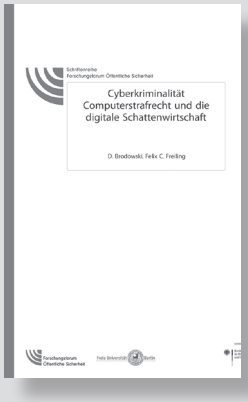
Eberhard Zehendner

Dominik Brodowski und Felix Freiling: „Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft“

Nicht selten würzen Darlegungen zum Thema *Cybercrime* eine dürftige Faktenlage mit spektakulären Fallbeschreibungen, Mutmaßungen und angsteinflößenden Bildern, die mit tatsächlichen Gefahren wenig zu tun haben. Ganz anders die von dem Rechtswissenschaftler Dominik Brodowski und dem IT-Sicherheitsexperten Felix Freiling gemeinsam verfasste, thematisch perfekt verzahnte Studie: Unaufgeregt, ohne die üblichen reißerischen Aufmacher und Übertreibungen, streng auf wissenschaftlicher Literatur und eigenen Erfahrungen der Autoren beruhend, so präsentiert sich das Werk, das klären, erklären, aufklären möchte – das Thema aus vielen Richtungen beleuchtend und mitunter keine leichte Kost.

Eingangs verdeutlichen die Autoren im amüsant geschriebenen Grundlagen-Kapitel *Informationstechnische Systeme,* das von Laien wie Experten mit Gewinn gelesen werden kann, fünf Prinzipien der Informationstechnik, die *im Zusammenspiel mit krimineller Energie die heutigen und vermutlich auch die zukünftigen Trends im Bereich der Cyberkriminalität erklären* könnten: *Automatisierbarkeit, Flüchtigkeit, räumliche Entgrenzung, Kopierbarkeit und Angreifbarkeit.* Sehr plastisch bedeutet z. B. räumliche Entgrenzung, *dass im Internet jeder eines jeden Nachbarn ist, man also nicht wie in der realen Welt versuchen kann, in einer »besonders sicheren Gegend« zu wohnen.* Überdies finden sich bereits in diesem Kapitel (unerwartet) programmatische Überlegungen, was sich schon im einleitenden Satz zeigt: *Ohne Zweifel ist die moderne Informationstechnologie ein wesentlicher Antrieb für neue Formen der Kriminalität.* Der aktuelle Zustand des *Cyberspace* wird als *mit all seinen Unsicherheiten zu einem gewissen Grad unvermeidbar* dargestellt, als historische Folge der technischen Rahmenbedingungen. Dass es *unmöglich ist, Software zu schreiben, die keine Fehler enthält,* und *unser Wissen über die prinzipiellen Ursachen und die Natur von Systemschwachstellen heute noch sehr gering* ist, kann dabei nicht oft genug betont werden.

Auf die *Unkundigkeit vieler Benutzer* und *unzureichende Erfahrung der gesamten Gesellschaft im Umgang mit vernetzten Computersystemen* gehen die Autoren anschließend bewusst nicht weiter ein, da sie die *Schwachstelle Benutzer* nicht als ursächlich ansehen. Wohl aber als problemverstärkend, denn der Wunsch nach immer mehr *Features* von Software führt typischerweise zu höherer Komplexität und damit zu mehr Schwachstellen. Ob in der Praxis tatsächlich *qualitativ kaum mehr ein Unterschied zwischen der Komplexität, die man von der realen Welt kennt, und der des Cyberspace besteht,* mag bezweifelt werden, doch die *Erkenntnis, dass es bei einer hinreichenden Komplexität des zugrunde liegenden informationstechnischen Systems im Cyberspace genauso wenig die spurenlose Straftat gibt wie in der realen Welt,* beleuchtet die Bedeutung der Computerforensik für die Strafverfolgung: Der Cyberspace, obwohl vielfach als virtuell verstanden, ist *schlussendlich doch wieder Teil der realen Welt;* Handlungen im Cyberspace können *auf Handlungen in der realen Welt zurückgeführt werden,* was *die rechtliche Erfassung und forensische Auswertung von Straftaten im Internet* ermöglicht.



Dominik Brodowski und Felix C. Freiling:
Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft.
Schriftenreihe Sicherheit, Nr. 4.
Berlin: Freie Universität Berlin, Forschungsforum Öffentliche Sicherheit, 2011.
ISBN 978-3-929619-66-9
Kartoniert, 222 Seiten

Bestellung und Download:
www.sicherheit-forschung.de/publikationen/schriftenreihe/
Liegt z. B. unter *www.sicherheit-forschung.de/publikationen/schriftenreihe/sr_v_v/sr_4.pdf*

Im Kapitel *Cyberkriminalität und Computerstrafrecht als ungeklärte Begriffe* führen die Autoren sodann aus, dass Begriffe wie *Cyberkriminalität, Computerkriminalität, Computerstrafrecht* oder *Internetstrafrecht* in der deutschen Strafrechtsordnung gesetzlich nicht definiert sind, im Recht der Europäischen Union uneinheitlich (und außerhalb juristischer Fragestellungen regelmäßig unpräzise) verwendet werden und daher erst zu erschließen sind. Denn mit diesen Begriffen muss ein weites Feld von Konstellationen erfasst werden, in denen die Verwendung informationstechnischer Systeme das Strafrecht vor neue Herausforderungen stellt. Aus dem Blickwinkel der Rechtswissenschaft werden informationstechnische Systeme einerseits als Mittel zur Vorbereitung oder Begehung herkömmlicher Straftaten betrachtet. Computer- und Internetdelikte im engeren Sinne (Ausspähen und Abfangen von Daten, Computersabotage, Computerbetrug u. a. m.) sehen informationstechnische Systeme dagegen als (unmittelbares) Angriffsobjekt vor, auch wenn die Strafnormen mittelbar Zwecken wie dem Vermögens- oder Geheimnisschutz dienen.

Die Informatik interessiert sich mehr für die Rolle der Technik als für die Begehungsmodalität; nicht scharf, aber für die Strafverfolgung nützlich, wird technikorientierte von menschenorientierter Cyberkriminalität unterschieden. *Technikorientierte* Cyberkriminalität (u. a. Phishing, Computersabotage, Datenmanipulation,

Botnetze) benutzt Schadsoftware und korrespondiert weitgehend zur Begehungsmodalität des Computers als Angriffsobjekt, obwohl teilweise auch Social-Engineering-Angriffe darunter fallen. *Menschenorientierte* Cyberkriminalität (wie Cyberstalking oder eBay-Betrug) basiert auf technisch unterstützter Kommunikation zwischen Menschen und entspricht eher dem Computer als Begehungsmittel, was *kriminalistisches Gespür* erfordert und der traditionellen Ausbildung vieler Strafverfolger entgegenkommt. In der Informatik ausgebildete IT-Sicherheitsexperten können ihre Stärken dagegen besser gegen technikorientierte Cyberkriminalität einsetzen. Die Autoren vertreten daher die Auffassung, dass es zur Bekämpfung technik- wie menschenorientierter Cyberkriminalität erforderlich ist, die Strafverfolgungsakteure (unterschiedlich gewichtet) sowohl sozial-kriminalistisch als auch technisch-kriminalistisch adäquat auszubilden.

Für ihr Werk wählen die Autoren nun eine (im juristischen Sinne) materielle Sichtweise: Cyberkriminalität wird verstanden als *alle sozialethisch erheblich zu missbilligenden, sozialschädlichen Verhaltensweisen, die verfassungskonform unter Strafe gestellt sind oder unter Strafe gestellt werden könnten, und die entweder als Angriffsobjekt oder als Begehungsmittel informationstechnische Systeme einsetzen; Computerstrafrecht als Oberbegriff für alle Aspekte des Straf- und Strafprozessrechts, welche eine Cyberkriminalität betreffende Strafdrohung anordnen und durchzusetzen versuchen.* Dies lenkt den Blick auch auf zukünftig erst noch als Delikt zu verstehende Praktiken sowie daran angepasste Methoden der Ermittlung und Strafverfolgung – einschließlich einer Bewertung von Sinnhaftigkeit, Nutzen und Risiken bestehender Strafnormen und zukünftiger Veränderungen. Verfassungsrechtliche Grenzen des materiellen wie auch des prozessualen Computerstrafrechts sowie mögliche Regelungsmodelle des Öffentlichen, Zivil- und Strafrechts zur Steuerung von Cyberkriminalität werden ausführlich im Kapitel *Cyberkriminalität: Verfassungsrecht, Regelungsmodelle und Alternativen* diskutiert.

Durch immer stärkere Nutzung des Cyberspace für bereits vorher übliche Aktivitäten treten darauf bezogene *klassische* Delikte wie Betrug oder Erpressung nun auch (in entsprechender Form und häufig vergrößerter Dimension) als Cyberkriminalität auf. Hinzugekommen sind aber auch qualitativ neue Delikte, die typisch für den Cyberspace sind, aus den dort veränderten Rahmenbedingungen resultieren und mit spezifischen technischen und juristischen Mitteln verfolgt werden müssen. Im Kapitel *Von klassischer Kriminalität zur Cyberkriminalität* werden diese Entwicklungen nachgezeichnet und damit verbundene Herausforderungen eng auf die eingangs erwähnten fünf Prinzipien der Informationstechnik bezogen erklärt. Hinsichtlich der Täter, der Cyberkriminellen, über die es insgesamt wenig gesicherte Erkenntnisse zu geben scheint, interessieren die Autoren sich vorwiegend für solche mit finanziellen Motiven und charakterisieren diese im spannenden Kapitel *Wertschöpfungsprozesse, Akteure, Schäden.* Die Tätergruppen zu klassischen Delikten scheinen beim Übergang ins Internet unverändert, IT-Sicherheitsvorfälle in Unternehmen und Behörden häufig von in deren Bereich Beschäftigten verursacht. Darüber hinaus fallen neben einer zunehmenden Zahl von Einzeltätern, die ohne besondere Kenntnisse mit frei im Netz verfügbaren Angriffswerkzeugen Straftaten im Netz begehen, vor allem weltweit vernetzte kriminelle Gruppen auf, die in ihrer Gesamtheit durch den Begriff *Schattenwirtschaft* zutreffend beschrieben werden, deren Organisationsformen sich aber stark von denen der klassischen organisierten Kriminalität unterscheiden. Im weiteren Verlauf des Kapitels werden Mechanismen der Arbeitsteilung und Wertschöpfung dieser Schattenwirtschaft sowie daraus entstehende Schäden prinzipiell dargestellt sowie an Beispielen verdeutlicht. Als wichtige Schlussfolgerung erscheint das individuell, in der Öffentlichkeit und auch in Institutionen bestehende Bild von Cyberkriminalität verzerrt, da von Überschätzung der Relevanz einzelner Tatbestände und gleichzeitig (durch hohe Dunkelziffern) einer Unterschätzung des Gesamtproblems geprägt.

Um Verunsicherung und Hilflosigkeit nicht unnötig Raum zu geben, beantworten die Autoren nun in einem umfangreichen handlungsorientierten Teil der Studie die Frage: *Was kann jeder Einzelne, was kann jedes Unternehmen und was kann Deutschland tun, um der Cyberkriminalität wirksam entgegen zu treten?* Im Kapitel *Schutz »im Kleinen«: Selbstschutz und nationale Strafverfolgung* stellen sie dazu eine Vielzahl möglicher Maßnahmen des technischen und organisatorischen Selbstschutzes für Privatpersonen, Unternehmen und Behörden dar – die allerdings intensiver umgesetzt werden müssten. Das deutsche Straf- und Strafprozessrecht scheint – rechtlich gesehen – gut gerüstet zur Verfolgung der meisten Delikte von Cyberkriminalität, bei den Strafverfolgungsbehörden bestehen diesbezüglich aber noch Defizite hinsichtlich Qualifizierung und Rekrutierung. Da Cyberkriminalität häufig auch Staatsgrenzen überschreitet, wird im Kapitel *Schutz »im Großen«: Strafverfolgung und Transnationalität* deren internationale Dimension betrachtet. Neben zahlreichen positiven Beispielen informeller internationaler Kooperation wird die (weltweite!) Bedeutung der Cybercrime-Konvention des Europarats für die internationale Harmonisierung des Strafrechts hervorgehoben. Dagegen werfen extraterritoriale Strafverfolgung und internationale justizielle Zusammenarbeit in Strafsachen eine Reihe bisher ungelöster Probleme auf.

Wer sich einen schnellen Überblick über die Ergebnisse der Studie verschaffen möchte, sei auf das Kapitel *Handlungsempfehlungen: Neun Thesen* verwiesen. Ein umfangreiches Literaturverzeichnis unterstützt das Nachprüfen getroffener Feststellungen sowie das Weiterlesen und Vertiefen zu einzelnen Fragestellungen; auch auf Ausgespartes wird kompetent weiterverwiesen. Und noch eine angenehme Überraschung: Das Werk kann kostenlos im Internet heruntergeladen werden. Die gedruckte Ausgabe ist gegen Portokostenersatz erhältlich.

Eberhard Zehendner

Eberhard Zehendner ist Professor für Technische Informatik an der Friedrich-Schiller-Universität Jena, wo er u. a. im Bereich *Informatik & Gesellschaft* lehrt. Seit 2013 gehört er dem FIfF-Vorstand an.