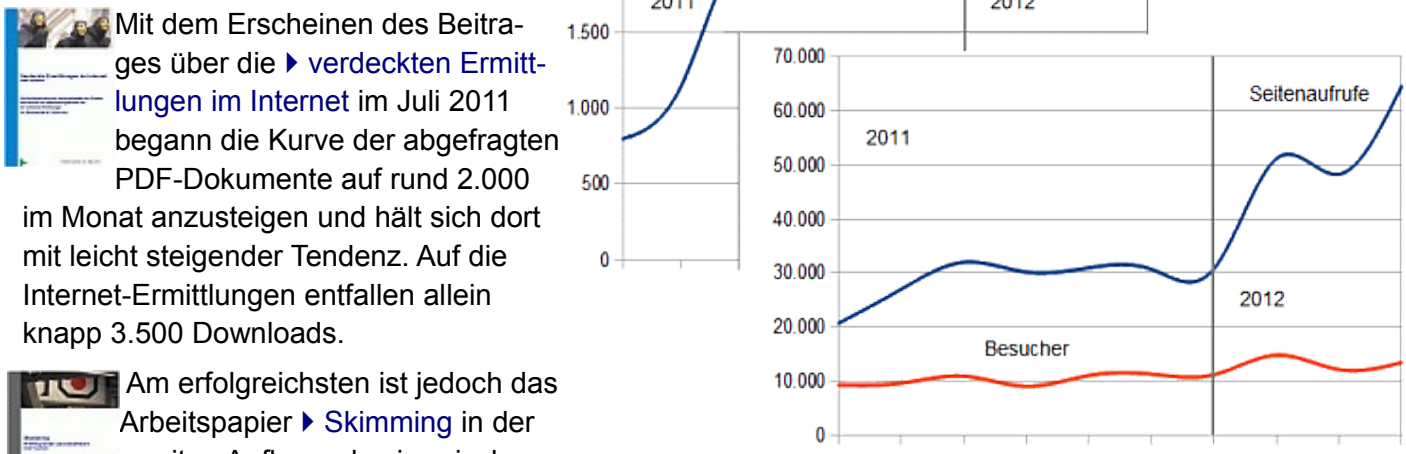
Cyberfahnder-Newsletter 10 vom 08.04.2012

5 Jahre Cyberfahnder

Steigende Nachfrage
Downloads, Besucher und Seitenaufrufe seit Juli 2011



Mit dem Erscheinen des Beitrages über die ▸ verdeckten Ermittlungen im Internet im Juli 2011 begann die Kurve der abgefragten PDF-Dokumente auf rund 2.000 im Monat anzusteigen und hält sich dort mit leicht steigender Tendenz. Auf die Internet-Ermittlungen entfallen allein knapp 3.500 Downloads.

Am erfolgreichsten ist jedoch das Arbeitspapier ▸ Skimming in der zweiten Auflage, das inzwischen rund 4.000 Mal abgerufen wurde. Im Dezember 2011 erschien die ▸ dritte Auflage, die seither ebenfalls mehr als 1.000 Mal nachgefragt wurde.

Im Mai 2010 war das Arbeitspapier ▸ Cybercrime erschienen, das bis jetzt 2.500 Downloads erfuhr. Es fasst die Beiträge im Cyberfahnder seit 2007 zusammen und brachte sie auf den Stand von 2010. Trotz fortschreitender Entwicklungen in den Bereichen der IuK-Technik und der Cybercrime bietet es noch immer einen passablen Einstieg in die Erscheinungsformen der IuK-Kriminalität.

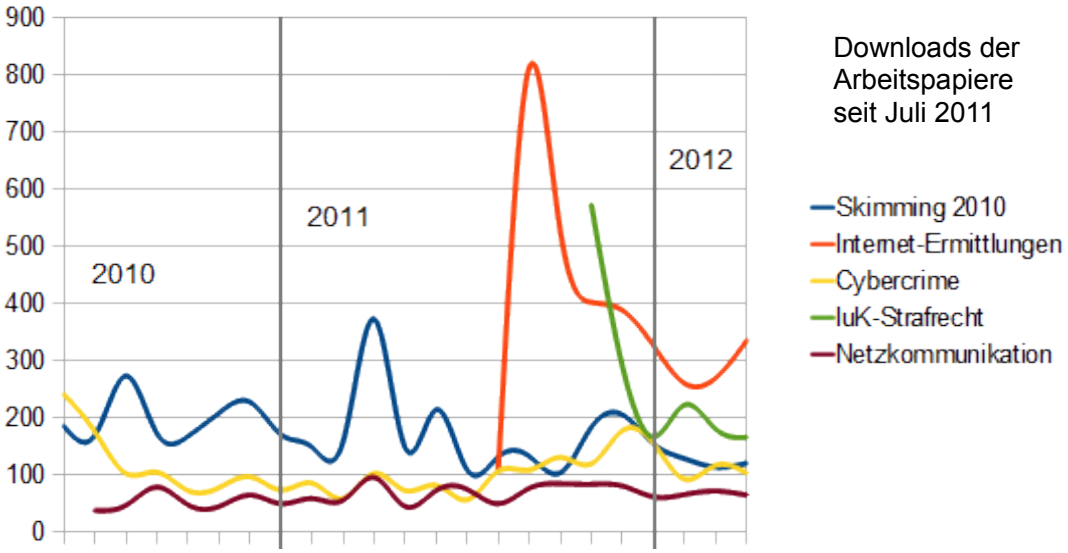
Im Oktober 2011 veröffentlichte ich schließlich das inzwischen 128 Seiten starke Arbeitspapier zum ▸ IuK-Strafrecht, das jetzt 1.600 Mal abgerufen wurde. Es bezeichnet die Besonderheiten des materiellen Cybercrime-Strafrechts und liefert einen Einstieg in die Materie. Vor der systematischen Behandlung der materiellen Rechtsfragen hatte ich mich bis dahin angesichts der Komplexität der Erscheinungsformen gedrückt. Bis 2011 waren eine ganze Menge an gerichtlichen Entscheidungen veröffentlicht worden, so dass nicht überall nur Neuland bestand.

Die „Dauerbrenner“ und die neuen ▸ Publikationen haben sicherlich einen großen Anteil an der gestiegenen Popularität des Cyberfahnders. Sie sind keine Schnellschüsse, sondern Aufsätze, die mit erheblichem Aufwand bei der Feinarbeit geschrieben und gelegentlich aktualisiert wurden.

In der zweiten Jahreshälfte 2011 verzeichnete der Cyberfahnder monatlich rund 10.000 Besucher, die durchschnittlich etwa 30.000 Seiten aufriefen (▸ Aufstellung) und im Schnitt 2,8 Seiten je Besucher. Im ersten Quartal 2012 stiegen diese Zahlen deutlich an: Es kamen monatlich rund 13.000 Besucher, die knapp 55.000 Seiten aufriefen und im Durchschnitt 4,1 Seiten.

Über die Gründe dafür kann ich nur spekulieren, weil – wie üblich – Rückmeldungen rar sind. Auch für Aufregungen in der Netzgemeinde habe ich, anders als noch Anfang 2011 (▸ wirre Argumentation), nicht mehr gesorgt. Die jüngsten Zugriffszahlen zeigen nur eine verstärkte Popularität des Lexikons (▸ Index) und der aktuellen Meldungen (▸ Cyberfahnder im März 2012: 3 Rekorde). Die Feinarbeit am Layout, die bessere Lesbarkeit der Texte und ihre thematische Zusammenfassung könnten einen Anteil an dem vermehrten Seitenaufrufen haben, erklären aber die Besucherzahlen nicht schlüssig.

Vielleicht sind das Publikum und die Zeit einfach nur reif geworden, um einen Bedarf für den Cyberfahnder zu entwickeln. Das sage ich ohne jede Böswilligkeit und ohne Trauer. Böswillig werde ich nur, wenn es um Sachthemen geht (▸ Gebt mir den Ehrensold ! ▸ Wozu brauchst Du einen Bagger, wenn Du Dein Löffelchen has(s)t?). Dazu ist alles gesagt!



Downloads der Arbeitspapiere seit Juli 2011

Recht und Technik

Von Anfang an habe ich versucht, technische Prozesse in ihren Grundzügen und Ausprägungen zu begreifen, um mit diesem Wissen das Recht anzuwenden. Das gilt gleichermaßen für das materielle Cybercrime-Strafrecht und das Strafverfahrensrecht. Die ungewöhnliche Kombination meiner praktischen Erfahrungen aus den Bereichen der Wirtschaftsstrafsachen, des IT-Managements und schließlich der Organisierten Kriminalität hat das Herangehen an die grundsätzlichen Fragen gefördert und unterstützt.

Rechtsfragen sind immer zunächst an Tatsachen orientiert. Man muss kein Informatiker sein, um IT-Recht zu entwickeln, und kein Systemadministrator, um die Netzwerksicherheit zu verstehen und zu hinterfragen. Allgemeines technisches Verständnis und eine gewisse Neugier bedarf es hingegen schon. Dabei geht es nur darum, Technik in ihrer Funktion, ihren allgemeinen Grundlagen und Wirkungen zu verstehen, also quasi als Blackbox, deren Innenleben weniger interessiert als das, was sie nach Eingabe von Input als Output liefert. Nicht ohne Grund habe ich deshalb die Fragen nach den ▸ Angriffspunkten und nach den ▸ Grundstrukturen des Internets an den Anfang und immer wieder gestellt (▸ Netzkommunikation).

In den letzten Jahren hat die Polizei immer mehr Fachkommissariate für IuK-Ermittlungen aufgebaut. Erfolgreiche Ermittlungsarbeit zeigt sich aber nicht in Organigrammen, sondern verlangt nach fachkundigen Ermittlern, die auch die Freiräume haben, neue Fragen und Formen von Kriminalität zu erkunden. Das Betreten solcher Neuländer ist immer mit der Gefahr verbunden, Irrwege zu gehen, falsche Zwischenergebnisse zu erlangen und ineffektiv Zeit und Kraft zu verschwenden – gemessen an klassischen Fahndungserfolgen mit breitem Erfahrungshintergrund.

Nichts anderes habe ich erfahren, als ich mich in das Thema Skimming vertiefte. Meine verschiedenen Anläufe geben davon ein ▸ bewegtes Bild. Mit immer tieferem Eindringen in das Thema und auch wechselnden Einschätzungen – zuletzt wegen der Frage nach dem Geschädigten (▸ Skimming #3, S. 19) – habe ich ein Werk geschaffen, das alle wesentlichen Fragen löst und in vielen Grundsatzfragen vom BGH bestätigt wurde. Darüber bin ich stolz. Der Aufwand, den ich dafür aufbringen musste, ist hingegen auch nicht zu unterschätzen. Wer sich heute mit dem Thema beschäftigt, hat jedenfalls einen leichteren Einstieg, nachdem die Rechtsprechung die meisten Fragen gelöst hat.

Die gleichen Erfahrungen hat die Polizei gemacht, wenn sie etwa danach fragte, wie zum Beispiel Vouchers oder Kreditkarten auf Guthabenbasis, Carding-Boards, Abofallen oder erpresserische Trojaner funktionieren. Gemessen am Einzelfall sind dabei immer unangemessene Aufwände geleistet worden. Die daraus gewonnenen

Erkenntnisse und praktischen Erfahrungen sind jedoch unbezahlbar.

Diese Erfahrungen machen jetzt auch die Staatsanwaltschaften, die fast überall neue Dezernate und Abteilungen für die Strafverfolgung der IuK-Kriminalität aufbauen. Das war überfällig und nötig. Die großen Erfolge lassen noch auf sich warten, was nicht verwundert. Sie brauchen Vorlauf und Zeit, Polizei und Staatsanwaltschaften müssen erst noch eine gemeinsame Arbeitsbasis entwickeln und das Vorgehen muss erst noch standardisiert werden. Das kennt man auch aus anderen Spezialmaterien wie der Wirtschaftskriminalität, der Korruption, den Finanzermittlungen oder der Kinderpornographie.

Die zunehmende Professionalisierung der Strafverfolgung im Zusammenhang mit der IuK-Technik könnte der Grund dafür sein, dass der Cyberfahnder immer stärker nachgefragt wird. Das ist immerhin eine plausible Erklärung. Sie steht jedenfalls im Einklang mit der stetigen Nachfrage nach den oben genannten Skripten.

Fehlende Instrumente

Im Zusammenhang mit dem großen Lauschangriff hat das BVerfG eine geniale und einfache Faustformel entwickelt [1]: *Von der besonderen Schwere einer Straftat ... ist nur auszugehen, wenn sie der Gesetzgeber jedenfalls mit einer höheren Höchststrafe als fünf Jahre Freiheitsstrafe bewehrt hat.* An ihr muss sich auch die Strafverfolgung im Zusammenhang mit der Cybercrime orientieren, wenn es um die Frage geht, welche Ermittlungsmethoden angemessen und welche Grundrechtseingriffe mit welcher Tiefe zulässig sind.

Neben der akustischen Wohnraumüberwachung (▸ § 100c StPO, großer Lauschangriff) sind die Überwachung der Telekommunikation (▸ § 100a StPO) und die Onlinedurchsuchung die am schwersten wiegenden Eingriffsmaßnahmen. Die polizeirechtliche Onlinedurchsuchung hat das BVerfG 2008 kassiert [2] und die Vorratsdatenspeicherung (▸ § 100g StPO, ▸ §§ 113a, ▸ 113b TKG) im Jahr 2010 [3]. Unlängst hat es auch die Beauskunftung von Bestandsdaten auf der Grundlage von Verkehrsdaten beanstandet [4]. In keinem dieser Fälle hat das höchste Gericht aber gesagt, dass die geprüften Eingriffsmaßnahmen überhaupt nicht geschaffen werden dürfen, sondern es hat immer nur die Eingriffsvoraussetzungen und die begleitenden Verwertungsrechte, den Datenschutz und die Benachrichtigungspflichten beanstandet. Für die Bestandsdatenauskünfte gilt ungeachtet der jüngsten Entscheidung immer noch, dass sie von keinem Straftatenkatalog abhängig sind [5]. In der kritischen Öffentlichkeit werden jetzt vor Allem die Quellen-TKÜ und die stille SMS in Frage gestellt. Die Fragen danach, unter welchen Voraussetzungen welche Maßnahme überhaupt zulässig ist und gegen wen sie sich in der Praxis richten, werden dabei ausgeblendet und der Überwachungsstaat herbeigeredet, der jedermann bespitzelt.

Besonders die fehlenden Vorratsdaten werden sich noch schmerzlich auswirken, weil sie in vielen Fällen die Grundlage für die Bestandsdatenauskünfte bieten und deshalb Ermittlungen bereits im Keim verhindern. Dies gilt ganz besonders für die Verfolgung der Cybercrime, die meistens keine anderen Ansätze hat als eine elektronische Kommunikation und die dabei entstandenen Verkehrsdaten.

Alle genannten Eingriffsinstrumente haben ihren Sinn und werden benötigt. Sie sind Optionen und die Praxis muss in die Lage versetzt werden, mit ihnen in den geeigneten Fällen umzugehen. Geeignet heißt, dass die Zulässigkeitsvoraussetzungen vorliegen und sie im Einzelfall Erfolg versprechen. Meine Erfahrungen, auch bei der Verfolgung der Cybercrime, zeigen mir, dass immer eine Auswahl und Kombination verschiedener Ermittlungsmethoden notwendig ist, um zum Erfolg zu kommen. Nur selten ist es das eine Ermitt-

---

1 **BVerfG**, Urteil vom 03.03.2004 - 1 BvR 2378/97, 1 BvR 1084/99, Rn 238

2 **BVerfG**, Urteil vom 27.02.2008 - 1 BvR 370/07, 595/07

3 **BVerfG**, Urteil vom 02.03.2010 - 1 BvR 256, 263, 586/08

4 **CF**, Auskünfte über die Telekommunikation, 26.02.2012; BVerfG, Beschluss vom 24.01.2012- 1 BvR 1299/05.

5 **BVerfG**, Beschluss vom 13.11.2010 - 2 BvR 1124/10

lungsmittel, das den Täter überführt. Umgekehrt aber gilt: Wenn wichtige Instrumente fehlen, dann ist der Erfolg insgesamt in Frage gestellt.

Nicht nur damit werden die Cybercrime-Ermittler zu kämpfen haben, sondern vor Allem mit den Massenphänomenen. Im Zusammenhang mit Betrugsserien kommen schnell Hunderte, beim Skimming Tausend und bei Malware-Kampagnen schnell Tausende von Einzelfällen zusammen. Unter diesen Voraussetzungen können sie vor den administrativen Anforderungen scheitern, ohne überhaupt in die Nähe der Täter und Hinterleute zu gelangen. Das klassische Strafverfahrensrecht ist nicht auf Massenverfahren eingestellt. Das zeigen besonders die Bescheidungs- und Mitteilungspflichten am Beispiel der ▸ §§ 171, ▸ 101 Abs. 4 StPO, Nr 89 Abs. 3 und 101 Abs. 2 ▸ RiStBV.

Cyberfahnders Zukunft

Zum Jahresauftakt habe ich gesagt: ▸ Nichts versprechen, das aber halten! Daran werde ich vorerst festhalten.

Eine Alternative zum Cyberfahnder sehe ich nicht und ich glaube, dass die Strafverfolgung in diesem Bereich weiterhin einen Vor- und Querdenker braucht. Vielleicht gelingt es doch noch, eine einfachere Plattform einzurichten und einen breiteren Autorenstamm aufzubauen. Ein Programm wie der Cyberfahnder kann schnell scheitern, wenn es an nur einer Person hängt. Das ist zwar fünf Jahre lang gut gegangen, aber keine Garantie für die Zukunft.

In den Bereichen Skimming und Carding-Boards habe ich mich auch beruflich engagiert und zu den Erfahrungen der Strafverfolgung beigetragen. Wenn ich darüber hinaus auch einen Anteil daran gehabt haben sollte, dass die IuK-Strafverfolgung insgesamt etwas erfolgreicher geworden ist, bin ich schon ganz zufrieden.

In diesem Sinne:

Angenehme Ostern weiterhin!

Ihr Cyberfahnder

Hannover, 08.04.2012