www.jusletter.ch

Simon Bächtold

Die strafprozessuale Netzsperre

Von der Öffentlichkeit weitgehend unbemerkt, sperren Schweizer Staatsanwaltschaften den Zugang zu ausländischen Webseiten. Der Autor zeigt die rechtlichen und technischen Grundlagen sowie die Möglichkeiten und Grenzen dieser wenig bekannten Zwangsmassnahme auf.

Beitragsart: Beiträge
Rechtsgebiete: Strafprozessrecht; Informatik und Recht

Zitiervorschlag: Simon Bächtold, Die strafprozessuale Netzsperre, in: Jusletter 21. Juni 2021

Inhaltsübersicht

1. Praxisbeispiel: Ransomware-Angriffe auf Schweizer Unternehmen – Kann die Datenverbreitung gestoppt werden?

[1] Immer wieder werden auch Schweizer Unternehmen Opfer von Ransomware-Angriffen: Eine organisierte, aus dem Ausland operierende Täterschaft nutzt eine Schwachstelle im Netzwerk des Unternehmens, dringt in dieses ein und schleust eine Crypto-Ransomware (Malware) ein. Diese Malware verschlüsselt die Server und weitere Rechner des Unternehmens und macht diese so unbrauchbar. Weil Unternehmen für gewöhnlich über Backups verfügen, welche die Wiederherstellung der verschlüsselten Daten erlauben, benötigt die Täterschaft ein zusätzliches Druckmittel: Sie lädt sensible Firmendaten auf einen Server hoch und droht mit deren Veröffentlichung im World Wide Web. Um diese Veröffentlichung abzuwenden, fordert die Täterschaft eine Lösegeldforderung von mehreren Millionen US-Dollar in Bitcoin. Das Unternehmen möchte seine Systeme möglichst rasch wieder in Betrieb nehmen, Sicherheitslücken im Netzwerk beheben und die Verbreitung seiner sensiblen Daten möglichst verhindern. Betroffene Unternehmen ziehen regelmässig spezialisierte externe Dienstleister bei, um die eigene Informatikabteilung bei der Erreichung der ersten beiden Ziele zu unterstützen. Die Primäraufgabe der Strafverfolgungsbehörden ist es, die Täterschaft zu lokalisieren und idealerweise zu de-anonymisieren. Aber können die Strafverfolgungsbehörden auch dazu beitragen, die Verbreitung gestohlener Daten zu verhindern?

2. Netzsperren – war da nicht etwas?

[2] Eine Möglichkeit, um der Veröffentlichung von gestohlenen Firmendaten über das Internet entgegenzuwirken, ist eine Netzsperre. Eine «Netzsperre», wie sie hier verstanden wird, meint die Begrenzung des Zugangs von Internet-Nutzern in der Schweiz auf Inhalte des Internets, insbesondere Webseiten, durch technische Mittel. Es handelt sich dabei typischerweise um Inhalte auf ausländischen Servern, welche nicht direkt dem Zugriff der Schweizer Behörden unterliegen. Zu den Details der technischen Umsetzung komme ich später. Solche Netzsperren sind – wenngleich der Eingriff im Einzelfall klein sein mag – hoch umstritten. Sie stehen im Konflikt mit dem Ziel eines offenen Internets, welches seit Beginn dieses Jahres als Art. 12e FMG[1] explizit

[1] Fernmeldegesetz vom 30. April 1997 (FMG; SR 784.10).

Eingang ins Gesetz gefunden hat. Schnell werden Begriffe wie «Internet-Zensur» gebraucht oder Vergleiche zu autoritären Staaten gezogen. Dieser Artikel geht der Frage nach, ob auch Schweizer Staatsanwaltschaften im Interesse der Strafverfolgung zu Netzsperren greifen dürfen und falls ja, unter welchen Voraussetzungen.

[3] Der Begriff «Netzsperre» dürfte manche an die Diskussion im Vorfeld der Revision des Geldspielgesetzes erinnern: Das seit dem 1. Januar 2019 gültige Geldspielgesetz[2] sieht in Art. 86 BGS die Sperrung von nicht bewilligten Geldspielangeboten im Internet vor.[3] Die Eidgenössische Spielbankenkommission publiziert auf ihrer Webseite eine Liste mit den entsprechenden Domains.[4] Diese Sperre richtet sich an die dem Bundesamt für Kommunikation (BAKOM) gemeldeten Fernmeldedienstanbieter. Aktuell gibt es in der Schweiz rund 300 solche Anbieter von Internetzugängen («Internet access provider» oder kurz «Provider»).[5] Die vier grössten sind jedoch Swisscom, Salt, Sunrise und UPC/Cablecom.[6]

[4] Auch das Fernmeldegesetz sieht Netzsperren vor. Art. 46a Abs. 3 FMG verpflichtet Anbieterinnen von Fernmeldediensten, verbotene pornographische Inhalte gemäss Artikel 197 Abs. 4 und 5 StGB zu «unterdrücken», wenn sie vom Bundesamt für Polizei (fedpol) darauf «hingewiesen» werden. Da das Bundesamt für Polizei selbst keine Zwangsmassnahmen verfügen kann – dafür wäre typischerweise die Bundesanwaltschaft zuständig – kann es sich bei dieser «Unterdrückung» von Inhalten nach der Vorstellung des Gesetzgebers nicht um eine strafprozessuale Zwangsmassnahme handeln. Es geht um eine präventive Tätigkeit der (Bundes-)Polizei und der Fernmeldedienstanbieter, konkret der Provider. Ich gehe entsprechend davon aus, dass die Provider auch ohne entsprechenden Hinweis berechtigt und verpflichtet wären, illegale pornographische Inhalte zu sperren, wenn sie solche entdecken.

3. Netzsperren im Strafverfahren – Rechtliche Grundlage

[5] Schweizer Staatsanwaltschaften verfügen – gerade auch im internationalen Vergleich – rechtlich über viel Macht. Täglich verlangen sie von Beschuldigten und unbeteiligten Dritten die Herausgabe von Unterlagen, wie zum Beispiel Bankunterlagen, aber auch Daten aller Art, wie Videoaufnahmen oder E-Mails. Sie Beschlagnahmen Gegenstände und Vermögenswerte, wie Bankguthaben oder Immobilien. Eine weitere praktisch sehr relevante Zwangsmassnahme ist die «Sperre», etwa von Bankkonten oder des Grundbuchs. Hier wird nichts physisch sichergestellt oder beschlagnahmt, aber dem Inhaber wird die Verfügungsmacht vorübergehend entzogen. Bank-

2 Bundesgesetz über Geldspiele vom 29. September 2017 (BGS; SR 935.51).

3 In der Referendumsabstimmung wurde das revidierte Geldspielgesetz von den Stimmbürgern am 10. Juni 2018 mit 72.9% gutgeheissen. Vgl. «Bundeskanzlei BK», «Volksabstimmung vom 10. Juni 2018, Bundesgesetz vom 29. September 2017 über Geldspiele (Geldspielgesetz, BGS)» (https://www.bk.admin.ch/ch/d/pore/va/20180610/det619.html, zuletzt besucht am 30. Mai 2021).

4 «Eidgenössische Spielbankenkommission ESBK», «Zugangssperren zu nicht bewilligten Online-Spielangeboten» (https://www.esbk.admin.ch/esbk/de/home/illegalesspiel/zugangssperren.html, zuletzt besucht am 30. Mai 2021).

5 «Bundesamt für Kommunikation», «BAKOM Online – Virtueller Schalter» (https://www.eofcom.admin.ch/eofcom/public/searchCatalog.do, zuletzt besucht am 30. Mai 2021).

6 Annahme gestützt auf die Zahlen für Breitbandanschlüsse/Festnetz: «Bundesamt für Kommunikation BAKOM», «Marktanteil Breitband Internetzugang auf dem Festnetz» (https://www.bakom.admin.ch/bakom/de/home/telekommunikation/zahlen-und-fakten/sammlung-statistischer-daten/marktstruktur-und-stellen/marktanteil-internetzugang.html, zuletzt besucht am 30. Mai 2021).

kontosperren werden regelmässig so ausgestaltet, dass Mittelzuflüsse weiterhin möglich sind, Abflüsse jedoch nicht oder nur bis zu einem bestimmten Kontostand. All dies erfolgt gestützt auf die Art. 263 ff. StPO[7].

[6] Art. 263 Abs. 1 StPO lautet:

> «*Gegenstände und Vermögenswerte einer beschuldigten Person oder einer Drittperson können beschlagnahmt werden, wenn die Gegenstände und Vermögenswerte voraussichtlich: a. als Beweismittel gebraucht werden; b. zur Sicherstellung von Verfahrenskosten, Geldstrafen, Bussen und Entschädigungen gebraucht werden; c. den Geschädigten zurückzugeben sind; d. einzuziehen sind.*»

[7] Die möglichen Beschlagnahmegründe liegen also in der Beweisführung, Deckung von Kosten und Entschädigungen, Rückgabe an die Geschädigten oder der Einziehung, insbesondere der Sicherungseinziehung (Drogen, Waffen etc.).

[8] Die Beschlagnahme immaterieller «Güter» wie Daten und Kryptowährungen wird in der StPO nicht erwähnt, findet aber in der Praxis andauernd auf dieser Rechtsgrundlage statt und ist, soweit ersichtlich, unbestritten. Die zu Grunde liegende juristische Argumentation ist simpel: Darf die Staatsanwaltschaft gestützt auf Art. 263 StPO einen ganzen Server (Hardware, inklusive Software) beschlagnahmen, mit all den disruptiven Folgen, welche dies mit sich bringt, darf sie – *a majore ad minus* – auch den weniger intensiven Eingriff der Sicherstellung und Beschlagnahme von sich auf dem Server befindlichen Daten anordnen. Man kann argumentieren, die Staatsanwaltschaft könne gestützt auf Art. 263 StPO – vergleichbar mit der Sperre eines Bankkontos – grundsätzlich auch eine Netzsperre verfügen. Bei der Kontosperre wird die Verfügungsmacht über (immaterielle) Vermögenswerte genommen, bei der Netzsperre die Verfügungsmacht über Datenflüsse.

[9] In mindestens einem Fall hatte das Bundesgericht sich mit einer staatsanwaltschaftlichen Netzsperre zu befassen. Der Nichteintretensentscheid erging jedoch noch vor Einführung der Eidgenössischen Strafprozessordnung und stützte sich auf das Einziehungsrecht gemäss Art. 70 StGB und auf Art. 292 StGB[8] (Ungehorsam gegen amtliche Verfügung). Das Bundesgericht beschäftigte sich in dem Entscheid leider nicht mit der Frage, ob eine strafprozessuale Netzsperre überhaupt zulässig ist, qualifizierte sie aber als vorsorgliche Massnahme gemäss Art. 46 Abs. 2 und Art. 98 BGG[9] (Urteil des Bundesgerichts 1B_242/2009 vom 21. Oktober 2009, E. 2).

[10] Auf Anfrage bei den vier grössten Schweizer Providern im Herbst 2020 antworteten drei, solche staatsanwaltschaftlichen Netzsperren kämen in der Praxis vor, beschränkten sich jedoch auf wenige Fälle pro Jahr. Bisher hat sich keiner der grossen Provider juristisch gegen eine staatsanwaltschaftliche Netzsperre gewehrt. Es kam also soweit ersichtlich nie zu einer gerichtlichen Überprüfung. Ein Provider hat die Anfrage nicht beantwortet.

[11] Die Provider haben selber nur ein geringes Interesse daran, gegen strafrechtliche Netzsperren juristisch vorzugehen. Die operativen Kosten für die Umsetzung gelegentlicher Verfügungen dürften weit geringer ausfallen als die Kosten einer Anfechtung vor Gericht. Solange die Staatsanwaltschaften die Netzsperren angemessen kurz befristen, könnten die Beschwerdeinstanzen

7 Schweizerische Strafprozessordnung vom 5. Oktober 2017 (StPO; SR 312.0).

8 Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (StGB; SR 311.0).

9 Bundesgesetz über das Bundesgericht vom 17. Juni 2005 (BGG; SR 173.110).

zudem versucht sein, auf allfällige Beschwerden nicht einzutreten mit dem Argument, es bestehe kein aktuelles Rechtsschutzinteresse (mehr).

4. Technische Umsetzung und deren Grenzen

[12] Gibt ein Internetnutzer in der Adresszeile des Webbrowsers eine Internetadresse (URL) ein (z.B. cybercrime.site), übersetzt der Webbrowser, für den Nutzer unsichtbar, diese URL in die IP-Adresse des Servers, welcher die Webseite zur Verfügung stellt (z.B. 49.12.167.22). Der Browser weiss selbst nicht, welche IP-Adresse zu welcher URL gehört und fragt diese Information bei einem Domain Name System (DNS)-Server an. Jeder Provider bietet seinen Kunden einen DNS-Server an, aber Nutzer können auch andere verwenden, wenn sie die Konfiguration entsprechend anpassen. Um die Verfügung Netzsperre umzusetzen, kann ein Provider also den Domainnamen in «seinem» DNS-Server sperren. Statt der gewünschten Seite wird dann eine entsprechende Meldung angezeigt, wie zum Beispiel: «*Die gewünschte Webseite wurde auf behördliche Anordnung gesperrt.*»

[13] Eine andere Variante wäre es, anstelle der Domain direkt die IP-Adresse zu sperren. In diesem Fall hätte der Nutzer auch keinen Zugriff, wenn er einen alternativen DNS-Server zur Übersetzung des Domainnamens verwendet. Diese Variante hat jedoch einen Nachteil: Erstens kommt es praktisch sehr häufig vor, dass zahlreiche Webseiten dieselbe IP-Adresse haben, weil sie über denselben Webserver angeboten (gehostet) werden. Dies würde dazu führen, dass eine grössere Zahl von Webseiten von einer IP-Sperre betroffen wären und nicht nur die eine, gegen welche sich die Netzsperre eigentlich richtet. Zweitens kommt es praktisch gerade bei Webseiten von Kriminellen vor, dass diese häufig «umziehen», sich also deren IP-Adresse alle paar Tage ändert, was die IP-Sperre unwirksam werden lässt. Eine ständige Aktualisierung der zu sperrenden IP-Adresse wäre in der Umsetzung recht anspruchsvoll.

[14] Praktisch in Frage kommt daher eigentlich nur die Sperre anhand des Domainnamens. Eine Einschätzung, die auch von den angefragten Providern geteilt wird, soweit sie sich dazu geäussert haben.

[15] Beide Ansätze sind wirkungslos, wenn sich ein Nutzer über einen ausländischen Proxy-Server[10] oder Virtual Private Network (VPN) in das Internet verbindet. Kurzum: Es gibt genügend technische Mittel, um eine Netzsperre zu umgehen. Eine Netzsperre kann folglich einen einigermassen versierten Nutzer nicht daran hindern, eine gewisse Webseite zu erreichen. Man kann jedoch annehmen, dass die Netzsperre bei einem Grossteil der Internetnutzer trotzdem wirkt, weil diese zu bequem oder technisch zu wenig versiert sind, sie zu umgehen.

5. Rechtliche Einwendungen gegen Netzsperren

[16] Rechtliche Einwendungen gegen eine staatsanwaltschaftlich verfügte Netzsperre gibt es viele. Da eine gerichtliche Überprüfung bisher offenbar unterblieben ist, nehme ich hier eine Auslegeordnung vor:

[10] Ein Server, vergleichbar mit einem «Strohmann» in der analogen Welt, über den der Datenverkehr eines Nutzers/Anschlusses umgeleitet wird, um dessen IP-Adresse gegenüber dem Internet zu verbergen.

5.1. Fehlende Rechtsgrundlage

[17] Genügt Art. 263 ff. StPO als Grundlage für eine Netzsperre? Die Beschlagnahme ist unproblematisch bei körperlichen Dingen. Bei unkörperlichen Dingen ist sie praktisch unbestritten, wenn auch nicht explizit im Gesetzeswortlaut enthalten. Praxisgemäss kann sich die Beschlagnahme sowohl auf vorhandene wie auf später zufliessende Dinge beziehen, wie bei der Kontosperre, die auch Gelder erfasst, die erst nach der Verfügung der Kontosperre zufliessen. In jedem Fall aber ist die Beschlagnahme nach Art. 263 ff. StPO eine konservatorische Massnahme. Über das Schicksal des Beschlagnahmegutes wird in vielen Fällen erst bei Verfahrensabschluss entschieden (Art. 267 Abs. 3 StPO). Bei einer Netzsperre wird aber nichts konserviert. Sie zielt darauf ab, einen Datenfluss zu verunmöglichen. Die Blockierung verhindert, dass Daten übertragen und beim Nutzer gespeichert werden. Da die fraglichen Daten nicht übertragen und gespeichert werden, kann im Endentscheid nicht darüber befunden werden. Dieser vermeintliche Widerspruch lässt sich jedoch nach der hier vertretenen Meinung auflösen. Art. 267 Abs. 2 StPO sieht vor, dass beschlagnahmte Gegenstände, die einer bestimmbaren Person (i.d.R. einer Geschädigten) entzogen wurden, der berechtigten Person vor Abschluss des Verfahrens zurückgegeben werden. Diese Bestimmung passt auf Daten, die beispielsweise im Rahmen einer Ransomware-Attacke einem Unternehmen gestohlen wurden. Das geschädigte Unternehmen ist zweifellos an den Daten berechtigt. Da Daten jedoch ubiquitär sind, ist eine Rückgabe nicht erforderlich, vielmehr ist die Blockierung der Datenübertragung sachgerecht und entspricht den Interessen der Geschädigten.

[18] Die mit Ransomware erpresste Unternehmung vom Eingangsbeispiel arbeitete ab dem Tag, an dem der Angriff bekannt wird fieberhaft an der Absicherung seiner Systeme und an der Wiederherstellung der Daten. Wochen später macht die Täterschaft ihre Drohung wahr und veröffentlicht einen Teil der gestohlenen Daten auf einer eigens dafür betriebenen Webseite im World Wide Web. Zu diesem Zeitpunkt hat die Unternehmung kein Interesse mehr daran, diese Daten zurückzuerhalten. Sie wird sie längst anhand der Backups wiederhergestellt haben. Die Unternehmung hat aber ein grosses Interesse daran, die Verbreitung der von ihr gestohlenen Daten zu hemmen. Durch die Netzsperre kann zumindest ein Teil der Schweizer Internetnutzer vom Zugriff auf diese Daten abgehalten werden.

5.2. Nicht in der Kompetenz der Staatsanwaltschaft

[19] Für die Überwachung des Fernmeldeverkehrs ist gemäss Art. 272 Abs. 1 StPO die Bewilligung eines Zwangsmassnahmengerichtes erforderlich. Es wurde schon argumentiert, dies müsse also auch für die Blockierung des Fernmeldeverkehrs gelten. Diese Annahme ist falsch: Überwachung hat nichts mit Sperrung zu tun. Der Genehmigungsvorbehalt für Überwachungsmassnahmen liegt im Schutz des Fernmeldegeheimnisses gemäss Art. 13 BV[11] und Art. 43 FMG begründet. Das Fernmeldegeheimnis wird jedoch durch eine Netzsperre nicht tangiert. Die Staatsanwaltschaft, welche diese anordnet, erhält weder Einblick in den Inhalt der (unterbundenen) Kommunikation, noch über die daran beteiligten Parteien. Die Zwangsmassnahmengerichte sind folglich nicht zuständig.

11 Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV; SR 101).

5.3. Nicht hinreichend spezifisch

[20] Eine staatsanwaltliche Sperrverfügung wird sich über die Details der technischen Umsetzung durch den Provider ausschweigen, weil diese der Staatsanwaltschaft nicht bekannt sind. Provider könnten versucht sein einzuwenden, eine Netzsperre sei deshalb nicht hinreichend spezifisch. Dies trifft nicht zu, solange sie alle nötigen Angaben enthält, welche der Provider benötigt, um die Verfügung praktisch umzusetzen. Dies ist bei der Angabe eines Domainnamens bereits erfüllt, sodass dieser Vorbehalt nie greifen dürfte.

5.4. Nicht verhältnismässig

[21] «Zwangsmassnahmen sind Verfahrenshandlungen der Strafbehörden, die in Grundrechte der Betroffenen eingreifen [..]» (Art. 196 StPO). Sie müssen verhältnismässig sein (Art. 36 Abs. 1 BV und Art. 5 BV). Zwangsmassnahmen, die in die Grundrechte nicht beschuldigter Personen eingreifen, sind besonders zurückhaltend einzusetzen (Art. 197 Abs. 2 StPO).

[22] Der Frage der Verhältnismässigkeit kommt bei der Netzsperre eine grosse Bedeutung zu, weil sie eine unbestimmte Vielzahl von Personen – sämtliche Internetnutzer, die eine gesperrte Seite besuchen möchten – betreffen kann. Zudem greift sie in das Grundrecht auf Informationsfreiheit nicht beschuldigter Personen (Internetbenutzer) ein und in das Grundrecht der Wirtschaftsfreiheit der ebenfalls nicht beschuldigten Provider, weshalb das Gesetz «besondere Zurückhaltung» vorschreibt (Art. 197 Abs. 2 StPO).

[23] Damit eine Zwangsmassnahme verhältnismässig ist, muss sie im öffentlichen Interesse liegen, geeignet, erforderlich und zumutbar sein (Art. 36 Abs. 1 BV). Das öffentliche Interesse ist hier das Interesse an der Strafverfolgung im weitesten Sinn. Dazu gehört neben der Aufklärung von Straftaten und der Bestrafung der Täter auch die Vereitelung von Straftaten und die Erschwerung des *modus operandi*.[12] Diese Ziele spiegeln sich in verschiedenen Rechtsnormen. Beispielhaft erwähnt seien nur die Bestimmungen zur Sicherungseinziehung gemäss Art. 69 Abs. 1 StGB oder die Geldwäschereinormen («*Straftaten dürfen sich nicht lohnen*»).

[24] Eine Netzsperre kann zweifellos im Interesse der Vereitelung von Straftaten liegen, solange sie sich – wie im eingangs erwähnten Beispiel – gegen eine Webseite richtet, die ausschliesslich der Tatbegehung dient. Eine andere Frage ist, wie vorzugehen wäre, wenn eine Webseite gesperrt werden soll, die nebst kriminellen auch legale Inhalte bereithält. Dies sprengt jedoch den Rahmen der vorliegenden Publikation.

[25] Es stellt sich weiter die Frage der Eignung einer Netzsperre, um das öffentliche Interesse zu verwirklichen. Gemäss Lehre und Rechtsprechung ist an die Eignung nur ein geringer Anspruch zu stellen. Alles was nicht geradezu schädlich oder zumindest wirkungslos ist, kann geeignet sein.[13] Da eine Netzsperre in der Lage sein dürfte, einen Grossteil der Internetnutzer vom Besuch der gesperrten Seiten abzuhalten, muss die Eignung bejaht werden. Ähnlich wurde auch im Vorfeld der Abstimmung zum revidierten Geldspielgesetz argumentiert.

---

12 In diesem Licht sind etwa die Einziehungstatbestände gemäss Art. 69 ff. StGB zu sehen, aber auch die Geldwäschereistrafnormen.

13 Felix Uhlmann/Beat Stalder, Unverhältnismässig weil unwirksam?, sic! 2018, S. 365 – 376, S. 365.

[26] Ein Grundrechtseingriff muss weiter erforderlich sein, es darf also kein milderes Mittel zur Verfügung stehen. Da eine Netzsperre nur eine einzelne Domain betrifft, die Massnahme also äusserst zielgerichtet ist, ist sie als das mildeste Mittel zu betrachten. Weniger als eine Domain kann nicht gesperrt werden und ein milderes Mittel, um den Zugang zu begrenzen, ist nicht ersichtlich. Die Netzsperre kann zudem angemessen befristet werden. Bei einem gewöhnlichen Internetnutzer, der nicht auf die Kenntnisnahme der gesperrten Inhalte angewiesen ist und beispielsweise bloss seine Neugierde befriedigen möchte, ist die Einschränkung auch ohne Weiteres als zumutbar zu betrachten. Anders könnte die Beurteilung ausfallen bei Journalisten, welche durch die Netzsperre in ihrer Recherchetätigkeit, also in ihrer Berufsausübung eingeschränkt werden. Gerade bei Journalisten ist jedoch anzunehmen, diese verwendeten die geeigneten technischen Mittel, um eine Netzsperre zu umgehen. Zusammengefasst wird hier davon ausgegangen, eine Netzsperre könne durchaus verhältnismässig ausgestaltet werden.

6. Jenseits nationaler Netzsperren

[27] Netzsperren, wie sie hier diskutiert wurden, können von einer Schweizer Staatsanwaltschaft einfach, rasch und (für die Behörde) kostenlos verfügt werden, entfalten jedoch nur auf dem Territorium der Schweiz eine Wirkung. Diese ist, angesichts des weltumspannenden Internets, offensichtlich recht begrenzt.

[28] Viel wirkungsvoller wären entsprechend Massnahmen «an der Quelle», wie etwa die Beschlagnahme oder Blockierung der Server-Infrastruktur im Ausland. Dies erfordert jedoch (langwierige) internationale Rechtshilfe und dies nicht selten durch Länder, welche nur unzuverlässig oder praktisch gar keine Rechtshilfe leisten.

[29] Auch eine Domain-Sperre an der Quelle ist denkbar. «ch»-Domains können direkt bei SWITCH beschlagnahmt werden. Auch alle übrigen so genannten top-level-Domains werden von bestimmten Organisationen verwaltet.[14] Diese sind technisch in der Lage, jede Domain unterhalb ihrer top-level-domain zu sperren, wobei sich eine solche Sperre auf das ganze Internet auswirkt. Es wird wenig überraschen, dass die meisten dieser Organisationen in den USA liegen, so dass auch hier grundsätzlich der Rechtshilfeweg zu beschreiten ist. Ob einige Organisationen missbräuchlich verwendete Domains auch auf eine begründete Anzeige einer Polizeibehörde hin sperren, entzieht sich meiner Kenntnis.

[30] Ein weiterer Ansatz wäre, nationale Netzsperren international zu koordinieren. Wenn beispielsweise sämtliche Signatarstaaten der Cyber Crime Convention (SR 0.311.43, CCC) nationale Netzsperren rasch und unkompliziert gegenseitig nachvollziehen würden, wäre schon einiges erreicht. Auch im zweiten Zusatzprotokoll zur CCC, welches aktuell ausgehandelt wird, ist jedoch nichts dergleichen vorgesehen.

14 «Internet Corporation for Assigned Names and Numbers», «Registry Listings» (https://www.icann.org/resources/pages/listing-2012-02-25-en, zuletzt besucht am 30. Mai 2021).

7. Fazit

[31] Netzsperren können dem öffentlichen Interesse dienen, die Verbreitung illegaler Inhalte zu hemmen. Netzsperren zur Blockierung ausländischer Internetseiten werden in der Praxis von Schweizer Staatsanwaltschaften angewendet, jedoch selten. Dabei erfolgt die Sperre über die Blockierung von Domainnamen durch die Schweizer Internetprovider. Von technisch versierten Internetznutzern können sie leicht umgangen werden. Eine verhältnismässige Ausgestaltung von Netzsperren ist möglich. Kontrovers ist die Frage, ob das Beschlagnahmerecht gemäss Strafprozessordnung als rechtliche Grundlage ausreicht. Eine gerichtliche oder gar höchstrichterliche Überprüfung dieser Frage steht bislang aus.

M.A. HSG in Law Simon Bächtold ist Rechtsanwalt, Wirtschaftsinformatiker (B.Sc. ZFH) und ehemaliger Staatsanwalt des Kantons Thurgau mit Spezialgebiet Cybercrime und digitalisierte Kriminalität. Er ist Inhaber der Kanzlei Bächtold Legal GmbH – in Partnerschaft mit Good Rechtsanwälte GmbH (www.good-zuerich.ch) und Co-Autor des Blogs unter www.cybercrime.site.