Digitalgespräch Folge 24

Was ist das Darknet und was passiert dort?

Mit Kai Denker von der Technischen Universität Darmstadt, 5. Juli 2022
https://zevedi.de/digitalgespraech-024-kai-denker/

[Der Vorspann mit Musik und Ausschnitten aus dem Gespräch beginnt.]

Marlene Görger [mg]: Herr Denker, Sie sind wissenschaftlicher Mitarbeiter am Institut für Philosophie der TU Darmstadt. In der Vergangenheit haben Sie sich intensiv mit dem Darknet beschäftigt. Sie sind sowohl Philosoph als auch Historiker und Informatiker.

Kai Denker [Denker]: Cloudflare hat mal gesagt, 94 Prozent des Traffics aus dem Tornetzwerk wären sowieso bösartig. Ich weiß jetzt nicht, wie sie das gemessen haben. Man ist natürlich bei Strafverfolgungsbehörden nie glücklich über alles, was irgendwelche Recherchesachen erschwert. Also man ist ja schon nicht glücklich darüber, dass es Datenschutz gibt – manchmal hat man das Gefühl. Wenn man es wirklich verhindern möchte, dass Leute verschlüsselt über das Tor-Netzwerk kommunizieren, dann muss man verhindern, dass Leute verschlüsselt kommunizieren. Und das können wir nicht wollen.

Petra Gehring [pgg]: Gibt es Beispiele, dass es doch einen Unterschied gemacht hat, dass man sich im Darknet bewegen konnte, mit einer Erwartung da politisch geschützt zu werden vor Verfolgung?

[Denker]: Das ist ja dann auch eine Designentscheidung der Software. Das ist dann nicht irgendwie eine demokratietheoretische Frage, sondern Software-Engineering-Frage, dass man das so gemacht hat. Und das könnte man sicherlich auch anders lösen. Emanzipationen sind ja auch politische Prozesse. Die haben immer sehr, sehr viel damit zu tun, auch Gesicht zu zeigen, politischen Druck zu machen. Und das gelingt nicht, indem ich im Darknet irgendwas poste.

[Der Vorspann endet. Das Gespräch beginnt.]

[mg]: Den Begriff Darknet verbinden viele Menschen vor allem mit Kriminalität. Fast so, als bezeichne er einen Ort, den unbescholtene Bürgerinnen und Bürger gar nicht erst finden würden, an dem sich zwielichtige Gestalten treffen, um mit Waffen oder Drogen zu handeln, Terroranschläge zu planen und um Bildmaterial auszutauschen, das Gewalt und Missbrauchshandlungen zeigt. Tatsächlich kann die Anonymität und die Abgeschiedenheit des Darknets Kriminelle, die für ihre Taten das Internet nutzen, vor Strafverfolgung schützen und tut es auch. Den Schutz zu brechen, ist eine große Herausforderung für ErmittlerInnen und gelingt oft erst, wenn der Zufall zu Hilfe kommt. Dieser Eindruck von Machtlosigkeit des Rechtsstaats ist vor allem, wenn Kindern Schlimmes angetan wird, nur schwer zu ertragen. In liberalen Gesellschaften wie der unseren dominiert dieser Aspekt die öffentliche Wahrnehmung dessen, was es mit dem Darknet auf sich hat. Allerdings bietet das Darknet Schutz durch Anonymität nicht nur VerbrecherInnen, sondern auch WhistleblowerInnen, die mit der Presse in Kontakt treten, JournalistInnen und ihren Quellen bei riskanten Recherchen oder AktivistInnen und Oppositionellen die Verfolgung durch Geheimdienste oder autoritäre Regime fürchten müssen. Und es kann auch schlicht den legitimen Wunsch

nach einem Maximum an Privatsphäre und dem Schutz persönlicher Informationen vor dem Zugriff Dritter erfüllen. Ganz ohne kriminelle Absichten, sondern viel mehr in Ausübung von Grundrechten. Hier erweist sich das anonyme Internet als wichtiges Instrument für politisches Engagement und emanzipatorische Bewegungen, womöglich sogar für die Stabilisierung liberaler Gesellschaften. Was das Darknet ist, für welche Zwecke es eingesetzt wird und wie mit dem Konflikt umgegangen werden könnte, den es zwischen Forderungen nach effektiver Strafverfolgung einerseits und dem Schutz von Grundrechten andererseits aufmacht, darüber wollen wir heute im Digitalgespräch reden. Mein Name ist Marlene Görger. Ich bin Physikerin und Technikphilosophin am Zentrum verantwortungsbewusste Digitalisierung.

[pgg]: Und ich bin Petra Gehring, Professoren für Philosophie an der Technischen Universität Darmstadt. Wie immer sind wir zu dritt im Digitalgespräch, denn bei uns ist natürlich wieder ein Experte für unser Thema. Es ist Dr. Kai Denker aus Darmstadt, der sich mit uns in der Videokonferenz trifft. Herzlich willkommen im ZEVEDI-Podcast, Herr Denker. Wir freuen uns, dass Sie sich die Zeit für uns nehmen.

[Denker]: Hallo, ich freue mich auch.

[mg]: Herr Denker, Sie sind wissenschaftlicher Mitarbeiter am Institut für Philosophie der TU Darmstadt und leiten dort ein internetbezogenes Verbundprojekt. Zu Ihren Forschungsschwerpunkten gehören Technikphilosophie und Philosophie des Digitalen. In Ihrer Arbeit bringen Sie bereits selbst mehrere fachliche Hintergründe zusammen, denn Sie sind sowohl Philosoph als auch Historiker und Informatiker. Mit diesen Perspektiven beobachten Sie auch Netzkulturen und Online-Communities in Winkeln des Internets, die auf viele Menschen abschreckend wirken und in die sich nicht unbedingt jede und jeder vorwagt. In der Vergangenheit haben Sie sich intensiv mit dem Darknet beschäftigt und untersucht, welche Strukturen und Praktiken sich dort vorfinden. Auf einige Fragen, die sich der Gesellschaft im Umgang mit dem Darknet stellen, kommen wir später im Detail zu sprechen. Vorher sollten wir aber verstehen, wovon genau wir reden. Was ist das Darknet eigentlich?

[Denker]: Ja, das ist tatsächlich die größte und schwierigste Frage, würde ich fast sagen. Denn es ist verdammt schwierig herauszufinden: Über was reden wir hier eigentlich? Definitionen werden nämlich oft so gewählt, wie sie gerade zu einer Forschungsfrage passen. Und eine einheitliche Definition gibt es nicht. Die meisten Leute denken an das Tor-Netzwerk. Das ist auch nicht falsch. Aber das ist eben nur so ein Teil der Geschichte. Wir müssen vielleicht erstmal ein paar Begriffe sortieren am Anfang, bevor wir auch nur so halbwegs auf die Idee kommen könnten, was das Darknet ist.

[pgg]: Geht schon los bei Tor-Netzwerk.

[Denker]: Genau.

[pgg]: Was ist ein Tor-Netzwerk?

[Denker]: Ja, also ich würde vorschlagen, das setzen wir uns kurz noch auf die Warteliste, die Frage. Und versuchen erst ein paar grundlegende Begriffe zu sortieren. Dann wird das nämlich leichter zu beantworten. Der grundlegende Begriff wäre erstmal, wir haben es einerseits mit einem Clearnet zu tun. Das ist sozusagen das

Internet, was alle kennen. Und dann auf der anderen Seite hätten wir das Darknet. Das können wir jetzt noch weiter differenzieren. Die meisten von uns werden das World Wide Web kennen. Also das, was man über den Internetbrowser besucht. Da kann man dann auch wieder unterscheiden, ob wir es mit dem Surface Web oder dem Deep Web zu tun haben. Und in beiden Begriffen befinden wir uns immer noch im Clearnet, wenn wir so wollen. Surface Web, das ist das, was wir über Google finden, kurz gesagt. Also die Oberfläche des World Wide Web, die leicht per Suchmaschine, per Google oder irgendwelchen anderen Anbietern zu finden ist. Und das Deep Web sind dann, das ist ein Begriffsvorschlag, die Teile des World Wide Web, die nicht zu finden sind. Zum Beispiel, weil sie nicht indiziert werden. Zum Beispiel, weil sie sich hinter Login-Pages verbergen. Das können dann auch Intranets sein und dergleichen mehr. Man kann noch sich wieder außerhalb des WWW überlegen, dass auch Sachen wie alte Chat-Protokolle, IRC oder dergleichen zu einem Deep Net gehören. Also jetzt muss ich aufpassen, dass ich die Begriffe nicht übermäßig verkompliziere. Also wir haben es zu tun, kurz gesagt, damit: Es gibt in dem Teil des Internets außerhalb des Darknets durchaus auch Bereiche, die schwer zu finden sind, die schwer zugänglich sind. Teilweise mit Passwortschutz, teilweise einfach nur, weil man nicht zufällig dahin gelangt, sondern schon wissen muss, wo man hingeht, um darauf zugreifen zu können. Und das ist aber der ganze Bereich noch Clearnet, wie man das nennen kann oder wie wir das nennen. Und auf der anderen Seite haben wir es dann mit dem Darknet zu tun. Und das ist dann ein Teil des Internets, der nur mit spezieller Software erreichbar ist. Und ich hatte jetzt vorhin schon das Tor-Netzwerk erwähnt. Das wäre in dem Fall dann ein Teil des Internets, der nur mit dem Tor-Browser zu erreichen ist. Der Tor-Browser, das ist eine modifizierte Version des Browsers Firefox, der schon alle Module mitbringt, die man braucht, um auf Tor zugreifen zu können. Und den kann man sich im Internet runterladen, installieren, startet das Programm und dann hat man Zugriff auf Tor. Das ist auch relativ einfach. So, Tor selbst ist im Grunde eine Art, das kann man sich glaube ich so vorstellen, verschachteltes VPN. Es benutzt also auch Technologien, die wir bei VPNs einsetzen, also Virtual Private Networks. Kennen wahrscheinlich die meisten, wenn man sich beim Arbeitgeber einwählt oder wenn man über Anbieter irgendwelche Geo-Blocking-Sachen umgehen möchte. Und das Tor-Netzwerk nutzt diese Technik, im Prinzip ist das dieselbe Technik, aber verschachtelt sie mehrfach ineinander. Daher kommt auch dieser Name. Also mittlerweile ist es einfach nur Tor, also das T groß, der Rest klein, früher war es TOR, komplett großgeschrieben, und es war dann The Onion Router. Und die Idee ist, ein Netzwerk zu haben, welches so einem Zwiebelprinzip folgt. Es werden also mehrere Verschlüsselungsschichten aufeinandergelegt. Es wird dann eine Verbindung im Netz gesucht, die über mehrere Knotenpunkte läuft, also sogenannte Relays, und jedes Relay ist nur in der Lage, eine Schicht dieser Verschlüsselung zu beseitigen und dann auch wieder zu entschlüsseln. Und das führt dazu, dass man kontrollieren kann, welches Relay welche Informationen über eine Verbindung im Netz hat. Die Idee ist, dafür zu sorgen, dass es kein Relay gibt, welches weiß, wo die Verbindung losgeht und wo die Verbindung hingeht. Also eine Verbindung im Internet ist ja immer definiert über eine IP-Adresse und einen Port. Das heißt, wenn Sie sich ins Internet einwählen, dann bekommen Sie eine IP-Adresse zugewiesen. Und wenn Sie dann auf eine Webseite zugreifen, zum Beispiel die Webseite der TU Darmstadt, dann geben Sie das in Ihren Browser ein. Ihr Browser sucht dann die passende IP-Adresse zu dem Namen TU Darmstadt und baut eine Verbindung auf. Und diese Verbindung beinhaltet dann, wie gesagt, Ihre eigene IP-Adresse und die Adresse der TU Darmstadt. Sie schicken sozusagen die Anfrage hin, ich möchte diese Webseite sehen, und der Server der TU Darmstadt schickt dann an Ihre IP-Adresse die Antwort wieder zurück. Das ist ganz

kurz gesagt das Prinzip. Das heißt, es kann dort sowohl die TU Darmstadt sehen, wo es herkommt, als auch jeder Knoten dazwischen, jeder Router, der das weiterleitet, kann beide Adressen sehen. Und das möchte man im Tor-Netzwerk nicht. Man möchte dafür sorgen, dass es nicht möglich ist, das zuzuordnen. Also, wer greift auf was zu? Und die Idee ist nun, dass ich mir drei Relay-Knoten suche im Tor-Netzwerk. Also mein Tor-Browser formuliert dann die Anfrage an die Webseite der TU Darmstadt und verschlüsselt die dreimal. Und zwar so, dass die äußerste Schicht von dem ersten Relay-Knoten geöffnet werden kann. Darin findet er dann wieder nur was Verschlüsseltes und die Information, wer der zweite Relay-Knoten ist. Das heißt, der erste Relay-Knoten kennt mich und den zweiten Relay-Knoten. Der erste schickt es dann, dieses verschlüsselte Paket, an den zweiten Relay-Knoten. Der kann das dann entschlüsseln, sieht dort Information, wer der dritte Relay-Knoten ist, und wieder nur ein verschlüsseltes Datenpaket. Der zweite kennt dann also den ersten Relay-Knoten und den dritten Relay-Knoten. Der zweite schickt es also an den dritten Relay-Knoten. Der kann die letzte Verschlüsselungsschicht öffnen. Und der sieht: Es ist eine Anfrage an die TU Darmstadt. Aber er sieht nicht, wo sie herkommt. Der dritte kennt also nur den zweiten Relay-Knoten und TU Darmstadt, schickt die Anfrage an die TU Darmstadt. Der Server der TU Darmstadt antwortet, sieht nur den dritten Relay-Knoten, schickt die Antwort also an den zurück. Und dann geht diese Verschlüsselungslogik wieder rückwärts zu mir zurück. Und ich sehe ja dann schlussendlich die Webseite der TU Darmstadt auf meinem Computerbildschirm. Und zumindest in der Theorie kann dann niemand sagen, dass der Herr Denker auf die Webseite der TU Darmstadt zugegriffen hat. Sondern man kann nur sehen: Der Herr Denker hat das Tor-Netzwerk verwendet. Und man kann sehen, dass das Tor-Netzwerk auf die Webseite der TU Darmstadt zugegriffen hat. Soweit die Theorie.

[pgg]: Es gibt also mit dieser Technik einen gut benutzbaren automatisierten Eingang. Insofern ist Tor im Deutschen natürlich schön doppeldeutig ein Eingang hinein in diesen Teil des Netzes, in dem dann wiederum alle anderen auch so gesichert eingestiegen sind. Sodass im Grunde klar ist: Man bewegt sich jetzt unter anonymisierten oder herkunftslosen Adressen.

[Denker]: Ja, also in dem Beispiel ist es nun so, dass die TU Darmstadt ja bekannt ist. Also es ist nicht unklar: Wer ist die TU Darmstadt? Man muss hier also vielleicht nochmal differenzieren. Ich habe jetzt beschrieben, wie ich das Tor-Netzwerk verwende, um auf eine Webseite im Clearnet zuzugreifen. Ich könnte ja meinen ganz normalen Webbrowser nehmen und auch auf die Webseite der TU Darmstadt zugreifen. Wenn man das so verwendet, hat Tor im Grunde die Funktion eines Privacy Preserving Networks. Also, es ist ein Netzwerk, welches Privatsphäre schützt, indem es weniger Datenspuren erzeugt. Beziehungsweise die Datenspuren, die es erzeugt, sind so gestaltet, dass es extrem schwierig ist, sie wieder zusammenzusetzen. Ich kann auch auf Dienste zugreifen, die nur im Tor-Netzwerk verfügbar sind. Das nennt sich dann Hidden Service, mittlerweile nennen wir es jetzt auch Onion Service. Und dabei ist dann auch unklar: Wer ist denn derjenige, mit dem ich spreche? Also dann kann auch jemand eine Webseite zur Verfügung stellen und bleibt als Anbieter einer Webseite noch anonym. Und man könnte sich überlegen, und ich halte das auch für die bessere Definition, zu sagen: Darknet ist nur der Bereich, in dem auch die Anbieter anonym sind. Denn es macht aus meiner Sicht wenig Sinn zu sagen, eine reguläre Webseite, das muss jetzt nicht die Uni sein, das kann auch irgendeine Zeitung sein oder Stadtwerk oder was auch immer, die wären jetzt erreichbar übers Darknet. Gut, ich kann mich dazu entscheiden, auf diese Weise darauf zuzugreifen, weil ich nicht

möchte, dass mich irgendjemand dabei beobachten kann. Aber das ist leider noch nicht der Bereich, der so anonym ist, dass auch die Anbieterseite anonym ist. Es lässt sich noch eine dritte Verwendung von diesem Tor-Netz überlegen, dass es auch dazu dienen kann, Zensur zu umgehen. Also wenn ich mich zum Beispiel in einem Land befinde, in dem der Zugriff auf bestimmte Webseiten beschränkt ist, ich aber auf Tor zugreifen kann, dann kann ich mit Tor sehr leicht auch meinen Internetdatenverkehr so umleiten, dass ich doch wieder Zugriff auf die Webseite habe. Also, es ist auch eine Technologie zur Zensurumgehung. Da gibt es natürlich auch andere Möglichkeiten. Also, man muss dafür nicht Tor nutzen, aber das ist sozusagen ein Nebeneffekt dieser Architektur. Und wie gesagt, Darknet ist eigentlich der Hauptpunkt, würde ich sagen, die Hidden Services oder Onion Services. Und in Ihrer Frage, Frau Gehring, steckt noch so ein zweiter Aspekt mit drin, nämlich dass es eine Frage der Masse ist. Wenn ich jetzt natürlich der Einzige bin, der das Tor-Netzwerk benutzt, und ich eine Anfrage reinschicke und aus dem Tor-Netzwerk kommt eine Anfrage irgendwo raus, naja, dann ist es nicht so überraschend, dass ich das wohl war. Das heißt, dass die Sicherheit des Tor-Netzwerks basiert auch darauf, dass es von einer hinreichend großen Menge Leuten, von vielen Leuten, benutzt wird. Dann wird es nämlich schwieriger, diese Korrelationsattacken durchzuführen. Das heißt, es wird schwieriger zu sagen: Okay, es wurde eine Anfrage reingeschickt und das, was herausgekommen ist, wird das wohl gewesen sein. Und je mehr das benutzen, desto schwieriger wird diese Zuordnung.

[pgg]: Korrelationsattacke, das war jetzt schon der Punkt, den Sie eben angedeutet hatten. In der Theorie kann man es gar nicht rauskriegen, aber es gibt indirekte Verfahren, wo man doch versuchen kann zu ermitteln, wer ist da unterwegs oder wer ist es im konkreten Fall gewesen?

[Denker]: Ja, es gibt eine ganze Reihe von Möglichkeiten, Tor zu deanonymisieren oder, ich sage mal, Schindluder zu treiben. Es könnte zum Beispiel sein: Man lädt sich über Tor eine Datei herunter und die hat einen aktiven Inhalt. Ich mache die dann außerhalb des Tor-Browsers auf und die würde mich deanonymisieren. Oder es gibt Phänomene wie Browser-Fingerprinting, also unsere Webbrowser schicken auch Einstellungen mit, informieren quasi über installierte Schriftarten, über Bildschirmauflösungen, über bevorzugte Sprachen und Ähnliches. Und auch das könnte dann jemand auf der anderen Seite wieder erkennen. Der Torbrowser hat ein paar Mechanismen, um das einzuschränken. Dann gibt es dieses Phänomen der Bad-Exit-Node. Also, ich hatte ja diese drei Relay-Knoten beschrieben. Man nennt die auch Guard-, Middle- und Exit-Node. Und die Exit-Node, die sieht ja den Inhalt meiner Kommunikation. Es macht also immer noch zusätzlich Sinn, etwas wie HTTPS zu benutzen, was wir ja zum Beispiel vom Online-Banking kennen. Das ist dann sozusagen eine vierte Verschlüsselungsschicht, die verhindert, dass der Exit-Knoten, die Exit-Node, sehen kann, was der Inhalt ist, den ich schicke. Und es ist natürlich so: Wenn ich auf eine Webseite zugreife und dort ein Formular ausfülle und dort meinen Namen eintrage, dann bin ich natürlich auch nicht mehr anonym. Also sowohl Benutzungsfehler als auch technische Attacken sind möglich. Diese Bad-Exit-Nodes könnten zum Beispiel auch versuchen, diese HTTPS-Verbindungen zu unterbrechen oder falsche Zertifikate einzuschleusen. Also auch hier muss man immer gucken, passt das Zertifikat wieder, wie wir das auch hoffentlich alle beim Online-Banking immer regelmäßig machen, aufzupassen, dass sich da nicht irgendetwas eingeschlichen hat und so weiter und so fort. Also Tor ist kein Allheilmittel. Es ist nicht perfekt. Es ist brechbar, aber es ist schwer. Und deswegen fühlen sich auch viele offensichtlich ja

sicher genug, es zu nutzen, sowohl zum Zugriff auf etwas als auch auf der Angebotsseite.

[mg]: Was sind denn Motivationen, die man so vorfindet? Ich meine, wir kennen natürlich so Beispiele, die gerade aus diesem kriminellen Umfeld kommen. Aber es ist ja nicht alles, was im Darknet stattfindet, illegal.

[Denker]: Nein, also nicht alles, was man im Darknet auf diesen Hidden Services findet, ist illegal. Es ist ein bisschen schwierig zu sagen: Wie viel ist denn legal oder illegal? Das fängt natürlich damit an, dass es erst mal eine durchaus schwierige Frage ist: Ist ein Angebot legal oder illegal? Das unterscheidet sich ja auch danach, in welchem Land sich das Angebot befindet. Das sehen wir natürlich bei einem Hidden Service nicht. Aber es ist natürlich ein Unterschied, ob ich mich in dieser oder jener Rechtsordnung bewege, wenn man sich anschaut, welche Inhalte ich anbiete. Also, selbst wenn wir diese Frage dann irgendwie versuchen zu vereinfachen oder einfach zu nehmen, zu sagen, was weiß ich, deutsche Rechtsordnung oder dergleichen, ist es natürlich immer noch schwierig, auch zu sagen, welche Onion Services habe ich denn alle. Also, es gibt zwar so Directories, aber viele sind auch nicht verfügbar. Viele kann man dann auch nur wieder mit so einem Trick erreichen und so weiter und so fort. Also, es ist nicht so trivial, das zu sagen, was dort auf der Angebotsseite stattfindet. Ich habe vorhin mal in der Vorbereitung geschaut, es gibt verschiedene Zahlen, die sind teilweise ein bisschen älter. Cloudflare hat mal gesagt, 94 Prozent des Traffics aus dem Tor-Netzwerk wären sowieso bösartig. Ich weiß jetzt nicht, wie sie das gemessen haben. Das scheint mir auch ein bisschen hoch, aber es ist vielleicht auch nicht ganz unrealistisch. Eine andere Information zum Beispiel: Dass unter 40 Prozent, also so 37,5 hatte ich gerade gelesen, der Inhalte des Darknets der Hidden Services überhaupt nur legal sein. Und wie gesagt, da ist die Frage: Welche Rechtsordnung ist damit gemeint und so fort? Man kann sich vielleicht noch eine Zahl vergegenwärtigen. Es gibt ungefähr 700.000 dieser Onion-Adressen. Also, so ein Hidden Service wird über eine Onion-Adresse abgefragt. Für die AnwenderInnen sieht das aus wie so ein 'Zeichensalat.onion'. Also wie so eine Top-Level-Domain '.de' oder '.org' steht da '.onion'. Das kann auch nur der Tor-Browser dann auflösen. Und dieser Zeichensalat davor, das ist ein kryptographischer Schlüssel, der verwendet wird, um darauf zuzugreifen. Und davon gibt es, habe ich vorhin geschaut, 700.000 derzeit. Die Tendenz ist sinkend. Das heißt aber nicht, dass es wirklich weniger funktionierende Angebote gibt oder so. Also die meisten sind auch, würde ich sagen, einfach nicht erreichbar. Das hat auch was damit zu tun, dass viele dieser Angebote auch Experimente sind, dass man das sehr, sehr leicht auf dem eigenen Rechner installieren kann. Und dann gibt es auch einfach Adressen, die nach kürzester Zeit schon wieder weg sind. Und das sind auch oft keine großen Anbieter oder Rechenzentren oder gut gepflegte Serverparks oder was auch immer, was dahintersteht. Sondern man kann das auf einem Raspberry Pi laufen lassen. Also auf einer kleinen Schachtel, die auch nicht sonderlich zuverlässig – die ist nicht dafür ausgelegt, wirklich so etwas anzubieten. Und dann ist das vielleicht eher Spielerei. Also man kann es nicht so genau sagen, oder ich kann es nicht so genau sagen. Was man aber sieht, ist, das Tornetz hat einen Traffic von ungefähr 200 Gigabit pro Sekunde. Und auf die Onion-Adressen fallen so ungefähr derzeit 20 bis 30 Gigabit. Das steigt dann interessanterweise. Also im Mai waren es 10 Gigabit. Es gibt auch immer wieder so Spikes, also was gerade zu sehen ist in der Statistik, das kann auch so ein Spike sein, dass es wieder runtergeht. Aber man kann vielleicht sagen: Naja, so ein Zehntel bis ein Zwanzigstel des Datenverkehrs im Tornetz entfällt dann überhaupt auf diese Hidden Services.

[mg]: Und der Rest sind dann Nutzer, die sich einfach anonym im normalen Internet, nenne ich es mal, bewegen?

[Denker]: Ja, und na gut, da war noch die Frage nach der Motivation. Das ist, wie gesagt, ja ein bisschen schwierig, weil nicht ganz klar ist, was für Angebote gibt es, wie werden die teilweise refrequentiert. Es gibt halt schon diese Märkte. Es gibt so einen Konzentrationsprozess dieser Märkte. Das hängt damit zusammen, dass ja auch immer mal wieder welche abgeschaltet werden. Also zum Beispiel jetzt im April hat ja das BKA gemeldet, dass sie den Hydra-Markt abgeschaltet haben. Und jetzt habe ich gelesen, jetzt wird Alpha Bay anscheinend wieder stärker. Das war ein Marktplatz, der ist schon mal vor ein paar Jahren abgeschaltet worden. Und jetzt ist zumindest dieser Name wieder da. Und die haben jetzt einen Wachstumskurs, nachdem Hydra-Market abgeschaltet wurde. Also, es gibt auch immer diese Ausweichbewegung. Das ist vielleicht auch noch wichtig zu wissen. Es gibt Sammlungen von Angeboten im Darknet, also auf Hidden Services, zum Beispiel Hidden Wiki. Da gibt es also so Listen, die sind dann teilweise auch recht schnell veraltet. Das muss man sich so ein bisschen vorstellen wie so Yahoo in den 90ern. Also als so eine Redaktion noch, die so eine Linkliste im Grunde kuratiert hat, so funktionieren die auch. Es gibt auch Suchmaschinen, die das listen. Und da findet man auch Imageboards. Man findet auch Social Networks. Die existieren nicht so lange. Ich habe mal vorhin versucht, ein funktionierendes zu finden. Das ist mir auf die Schnelle nicht geglückt. Das heißt nicht, dass die nicht mehr existieren. Das kann auch sein, dass die gerade ausgefallen sind. Also, die haben nicht so eine Verfügbarkeit, wie man das so von Facebook gewohnt ist. Ja, also es gibt schon viel. Es gibt auch private Blogs. Man kann darüber auch E-Mail machen. Man kann auch Filesharing betreiben. Es gibt auch Hidden Services mit zum Beispiel E-Books, die dort angeboten werden. Also Urheberrechtsverletzungen sind das dann effektiv. Das sind so Sachen. Und natürlich hat man, was viel diskutiert wird, was man aber natürlich auch aus Gründen wenig sieht, Angebote für Dissidenten in totalitären Staaten oder dergleichen. Also man sieht natürlich solche Angebote. So Secure Drops. Also zum Beispiel die Süddeutsche Zeitung betreibt so eine Seite. Ich kann nur nicht sagen, wie gut die frequentiert werden. Da müssten Sie die Süddeutsche Zeitung fragen.

[pgg]: Die Frage hätte ich jetzt gehabt. Wahrscheinlich ist sie nicht beantwortbar. Ich weiß nicht, ob Sie eine Einschätzung haben. Wenn es sowas gibt, wie doch auch so eine demokratietheoretische Bedeutung dieser Räume, in denen man mit der Presse geschützt Kontakt aufnehmen kann, in denen sich vielleicht AktivistInnen austauschen können etc., wie gewichtig ist das im Darknet? Der Anteil wird wahrscheinlich eher gering sein. Aber er ist ja doch da. Wie bedeutsam ist das? Gibt es Beispiele, an denen man ablesen kann, dass es doch einen Unterschied gemacht hat, dass man sich im Darknet bewegen konnte? So mit einer gut nachvollziehbaren Erwartung, da politisch geschützt zu werden vor Verfolgung?

[Denker]: Ich glaube, hier muss man doch nochmal diese Unterscheidung machen: Nutze ich Tor als ein Anonymisierungsnetzwerk, um auf etwas zuzugreifen, oder nutze ich es, um auf anonymisierte Dienste, Hidden Services, Onion Services, zuzugreifen? Ich glaube, für die Anonymisierungsfunktion ist das im Grunde offensichtlich, dass das einen Nutzen hat. Dass das auch gerechtfertigt ist, das zu haben. Also durchaus auch für Whistleblowing und dergleichen. Ich finde es ein bisschen schwieriger zu sagen, das müssten auch Hidden Services sein. Durch die Verwendung von Hidden Services

hat man im Prinzip schon eine zusätzliche Sicherheit. Die ist aber technisch gesehen auch nicht so dramatisch. Ich kann ja auch durch Tor zum Beispiel auf die normale Webseite, die Clearnet-Webseite der Süddeutschen Zeitung zugreifen. Es gibt eine ganze Reihe von Redaktionen, die solche Secure Drops betreiben. Ich kann ja also, wie gesagt, durch das Tor-Netzwerk einfach darauf zugreifen und dann auch noch was hochladen. Die einzige zusätzliche Sicherheit, die mir es gäbe, den Hidden Service der Süddeutschen Zeitung zu verwenden, wäre, dass die Exit-Node nicht sich dort einmischen könnte. Das heißt, die Exit-Node kann dann, wenn ich den Hidden Service verwende, weil es ja da keine Exit-Node gibt, die kann dann also nicht versuchen, in die verschlüsselte Verbindung irgendwie einzubrechen. Dem kann ich natürlich begegnen, indem ich das Zertifikat mir nochmal anschaue und so weiter und so fort. Also ich finde es schwierig zu sagen, dass wir für diese schon fast hypothetische zusätzliche Sicherheit diese Hidden Services brauchen. Also ich glaube, es reicht völlig aus, zu sagen, ich greife dann auf die normale Webseite der Süddeutschen oder eines anderen Presseerzeugnisses zu und kontaktiere auf die Weise die Redaktion. Und die bieten auch verschiedene Sachen an. Also, man kann das auch per E-Mail oder Messenger-Dienste und dergleichen. Vielleicht wird dieses Secure Drop auch betrieben, weil es eine bekannte Software ist, die einen Sicherheitsaudit hat und die von sich aus schon erzwingt, dass es eine Onion-Adresse ist. Aber das ist ja dann auch eine Designentscheidung der Software. Das ist dann nicht irgendwie eine demokratietheoretische Frage, sondern Software-Engineering-Frage, dass man das so gemacht hat. Und das könnte man sicherlich auch anders lösen. Und ich tue mich schon schwer zu sagen, das ist jetzt der Grund, warum wir diese Hidden Services toll finden sollten oder diese Technik positiv bewerten sollten, wenn man gleichzeitig überlegt, dass 2021 auf solchen Marktplätzen, soweit man das sehen konnte, über zwei Milliarden Dollar umgesetzt wurden und davon 1,8 Milliarden Dollar in Drogen. Nun muss man jetzt nicht jede Drogenpolitik gut finden, aber ich glaube, es ist trotzdem keine gute Idee, sich irgendwelche Substanzen zu verabreichen, die man irgendwo im Darknet auf irgendwelchen Webseiten gefunden hat. Gäbe es da ein Reputationssystem oder nicht? Ich halte das für keine gute Strategie und auch etwas, was wir aus guten Gründen nicht für, ich sage mal, demokratietheoretisch geboten halten sollten.

[mg]: Gibt es denn trotzdem Verteidiger, auch dieser Onion Services oder Hidden Services, die demokratietheoretisch argumentieren? Oder ist das schon so, dass sich alle darauf einigen können: Dieser schlechte Ruf des Darknets hat vor allem mit den Hidden Services zu tun?

[Denker]: Ich glaube, das sind zwei Fragen. Die zweite Frage: Ich glaube, man kann sich schon darauf einigen, dass der schlechte Ruf sehr viel mit den Hidden Services zu tun hat. Wenn diese Hidden Services nicht wären, dann würde man sagen: Okay, das ist ein Anonymisierungsdienst, und dann kann man vielleicht immerhin noch überlegen, dass da irgendwie Sachen problematisch sind. Aber die Diskussion rotiert ja immer um diese Darknet-Marktplätze herum. Das heißt natürlich nicht – das ist dann der erste Teil dieser Doppelfrage –, dass es nicht auch Verteidiger geben würde. Und natürlich ist das das Tor-Netz selbst, das ist die gesamte Datenschutz-Community, würde ich mal sagen. Also, es ist auch sehr viel Mythos. Ich mache mich jetzt unbeliebt, wenn ich das so formuliere, aber ich glaube, es ist sehr viel Mythos daran, zu sagen: Das ist etwas, was wir unbedingt brauchen, um Überwachungen und vielleicht totalitäre Tendenzen im Netz zu verhindern. Da mache ich mir über andere Angebote viel mehr

Sorgen als die Frage: Ist nun ein Secure Drop übers Clearnet erreichbar oder nur übers Darknet erreichbar?

[pgg]: Wie stehen denn rechtsstaatliche Behörden zum Tor-Netzwerk?

[Denker]: Also es gibt ja in diesen Snowden-Leaks, diesen berühmten Slide, in dem die NSA gesagt hat, dass das Tor-Netzwerk nerfe. Also, es ist schon schwierig, da Ermittlungen durchzuführen. Es ist aber ganz offensichtlich so, dass das gemacht werden muss. Es gibt eindeutig illegale Angebote, die gar keine Frage sind. Es gibt ja zum Beispiel die ZIT, also die Zentralstelle zur Bekämpfung der Internetkriminalität bei der Generalstaatsanwaltschaft in Frankfurt. Die halt einen großen Teil ihrer Zeit damit verbringt, diesen Angeboten auf die Schliche zu kommen. Und das ist schwierig. Also man hört immer mal, man hätte gerne zum Beispiel zusätzliche rechtliche Regelungen, wie zum Beispiel das Anbieten von Hidden Services selbst schon zu pönalisieren. Das ist es, soweit ich da jetzt informiert bin, zurzeit nicht. Ich glaube, das ist nicht durchgegangen. Da müsste ich jetzt aber ehrlich gesagt nochmal nachgucken. Ich weiß aber, dass es diese Diskussion gab. Und man ist natürlich bei Strafverfolgungsbehörden nie glücklich über alles, was irgendwelche Recherchesachen erschwert. Also man ist ja schon nicht glücklich darüber, dass es Datenschutz gibt – manchmal hat man das Gefühl. Oder dass die Vorratsdatenspeicherung nicht voll umgesetzt ist bzw. wahrscheinlich auch wieder ganz oberrechtlich da durchfallen wird mit allem Drum und Dran. Darüber ist man ja auch nicht glücklich. Also, man möchte ja gerne Spuren haben, die man auswerten kann. Und da ist jede Technik, die das Auswerten von Spuren irgendwie erschwert, natürlich nicht gerade beliebt.

[mg]: Wie wäre das denn überhaupt möglich, wenn man jetzt sagt, man setzt sich politisch das Ziel, ich sage jetzt mal, das Darknet abzuschaffen, Hidden Services abzuschaffen? Was für Maßnahmen wären das denn dann? Müssten das technische auch sein oder wären das nur juristische? Und wäre das überhaupt möglich?

[Denker]: Ich glaube, es wäre nicht möglich. Also China versucht, den Zugriff auf Tor massiv zu behindern. Das ist so ein bisschen Katz-und-Maus-Spiel. Also diese Great Firewall of China, wie man es so gerne nennt, die haben auch Mechanismen, um Tor Relays, die sie noch nicht kennen, zu identifizieren, also sogenannte Bridges. Das sind einfach nur Tor Relays, die nicht in so einer offiziellen Liste drinstehen. Wenn also z.B. jemand aus China heraus sich auf so eine Bridge connectet, dann fängt automatisch so ein System an zu prüfen: Ist das ein Tor Relay? Und wenn ja, dann wird das auch noch geblockt. Also, es ist so ein Katz-und-Maus-Spiel. Und es ist jetzt, glaube ich, schon so, dass die chinesischen Behörden damit so am besten abschneiden, was das Blockieren von Tor angeht. Aber auch da ist es sicherlich nicht perfekt. Es ist z.B. auch möglich, Verbindungen zu Tor in anderen Verbindungen wieder zu verstecken. Das hat dann, wenn man es so kurz auf den Punkt bringen möchte, zur Folge: Wenn man es wirklich verhindern möchte, dass Leute verschlüsselt über das Tor-Netzwerk kommunizieren, dann muss man verhindern, dass Leute verschlüsselt kommunizieren. Und das können wir nicht wollen. Das würde nämlich den gesamten E-Commerce, die Marktplätze, das Online-Banking, das würde das komplett kaputt machen, weil alles im Klartext mitlesbar wäre. Das heißt, der technische Eingriff wäre schon so riesig. Wir würden so viele andere Sachen kaputtmachen, dass ein Abschalten vermutlich nicht möglich ist. Man kann natürlich, wenn man das unbedingt möchte, den Verfolgungsdruck versuchen zu erhöhen. Ich vermute, dann wird es auch Ausweichbewegungen geben.

Es wird auch sicherlich nicht so sein, dass es in allen Staaten gleichermaßen zu entsprechendem Verfolgungsdruck kommt. Also auch das ist dann auch wieder so ein kompliziertes Thema. Also, ich halte das nicht für realistisch. Also kurz: Die Antwort ist nein. Ich glaube nicht, dass es möglich ist, das technisch abzuschalten, und rechtlich: Gut, man kann es rechtlich in dem Sinne nicht abschalten. Man kann halt einfach nur den Verfolgungsdruck erhöhen.

[pgg]: Die ganze Thematik ist ja schon ziemlich kompliziert. Also wenn man es dann gewöhnt ist, ist es wahrscheinlich wie ein Stück Netznutzung und nicht so lernbedürftig jetzt auch für Nicht-InformatikerInnen, wie es jetzt im Moment klingt, wenn wir darüber reden. Aber wenn es denn so ist, dass neben dem Internet eben auch das Darknet einfach ein Faktum ist, es gibt das, wichtige Stücke Welt spielen sich da auch ab, müsste man mehr darüber wissen, auch öffentlich mehr erklären, was das ist und wie es funktioniert. Vielleicht sogar im Schulunterricht deutlich machen: Es gibt Clearnet, es gibt Darknet, es gibt noch weitere Teile des Netzes – oder gibt es da ohnehin, ich sag mal, umlaufendes Wissen, gerade bei jüngeren Leuten, und man braucht es nicht eigens zu erklären, beizubringen?

[Denker]: Das ist eine schwierige Frage, mal ganz ehrlich gesagt, denn ich sehe das schon so ein bisschen zweischneidig. Also ich weiß nicht, ob es wirklich gut ist, Leuten beizubringen, wie man ins Darknet kommt und wie man das verwendet. Andererseits: Das ist nicht schwer. Also das kriegt man sicherlich auch mal selbst zusammengegoogelt. Es gibt YouTube-Tutorials und dergleichen mehr. Man findet sich da rein, wenn man möchte. Ich würde es vielleicht so sehen: Man geht ja vielleicht mit Schulklassen auch nicht auf eine Exkursion durch das sprichwörtliche Bahnhofsviertel. Und trotzdem warnt man halt Schüler:innen vor Drogen, Verbrechen, Menschenhandel und so fort. Also man informiert ja, dass es das gibt, aber man geht nicht hin. Und das ist vielleicht so ein Punkt. Also naja, das Wort Medienkompetenz, da sträuben sich mir immer alle Nackenhaare. Aber im Prinzip ist es so was. Also die aufmerksam machen, dass es eben auch kriminelle Angebote gibt, betrügerische Angebote gibt, dass man extrem kritisch sein muss. Auf welchen Webseiten man irgendwelche Zahlungen tätigt und dergleichen mehr. Deswegen, ich bin gar nicht so ein Fan davon zu sagen, das müssen jetzt irgendwie alle da die komplette Aufklärungsschiene fahren. Ich glaube, auf so einem High-Level zu wissen: Okay, es gibt da so Bereiche, die, ich sag mal, heikel sind, das sicher, aber ich würde da jetzt nicht allzu viel Schulungsaufwand reinstecken wollen.

[pgg]: Und die Sache scheint sich ja auch ziemlich schnell zu verändern. Also wahrscheinlich sind Erklärungen, die zwei, drei Jahre alt sind, auch gar nicht mehr passend?

[Denker]: Also technisch verändert es sich nicht so schnell. Das heißt, technisch gesehen sind die Erklärungen schon längerfristig okay. Also es gab eine Änderung an diesem Onion-Dienstprotokoll, Version zwei auf Version drei. Da hat sich die Schlüssellänge geändert. Aber das ist jetzt nicht irgendwie so wichtig, dass man da jetzt neu schulen muss. Das sieht die Anwender:in, wenn sie den Tor-Bowser benutzt, nur dadurch, dass die Adressen länger sind. Inhaltlich ist es halt relativ schnell. Aber da stellt sich für mich die Frage: Muss man den Leuten jetzt sagen, wie gerade der aktuelle Drogenmarktplatz heißt? Und ich meine, ich habe jetzt Namen genannt, aber das ist auch leicht zu googeln. Aber es gibt sicherlich auch andere Sachen, die nicht irgendwie leicht zu finden sind. Und muss man die dann darüber informieren und

dergleichen? Ja, aber da ist das natürlich schon so: Es fluktuiert, die Marktplätze, weil sie halt teilweise einfach abgeschaltet werden von Behörden, wenn sie dann mal einen Ermittlungserfolg hatten. Und auch, wie gesagt, andere Dienste, die auch einfach einschlafen, da vielleicht technisch kaputtgehen. Und dann hat die Person, die das angeboten hat, keine Lust, das zu reparieren. Oder beschäftigt sich jetzt mit etwas anderem oder merkt es vielleicht nicht mal. Und von daher ist es einfach nicht so ein gut gepflegtes Internet. Das Internet ist auch nicht gut gepflegt. Aber es ist trotzdem noch mal ein ganz anderes Kaliber. Es macht übrigens auch nicht sonderlich viel Spaß, es zu benutzen. Nicht nur, weil die Dienste nicht erreichbar sind, sondern auch, weil die Latenz sehr hoch ist. Also, wir sind es ja mittlerweile gewohnt, wir klicken auf einen Link. Und im Grunde im Wimpernschlag ist die Webseite dann da oder es passiert zumindest irgendwas. Wir reden ja über Latenzen im Millisekundenbereich, im Clearnet. Und im Darknet, also nicht nur Hidden-Services, sondern auch wenn wir über das Tor-Netzwerk auf irgendwas zugreifen, sehen wir also Latenzen, die dann durchaus auch mal im Sekundenbereich liegen können. Und das macht es einfach extrem langsam. Und wenn man wirklich sicher gehen möchte, dann schaltet man aktive Inhalte komplett ab im Tor-Browser. Also, da gibt es auch so eine Einstellung, so Standard-Sicherheit und erhöhte Sicherheit und dergleichen. Und dann wird halt so etwas wie JavaScript und dergleichen ausgeschaltet. Und dann fühlt sich das, was man sieht, ganz schnell an wie so das Internet der 1990er Jahre. Und gut, einige werden sich daran erinnern. Das war nicht so schön polished und shiny, wie es heute ist. Hat auch einen Charme. Ja, also es hat einen Retro-Charme, den das dann entwickelt. Das ist ohne Frage so.

[mg]: Das eine ist ja so ein bisschen das, was Sie jetzt als das Bahnhofsviertel des Internets bezeichnet haben. Es ist nicht so gepflegt, es ist irgendwie gefährlich. Aber dieser Punkt, dass bestimmte emanzipatorische Bewegungen sich da formieren oder da eine Möglichkeit sehen, sich zu entwickeln, das wird ja immer wieder angebracht. Meinungsfreiheit ist ein Stichwort, das auch manchmal genannt wird, wenn das Darknet verteidigt wird. Wie soll das anonyme Kommunizieren im Darknet Meinungsfreiheit aus Sicht der Verteidiger:innen fördern?

[Denker]: Ja, also da geht es ja um Attribution. Also, es geht um die Frage: Wer hat eine Äußerung getätigt? Und wenn ich über Tor entweder anonymisierend oder über vielleicht einen Hidden Service Social Media da ein Posting hinterlasse und jetzt nicht sage, wer ich bin, und vielleicht nicht irgendwie ein Bild poste, wo noch irgendwelche Metadaten drin sind, dann ist ja das, was ich dort hingeschrieben habe, mir nicht zuzuordnen. Es stellt sich natürlich die Frage: Was könnte ich denn reinschreiben wollen, was ich im Clearnet nicht irgendwo hinschreibe? Also, was weiß ich, auf Telegram oder meinetwegen auch auf Facebook oder so. Ich meine, es ist ja eine Diskussion, die wir seit Jahren haben, dass diese Plattformen zu zögerlich sind, manche Inhalte zu löschen oder Informationen über Leute, die, was weiß ich, volksverhetzende Inhalte gepostet haben, weiterzugeben. Also man muss sozusagen schon die Hypothese haben, dass die Meinungsfreiheit im Clearnet massiv gefährdet ist, um zu sagen: Tor kann das verteidigen. Ich bin vielleicht zu konservativ, ich weiß es nicht, zu sagen: Ich sehe das nicht. Also, natürlich haben wir keine grenzenlose Meinungsfreiheit in Deutschland. Es gibt Schranken, das ist auch okay, finde ich. Also, das ist jetzt meine Bewertung, das mögen andere Leute anders sehen. Und ich sehe jetzt nicht, warum ich jetzt das Tor-Netz verteidigen sollte, um das, was rechtlich hier nicht möglich ist, also im Clearnet nicht möglich ist, dort umzusetzen. Das mögen andere anders sehen. Was diese Emanzipationsfrage angeht: Ich muss sagen, ich glaube nicht daran. Also

Emanzipationen sind ja auch politische Prozesse. Die haben immer sehr, sehr viel damit zu tun, auch, ich sage mal, Gesicht zu zeigen, offen zu sein, auch politischen Druck zu machen. Und das gelingt nicht, indem ich auf einem sozialen Netzwerk im Darknet irgendwas poste. Das gelingt nicht, indem ich einen Blog im Darknet betreibe. Also das ist technisch leicht, also dann kann ich da meine persönlichen Meinungen und dergleichen hinschreiben. Das bringt allein schon deshalb nichts, weil ich vermute, es gibt relativ wenig Leute, die darauf aufmerksam werden. Das müsste ja erstmal gefunden werden und da müssen Leute interessiert sein und so weiter und so fort. Und es hat, ich glaube, das ist schon eine Erfahrung, die wir so aus dem 20. Jahrhundert noch mitnehmen können (zweite Hälfte), viele Emanzipationsprozesse haben auch immer was damit zu tun gehabt, dass Leute auch Gesicht gezeigt haben. Also ich denke da immer an dieses Sterncover da 'Ich habe abgetrieben', wo einfach Gesichter zu sehen waren. Das ist ein politisches Statement. Und das erzeugt man nicht, indem man irgendeinen Blog irgendwo anlegt und dann anonym reinschreibt: Ich habe abgetrieben. Das ist einfach keine politische Aussage in dem Sinne. Und daher kaufe ich diese ganzen Emanzipationsnarrative nicht. Andersrum natürlich: Irgendwelche Foren, wo sich Leute über stigmatisierte Krankheiten austauschen wollen, weil sie sich gerade nicht emanzipieren. Also sie wollen nicht in den politischen Prozess einsteigen, sondern sie wollen sich nur austauschen. Da sehe ich da schon eher einen Nutzen darin. Wobei ich auch glaube, dass sich über Krankheiten austauschen ist im Zweifelsfall auch nicht pönalisiert. Da kann man dann auch Clearnet-Foren anonymisiert benutzen. Und ich halte es für sehr, sehr überschaubar, zu sagen, ich habe hier etwas, was ich jetzt – ich bleibe jetzt beim Krankheitsbild – was ich für eine Krankheit halte, was aber irgendwie rechtlich problematisch ist. Und dann möchte ich darüber reden. Also ja, man kann sicherlich solche Extrembeispiele finden und mit diesen Extrembeispielen oder sehr seltenen Beispielen auch argumentieren. Aber es ist dann eben trotzdem nur ein verschwindend geringer Anteil gegenüber 1,8 Milliarden Dollar Drogenmarktplatz in 2021.

[pgg]: Privatheit einer Aussage, die sich schützen möchte, ist also möglicherweise das Gegenteil einer politischen Meinung, die vielleicht gerade davon lebt, sich auch zu exponieren und die entsprechenden politischen Bürgerrechte namentlich in Anspruch zu nehmen?

[Denker]: Ganz genau. Also wenn wir uns das überlegen, z.B. die queere Bewegung, damals hieß es dann Schwulen-Lesben-Bewegung, die haben viel auch einfach dadurch erreicht, dass die Leute auf der Straße gestanden haben und sich zu erkennen gegeben haben mit ihren Demonstrationen/Paraden. Das passiert nicht, indem man dafür sorgt, dass ich ein soziales Netzwerk für Schwule benutzen kann, wo ich datenschutztechnisch so sicher bin, dass das garantiert nie jemand mitkriegt. Also, das kann ich wollen, das kann völlig legitim sein. Nur das ist eben keine politische Position, das ist kein politischer Prozess. Das ist dann einfach nur Privatheit. Eine Privatheit, die nur in so einem ganz negativen Sinne noch politisch ist.

[mg]: Können wir das so, ich sage mal, so in einzelnen Rechtssystemen betrachten oder müssen wir das Darknet nicht auch dann globaler sehen? Also das, was wir jetzt hier besprechen, gilt ja für freie Gesellschaften, in denen es dann eben auch entsprechende Sicherungen von Grundrechten gibt, die dann eben auch der Meinungsäußerungen auf der Straße den entsprechenden Schutzstatus geben. Das ist ja nicht überall so. Also, müssen wir sozusagen das Darknet für Deutschland anders

besprechen als das Darknet für China zum Beispiel, wie wir es schon mal angedeutet hatten?

[Denker]: Ja, man kann sich auf so eine Position stellen. Ich glaube, trotzdem können auch die chinesischen Dissidenten oder die iranischen Dissidenten die Dienste zum Beispiel im europäischen Clearnet benutzen. Also das ist ein Argument für das Tor-Netz selbst, für diese Anonymisierungsfunktion, sich darüber zu koordinieren, auch ein Whistleblowing zu betreiben oder Berichte weiterzugeben. Das ist aber kein Argument, aus meiner Sicht, für die Hidden Services, auch wenn es oft so verkauft wird.

[mg]: Das heißt, das wäre sowas, dass man wirklich als Botschaft mitnehmen kann, dass man diese Hidden Services als was betrachtet, was man absondern könnte, auch aus der Logik dieses anonymen Internets, und damit hätte man ein anderes Darknet. Man hätte vielleicht eins, in dem diese Gleichstellung von Darknet und Kriminalität aufgeweicht wäre?

[Denker]: Ja, also wenn wir Darknet als das betrachten, was diese Hidden Services darstellen, also einen ganz engen Darknet-Begriff nehmen, dann wäre das Darknet in dem Sinne dann natürlich schon weg. Es ist halt technisch nicht irgendwie möglich, zu sagen: Okay, wir wollen das jetzt abschaffen. Die einzige Möglichkeit wäre natürlich, dass das Tor-Projekt selber diese Funktion entfernt, aber es ist eine freie Software, also dann werden andere Leute die Funktion wieder einführen, ein anderes Netz aufbauen. Also die Katze ist sozusagen da aus dem Sack. Das wird man nicht einfach wegkriegen. Aber in dem Bereich der Anonymisierungsfunktion stellt sich die Frage, glaube ich, nicht wirklich. Das ist schon ganz gut, dass wir das haben. Es gibt Leute, die haben auch legitime Interessen, irgendwo anonym zu kommunizieren. Aber man muss vielleicht auch die Kirche im Dorf lassen. Also die Hypothese: Irgendwie global hätten wir es nur noch mit totalitären Staaten zu tun und es gibt da irgendwie so eine Dissidenzbewegung und für die brauchen wir dann diese Hidden Services usw. Das hat schon sehr was von Hollywood. Also da sind wir zum Glück sehr weit vorn entfernt und es wird sicherlich auch auf die nächsten Jahrzehnte und hoffentlich noch sehr, sehr viel länger sehr, sehr viele demokratische Rechtsstaaten geben, die auch bereit sind, Dienste zu hosten, die dann vielleicht in anderen Ländern nicht gerne gesehen werden oder verfolgt werden.

[mg]: Gibt es denn entsprechende Debatten innerhalb der Netzcommunity, die sich im Darknet bewegt oder die das versteht? Oder ist das Mainstream, die Hidden Services einzufordern und zu verteidigen?

[Denker]: Also mir sind nicht alle Diskussionen bekannt. Das, was ich so mitkriege, Konferenzvorträge und dergleichen, ist man sich schon sehr einig, dass das eine Technik ist, die man will, die man positiv findet.

[pgg]: Frage Forschung zu diesen Themen: Wird da viel geforscht oder ist das eine ganz kleine Community?

[Denker]: Also man könnte sagen, es ist eine überschaubar große Community. Das heißt aber nicht, dass wenig Forschung stattfindet. Also ich habe nicht das Gefühl, da ist noch eine riesengroße Forschungslücke. Das heißt jetzt nicht, dass es nicht noch Fragen gibt, die interessant sind. Aber es ist jetzt nicht so, dass das irgendwie groß terra incognita ist oder dergleichen. Es finden Forschungsprojekte statt, aber ich

glaube, es ist in angemessenem Umfang, wenn man sich überlegt, wie viel dort stattfindet oder wie groß das Darknet ist und dass wir andere Phänomene haben, die uns vielleicht viel mehr auf den Nägeln brennt. Also ich finde eine inhaltsorientierte Forschung, da spreche ich jetzt vielleicht natürlich irgendwie aus eigenem Interesse auch ein Stück weit heraus, die sich zum Beispiel mit politischem Extremismus im Netz befasst, interessanter als die Frage: Welche Kommunikationstechnik wird eingesetzt? Also die Forschung der Inhalte ist, glaube ich, noch viel heikler und viel interessanter und unterforscht in vielen Ecken als die Erforschung der technischen Strukturen.

[Der Abspann mit Musik beginnt.]

[mg]: Und damit ist dieses Digitalgespräch zu Ende. Vielen Dank an Kai Denker von der Technischen Universität Darmstadt für das spannende Gespräch und die interessanten Einblicke. Viele Grüße und vielen Dank auch Ihnen, liebe Zuhörerinnen und Zuhörer, für Ihr Interesse und die Aufmerksamkeit. Wir verabschieden uns jetzt in die Sommerpause und melden uns wieder in sechs Wochen, das heißt am 16. August. Wenn Sie mögen, hören wir uns dann wieder zur nächsten Folge des Digitalgesprächs, dem Podcast von ZEVEDI, dem Zentrum verantwortungsbewusste Digitalisierung.