NZZ LIBRO E-Book

Die Schattenwelt des Internets

Otto Hostettler

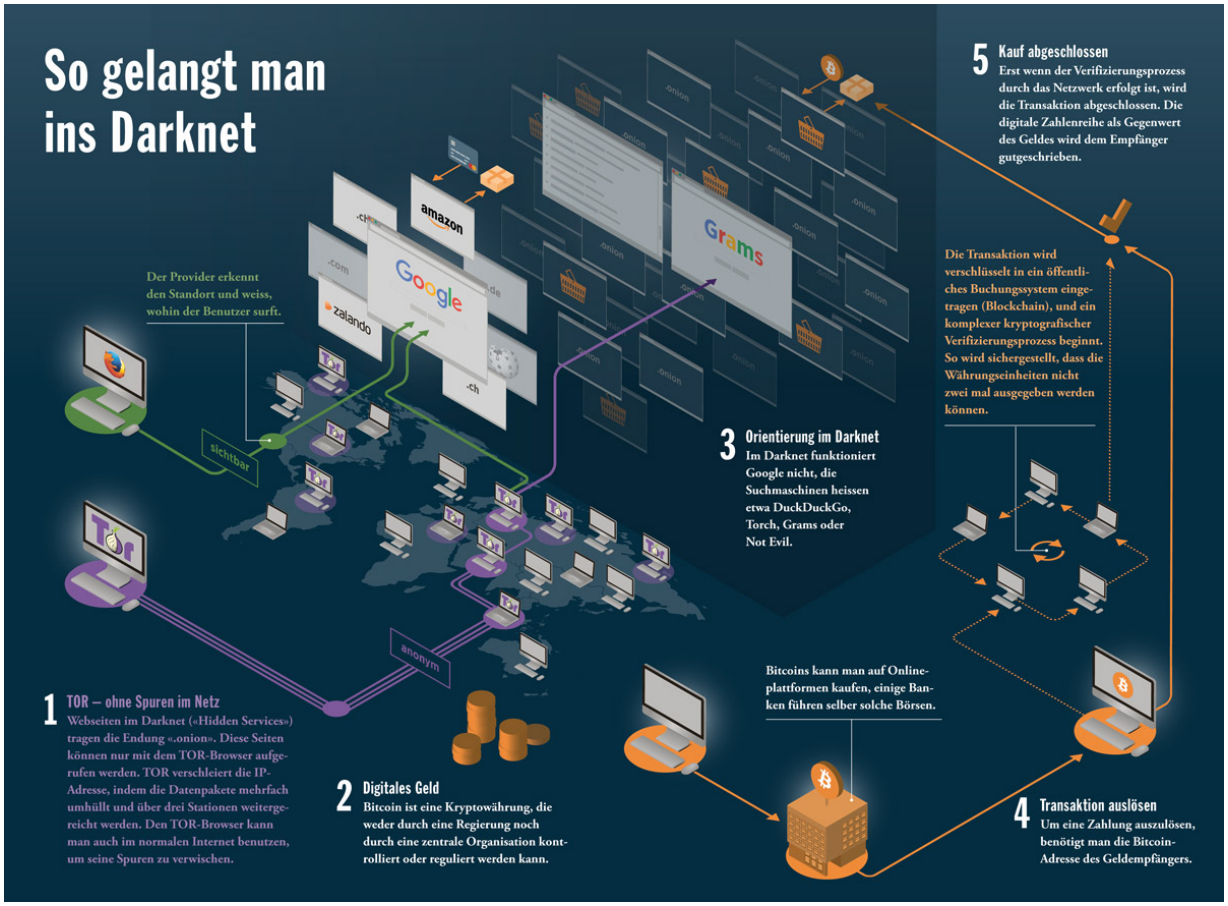
NZZ LIBRO Frankfurter Allgemeine Buch

NZZ LIBRO E-Book

Die Schattenwelt des Internets

Otto Hostettler

NZZ LIBRO Frankfurter Allgemeine Buch


So gelangt man ins Darknet
5 Kauf abgeschlossen
Erst wenn der Verifizierungsprozess durch das Netzwerk erfolgt ist, wird die Transaktion abgeschlossen. Die digitale Zahlenreihe als Gegenwert des Geldes wird dem Empfänger gutgeschrieben.
Die Transaktion wird verschlüsselt in ein öffentliches Buchungssystem eingetragen (Blockchain), und ein komplexer kryptografischer Verifizierungsprozess beginnt. So wird sichergestellt, dass die Währungseinheiten nicht zwei mal ausgegeben werden können.
Der Provider erkennt den Standort und weiss, wohin der Benutzer surft.
sichtbar
anonym
3 Orientierung im Darknet
Im Darknet funktioniert Google nicht, die Suchmaschinen heissen etwa DuckDuckGo, Torch, Grams oder Not Evil.
1 TOR – ohne Spuren im Netz
Webseiten im Darknet («Hidden Services») tragen die Endung «.onion». Diese Seiten können nur mit dem TOR-Browser aufgerufen werden. TOR verschleiert die IP-Adresse, indem die Datenpakete mehrfach umhüllt und über drei Stationen weitergereicht werden. Den TOR-Browser kann man auch im normalen Internet benutzen, um seine Spuren zu verwischen.
2 Digitales Geld
Bitcoin ist eine Kryptowährung, die weder durch eine Regierung noch durch eine zentrale Organisation kontrolliert oder reguliert werden kann.
Bitcoins kann man auf Onlineplattformen kaufen, einige Banken führen selber solche Börsen.
4 Transaktion auslösen
Um eine Zahlung auszulösen, benötigt man die Bitcoin-Adresse des Geldempfängers.

Otto Hostettler

DARKNET

Die Schattenwelt des Internets

NZZ LIBRO Frankfurter Allgemeine Buch

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Der Text des E-Books folgt der gedruckten 1. Auflage 2017 (ISBN 978-3-03810-257-1)

Lektorat: Karin Schneuwly, Text Praxis, Zürich
Titelgestaltung: TGG Hafen Senn Stieger, St. Gallen
Datenkonvertierung: CPI books GmbH, Leck

ISBN E-Book 978-3-03810-302-8
www.nzz-libro.ch
NZZ Libro ist ein Imprint der Neuen Zürcher Zeitung

Gedruckte Lizenzausgabe für Deutschland und Österreich:
Frankfurter Allgemeine Buch

Frankfurter Societäts-Medien GmbH
Frankenallee 71–81
D-60327 Frankfurt am Main
Geschäftsführung: Oliver Rohloff
ISBN 978-3-95601-201-3
www.fazbuch.ch

Inhaltsverzeichnis

Vorwort

Der Begriff «Darknet» taucht immer mal wieder in den Medien auf. In letzter Zeit gerade im Zusammenhang mit schweren Straftaten. Als gewichtiges Beispiel ist die Amoktat in München von Juli 2016 zu nennen. Der Täter soll seine Waffe im Darknet bezogen haben. Das Darknet wird aber auch bei illegalen Drogen- und Medikamentenbezügen oder der Verbreitung von kinderpornografischen Inhalten erwähnt. Prominent diskutiert wurde auch der Fall Maximilian S. («Shiny Flakes»), der in Deutschland im November 2015 verurteilt wurde – wegen Handel mit Betäubungsmitteln via Darknet.

Als Strafverteidiger und Konsulent von Unternehmen stelle ich fest, dass es für eine erfolgreiche Mandatsausübung essenziell ist, aktuelle gesellschaftliche und technische Entwicklungen zu kennen. Gerade im Bereich des Internets ist dies von besonderer Relevanz. Auf dem Gebiet Cybercrime hat in den letzten Jahren vor allem die Entwicklung im Bereich Datendiebstahl für Schlagzeilen gesorgt. Die Strafverfolgungsbehörden mussten darauf reagieren. Es galt, diese neuere Erscheinungsform zu erfassen und Methodik und Prozesse daran anzupassen. Eine neue Herausforderung ist nun das Darknet; dessen Inhalt und Funktionsweise ist für viele Personen schlichtweg nicht fassbar und lediglich ein dunkler Fleck auf der Landkarte. Dies gilt nicht nur für den durchschnittlichen Internetnutzer, sondern teilweise auch für Strafverfolger.

So bemerkten Technikexperten, dass diesbezüglich bei Staatsanwälten die Kluft zwischen dem erforderlichen und tatsächlichen Wissen immer grösser wird. Auf verhältnismässig kostenintensive Weiterbildungen wird bei Behörden vermehrt

verzichtet. Es besteht zwar das Bewusstsein um die zunehmende Wichtigkeit des Darknets als Mittel zu kriminellen Handlungen. Dennoch übersteigen damit zusammenhängende Strafverfahren häufig die Kapazitäten und Möglichkeiten der Behörden. Aus Sicht der Strafverfolger kommen erschwerend die tatsächlichen Umstände hinzu, die im Bereich der Internetkriminalität ohnehin existieren. Dazu gehören die Anonymisierung von Spuren, verschlüsselte Kommunikationsmöglichkeiten, internationale Zahlungsströme und Kryptowährungen. Entscheidend ist aber auch die Qualifikation der Ermittler und Staatsanwälte. Die Folge ist eine verzögerte Reaktion auf Straftaten, die gerade mittels Darknet begangen werden. Wenn solche Taten überhaupt erkannt werden.

Nun schildert Otto Hostettler im vorliegenden Buch *Darknet – die Schattenwelt des Internets* eindrücklich und faktenbasiert den Mechanismus und die Wirkungsweise des Darknets. Herausragend macht dieses Werk, dass der Autor monatelang eigenständige Feldforschungen im Darknet tätigte und Anbieter und Kenner der Branche dazu interviewte. Er ging der Materie auf den Grund. Auch fühlte er Behördenexponenten auf den Zahn. Er legt seine Erkenntnisse schonungslos offen und zeigt Möglichkeiten und Grenzen der Strafverfolger. Die Ergebnisse seiner Ermittlungen stützt er breit ab. In diesem Sinne ist das vorliegende Werk ein einzigartiger Beitrag zur Aufklärung über Umfang und Hintergründe des Darknets.

Schätzungen zufolge ist die Zahl der Internetseiten, die Google *nicht* findet, x-fach grösser als jene Anzahl Seiten, die von der Suchmaschine gefunden werden. Viele nehmen diese riesige, teils gar nicht sichtbare Welt des Internets – und damit auch das Darknet – als rechtsfreien Raum wahr. Doch die Gesetze gelten auch dort. Faktisch stehen Ermittler aber bei der Durchsetzung der Gesetze vor den erwähnten Problemen. Diese Schwachstellen

im Dispositiv der Behörden werden ausgenutzt. Deshalb ist es wichtig zu wissen, was das Darknet beinhaltet und welche Bedeutung dieses anonyme Netzwerk für die Entwicklung der Kriminalität hat. Die Gesellschaft kann sich diesem Thema nicht verschliessen, sondern sollte die Herausforderungen dieser «Schattenwelt des Internets» breit diskutieren. Das vorliegende Werk bietet eine hervorragende Grundlage dazu, öffnet die Augen und lässt aufhorchen. Besten Dank dem Autor für die höchst interessante und anregende Arbeit.

Cornel Borbély

Dr. iur. Cornel Borbély; Rechtsanwalt, Dozent für Wirtschaftsstrafrecht und Strafprozessrecht

1 Darknet, Cybercrime und Ermittler-PR: Einleitung

Wenn es am Morgen hell wird, macht er Feierabend. Dann hat er alle Cannabis-Bestellungen abgearbeitet. Das Kraut abgewogen, in Plastikbeutel verschweisst, in DVD-Hüllen gelegt, in luftgepolsterte Kuverts verpackt, adressiert und frankiert. Das Ende eines ganz normalen Arbeitstags im Leben von «Edelweiss», einem Schweizer Ende 30, der im grossen Stil Cannabis anbaut und vertreibt – über das Internet. Genauer gesagt: über das sogenannte Darknet. Nicht einmal sein nahes Umfeld weiss von seinem Online-Drogenhandel. Tagsüber reist «Edelweiss» per Zug mit einer Tasche voller Kuverts durch die Schweiz und gibt sie, um seine Spuren zu verwischen, auf allen möglichen Poststellen auf. Routiniert und unauffällig.

«Edelweiss» handelt nicht alleine. Ein Kumpel pflegt den «Garten», die Indoor-Hanfplantage. Ein anderer Kollege übernimmt Sonderaufgaben. Er zapfte den Strom vom öffentlichen Netz und installierte einen neuen Hausanschluss. Der massive Energiebedarf der Anlage wäre sonst dem lokalen Elektrizitätswerk aufgefallen, und die Polizei hätte dem Treiben vermutlich längst ein Ende gesetzt. Doch «Edelweiss» überliess nichts dem Zufall. Er selber, der gelegentlich wieder in der Gastronomie arbeitet, ist für den Verkauf und den Vertrieb der Hanfblüten zuständig. Und so wachsen in einem Keller an einem geheimen Ort in der Schweiz um die 2000 Pflanzen dem künstlichen Licht entgegen. Pro Erntezyklus gewinnen «Edelweiss» und sein «Gärtner» zehn Kilo Marihuana.

Bis vor einem Jahr verkaufte er das selbst gezogene Kraut ausschliesslich direkt an Freunde und Arbeitskollegen. Jetzt hat er einen neuen Absatzkanal gefunden: die anonymen Shops im

Darknet. Noch immer vertreibt er zwar den grössten Teil seines Krauts persönlich an seine Freunde, wie früher. Doch im Netz wartet eine neue Käuferschaft. Regional, national, international. Diese Kunden sind anonym, aber sie bezahlen zuverlässig. Gleich bei der Bestellung. Ist die Lieferung erfolgt, geben viele von ihnen eine Bewertung für seinen Service ab. Und manche machen damit Werbung für die nächsten Käufer. Innerhalb von etwas mehr als einem Jahr verarbeitete er ziemlich genau 1000 Bestellungen. Und erreichte einen Umsatz von gut 100 000 Franken. Es hätte gut und gern noch etwas mehr werden können. Aber letzten Herbst ist eine ganze Ernte ausgefallen, weil der «Garten» ein Wochenende lang keinen Strom hatte. Bauarbeiter hatten auf der Strasse vor dem Gebäude irrtümlicherweise die Stromleitung zertrennt. «Edelweiss» konnte nicht einfach das Elektrizitätswerk anrufen. Berufsrisiko eines Drogenhändlers (s. a. Kapitel 10).

«Edelweiss» ist Teil eines Phänomens: des Darknets. Innerhalb weniger Jahre ist dort eine schier grenzenlose Parallelwirtschaft entstanden. Um diese verborgene Seite des Internets geht es in diesem Buch. Fast zwei Jahre lang war ich selber im Darknet unterwegs, habe neun anonyme Marktplätze beobachtet, analysiert und bin selber als Käufer aktiv geworden. Meine Erkenntnisse sind zuerst in die Abschlussarbeit für den Masterlehrgang Economie Crime Investigation (MAS ECI) an der Hochschule Luzern geflossen und danach in journalistische Texte, die bei der Schweizer Zeitschrift *Beobachter* publiziert wurden. Ich habe mich auf den Handel mit pharmazeutischen Produkten fokussiert, nicht zuletzt aufgrund der Tatsache, dass heute bei der Bekämpfung der Produktepiraterie im Bereich der Medikamente oft von fast unglaublichen Gewinnmargen die Rede ist. Um die Abläufe dieser Verkaufsplattformen zu verstehen und nachzuvollziehen und um erfahren zu können, wie die Zahlungsabläufe und die Kommunikation unter anonymen

Geschäftspartnern im Detail funktionieren, habe ich diverse Produkte bestellt. Um nicht selber mit dem Gesetz in Konflikt zu geraten, wurden diese Käufe wissenschaftlich begleitet und die Produkte bei einem Notar registriert, aufbewahrt und schließlich vernichtet. Das vorliegende Buch will das Phänomen dieser anonymen Marktplätze erklären und die Dimension sowie die gesellschaftliche Bedeutung aufzeigen. Gleichzeitig soll es vor Augen führen, wie sich diese Handelsplätze auf die Entwicklung der Kriminalität auswirken und inwieweit Ermittlungsbehörden das Ausmass und die Tragweite dieser Entwicklung unterschätzen.

Das Fazit dieser Recherchen: Im Darknet bietet eine rapid wachsende Zahl Händler einer weltweiten Kundschaft eine schier unglaubliche Palette von illegalen Waren und Dienstleistungen aller Art an. Ihre Onlineshops sind so geschickt gebaut wie Amazon, Zalando oder E-Bay. Um auf diese Marktplätze zu gelangen, bedarf es keinerlei technischer Vorkenntnisse. Das Einzige, was man wissen muss: Sie können mit herkömmlichen Browsern wie Firefox, Chrome oder Safari nicht erreicht werden. Nötig ist ein sogenannter TOR-Browser (TOR: The Onion Router), der – legal – die eigenen Spuren im Internet verwischt. Statt «.ch» oder «.com» tragen die Seiten im Darknet die Endung «.onion» in Anlehnung an die zwiebelartige Verschlüsselung der Daten, die mit dem TOR-Browser durchs Internet geschickt werden (s. Kapitel 2). Die Onlineshops im Darknet haben auch keine einprägsamen Bezeichnungen, sie gleichen einer willkürlichen Aneinanderreihung von Buchstaben, Zahlen und Sonderzeichen – und wechseln oft. Käufer benötigen einfach den richtigen Link, um auf diese Onlineshops zu gelangen. Die Links sind auf einschlägigen Seiten im offenen Internet für jedermann zugänglich.

Grafik 1: Wo ist das Darknet?
Wenn man das Internet mit einem Meer vergleicht, bewegen wir uns mit Google, Facebook und Co. nur an der Oberfläche.

Seit nach dem Amoklauf im Münchner Olympia-Einkaufszentrum im Sommer 2016 bekannt wurde, dass der Täter

seine Waffe im Darknet gekauft hatte, taucht der Begriff plötzlich vermehrt in den Medien auf. Dabei wird die Schattenwelt des Internets mit seinen anonymen Marktplätzen geradezu mystifiziert und als geheimnisumwitterte Welt beschrieben. Das ging so weit, dass in verschiedenen Medien – fälschlicherweise – sogar dann von Darknet die Rede war, wenn sich Kriminelle auf dubiosen oder etwas versteckten Seiten im normalen, sogenannten visible (sichtbaren) Internet tummeln. Solche Fälle haben jedoch nichts mit dem Darknet zu tun, es handelt sich oft um alltägliche kriminelle Vorfälle, in denen das Internet als Tatwerkzeug benutzt wird. Etwa wenn auf fernöstlichen Webseiten gestohlene Waren oder Potenzpillen angeboten werden. Unter dem Begriff Cybercrime versteht man hingegen all die Delikte, bei denen mithilfe des Internets Schranken von Computern überwunden werden, also vom Passwortklau bis zum Hackerangriff auf eine Firma. Kaum ein Tag vergeht heute, an dem nicht publik wird, dass eine Bank oder ein internationaler Konzern von einem Hackerangriff betroffen ist.

Doch was ist eigentlich das normale Internet? Und wo liegt das Darknet? Unter dem Begriff «Internet» versteht man alle online gestellten Inhalte. Derzeit gibt es gemäss dem statistischen Online-Auswertungsdienst Internetlivestats rund eine Milliarde Webseiten. Allerdings ist mit Suchmaschinen nur ein Teil dieser im Netz aufgeschalteten Webseiten auffindbar. Der Grund liegt möglicherweise darin, dass Webseiten erst kurze Zeit online sind, die Internetadresse (URL) gewechselt hat oder die Adresse von Robots blockiert wird.[1] Die Schätzungen, wie viele Seiten von Google und anderen Suchmaschinen nicht aufgefunden werden, liegen weit auseinander.

Fachleute sind sich aber einig, dass der allergrösste Teil der weltweit ins Netz gestellten Seiten mit einer Google-Suche gar nicht erst gefunden wird. Dieser Bereich wird «Deep Web» oder

«Invisible Web» genannt. Der ehemalige Leiter des Europol-Kompetenzzentrums Cybercrime (EC3) Troels Oerting schätzte bei einer internationalen Ermittlertagung, dass nur gerade 4 Prozent aller existierenden Webseiten von Suchmaschinen indexiert und damit für die gesamte Öffentlichkeit sichtbar sind. Anders gesagt: 96 Prozent aller Internetseiten liegen gemäss dieser Beurteilung im Deep Web. Der niederländische Journalist und Recherchetrainer mit Schwerpunkt Internet/Social Media, Henk Van Ess, kommt zu einem etwas anderen Schluss. Er schätzt, dass Google immerhin etwa 35 Prozent aller Webseiten indexiert. Die anderen 65 Prozent liegen gemäss Van Ess im Bereich des Deep Web. Davon finden sich je ein Drittel in sozialen Netzwerken sowie im versteckten Web («Hidden Web»). Das restliche Drittel sind laut Van Ess im Internet verlorene Inhalte («Lost Web»).

Henk Van Ess ist überzeugt, dass Inhalte im nicht sichtbaren Web nicht a priori gleichzusetzen sind mit problematischen Inhalten oder dubiosen Angeboten. Tatsächlich gibt es eine nicht abschätzbare Zahl Internetangebote, die sich beispielsweise hinter einer Passwortschranke befinden – und nur schon deshalb von Google nicht gefunden werden. In diesen Bereich fallen etwa Bibliotheken, Datenbanken oder Mitgliederbereiche. Van Ess rechnet dem Deep Web auch Webseiten zu, die «lost» sind, also verloren. Darunter versteht er nicht mehr verlinkte Unterseiten («Subdomains») und Dateien, die aber weiterhin im Netz gespeichert sind. Letztere sind mit einer gezielten Google-Suche auffindbar. Dazu werden beispielsweise die Operatoren von Google systematisch eingesetzt.[2] Dieser auf den ersten Blick nicht sichtbare Bereich wird auch «Below the Surface» genannt.

Wo beginnt das Darknet?

Unter dem Begriff «Darknet» oder «Darkweb» versteht man primär sogenannte Hidden Services, die aufgrund der Struktur ihrer Domainnamen lediglich mit dem TOR-Browser auffindbar sind. Das Darknet kann damit als Teilmenge des Deep Web bezeichnet werden. In englischsprachigen Ländern ist auch der Begriff «Onionland» verbreitet, in Anlehnung an die Endung der Webangebote (.onion). Die Zwiebel symbolisiert beim TOR-Projekt die schichtartige Verschlüsselung (s. a. Kapitel 2). Der Begriff «Hidden Web» wird oft als Synonym für Deep Web verwendet. Doch mit «Hidden Services» sind jene verborgenen Webseiten gemeint, die mit herkömmlichen Browsern wie Firefox oder Safari nicht auffindbar sind. Ins Netz gestellt werden solche Webseiten über TOR. So können beispielsweise Systemkritiker, Menschenrechtsaktivisten und Whistleblower vollständig anonym Informationen verbreiten, mit TOR können sie ihren Standort gänzlich verschleiern. Die Seiten von Wikileaks beispielsweise waren ursprünglich nur über diesen Dienst erreichbar. Gleichzeitig ermöglicht TOR in Ländern mit eingeschränkter Internetnutzung den Zugang zu westlichen Informationen. Weil beispielsweise China die Webseite der *New York Times* bereits seit mehreren Jahren blockiert, können Bürgerrechtler nur dank TOR die Zeitung lesen.

Die anonymen Marktplätze im Darknet nutzen ebenfalls diese Hidden Services. Sie werden in Anlehnung an die Verschlüsselung auch als «Cryptomarkets» bezeichnet. Im englischen Sprachraum hat sich auch der Terminus der «Dark Markets» etabliert. Neben den anonymen Marktplätzen gibt es noch weitere dunkle Bereiche, andere Darknets.

Dazu zählen beispielsweise die verborgenen Seiten von The Free Network oder von I2P. Für beide Netzwerke benötigt man

einen entsprechenden Browser, der – ähnlich wie TOR – die eigene Identität (IP-Adresse) verschleiert. Diese Netzwerke haben grosse Ähnlichkeiten mit dem TOR-Projekt. Es ist aber davon auszugehen, dass sie wesentlich kleiner sind. Auch die bereits seit Jahren aktiven Peer-to-Peer-Netzwerke (P2P) – also geschlossene, gegen aussen nicht einsehbare Kreise von Personen – sind eigentlich Darknets. Diese Netzwerke sind aber Nischenangebote geblieben, oftmals mit kriminellen Inhalten. Kreise mit speziellen Vorlieben tauschen hier etwa pornografisches und kinderpornografisches Material oder Waffen aus. Entsprechend stehen sie regelmässig im Fokus der Ermittler. Das Darknet ist nur ein Teil des Deep Web, das eine ganz andere Dimension hat. Dieser Teil des Netzes dürfte ein Vielfaches dessen umfassen, was heute einer breiten Öffentlichkeit bekannt ist. Es gibt Schätzungen, wonach das Deep Web etwa 500-mal grösser sein soll als das normale World Wide Web.

Seit das Internet existiert, wird es auch für kriminelle Zwecke genutzt. Vor lauter spektakulären Fällen geht heute vergessen, dass Betrüger im Netz längst Alltag sind. Sie verüben kleinere Delikte, indem sie beispielsweise über Versteigerungsplattformen wie E-Bay oder Ricardo ahnungslosen Kunden nicht existierende Produkte verkaufen und sie um ihr Geld prellen. Oder sie verschicken massenweise Werbe-E-Mails und bieten wertlose Produkte an, verkaufen fragwürdige Geldanlagen und hauen blauäugige Konsumenten übers Ohr (Spam). In all diesen Fällen bewegen sich die Täter aber im offen zugänglichen Internet. Für diese Art Delikte hat das Darknet aber ebenfalls eine wichtige Funktion. Die Täter können sich auf Onlineshops im Darknet Schadprogramme besorgen. Denn dort bieten nicht nur Leute wie «Edelweiss» Cannabis an, sondern Unbekannte verkaufen hier eine Vielzahl von Drogen, Waffen und IT-Dienstleistungen. Man muss nicht einmal besondere IT-Kenntnisse besitzen, jedermann

kann sich dort für kriminelle Zwecke Informatikdienstleistungen besorgen. Man bezahlt beispielsweise einen Hacker, der für einen in das E-Mail-Konto einer Zielperson eindringt («Crime-as-a-Service»).

Oder die Täter kaufen im Darknet Programme, versenden damit Tausende von E-Mails und gaukeln Empfängern vor, sie seien ihr Finanzdienstleister und würden sie aus Sicherheitsgründen auffordern, ihr Bankkonto neu zu authentifizieren. Auch wenn hinlänglich bekannt ist, dass solche Phishing-Attacken nur zum Ziel haben, Benutzernamen und Passwörter abzugreifen, funktioniert dieser Trick bis heute. Wer gutgläubig handelt, wird auf eine Webseite geführt, die der eigenen Bank-Webseite zum Verwechseln ähnlich sieht, aber lediglich dazu dient, die Tastenkombinationen bei der Eingabe von vertraulichen Login-Angaben aufzuzeichnen.

Solche Cybercrime-Delikte sind heute alltäglich. Die Schweizerische Koordinationsstelle für Internetkriminalität (Kobik) verzeichnet seit einigen Jahren mehr Meldungen zu Phishing, Hacking und Schadprogrammen als zu verbotener Pornografie, die jahrelang Nummer eins bei der Bekämpfung der Internetkriminalität war. Ein Cyberspezialist des Bundes sagt: «Beim Fedpol stellen wir eine Verschiebung fest: mehr Wirtschaftskriminalität, weniger Pädokriminalität. Jedenfalls was die Zahl der Meldungen ausmacht.» Das heisse aber nicht, dass es tatsächlich weniger Pädokriminalität gebe, sagt der Ermittler. «Denn für diese spielt gerade das Darknet eine wichtige Rolle.»

Massiv zugenommen hat in den letzten Jahren die Zahl der Hackerattacken mit konkreten erpresserischen Zielen. Die Tätergruppen sind international organisiert und gehen gezielt vor: Server von Unternehmen aus der Finanz- und Versicherungsbranche oder Firmen mit starker Onlinepräsenz (E-Commerce) werden mit automatisierten Massenanfragen –