Schriftenreihe Sicherheit

CYBERKRIMINALITÄT, COMPUTERSTRAFRECHT UND DIE DIGITALE SCHATTENWIRTSCHAFT

Kurzfassung

Cyberkriminalität umgibt in der öffentlichen Diskussion eine Aura des Geheimnisvollen und Konspirativen. Es ist die Rede von „rechtsfreien Räumen“, von „omnipotenten Hackern“ und von der Machtlosigkeit der Nationalstaaten, auf diese neuartigen Kriminalitätsformen zu reagieren. Als Basis für eine sachliche Diskussion dieses Themenkomplexes wurde im Auftrag des Forschungsforums Öffentliche Sicherheit die Expertise „Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft“ von Rechtswissenschaftler Dominik Brodowski, LL.M. (UPenn), Eberhard Karls Universität Tübingen, und Informatikprofessor Felix C. Freiling, Friedrich-Alexander-Universität Erlangen-Nürnberg erstellt.

ENTMYSTIFIZIERUNG DER CYBERKRIMINALITÄT

Der Begriff „Cyberkriminalität“ bezeichnet vereinfacht gesprochen diejenige Kriminalität, die im Cyberspace stattfindet. Im Cyberspace herrschen durch die Automatisierbarkeit von Aktivitäten, die perfekte Kopierbarkeit digitaler Informationen, die Flüchtigkeit von Daten und die räumliche Entgrenzung von Berechnungen andere Spielregeln als in der realen Welt, so dass die Gesellschaft und vor allem die Strafverfolgungsbehörden vor neue Herausforderungen gestellt werden. Einerseits werden alte Kriminalitätsformen in den Cyberspace verlagert, andererseits entstehen hierdurch auch neuartige Kriminalitätsformen. Folglich kann man Cyberkriminalität grob in zwei Bereiche unterteilen, je nachdem, ob Informationstechnologie als Begehungsmittel (z.B. Internet-Betrügereien oder Urheberrechtsverletzungen) oder als Angriffsobjekt (z.B. bei Hacking-Vorfällen, Spam und Botnetzen) fungiert.

Dennoch: *Cyberkriminalität* ist so etwas Besonderes nicht. Wie auch bei sonstiger Kriminalität scheint die massenhaft begangene, mit jeweils nur geringen Schäden verbundene *leichtere bis mittlere Kriminalität* zu dominieren; nur vereinzelt sind schwerere Straftaten zu verzeichnen. Cyberkriminalität verfolgt zumeist *ökonomische Motive*, was viele Anknüpfungspunkte hin zu einer effektiven Verfolgung und Minimierung der Cyberkriminalität eröffnet. Diese ökonomisch motivierte Cyberkriminalität zeichnet sich aus durch eine *ausdifferenzierte Arbeitsteilung* und einen *hohen Grad an Organisation*. Es gibt allerdings keine wissenschaftlichen Belege dafür, dass es engere Verbindungen zwischen der traditionellen organisierten Kriminalität (etwa im Bereich Drogen- oder Menschenhandel) und der sich eher flüchtig und kurzfristig organisierenden Cyberkriminalität gibt.

Das drängendste Problem ist die unzureichende Kenntnis, die unzureichende kriminologische Erforschung der Cyberkriminalität. Dieses *Dunkelfeld* gilt es aufzuhellen, denn anekdotisches Wissen über Cyberkriminalität und über mutmaßliche Erfolge einzelner Ermittlungsmethoden reicht nicht aus, um angemessen auf Cyberkriminalität zu reagieren.

Schutz „im Kleinen": Selbstschutz und nationale Strafverfolgung

Die *technischen Möglichkeiten*, die jeder Einzelne ergreifen kann, um Cyberkriminellen ihr Handwerk zu erschweren, sind zwar allgemein bekannt. Doch Cyberkriminalität ist kein rein technisches Problem. Es fehlen Anreize, in sichere IT-Systeme zu investieren. Es fehlt eine adäquate Wahrnehmung, wie wichtig eine sichere IT-Infrastruktur ist. Dafür ist es notwendig, dass jeder Einzelne, auch zuhause, seine Computer gegen Cyberkriminalität absichert.

Wo andere *Regelungsmodelle des Zivil- und des Polizeirechts* scheitern, kann der Einsatz des Strafrechts erforderlich werden. Das deutsche Straf- und Strafprozessrecht bietet dabei einen weitgehend ausreichenden und auch angemessenen Rahmen zur Verfolgung von Cyberkriminalität. Nahezu sämtliche Verhaltensweisen der Cyberkriminalität, die eine strafrechtliche Sanktion erfordern, werden bereits durch mindestens einen Straftatbestand erfasst. Auch das strafprozessuale Instrumentarium ist – insbesondere bei Berücksichtigung der weitgehenden, teilweise noch unerforschten *forensischen Möglichkeiten* – ebenfalls auf gutem Stand.

Gleichwohl ergibt sich *Korrekturbedarf*: Aus rechtlicher Sicht ist etwa die Finanzierung der Kinderpornographie, das Phishing und das Skimming zielgerichteter als bisher zu verfolgen und juristisch tragfähige Grundlagen für eine Quellen-Telekommunikationsüberwachung sowie für eine Bestandsdatenabfrage anzustreben.

Schutz „im Großen": Strafverfolgung und Transnationalität

Cyberkriminalität überwindet räumliche Grenzen in Windeseile. Dem treten erstens höchst erfolgreiche, *informelle, internationale Kooperationen* der Praxis entgegen, etwa von Forschungsverbünden, von Unternehmen und auch von Internetprovidern (INHOPE).

Zweitens bestehen weitreichende rechtliche Möglichkeiten für die Strafverfolgungsbehörden, eng und schnell zur Verfolgung von Cyberkriminalität zusammenzuarbeiten. Insoweit ist das G8-Kontaktstellennetz hervorzuheben, aber auch der *informelle, spontane Austausch* von Erkenntnissen und ermittlungsrelevanten Informationen über Ländergrenzen hinweg.

Drittens bieten auch neuartige Instrumente der *Rechtshilfe in Strafsachen* zwischen den Mitgliedsstaaten der Europäischen Union weitreichende Möglichkeiten für eine transnationale Beweisgewinnung, wenn auch die Praxis diese Chancen zum Teil noch nicht hinreichend wahrnimmt.

HANDLUNGSEMPFEHLUNGEN: NEUN THESEN

1. Ein sicheres Internet beginnt mit jedem Einzelnen.

Eine Vielzahl von Gefahren im Internet entsteht durch unzureichend geschützte Rechner, durch unsicheres Verhalten im Netz und durch unsicheres Verhalten an lokalen Arbeitsplatzrechnern. Dem gilt es durch sicherheitsbewusstes Verhalten und durch das Ergreifen technischer Maßnahmen entgegenzuwirken.

2. Es fehlen verlässliche kriminologische Daten über die Bedrohungslage durch Cyberkriminalität in Deutschland und Europa.

Cyberkriminalität ist in der Regel ökonomisch motivierte Kriminalität. Sie reicht dabei von der kostenlosen Nutzung urheberrechtlich geschützter Musik und Filme über Betrügereien bis hin zur Verwertung fremder Betriebsgeheimnisse durch Industriespionage. Hinzu treten die Verbreitung von kinderpornographischen und sonstigen verwerflichen, inkriminierten Schriften, aber auch Beleidigungen und die Nutzung des Internets zur Kommunikation unter Terroristen.

Eine Betrachtung des Umfangs und der Schäden der Cyberkriminalität wird allerdings durch verschiedene Faktoren erschwert, insbesondere durch das nur unzureichend analysierte Dunkel-

feld. Eine evidenzbasierte Kriminalpolitik erfordert eine hinreichend verlässliche Datengrundlage, die dringend zu schaffen ist.

3. Soweit der technische Schutz reicht, ist rechtlicher Schutz nicht nötig.
Wo sich Angriffsmöglichkeiten für Cyberkriminelle reduzieren oder gänzlich vermeiden lassen, lässt sich auch Cyberkriminalität reduzieren oder ganz vermeiden. Daher ist es dringend erforderlich, den technischen Schutz von Hard- und insbesondere Software zu erhöhen. Hoch entwickelte Gesellschaften sind in erheblichem Maße auf sichere Informationstechnik angewiesen.

Dennoch: der technische Schutz kann nicht perfekt sein, insbesondere nicht gegen gezielte Angriffe; ein Restrisiko für Cyberkriminalität wird stets bestehen bleiben. Die damit verbundenen Risiken lassen sich reduzieren, sofern man sensible Bereiche – etwa der Steuerung von Industrieanlagen und von kritischer Infrastruktur – komplett vom Internet entkoppelt.

4. Das Internet ist kein rechtsfreier Raum.
Das Internet ist kein eigener Raum, sondern nur ein Kommunikationsnetz zwischen Endpunkten, die sich im physischen Raum befinden. Daraus ergibt sich auch eine Vielzahl von Anknüpfungspunkten für das Strafrecht. Aufgrund harmonisierter Straftatbestände kann Cyberkriminalität auch in vielen Staaten der Welt angemessen strafrechtlich geahndet werden.

5. Das deutsche Strafrecht ist gut aufgestellt zur Verfolgung von Cyberkriminalität.
Die im deutschen Strafgesetzbuch und in weiteren Gesetzen zu findenden Strafbestimmungen sind weitestgehend ausreichend und adäquat zur Verfolgung von Cyberkriminalität. Die wenigen verbliebenen Schutzlücken lassen sich durch behutsame Korrekturen korrigieren.

6. Die forensischen und praktischen Möglichkeiten zur Verfolgung von Cyberkriminalität werden unterschätzt; sie gilt es fruchtbar zu machen.
Auch Cyberkriminelle machen Fehler. Sie hinterlassen also unvermeidlich Spuren ihrer Taten. Die Auswertung dieser digitalen Spuren – die digitale Forensik – ist noch nicht hinreichend erschlossen. Forschung in diesem Gebiet, auch im Bereich offensiver Techniken, gilt es ebenso zu fördern wie die Ausbildung von Experten in digitaler Forensik zu stärken.

7. Die prozessualen Möglichkeiten zur Verfolgung von Cyberkriminalität sind besser als ihr Ruf.
Das deutsche Strafprozessrecht ist gut aufgestellt zur Verfolgung von Cyberkriminalität. Insbesondere bei ökonomisch motivierter Kriminalität bieten sich mehrere Ansätze zu einer effektiven Verfolgung und Minimierung. Drei Schwächen des Strafprozessrechts sollten aber beschleunigt korrigiert werden: So ist eine Bestandsdatenabfrage wenigstens für eine gewisse Zeit, aber nicht notwendigerweise für 6 Monate zu ermöglichen, so ist der strafprozessuale Zugriff auf E-Mail-Kommunikation einheitlich und adäquat zu gestatten, und so ist die derzeit den Ermittlungsbehörden nicht gestattete Quellen-Telekommunikationsüberwachung auf eine juristisch tragfähige Grundlage zu stellen.

8. Internationale Kooperationen zur Verfolgung von Cyberkriminalität sind erfolgversprechend.
Flexible internationale Kooperationen zur Verfolgung von Cyberkriminalität sind ein Erfolgsmodell. Diese reichen vom Verbund der European Government CERTs über Kontaktstellennetze der G8, des Europarats und der Europäischen Union hin zu informellen Kontakten von Strafverfolgern, welche dieselben Cyberkriminellen verfolgen. Ein reger internationaler Informationsaustausch zwischen Strafverfolgungsbehörden erweist sich dabei als ausgesprochen nützlich; ob hierbei die Beschuldigtenrechte und die Belange von Drittbetroffenen ausreichend geschützt werden, muss zukünftige Forschung erst zeigen.

9. Die Staatengemeinschaft ist nicht machtlos gegenüber der Cyberkriminalität.
Durch effektive Nutzung der forensischen und praktischen Möglichkeiten zur Verfolgung von Cyberkriminalität, durch die Stärkung informeller und formeller Kooperationen zwischen privaten Akteuren und zwischen Strafverfolgern, und durch eine Harmonisierung der Strafbestimmungen ist es den Staaten möglich, effektiv gegen ökonomisch motivierte Cyberkriminalität und auch gegen weitere Formen der Cyberkriminalität vorzugehen.

Allerdings ist es erforderlich, mit einer gewissen Kontrollreduktion über Inhalte umgehen zu lernen. Das heißt für Staaten und Unternehmen, auf eine veränderte „interessierte Öffentlichkeit" zu reagieren und von sich aus die demokratische Teilhabe zu fördern. Das heißt für Künstler und Unternehmen, adäquate, leicht bedienbare Angebote zum Erwerb urheberrechtlich geschützter Werke anzubieten. Das heißt für Eltern, ihre Kinder im Umgang mit dem Internet, mit sozialen Netzwerken und den Medien angemessen zu erziehen. Und es bedeutet auch, dass die vom Staat vermittelte Werteordnung sich neu orientieren muss: Weg von einer freien „Verfügbarkeit von Daten", hin zu einer Datensparsamkeit. Der Staat muss seinen Bürgern vorleben, dass Daten schützenswert sind, und dass sparsam mit Daten umzugehen ist. Um dieses den Bürgern zu vermitteln, sollte der Staat selbst mehr Respekt vor den Daten der Bürger zeigen. Respekt zeigen bedeutet hier auch, nicht alle Eingriffe, die denkbar und verfassungsgemäß wären, auch umzusetzen, sondern dem Bürger auch über das verfassungsrechtlich gebotene Minimum hinaus Freiräume und Freiheiten zu belassen.

Ansprechpartner: Dr. Lars Gerhold
Wissenschaftlicher Koordinator Forschungsforum Öffentliche Sicherheit

---

Dominik Brodowski, Felix C. Freiling (2011):
Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft
ISBN: 978-3-929619-66-9
Die Vollversion der Studie ist erhältlich unter www.schriftenreihe-sicherheit.de

---

Das 2009 an der Freien Universität Berlin gegründete Forschungsforum Öffentliche Sicherheit (www.sicherheit-forschung.de) führt Forschung unterschiedlicher Disziplinen zu sicherheitsrelevanten Themen zusammen und trägt dazu bei, zukünftig relevante Forschungsthemen zu identifizieren. Hauptsächlich geschieht dies durch Workshops und Expertisen zu verschiedenen Facetten der Sicherheitsforschung. Ziel ist es, wissenschaftliche Handlungsempfehlungen aus diesem heterogenen Feld zu generieren und für Politik, Industrie, und Organisationen der Sicherheit zugänglich zu machen. Die Idee zu diesem Projekt entstand auf Anregung des am Bundestag gegründeten Zukunftsforums Öffentliche Sicherheit e.V., dem Abgeordnete aller Parteien sowie Stakeholder aus Behörden, Wirtschaft und Wissenschaft angehören.

Forschungsforum Öffentliche Sicherheit
Freie Universität Berlin
GEFÖRDERT VOM Bundesministerium für Bildung und Forschung

Impressum:
Forschungsforum
Öffentliche Sicherheit
Freie Universität Berlin
Fabeckstr. 15, 14195 Berlin
Tel: +49 (0)30 838 57367
Fax: +49 (0)30 838 57399
www.schriftenreihe-sicherheit.de
kontakt@schriftenreihe-sicherheit.de