Web". Er bezeichnet Inhalte, die nicht von Suchmaschinen erfasst werden können. Das kann unterschiedliche Gründen haben: weil es sich um geschlossene Intranets von Unternehmen oder Organisationen handelt, weil Seiten nicht oder nur kaum über Links mit dem sonstigen Web verbunden sind oder weil Inhalte von Bezahlschranken vor einem automatisierten Zugriff geschützt sind.

Oft heißt es, das World Wide Web sei wie die sichtbare Spitze eines Eisbergs, und darunter liege ein digitaler Koloss an Inhalten: das Deep Web. „10- bis 100-mal größer als das Surface Web" seien die „Tiefen des Internets", heißt es in einer für die Presse bestimmten Infografik des Bundeskriminalamts.[01] Redaktionen, denen die anschauliche Bebilderung digitaler Phänomene schwerfällt, illustrieren Artikel über das Darknet gern mit einer Skizze dieses Deep-Web-Eisbergs. Das legt den Eindruck nahe, es gebe „da draußen" einen riesigen, noch unerschlossenen digitalen Kosmos, und das Darknet sei ein nicht quantifizierbarer, aber beträchtlich großer Teil davon.

Die Eisberg-Metapher stammt aus einem „Whitepaper" der Firma BrightPlanet aus dem Jahr 2001.[02] Das US-amerikanische Unternehmen für Datenanalyse war auf Basis von Hochrechnungen zu dem Schluss gekommen, dass das Deep Web 400 bis 550 Mal so groß sei wie das bekannte World Wide Web. Zu dieser Zeit lieferten Suchmaschinen wie Google nur einen begrenzten Überblick über das Netz. Mehr als 15 Jahre später gelingt es ihnen aber, das World Wide Web fast flächendeckend abzubilden. Die Eisberg-Metapher, die aus einer längst vergangenen Epoche der Internetentwicklung stammt, wird trotzdem immer noch bemüht.

Etwa zehn verschiedene Darknets listet der gleichnamige englischsprachige Wikipedia-Artikel auf. Zu größerer Bekanntheit hat es bisher aber nur eine Lösung gebracht: das Darknet auf Basis der Anonymisierungstechnologie Tor.

TOR ALS FÜHRENDE DARKNET-TECHNOLOGIE

Als eine Art digitale Tarnkappe ermöglicht Tor es, einfache Nutzer sowie Anbieter von Websites zu verstecken. Tor stand ursprünglich für „The

Onion Router“. Der Vater der Technologie hatte die Architektur seiner Erfindung mit dem Aufbau einer Zwiebel verglichen: Bei der Zwiebel ist der Kern unter mehreren Schalen versteckt, und bei Tor verberge sich der „Kern“ aus Identität und Aktivität der jeweiligen Internetnutzer unter mehreren Anonymisierungsschichten.

Tor basiert auf einem simplen Prinzip: der mehrfachen Weiterleitung von Datenverkehr. Dafür steht ein Netzwerk von etwa 7000 unentgeltlich betriebenen Internetknoten zur Verfügung. Sie sind über die halbe Welt verteilt. 60 Prozent der Knoten befinden sich jedoch in den vier Ländern Deutschland, Frankreich, Holland und USA, wobei die Bundesrepublik mit etwa 1300 Knoten Spitzenreiterin ist.

Hinter vielen der großen Knoten, über die vergleichsweise viel Datenverkehr abgewickelt wird, stehen universitäre oder zivilgesellschaftliche Projekte – in der Bundesrepublik beispielsweise die NGO Reporter ohne Grenzen, der Tor-Unterstützerverein Zwiebelfreunde und die Hacker-Organisation Chaos Computer Club. Tor-Knoten lassen sich allerdings auch anonym betreiben. Somit können sich auch Geheimdienste oder Cyberkriminelle in die Infrastruktur einschleichen und mithilfe eigener Knoten den Datenverkehr mitschneiden oder manipulieren.

Tor nutzt die Grundstruktur des Internets, bei der IP-Adressen miteinander kommunizieren. Diese Ziffernfolgen machen einzelne Nutzer und auch Websites adressierbar und identifizierbar. Die zwiebelartige Anonymisierungstechnologie überlagert die Internetarchitektur jedoch mit einer weiteren Ebene: Ein Datenpaket, beispielsweise eine Anfrage nach einer Website, wird nicht mehr direkt von IP-Adresse zu IP-Adresse geschickt, sondern über eine Abfolge von jeweils drei Knoten geleitet. Dabei kennt jeder Knoten jeweils nur seinen Vorgänger, von dem er das Datenpaket entgegennimmt, und seinen Nachfolger, an den er es weitergibt.

Das sorgt für Anonymität: Die aufgerufene Website, sei es beispielsweise die von „Spiegel Online“ oder die des Bundeskriminalamts, erfährt nicht, von wem die Anfrage eigentlich ausging. Und auch der Internetanbieter, zum Beispiel die Telekom, sieht nicht, welche Website aufgerufen werden soll.

Das Prinzip der anonymisierenden Weiterleitung wird von zwei Anwendungen genutzt. Die erste ist der Tor-Browser, eine Abwandlung des bekannten, nichtkommerziellen Firefox-Browsers. Er lässt sich kostenlos herunterladen und leitet den Datenverkehr über den beschriebenen Umweg von drei Tor-Knoten. Das macht ihn langsamer als handelsübliche Browser, vor allem bei Websites mit vielen multimedialen Elementen und Werbeeinblendungen. Mit dem Tor-Browser kann man anonym im klassischen Netz surfen und Netzsperren umgehen, da er verschleiert, welche Website tatsächlich angesteuert wird. Zum anderen erlaubt er einen Zugriff auf das Tor-basierte Darknet, das für andere Browser nicht sichtbar ist.

Die zweite Anwendung ermöglicht den anonymen Betrieb von Websites unter der inoffiziellen Darknet-Endung .onion. Diese Seiten werden, da ihr Standort von der Tor-Software versteckt wird, auch *hidden services* genannt. Die einzelnen .onion-Adressen werden auf Basis von Zufallszahlen von der Tor-Software berechnet und bestehen in der Regel aus einer kryptisch anmutenden Folge von 16 Zeichen. So lautet beispielsweise eine Darknet-Adresse: expyuzz4wqqyqhjn.onion.

Die Kommunikation mit einer Darknet-Seite geschieht über eine Art toten Briefkasten. Sowohl die User als auch die Seitenbetreiber kommunizieren mit dieser Zwischenstation über eine jeweils eigene Route aus drei Tor-Knoten. Die Seiten haben einige Vorzüge: Sie bewahren Nutzer davor, sich aus Unwissenheit zu de-anonymisieren, da sich .onion-Seiten nur per Tor-Browser betreten lassen. Zudem können .onion-Adressen weder zensiert noch von staatlichen Stellen gelöscht werden, was bei Adressen im klassischen Netz durchaus möglich ist.

Dieser vor Überwachung und Zensur geschützte digitale Kosmos ist meist gemeint, wenn in der öffentlichen Diskussion über „das“ Darknet gesprochen wird. In der Praxis gibt es allerdings auch eine breitere Definition des Tor-Darknets. Die engere Definition, die auch im Folgenden verwendet wird, umfasst ausschließlich die .onion-Seiten. Für die weitere Definition zählt zum Darknet bereits, wenn mit dem Tor-Browser anonym im klassischen Netz gesurft wird.

01 Siehe Bundeskriminalamt, Die Tiefen des Internets, Infografik vom 12.10.2016.

02 Siehe Michael K. Bergman, White Paper: The Deep Web: Surfacing Hidden Value, in: The Journal of Electronic Publishing 1/2001.

Hinter Tor und somit auch hinter dem .onion-Darknet steht eine nicht profitorientierte Organisation mit Hauptsitz in Seattle: The Tor Project, Inc. Diese betreut die Software und entwickelt sie weiter. Ihr steht eine ehrenamtliche Community zur Seite, die die Infrastruktur aus Tausenden Tor-Knoten zur Verfügung stellt.

EIGENSCHAFTEN DES TOR-DARKNETS

Das Tor-Darknet ist klein, und seine überschaubaren Ausmaße stehen in einem auffälligen Missverhältnis zur großen medialen Präsenz. Das Tor Project zählt etwa 50 000 einzelne .onion-Adressen (Stand Oktober 2017). Von denen enthalten allerdings, wie verschiedene Studien ergeben haben, weniger als 10 000 tatsächlich per Browser ansteuerbare Inhalte.[03]

Ähnlich sieht es bei der User-Basis des Darknets aus. Laut Tor Project nutzen etwa 2,5 Millionen Menschen täglich die Tor-Software, dabei stammen etwa acht Prozent aus der Bundesrepublik.[04] Wie viele davon mit dem Tor-Browser „nur" anonym im normalen Netz surfen oder tatsächlich im .onion-Darknet unterwegs sind, erhebt die Organisation nicht. Geschätzt wird aber, dass nur etwa 3,4 Prozent des Tor-Datenverkehrs auf die Darknet-Nutzung entfällt. Zieht man diese Zahl, in Ermangelung präziserer Angaben, für eine Schätzung der Darknet-Nutzung heran, ergibt sich ein Wert von deutlich weniger als 100 000 Usern.

Bei der Nutzung von .onion-Adressen lassen sich drei Modelle unterscheiden:

Originäre .onion-Inhalte

Orientiert man sich an der gängigen Berichterstattung über das Darknet, ließe sich nicht nur eine große Zahl an ethisch fragwürdigen, sondern auch an gesellschaftlich erwünschten, politischen Inhalten erwarten, die es so nur unter .onion-Seiten und nicht im klassischen Web gibt. Diese Erwartung wird jedoch überwiegend enttäuscht. Eine nennenswerte inhaltliche Vielfalt gibt es lediglich auf der illegalen Seite des Darknet-Kosmos. Dort findet sich eine breite Palette an professionalisierten Marktplätzen, die verschiedene „Produkte" in ihren digitalen Regalen stehen haben. Hauptsächlich werden aber Drogen verkauft. Auf der legalen Seite finden sich vor allem selbstreferenzielle Inhalte, etwa Überblickslisten zum Darknet.

.onion als Programmbaustein

Beim zweiten Modell dient die .onion-Technologie als Baustein für spezielle Darknet-Programme. Das prominenteste Bespiel ist die Software OnionShare, über die sich Dateien tauschen lassen. Die Software erzeugt auf dem Rechner ihrer Nutzer eine temporäre .onion-Adresse mit einem Download-Link. Von dieser kurzzeitig existierenden Darknet-Seite kann dann jemand anderes die zu tauschende Datei herunterladen – ohne dass Dritte zwischengeschaltet sind, wie das bei anderen Lösungen, etwa dem Versand per E-Mail oder über Anbieter wie Dropbox, der Fall ist.

.onion als alternative Zugangstür

Bei der derzeit typischsten Nutzungsform von .onion jenseits der illegalen Darknet-Marktplätze haben sich Projekte aus dem klassischen Netz eine .onion-Adresse eingerichtet. Diese bieten dann einen alternativen Zugang für die kompletten Inhalte der jeweiligen Websites oder für bestimmte Teilinhalte oder -funktionen. Facebook beispielsweise verfügt über eine parallele Darknet-Adresse, aber auch zivilgesellschaftliche Akteure wie der Chaos Computer Club. Auch das von verschiedenen linken Strömungen frequentierte deutschsprachige Diskussionsportal „Indymedia" sowie dessen Schwesterprojekt „Indymedia Linksunten" haben sich eine .onion-Adresse zugelegt. In der Verfügung zum umstrittenen[05] Verbot von „Indymedia Linksunten" durch das Bundesministerium des Innern im August 2017 nannte die die oberste Bundesbehörde neben der klassischen Webadresse „linksunten.indymedia.org" auch die Darknet-Präsenz unter

03 Siehe Daniel Moore/Thomas Rid, Cryptopolitik and the Darknet, in: Survival 1/2016, S. 7–38. Die Autoren fanden zwar anfangs eine große Zahl an .onion-Adressen. Allerdings waren nur 5205 von ihnen aktiv und live, und wiederum nur etwa die Hälfte davon (2723) enthielten tatsächlich abrufbare Inhalte.

04 Siehe Tor Metrics, https://metrics.torproject.org.

05 Siehe Reporter ohne Grenzen, Rechtsstaatlich fragwürdiges Verbot, Pressemitteilung vom 28. 8. 2017, www.reporter-ohne-grenzen.de/presse/pressemitteilungen/meldung/rechtsstaatlich-fragwuerdiges-verbot.

„fhcnogcfx4zcq2e7.onion“ explizit mit.[06] Auch einige große Medien verfügen über eine alternative Zugangstür. Der britische „Guardian“, die „New York Times“, die Nachrichtenagentur AP und in der Bundesrepublik „Heise online“ haben sich im Darknet anonyme Postfächer für Whistleblower eingerichtet. Seit Oktober 2017 bietet die „New York Times“ zudem auch ihre kompletten Inhalte über eine Darknet-Adresse an.

In einigen Punkten ähnelt das heutige Tor-Darknet dem Internet der 1990er Jahre. Die wichtigste Parallele ist, dass die größte Herausforderung im Auffinden von Inhalten besteht. Es gibt einige Suchmaschinen, die aber nicht sonderlich gut funktionieren. Die wichtigste Navigationshilfe sind stattdessen lange Listen von .onion-Adressen. Eine besondere Rolle spielen dabei sogenannte *hidden wikis*, die teilweise auch im World Wide Web verfügbar sind. Diese spielen eine undurchsichtige Rolle: Sie prägen als vermeintlich repräsentative Überblicksseiten den Blick auf das Tor-Darknet und dessen Bild als Gruselkabinett. Der inhaltliche Fokus der *hidden wikis* liegt auf illegalen Angeboten, etwa zu diversen Shops für Drogen, Falschgeld und Waffen. Wer diese *hidden wikis* betreibt und unter welchen Gesichtspunkten die Links eingepflegt werden, ist unklar. Laien ist zur Vorsicht geraten: Es ist denkbar, dass sich hinter den Links reine Fake-Angebote verbergen, „Honeypots“ von Behörden oder Seiten, die nach einem Klick gefährliche Schadsoftware auf die Rechner der Nutzer laden.

ANDERE DARKNETS

Tor war und ist nicht der einzige Ansatz für eine Darknet-Technologie. Die bekanntesten Alternativen heute sind Freenet und I2P. Diese haben zum Teil eine andere inhaltliche Dynamik und eine radikalere technologische Architektur.

Auch beim I2P – kurz für „Invisible Internet Project“ – gibt es eine inoffizielle Internetendung (.i2p). Unter dieser sind die „Eepsites“ genannten Darknet-Seiten organisiert. Die Adressen bestehen anders als bei Tor nicht aus kryptischen Zeichenfolgen, sondern haben Namen wie „forum.i2p“ oder „planet.i2p“. Zudem gibt es keine Unterscheidung zwischen „einfachen“ Usern und Knotenbetreibern, die die Infrastruktur stellen. Jeder angeschlossene Rechner empfängt und sendet gleichermaßen die Daten der eigenen Kommunikation und leitet den Datenverkehr anderer weiter. Das geschieht über sich immer wieder neu zusammensetzende „Tunnel“-Pfade aus Rechnern. Um I2P zu nutzen, muss eine Software heruntergeladen werden. Navigiert wird letztlich über gängige Browser, bei denen zuvor jedoch eine Veränderung in den technischen Einstellungen vorgenommen werden muss. Die 2003 vorgestellte I2P-Technologie wird von einem losen Zusammenschluss meist anonym agierender Personen betrieben. Laut I2P-Angaben besteht das Kern-Team aus 15 Personen. Eine Sprecherin des Projekts schätzte im Sommer 2017, dass es etwa 400 aktive i2p-Adressen und eine User-Basis von 40 000 bis 50 000 gibt.[07] Viele I2P-Seiten widmen sich dem (oft illegalen) Tausch von Mediendateien wie Filmen oder E-Books. Es gibt aber auch thematisch breit aufgestellte Diskussionsforen und spezielle I2P-basierte Softwareangebote wie Mail- und Chatprogramme sowie ein Tool zum Erstellen von Blogs.

Das Freenet-Darknet verwendet das technologisch fortschrittlichste Konzept. Auch hier stellen alle User gemeinschaftlich die Infrastruktur. Allerdings werden Inhalte nicht wie bei .i2p oder .onion von den jeweiligen Anbietern der Inhalte auf externen Servern gespeichert. Sie werden stattdessen in Einzelteile zerlegt, verschlüsselt und auf zufällig ausgewählten Rechnern abgelegt. Damit das möglich ist, stellt jeder Rechner dem Freenet-Netzwerk automatisch einen Teil seines Speicherplatzes zur Verfügung. Auch für Freenet muss man eine eigene Software installieren, die auf dem Rechner verfügbare Browser dazu befähigt, auf das Freenet-Darknet zuzugreifen. Es existiert keine spezielle Darknet-Endung, die Adressen beginnen stets mit dem technischen Befehl „localhost:8888“, an den sich eine lange Zeichenfolge und schließlich der Titel der Seite anschließt.

Die Navigation erfolgt über Link-Listen, die allerdings sorgfältiger kuratiert sind als die *hidden wikis* des Tor-Darknets. Die größte Liste blendet FreeSites mit „unerwünschte Inhalten“ wie Dro-

06 Vgl. Bundesministerium des Innern, Was umfasst das Verbot der Internetplattform #linksunten.#indymedia? #BMIantwortet, Nachricht des offiziellen Twitter-Kanals des Bundesministeriums des Innern, 25. 8. 2017, https://twitter.com/bmi_bund/status/901000148209283072.

07 Siehe hierzu und im Folgenden Stefan Mey, Darknet: Waffen, Drogen, Whistleblower – Wie die digitale Unterwelt funktioniert, München 2017, S. 208 ff.

gen- und Waffen-Shops aus und enthält dennoch etwa 2500 Einträge in unterschiedlichen Sprachen und Themengebieten. Die inhaltliche Vielfalt ist größer als unter .i2p und .onion. Wie unter I2P gibt es diverse Seiten zum Download urheberrechtlich geschützter Medieninhalte. Allerdings handelt es sich bei einem Drittel der FreeSites um Blogs zu verschiedensten gesellschaftlichen, Politik- und Alltagsthemen. Und verschiedene Freenet-Adressen tragen *leaks* und geheime Unterlagen zusammen.

Hinter dem Freenet-Projekt steht eine Organisation mit Sitz in Austin (Texas). Der Freenet-Erfinder und heutige Präsident der Organisation Ian Clarke schätzt, dass im Sommer 2017 zu einem gegebenen Zeitpunkt etwa 15 000 Knoten – also einzelne Rechner und somit User – im Netzwerk online waren. Zahlen zu allen existierenden FreeSites kennt auch Clarke nicht. Die Größe der ehrenamtlichen Community schätzt er im Kern auf fünf Personen sowie 20 weitere Personen, die gelegentlich mitarbeiten.

WIESO TOR?

Wieso hat sich nun ausgerechnet Tor als Anonymisierungs- und Darknet-Technologie durchgesetzt und nicht etwa die beiden anderen Lösungen? Vor allem technologische Unterschiede ließen sich als mögliche Erklärung diskutieren: Sowohl I2P als auch Freenet sind reine Darknet-Technologien und ausschließlich darauf ausgelegt, Informationen in einem geschlossenen Darknet kursieren zu lassen. Auf der anderen Seite gibt es Technologien, die ausschließlich einen anonymen Zugriff auf das klassische Web ermöglichen. Die gängigste Lösung sind kommerzielle Virtual Private Networks (VPN), bei denen Datenverkehr von einem VPN-Anbieter gebündelt und dann zur Zielseite weitergeschickt wird.

Tor dagegen vereint beide Funktionen: Mit dem Browser lässt sich anonym im klassischen Netz surfen, und .onion ist eine vollwertige Darknet-Technologie. Ein Grund, wieso Tor das Rennen gewonnen hat, dürfte die Finanzlage sein: I2P verfügt über ein kleines Budget von jährlich wenigen Tausend Euro, bei Freenet waren es 2015 rund 14 000 US-Dollar. Das Tor Project dagegen verfügte laut seinem Finanzbericht im Jahr 2015 über ein Budget von 3,3 Millionen US-Dollar. Das Geld erlaubt es, Tor kontinuierlich weiterzuentwickeln und Mitarbeiter zu Werbezwecken um die Welt reisen zu lassen. Diese Arbeit muss nicht ehrenamtlich geschehen: 2015 hatte das Tor Project zehn Festangestellte, die Spitzengehälter lagen bei jährlich 135 000 US-Dollar.[08]

Die Finanzsituation ist allerdings Segen und Fluch zugleich und geht mit einer paradoxen Abhängigkeit einher: eine wirtschaftliche Abhängigkeit von der US-Regierung, zu deren Behördenapparat auch die National Security Agency (NSA) gehört. Spätestens seit den Enthüllungen Edward Snowdens weiß man, dass die NSA einen gigantischen Aufwand betreibt, weltweit Datenverkehr abzugreifen, und bemüht ist, Werkzeuge der „digitalen Selbstverteidigung" wie Tor zu knacken.

Das Budget des Tor Project setzte sich 2015 folgendermaßen zusammen:[09]

962 055 US-Dollar (29 Prozent) kamen vom US-Außenministerium, davon 857 515 direkt über das Bureau of Democracy, Human Rights and Labor Affairs (DRL) sowie 104 540 US-Dollar über die NGO Internews. Hierbei handelte es sich aber um weitergereichte Zuschüsse des DRL.

886 724 US-Dollar (27 Prozent) erhielt das Tor Project von Radio Free Asia (RFA), einem staatlichen Auslandssender mit Fokus auf den asiatischen Raum. Das RFA wurde ursprünglich als Werkzeug im Kalten Krieg vom CIA gegründet, untersteht aber mittlerweile der eigenständigen Rundfunkbehörde Broadcasting Board of Governors.

719 500 US-Dollar (22 Prozent) steuerte das Stanford Research Institute (SRI) bei. Das SRI ist ein unabhängiges Forschungsinstitut, sein Budget speist sich aber zu etwa zwei Dritteln aus Geldern des US-Verteidigungsministeriums.

226 364 US-Dollar (7 Prozent) kamen von der National Science Foundation, die staatliche Forschungsförderung der USA.

460 298 US-Dollar (14 Prozent) waren „andere" Einnahmen wie Geschenke, Stipendien und Zuschüsse.

Die Abhängigkeit von Regierungszuwendungen ist sogar noch höher, als es die Angaben auf den ersten Blick vermuten lassen. Wie Ro-

08 Siehe Stefan Mey, Anonymisierungs-Dienst Tor: Das Tor Project bleibt überwiegend regierungs-finanziert, 25. 4. 2017, www.heise.de/newsticker/meldung/Anonymisierungs-Dienst-Tor-Das-Tor-Project-bleibt-ueberwiegend-regierungs-finanziert-3693816.html.

09 Tor Project, Tor: Financial Reports, Fiscal Year 2015, o. D., www.torproject.org/about/findoc/2015-TorProject-combined-Form990_PC_Audit_Results.pdf.

ger Dingledine, Forschungsdirektor und öffentliches Gesicht des Tor Project, in einer die Veröffentlichung des Jahresberichts flankierenden Stellungnahme schrieb, setzte sich das Budget zu 85 bis 90 Prozent aus staatlichen Zuwendungen zusammen.[10]

Der Zusammenhang erklärt sich über die Geschichte des Softwareprojekts. Die Tor-Technologie wurde ab 1995 vom Mathematiker Paul Syverson im Naval Research Laboratory entwickelt, einer der Marine zugehörigen Forschungsabteilung des US-Verteidigungsministeriums. Die Technologie wurde jedoch auch anderen gesellschaftlichen Kreisen zugänglich gemacht. Wieso man solchen „Cover Traffic" brauche, erläuterte der später zum Projekt hinzugestoßene Roger Dingledine in einem Vortrag 2004: „Die US-Regierung kann nicht ein Anonymisierungssystem für jedermann betreiben und es dann nur selbst nutzen. Jedes Mal, wenn es eine Verbindung gibt, würden die Leute dann sagen: ‚Oh, es ist ein CIA-Agent.' Wenn das die Einzigen sind, die das Netzwerk nutzen."[11]

2003 wurde das Tor-Netzwerk für externe Knoten und der Quellcode der Software über eine Open-Source-Lizenz freigegeben. Seitdem ist die Software öffentlich einsehbar und frei verwendbar. 2006 wurde The Tor Project Inc. als formal unabhängige, nicht profitorientierte Organisation mit Sitz in Boston gegründet. Bei aller formaler Trennung vom Behördenapparat finanziert sich das Tor Project dennoch bis heute überwiegend über Forschungstöpfe der US-Regierung.

Das kann aus verschiedenen Gründen problematisch sein: Da Tor innerhalb der US-Verwaltung entwickelt wurde, besteht dort ein erhebliches Knowhow über die Anonymisierungstechnologie, die andere Teile des Behördenapparates, wie die NSA, zu knacken versuchen. Über die kleinteilig aufgeschlüsselten Förderanträge erhalten US-Behörden quasi frei Haus Einblicke in Vorhaben und strategische Überlegungen beim Tor Project, und sie haben einen verlässlichen Zugang zu seinen wichtigsten Protagonisten. Darüber hinaus hat die Organisation ihren formalen Sitz in den USA und wäre im Fall der Fälle juristisch dort greifbar.

SCHLUSS

Das Darknet, das derzeit vor allem das Tor-Darknet ist, stellt nur teilweise einen digitalen Gegenentwurf dar. Unzweifelhaft ist es in entscheidenden Teilen ein Gegenmodell: Die großen Netzkonzerne spielen dort keine Rolle, gesetzliche Regelungen, wie etwa Drogenkontrollregime, haben deutlich weniger Autorität, und Geheimdiensten wird die flächendeckende Ausforschung von Nutzungsverhalten erschwert. Auf der anderen Seite gibt es starke Parallelen zum klassischen Internet: Trotz theoretischer Vielfalt von Anonymisierungs- und Darknet-Technologien dominiert die Lösung eines einzelnen Anbieters. Dieser sitzt im selben Land wie die Platzhirsche des World Wide Web Google, Facebook und Apple und steht darüber hinaus noch in einem finanziellen Abhängigkeitsverhältnis zu US-Behörden.

Wenn die Grundidee des Darknets ist, ein staatsfernes „Gegen-Internet" zu erschaffen, lässt sich argumentieren, dass Tor die für ein solches Projekt politisch und organisatorisch am wenigsten geeignete technologische Lösung ist. Paradoxerweise hat sich Tor zur Umsetzung dieses Ziels dennoch durchgesetzt. Das ist vielleicht der am wenigstens beachtete Widerspruch beim Darknet, dieser großen Projektionsfläche eines Gegen-Internets, das auf der einen Seite die Machtverhältnisse der sonstigen Welt infrage stellt und auf der anderen mehr damit gemeinsam hat, als vielen bewusst und lieb sein dürfte.

10 Vgl. Tor Blog, Transparency, Openness, and Our 2015 Financials, 21.4.2017, https://blog.torproject.org/transparency-openness-and-our-2015-financials. In den Finanzberichten 2012 und 2013 waren die SRI-Gelder als weitergereichte Zuschüsse des Verteidigungsministeriums deklariert. In den Berichten 2014 und 2015 fand sich keine derartige Anmerkung. Wie genau die Rechnung von Dingledine aussieht, lässt sich nicht rekonstruieren. Auf eine Presseanfrage des Autors hin, ob es sich bei den SRI-Geldern auch 2015 um weitergereichte Mittel des Pentagons handelte, antwortete der damalige Kommunikationsdirektor des Tor Project Joshua Gay lediglich: „Ja, ich glaube, es handelt sich dabei ebenfalls um weitergereichte Mittel." Siehe hierzu auch Mey (Anm. 8).

11 Siehe Yasha Levine, Almost Everyone Involved in Developing Tor Was (or Is) Funded by the US Government, 16.7.2014, https://pando.com/2014/07/16/tor-spooks.

STEFAN MEY
ist Journalist und Buchautor. Zuletzt erschien „Darknet: Waffen, Drogen, Whistleblower – Wie die digitale Unterwelt funktioniert" (2017).
twitter.com/omydot

HILFLOSE ERMITTLER

Warum Kriminelle im Darknet wenig zu befürchten haben

Otto Hostettler

Es gibt sie, die spektakulären Erfolge der Ermittler. Wie etwa bei der Aufklärung der Hintergründe zum Münchner Amoklauf im Juli 2016. Damals erschoss ein 18-jähriger Schüler beim und im Olympia-Einkaufszentrum neun Menschen und richtete sich anschließend selber. Seine Waffe besorgte er sich im Darknet. Wenige Wochen nach der schrecklichen Tat schnappte die Polizei den Waffenhändler, der dem Amokläufer für 4350 Euro eine Pistole des Typs Glock 17 verkauft hatte. Der Fall zeigt mustergültig, wie die Polizei die Barriere von der realen Welt in die anonymen Tiefen des Internets überwinden kann: über Umwege, mit klassischer kriminalistischer Ermittlung – aber vor allem einer Portion Zufall.

In Vorträgen berichtet der für den Fall verantwortliche Cai Rüffer von der Frankfurter Generalstaatsanwaltschaft mitunter nicht ohne Stolz, wie seine Ermittler den Waffenhändler schnappten.[01] Viel früher kamen sie in ganz anderem Zusammenhang einem Waffenkäufer auf die Schliche, der darauf mit der Staatanwaltschaft kooperierte. Er überließ den Beamten sein Nutzerkonto, diese pflegten es weiter. Unter dieser Tarnidentität kontaktierten sie den Waffenanbieter „Rico“ später erneut. Es entwickelte sich eine Chatkonversation, bei dem die verdeckten Ermittler vorgaben, erneut an einer Waffe interessiert zu sein. Ohne es zu wissen, lieferte der Waffenhändler den Ermittlern ein ausführliches Geständnis: „Rico“ prahlte und erzählte ausführlich, wie er dem Münchner Attentäter die Waffe geliefert habe.

„Rico“ stand schon zwei Jahre lang im Visier der Behörden. Er verkaufte auf der inzwischen geschlossenen Darknet-Plattform „Deutschland im Deep Web“ Waffen und Munition, wie aus der Anklageschrift im Prozess vor dem Münchner Landgericht im Sommer hervorgeht. Aus dem Verkehr ziehen konnten ihn die Beamten der hessischen Zentralstelle zur Bekämpfung der Internetkriminalität – eine Einheit mit gerademal sechs Juristen – aber erst nach der Münchner Amoktat. Bei der Übergabe der Waffen verhaftete ein Spezialkommando der Zollfahndung den 31-Jährigen. In seinem Auto hatte er eine Glock-Pistole, eine Maschinenpistole und hunderte Schuss Munition.

Ein ähnlich spektakulärer Ermittlungserfolg ereignete sich in der Schweiz. Tobias K. war monatelang auf der Flucht, wurde international gesucht. Im Sommer 2016 soll er während eines Hafturlaubs in Zürich einen IT-Fachmann auf offener Straße erstochen haben. Im Januar 2017 konnte ihn schließlich die Kantonspolizei Bern verhaften, nachdem er im Darknet eine Waffe kaufen wollte. Aus dem sogenannten Zürcher Seefeld-Mord wurde ein „Fall Darknet“.

Tatsächlich war aber auch dieser Fall ein Zufallstreffer. Denn die Schweizer Bundespolizei erhielt von einem ausländischen Dienst ein unter einer Tarnidentität geführtes Profil eines Händlers, der drauf und dran war, über eine Darknet-Plattform einem Schweizer eine Waffe zu verkaufen. Die Bundesbehörden in Bern führten den Dialog fort, es stellte sich heraus, dass es sich beim potenziellen Käufer um den mutmaßlichen Mörder handelte. Die Polizei arrangierte mit ihm ein Treffen zur Waffenübergabe – die Falle schnappte zu. Fast wäre die Ermittlung aber gestrandet, weil sich keine kantonale Behörde bereit erklären wollte, den Fall zu Ende zu führen. Die Bundesanwaltschaft kontaktierte 100 Staatsanwälte und nur zwei boten Hand, den Fall zu übernehmen.

Von diesen Hintergründen erfuhr die Öffentlichkeit aber nichts, kommuniziert wurde ein Ermittlungserfolg. Die Behörden brauchen solche Meldungen. Und sie sorgen damit in den einschlägigen Kreisen auch für Wirkung. In den Foren der anonymen Marktplätze im Darknet diskutieren die Marktteilnehmer nach solchen Ereignissen eifrig, ob bereits eine nächste Razzia ansteht. Denn die Frage lautet, auf welche Daten die Polizei bei aufgeflogenen Händlern stößt.

Den teils spektakulären Erfolgen spezialisierter Behörden zum Trotz: Erschreckend ist, dass vie-

le Ermittler, Staatsanwälte und Gerichtsbehörden kaum vertieftes Wissen über das Darknet haben. Meist wissen nur Spezialermittler, wie die anonymen Marktplätze funktionieren, wie Kriminelle mit gefälschten Pässen, geklauten Kreditkarten oder Waffen handeln oder Drogen und Medikamente verschieben. Kaum ein Staatsanwalt hat jemals selbst mit der Kryptowährung Bitcoin bezahlt, die im Darknet als Standardwährung verwendet wird und bequem an zahlreichen – legalen – Online-Börsen oder Geldautomaten zu kaufen ist.[02]

DROGEN, WAFFEN UND SCHADSOFTWARE

Das Handelsvolumen auf den anonymen Marktplätzen im Darknet hat sich innerhalb der vergangenen Jahre vervielfacht. Auf „Silk Road", dem eigentlichen Pionier dieser Markplätze, sollen 2013 etwa 4000 anonyme Anbieter Produkte verkauft haben, bevor es im Oktober 2013 vom US-amerikanischen FBI geschlossen wurde.[03] Als ein Jahr später das FBI in einer weiteren Operation namens Onymous auch die Nachfolgeplattform „Silk Road 2.0" stilllegte, waren alleine im Bereich Drogen und Medikamente über 13 000 Angebote online.[04]

Auf „Silk Road" folgten „BlackBank", „Sheep Market", „Agora", „Nucleus" und viele andere. Rasend schnell entwickelte sich „AlphaBay" zum Marktführer. Im September 2015 waren in der Sparte Drogen und Medikamente schon 16 800 Angebote geschaltet. Im Februar 2016 waren es bereits 63 100, im April 2017 knapp 230 000 Online-Annoncen. Wenige Tage vor der Schließung dieser Plattform im Juli 2017 umfasste das Angebot an Drogen und Medikamente rund 260 000 Produkte.[05]

Die Bedeutung dieser verborgenen Märkte für die Kriminalität wird von vielen Strafverfolgern bis heute verkannt. Spezialisten sorgen sich um das Desinteresse ihrer ahnungslosen Kollegen. Nur wenigen Strafverfolgern scheint bewusst zu sein, welche Möglichkeiten das Darknet den Kriminellen bietet und welche Dimension das Ausmaß dieser Marktplätze inzwischen erreicht hat. Ein hoher Ermittler einer Schweizer Spezialbehörde sagt geradezu zynisch: „Rein aus Täterperspektive: Ich könnte mir keinen sichereren und besseren Ort vorstellen als das Darknet." Eigentlich möchte er sagen: „Wäre ich ein Krimineller, würde ich das Darknet nutzen."

Fast vollständig unbeobachtet sind bis heute die anonymen Foren der Hacker geblieben. In lediglich einer Handvoll solcher Plattformen tummelt sich die Weltelite der Codierer. Vorwiegend Russen, Chinesen, Iraner, Nordkoreaner und Nordafrikaner bieten auf diesen wenig bekannten Darknet-Plattformen ihre Ware an – fertig programmierte Hackersoftware, um in westliche Industrieanlagen einzudringen, diese lahmzulegen oder irgendwie zu schädigen. Einem schwarzen Brett gleich können Kunden ihre Aufrufe für einen Angriff auf eine Firma X deponieren – und Hacker liefern gegen Bezahlung auch mal ein Programm zum Test.

Längst sind Hackerangriffe bei mittleren und größeren Unternehmen zum Alltag geworden. Nur selten werden Attacken publik, denn die Unternehmen befürchten einen Reputationsschaden. Yahoo wurde innerhalb von zwei Jahren gleich zwei Mal Opfer. 2014 wurden die Daten von 500 Millionen Kunden gestohlen, im Oktober 2017 gab der Internetkonzern bekannt, dass 2013 die Daten von drei Milliarden Kunden entwendet wurden. Bei diesem größten Datenklau aller Zeiten beschafften sich Unbekannte Namen, E-Mail-Adressen, Telefonnummern, Geburtstagsdaten und Passwörter. Die Urheber des riesigen Hacks konnten nie ermittelt werden. Die Liste der in den vergangenen Jahren gehackten Dienstleister, bei denen sensible Daten im zwei- oder dreistelligen Millionenbereich gestohlen wurden, ist ein Who is Who der Branche: LinkedIn, Adobe, Badoo, MySpace, River City Media, B2B USA, Dropbox, Ashley, Nexus, Snapchat, Money Bookers und viele mehr.

International für Aufsehen sorgte auch ein Angriff auf den Schweizer Rüstungskonzern RUAG: Russische Hacker sogen beim staatlichen Rüstungsunternehmen über 20 Gigabyte heikler Daten ab – und über ein Jahr lang bemerkte dies niemand.[06] Es ist fraglich, ob die Täterschaft

01 Etwa Cai Rüffer, Fraunhofer-Institut für Sichere Informationstechnologie SIT, Vortrag, 8. Anwendertag IT-Forensik, Darmstadt 26.9.2017.

02 Siehe hierzu auch den Beitrag von Friedemann Brenneis in dieser Ausgabe (*Anm. d. Red.*).

03 Vgl. Jamie Barlett, The Dark Net, London 2014.

04 Siehe U.S. Attorney's Office, Operator Of „Silk Road 2.0" Website Charged in Manhattan Federal Court, Pressemitteilung vom 6.11.2014.

05 Eigene Erhebung 2015–2017.

06 Vgl. APT Case RUAG, Technical Report, Swiss Government Computer Emergency Response Team, 23.5.2016.

überhaupt jemals eruiert werden kann. Den Ermittlern blieb nichts anderes übrig, als den Cyberangriff zu rekonstruieren und für die Zukunft mögliche Abwehrstrategien zu entwickeln.

Viele verwendeten Ransomware (Erpressungssoftware) oder DDoS-Programme (Distributed Denial of Service) oder andere Malware, die man im Darknet kaufen kann. Die Anbieter solcher Schadprogramme haben wenig zu befürchten, denn die meisten dieser Straftaten – bis auf wenige Ausnahmen – werden weder geklärt noch strafrechtlich aufgearbeitet. Immerhin gilt in Deutschland seit 2016 eine Meldepflicht für außergewöhnliche IT-Störungen bei Anlagen der Infrastruktur. Unternehmen aus den Sektoren Energie, Informationstechnik und Telekommunikation sowie Wasser und Ernährung müssen Vorkommnisse dem Bundesamt für Sicherheit in der Informationstechnik melden.

HERAUSFORDERUNGEN OHNE ENDE

Auch jene, die Malware benutzen, haben wenig zu befürchten. Der Fall des marokkanischen Hackers F. E. hätte zu einem internationalen Musterfall werden sollen, handelte es sich doch weltweit um die erste Anklage wegen Phishing. Er ergaunerte mit zwei Kollegen und gefälschten Phishing-E-Mails die Zugangsdaten von weltweit 133 600 Kreditkartenbesitzern – und räumte deren Konten leer. Ermittelt wurde der Fall von den Schweizer Behörden, alleine hier sollen die drei mutmaßlichen Täter über drei Millionen Franken erbeutet haben. Der Fall entwickelte sich aus Ermittlersicht erfreulich, endete aber schließlich im Desaster: Die thailändische Polizei verhaftete die drei 2014 und 2015 und lieferte sie an die Schweiz aus. Es sah anfänglich gut aus für die Bundesanwaltschaft, die Schweiz wollte an den Cyberkriminellen ein Exempel statuieren. Alle drei hatten Geständnisse abgelegt, sie traten sogar den vorzeitigen Strafvollzug an. Im sogenannten abgekürzten Verfahren wurde ihnen in Aussicht gestellt, dass sie im Gegenzug zu ihren Geständnissen mit einer glimpflichen Gefängnisstrafe von drei Jahren davon kämen und ihre im Ausland verübten Straftaten nicht weiter verfolgt würden.

Doch der Musterfall, in den die Bundesanwaltschaft mehrere Jahre Arbeit investiert hatte, endete abrupt. Das Bundesstrafgericht lehnte im Oktober 2016 den Deal zwischen der Bundesanwaltschaft und den Cyberkriminellen ab. Die Schweiz sei nicht zuständig für die Beurteilung von Straftaten im Ausland, hieß es. Das Gericht ordnete die Freilassung der drei Täter an.

Ein Missstand ist der chronische Personalmangel bei den Ermittlungsbehörden. Doch die fehlenden personellen Ressourcen sind nur das eine. Teils mangelt es auf Seiten der Ermittlungsbehörden auch am notwendigen Wissen. Nicht unbedingt an der Basis, sondern bei den Entscheidungsträgern. Jüngere Mitarbeiter machen sich hinter vorgehaltener Hand lustig über ihre Vorgesetzten. Viele Führungskräfte wüssten kaum, von was die Rede sei, wenn an Sitzungen über „Botnet“ (infizierte Computer werden zum Versand von Massen-Mails verwendet), „DDoS“ (Websites von Unternehmen werden mit einer großen Anzahl Anfragen bombardiert, bis sie zusammenbrechen) oder über „AlphaBay“ (inzwischen stillgelegter anonymer Markplatz im Darknet) diskutiert werde.

Doch nicht nur das Darknet ist bei Strafverfolgern Terra incognita. Bei vielen Staatsanwaltschaften fehlt es bereits an den grundlegenden technischen Kenntnissen über das Internet als Tatmittel für kriminelle Machenschaften. Nur will das kaum jemand bestätigen. Der IT-Forensiker Maurizio Tuccillo, der bei Wirtschaftsdelikten im Auftrag von Schweizer Gerichten Computer analysiert und elektronische Spuren rekonstruiert, formuliert es so: „Staatsanwälte können mit der rasenden technischen Entwicklung nicht Schritt halten. Die Kluft zwischen dem erforderlichen und dem tatsächlichen Wissen wird immer größer.“[07] Tatsächlich scheint schon das normale Internet für viele Ermittler Neuland zu sein. Parkiert ein Betrüger seine Website auf einer fernen Pazifikinsel und domiziliert die Firma in Panama, hat er gute Chancen, ungeschoren davon zu kommen.

Staatsanwälte und andere Ermittler beklagen informell, dass sie bei solchen Sachverhalten an ihre Grenzen kommen. Häufig resignieren sie schon, wenn sie die Kommunikation eines Tatverdächtigen analysieren sollten. Heute nutzen Dienste wie WhatsApp, die von Millionen von Leuten genutzt werden, eine Ende-zu-Ende-Verschlüsselung. Um seine Spuren zu verwischen, muss man nicht mal mehr ins Darknet gehen.

07 Otto Hostettler, Eldorado Onionland, Masterarbeit, Hochschule Luzern, 2015.

Bei einigen Spezialermittlern hat inzwischen ein Sinneswandel stattgefunden. Gefragt sind auch wieder herkömmliche Ermittlungsansätze. Denn ist von Bitcoin, Tor-Anonymisierung und Darknet die Rede, geht es nicht nur um Informatik. „Interessanterweise führen die neuen Technologien zu einer Rückkehr zu klassischen Ermittlungsmethoden", sagt ein leitender Ermittler. „Das heißt, es braucht ‚Human Ressources'; also Personen, die wie vor 50 Jahren versuchen, das Vertrauen eines Kreises zu erlangen, um so an die Informationen zu gelangen, die man sonst über eine IP-Adresse erhalten würde."

Was den Umgang mit Bitcoin betrifft, herrscht bei den Ermittlungsbehörden ein eklatantes Informationsdefizit. Verbreitet ist die Meinung, mit Bitcoin gebe es keine Möglichkeiten mehr zur Rückverfolgung der Gelder. Dabei bestehen auch sehr einfache Ermittlungsansätze. Haben Ermittler eine Zielperson definiert und haben sie beispielsweise aufgrund eines fingierten Kaufs die Bitcoin-Adresse eines Händlers eruiert, können sie auf das vom Täter benutzte Cyberwallet schließen, der Aufbewahrungsort für digitales Geld. Jedes Wallet, in der Regel eine App auf dem Handy oder ein Programm auf dem Rechner, verfügt über einen standardisierten Aufbau. Ähnlich wie bei IBAN-Nummern der Banken definiert der erste Teil der Bitcoin-Adresse den Wallet-Anbieter. Ist den Ermittlern nun die verwendete App bekannt, können sie beim entsprechenden Dienstleister vorstellig werden und weitere Schritte zur Beweiserhebung einleiten. Denn die mit Bitcoin handelnden Unternehmen und Börsen, die solche Wallets anbieten, unterstehen den Finanzmarkt-Aufsichtsbehörden.

Klar ist: Das Darknet und die Kryptowährungen stellen Ermittler vor grundlegend neue Probleme. Es wird als Tatwerkzeug genutzt oder bildet den virtuellen Handlungsort. Der Europol-Ermittler Pedro Felicio schrieb in einer Analyse in der Fachzeitschrift „Kriminalistik": „In jüngerer Zeit ergeben sich neue Herausforderungen durch virtuelle Währungen, die ein ideales Instrument für Geldwäsche zu werden scheinen. Kryptowährungen (…) werden die Ermittlungsbeamten, vor allem die Finanzermittler, schon in naher Zukunft und in der gesamten Europäischen Union, vor immer größere Probleme stellen."[08]

08 Pedro Felicio, Wenn Geld spricht. Geldwäschebekämpfung durch Europol, in: Kriminalistik 7/2015, S. 434.

Tatsächlich steht die Polizei in Bezug auf die illegalen Marktplätze im Darknet vor großen Herausforderungen. Es geht um die Kombination verschiedener Phänomene, jedes ist für sich bereits komplex: Anonymisierung der Spuren im Internet, verschlüsselte Kommunikation, anonymisierte Zahlungsströme. Das Besondere daran: Fahnder müssen zwar über grundlegende Kenntnisse zum Aufbau des Internets verfügen. Gleichzeitig ist aber Erfahrung in der klassischen Ermittlungsarbeit unabdingbar.

NEUE DIMENSION DER ZUSAMMENARBEIT

Immer wichtiger wird die internationale Kooperation: Ein Verfechter solcher Zusammenarbeit ist auch Carsten Meywirth, bis Mitte 2016 Leiter der Gruppe Cybercrime beim Bundeskriminalamt in Wiesbaden: „Ein wesentlicher Erfolgsfaktor ist die internationale Kooperation. Keiner kommt alleine zurecht, ohne Zusammenarbeit geht es nicht." Dazu brauche es Mitarbeiter in den Ermittlungsteams, die besondere Cyber-Kompetenzen besitzen. Ein Team setze sich idealerweise sowohl aus Cyber-Ermittlern als auch aus Cyber-Analysten, also Fachinformatikern, zusammen.

Vorreiter in Sachen internationaler Kooperation war bisher laut verschiedenen Sachverständigen Europol. Deren Spezialeinheit European Cybercrime Center lancierte im Herbst 2014 die sogenannte Joint Cybercrime Action Taskforce (J-CAT). Hier tauschen sich Spezialisten aus Frankreich, Deutschland, Italien, Österreich, den Niederlanden, Spanien und Großbritannien aus. Dazu kommen jeweils Abgesandte aus Australien, Kanada, Kolumbien und den USA. Aus den USA sind sowohl Vertreter der Bundespolizei FBI als auch des Geheimdienstes CIA dabei. Die Schweiz ist über drei Polizeiattachés bei Europol auch im J-CAT vertreten.

Das Ziel des informellen, aber doch strukturierten Kreises ist klar: Europol will länderübergreifende Aktionen initiieren, wichtige Fälle priorisieren und Schlüsseldelikte definieren und deren Ziele identifizieren. Im Zentrum stehen bei der J-CAT die *high-tech-crimes* – Malware, Botnets und Eindringen in Computersysteme – sowie Delikte, die solche Verbrechen möglich machen. Neben dieser Taskforce lancierte Europol auch sogenannte Joint Investigation Teams. Hier tauschen sich in aktuellen Fällen ad hoc zusammengesetz-

te Teams aus unterschiedlichen Ländern aus. Die zuständigen Ermittler werden jeweils von ihren Ländern mit klar umrissenen Mandaten für diesen internationalen Informationsaustausch legitimiert und können fallweise bestimmte Informationen zur Verfügung stellen, die sonst über ein umständliches und womöglich langwieriges Rechtshilfeverfahren eingeholt werden müssten.

In den vergangenen zwei Jahren hat sich außerdem ausgehend von den USA so etwas wie eine „Weltpolizei" gebildet. Das Gremium nennt sich „Five Eyes Law Enforcement Group" (FELEG) und ist weit mehr als nur ein informelles Austauschgremium. Hier arbeiten Ermittlungsbehörden der USA, Großbritanniens, Neuseelands, Kanadas und Australiens zusammen. Klares Ziel ist der Kampf gegen die transnationale Kriminalität. Strukturiert ist FELEG in verschiedene Arbeitsgruppen, eine davon nennt sich „Cyber Crime Working Group". Dieses Team hat sich zum Ziel gesetzt, die Hintermänner, die auf den anonymen Marktplätzen eine Schlüsselstellung einnehmen, zu identifizieren und sie aus dem Verkehr zu ziehen.

Doch die internationale Zusammenarbeit ist komplex. Bereits innerhalb der USA ist die Koordination der unterschiedlichen Behörden anspruchsvoll. Aktiv sind hier etwa die Einwanderungsbehörde, die Gruppe für die innere Sicherheit Homeland Security Investigations, die US Customs and Border Protection, der US Postal Inspection Service, die Bundespolizei FBI, die Drogenvollzugsbehörde DEA und der Secret Service, die Internal Revenue Service, Criminal Investigation Division sowie das Bureau of Alcohol, Tobacco, Firearms and Explosives.

Hoffnungen setzen die Behörden auch in neue, technisch geleitete Ermittlungsmöglichkeiten. Neben klassischen Methoden wie verdeckte Ermittlungen wenden Spezialeinheiten inzwischen auch informationsbasierte Techniken an, um bei schweren Straftaten den potenziellen Tätern auf die Schliche zu kommen. Beispielsweise erarbeitete in Großbritannien die Cybersecurity Research Group der University of Bedfordshire ein neuartiges Angriffs- und Vorhersagemodell.

Dieses Monitoringmodell basiert auf der Verhaltensanalyse von Usern. Es wertet die Tätigkeiten einer Person aus, ausgehend von der Theorie, dass sich Täter in der Regel primär zu Gunsten ihrer eigenen Interessen verhalten. Mit diesem Modell soll deshalb das Verhalten eines Täters in Bezug auf unerlaubte finanzielle Gewinne, Terrorismus, Verbreitung von extremistischen Ansichten, extreme Formen von Rassismus, Pornografie und anderen Bereichen geprüft und die Radikalisierungstendenzen erkannt werden. Daraus ergibt sich ein Modell, das geeignet scheint, auch Darknet-User gezielt zu verfolgen. Fachleute attestieren diesem datenbasierten Monitoringmodell das Potenzial, Ermittler auf Aktivitäten von Nutzern hinzuweisen, die womöglich mit schweren Straftaten in Verbindung stehen könnten.

KLASSISCHE KRIMINALISTISCHE METHODEN

Entgegen den pauschalen Äußerungen verschiedener Strafverfolger sind Ermittlungen im Darknet nicht per se unmöglich. Nur weil mit dem Tor-Browser keine Rückschlüsse auf den Standort eines Computerbenutzers gezogen werden kann und die Benutzung von Bitcoin die Nachverfolgung von Zahlungsströmen erschwert, heißt dies noch lange nicht, dass keine Erkenntnisse über eine allfällige Täterschaft gewonnen werden können. Beispielsweise kann die gezielte Auswertung von Nutzerprofilen auf mehreren Marktplätzen und deren Äußerungen in verschiedenen Foren vielfach sehr konkrete Rückschlüsse auf ihr Umfeld liefern und Ausgangslage für eine weiterführende gezielte Personenrecherche sein.

Wertvolle Ansätze ergeben sich für Ermittler auch aus der Tatsache, dass Cyberkriminelle ihre Arbeitsweise letztlich – wie in der normalen Wirtschaft auch – effizient gestalten wollen. Wer Bilder wiederverwenden kann, tut dies im normalen Leben genauso wie bei kriminellen Tätigkeiten. Wer in der normalen Geschäftswelt bei der Textbearbeitung die Funktion Copy-and-paste benutzt, tut dies womöglich auch im Darknet. So kann beispielsweise mit einer Google-Bildersuche mit wenigen Klicks überprüft werden, ob ein Drogendealer neben seinem Shop im Darknet auch im offenen Internet präsent ist. Im Darknet verwendete Symbole, Logos, Fotos oder Schriftzüge führen womöglich zu einem „Underground Economy"-Shop im offenen Internet. Je nach Land, in dem die fragliche Website gehostet wird, kann die Identität einer Zielperson über den Weg der internationalen Rechtshilfe innerhalb nützlicher Frist eingeholt werden.

Eine ähnliche Möglichkeit ergibt sich aus einer Google-Suche mit einem ganzen Textausschnitt, etwa einer Produktebeschreibung oder einer Passage eines Händlerprofils auf einem Darknet-

Marktplatz. Wer solche Textelemente von fraglichen Händlern im normalen Netz googelt, staunt unter Umständen über das Resultat: Eine herkömmliche Ermittlung über das „normale" Internet kann womöglich schneller zum Ziel führen als eine langwierige IT-forensische Analyse.

Aus Ermittlersicht beruhigend, für Marktteilnehmer im Darknet eher beunruhigend zu wissen: Selbst wenn sich Händler mit aufwendigen Vorkehrungen schützen, können sie irgendwann doch von der Polizei erwischt werden. Denn das größte Risiko sind die Betrüger selber – im Internet genauso wie im normalen Leben. Mehrere international aufsehenerregende Fälle zeigen, wie effektiv es sein kann, wenn technische Ermittlungen im Darknet mit klassischen kriminalistischen Methoden im offenen Internet kombiniert werden.

Ein solches Beispiel lieferte „Shiny Flakes", der bisher wohl größte Fall von Drogen- und Medikamentenhandel im Darknet seit Auffliegen von „Silk Road" Ende 2013. Im Juli 2015 hat die Staatsanwaltschaft Leipzig Anklage gegen den 20-jährigen Maximilian S. erhoben, der anfänglich im Darknet – später auch im offen zugänglichen Internet – unter dem Namen „Shiny Flakes" Drogen und Medikamente in riesigem Umfang vertrieben hatte. Zwischen Dezember 2013 und Februar 2015 – innerhalb von nur etwa 15 Monaten – hatte er fast eine Tonne verschiedener Drogen sowie Tausende Tabletten verschreibungspflichtiger Arzneimittel im Wert von rund vier Millionen Euro verkauft, rechnete die Staatsanwaltschaft Leipzig vor.[09] Der junge Leipziger wohnte noch bei der Mutter, war im Gymnasium gescheitert, brach später eine Kellnerlehre ab. Von seinem Zimmer aus vertrieb er Crystal Meth, Kokain, Amphetamin (Speed), Ecstasy-Pillen, LSD, Haschisch und Marihuana. Dazu kamen verschreibungspflichtige Medikamente von Alprazolam bis Zolpidem. Er verschickte die Ware an seine Käufer in Deutschland, Indonesien, Australien – kurz: in die ganze Welt.

09 Siehe Staatsanwaltschaft Leipzig, Anklage gegen Betreiber von „Shiny Flakes" erhoben, Pressemitteilung vom 13.7.2015.
10 Siehe Manfred Dworschak/Steffen Winter, Shiny, der Drogenprinz des Darknet, in: Der Spiegel 34/2015, S. 20–26.
11 Zit. nach Shiny Flakes: Internet-Drogenhandel bringt „Kinderzimmer-Dealer" lange Strafe, 2.11.2015, www.heise.de/newsticker/meldung/Shiny-Flakes-Internet-Drogenhandel-bringt-Kinderzimmer-Dealer-lange-Strafe-2867741.html.
12 Vgl. Otto Hostettler, Darknet. Die Schattenwelt des Internets, Zürich 2017.

Der Versandhandel war alles andere als virtuell: Er musste die Ware wiegen, verpacken und auf die Post bringen. Schon Anfang 2014, also kurz nach dem Start seines Versandhauses, fielen der Leipziger Polizei falsch frankierte Briefe und Pakete auf – alle mit fiktiven Absenderadressen, wie der „Spiegel" später berichtete.[10] Die Polizei ging den auffälligen Paketen nach und verfolgte die Sendungsnummern der Pakete. Sie fanden schließlich eine E-Mail-Adresse, mit der sich ein unbekannter Täter zum Onlinefrankieren angemeldet hatte. Schließlich stießen die Beamten auf die Packstation 145 in der Leipziger Dantestraße, die der Verdächtige bevorzugt nutzte. Ab diesem Zeitpunkt wurde die Poststelle per Video überwacht.

Am 26. Februar 2015 schlug ein Spezialkommando der Ermittler zu. Maximilian S., der innerhalb von etwas mehr als einem Jahr vom eigenbrötlerischen Computerfreak zum Großdealer aufgestiegen war, gestand schließlich seine Darknet-Aktivitäten. Er wurde zu einer Jugendstrafe von sieben Jahren verurteilt. Dass er aufgeflogen ist, muss er sich selber zuschreiben. „Er wollte im Internet als Drogenhändler der Größte und Beste sein", sagte Staatsanwalt André Kuhnert vor Gericht.[11] Mit hoher Professionalität und erheblicher krimineller Energie habe er die Drogenbörse betrieben – basierend auf einem ausgeklügelten System mit Verschlüsselungen, anonymen Mailadressen und ausländischen Servern. Aus technischer Sicht gesehen wäre die Polizei ihm wohl kaum auf die Spur gekommen, sagte ein Ermittler vor Gericht. Doch „Shiny Flakes" schlampte im normalen Leben, bei der Frankierung – und machte sich damit bei der Post verdächtig.

Über dilettantische Händler und ahnungslose Ermittler schütteln Darknet-Verkäufer wie etwa „Edelweiss" nur den Kopf.[12] Das einzige was ihn beunruhigt, sind Schlagzeilen wie „Schlag gegen Drogendealer im Internet". Als erstes schaut er, ob die in Zeitungsmeldungen erwähnten Pseudonyme von verhafteten Akteuren der Darknet-Plattformen auch unter seinen Kunden sind. Er will wissen, wie nahe „der Einschlag" ist. Lange fühlte sich „Edelweiss" sicher, inzwischen sitzt auch er in Haft. Zum Verhängnis wurde ihm, womit er nicht gerechnet hat: Er wurde verpfiffen.

OTTO HOSTETTLER
ist Journalist und Buchautor. Zuletzt erschien „Darknet. Die Schattenwelt des Internets" (2017).
otto.hostettler@bluewin.ch

NETZ DER DISSIDENTEN

Die helle Seite im Darknet

Daniel Moßbrucker

Wer zum ersten Mal ins Darknet absteigt, wird das medial gern vermittelte Bild vom Netz der Kriminellen rasch bestätigt finden. Drogen, Waffen oder Hacking-Tools – all das gibt es dort zu erwerben. Diese kriminelle Seite sollte niemand verharmlosen, weshalb eine Diskussion über die Grenzen der Anonymität im Internet grundsätzlich berechtigt ist. Tatsächlich gibt es jedoch auch eine zweite Seite im Darknet, die weit seltener im Fokus von Medien, Ermittlern, Privatnutzern und politischen Diskussionen steht – zumindest in Deutschland.

Es ist die helle Seite des Darknets, in denen Menschen ihre Privatsphäre durch den Tor-Browser schützen wollen oder Dissidenten die Technologie der *hidden services*[01] für ihre Zwecke nutzen, um das zu tun, was hierzulande nur Erstaunen auslösen kann: Journalisten und Menschenrechtsverteidiger recherchieren unter hohem persönlichen Risiko Missstände in Autokratien und Diktaturen, um sie trotz Zensur zu veröffentlichen – entweder in ihrem Heimatland oder im Ausland, um der Weltöffentlichkeit von Geschehnissen berichten zu können. In diesem Teil des Darknets herrschen grundsätzlich andere Gesetzmäßigkeiten als im Netz der Kriminellen. Sie nutzen das Tor-Netzwerk dafür, wofür es eigentlich gemacht ist: die Identität verschleiern, vom Radar abtauchen und sich letztlich unsichtbar machen. Wer keine Offline-Kontakte zu solchen Menschen hat, bekommt diese Seite des Darknets praktisch nie zu sehen. Daraus jedoch den Schluss zu ziehen, dass sie nicht existiert, ist schlichtweg falsch. Vielmehr gilt es, das romantische Bild, wonach im Darknet reihenweise regierungskritische Blogs existieren und Whistleblower Skandale enthüllen, endlich zu korrigieren – und zu verstehen, wie Aktivisten auf Darknet-Technologien angewiesen sind.

GEHACKT, ÜBERWACHT, VERSTUMMT

Hisham Almiraat ist jemand, der ohne Anonymität im Internet wohl längst im Gefängnis sitzen würde. Der praktizierende Arzt war einer derjenigen in seinem Heimatland Marokko, der während der politischen Proteste im Arabischen Frühling Mut fasste. Um der Bewegung eine Stimme im Netz zu geben, gründete er im Februar 2011 mit einigen Mitstreitern das regierungskritische Blog „Mamfakinch“, zu Deutsch: „Wir geben nicht auf“. Sie posteten Berichte und Videos von Demonstrationen, um ihre Mitbürger zum demokratischen Aufstand zu ermutigen. „Mamfakinch“ entwickelte sich rasch zu einer verlässlichen Quelle für all jene, die mehr wissen wollten als das, was staatlich gelenkte Medien bereitstellten. Schnell hatte die Redaktion bis zu 35 Mitarbeiter. Im Sommer 2012 sank die Zahl jedoch abrupt auf fünf. Was war passiert?

Überwachungssoftware der italienischen Firma Hacking Team wurde auf die Computer der Redaktion gespielt, um die Kommunikation der Bürgerjournalisten zu durchleuchten: Skype-Gespräche wurden mitgeschnitten, E-Mails gelesen, Passwörter von Social-Media-Accounts erfasst. Wie Sicherheitsforscher des kanadischen Citizen Lab herausfanden, führte die Spur der Attacke in die marokkanische Hauptstadt Rabat.[02] Die über eine halbe Million Euro teure Software ist mutmaßlich von der Regierung beschafft worden, um Kriminelle zu überwachen – und nun waren Almiraat und seine Mitstreiter von unbescholtenen Bürgern zu Kriminellen erklärt worden. Aus Furcht vor weiteren Angriffen verließ ein Großteil der Mitarbeiter „Mamfakinch“. Ebenso schlimm war, dass Informanten aufgeflogen waren und andere Hinweisgeber das Vertrauen in das Medium verloren hatten. Schleichend sank die Frequenz der Berichte, 2014 schließlich stellte das Blog sein Angebot ein.

Will man sich heute über Hisham Almiraat im Internet informieren, scheint es, als sei alles in Ordnung. Er hat eine eigene Website und ein Twitter-Profil mit knapp 20 000 Followern, auf dem zumindest gelegentlich Tweets von ihm er-

scheinen. Als Standort gibt er Marokko an. Doch das stimmt nicht: Almiraat lebt im Exil an einem Ort in Europa, den er nirgendwo veröffentlicht sehen will. In Marokko laufen mehrere Prozesse gegen ihn, unter anderem wegen „falscher Berichterstattung", „Beleidigung öffentlicher Autoritäten" sowie „Gefährdung der Inneren Sicherheit". Ihm drohen bis zu zehn Jahre Haft. Seinen wahren Aufenthaltsort preiszugeben, würde ihn in Gefahr bringen. Doch dazu müsste er nicht in einem Blogpost darüber schreiben, wo er gerade wohnt. Die einmalige Verknüpfung seiner Social-Media- oder E-Mail-Konten mit seiner echten IP-Adresse könnte ihn verraten. Öffentliche IP-Adressen enthüllen zwar nicht automatisch die Wohnadresse samt Straße und Hausnummer, aber zumindest die ungefähre Region, also zum Beispiel Berlin, Paris oder Warschau. Es wäre für diejenigen, die nach ihm suchen, ein wichtiger Anhaltspunkt für Recherchen. Der jeweilige Internetprovider könnte dann zweifelsfrei sagen, wer hinter dem Anschluss steckt. Almiraats Kommunikation läuft daher über Anonymisierungsdienste, um solche Informationen über ihn zu verschleiern. Nur engen Vertrauten teilt er mit, wo er sich tatsächlich aufhält.

Schicksale wie die von Hisham Almiraat tauchen in den *hidden wikis* zwischen den Drogen- und Waffenshops nicht auf. Selbst wenn der Aktivist einen eigenen *hidden service* betreiben würde, um zum Beispiel mit Kollegen zu chatten oder Dateien als Backup sicher abzulegen, würde er den Link hierzu niemals öffentlich teilen. Wieso auch? Er hat kein Interesse daran, dass seine Anonymität an irgendeiner Stelle gefährdet wird. Anders als ein Drogendealer, der Anonymisierungsnetzwerke missbraucht und Sichtbarkeit erlangen muss, suchen Dissidenten geradezu die Unsichtbarkeit. Sie nutzen das Tor-Netzwerk dafür, wofür es eigentlich entwickelt wurde.

Es wäre daher unlogisch für Aktivisten, im Darknet selbst zu publizieren. Die technischen Hürden sind für die Massennutzung immer noch zu hoch, sodass sie dort praktisch kein Publikum hätten. Außerdem sehen Darknet-Seiten aus wie das Internet der 1990er Jahre, ein Abspielen von Videos zum Beispiel wäre aufgrund der extrem langsamen Ladezeit kaum möglich. Die Informationsinteressen moderner Gesellschaften können über Tor betriebene Internetseiten nicht befriedigen. Das zensurresistente Darknet ist für Journalisten eher eine Kommunikationstechnologie, um sicher arbeiten und Daten an Menschen schleusen zu können, die es frei im Internet publizieren oder traditionellen Medien weiterleiten können. Ein Beispiel hierfür ist die syrische Aktivistengruppe „Raqqa Is Being Slaughtered Silently", die mittels Anonymisierungsdiensten ihre Videos über Gräueltaten des sogenannten Islamischen Staates an Mitarbeiter im Ausland schaffte, um sie hier zu veröffentlichen.

Das Darknet ist somit als Synonym für das Bedürfnis einer Gesellschaft zu begreifen, auch in einem volldigitalisierten (und zunehmend überwachten) Zeitalter einen geschützten Raum zu haben, in dem Vertraulichkeit möglich ist. Volle Kontrolle gibt es nur in der Diktatur, eine starke Demokratie hingegen schafft Rückzugsmöglichkeiten, in denen Menschen dem staatlichen Zugriff entgehen dürfen. Die *hidden services* des Tor-Netzwerkes sind die extreme Version eines solchen Raumes. Sie werden aus politischen Gründen bisher nur von denjenigen genutzt, die aus Furcht um Leib und Leben nicht mehr darauf verzichten können. Doch auch andere Formen der geschützten Kommunikation – etwa über Virtual Private Network (VPN) oder verschlüsselte Messenger, die Teilaspekte der *hidden services* betonen – decken auf einer nachgelagerten Ebene diesen Bedarf ab. Sie im Zeichen der Kriminalitäts- und Terrorbekämpfung unverhältnismäßig stark zu bekämpfen, führt langfristig zu Kollateralschäden wie etwa einer enormen Beschränkung der Presse- und Meinungsfreiheit. Eine interne Auswertung der Menschenrechtsorganisation Reporter ohne Grenzen hat ergeben, dass bei etwa der Hälfte der Nothilfe-Fälle, in denen Journalisten in Krisensituationen geholfen worden ist, digitale Überwachung eine Rolle gespielt hat. Die NGO betreibt selbst zwei Knotenpunkte im Tor-Netzwerk, um einen Beitrag zum anonymisierten Internet zu leisten.[03] Der Fall von „Mamfakinch" und Hisham

01 Siehe hierzu auch den Beitrag von Stefan Mey in dieser Ausgabe (*Anm. d. Red.*).

02 Vgl. Morgan Marquis-Boire, Backdoors Are Forever. Hacking Team and the Targeting of Dissent?, 10. 10. 2012, https://citizenlab.ca/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent.

03 Vgl. Reporter ohne Grenzen, Schutz vor Überwachung im Internet: ROG unterstützt das Tor-Netzwerk, 24. 10. 2013, www.reporter-ohne-grenzen.de/pressemitteilungen/meldung/schutz-vor-ueberwachung-im-internet-rog-unterstuetzt-das-tor-netzwerk.

Almiraat steht in all seinen Facetten sinnbildlich für diese Entwicklung, in der die Freiheitspotenziale des Internets systematisch beschnitten werden – einschließlich des traurigen Endes.

GLOBALER HANDEL MIT ÜBERWACHUNGSSOFTWARE

Der Anfang vom Ende von „Mamfakinch" beginnt lange, bevor sich das Portal überhaupt gegründet hat. Als die ersten Ideen für das Tor-Netzwerk zu Beginn der 2000er Jahre öffentlich wurden, mehrten sich nur wenige Jahre später die Anstrengungen, solche Anonymisierungs- und Verschlüsselungsangebote umgehen zu können. Mit der massenhaften Verbreitung des Internets erwuchs zu Beginn der 2000er Jahre weltweit, vor allem aber auch in Europa, eine Überwachungsindustrie, deren globaler Handel jahrelang kaum beachtet und schon gar nicht reguliert worden ist. Firmen schlossen millionenschwere Kaufverträge mit Regierungen, die die Menschen- und Bürgerrechte ihrer Bevölkerung kaum achteten. Beispiel Syrien: Anfang 2017 veröffentlichte die ARD in einer Dokumentation über das Darknet ein Interview mit einem ehemaligen Mitarbeiter des syrischen Geheimdienstes, demzufolge sogar noch Anfang 2012 das Regime seine Überwachungstechnologie modernisieren konnte.[04] Damals tobte bereits der Bürgerkrieg, dem bis heute über 400 000 Menschen zum Opfer gefallen sind. Die Aussagen des Whistleblowers deckten sich mit Recherchen der britischen NGO Privacy International und des deutschen Blogs „netzpolitik.org". Demnach habe unter anderem die in Dubai ansässige Firma Advanced German Technology mit Sitz in Berlin den Aufbau des syrischen Überwachungsapparates bis 2012 mit ermöglicht.[05] Die Staaten im Nahen Osten rüsteten digital auf mit europäischer Technologie – und hatten im Arabischen Frühling leichtes Spiel, Initiativen wie die von Hisham Almiraat im Keim zu ersticken. Unternehmen wie das genannte Hacking Team aus Italien machen sich dabei einen schlanken Fuß: Sie lassen sich zusichern, dass ihre Überwachungstools nur zur legitimen Kriminalitäts- und Terrorbekämpfung eingesetzt werden wird. Ob das eingehalten wird, ist für Außenstehende praktisch nicht zu kontrollieren. Überwachung zeichnet sich schließlich dadurch aus, dass sie im Normalfall niemand mitbekommt.

Die EU wurde durch die Vorfälle im Arabischen Frühling wachgerüttelt und sah in einer strengeren Kontrolle solcher Verkäufe wohl auch die Möglichkeit, von eigenen Problemen und unangenehmen Diskussionen abzulenken. Auch innerhalb der EU wurde die Überwachung damals spürbar ausgeweitet, sinnbildlich dafür ist die prägende Debatte über die Vorratsdatenspeicherung. Eine Richtlinie aus dem Jahr 2006 verpflichtete die Mitgliedsstaaten, bis 2009 die Massenspeicherung im nationalen Recht zu verankern, was vielerorts zu Demonstrationen führte. 2014 kippte der Europäische Gerichtshof das Vorhaben wieder. Die Technologie dafür hatten die europäischen Regierungen jedoch zuvor bei jenen Firmen eingekauft, die nach den Protesten des Arabischen Frühlings in der Kritik standen. Manche sind dort bis heute Kunden. Schnell wuchs daher die Erkenntnis, dass es mit den eigenen Werten nicht vereinbar sei, wenn demokratische Bewegungen mit europäischer Technologie unterdrückt werden. Seit 2015 wird der Handel mit Spähsoftware reguliert. Wollen Firmen ihre Produkte außerhalb der EU anbieten, müssen sie für jedes Geschäft einen Antrag bei nationalen Behörden stellen. Die Situation hat sich seitdem verbessert, und einige Anbieter haben erkannt, dass Kunde nicht gleich Kunde ist. Dennoch gibt es immer noch Unternehmen, die Schlupflöcher in den Exportregimen gezielt ausnutzen oder sich um Handelsverbote gar nicht erst scheren. Eine Undercover-Recherche von „Al Jazeera" enthüllte im Frühjahr 2017, dass etwa die italienische Firma Intelligence and Peoples Security über außerhalb der EU ansässige Tochterfirmen bereit gewesen wäre, ihre Produkte an Kunden in Iran zu liefern. Europäische Kontrollen wären damit ebenso umgangen worden wie Wirtschaftssanktionen auf internationaler Ebene.[06]

Doch auch die Mitgliedsstaaten selbst erlauben bis heute fragwürdige Exporte von Unternehmen, die ihre Überwachungstechnologie an Länder liefern möchten, in denen die Menschen-

04 Siehe Annette Dittert/Daniel Moßbrucker, Überwachung in Syrien. Assads „elektronische Armee", 6.1.2017, www.tagesschau.de/ausland/darknet-doku-103.html.

05 Vgl. Andre Meister, Arabischer Frühling als Jagdsaison: Wie westliche Firmen den syrischen Überwachungsstaat aufgebaut haben, 13.12.2016, https://netzpolitik.org/2016/arabischer-fruehling-als-jagdsaison-wie-westliche-firmen-den-syrischen-ueberwachungsstaat-aufgebaut-haben.

06 Siehe Al Jazeera, Spy Merchants, 10.4.2017, www.aljazeera.com/investigations/spy-merchants.html.

rechtssituation problematisch ist. Großbritannien etwa genehmigte im ersten Quartal 2017 einen Deal zwischen einem britischen Hersteller und der Türkei für den Verkauf von Software zur Telefon- und Internetüberwachung zum Zweck der Strafverfolgung.[07] Zur Erinnerung: Wenige Wochen vorher wurden mindestens 13 Journalisten der regierungskritischen Zeitung „Cumhuriyet" wegen angeblicher Terror-Unterstützung festgenommen. Solche Redaktionen oder einzelne Journalisten zu überwachen, gilt in der Türkei als legale Strafverfolgung. Auch Deutschland, das in Europa eher als Vorreiter einer strengen Exportkontrolle gilt, erlaubt weiterhin Handel mit Ländern, in denen Journalisten erwiesenermaßen illegitim überwacht werden. Zwischen 2014 und 2016 gingen insgesamt neun Lieferungen an die Länder Ägypten, Algerien, Marokko, Nigeria, Saudi-Arabien und die Vereinigten Arabischen Emirate, wie die Bundesregierung in einer parlamentarischen Anfrage von Bündnis 90/Die Grünen im September 2017 mitteilte.[08] Darunter befanden sich wohl auch sogenannte Network Monitoring Systems, mit denen Geheimdienste bei großflächigem Einsatz ganze Netzwerke überwachen und damit potenziell auch die Anonymität im Darknet aufheben können.

Das Bekenntnis deutscher und europäischer Regierungen zur Stärkung der Demokratie auch außerhalb der EU hat somit weiterhin einen blinden Fleck. Aus wirtschaftlichen Interessen wird Staaten wie Marokko weiterhin ermöglicht, mithilfe modernster Technologie Aktivismus wie den von Hisham Almiraat zu unterdrücken. Die neun genannten Exporte aus Deutschland hatten einen Warenwert von 3,3 Millionen Euro. Offenbar die Schmerzgrenze, bei der eine potenzielle Überwachung von Millionen von Menschen ins Verhältnis von Geschäftserfolgen weniger Unternehmen gesetzt wird. Die Konsequenz ist eine Stärkung autoritärer Strukturen, sodass Nachfrage und Weiterentwicklung des Darknets notwendig bleibt – und hierzulande von Kriminellen missbraucht werden kann.

MEHR ÜBERWACHUNG GLEICH MEHR SICHERHEIT?

Westliche Regierungen sorgen jedoch auch durch ihre Überwachungspolitik im Inneren dafür, dass die demokratisch genutzten Rückzugsräume im Darknet schleichend beschnitten werden. Im natürlichen Spannungsfeld von Sicherheit und Freiheit schlägt das Pendel durch die Bedrohungen des internationalen Terrorismus erkennbar in Richtung der Sicherheit – die fälschlicherweise häufig mit einem Mehr an Überwachung gleichgesetzt wird. 63 Prozent der Deutschen fürchten sich vor einem Terroranschlag, wie eine im August 2017 veröffentlichte Umfrage im Auftrag der Funke Mediengruppe herausfand.[09]

Verantwortliche Politiker in Europa reagieren auf solche gesellschaftlichen Ängste regelmäßig mit Aktionismus, der meist in Überwachung mündet. Im März 2017 etwa legte die Partei von Großbritanniens Premierministerin Theresa May ein Manifest vor mit dem Ziel, dass das Vereinte Königreich der „weltweite Anführer bei der Regulierung persönlicher Daten und dem Internet" wird. Es dürfe keinen Ort im Netz geben, in dem Terroristen sicher kommunizieren können. Bereits heute hat Großbritannien die wohl schärfsten Überwachungsgesetze einer westlichen Demokratie.[10] Mit dem 2016 eingeführten Investigatory Powers Act dürfen Internet-Provider ein Jahr lang jede Online-Aktivität ihrer Kunden speichern. Jede aufgerufene Website landet in einer Datenbank, in der selbst intimste Informationen gespeichert werden. Jeder Bürger wird gläsern, obwohl er sich nie etwas zu Schulden kommen lassen hat und seine Online-Aktivität komplett legal ist.

In einer solchen Massenüberwachung wird unweigerlich auch Kommunikation erfasst, die Journalisten mit ihren Informanten pflegen. Wozu diese gestörte Vertraulichkeit führt, hat das Beispiel „Mamfakinch" eindrücklich gezeigt: Wenn kein Grundvertrauen in Medien besteht, wenden sich Hinweisgeber ab. Sukzessive wird es damit für eine Redaktion unmöglich, kritisch zu

07 Vgl. Joseph Cox, The UK Granted Spy Tech Export to Turkey Amid Its Massive Crackdown on Dissent, 19.7.2017, https://motherboard.vice.com/en_us/article/3knypk/the-uk-granted-spy-tech-export-to-turkey-amid-massive-crackdown.

08 Vgl. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Omid Nouripour, Agnieszka Brugger, Dr. Konstantin von Notz, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN (Export von Überwachungstechnik und Schutz der Menschenrechte), 27.9.2017, Bundestagsdrucksache (BT-Drs.) 18/13647.

09 Siehe Klima? Terror? Jobs? Das sind die größten Ängste der Deutschen vor der Bundestagswahl, 1.8.2017, www.derwesten.de/politik/-id211430395.html.

10 Siehe Andrew Griffin, Theresa May to Create New Internet that Would Be Controlled and Regulated by Government, 19.5.2017, www.independent.co.uk/life-style/-a7744176.html.

berichten. Diese Gefahr ist der eigentliche Grund, warum in westlichen Demokratien Journalisten besondere Schutzrechte vor einer Überwachung ihrer Arbeit haben – sowohl analog wie auch digital. Der Informantenschutz geht hierzulande auf das sogenannte „Spiegel"-Urteil des Bundesverfassungsgerichts zurück. Der damalige Verteidigungsminister Franz-Josef Strauß hatte 1962 die „Spiegel"-Affäre ins Rollen gebracht, als Polizeibeamte in Hamburg kistenweise Rechercheunterlagen aus der „Spiegel"-Redaktion trugen und Rudolf Augstein wegen des Verdachts auf Landesverrat 103 Tage im Gefängnis saß. Die Karlsruher Richter stellten später fest, dass zur Pressefreiheit auch ein Schutz des Vertrauensverhältnisses zwischen Presse und Informanten gehöre. „Er ist unentbehrlich, da die Presse auf private Mitteilungen nicht verzichten kann, diese Informationsquelle aber nur dann ergiebig fließt, wenn sich der Informant grundsätzlich darauf verlassen kann, dass das ‚Redaktionsgeheimnis' gewahrt bleibt", heißt es in dem Urteil von 1966.[11]

Es sind historische Grundpfeiler der Presse- und Meinungsfreiheit, die bei aktuellen Debatten über neue Überwachungsbefugnisse heute nicht mehr den entscheidenden Unterschied machen. Kennzeichnend ist die Diskussion um die Vorratsdatenspeicherung, die in Deutschland schon zwei Mal trotz enormer Proteste – unter anderem von Medienorganisationen – eingeführt worden ist. Hierbei wird herkömmliche Kommunikation flächendeckend erfasst, indem die Metadaten von Telefongesprächen und SMS gespeichert werden. Außerdem wird festgehalten, wem bestimmte IP-Adressen zugeordnet werden können. Begründet wird die Vorratsdatenspeicherung auch mit der sogenannten Cyberkriminalität, die nur so wirksam zu bekämpfen sei. Solche Massenüberwachung ist jedoch paradoxerweise der eigentliche Grund, warum das Darknet überhaupt existieren muss. Wer Anonymität braucht, sie aber in gewöhnlichen Umgebungen nicht mehr findet, sucht unweigerlich nach Alternativen. Auch hierzulande müssen Journalisten intensive Verschlüsselung in ihrem Berufsalltag einsetzen, und Redaktionen richteten im Zuge der Veröffentlichungen von Edward Snowden anonyme Briefkästen ein, die auf der Darknet-Technologie der *hidden services* beruhen.

11 BVerfGE (Entscheidungen des Bundesverfassungsgerichts) 20, 162 (Spiegel) 5.8.1966.

Regierungen arbeiten nun auch daran, letzte Bastionen der Anonymität wie das Darknet zu brechen. Der Schutz des Tor-Netzwerkes kann vor allem mit zwei verschiedenen Methoden ausgehebelt werden – und beide werden in Deutschland vorbereitet und durchgeführt. Einerseits können Angreifer jeden Knotenpunkt eines Anonymisierungsnetzes überwachen und damit sehen, wie die einzelnen Datenpakete durch das Netzwerk wandern. Wer also nicht nur das Ergebnis einer Verschleierung überwacht, sondern den gesamten Prozess der Verschleierung live mitschneiden kann, sieht letztlich doch wieder, wer etwa auf einen *hidden service* im Tor-Netzwerk zugreift. Was einfach klingt, ist in der Praxis extrem aufwändig. Ein Netzwerk wie das von Tor mit über 7000 Servern zu durchleuchten, verschlingt enorme Ressourcen. Im September 2017 enthüllte „netzpolitik.org" allerdings, dass der Bundesnachrichtendienst bereits 2008 ausländische Geheimdienste in Pläne einweihte, Tor mit solchen Angriffen zu überwachen. Der deutsche Auslandsgeheimdienst habe Bundesbehörden demnach gewarnt, dass das Tor-Netzwerk nicht mehr sicher sei. Der Bericht legt nahe, dass ein signifikanter Anteil der Tor-Server von Geheimdiensten betrieben wird.[12] In der 2016 verabschiedeten Novelle des BND-Gesetzes wiederum wurde dem BND das weitgefasste Recht eingeräumt, Informationen mit ausländischen Diensten auszutauschen. Mit welchen genau, erfährt die deutsche Öffentlichkeit wegen Geheimhaltungsbestimmungen nicht. Ob Erkenntnisse solcher Angriffe also auch in Ländern landen, in denen die Menschenrechte unter Druck sind, bleibt unklar. Eine Debatte, ob unsere Gesellschaft solche Angriffe ihrer Geheimdienste überhaupt billigt, beginnt damit erst gar nicht.

Andererseits kann die Verschlüsselung und Anonymisierung im Darknet ausgehebelt werden, indem die Geräte der Nutzer selbst angegriffen werden. Bei der sogenannten Quellen-Telekommunikationsüberwachung nisten sich Trojaner auf Computern und Smartphones ein, um Kommunikation abzufangen, bevor sie ver-

12 Vgl. Andre Meister, Geheime Dokumente: Der BND hat das Anonymisierungs-Netzwerk Tor angegriffen und warnt vor dessen Nutzung, 14.9.2017, https://netzpolitik.org/2017/geheime-dokumente-der-bnd-hat-das-anonymisierungs-netzwerk-tor-angegriffen-und-warnt-vor-dessen-nutzung.

schlüsselt wird. Beispielsweise können ohne Wissen des Nutzers Screenshots vom Bildschirm gemacht werden oder jeder Tastaturschlag mitgeschnitten werden. Es ist die Methode, mit der die gesamte Kommunikation der „Mamfakinch"-Redaktion abgegriffen worden war. Den Mitarbeitern wurde zum Verhängnis, dass sie auf einen Link geklickt hatten, der ihnen von den Angreifern zugeschickt worden war und vorgab, eine persönliche Botschaft zu enthalten. Tatsächlich lud sich im Hintergrund jedoch der Trojaner auf die Computer. Klar ist: Mit diesem Angriff hätte auch damals schon eine Nutzung des Darknets keinen effektiven Schutz mehr geboten.

Der Einsatz von Trojanern gilt daher als besonders gefährlich, weil er invasiver in Grundrechte eines Menschen eingreift als im analogen Zeitalter zum Beispiel noch das „bloße" Abhören eines Telefonats. Mit einem Trojaner kann der gesamte Computer durchsucht werden, auch privateste Informationen sind sichtbar. In Deutschland ist der Einsatz dieses sogenannten Staatstrojaners im Juni 2017 mit den Stimmen von Union und SPD beschlossen worden. Nicht nur zur Verfolgung von hochgefährlichen Terroristen, sondern im regulären Strafverfahren. Auch verschlüsselte Gespräche von Journalisten können prinzipiell überwacht werden.

Es mag zunächst nachvollziehbar klingen, wenn eine gefestigte Demokratie wie Deutschland solche Instrumente einführt, um Ermittlern das passende Werkzeug für die digitale Sphäre an die Hand zu geben und damit dem legitimen Strafverfolgungsinteresse des Staates gerecht zu werden. Spezialisierte Internet-Ermittler müssen im Darknet teilweise mit ansehen, wie Straftaten begangen werden, doch aus technischen Gründen können sie die Täter nicht überführen. Ferner ist eine Nutzung der Trojaner hierzulande rechtsstaatlich eingebettet, etwa durch einen Richtervorbehalt.

Doch die isolierte Fokussierung auf Deutschland missachtet, dass sich digitale Ermittlungen in einem internationalen Kommunikationsraum abspielen. Deutsche Sicherheitsbehörden müssen sich heute eigene Trojaner programmieren, weil die von der Industrie gelieferten Produkte mit den Anforderungen des Grundgesetzes nicht vereinbar sind. Solche Lösungen „von der Stange" sind zu invasiv, um rechtsstaatlich eingesetzt werden zu können, zum Beispiel weil sie zumeist keinen Unterschied machen zwischen der Erhebung von Telefongesprächen und dem Durchsuchen einer Festplatte. Es ist nur ein sogenannter Full Take möglich, der jedoch nach deutschem Recht nicht immer gestattet ist. Der Chaos Computer Club veröffentlichte 2011 den von einem hessischen Dienstleister hergestellten Trojaner, der von bayerischen Behörden zwar eingesetzt worden war, aber den engen verfassungsrechtlichen Maßgaben nicht entsprach.[13] Trotzdem verbietet es die EU bis heute nicht, solche privat hergestellten Trojaner aus der EU heraus an Drittstaaten zu verkaufen, obwohl deren Einsatz gegen Grundrechte im Inneren verstoßen würde.

Ferner nutzt ein Trojaner Sicherheitslücken in der Software aus, um sich unbemerkt auf Geräte schleichen zu können. Diese Lücken müssen im Ermittlerinteresse geheim bleiben. Doch wenn eine Software unsicher ist und Türen zur Überwachung öffnet, dann kann hier jeder hindurchgehen. Es können deutsche Staatsanwälte sein, die damit einem Drogendealer auf die Schliche kommen. Oder der marokkanische Geheimdienst, der Hisham Almiraat einen weiteren Trojaner auf seinen Computer schleust, um herauszufinden, wo er sich aufhält – und ihn in seinem Heimatland einem politisch motivierten Gerichtsverfahren zu unterziehen. Entschieden sich deutsche Sicherheitsbehörden jedoch, solche Sicherheitslücken zu melden und damit die Privatsphäre und IT-Sicherheit aller Bürger zu stärken, profitierten damit auch Menschen wie Almiraat, deren persönliche Sicherheit von der Integrität ihrer digitalen Geräte abhängt.

Gewiss ist dies eine zugespitzte Darstellung. Im Kern jedoch steht die Gesellschaft bei Ermittlungsmaßnahmen in Anonymisierungsnetzwerken wie dem Darknet heute vor einem Dilemma: Die Weiterentwicklung und der Einsatz technischer Ermittlungsinstrumente im Digitalen ist häufig nur möglich, wenn die Privatsphäre und fundamentalen Freiheitsrechte der ganzen Gesellschaft beschnitten werden – und dies nicht nur im eigenen Land, sondern insbesondere auch in weniger demokratischen Staaten.[14] Es ist riskant, sich dieses Eingeständnisses zu verweigern. Doch genau das passiert.

13 Siehe Chaos Computer Club, Chaos Computer Club analysiert Staatstrojaner, 8. 10. 2011, www.ccc.de/de/updates/2011/staatstrojaner.

14 Siehe hierzu auch den Beitrag von Matthias Schulze in dieser Ausgabe (*Anm. d. Red.*).

INSTRUMENTALISIERUNG DES DARKNETS

Prägend für die hiesige Sicherheitsdebatte sind die Fokussierung auf Bedrohungen sowie ein fehlender Diskurs darüber, ob mehr Überwachung überhaupt mehr Sicherheit bringt. Bei der Vorratsdatenspeicherung etwa haben diverse Studien bereits bestätigt, dass die Massenspeicherung die Aufklärungsquote von Straftaten nicht messbar erhöht hat, unter anderem ein Gutachten des Max-Planck-Instituts für ausländisches und internationales Strafrecht von 2011.[15] Das Bild des Darknets ist in Deutschland aber auch deshalb so schlecht, weil in der politischen Auseinandersetzung ganz bewusst die Missbrauchspotenziale betont werden. Im Juni 2017 gaben Ermittler der Generalstaatsanwaltschaft Frankfurt am Main bekannt, das bis dato größte deutschsprachige Darknet-Forum abgeschaltet zu haben. In der Pressemitteilung werden kriminelle Seiten des Forums betont, etwa dass der Amokschütze aus München hierüber seinen Waffenkauf angebahnt habe.[16] Dass der Täter die Pistole letztlich jedoch im „echten" Leben erhalten hat, bleibt unerwähnt. Vor allem aber war „Deutschland im Deep Web" kein Marktplatz, sondern eine Diskussionsplattform für über 20 000 registrierte Nutzer. Solche Seiten des Darknets fehlen in behördlichen Versionen regelmäßig. Insbesondere zum Thema Onlinesicherheit gab es fachkundige Debatten auf hohem Niveau. Mehrere tausend Menschen haben hier ihr Recht auf freie Meinungsäußerung ausgeübt. Das gesamte Forum einfach abzuschalten, ist ein massiver Eingriff in dieses Grundrecht. Öffentlicher Protest dagegen blieb jedoch aus – zu unwahrscheinlich scheint es, dass in einem Darknet-Forum legale Dinge vor sich gehen können. Zweites Beispiel: Als im März 2017 ein 19-Jähriger aus Herne einen Jungen tötete, vermeldete die Polizei rasch, der Täter habe Videos der Tat im Darknet hochgeladen und die Tat dort auch angekündigt. Bis heute findet sich in nahezu allen Presseberichten diese Version. Wenige Tage später korrigierte die Polizei in einem Nebensatz jedoch ihre Darstellung. Tatsächlich hatte der Mann über WhatsApp Videos der Tat verschickt und darum gebeten, sie in das Forum „4Chan" zu stellen. Das Darknet war an keiner Stelle involviert.[17]

Doch solche Narrative des kriminellen Darknet prägen sich ein im kollektiven Bewusstsein. Dagegen zu argumentieren, wird schnell unmöglich. Wer kann schon dagegen sein, Kriminalität zu bekämpfen? Zumal die demokratischen Potenziale des Darknets kaum sichtbar sind und der Bedarf weniger vor der eigenen Haustür als vielmehr in anderen Teilen der Welt besteht. Dennoch muss in der Sicherheitsdebatte das demokratische Moment wieder stärkere Beachtung finden. „Wer die Freiheit aufgibt, um Sicherheit zu gewinnen, wird beides verlieren", sagte Benjamin Franklin schon im 18. Jahrhundert. Seine Worte sind heute aktueller denn je. Zweifelsohne gibt es im Darknet Kriminalität, natürlich missbrauchen die Feinde der Freiheit Technologie für ihre Zwecke. Dem muss der Staat mit Augenmaß begegnen und im Rahmen seiner Möglichkeiten mit regulatorischen Mitteln entgegenwirken. Das Internet benötigt jedoch Rückzugsräume im Schutze der Anonymität. Zur Freiheit gehört auch die Bereitschaft, das Missbrauchspotenzial dieser Räume zu akzeptieren und bis zu einem gewissen Maß auch auszuhalten. Eine offene Gesellschaft ist naturgemäß anfällig für Kriminalität und Terrorismus. Sie wird es immer sein, wenn ihre Mitglieder freiheitlich-demokratische Werte leben. Den Wert des Darknets an sich zu verneinen, heißt damit zwangsläufig, unsere Freiheitsrechte infrage zu stellen.

15 Siehe Hans-Jörg Albrecht et al., Schutzlücken durch Wegfall der Vorratsdatenspeicherung?, Max-Planck-Institut für ausländisches und internationales Strafrecht, Juli 2011, www.mpg.de/5000721/vorratsdatenspeicherung.pdf.

16 Vgl. Generalstaatsanwaltschaft Frankfurt am Main, BKA: Festnahme des mutmaßlichen Betreibers einer großen deutschsprachigen Darknet-Plattform und Beschlagnahme des Servers der Plattform, 12.6.2017, www.presseportal.de/blaulicht/pm/7/3657474.

17 Vgl. Daniel Mützel/Theresa Locker, Warum der mutmaßliche Kindermörder von Herne auf 4chan gefeiert wird, 3.9.2017, https://motherboard.vice.com/de/article/vvjb9d/warum-der-mutmassliche-kindermorder-von-herne-auf-4chan-gefeiert-wird.

DANIEL MOßBRUCKER
ist Referent für Internetfreiheit bei Reporter ohne Grenzen und arbeitet als freier Journalist sowie Security-Trainer in Berlin. Er ist Co-Autor der ARD-Dokumentation „Das Darknet – Reise in die digitale Unterwelt" (2017).
mail@daniel-mossbrucker.de

GOING DARK?

Dilemma zwischen sicherer, privater Kommunikation und den Sicherheitsinteressen von Staaten

Matthias Schulze

In einer digitalisierten Welt verwenden immer mehr Kommunikationsdienste wie WhatsApp nicht abhörbare Verschlüsselung. Aus diesem Grund warnen Nachrichtendienste und Strafverfolgungsbehörden mit jedem neuen Terroranschlag vor dem „Going dark"-Problem. „Going dark" meint im Geheimdienstjargon das Versiegen eines Informationskanals. Das umfasst ein hypothetisches Zukunftsszenario, in dem alle oder ein Großteil digitaler Kommunikation verschlüsselt, und somit nicht mehr nachvollziehbar für staatliche Behörden, stattfindet. Das legitime Sicherheitsinteresse des Staates und der Schutz der Bürger, etwa vor Terroranschlägen, seien dadurch gefährdet. „Verschlüsselung birgt die Gefahr eines dunklen Pfades", so der ehemalige FBI-Direktor James Comey.[01] Aus diesem Grund tauchen weltweit immer mehr Forderungen auf, staatliche Zugriffe auf verschlüsselte Kommunikationsinhalte zu gewährleisten, etwa durch eine mandatierte Schwächung von Verschlüsselung, den Einbau von Hintertüren oder dem Einsatz von Spionagesoftware. Im Kontext ansteigender Cyberbedrohungen argumentieren neben Datenschützern und Computerwissenschaftlern allerdings auch zunehmend Geheimdienste gegen eine absichtliche Schwächung von Software und Verschlüsselung.

DATEN ZUM EINSATZ VON VERSCHLÜSSELUNG

Weltweit gibt es rund 865 verschiedene Verschlüsselungsprodukte aus 55 Ländern, davon 112 aus Deutschland.[02] Dazu kommen diverse Open-Source-Projekte, die von jedem frei weiterentwickelt und vermarktet werden können. Kommunikationsverschlüsselung wird zunehmend bei Messenger-Diensten wie WhatsApp, Threema, Signal und iMessage eingesetzt. Andere Dienste wie Google Allo, Facebook Messenger oder Telegram bieten die Verschlüsselung optional an. 69 Prozent der Deutschen nutzen solche Messenger. Davon verwenden 63 Prozent WhatsApp, das zu Facebook gehört, gefolgt von Skype (16 Prozent), Facebook Messenger (15 Prozent) und Apples iMessage (9 Prozent).[03]

Unverschlüsselte SMS sind weltweit auf dem Rückzug. 2015 wurden in Deutschland etwa 667 Millionen WhatsApp-Texte, aber nur noch 40 Millionen SMS verschickt.[04] Klassische Telefonate finden in der Regel noch unverschlüsselt statt. Ein Großteil der jährlich rund 625 Milliarden deutschen E-Mails ist zudem im Klartext abfangbar, da nur circa 16 Prozent der Deutschen PGP-Verschlüsselung nutzen.[05] Bei diesem Verfahren besitzt jeder Nutzer zwei Codeschlüssel. Seit der Erfindung von Web-Verschlüsselung für Browser (HTTPS) 1996 nutzt gegenwärtig die Hälfte aller Websites Verschlüsselung.[06] Die gesamte Internetkommunikation kann mit VPN-Software (Virtual Private Network) verschlüsselt werden, die von circa 16 Prozent der Deutschen genutzt wird.[07]

Neben sicherer Kommunikation spielt Verschlüsselung von Datenträgern eine zunehmende Rolle. Seit 2014 sind zum Beispiel alle iPhones ab Werk verschlüsselt. Dabei wird der Schlüssel aus dem Nutzer-Pin und einem einzigartigen Gerätecode generiert und auf einem speziellen Chip (*secure enclave*) auf den Endgeräten gespeichert. Dieser Diebstahlschutz führt dazu, dass Apple selbst nicht in der Lage ist, Geräte der Kunden zu entschlüsseln. Etwa 17 Prozent der Deutschen verwenden iPhones und 80 Prozent Android-Smartphones.[08] Googles Android bietet Verschlüsselung lediglich optional bei neueren Versionen an. Android-Smartphones sind in der Regel einfacher von Strafverfolgungsbehörden auszulesen. Daten zur Anzahl verschlüsselter PCs liegen leider nicht vor, aber alle modernen Betriebssysteme bieten Verschlüsselung optional an.

GESCHICHTE DES „GOING DARK"-PROBLEMS

Bereits 1979 warnte der damalige Direktor der US-amerikanischen National Security Agency (NSA) Bobby Inman, dass eine öffentliche Nutzung von Verschlüsselungstechnologie die Auslandsüberwachung erschweren würde.[09] Er forderte daher ein Verbot ziviler Nutzung dieser Technologie, die damals noch ähnlichen Exportrestriktionen unterlag wie zum Beispiel Rüstungstechnologie.

1993 erneuerten FBI und NSA ihre Warnungen vor dem „Going dark"-Problem: Kriminelle und Terroristen würden bald digital über das Internet kommunizieren, und analoge Telefonüberwachung werde wirkungslos. Deshalb forderten sie, dass neue digitale Kommunikationsgeräte einen sogenannten Clipper Chip per Werk enthalten sollten, der von der NSA entwickelte wurde. Dieser Chip ermöglichte zwar verschlüsselte Kommunikation, hatte aber eine Hintertür: Eine Kopie des Schlüssels sollte bei staatlichen Stellen gespeichert werden (*key escrow*). Wenn also eine laufende Ermittlung die Kommunikationsüberwachung von Kriminellen erforderlich gemacht hätte, wäre es möglich gewesen, eine Schlüsselkopie per Richterbescheid abzurufen, um die Kommunikation zu entschlüsseln. Der Clipper Chip versprach einen Kompromiss zwischen sicherer Kommunikation und einem legalen, staatlichen Zugang.[10]

Es gab allerdings einen Haken: Die Technik war unsicherer als die Alternativen, die es bereits auf dem Markt gab, und konnte schnell geknackt werden. Computerwissenschaftler argumentieren seitdem, dass Systeme mit legalen staatlichen Hintertüren inhärent unsicher sind. Hintertüren müssen aufwendig getarnt sein. Zudem muss die Authentizität der Kommunikationsteilnehmer gewährleistet sein, damit sich Hacker nicht als Behörden ausgeben. Genau das ist aber zu befürchten, weil die Sicherstellung exklusiver Regierungshintertüren technisch unmöglich ist. Jede Lücke kann von jedem ausgenutzt werden.[11] Kurzum: Je mehr Zugangsmöglichkeiten existieren, desto komplexer und somit unsicherer wird die Verschlüsselungstechnologie. Wenn Verschlüsselung heutzutage durchbrochen wird, liegt das häufig an Fehlern in der Software-Implementierung und nicht an den Verschlüsselungsalgorithmen selbst.

Dazu kommt, dass die externe Speicherung von Schlüsseln das Diebstahl- oder Missbrauchsrisiko erhöht, was insbesondere in Zeiten allumfassender krimineller Cybervorfälle ein immenses Problem ist. 2015 stahlen Hacker etwa eine sensible Datenbank aller Mitarbeiter der US-Regierung, inklusive Fingerabdrücke und Sicherheitsklassifikation.[12] Unter dem Codenamen „Vault 7" veröffentlichte Wikileaks im März 2017 streng geheime Dokumente über staatliche Cyber-Angriffstools der CIA. Eine zentrale Schlüsseldatenbank wäre außerdem ein hochrangiges Ziel für alle Hacker weltweit, sowohl staatliche als auch nicht staatliche. Gegen die Schlüsselhinterlegung spricht auch der Trend zu Einmalpasswörtern, Zwei-Faktor-Authentifizierung und Gerätepins, bei denen es rein technisch keinerlei Schlüsselkopie geben kann und IT-Hersteller selbst nicht die Kommunikationsinhalte ihrer Kunden auslesen können.[13]

01 James Comey, Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?, 6.10.2014, www.brookings.edu/events/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

02 Vgl. Bruce Schneier/Kathleen Seidel/Saranya Vijayakumar, A Worldwide Survey of Encryption Products, Berkmann-Klein Center Research Publication, 11.2.2016.

03 Vgl. Andreas Weck, WhatsApp, Telegram und Co, 2.7.2016, http://t3n.de/news/messenger-nutzung-deutschland-whatsapp-threema-723684.

04 Vgl. Statista, Anzahl der verschickten SMS- und WhatsApp-Nachrichten in Deutschland von 1999 bis 2014 und Prognose für 2015 (in Millionen pro Tag), 2017.

05 Vgl. Daniel Berger, Umfrage: Nur 16 Prozent der Deutschen verschlüsseln ihre E-Mails, 22.5.2017, www.heise.de/newsticker/meldung/Umfrage-Nur-16-Prozent-der-Deutschen-verschluesseln-ihre-E-Mails-3720597.html.

06 Vgl. Klint Finley, Half the Web Is Now Encrypted, 30.1.17, www.wired.com/2017/01/half-web-now-encrypted-makes-everyone-safer.

07 Vgl. Kathryn Nave, How VPN Use Varies by Country, 1.7.2016, www.wired.co.uk/gallery/vpn-use-varies-by-country.

08 Vgl. Stefan Beiersmann, Marktanteil von iOS steigt – außer in Deutschland, 9.12,2016, www.zdnet.de/88284256.

09 Vgl. Thomas Rid, Maschinendämmerung. Eine kurze Geschichte der Kybernetik, Berlin 2016, S. 303–310.

10 Vgl. Steven Levy, Battle of the Clipper Chip, 12.6.1994, www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html.

11 Siehe Priscilla Guo, Who is Our Enemy?, 27.4.2016, http://harvardpolitics.com/covers/going-dark-who-is-our-enemy.

12 Vgl. Ellen Nakashima, Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say, 9.6.2015, www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say.

13 Vgl. Harold Abelson et al., Mandating Insecurity by Requiring Government Access to All Data and Communications, Computer Science and Artificial Intelligence Laboratory Technical Report, 6.7.2015, S. 18.

Kryptografie erzeugt also ein Dilemma: Entweder fördert man eine starke Verschlüsselung, die Schutz vor Hackern bietet, aber auch die Nutzung durch Terroristen ermöglicht; oder man nutzt schwächere Verschlüsselungstechnologien, um Terroristen überwachen zu können, mit der Folge eines geringeren Sicherheitsniveaus gegen Hacker und Cyberangriffe. Aus diesem Grund setzte sich in den 1990er Jahren der von liberalen und konservativen Gruppen getragene Konsens durch, dass die Vorteile von guter Verschlüsselung die Nachteile im digitalen Zeitalter aufwiegen würden. Mit einem weltumspannenden, grenzüberschreitenden Internet war ein Verbot von Verschlüsselung ohnehin nicht mehr realisierbar – Verschlüsselungssoftware ist frei verfügbar. Staaten können kaum kontrollieren, welche Software auf den Geräten ihrer Bürger installiert ist. Deswegen wurden weltweit Exportverbote und die Reglementierung von Verschlüsselung weitgehend aufgehoben.

VERSCHLÜSSELUNG UND ANTITERRORKAMPF

Im Zuge des Antiterrorkampfes gerät dieser Konsens zunehmend unter Beschuss, unter anderem weil Verschlüsselung, etwa durch VPN-Clients oder das Tor-Netzwerk, ein Umgehen zahlreicher technischer Überwachungslösungen wie die anlasslose Datensammlung an zentralen Internetknoten ermöglicht. Der Inhalt verschlüsselter Internetdatenpakete kann nicht ohne erheblichen technischen Aufwand im Transit ausgelesen werden. Verschlüsselung ist der natürliche Gegner all jener, die mit Überwachung zu tun haben. Allerdings darf nicht vergessen werden, dass die Metadaten der Kommunikation – wann und wie oft welcher Sender mit welchem Empfänger kommuniziert – auch mit Verschlüsselung sichtbar bleiben. Verschlüsselung allein sorgt noch nicht für Anonymität.

Die Debatten um staatlichen Zugang zu verschlüsselter Kommunikation werden immer wieder nach Terroranschlägen entfacht. Großbritannien und Frankreich forderten kurz nach den Angriffen von Paris im November 2015 legale Zugriffsmöglichkeiten für Behörden auf WhatsApp-Kommunikation, obwohl die Täter nachweislich über unverschlüsselte SMS kommunizierten und den Behörden im Vorfeld bekannt waren.[14] Das Argument ist seit den 1990er Jahren dasselbe: Verschlüsselung schaffe abhörsichere Bereiche, die legitime staatliche Strafverfolgung behindern.[15]

Als 2016 das FBI das iPhone des Attentäters von San Bernardino wegen Verschlüsselung nicht auslesen konnte, brachten Innenpolitiker einen Vorschlag ins Spiel, der bereits in den sogenannten Crypto Wars der 1990er Jahre diskutiert wurde. In Anlehnung an die ursprüngliche Fassung des Communications Assistance for Law Enforcement Act von 1994 sollten IT-Hersteller verpflichtet werden, auf staatliche Anordnung ihre Produkte zu verändern, um Überwachung zu ermöglichen.[16] Genau dies sah auch das Burr-Feinstein Encryption Bill von 2016 vor: Cyber-Sicherheitsfeatures zum Schutz vor Hackern und Cyberspionage sollten deaktiviert werden, um staatliche Überwachung zu ermöglichen. Dass eine liberale Demokratie transnational agierende IT-Unternehmen zwingen wollte, absichtlich Sicherheitsmechanismen zu schwächen, galt damals wie heute als Normüberschreitung, sodass die Initiative seitdem auf Eis liegt.[17] Allerdings hatte der Vorschlag sogenannter staatlich mandatierter Schwachstellen internationale Strahlkraft, sodass ähnliche Initiativen etwa in Russland und China eingeführt wurden. Auch andere autoritäre Regime gehen zunehmend gegen Verschlüsselung vor. Aber auch Großbritannien führte mit dem Investigatory Powers Act 2016 ähnliche Vorgaben ein.[18] Die Vereinten Nationen kritisieren diese Maßnahmen als unverhältnismäßig und sehen sie im Konflikt mit demokratischen Grundrechten.[19] Neben der Schweiz diskutiert Australien gegenwärtig ebenfalls diese Idee.

14 Vgl. Glen Moody, Paris Terrorists Used Burner Phones, Not Encryption, to Evade Detection, 21.3.2016, https://arstechnica.com/tech-policy/2016/03/paris-terrorist-attacks-burner-phones-not-encryption.

15 Vgl. Matthias Schulze, Clipper Meets Apple vs. FBI, in: Media and Communication 1/2017, S. 54–62.

16 Siehe Susan Landau, The Risks Posed by New Wiretapping Technologies, Cambridge MA 2011, S. 82–89.

17 Siehe Rainey Reitman, Burr-Feinstein Proposal Declared „Dead" for This Year, 27.5.2016, www.eff.org/de/deeplinks/2016/05/win-one-security-burr-feinstein-proposal-declared-dead-year.

18 Vgl. Alex Hern, UK Government Can Force Encryption Removal, but Fears Losing, Experts Say, 29.3.2017, www.theguardian.com/technology/2017/mar/29/uk-government-encryption-whatsapp-investigatory-powers-act.

19 Vgl. Matt Burgess, UN Warns UK's IP Bill „Undermines" the Right to Privacy, 9.3.2016, www.wired.co.uk/article/un-privacy-ip-bill-not-compliant-international-law.

Wenn westliche Demokratien mit dem Argument der Terrorabwehr Unternehmen zwingen, ihre Software zu schwächen, legitimiert dies ähnliche Praktiken in autoritären Regimen – mit dem Unterschied, dass dort mit diesem Argument auch gegen Dissidenten, Journalisten und Menschenrechtsorganisationen vorgegangen wird. Teil des Dilemmas ist, dass Terroristen, Dissidenten und Journalisten verschlüsselte Kommunikation gleichermaßen nutzen, um nicht von Behörden überwacht zu werden. Bei den Anschlägen von Ansbach, Saint-Étienne-du-Rouvray (beide Juli 2016) und London 2017 konnte festgestellt werden, dass der sogenannte Islamische Staat (IS) mit den Tätern über verschlüsselte Messenger wie Telegram in Kontakt stand, sie instruierte und womöglich radikalisierte.[20] Manuale des IS empfehlen eine ganze Reihe verschiedener Verfahren, um der zunehmenden staatlichen Kommunikationsüberwachung zu begegnen. Dazu zählt, Technologie zu meiden, die von Behörden kompromittiert ist oder im Verdacht steht, staatliche Hintertüren zu enthalten.[21]

Diese Manuale deuten darauf hin, dass eine staatliche Schwächung von Verschlüsselung als Argument im Antiterrorkampf mehr schadet als nützt. Wenn Staaten auf ihrem Territorium Software mit staatlichen Hintertüren mandatieren, trifft dies nicht die Terroristen. Hingegen würden die eigenen Bürger gezwungen, unsichere Software zu nutzen und sich größeren Gefahren durch Hacker auszusetzen, während Kriminelle in der Regel zu sicheren Diensten wechseln. Diese sind frei im Internet verfügbar. Zudem gibt es diverse Open-Source-Anwendungen, hinter denen eine Entwicklercommunity und kein Unternehmen steht, das per Gesetz zu Schwachstellen gezwungen werden könnte.

STAATSTROJANER UND STAATLICHES HACKING

Neben Krypto-Verboten, Schlüsselhinterlegung und staatlich mandatierten Schwachstellen gibt es noch die Idee, Softwareschwachstellen in Betriebssystemen auszunutzen, um Verschlüsselung zu umgehen. Staatliche Spionageprogramme würden dabei wie Schadsoftware ein Gerät infizieren und die Kommunikation mitprotokollieren, noch bevor die Verschlüsselung einsetzt. In Deutschland gibt es seit mindestens 2008 Überlegungen dazu, also bevor Ende-zu-Ende-Verschlüsselung in Messenger Einzug hielt.[22] Das Problem ist, dass solche Staatstrojaner – wie jede andere Form von Schadsoftware – die Sicherheit des betroffenen Systems gefährden. Damit diese Schadsoftware unerkannt bleibt, müssen Sicherheitsmechanismen wie Sandboxen oder Antivirensysteme umgangen werden. Zudem können prinzipiell alle Daten (Fotos, biometrische Daten, Ortsbestimmungen) des betroffenen Systems heimlich an Polizei-Server gesendet werden. Solch mächtige Überwachungssoftware hebelt also zentrale Cyber-Sicherheitsmechanismen auf den Geräten aus und schafft weitere Angriffsflächen, etwa wenn die Software mit den Behörden über das Internet kommuniziert. Diese Gefahr ist keinesfalls abstrakt.

2016 wurde eine Schadsoftware Namens Pegasus bekannt, die auf eine bisher unbekannte Softwareschwachstelle des Betriebssystems iOS setzte. Diese Schwachstelle betraf alle iPhones, also weltweit über eine Milliarde Geräte, die sowohl von Privatnutzern als auch von Politikern genutzt wurden. Pegasus wurde als Staatstrojaner an Mexiko verkauft und dort gegen Journalisten und Mitarbeiter von NGOs eingesetzt, die in staatlichen Korruptionsfällen ermittelten.[23] Die israelische Entwicklerfirma NSO Group bewirbt die Software aber auch als Angriffstool für den staatlichen Cyberkrieg.[24]

VERSCHLÜSSELUNG UND CYBERSICHERHEIT

Mittlerweile vergeht kaum ein Monat ohne einen Cyber-Sicherheitsvorfall, der Millionen Internetnutzer betrifft. So meldete Yahoo im Oktober 2017 etwa, dass im August 2013 alle drei Milliarden Nutzerkonten von Cyberangriffen kompromit-

20 Siehe Greg Toppo, London Terror Attacker Used WhatsApp, the Encrypted Messaging App, Before Rampage, 26.3.2017, www.usatoday.com/story/news/2017/03/26/london-attacker-whatsapp-message/99668890.

21 Vgl. Aaron Brantly, Innovation and Adaptation in Jihadist Digital Security, in: Survival 1/2017, S. 79–102.

22 Siehe etwa Kai Biermann, Vertraulichkeit geht vor, 27.2.2008, www.zeit.de/online/2008/09/online-durchsuchung-urteil.

23 Vgl. John Scott-Railton et al., Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware, 19.6.2017, https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso.

24 Vgl. Lilian Ablon/Andy Bogart, Zero Days, Thousands of Nights. The Life and Times of Zero-Day Vulnerabilities and Their Exploits, Santa Monica 2016.

tiert wurden.[25] Data Breach Statistics zählt insgesamt knapp neun Milliarden individuelle Datenpunkte wie Benutzernamen und E-Mail-Konten, die seit 2013 von Hackern gestohlen wurden. In lediglich vier Prozent der Fälle konnten diese Daten nicht von Hackern weiterverwendet werden – zum Beispiel für Spam, Phishing oder Identitätsdiebstahl –, weil die Daten verschlüsselt waren.[26]

Statistisch betrachtet, ist eher früher als später jeder von einem Cyber-Sicherheitsvorfall betroffen. Das liegt unter anderem daran, dass immer mehr Akteure, privat und staatlich, Kapazitäten für komplexe, offensive Cyberoperationen zur Spionage und Sabotage aufbauen. Hacking wird zunehmend als legitimes Werkzeug staatlichen Handelns begriffen. Mehr als 30 Staaten weltweit bauen derzeit Kommandostrukturen zur Cyber-Kriegführung auf.[27] Hierzu gehören westliche Regierungen, aber auch Russland, China, Nordkorea oder die Türkei. Dadurch entsteht ein digitaler Rüstungswettlauf. IT-Unternehmen bezahlen jedes Jahr Millionen Euro, um Softwareschwachstellen in ihren Produkten zu beheben. Gleichzeitig geben Staaten Steuergelder für Überwachungssoftware und Sicherheitslücken aus, die je nach Funktionsumfang zwischen Tausenden und Millionen Euro kosten. Die üblichen Marktpreise zum Einkauf von Sicherheitslücken in WhatsApp und anderen Diensten bewegen sich bei 500 000 US-Dollar.[28] Staaten befeuern also einen grauen, internationalen Markt für Schadsoftware und Schwachstellen, unter dem sie selbst leiden. Je nach Schätzung kosten Cybervorfälle im Jahr bis zu 400 Milliarden US-Dollar, Tendenz steigend.[29]

Daher kommen immer mehr Experten zu dem Schluss, dass Cyberbedrohungen ein viel größeres Problem darstellen als Terrorangriffe, die nach wie vor sehr selten sind. US-Geheimdienste argumentieren, dass Verschlüsselung und besserer Datenschutz die beste Verteidigungslinie gegen Cyberbedrohungen sind. In einem US-Geheimdienstreport heißt es, die Auswirkungen von Datenlecks würden abgemildert, wenn Daten verschlüsselt und anonymisiert und somit wertlos für Diebe wären.[30]

Gegen eine absichtliche Schwächung von Verschlüsselung und Software argumentiert zum Beispiel auch der ehemalige Chef des britischen Inlandsgeheimdienstes MI5 Jonathan Evans: Zwar sei Terrorismus ein Problem, aber der Nutzen von Verschlüsselung für die Cybersicherheit in Zeiten von Cyberangriffen auf kritische Infrastrukturen größer.[31] Ähnlich argumentiert der ehemalige NSA-Direktor Michael Hayden: Die strategische Cybersicherheit der amerikanischen Computerindustrie sei wichtiger als der taktische Gewinn, der durch Kommunikationsüberwachung entstehe. Insgesamt sei Amerika mit mehr Verschlüsselung sicherer, auch wenn dadurch nicht mehr jede kriminelle Kommunikation überwacht werden könne.[32]

ZUKUNFT VOLLER VERSCHLÜSSELUNG?

Solche Statements lassen Zweifel an der Stichhaltigkeit der „Going dark"-These aufkommen. Die Annahme einer Zukunft voller Verschlüsselung ist heute genauso unwahrscheinlich, wie sie es in den 1990er Jahren war. Hohe Komplexität und geringe Nutzerfreundlichkeit schrecken die meisten Anwender ab, PGP-Verschlüsselung und andere Anwendungen zu benutzen. Zudem gibt es Industrietrends, die eine weite Verbreitung von Verschlüsselung verhindern. Unternehmen wie Google werten die Kommunikationsinhalte ihrer Dienste aus, um personalisierte Werbung schalten zu können. Diese Dienste werden außerdem immer häufiger mit Drittanbieterdiensten verknüpft, die ihrerseits an der Auswertung von Kundenkommunikationsinhalten interessiert sind. Verschlüsselung würde die Integration dieser Dienste erschweren

25 Vgl. Daniel AJ Sokolow, Rekordhack bei Yahoo war drei Mal so groß, 4. 10. 2017, www.heise.de/security/meldung/Rekordhack-bei-Yahoo-war-drei-Mal-so-gross-3849303.html.

26 Siehe Breach Level Index 2017, http://breachlevelindex.com.

27 Vgl. Steve Ranger, US Intelligence: 30 Countries Building Cyber Attack Capabilities, 5. 1. 2017, www.zdnet.com/article/us-intelligence-30-countries-building-cyber-attack-capabilities.

28 Vgl. Michael Mimoso, Zerodium Offers $ 500K for Secure Messaging App Zero Days, 23. 8. 2017, https://threatpost.com/zerodium-offers-500k-for-secure-messaging-app-zero-days/127610.

29 Siehe Tom Risen, Study: Hackers Cost More Than $ 445 Billion Annually, 9. 6. 2014, www.usnews.com/news/articles/2014/06/09/study-hackers-cost-more-than-445-billion-annually.

30 Vgl. James Ball, Secret US Cybersecurity Report: Encryption Vital to Protect Private Data, 16. 2. 2015, www.theguardian.com/us-news/2015/jan/15/-sp-secret-us-cybersecurity-report-encryption-protect-data-cameron-paris-attacks.

31 Siehe James Grierson, Ex-MI5 Chief Warns Against Crackdown on Encrypted Messaging Apps, 11. 8. 2017, www.theguardian.com/technology/2017/aug/11/ex-mi5-chief-warns-against-crackdown-encrypted-messaging-apps.

32 Michael Hayden, The Pros and Cons of Access to Encrypted Files, 17. 2. 2016, www.youtube.com/watch?v=6HNnVcp6NYA.

und die Auswertung von Nutzerkommunikation verhindern. Diese Big-Data-Geschäftsmodelle sorgen nicht nur für gläserne Kunden, sondern bringen enorm viel Licht ins Dunkel. Noch niemals zuvor gab es derartige Mengen teils frei zugänglicher Daten, die tiefe Einblicke in das Handeln und die Vorlieben von Individuen ermöglichen. Zudem tragen heute 78 Prozent der Deutschen permanent ein Smartphone mit eingebautem GPS-Peilsender mit sich herum.[33]

Vor diesem Hintergrund ist das Versiegen von Datenquellen zu hinterfragen. Jeder Evolutionsschritt der Kommunikationstechnologie bringt neue Abhörmöglichkeiten mit sich. Das Aufdampfen von Briefen wurde von analoger Telefonüberwachung ersetzt, die zunehmend von digitaler Überwachung ersetzt wird. Im Datenzeitalter werden Kommunikationsinhalte unwichtiger, und die Kombination verschiedener Metadaten spielt eine größere Rolle. Immer mehr Datenquellen stehen auch Behörden zur Verfügung, etwa biometrische Datenbanken, Videoüberwachung, automatisierte Kennzeichenüberwachung und Vorratsdatenspeicherung. Die Einsatzschwellen dieser teils rechtsstaatlich problematischen Maßnahmen wurden im Krieg gegen den Terror zudem immer weiter gesenkt und auf immer mehr Tatbestände ausgeweitet. Gegenwärtig wird weltweit das sogenannte *predictive policing* getestet, also die Vorhersage von Verbrechen noch bevor diese stattfinden.[34] Big Data und künstliche Intelligenz werden den Trend zur biometrischen Verhaltensmusteranalyse – wie etwa beim Pilotprojekt zur automatischen Gesichtserkennung am Berliner Bahnhof Südkreuz – bestärken. Es gibt also nicht mehr Dunkelheit, sondern immer mehr Licht. Gleichzeitig war Deutschland, laut polizeilicher Kriminalstatistik, noch nie so sicher wie heute.

Was allerdings weitgehend im Dunkeln liegt, sind Daten darüber, in wie vielen Ermittlungsfällen verschlüsselte Kommunikation wirklich zum Erliegen der Ermittlungen geführt hat. Einiges spricht dafür, dass Behörden das Problem größer machen, als es letztlich ist, um zum Beispiel neue Kompetenzen zu erhalten. Als etwa das FBI 1993 vor dem „Going dark"-Problem warnte, gab es von 925 Fällen jährlicher Telekommunikationsüberwachung keinen einzigen Fall, in dem Verschlüsselung vorkam. Das FBI hatte also rein proaktiv gewarnt.[35] 2015 wurden in den USA bereits 4148 Überwachungsanordnungen erteilt, und es gab nur sieben Fälle mit Verschlüsselung, wovon vier nicht entschlüsselt werden konnten.[36]

Schaut man sich die Ermittlungen der jüngsten Terrorvorfälle in Europa an, so fällt auf, dass Behörden heute besser denn je in der Lage sind, rasch Täter zu identifizieren. Alternative Methoden wie Hausdurchsuchungen oder Personenobservationen führen zudem oftmals zu einem reichen Fundus an Daten. Allerdings ist die Datenbeschaffung teuer, zeitaufwendig und weniger bequem als scheinbar einfache technische Lösungen – ein Problem in Zeiten von Personaleinsparungen und knappen Haushalten für Polizeibehörden. In diversen Fällen agierten die Täter sogar komplett ohne Verschlüsselung und waren den Behörden im Vorfeld bekannt. Insofern ist es fraglich, welchen zusätzlichen Nutzen eine Schwächung von Verschlüsselung haben würde.

Diese fehlende Kosten-Nutzen-Abwägung unterscheidet heutige Krypto-Debatten von denen der 1990er Jahre. Seit den Anschlägen vom 11. September wird die Terrorabwehr als oberstes Ziel definiert, unter dem sich alle anderen sicherheitspolitischen Interessen unterzuordnen haben. Verschlüsselung lädt einer Gesellschaft aber nicht nur Kosten in Form von schwieriger zu fangenden Kriminellen auf, sondern hat auch Nutzen im Bereich der Cybersicherheit. Wenn also aus Gründen der Terrorbekämpfung Verschlüsselung oder Software geschwächt wird, erhöht man nicht die Sicherheit, sondern senkt sie. Das liegt daran, dass Verschlüsselung divergierende Konzepte von Sicherheit betrifft: moderne Cybersicherheit und innere Sicherheit.

33 Vgl. Heise online, Umfrage: 78 Prozent der Deutschen nutzen Smartphones, 22.2.2017, www.heise.de/newsticker/meldung/Umfrage-78-Prozent-der-Deutschen-nutzen-Smartphones-3632629.html.
34 Vgl. Simon Egbert, Siegeszug der Algorithmen? Predictive Policing im deutschsprachigen Raum, in: APuZ 32–33/2017, S. 17–23.
35 Vgl. The Administration's Clipper Chip Key Escrow Encryption Program: Hearing Before the Subcommittee on Technology and the Law of the Committee on the Judiciary, United States Senate, 3.5.1994.
36 Siehe Wiretap Report 2015, 31.12.2015, www.uscourts.gov/statistics-reports/wiretap-report-2015.

MATTHIAS SCHULZE
ist wissenschaftlicher Mitarbeiter bei der Stiftung Wissenschaft und Politik im Bereich Cyber-Sicherheitspolitik.
matthias.schulze@swp-berlin.org

PHÄNOMEN BITCOIN

Geld, Technologie und gesellschaftliches Ereignis

Friedemann Brenneis

Am 3. Januar 2009 drückte Satoshi Nakamoto eine Taste und startete damit ein Projekt, das die Welt verändern sollte: Bitcoin, das erste rein digitale Geld, das nicht durch Staaten und Banken verwaltet und organisiert wird, sondern durch Mathematik, Kryptografie und Algorithmen. Ziel des Projekts war ein freies, offenes und dezentrales Geldsystem als Alternative zu einem zentralisierten, undurchsichtigen und krisenanfälligen Finanzsystem, das sich zu diesem Zeitpunkt von seiner hässlichsten Seite zeigte und die Regierungen der Welt zwang, Banken mit dem Geld der Steuerzahler zu retten. Mitten in der Krise begann also ein einzelner Computer zu arbeiten – öffentlich, aber von der Öffentlichkeit unbeachtet. Kurze Zeit später gab es das erste Ergebnis: Als Gegenleistung für das Lösen einer komplexen Rechenaufgabe hatte das Programm seinem Schöpfer 50 Bitcoins gutgeschrieben und dieses Guthaben in einer eigens dafür geschaffenen Datenbank vermerkt: der Blockchain. Einige Zeit später folgte der nächste Eintrag, dann der dritte und immer so weiter.

Alle zehn Minuten wird ein neuer Datenblock erstellt und mit ihm neue Bitcoins erzeugt. So läuft es seit nunmehr bald neun Jahren ununterbrochen. Datenblock für Datenblock wächst die Blockchain und mit ihr die Anzahl verfügbarer Bitcoins. Mehr als 16 Millionen von ihnen kursieren bereits im Netz. Und sie sind längst nicht mehr nur irgendwelche Daten, sondern wertvolle Daten. Mittlerweile wird jeder einzelne Bitcoin für einen Preis von 6000 Euro und mehr gehandelt. Längst schon läuft die Bitcoin-Software nicht mehr nur auf einem einzigen Computer, sondern auf Tausenden, global verteilten und über das Internet miteinander verbundenen Rechnern. Millionen Menschen besitzen mittlerweile Bitcoins (oder zumindest Bruchteile davon) und nutzen diese, um physische Waren, Dienstleistungen und digitale Güter zu kaufen.[01] Oder sie spekulieren mit ihnen auf weiter steigende Kurse als moderne Form der Geldanlage.

Bitcoin hat sich binnen weniger Jahre von einem Nischenprojekt zu einem bemerkenswerten Phänomen entwickelt. Das Phänomen spielt längst nicht mehr nur in Nerd-, Hacker- und Darknetkreisen eine Rolle, sondern gewinnt zunehmend gesamtgesellschaftliche Relevanz, und es wirft viele Fragen auf. Denn eigentlich dürfte es Bitcoin nicht geben – zumindest nicht, wenn man auf die Expertise von erfahrenen Ökonomen, Bankenvertretern und der Medienöffentlichkeit vertraut. Diese haben das digitale Geld in den vergangenen Jahren immer wieder für gescheitert erklärt und erläutert, warum ein Zahlungsmittel, das nicht durch den Staat und Banken abgesichert wird, eigentlich nicht funktionieren kann.[02] Eigentlich, denn die Realität zeigt: Bitcoin ist nicht nur immer noch da, sondern wächst und entwickelt sich weiter. Mit einer Marktkapitalisierung von über 100 Milliarden US-Dollar ist das Open-Source-Projekt längst mehr als doppelt so viel wert wie das größte deutsche Geldinstitut, die Deutsche Bank. Scheitern, so sollte man meinen, sieht eigentlich anders aus.

Wie kommt es zu diesem Widerspruch? Auf der einen Seite die mitunter gut begründete Expertise, die argumentiert, dass eine staaten- und bankenlose Kryptowährung wie Bitcoin nicht funktionieren kann. Auf der anderen Seite die Realität, die zeigt, dass Bitcoin offensichtlich doch funktioniert. Um diese Diskrepanz aufzulösen, muss man sich den Fragen stellen, die das Projekt aufwirft. Allen voran der Frage: Was ist Bitcoin?

BITCOIN-GRUNDLAGEN

Schon auf die naheliegendste Frage eine befriedigende Antwort zu finden, ist überraschenderweise schwierig. Denn Bitcoin ist ein vielschichtiges und facettenreiches Phänomen, und die Antwort auf die Frage „Was ist Bitcoin?“ variiert je nach Standpunkt und Perspektive des Fragenden: Für

die einen ist Bitcoin eine zeitgemäße Form des Bezahlens. Ein rein digitales Geldmedium, das die monetären Bedürfnisse der Bürger in einer hochgradig vernetzten Gesellschaft besser erfüllt als alle bisherigen Optionen. Andere sehen in der Technologie hinter Bitcoin, der Blockchain, die nächste große technische Evolutionsstufe des Internets und aus ihr resultierend eine Vielzahl wirtschaftlicher und gesellschaftlicher Chancen. Wieder andere erhoffen sich mit Bitcoin einen Beitrag zur Demokratisierung und sehen ihn als Werkzeug, um den modernen Menschen aus der Abhängigkeit von Staaten, Banken und Konzernen zu führen und ihm mehr Freiheit, Autonomie und Hoheit über sein eigenes Leben zu ermöglichen. Es ist diese Vermengung von gesellschaftspolitischen Idealen, neuer Technologie und dem Machtkatalysator Geld, die das Phänomen Bitcoin vorantreibt, und wer es verstehen will, muss sich mit diesen drei Dimensionen beschäftigen: Bitcoin dem Geld, Bitcoin der Technologie und Bitcoin dem gesellschaftlichen Ereignis. Und man muss sich fragen, wo es eigentlich herkommt.

Die Idee eines digitalen Internetgeldes ist keineswegs neu, sondern so alt wie das Internet selbst. Immer wieder haben in den vergangenen Jahrzehnten Wissenschaftler, Internetpioniere und Idealisten versucht, eine nutzbare Form von E-Cash zu entwickeln. Verschiedene Verfahren sind dabei erprobt worden, die jedoch aus unterschiedlichen Gründen alle scheiterten: mangelnde Akzeptanz, Probleme mit der Software, fehlende technische Infrastruktur oder juristischer Druck durch politische Interessen- und Lobbygruppen, die eine privat initiierte Geld-Alternative gar nicht erst aufkommen lassen wollten. Die lange Geschichte des E-Cash zeigt damit vor allem eines: Es ist alles andere als einfach, mal eben alternatives Geld zu erfinden, das auch tatsächlich als solches genutzt wird.

Allein die dauerhafte Existenz von Bitcoin macht das Phänomen zu etwas Bemerkenswertem. Denn je größer und prominenter solch ein Projekt wird, desto stärker wird auch der Gegenwind – insbesondere wenn dieses den Machtanspruch von Regierungen und die ertragreichen Geschäftsmodelle der Finanzwirtschaft bedroht. Der Idee eines freien und unabhängigen Internetgeldes haben diese widrigen Umstände dennoch keinen Abbruch getan. Im Gegenteil: Sie wurde als logische und notwendige, wenngleich politisch noch nicht durchsetzbare Vision unbeirrt weiterverfolgt. In einem Interview erklärte beispielsweise der Wirtschaftsnobelpreisträger Milton Friedman 1999 seine Vorstellung eines für ihn unausweichlich kommenden internetbasierten Bargeldes.[03] Seine damalige Beschreibung trifft nahezu perfekt auf Bitcoin zu: ein elektronisches Geld, das so einfach und anonym wie Bargeld über das Netz ausgetauscht werden könne und das die Rolle des Staates reduzieren werde – mit all den sich daraus ergebenen positiven und negativen Konsequenzen. Friedman selbst hat die Umsetzung dessen nicht mehr erlebt. Es sollte noch zehn Jahre dauern, bis Satoshi Nakamoto Bitcoin präsentierte und schaffte, woran viele vor ihm geglaubt und gearbeitet hatten, in der Umsetzung aber letztlich alle gescheitert waren: das erste digitale, staaten- und bankenlose Geldsystem. Wie ist Satoshi Nakamoto gelungen, woran vor ihm alle scheiterten? Wie hat er es geschafft, dass Bitcoin überhaupt entstehen, wachsen und sich binnen acht Jahren als digitale Leitwährung mit Milliardenwert etablieren konnte?

MYSTERIUM SATOSHI NAKAMOTO

Satoshi Nakamoto ist zunächst nur ein Name und keine Person. Es handelt sich vielmehr um eine Persona, eine digitale Identität, von der bis heute nicht bekannt ist, wer und wie viele Menschen sich dahinter verbergen beziehungsweise verborgen haben. Zum ersten Mal in Erscheinung trat Satoshi Nakamoto im November 2008. Über eine Mailingliste, die sich auf die Diskussion von Verschlüsselung und deren politischen Implikationen spezialisierte, veröffentlichte er das Bitcoin-Whitepaper, in dem er sein Konzept eines „Peer-to-Peer Electronic Cash Systems“ erstmals darstellte.[04] Menschen, so seine Idee, sollten sich mit ihren Computern zu einem Netzwerk zu-

01 Vgl. Garrick Hileman/Michel Rauchs, Global Cryptocurrency Benchmarking Study, Cambridge Centre for Alternative Finance, 6. 4. 2017, www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf.

02 Siehe 99 Bitcoins, Bitcoin Obituaries, https://99bitcoins.com/bitcoinobituaries.

03 Milton Friedman Predicts the Rise of Bitcoin in 1999!, www.youtube.com/watch?v=6MnQJFEVY7s.

04 Satoshi Nakamoto, Bitcoin P2P E-Cash Paper, 1. 11. 2008, http://satoshi.nakamotoinstitute.org/emails/cryptography/1/#selection-101.0-101.29.

sammenschließen und allein mithilfe dieses Netzwerks Geldwerte rein digital untereinander austauschen können. Kryptografie, Algorithmen und das Interesse aller Teilnehmer daran, dass das System stabil und verlässlich läuft, sorgen für die Sicherheit. Jeder, der wolle, solle Bitcoin nutzen, aber niemand das System nach seinen Interessen manipulieren oder zensieren können. Die im Code verankerte, unveränderliche Anzahl aller jemals verfügbaren Bitcoins würden sie zu einem knappen Gut machen. Mit beständig steigendem Interesse daran stiege auch die Nachfrage und damit der Wert. Langfristig entstünde so ein stabiles, sich selbst verwaltendes und erhaltendes System, von dem alle profitieren, die es nutzen.

Einige Zeit nach der Veröffentlichung des Whitepaper meldete sich Satoshi Nakamoto in einem Online-Forum an, um Mitstreiter für das Bitcoin-Projekt zu finden und das Potenzial des Konzepts zu diskutieren. Seine Hinterlassenschaft – E-Mails, das Whitepaper, Foreneinträge und der originale Quellcode der Bitcoin-Software – ist in ihrem Umfang überschaubar, ganz im Gegensatz zu seinem ideellen Vermächtnis, das sich beständig verbreitete. Denn spätestens mit dem Start der Blockchain am 3. Januar 2009 und dem daraus resultierenden Beweis, dass Bitcoin technisch funktionieren kann, wuchs auch das Interesse an Bitcoin und der Frage, ob dieses neue Medium tatsächlich auch als digitales Geld verwendet werden könne. Anhand dieser Frage bildete sich schon bald eine Community. Weitere Entwickler kamen hinzu und nach Tausenden rein virtuellen Transaktionen wurde schließlich im Mai 2010 zum ersten Mal reale Ware mit Bitcoins bezahlt: Zwei Pizzen wechselten für 10 000 Bitcoins den Besitzer. Für das digitale Geld war dieser privat initiierte Handel ein Meilenstein. Denn zum ersten Mal konnte man Bitcoins einen tatsächlichen monetären Wert zuordnen. Die Pizzen hatten rund 20 US-Dollar gekostet. Ein einzelner Bitcoin hatte somit einen Wert von 0,2 Cent.

Da die Bitcoin-Idee inzwischen eine hinreichende Menge Anhänger überzeugt und ökonomisch Fuß gefasst hatte, begann Satoshi Nakamoto sich immer mehr zurückzunehmen. Als er sich im April 2011 endgültig aus der Öffentlichkeit zurückzog, wurde ein Bitcoin bereits für mehr als einen Dollar gehandelt. Über tausend Transaktionen wickelte das Bitcoin-Netzwerk täglich online ab, und kurze Zeit später sollte in Berlin mit einer Kneipe sogar das weltweit erste Ladengeschäft das neue digitale Geld als Bezahlung für Bier und Burger akzeptieren. Auch im Darknet erlebte Bitcoin damals einen Boom. Die Möglichkeit anonymer Transaktionen stieß insbesondere auf verborgenen Handelsplätzen wie „Silk Road“ auf großes Interesse und sorgte für eine stetig wachsende Nachfrage. Satoshi Nakamoto war zu diesem Zeitpunkt bereits Millionär. Doch deutet nichts darauf hin, dass persönliche Bereicherung Teil seiner Motivation war, das digitale Geld überhaupt ins Leben zu rufen. Bis heute hat er nachweislich keinen einzigen der rund eine Million Bitcoins, die sich seinem Besitz zurechnen lassen, ausgegeben – obwohl sie mittlerweile einen Gesamtwert von über sechs Milliarden Euro haben. Für Satoshi Nakamoto scheint diese Summe keine Bedeutung zu haben. Doch wenn es nicht der Wunsch nach persönlichem Wohlstand und Reichtum war, was hat ihn dazu bewogen, Bitcoin zu erschaffen?

Mit letzter Gewissheit wird man es wohl nie erfahren. Denn trotz großer Anstrengungen ist es bisher weder gelungen, die wahre Identität von Satoshi Nakamoto aufzudecken, noch ist davon auszugehen, dass er sich selbst offenbaren wird. Zu gravierend wären die Folgen: Nicht ohne Grund wurde die digitale Wegwerf-Identität erschaffen und sämtliche Spuren zu realen Personen verschleiert. Diesen mühsam aufgebauten Schutz wieder aufzugeben, hätte für die Person(en) hinter dem Pseudonym Satoshi Nakamoto unkalkulierbare und unumkehrbare Folgen. Denn dass der oder die Erfinder solch eines ökonomisch kontroversen und politisch brisanten Milliardenexperiments früher oder später zu Personen des öffentlichen Interesses werden und zunehmend in den Fokus von Regierungen, Unternehmen und anderen Interessenvertretern rücken, ist unausweichlich. Auch das haben gescheiterte Versuche der E-Cash-Historie gezeigt.

Mindestens ebenso wichtig ist: Die De-Anonymisierung von Satoshi Nakamoto würde das komplette Bitcoin-Projekt gefährden und dessen grundsätzliches Ideal verraten. Bitcoin wurde nämlich nicht nur als Geldsystem konzipiert, das ohne Staaten und Banken auskommt, sondern grundsätzlich ohne jegliche zentrale Institution, die es kontrollieren oder mit deren Hilfe sich das Projekt in irgendeiner Weise manipulieren ließe. Anstelle von Wenigen, die Macht über das System haben, verlagerte Satoshi Nakamoto die gesamte Entscheidungshoheit in ein computergestütztes Netzwerk und in die Hände einer weltweit operierenden Community, die dieses

Netzwerk pflegt und nutzt. Doch lässt sich dieses Konzept der radikalen Enthierarchisierung nur konsequent umsetzen, wenn es gelingt, wirklich alle potenziellen Autoritäts- und Machtinstanzen zu eliminieren. Wenn Bitcoin Erfolg haben soll, darf es auch keine Person mit dem einflussreichen Status des Gründers geben, deren Meinung im Ernstfall ein höheres Gewicht hätte als die aller anderen Mitglieder der Community.

Die Persona Satoshi Nakamoto wieder verschwinden zu lassen, war deshalb unumgänglich. So notwendig dieser Schritt auf konzeptioneller Ebene ist, diesen letztendlich auch umzusetzen, ist außerordentlich. Immerhin verzichtete Satoshi Nakamoto im Gegenzug für die Wahrung seiner Anonymität und die Integrität des von ihm geschaffenen Bitcoin-Projekts auf Prominenz, Anerkennung für eine bemerkenswerte intellektuelle Leistung und die Würdigung für ein technisch brillantes Konzept, von dem bereits erwähnten Milliardenvermögen einmal ganz abgesehen.

Tatsächlich gibt es Hinweise auf eine politisch-altruistisch geprägte Motivation: Bitcoin als demokratische Alternative zu einem intransparenten und zu Reformen unfähigen Finanzsystem. Dieses politische Ziel lässt sich nicht nur am Konzept Bitcoin selbst ablesen, dessen Prinzip es ist, frei und offen für jeden zu sein, der es nutzen möchte. Es offenbart sich auch in den wenigen Spuren, die Satoshi Nakamoto bewusst im Netz hinterließ. So versteckte er beispielsweise im Code des allerersten Blocks der Blockchain, dem sogenannten Genesis Block, die Schlagzeile der Londoner Times vom 3. Januar 2009: „Schatzkanzler kurz vor zweitem Banken-Rettungspaket". Darüber hinaus wählte er als Geburtsdatum seines Profils im Online-Forum mit dem 5. April ein fiktives, aber geldpolitisch durchaus symbolträchtiges Datum: An diesem Tag im Jahr 1933 verbot der damalige US-Präsident Franklin D. Roosevelt den Bürgern der USA den Besitz von Gold, konfiszierte dieses und zwang sie damit, den von der Notenbank ausgegebenen Dollar zu akzeptieren und damit das Währungssystem. Und zu diesem sollte Bitcoin ein alternatives System bieten:[05] ein Geldsystem, in dem die Menschen unabhängig sind von interessengeleiteten geldpolitischen Entscheidungen Weniger und das nicht durch Staats- und Bankenkrisen erschüttert werden kann. Denn zu diesen kam und kommt es immer wieder: Allein zwischen 1970 und 2007 zählte der Internationale Währungsfonds 124 Bankenkrisen, 326 Währungskrisen und 64 Staatsverschuldungskrisen auf nationaler Ebene.[06] Wer also argumentiert, dass ein staaten- und bankenloses Geld wie Bitcoin nicht funktionieren kann, muss auch anerkennen, dass Staaten und Banken nicht automatisch ein Garant für Stabilität sind.

BANKEN ALS NOTWENDIGES ÜBEL

Doch der Wunsch nach Veränderung und das Ideal eines alternativen demokratischeren Geldsystems reichen nicht aus, um dieses auch zu erschaffen. Nicht ohne Grund sind Banken und andere Finanzdienstleister fundamentaler Bestandteil des bestehenden Finanzsystems. Sie erfüllen wichtige und notwendige Funktionen, indem sie als zentrale Institutionen mit besonderem Status etwa die Gültigkeit von Finanztransaktionen sicherstellen. Ohne Intermediäre wie sie, die überprüfen, ob Person A oder Unternehmen X tatsächlich über das entsprechende Guthaben verfügt, um Rechnungen bei Person B oder Unternehmen Y zu begleichen, und den Geldtransfer letztlich ordnungsgemäß abwickeln, würden unsere Ökonomien noch immer auf Tauschhandel basieren. Denn wenn es ums Geld geht, muss letztendlich immer eine Instanz beteiligt sein, der man vertrauen kann – eine Instanz, die bestätigt, dass das Geld, das man für Leistungen und Produkte erhält, auch als solches in Zukunft wieder für andere Leistungen und Produkte ausgegeben werden kann.

Auf den ersten Blick scheint die Behauptung also plausibel, ein Geldsystem könne ohne Banken nicht funktionieren. Doch dies ist eben nicht die ganze Wahrheit. Zwar braucht ein funktionierendes Geldsystem eine vertrauenswürdige Instanz, die die Validität der Geldeinheiten überprüft, ordnungsgemäße Transaktionen abwickelt und das Guthaben der Nutzer vor Manipulation schützt. Diese Instanz muss im Zeitalter des Internets und der fortschreitenden Digitalisierung der Gesellschaft aber nicht zwingend eine Bank sein, sondern könnte – und genau das zeigt Bitcoin – auch mithilfe eines dezentralen Netzwerks

05 Vgl. Elfriede Sixt, Bitcoins und andere dezentrale Transaktionssysteme. Blockchains als Basis einer Kryptoökonomie, Wiesbaden 2017.

06 Vgl. Größere Finanzkrisen seit 1970, 25.9.2010, www.bpb.de/52625.

etabliert werden. Denn während das bestehende Finanzsystem das Internet nutzt, um über Zahlungen zu kommunizieren, die hinter verschlossenen Türen auf IT-Systemen aus dem vergangenen Jahrhundert verarbeitet werden, macht Bitcoin das Internet selbst zur universellen Finanzinfrastruktur. Zahlungen, Konten, Buchungen – das alles findet mithilfe des Bitcoin-Protokolls rund um die Uhr in Echtzeit im Netz statt, und bislang ist es offen, ausfall- und manipulationssicher sowie überall auf der Welt verfügbar.

Solch eine internetbasierte Finanzinfrastruktur technisch zu etablieren, ist alles andere als trivial, sondern vielmehr hochgradig experimentell. Man kann zwar nicht beweisen, dass Bitcoin funktioniert. Aber wir sehen, dass es bislang nicht gescheitert ist. Wie relevant das „bislang" ist, darüber wird gestritten. Fest steht jedoch: Je länger Bitcoin besteht und je stärker das Phänomen wächst, desto sicherer und vertrauenswürdiger wird es und desto mehr zeigt sich, dass Kryptowährungen und das ihnen zugrundeliegende Blockchain-Konzept die wachsenden Erwartungen erfüllen könnten, die derzeit an sie gestellt werden. Binnen 20 Jahren, so erklärte immerhin erst kürzlich die Direktorin des Internationalen Währungsfonds, Christine Lagarde, könnten Kryptowährungen nationale Währungen ablösen.[07] Um zu verstehen, warum das Interesse an dem Phänomen Bitcoin mittlerweile selbst auf institutioneller Ebene wächst, muss man sich mit der Funktionsweise des Netzes beschäftigen, wie wir es bisher kennen und nutzen.

FUNKTIONSWEISE DER BLOCKCHAIN

Die große Stärke des World Wide Web ist es, Daten und Informationen schnell, billig und beliebig oft zu vervielfältigen. E-Mails verschicken, Dokumente in der Cloud synchronisieren, bloggen, posten, tweeten, sharen, liken – das Internet ist eine riesige Kopiermaschine für Daten und Informationen jeglicher Art. Das ist praktisch, führt allerdings auch zu Problemen. Denn nicht alle Daten im Netz sollten beliebig kopierbar sein. Doch stellen wir Daten ins Netz, verlieren wir unweigerlich die Kontrolle über sie. In einem solchen Copy-and-Paste-Netz eine Geldinfrastruktur aufzubauen, ist eigentlich unmöglich. Wie sollte das Geld seinen Wert behalten, wenn es sich unkontrollierbar beliebig oft vervielfältigen lässt?

An dieser Stelle kommt die Blockchain ins Spiel, eine Datenbank, die es erstmals technisch ermöglicht, einmalige Daten im Internet zu erzeugen und sicher zu verwalten. Ihre Daten können nicht beliebig oft kopiert werden, sondern wechseln den Besitzer, wenn sie verschickt werden. Werden sie geteilt, vervielfältigen sie sich nicht, sondern werden aufgeteilt und verkleinert. Ihre Anzahl ist begrenzt, weshalb sie die Möglichkeit haben, wertvoll zu werden. Diese Daten sind die Bitcoins, und aufgrund ihrer speziellen Eigenschaften lassen sie sich wie Geld verwenden: Sie sind einmalig, fälschungssicher und lassen sich schnell, einfach und kostengünstig im Netz verschicken. Bitcoin ist damit für Bargeld das, was die E-Mail für den Brief ist: ein digitales Pendant, das die Möglichkeiten des Internets nutzt, um die sich verändernden Bedürfnisse einer zunehmend vernetzten Gesellschaft zu erfüllen. Eines dieser Bedürfnisse ist zum Beispiel, Geld so schnell, günstig und einfach zu versenden wie eine E-Mail und nicht aufwendig und abhängig von den AGB und den Arbeitszeiten von Banken. Genau das ermöglicht die Blockchain.

Als zentrale Datenbank ist die Blockchain das Herzstück des Bitcoin-Netzwerks und hält dieses am Laufen, indem sie Transaktionen abwickelt, die Gültigkeit von Zahlungsvorgängen kontrolliert und Buch darüber führt, auf welchem ihrer Konten sich gerade wie viele Bitcoins befinden. Die Blockchain vergisst dabei nichts. Alle jemals getätigten Bitcoin-Transaktionen befinden sich gebündelt in ihren namengebenden Datenblöcken. Diese werden mithilfe kryptografischer Funktionen untrennbar miteinander verknüpft und schützen so vor nachträglicher Manipulation. Denn da alle Blöcke sowohl chronologisch als auch kryptografisch aufeinander aufbauen, würde jede noch so kleine Veränderung der Kette sofort auffallen und zurückgewiesen werden. Die Blockchain übernimmt damit quasi die Rolle einer Zentralbank. Allerdings mit einem entscheidenden Unterschied: Die Blockchain wird nicht zentral, sondern dezentral organisiert. Sie ist nicht einfach nur eine Datenbank, sondern Tausende Datenbanken auf Tausenden Rechnern gleichzeitig. Und was in ihr steht, ist das Ergebnis eines global verteilten Netzwerks aus unabhängigen, aber gleichberechtigten Com-

07 Vgl. Jeffrey A. Tucker, IMF Head Foresees the End of Banking and the Triumph of Cryptocurrency, 30. 9. 2017, https://fee.org/articles/imf-head-predicts-the-end-of-banking-and-the-triumph-of-cryptocurrency.

putern, den sogenannten Minern, von denen jeder seine eigene Version der Blockchain besitzt und die sich dennoch alle zehn Minuten verlässlich darauf einigen, wem gerade welcher Bitcoin gehört.

Dass das funktioniert, ist paradox. Denn eigentlich dürfte es das nicht. In der Informatik gibt es sogar einen Beweis, dem zufolge in einem dezentralen Netzwerk niemals ein Konsens gefunden wird, weil man nie weiß, wer gerade nach den Regeln spielt und wer nicht. Daher dürften sich eigentlich auch die Teilnehmer der Blockchain nicht über ihre Zusammensetzung und den Bitcoin-Bestand einigen können. Dass sie es dennoch tun, ist vermutlich Satoshi Nakamotos größte intellektuelle Leistung. Zwar hat auch er das Koordinationsproblem nicht lösen können, aber er hat es mit einem geschickten Kniff überwunden. In seine technische Lösung implementierte er ein ökonomisches Anreizsystem: Die Blockchain funktioniert, weil sie diejenigen finanziell belohnt, die sie unterstützen. Wer dem Bitcoin-Netzwerk Rechenleistung zur Verfügung stellt und damit hilft, es gegen Manipulationen abzusichern, wird dafür in Bitcoins bezahlt. Diese interne Ökonomie führt dazu, dass es für die Teilnehmer des Netzwerks lukrativer ist, sich dem Blockchain-System anzuschließen, anstatt es anzugreifen. Und je größer das Netzwerk wird, desto sicherer sind die Bitcoins aller Beteiligten.

Dass diese technisch-ökonomische Anreizstruktur auf Dauer funktioniert, lässt sich zwar wissenschaftlich nicht beweisen, der seit Jahren laufende Praxistest spricht jedoch für sich. Obwohl der Bitcoin-Quellcode offen im Netz steht, ist es bisher noch niemandem gelungen, die Blockchain und die Milliardenwerte, die sie verwaltet, zu knacken. Denn ohne zentrale Institution, auf die sich ein Angriff konzentrieren könnte, muss man es in einem dezentralisierten System immer gleich mit dem gesamten Netzwerk aufnehmen. Das macht eine erfolgreiche Attacke zwar nicht unmöglich, aber komplex, teuer und aufwendig. Schon längst steht hinter Bitcoin das mit großem Abstand rechenstärkste Computer-Netzwerk der Welt, dessen Strombedarf bereits enorm ist und in absehbarer Zeit sogar auf das Niveau einer kleineren Industrienation steigen könnte.[08]

08 Vgl. Sebastiaan Deetman, Bitcoin Could Consume as Much Electricity as Denmark by 2020, 29.5.2016, https://motherboard.vice.com/en_us/article/aek3za/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020.

KRITIK UND AUSBLICK

Diese energiehungrige Rechenpower sichert die Milliardenwerte, die Bitcoin heute schon verwaltet, sorgt aber auch für berechtigte Kritik. Denn trotz seines enormen Ressourcenbedarfs ist Bitcoin noch weit davon entfernt, eine echte Alternative zum Euro und US-Dollar zu sein. Viel zu gering sind die Kapazitäten, die Bitcoin bislang bietet. Mit 350 000 Transaktionen kann die dezentrale Blockchain aktuell so viele Transaktionen an einem Tag verwalten wie die zentralisierten Transaktionssysteme von Banken und Zahlungsdienstleistern in Sekunden.

Doch solche quantitativen Vergleiche sind nur Momentaufnahmen. Dass Bitcoin im Vergleich zur globalen Finanzindustrie noch ein Experiment und Nischenphänomen ist, sollte nicht über das mögliche Potenzial hinwegtäuschen. Schließlich hat sich Bitcoin bereits binnen weniger Jahre von einem theoretischen Konzept zu einem globalen Milliarden-Projekt entwickelt. Das Image als Darknet-Währung hat Bitcoin dabei längst hinter sich gelassen. Denn auch die Ermittlungsbehörden wissen mittlerweile, wie sie die offenen Daten der Blockchain systematisch analysieren können. Im Darknet sind daher schon seit einiger Zeit andere, noch stärker auf Anonymität bedachte Kryptowährungen im Einsatz. Das Phänomen Bitcoin hingegen weckt längst auch außerhalb des Darknets das Interesse von immer mehr Menschen, die sich ähnliche Fragen wie Satoshi Nakamoto stellen: Ist unser bestehendes Finanzsystem tatsächlich alternativlos? Kann ein staaten- und bankenloses Geld wie Bitcoin funktionieren und wenn ja, ist es eine Bedrohung oder eine Bereicherung für die Gesellschaft? Dank Satoshi Nakamoto liegt es nun in der Hand jedes einzelnen Menschen, Antworten auf diese Fragen zu finden. Denn Bitcoin ist zwar digitales Geld und eine neue Technologie, vor allem ist es aber eine Idee, wie sich die Welt fairer, transparenter und krisensicherer gestalten lässt. Ohne Menschen, die diese Idee teilen, weiterentwickeln und umsetzen, ist Bitcoin jedoch nichts.

FRIEDEMANN BRENNEIS
ist freier Journalist. Er betreibt einen Rechercheblog zum Thema Bitcoin, Blockchain und Kryptowährungen unter www.coinspondent.de.
redaktion@coinspondent.de

EINE KURZE GESCHICHTE DER KRYPTOGRAFIE

Albrecht Beutelspacher

Das primäre Ziel der Kryptografie ist, die Kommunikation zwischen zwei oder mehreren Personen vor anderen Personen zu schützen. Hierfür stellt sie Mittel bereit, um die Geheimhaltung der Kommunikation auf die Geheimhaltung weniger Daten, auch Schlüssel genannt, zu reduzieren. Viele frühe Verfahren sind im militärischen und politischen Bereich angesiedelt und spielten sich zwischen Staaten ab. In der Geschichte gab es aber auch immer wieder Versuche, sich mithilfe von Verschlüsselung vor dem staatlichen Zugriff selbst zu schützen. Die heutige Kryptografie bietet dazu ideale Möglichkeiten. Daher ist es nicht verwunderlich, dass bei vielen Kämpfen von Minderheiten um ihre Rechte anonymisierte und verschlüsselte Kommunikation – etwa im Darknet – ein wichtiges Instrument ist.[01] Genauso klar ist, dass unter dem Schutz des Darknets auch Geschäfte getätigt oder angebahnt werden, die das Licht der Öffentlichkeit scheuen.

GRUNDLEGENDE ERFINDUNG: DER SCHLÜSSEL

Die Erfindung des variablen Schlüssels markiert die Geburtsstunde der Kryptografie. Seit dieser Zeit unterscheiden wir zwischen „Algorithmus" und „Schlüssel". Damit wird zum ersten Mal auch die Rolle des Angreifers klar. Am einfachsten lässt sich dies an der sogenannten Cäsar-Scheibe verdeutlichen. Der ihr zugrundeliegende Mechanismus geht auf Gaius Julius Cäsar zurück und wurde im 15. Jahrhundert vom Mathematiker Leon Battista Alberti weiterentwickelt. Seit Erfindung der Scheibe ist sie aus kryptografischen Algorithmen nicht mehr wegzudenken.

Die Cäsar-Scheibe besteht aus einer kleinen und eine großen Kreisscheibe, die an ihren Mittelpunkten drehbar verbunden sind. Auf jeder Scheibe steht das Alphabet in zyklischer Anordnung. Das Alphabet auf der äußeren Scheibe nennt man das Klartextalphabet, das auf der inneren Scheibe wird Geheimtextalphabet genannt. Nun legen Sender und Empfänger zunächst eine bestimmte Einstellung ihrer Scheiben fest. Diese kann zum Beispiel dadurch bestimmt werden, indem man den Buchstaben auf der inneren Scheibe angibt, der bei dem Klartextbuchstaben A steht. Wenn sie sich zum Beispiel auf den Buchstaben R einigen, sind die Scheiben so gedreht, dass dort, wo außen A steht, innen R steht. Wir sprechen kurz von der „Einstellung R". Die Verschlüsselung erfolgt nun so, dass ein Klartextbuchstabe durch den Geheimtextbuchstaben ersetzt wird, der an ihn auf der inneren Scheibe direkt anschließt. Beim Verschlüsseln liest man also von außen nach innen; entsprechend erfolgt das Entschlüsseln durch Lesen von innen nach außen.

Grundsätzlich können wir zwei Dinge unterscheiden: erstens die Maschine, also das generelle Verschlüsselungsverfahren, das auch Verschlüsselungsalgorithmus genannt wird; zweitens der Schüssel, in unserem Fall also die spezielle Einstellung der Scheiben. Damit kann verschlüsselt, also Klartext in Geheimtext überführt werden.

Der originale Cäsar-Code ist viel spezieller. Cäsar ersetzte nämlich jeden Klartextbuchstaben durch den Buchstaben, der im Alphabet drei Stellen danach kommt. So wird etwa A zu D, B zu E und C zu F. Aus CAESAR wird folglich FDHVDU. Offensichtlich bietet dieses Verfahren praktisch keine Sicherheit.

Das gilt ebenso für alle Verfahren, die mit Geheimzeichen arbeiten. Sehr bekannt ist der sogenannte Freimaurercode: Bei diesem wird jeder Buchstabe durch die Linien ersetzt, die ihn umgeben (*Abbildung 1*). Zum Beispiel wird statt E ein Quadrat gemalt, statt J ein V-ähnliches Zeichen und statt P ein L-förmiges Zeichen mit einem Punkt.

Geheimzeichen bieten, nüchtern betrachtet, keinerlei Sicherheit, sie sind aber sehr populär – vielleicht weil man glaubt, dass echte Geheim-

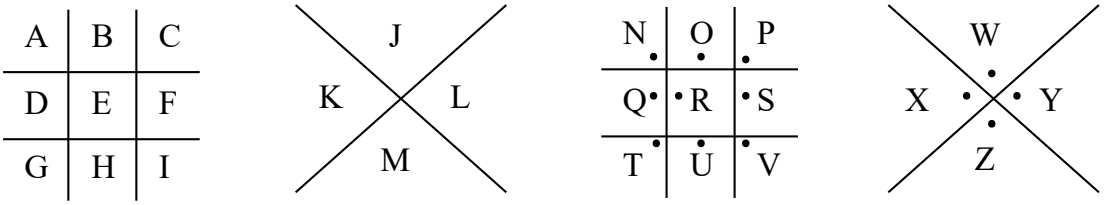

Abbildung 1: Freimaurercode
Quelle: Eigene Darstellung

zeichen „sich selbst schützen". Die Sicherheit all dieser Verfahren kann jederzeit zusammenfallen wie ein Kartenhaus. Wenn ein Unbefugter Kenntnis von dem Zuordnungsschema bekommt, dann hat das System auf einen Schlag all seine Sicherheit verloren.

Im Laufe der Geschichte hat sich gezeigt, dass es fast unmöglich ist, Algorithmen, also die prinzipiellen Verfahren, geheim zu halten. Immer wieder wurden Grundprinzipien der Verfahren veröffentlicht oder verraten, Verschlüsselungsmaschinen wurden gestohlen oder konnten legal gekauft werden. Die Befürchtung der Erfinder und Entwickler war lange Zeit, dass dadurch auch das Verfahren selbst unsicher war. Die Sorge war die folgende: Wer das Verfahren kennt, insbesondere wer es erfunden hat, der kann es auch brechen. Dass dies nicht sein darf, war intuitiv vielen bewusst, aber erst 1833 wurde es vom Kryptologen Auguste Kerckhoffs formuliert: Ein Bekanntwerden des Verfahrens darf die Sicherheit nicht gefährden. Die Sicherheit beruht allerdings entscheidend darauf, dass der Schüssel geheim gehalten wird.

Der Schlüssel ist das exklusive Geheimnis von Sender und Empfänger. Damit schützen sie sich gegen den Rest der Welt. Man kann auch sagen, der Schlüssel ist der strategische Vorteil, den der Empfänger gegenüber einem Angreifer hat. Der Angreifer besitzt eventuell große Mengen Geheimtext, er kennt das Verfahren, und er möchte den Klartext erhalten. Die Frage ist, ob ihm das ohne Kenntnis des Schlüssels gelingt. Man kann den Spieß auch umdrehen und die Sicherheit eines Verfahrens nach den Erfolgsaussichten eines Angreifers bemessen. Wenn es leicht ist, ohne Schlüssel den Klartext zu erhalten, dann ist das Verfahren unsicher. Es ist sicher, wenn sich ein Angreifer vor ein, für ihn, unlösbares Problem gestellt sieht.

Die oberste Anforderung an die Sicherheit eines Verschlüsselungsverfahrens ist, dass ein Angreifer keine Chance hat, alle Schlüssel durchzuprobieren. Bei der Cäsar-Scheibe mit ihren 26 möglichen Einstellungen ist das nicht gewährleistet. Bei heutigen Verfahren sollte der Schlüsselraum über mindestens 2^{128}, besser noch 2^{256} Elemente verfügen. Letztere Zahl ist größer als die Anzahl der Atome im Universum. Insofern ist klar, dass niemand, auch nicht alle Rechner des Internets, jemals so viele Ver- oder Entschlüsselungen umsetzen kann.

Ein weiterer Aspekt ist dabei von Bedeutung: Mit einem gemeinsamen Schlüssel kann man nicht nur für zwei, sondern für beliebig viele Personen Raum für geheime Kommunikation schaffen. Wenn alle Personen einer Gruppe den gleichen Schlüssel besitzen und die Verschlüsselung nicht gebrochen werden kann, dann wirkt dieser Schlüssel wie eine Mauer, die diese Gruppe vor der restlichen Welt schützt.

ERSTE SICHERE CODES: POLYALPHABETISCHE CODES

Etwa um 1500 war klar, dass monoalphabetische Codes – wie die Cäsar-Verschlüsselung – keine wirkliche Sicherheit bieten. Interessanterweise hatten mehrere Gelehrte im 16. Jahrhundert eine ähnliche Idee für eine neue Dimension von Sicherheit. Sie bestand darin, monoalphabetische Chiffrierungen, ja sogar die Cäsar-Scheibe, zu nutzen, allerdings diese in einer komplexen Weise einzusetzen. Das Ziel musste sein, nicht für alle Buchstaben das gleiche Geheimtextalphabet zu verwenden, sondern eine ganze Reihe, und zwar in einer bestimmten Reihenfolge.

01 Für übergreifende Darstellungen zur Geschichte der Kryptografie und weiterführende Literaturverweise siehe Albrecht Beutelspacher, Kryptologie, Heidelberg 2014[10]; ders., Geheimsprachen. Geschichte und Techniken, München 2012[5]; Simon Singh, Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet, München 2017[14].

Ein Beispiel: Der Schlüssel ist ein Wort. Sender und Empfänger einigen sich auf das Wort „Rot“. Der Sender nimmt seine Cäsar-Scheibe und stellt sie so ein, dass das Klartext-A genau bei dem Geheimtext-R, dem ersten Buchstaben des Schlüsselworts, steht. Mit dieser Einstellung R wird der erste Buchstabe des Klartexts verschlüsselt. Um den zweiten Buchstaben zu verschlüsseln, benutzt er die Einstellung, bei der das Klartext-A beim Geheimtext-O steht, und für den dritten Buchstaben verwendet er die Einstellung T. Wenn die Buchstaben des Schlüsselworts aufgebraucht sind, fängt er wieder von vorne an. Das heißt, für den vierten Buchstaben nutzt er wieder die Einstellung R.

Die Entschlüsselung ist entsprechend einfach: Der Empfänger muss die Einstellungen der Scheibe in gleicher Reihenfolge anwenden wie der Sender und jeweils den entsprechenden Buchstaben entschlüsseln. Man spricht von einem polyalphabetischen Verfahren, weil viele Alphabete zum Einsatz kommen. Diese polyalphabetischen Codes waren die erste große Herausforderung für Kryptoanalytiker. Einige Jahrhunderte lang boten sie echte Sicherheit. Es dauerte ziemlich lange, bis man im 19. Jahrhundert eine Möglichkeit, den sogenannten Kasiski-Test, entdeckte, die Länge des Schlüsselworts zu bestimmen und dann mithilfe einer Häufigkeitsanalyse die einzelnen Buchstaben des Schlüsselworts herauszufinden.

Polyalphabetische Verfahren waren stark, und sie hatten ein Potenzial, das in ihrer Gänze erst 1916 durch den Ingenieur Gilbert Vernam ausgeschöpft wurde. Er erfand einen unknackbaren binären Code, der auf den Zeichen 0 und 1 aufbaute. Tatsächlich kann man aber jedes polyalphabetische Verschlüsselungsverfahren zu einem Verfahren mit perfekter Sicherheit, also einem unknackbaren Verfahren, weiterentwickeln. Die Idee dazu ist recht simpel: Anstelle eines Schlüsselworts der zum Beispiel deutschen Sprache wählt man eine zufällige Folge von Buchstaben. Wenn diese mindestens so lang ist wie der Klartext, dann ist die Verschlüsselung unknackbar. Dies bewies 1949 der Mathematiker Claude Shannon. Der Nachteil, dass man solche perfekten Chiffrierungen nur dann erhält, wenn die zufällige Schlüsselfolge mindestens so lang ist wie der Klartext, macht das Verfahren für die meisten praktischen Anwendungen unbrauchbar. Man bezeichnet das Verschlüsselungsverfahren auch als *one-time-pad*, weil man die Folge nur einmal verwendet.

MASCHINEN MIT BESCHRÄNKTEN FÄHIGKEITEN

Um vernünftig verschlüsseln und entschlüsseln zu können, braucht man technische Unterstützung. Wir sind gerade noch in der Lage, einfache Geheimsprachen zu lernen. Schon bei der Ausführung des Cäsar-Codes haben wir enorme Schwierigkeiten – etwa die Kombination MTARVQ zu entschlüsseln, wenn man weiß, dass die Verschlüsselung darin besteht, jeden Buchstaben durch den übernächsten zu ersetzen. Daher lag die Suche nach mechanischen Hilfsmitteln zur Verschlüsselung nahe. Im Grunde kann man zwar schon die antike Skytale als erste Verschlüsselungsmaschine bezeichnen,[02] üblicherweise wird aber die Cäsar-Scheibe als Beginn der mechanischen Kryptografie angesehen.

Die Blütezeit der kryptografischen Maschinen war in der ersten Hälfte des 20. Jahrhunderts. Bei fast jedem mechanischen Schlüsselgerät fallen die Rotoren und Walzen auf, die in mehr oder weniger komplexer Weise zusammenspielen. Neben dem Vorbild der Cäsar-Scheibe standen hierfür auch die mechanischen Rechenmaschinen Pate, die seit der zweiten Hälfte des 19. Jahrhunderts weitverbreitet waren.

Die berühmteste Chiffriermaschine der Welt ist die Enigma, die 1918 vom Erfinder Arthur Scherbius zum Patent angemeldet wurde. Sie machte das Verschlüsseln kinderleicht. Auf den ersten Blick ähnelt sie einer Schreibmaschine. Drückt man auf eine Taste, erleuchtet ein anderer Buchstabe auf dem darüber liegenden Lampenfeld. Dies ist der zugehörige Geheimtextbuchstabe. Verschlüsseln mit der Enigma ist folglich nicht schwieriger als das Tippen auf einer Schreibmaschine.

Innerlich ist die Enigma allerdings sehr komplex. Das Herz des Kyptogeräts besteht aus drei Walzen und einer Umkehrwalze (*Abbildung 2*). Sie alle liegen nebeneinander: rechts die erste Walze, links davon die zweite, dann die dritte und schließlich ganz links die Umkehrwalze. Die Walzen und die Umkehrwalze sind jeweils in 26 Sektoren eingeteilt, die man mit den 26 Buchstaben des

02 Die Skytale war ein Holzstab, um den ein Band gewickelt wurde. Auf dieses wurde der Text in Längsrichtung geschrieben, bevor er verschickt wurde. Der Empfänger konnte die Nachricht entschlüsseln, wenn er das Band um einen Zylinder gleichen Durchmessers wickelte.

Abbildung 2: Enigma-M4
Quelle: picture-alliance/dpa

Alphabets identifizieren kann. Jede Walze hat in jedem Sektor eine Kontaktstelle, und zwar auf beiden Seiten. Auch die Umkehrwalze ist verdrahtet. Nach jedem Tastendruck dreht sich die erste Walze um eine Stelle weiter. Nach 26 Buchstaben nimmt sie die zweite Walze um eine Stelle mit. Nach 26 Mal 26 Tastendrücken wird auch die dritte Walze um eine Stelle weitergedreht, dies wird durch die Umkehrwalze ermöglicht. Das bedeutet, dass jeder Buchtstabe anders verschlüsselt wird, und die Anfangseinstellung der Walzen ist der Schlüssel des Verfahrens. In der militärischen Praxis mussten deshalb die Walzen jeden Tag neu eingestellt werden. Das Entschlüsseln erfolgt bei der Enigma fast genau so leicht wie das Verschlüsseln: Wenn man mit der gleichen Walzeneinstellung beginnt, muss man lediglich den Geheimtext abtippen, um den Klartext auf dem Lampenfeld zu lesen.

Die Enigma wurde im Zweiten Weltkrieg von der Wehrmacht flächendeckend eingesetzt. Es wurden sicher Zehntausende dieser Maschinen hegestellt. Allerdings konnten die Briten schon zu Beginn des Zweiten Weltkriegs die Enigma entschlüsseln. Dabei bauten sie auf entscheidende Vorarbeiten polnischer Mathematiker auf. Die Möglichkeit, die Enigma zu knacken, wurde erleichtert durch Bedienungsfehler. Zum Beispiel wurden als Schlüssel für die Einstellung der Walzen häufig nicht zufällige Kombinationen aus drei Buchstaben gewählt, sondern einfach zu merkende Kombinationen wie AAA, ABC oder XYZ. Die entscheidende, konstruktionsbedingte Schwäche der Enigma liegt aber vielmehr darin, dass nie ein Buchstabe zu sich selbst verschlüsselt wird. Was sich im ersten Moment positiv anhört, ist in Wirklichkeit die Achillesferse des Systems. Angenommen ein Angreifer ist im Besitz einer größeren Menge Geheimtext und einem kleineren Teil Klartext. Dann kann er leicht feststellen, von welchem Teil des Geheimtexts der Klartext nicht stammt: Wenn beim Übereinanderlegen auch nur ein Buchstabe übereinstimmt, dann stammt der Klartext nicht von dieser Stelle. Da man so sehr viele Möglichkeiten ausschließen kann, bleiben nur wenige übrig, mit denen man dann weiterarbeiten kann.

Sicherlich gab es Kryptogeräte neben der Enigma, die noch komplexer waren und eine höhere Sicherheit boten. Doch spätestens das Aufkommen des Computers in der zweiten Hälfte des 20. Jahrhunderts markierte den Niedergang aller mechanischen Verschlüsselung.

DES-ALGORITHMUS UND PUBLIC-KEY-KRYPTOGRAFIE

In der zweiten Hälfte der 1970er Jahre geschahen zwei Dinge, die die Kryptografie revolutionierten: erstens die Publikation des DES-Algorithmus (Data Encryption Standard) und zweitens die Erfindung der Public-Key-Kryptografie. Der DES-Algorithmus war der erste standardisierte Algorithmus. Mit ihm hatte jeder Anwender sichere Verschlüsselungsverfahren zur Hand, derer man sich einfach bedienen konnte. Das Hauptproblem der Kryptografie blieb aber bestehen: das Schlüsselverteilungsproblem.

Da sowohl Sender als auch Empfänger zur Kommunikation den gleichen geheimen Schüssel brauchen, muss dieser mindestens einmal übertragen werden – von Sender zum Empfänger beziehungsweise umgekehrt oder auch von einer Schlüsselverteilzentrale an Sender und Empfänger. Will ich zum Beispiel mit 100 Menschen per E-Mail kommunizieren, brauche ich 100 Schlüssel, die ich mit meinen Kommunikationspartnern teilen muss. Wenn in einem Netz von 1000 Personen jeder mit jedem geheim kommunizieren möchte, sind eine halbe Million Schlüssel erforderlich. Die Schlüssel müssen erzeugt, geheim gehalten und in regelmäßigen Abständen neu verteilt werden. Daher wurden in den 1960er und 1970er Jahren zahlreiche Schlüsselaustauschprotokolle entwickelt, die das Ziel hatten, die Anzahl der händisch zu verteilenden Schlüssel zu minimieren. Damit konnten sie das Problem zwar verkleinern, aber nicht lösen.

1976 hatten zwei junge amerikanische Wissenschaftler, Whitfield Diffie und Martin Hellman, schließlich einen kühnen Traum: Verschlüsselte Kommunikation sollte so einfach sein wie Telefonieren. Hat man den Namen der Person, die man anrufen möchte, muss man im Telefonbuch nur nach ihrer Nummer nachschlagen. Genau so müsste auch geheime Kommunikation funktionieren. Übertragen auf die geheime Kommunikation ist die Telefonnummer der öffentliche Schlüssel. Dieser wird verwendet, um die Nachricht zu verschlüsseln und abzuschicken. Der Empfänger kann sie entschlüsseln, indem er seinen eigenen geheimen Schlüssel verwendet. Entscheidend dafür ist, dass man aus dem öffentlichen Schlüssel nicht auf den geheimen schließen kann und dass die Kommunikationspartner keinen gemeinsamen geheimen Schlüssel benötigen, um geheim zu kommunizieren.

Auch wenn es zu dieser Zeit noch keine sogenannten Public-Key-Verschlüsselungsverfahren gab, das grundsätzliche Prinzip hinter öffentlichen und privaten Schlüsseln war bereits alltäglich – etwa beim Briefkasten an einem Hochhaus: Will zum Beispiel Bob eine geheime Nachricht an Alice schreiben – eine Nachricht, die nur Alice lesen kann –, dann schreibt er die Nachricht auf ein Blatt Papier, steckt es in einen Umschlag, sucht Alice' Briefkasten auf und wirft den Brief hinein.[03] Der Briefkasten stellt sozusagen den öffentlichen Schlüssel dar. Lediglich Alice kann mit ihrem Briefkastenschlüssel den Briefkasten aufschließen, den Brief herausholen und ihn lesen. Alice' Briefkastenschlüssel entspricht somit dem geheimen Schlüssel.

Selbst wenn die Wissenschaftler damals das Briefkasten-Beispiel im Sinn gehabt hätten – die technische Möglichkeit zur Umsetzung existierte noch nicht. Zumindest aber arbeiteten Diffie und Hellman die ersten Theorien aus. Zwei Jahre später entwickelten die Wissenschaftler Ron Rivest, Adi Shamir und Len Adleman das erste Public-Key-Kryptosystem: der sogenannte RSA-Algorithmus, der nach ihren Initialen benannt ist. Das Verfahren nutzt klassische Mathematik; genauer gesagt einen wohlbekannten Satz der Zahlentheorie, der auf den Mathematiker Leonhard Euler aus dem 18. Jahrhundert zurückgeht. Dieser Satz sagt ganz grob, dass man im ersten Schritt mit einer beliebigen Zahl m etwas Kompliziertes macht und am Ende wieder die Zahl m herauskommt. Der Grundgedanke des RSA-Verschlüsselungsverfahrens ist, diesen komplizierten Vorgang, der aus Potenzieren und Berechnen von Resten besteht, in zwei Vorgänge aufzuteilen: Der erste ist die Verschlüsselung, der zweite die Entschlüsselung. Damit sollte das Hauptproblem des Schlüsselaustauschs gelöst werden. Zwei oder mehr Personen nutzen für die Kommunikation ein schnelles traditionelles Verschlüsselungsverfahren wie den DES-Algorithmus. Dann kommt die Public-Key-Kryptografie ins Spiel: Alice erzeugt zunächst einen DES-Schlüssel, den sie für die Kommunikation mit Bob verwenden möchte. Dann verschlüsselt sie diesen mithilfe von Bobs öffentlichem RSA-Schlüssel. Bob entschlüsselt nun mit seinem privaten RSA-Schlüssel und erhält damit den eigentlichen DES-Schlüssel für die Kommunikation und kann damit Alices Nachricht entschlüsseln. Dieses Verfahren macht es nicht nur für Großanwender, sondern auch für Privatanwender einfach, Kryptografie einzusetzen. Public-Key-Kryptografie ist heute aus unserem Alltag kaum wegzudenken und ermöglicht uns E-Mail-Verkehr, Surfen im Internet oder Onlinebanking.

SCHLUSS

Die heutige Kryptografie ist wie eine Wundertüte: Sie enthält sinnvolle und wichtige Dinge wie sichere Verschlüsselungsverfahren und verlässliche Anwendungen. Jeder kann sich aus diesem Angebot etwas raussuchen, und einige können mit geringem Aufwand die Verfahren so sicher machen, dass sie von keiner Institution der Welt geknackt werden können. Natürlich enthält eine Wundertüte aber auch Überraschungen: Die Verfahren sind möglicherweise nicht so „unknackbar" wie gedacht, Fehler werden erst spät entdeckt oder Innovationen für kriminelle Machenschaften missbraucht.

Die heutige Kryptografie stellt jedoch erstmal prinzipiell jedem Sicherheit in beliebiger Qualität zur Verfügung. Viele für uns selbstverständliche Anwendungen wie sicheres Internet oder sichere mobile Kommunikation wären ohne moderne Kryptografie nicht möglich. Insbesondere hochwertige komplexe Anwendungen wie elektronisches Bezahlen und elektronisches Wählen basieren entscheidend auf Mechanismen der modernen Kryptografie. Es liegt jedoch ebenso auf der Hand, dass mit Verschlüsselungsverfahren Daten jeglicher Art verschlüsselt werden können. So setzt etwa auch der Tor-Browser, der Zugang zum Darknet ermöglicht, für die Anonymisierung seiner Nutzer unter anderem den RSA-Algorithmus ein. Ob die Verwendung kryptografischer Mechanismen zum Schutz der Privatsphäre, zur Sicherung von Unternehmensdaten oder zur Verschleierung illegaler Machenschaften geschieht, darauf hat die Kryptografie wenig Einfluss.

ALBRECHT BEUTELSPACHER
ist Professor für Geometrie und Diskrete Mathematik an der Universität Gießen, Direktor des Mathematikums in Gießen und Buchautor.
albrecht.beutelspacher@mathematikum.de

03 Alice und Bob sind Platzhalternamen in der Kryptografie. Sie werden häufig verwendet, um Kommunikationsteilnehmer zu benennen und Erklärungen zu vereinfachen.

DROGENHANDEL IM DARKNET

Gesellschaftliche Auswirkungen von Kryptomärkten

Meropi Tzanetakis

Die ersten Medienberichte über Drogenmärkte im Darknet gehen auf das Jahr 2011 zurück. Auf dem digitalen Schwarzmarkt „Silk Road" könne jede nur erdenkliche Droge gekauft werden – ähnlich einfach und vermeintlich sicher wie Elektronikprodukte auf Amazon, hieß es etwa in einem Beitrag des US-amerikanischen Blogs „Gawker".[01] Um anonyme Bestellungen von Drogen per Mausklick zu ermöglichen, werde allerdings spezielle Software benötigt, die IP-Adressen oder Domainnamen verberge und dadurch herkömmliche Ermittlungsansätze erschwere, erläutert die „Süddeutsche Zeitung".[02]

Während der Begriff „Darknet" zum damaligen Zeitpunkt nicht Teil der öffentlichen Debatte war, erlangte dieser im Sommer 2016 traurige Berühmtheit, weil der Amokläufer von München den Kauf der Tatwaffe über das Darknet anbahnte.[03] Bezahlt und übergeben wurde die Waffe jedoch nicht anonym über eine Onlinebestellung, sondern durch ein persönliches Treffen im Mai 2016. Im Zusammenhang mit dem Amoklauf von München, der zehn Menschenleben forderte, entbrannte eine Sicherheitsdebatte. Forderungen nach strengeren Waffengesetzen und einem Verbot von gewaltverherrlichenden Computerspielen wurden laut, aber auch nach einer besseren personellen und finanziellen Ausstattung der Sicherheitsbehörden sowie nach mehr Ermittlungsbefugnissen.[04] Gleichsam verfestigte sich in der Öffentlichkeit das Bild vom Darknet als die dunkle Seite des Internets – als Ort, der vorrangig dem Vertrieb von Drogen, Waffen und Kinderpornografie diene.

Im Folgenden wird zunächst erläutert, was unter Kryptomärkten für Drogen verstanden werden kann und wie verbreitet sie im Vergleich zu anderen Darknet-Inhalten sind. Anschließend werden die von ihnen ausgehenden Risiken und Gefahren analysiert sowie die Chancen und Potenziale erörtert, die mit der Verlagerung des Drogenkaufs ins Darknet einhergehen. „Chance" wird im Sinne des Schadensminimierungsansatzes verstanden, der darauf abzielt, gesundheitliche und soziale Folgeschäden des Drogenkonsums zu minimieren.

WAS SIND KRYPTOMÄRKTE?

Obwohl der Onlinehandel mit Drogen so alt ist wie das Internet selbst, hat eine Reihe von technologischen Entwicklungen zu einem systematischen Vertrieb von legalen wie illegalen Drogen und weiteren Produkten im Web beigetragen. Dazu zählen etwa verschreibungspflichtige Medikamente, Falschgeld, gestohlene Kreditkartendaten, gehackte Bankkontodaten, Schusswaffen, aber auch Anleitungen zur Herstellung psychoaktiver Substanzen. Durch die Kombination aus Anonymisierungssoftware, wie dem Tor-Browser, und virtuellen Währungen, wie Bitcoin, sind digitale Plattformen entstanden, die sich nicht grundlegend von anderen Online-Marktplätzen unterscheiden.

Der Begriff „Kryptomarkt" hat sich in der Forschungsgemeinschaft zur Bezeichnung dieser technologischen Neuerung durchgesetzt.[05] Zum Kryptomarkt gehören zwei wesentliche Merkmale: Drogenbestellungen werden *erstens* nicht mit Kreditkarten bezahlt, sondern mit Kryptowährungen wie Bitcoin, die Nutzern und Nutzerinnen dezentrale Transaktionen ermöglichen.[06] *Zweitens* erlaubt die Verschlüsselungssoftware Tor das Aufrufen der *hidden services* und damit den Zugang zum Darknet.[07] Die Tor-Technologie wurde Mitte der 1990er Jahre in einer der US-Marine zugehörigen Forschungsabteilung entwickelt und 2002 mit der Veröffentlichung der Alpha-Version der Tor-Software öffentlich zugänglich gemacht. Tor basiert auf einem weltweiten Netzwerk von etwa 7000 unentgeltlich betriebenen Servern, die Ver-

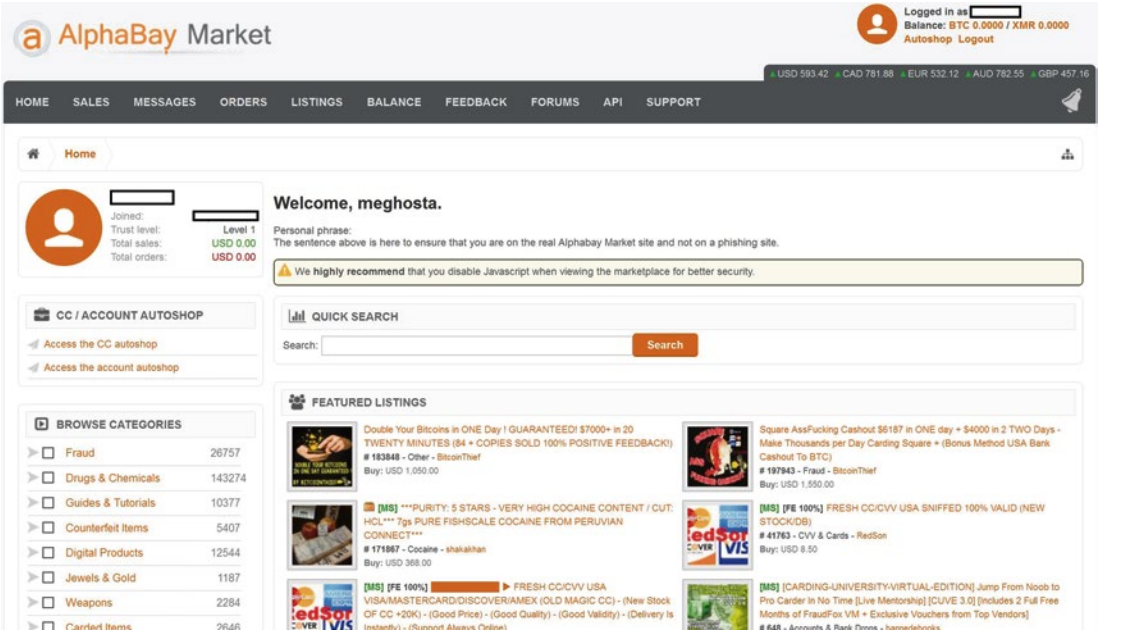

Abbildung: Kryptomarktplatz „AlphaBay"
Quelle: Screenshot aus eigenem Bestand

bindungen verschlüsseln. Die Verschlüsselung verhindert, dass der Datenverkehr der zwei Millionen Nutzer auf sie zurückgeführt werden kann. Das Darknet kann als ein Bereich des Internets verstanden werden, der mittels technologischer Lösungen die Identität und den Standort der Benutzer und Benutzerinnen verschleiert. Zwar ist das Tor-Netzwerk nicht das einzige Darknet, es ist aber das weitverbreitetste und bietet die größte Auswahl an Kryptomärkten.

Es gibt zwei empirische Studien, die Aufschluss über den Umfang und die Zusammensetzung des Netzwerks geben: Die von der britischen Sicherheitsfirma Intelliagg an rund 13 000 Websites im Tor-Netzwerk vorgenommene Untersuchung zeigt, dass etwa die Hälfte von ihnen nach britischem oder US-Recht einen legalen Inhalt haben.[08] Die Wissenschaftler kategorisierten die Websites zudem: 29 Prozent fielen unter die Kategorie „Filesharing-Dienste", 28 Prozent unter „geleakte Daten" – worunter man nicht autorisierte Veröffentlichungen von Informationen versteht – und 12 Prozent unter „Finanzbetrug". Auf 4 Prozent der untersuchten Websites wird mit Drogen gehandelt und 0,3 Prozent haben Bezug zu Waffen. Die Ergebnisse decken sich größtenteils mit einer Studie des Londoner King's College: Von den 2723 untersuchten Websites im Tor-Netzwerk, sind 57 Prozent strafrechtlich relevant: 15 Prozent stehen im Zusammenhang mit Drogen, 12 Prozent mit Finanzgeschäften, 7 Prozent mit anderen illegalen Inhalten und 1,5 Prozent mit Waffen.[09]

01 Vgl. Adrian Chen, The Underground Website Where You Can Buy Any Drug Imaginable, 1.6.2011, http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160.
02 Vgl. Moritz Koch, Internet-Portal Silk Road – Drogen per Mausklick, 6.7.2011, www.sueddeutsche.de/digital/-1.1116625.
03 Vgl. Tom Sundermann, Amoklauf von München: Der rechte Waffendealer, 27.8.2017, www.zeit.de/gesellschaft/zeitgeschehen/2017-08/amoklauf-muenchen-prozess-pistole-haendler.
04 Vgl. Stephan Haselberger et al., Nach dem Amoklauf in München: Politische Forderungen und soziale Hintergründe, 24.7.2016, www.tagesspiegel.de/13920780.html.
05 Vgl. James Martin, Drugs on the Dark Net. How Cryptomarkets Are Transforming the Global Trade in Illicit Drugs, New York 2014, S. 3.
06 Siehe hierzu auch den Beitrag von Friedemann Brenneis in dieser Ausgabe (*Anm. d. Red.*).
07 Siehe hierzu auch den Beitrag von Stefan Mey in dieser Ausgabe (*Anm. d. Red.*).
08 Vgl. Intelliagg, Deeplight: Shining a Light on the Dark Web, Report 2016, http://deeplight.intelliagg.com/deeplight.pdf.
09 Vgl. Daniel Moore/Thomas Rid, Cryptopolitik and the Darknet, in: Survival 1/2016, S. 7–38.

„Silk Road" war der erste Kryptomarkt und ab Februar 2011 online. Er wurde im Oktober 2013 vom FBI geschlossen. Heute sind etwa zwei Dutzend Kryptomärkte online.[10] Allen Plattformen ist der Vertrieb von psychoaktiven Substanzen aller Art gemein, doch sie unterscheiden sich in puncto Marktgröße, Sprache, Bezahlsystem, Lebensdauer und der Frage, ob mit Waffen gehandelt wird oder nicht. Auf den meisten Plattformen hat sich die Norm etabliert, dass kein kinderpornografisches Material weitergegeben werden darf.[11] In einer Erhebung von 2012 wurde der monatliche Umsatz des damaligen Monopolisten „Silk Road" auf 1,22 Millionen US-Dollar geschätzt.[12] Die Schätzung umfasst alle angebotenen Güter und Dienstleistungen. Dieses Volumen ist laut einer weiteren Studie 2013 auf 100 Millionen US-Dollar gestiegen.[13] Nachdem „Silk Road" vom FBI geschlossen wurde, stieg die im Dezember 2013 gegründete Plattform „AlphaBay" zum Marktführer auf. Laut einer jüngeren Studie konnte sie den Umsatz halten: Allein aus dem Drogenhandel betrug er zwischen September 2015 und August 2016 94 Millionen US-Dollar.[14] Zusammenfassend kann festgehalten werden: Nach einem deutlichen Zuwachs während der Anfangsphase des Phänomens erreichten die Umsätze von Kryptomärkten ab 2013 ein relativ stabiles Niveau. Im Vergleich zum materiellen Drogenmarkt ist das Handelsvolumen jedoch sehr klein. Laut Schätzungen der Europäischen Beobachtungsstelle für Drogen und Drogensucht und Europol werden in der EU jährlich insgesamt 28 Milliarden US-Dollar mit dem Verkauf von Drogen erzielt – Kryptomärkte machen hiervon nur einen Bruchteil aus.[15]

RISIKEN ANONYMER DROGENMÄRKTE

Mit den oben skizzierten technologischen Innovationen, die den systematischen anonymen Verkauf und Kauf von Drogen aller Art möglich machten, traten Risiken in Erscheinung – allen voran das Risiko, das mit Verfügbarkeit und Zugänglichkeit einhergeht.[16] Auf anonymen Drogenmärkten im Darknet können sämtliche psychoaktive Substanzen mit einigen Mausklicks bestellt und bezahlt werden. Der Bestellvorgang unterscheidet sich kaum von dem anderer Online-Marktplätze. Ebenso niederschwellig ist die Aneignung des technisch erforderlichen Wissens, um Drogen zu bestellen. Das gilt vor allem für Digital Natives. Die Affinität lässt sich entsprechend auf einen neuen Typ technikaffiner Drogenhändler übertragen sowie auf einen neuen Typ Drogenkonsument. Durch die Nutzung von Verschlüsselungssoftware und Kryptowährungen wird der globale Verkauf und Kauf von Drogen rund um die Uhr, sieben Tage die Woche möglich. Zudem sind sämtliche Drogenarten in unterschiedlichen Mengen auf Kryptomärkten zugänglich, ohne regionale Einschränkung und Altersbeschränkung.

Ein Nebeneffekt des neuartigen Phänomens, der ebenfalls die Zugänglichkeit erleichtert, betrifft die Art der Lieferung. Die Übergabe der über das Darknet bestellten Drogen findet nicht bei persönlichen Treffen der beteiligten Akteure statt, wie auf materiellen Drogenmärkten üblich. Vielmehr übernehmen Zustelldienste unwissentlich die Rolle des Drogenkuriers. Händlerinnen und Konsumenten nehmen die Drogentransaktionen im Internet als Vorteil wahr. So gaben etwa bei einer anonymen Onlinebefragung 9470 Teilnehmer und Teilnehmerinnen an, der höhere Komfort bei der Bestellung sowie die einfache Lieferung der Drogensendungen seien unter anderem Hauptmotive dafür gewesen, auf Kryptomärkten Drogen zu kaufen.[17]

Die Verfügbarkeit und Zugänglichkeit stellen besonders für zwei Konsumtypen ein besonderes Risiko dar: zum einen für Konsumenten, die über keine hohe Impulskontrolle verfügen und zum

10 Siehe DarkNet Stats, https://dnstats.net.

11 Vgl. Martin (Anm. 5), S. 6.

12 Vgl. Nicholas Christin, Traveling the Silk Road: A measurement Analysis of a Large Anonymous Online Marketplace, Proceedings of the 22nd International Conference on World Wide Web, International World Wide Web Conferences Steering Committee 2013.

13 Vgl. Kyle Soska/Nicholas Christin, Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem, in: The USENIX Association (Hrsg.), Proceedings of the 24th USENIX Security Symposium, Washington D.C. 2015, S. 33–48.

14 Vgl. Meropi Tzanetakis/Heino Stöver (Hrsg.), Drogen, Darknet und Organisierte Kriminalität, Baden-Baden 2017.

15 Vgl. European Monitoring Centre for Drugs and Drug Addiction/Europol, EU Drug Markets Report. In-depth Analysis 2016, Luxemburg 2016, S. 27.

16 Vgl. Tzanetakis/Stöver (Anm. 14).

17 Vgl. Monica J. Barratt/Adam R. Winstock, Use of Silk Road, the Online Drug Marketplace, in the United Kingdom, Australia and the USA, in: Addiction 109/2014, S. 774–783.

unkontrollierten Konsum neigen. Zum anderen sind durch Kryptomärkte besonders Konsumenten gefährdet, die sozial isoliert Drogen konsumieren und sich dabei nicht Freunden und Bekannten anvertrauen.[18]

Auf Gelegenheitskonsumenten hat die hohe Verfügbarkeit sämtlicher Drogen im Internet hingegen eine andere Wirkung: User und Userinnen von „Silk Road" berichteten, dass es zunächst zum Konsumanstieg und Konsum verschiedener Drogen gekommen sei. Dieser Anstieg sei bei den Befragten allerdings früher oder später der Selbstregulierung des Konsums gewichen, eine Sättigung sei eingetreten. Die Befragten teilten weiter mit, dass die ständige Verfügbarkeit mittelfristig dazu geführt habe, dass das vorhergehende Konsumniveau wieder erreicht worden sei.[19]

Trotz der angesprochenen Gefahren bieten die Kryptomärkte paradoxerweise auch Potenziale – allen voran für den in der Drogenhilfe diskutierten Ansatz der Schadensminimierung.

POTENZIALE ANONYMER DROGENMÄRKTE

Der Schadensminimierungsansatz zielt darauf ab, den körperlichen, psychischen und sozialen Zustand von Drogenkonsumenten zu verbessern, ohne dabei unmittelbar den Zugang zu den Substanzen zu unterbinden.[20] Für materielle Drogenmärkte gilt, dass die Herstellung, der Anbau, Handel, Besitz und Konsum von Drogen verboten sind und Zuwiderhandlungen strafrechtlich verfolgt werden. Dies hat zur Folge, dass *erstens* die Qualität der im Einzelhandel vertriebenen Drogen relativ niedrig ist, auch weil staatlich kontrollierte Qualitätsstandards für Drogen fehlen.[21] *Zweitens* bedingt die internationale Drogenkontrollpolitik auf Basis der UN-Konventionen, dass sämtliche Akteure des Anbaus, der Produktion, des Erwerbs, Besitzes und Konsums von illegalen Substanzen der Gefahr der Strafverfolgung ausgesetzt sind.

Paradoxerweise kommt es bei Kryptomärkten für Drogen zu einer Umkehrung: Die technisch ermöglichte Verschleierung des Standorts und der personenbezogenen Daten hat für die Beteiligten einerseits ein reduziertes Risiko von Interventionen durch Strafermittlungsbehörden zur Folge, wenngleich weltweit zahlreiche Plattformen geschlossen und Händler sowie Kunden verhaftet und verurteilt worden sind. Andererseits bedingen Kryptomärkte auch den Vertrieb von qualitativ hochwertigen illegalen Drogen, zumindest im Vergleich zu den Substanzen, die auf der „Straße" gehandelt werden.[22] Der Erwerb von Substanzen, deren Konsum aufgrund ihrer Qualität mit geringeren gesundheitlichen Folgeschäden einhergeht, wird hier als Chance im Sinne des Schadensminimierungsansatzes begriffen.

Warum aber werden über Kryptomärkte tendenziell hochwertigere illegale Drogen gehandelt? Ein Erklärungsansatz liegt im Wettbewerb. Eine Studie zu Drogenangeboten, Umsätzen, Preisen sowie Herkunfts- und Zustellländern verdeutlicht den Grad der Wettbewerbsintensität im Darknet: Zwischen September 2015 und August 2016 haben allein auf der Plattform „AlphaBay" rund 2200 Händler etwa 12 000 verschiedene Drogenartikel angeboten.[23]

Für die Qualitätssteigerung ist ein weiterer Aspekt verantwortlich: das Bewertungssystem.[24] Der Ausgangspunkt für das Bewertungssystem war die Frage, warum Kunden ein illegales Produkt im Internet erwerben, wenn sie nicht wissen, von wem sie es kaufen, und wo doch das Risiko besteht, dafür strafrechtlich belangt zu werden. Anonyme Drogenplattformen haben hierbei auf einen Mechanismus zurückgegriffen, der bei konventionellen Online-Marktplätzen wie Amazon seit Längerem erfolgreich praktiziert wird. Auf Kryptomärkten bewerten Kunden die Qualität der Drogen, die Korrektheit der bestellten Menge, den Kundenservice, die verwendete Verschlei-

18 Vgl. Monica J. Barratt et al., ‚What if you live on top of a bakery and you like cakes?' – Drug Use and Harm Trajectories Before, During and After the Emergence of Silk Road, in: International Journal of Drug Policy 35/2016, S. 50–57.

19 Vgl. ebd., S. 53.

20 Vgl. Meropi Tzanetakis/Roger von Laufenberg, Harm Reduction durch anonyme Drogenmärkte und Diskussionsforen im Internet?, in: akzept e. V. Bundesverband für akzeptierende Drogenarbeit und humane Drogenpolitik (Hrsg.), 3. Alternativer Drogen- und Suchtbericht 2016, S. 189–194.

21 Vgl. Peter Reuter, Disorganized Crime: The Economics of the Visible Hand, Cambridge 1983.

22 Vgl. Barratt/Winstock (Anm. 17), S. 780.

23 Vgl. Tzanetakis/Stöver (Anm. 14).

24 Vgl. Meropi Tzanetakis et al., The Transparency Paradox. Building Trust, Resolving Disputes and Optimising Logistics on Conventional and Online Drugs Markets, in: International Journal of Drug Policy 35/2016, S. 58–68.

erungstechnik für die Sendung sowie die Kommunikation des Verkäufers oder der Verkäuferin. Dies geschieht sowohl über ein Punktesystem als auch über ausführliche Rezensionen. Diese Bewertungen und die detaillierten Angaben der Händler sind die Entscheidungsgrundlage für andere Kunden.

Wenn sich wie auf „AlphaBay" rund 2200 Händler um das Interesse der Kunden bemühen, ist zu vermuten, dass diejenigen Anbieter und Anbieterinnen, die qualitativ schlechte Drogen verkaufen und einen schlechten Kundenservice haben, ein entsprechend negatives Feedback erhalten. Folglich können nur diejenigen Händler ihre Waren absetzen, die hochwertige Drogen zum Verkauf bereitstellen. Es ist nicht auszuschließen, dass in näherer Zukunft nur noch einige wenige Händler den Markt beherrschen, ähnlich wie es bei den Internetunternehmen Amazon, Ebay, Facebook und Google auf ihren jeweiligen Märkten der Fall ist.[25]

Im Vergleich zum materiellen Einzelhandel sind Kryptomärkte für die Kunden zudem wesentlich transparenter. Drogenkonsumenten können nunmehr auf der Basis vergleichbarer Informationen über eine breite Palette an psychoaktiven Substanzen, Preisen und Qualitäten entscheiden, auf welchem Kryptomarkt sie bei welchem Händler welche Droge bestellen wollen. Damit ermöglicht der Drogenvertrieb über anonyme Plattformen im Darknet, soziale und gesundheitliche Risiken zu minimieren, die mit dem Erwerb und Konsum von illegalen Substanzen auftreten.

Selbstverständlich gibt es aber auch im Darknet Streitfälle: etwa wenn eine Drogenbestellung nicht beim Kunden eintrifft oder dieser fälschlicherweise behauptet, keine Lieferung erhalten zu haben. Auch das Darknet ist nicht gefeit vor größeren Konflikten wie Erpressung und Betrug – etwa wenn ein Teilnehmer droht, persönliche Informationen eines anderen zu veröffentlichen.

Institutionalisierte Mechanismen wie das Treuhandverfahren sollen auf Kryptomärkten diese Konflikte lösen:[26] Die Mechanismen unterscheiden sich je nach Bezahlsystem. Bislang haben sich drei bargeldlose Bezahlsysteme etabliert, die von fast allen Kryptomärkten unterstützt werden: *erstens* das sogenannte zentralisierte Treuhandverfahren. Dabei wird der Zahlungsbetrag in virtueller Währung wie Bitcoin auf der Plattform zwischengelagert und erst nach Erhalt der Sendung an den Händler freigegeben. Im Konfliktfall besteht die Möglichkeit, ein Schlichtungsverfahren einzuleiten, das vom Betreiber beziehungsweise der Betreiberin des Kryptomarkts geführt wird. Bei einer *zweiten* Variante, dem frühzeitigen Zahlungsabschluss, wird der Zahlungsbetrag direkt vom Kunden an den Händler transferiert, noch bevor die Bestellung beim Kunden eingetroffen ist. Bei dieser Bezahlvariante findet im Konfliktfall keine Vermittlung durch den Marktplatzbetreiber statt. Das Mehrparteien-Treuhandverfahren ist die *dritte* Bezahlmöglichkeit. Sie ist die technisch anspruchsvollste. Die Zahlungsbeträge werden erst freigegeben, wenn zwei der drei Akteure – Käufer, Verkäufer und Marktplatzbetreiber – die Transaktion bestätigen. Während die letztgenannte als die sicherste gilt, bestehen bei den ersten beiden Bezahlvarianten Betrugsmöglichkeiten durch den Akteur, der den Zahlungsbetrag zwischenlagert beziehungsweise erhält. Diese drei Mechanismen sind ein Indiz für die Selbstregulierung von Kryptomärkten abseits staatlicher Interventionen.

Mit Blick auf das Konfliktpotenzial besteht der entscheidende Unterschied zwischen materiellen Drogenmärkten und Kryptomärkten in der Qualität der „Streitfälle":[27] Auf Ersterem gehören physische und psychische Gewalt zum Mittel der Wahl, um Konflikte zu „lösen", um Transaktionen durchzusetzen oder um die Zusammenarbeit mit der Polizei zu bestrafen.[28] Da auf Kryptomärkten Transaktionen anonym und entpersonalisiert stattfinden, ist interpersonelle Gewalt kaum möglich. Laut einer Studie, an der weltweit 3794 aktive Nutzer von Kryptomärkten teilgenommen haben, ist auf Plattformen im Darknet das Risiko für drogenbezogene Ge-

25 Vgl. Ulrich Dolata/Jan-Felix Schrape (Hrsg.), Kollektivität und Macht im Internet. Soziale Bewegungen – Open Source Communities – Internetkonzerne, Wiesbaden 2018 (i. E.).

26 Vgl. Tzanetakis et al. (Anm. 24), S. 64.

27 Vgl. Meropi Tzanetakis, Online Drug Distribution: Alternatives to Physical Violence in Conflict Resolution, in: Marije Wouters/Jane Fountain (Hrsg.), Between Street and Screen. Traditions and Innovations in the Drugs Field, Lengerich 2015, S. 41–56.

28 Vgl. Peter Reuter, Systemic Violence in Drug Markets, in: Crime, Law and Social Change: An Interdisciplinary Journal 3/2009, S. 275–284.

walt beziehungsweise für die Androhung dieser wesentlich kleiner als auf materiellen Drogenmärkten.[29] 35 Prozent der Befragten berichteten von Gewalterfahrungen mit unbekannten Dealern auf der Straße; 24 Prozent gaben an, von einem ihnen bekannten Dealer bedroht worden zu sein und 14 Prozent berichteten von persönlichen Bedrohungen beim Handel mit befreundeten Dealern. Im Vergleich dazu erlebten lediglich 3 Prozent der Befragungsteilnehmer persönliche Bedrohungen beim Drogenkauf im Darknet.

UMGANG MIT ANONYMEN DROGENMÄRKTEN

Der Prozess der Digitalisierung bringt weitreichende Veränderungen in verschiedenen Bereichen der Gesellschaft mit sich. Dies hat selbstverständlich ebenso Auswirkungen auf unterschiedliche Kriminalitätsformen. Beruhend auf neuen Informations- und Kommunikationstechnologien konnte sich ein Phänomen etablieren, das als kriminelle Innovation eingestuft werden kann.[30] Dabei finden Drogenübergaben nicht in Form persönlicher Treffen statt, sondern werden mit virtuellen Währungen bezahlt und in äußerlich unauffälligen Sendungen verschickt. Die Zustellung übernimmt der ahnungslose Postdienst. Entsprechend groß sind die Herausforderungen, vor denen Strafermittlungsbehörden stehen.[31]

Wie ist mit diesem neuen Phänomen auf politischer Ebene umzugehen? Laut einer empirischen Studie haben die Schließungen von Kryptomärkten durch Strafverfolgungsbehörden kaum Einfluss auf die Resilienz des Systems der anonymen Drogenmarktplätze.[32] Die Autoren der Studie untersuchten die Auswirkungen der Operation Onymous – Behörden aus den USA und Europa legten im November 2014 zahlreiche Kryptomärkte still – auf die Umsätze im Darknet. Zwar habe die Aktion zum sofortigen Rückgang der Gesamtumsätze der Kryptomärkte geführt, aber schon nach einigen Wochen sei die Hälfte des Umsatzniveaus wieder erreicht worden. Nach Schließung der Marktplätze wichen die Kunden scheinbar nach einer kurzen Phase der Verunsicherung auf andere Märkte beziehungsweise Händler aus. Anhand des Verlaufs von Umsätzen ließ sich die begrenzte Wirkung von Strafverfolgungsaktivitäten verdeutlichen.

Unabhängig davon, ob die Operation Onymous zum gewünschten Resultat geführt hat oder nicht, müssen politische Entscheidungsträger neue Ansätze für den Umgang mit Kryptomärkten entwickeln. Neben den offensichtlichen Risiken, die mit dem erleichterten Zugang zu Drogenmärkten einhergehen, gibt es ebenso Chancen für eine Drogenpolitik, die sich dem Ansatz der Schadensminimierung verschreibt: zum einen aufgrund des geringeren Gewaltpotenzials beim anonymen Drogenkauf, zum anderen wegen der erhöhten Qualität der Substanzen – zumindest im Vergleich zur Qualität der Produkte auf der „Straße“.

29 Vgl. Monica J. Barratt/Jason A. Ferris/Adam R. Winstock, Safer Scoring? Cryptomarkets, Social Supply and Drug Market Violence, in: International Journal of Drug Policy 35/2016, S. 24–31.
30 Vgl. Judith Aldridge/David Décary-Hétu, Not an „Ebay for Drugs“: The Cryptomarket „Silk Road“ as a Paradigm Shifting Criminal Innovation, 13. 5. 2014, https://ssrn.com/abstract=2436643.
31 Siehe hierzu auch den Beitrag von Otto Hostettler in dieser Ausgabe (*Anm. d. Red.*).
32 Vgl. Soska/Christin (Anm. 13).

MEROPI TZANETAKIS
ist Erwin-Schrödinger-Fellow des österreichischen Wissenschaftsfonds und Gastforscherin am Institut für Kriminologie und Rechtssoziologie der Universität Oslo. Zu ihren Forschungsschwerpunkten gehören digitale Technologien, illegale Märkte sowie organisierte Kriminalität.
meropi.tzanetakis@univie.ac.at

Herausgegeben von der
Bundeszentrale für politische Bildung
Adenauerallee 86, 53113 Bonn
Telefon: (0228) 9 95 15-0

Redaktionsschluss dieser Ausgabe: 3. November 2017

ISSN 0479-611 X

bpb:

APuZ

Nächste Ausgabe
48/2017, 27. November 2017

STADTPOLITIK

APuZ
AUS POLITIK UND ZEITGESCHICHTE
www.bpb.de/apuz