Alexander Nemzov: Strafbarkeit von Online-Blockaden und DDoS-Angriffen vor und nach dem Inkrafttreten des 41. Strafrechtsänderungsgesetzes unter Berücksichtigung von verfassungsrechtlichen und europarechtlichen Vorgaben

von Prof. Dr. Anja Schiemann

2017, Dr. Kovač, Hamburg, ISBN: 978-3-8300-9507-1, S. 271, Euro 99,80.

Die Dissertation untersucht, inwieweit das deutsche Strafrecht vor und nach der Novelle des Computerstrafrechts (41. Strafrechtsänderungsgesetz vom 7.8.2007) gegen diverse Formen der Online-Blockaden und DDoS-Attacken gewappnet ist. Dabei betrifft die erste Konstellation der Online-Blockade die Fälle, in denen Tausende von Nutzern die zu blockierende Seite gleichzeitig aufrufen, um den Server zum Absturz zu bringen. Die zweite Konstellation umfasst die Fälle, in denen ein einzelner Angreifer mit Hilfe von gekaperten oder infizierten Fremdrechnern die nötige Anfragenflut auf die Homepage produziert, um letztlich ebenfalls den angegriffenen Webserver zu überlasten und damit zu blockieren.

Zunächst wird in der Arbeit der historische und internationale Kontext virtueller Proteste geschildert und der technische Hintergrund dargestellt. Auf rund 40 Seiten werden dann die einschlägigen Grundrechte untersucht. Dabei scheitert nach Ansicht des Verfassers der Schutz der Versammlungsfreiheit für Online-Blockaden an zwei Faktoren. Zum einen hätten die Teilnehmer keinen Überblick über die anderen Teilnehmer, so dass ihre innere Verbundenheit nicht gewährleistet sei. Zum anderen fände die Versammlung auf einem fremden Server und nicht im öffentlichen Raum statt.

Hinsichtlich der Meinungsfreiheit sieht der Autor den Aufruf zur Internetblockade vom Schutzbereich des Art. 5 Abs. 1 GG gedeckt. Zur Frage, ob die Grenzen der Schranke nach Art. 5 Abs. 2 GG überschritten seien, verweist er auf die spätere strafrechtliche Prüfung. Dagegen sei die Informationsfreiheit nicht tangiert, da es den Betroffenen ja gerade darum gehe, ihren Protest zu artikulieren und nicht, sich zu informieren. Schließlich stellt der Verfasser fest, dass eine Internetseite Rundfunk i.S. von Art. 5 Abs.1 S. 2 GG darstellt und insofern ein dort veröffentlichter Aufruf zur Internetblockade in den Schutzbereich der Rundfunkfreiheit fällt. Da ein Aufruf zur Online-Demo über eine Internetseite vom Schutzbereich des Art. 5 Abs. 1 GG gedeckt sei, bedürfe ein Eingriff einer Rechtfertigung, die aber durch eine verfassungsgemäße Strafnorm gegeben wäre. Zudem sei eine Online-Demo auch von dem Schutzbereich des Art. 2 Abs. 1 GG erfasst, jedoch kann dieser durch die verfassungsmäßige Ordnung und die Rechte anderer regelmäßig eingeschränkt werden.

Den Schwerpunkt der Dissertation bildet sodann die strafrechtliche Beurteilung einer DDoS-Attacke oder politisch motivierten Online-Blockade (S. 65-247). Das Hauptziel liegt in einer Überprüfung des 41. Strafrechtsänderungsgesetzes auf seine Praxistauglichkeit. Hierfür wird zunächst der Rechtszustand vor der Gesetzesnovellierung ausführlich und kritisch analysiert. Der Verfasser kommt zu dem Ergebnis, dass die strafrechtliche Sanktionierung vor der Novellierung defizitär war. Online-Blockaden waren strafrechtlich schwer zu fassen, da diese sowohl den Datenbestand als auch die stoffliche Integrität des angegriffenen Servers unverändert lassen, so dass §§ 303a und 303b StGB weitgehend leerliefen. Lediglich beim Tatbestandsmerkmal des Unterdrückens von Daten gem. § 303a StGB bestand ein Anknüpfungspunkt für die Strafbarkeit, allerdings schloss zumindest das *OLG Frankfurt a.M.* diesen Tatbestand bei kurzfristigen Online-Blockaden aus (MMR 2006, 557). Diese Strafbarkeitslücke kann nach eingehender Untersuchung durch den Verfasser nur zu einem geringen Teil von § 240 StGB geschlossen werden. Die Drohungsalternative des Nötigungstatbestandes kann bei Online-Blockaden oder DDoS-Angriffen dann erfüllt sein, wenn diese mit einer ausdrücklichen oder konkludenten Ankündigung weiterer solcher Angriffe verbunden wäre, falls das Anliegen der Täter nicht erfüllt wird. Die Verwerflichkeitsklausel sei aber erst dann überwunden, wenn es sich um erpresserische, auf finanziellen Gewinn gerichtete Aktionen handele. Bei rein politisch motivierten Blockaden müssten im Rahmen der Verwerflichkeitsklausel noch die Umstände der Aktion berücksichtigt werden. Zusammengefasst werden diese ausführlich hergeleiteten Ergebnisse in einer übersichtlichen Tabelle (S. 159 f.), die dem Leser sehr schnell die Schwachstellen der Regelungen vor Inkrafttreten des 41. Strafrechtsänderungsgesetzes vor Augen führt.

Im Anschluss daran wird die Rechtslage nach Inkrafttreten des 41. Strafrechtsänderungsgesetzes geschildert (S. 163 ff.). Hierzu werden zunächst die internationalen Grundlagen erörtert, d.h. die Vorgaben der Convention of Cybercrime, der Rahmenbeschluss des Rates der Europäischen Union über Angriffe auf Informationssysteme vom 24.02.2005 und die Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12.8.2013 über Angriffe auf Informationssysteme vorgestellt. Dies führt dann zu einem ersten Überblick über die gesetzlichen Neuregelungen bzw. Ergänzungen des StGB:

- § 202a StGB (teilweise Änderung des Schutzzweckes und Einführung der Strafbarkeit des bloßen „Hackings“
- § 202b StGB (Neueinfügung der Strafbarkeit des Abfangens von Daten)

- § 202c StGB (Neueinfügung der Strafbarkeit von Vorbereitungshandlungen zu §§ 202a und 202b StGB)
- 303a StGB (Ergänzung um Abs. 3 unter Verweis auf § 202c StGB)
- § 303b StGB (Erweiterung des Schutzgutes sowie der erfassten Tathandlungen).

Der Verfasser kommt zu dem Ergebnis, dass auch nach der neuen Fassung des § 202a StGB Handlungen im Vorfeld einer Internetblockade nur im Einzelfall strafbar sind. Weder die Installation der „Agents" noch das Anbieten oder Sichverschaffen einer zugriffsverstärkenden Software würden eine Strafbarkeit begründen. Einziger Anknüpfungspunkt sei eine noch weiter ins Vorfeld reichende Vorbereitungshandlung wie die Infiltration fremder Rechner mit Trojanern oder der Einsatz eines Exploits. Allerdings räumt der Autor ein, dass diese Fälle nur schwer nachweisbar sein werden und zudem nur dann vorliegen, wenn zum einen der Datenbestand gegen Fremdzugriff gesichert und zum anderen die Person, die den fremden Rechner infiltriert und später den Agenten installiert, identisch ist. Eine Strafbarkeit nach § 202a StGB ist demnach von vielen Eventualitäten abhängig und wohl in der Regel zu verneinen.

Dagegen erfasse der neu geschaffene § 202c StGB den Fall, dass bei der Installation der Agent-Software gleichzeitig das Hacking des fremden Computersystems erfolgt, also wenn die Agent-Software im Trojaner selbst enthalten ist. Der Täter, der die Agents ohne Zuhilfenahme anderer Schadsoftware auf einem fremden Rechner installiere, bleibe dagegen straffrei. Eine Strafbarkeit nach § 303b StGB wird auch für die meisten Fallkonstellationen verneint und nur bei Vorbereitungshandlungen von DDoS-Attacken angenommen, sofern eine erhebliche Schädigung gegeben ist.

Diese nach wie vor bestehenden Strafbarkeitslücken lassen für den Autor nur den folgerichtigen Schluss zu, dass die Reform in großen Teilen misslungen ist, soweit sie das Ziel verfolgte, Online-Blockaden zu erfassen (S. 207). Trotz des ausdrücklichen gesetzgeberischen Willens, mit § 303b Abs. 1 Nr. 2 StGB n.F. DDoS-Angriffe zu sanktionieren, ist dies in den meisten Konstellationen nicht der Fall und die Konsequenzen der Neuformulierung weitreichend. Denn anstatt bestehende Lücken zu schließen, würden sich Auslegungsprobleme ergeben, die zu erhöhter Rechtsunsicherheit führten. Auch wenn man im Gegensatz zur Auffassung des Verfassers eine weite Auslegung im Rahmen des § 303b StGB bevorzugen würde, so blieben eine ganze Reihe von Strafbarkeitslücken. Den Grund verortet der Autor im Festhalten des Gesetzgebers an überkommenen gesetzlichen Strukturen, die weder zur technischen Realität noch zu den europarechtlichen Vorgaben passen würden. Vor allem durch das Festhalten am Datenbegriff des § 202a StGB werde die Chance vertan, nicht nur die DDoS-Angriffe eindeutig zu erfassen, sondern auch die Streitfrage beizulegen, ob denn nur dauerhaft gespeicherte Daten in den Schutzbereich der §§ 303a, 303b StGB fallen oder auch Daten im temporären Arbeitsspeicher. Der Schutzbereich wäre ungleich größer, wenn man es bei einer schlichten Bezugnahme auf „Daten" unter dem Hinweis auf die europarechtlichen Grundlagen belassen hätte. Dann würden nämlich auch Daten im flüchtigen Arbeitsspeicher unstreitig vom Schutzbereich der §§ 303a, 303b StGB erfasst.
Dadurch, dass der Datenbegriff nicht erweitert wurde, bleibe es jedoch bei einer Anwendung des § 303a StGB, der aber auch nur in geringem Umfang zum Zuge komme. Auch für § 202a StGB gelte das zuvor Gesagte, das nämlich die enge Anlehnung an die europarechtlichen Grundlagen und ein Loslösen von überkommenen Gesetzesstrukturen zu einer deutlich besseren Gesetzeswirkung geführt hätte. So aber würden die Schwächen der alten Fassung in die neue Fassung überführt.

Letztlich sieht der Verfasser in § 240 StGB die in der Praxis vor und nach den Gesetzesänderungen durch das 41. Strafrechtsänderungsgesetz am leichtesten anwendbare und umsetzbare Vorschrift im Hinblick auf DDoS-Angriffe und Online-Demonstrationen (S. 215). Hilfreich ist am Ende dieser ernüchternden Gesamtbewertung der Gesetzesnovellierung wiederum die tabellarische Übersicht mit einer Zusammenstellung der – sehr überschaubaren – Strafbarkeitsrisiken im Zusammenhang mit Online-Blockaden und DDoS-Attacken (S. 217 f.).

Schließlich wird noch ein Exkurs auf die Mittäterschaftsproblematik bei Online-Demonstrationen gelenkt (S. 219 ff.). Im Ergebnis kommt der Verfasser zu dem logischen Schluss, dass eine Mittäterschaft der einzelnen Demonstranten nicht in Betracht kommt. Sie wären damit lediglich Teilnehmer, wobei sich im Rahmen der Akzessorietät die Frage nach dem Haupttäter stellt. Da ein solcher in der Regel mangels Verwirklichung der einschlägigen Straftatbestände nicht identifiziert werden kann, scheitere auch eine Strafbarkeit wegen Teilnahme (S. 241).

Insofern kommt der Autor zu dem unbefriedigenden Fazit, dass es der deutsche Gesetzgeber nicht geschafft hat, wenigstens die internationalen Vorgaben für die strafrechtliche Erfassung der den Untersuchungsgegenstand betreffenden Taten so umzusetzen, dass eine eindeutige Grundlage für die Strafverfolgung geschaffen wird. Ganz im Gegenteil werden trotz Reformbemühungen die Phänomene der Internetkriminalität nach wie vor nicht vollständig erfasst. Auch Lösungswege werden im Rahmen der Dissertation angerissen. Neben der „radikalen" Lösung einer Abschaffung des Schutzgutes wird die Einführung eines „Einheitstäters" bei speziellen Internetdelikten gefordert. Zudem sollte die systemwidrige Verweisung in §§ 303a und 303b StGB auf den Datenbegriff des § 202a StGB aufgegeben werden, um auch Daten im temporären Arbeitsspeicher zweifellos zu erfassen. Darüber hinaus macht der Verfasser explizite de lege ferenda Vorschläge (S. 252), um hier Strafbarkeitslücken zu schließen und DDoS-Angriffe und exzessive Online-Blockaden strafrechtlich zu erfassen.

Die Dissertation liefert ein anschauliches Beispiel dafür, wie ambitionierte Gesetzgebung leerläuft und nicht das bewirkt, was sie bewirken sollte. Sie zeigt, dass das deutsche Computerstrafrecht Stückwerk ist und durch die Einfügungen und Änderungen in bestehende materiell-strafrechtliche Gesetzessystematik die Chance verpasst wird, mit den neuen Facetten der Internetkriminalität Schritt zu halten. Insofern tut eine Neujustierung der Straftatbestände mit Cybercrime-Bezug im deutschen Strafgesetzbuch Not, die mit Mut zu Neuem, alte Straftatbestände auflöst und Cybercrime neu denkt und sanktioniert. Nur dann kann der gute Wille des Gesetzgebers, Strafbarkeitslücken sinnvoll zu schließen, aufgehen. Zahllose Ergänzungen führen zu dem faden Beigeschmack, keine wirkliche Neuerung herbeizuführen. Jedenfalls – so zeigt auch die Dissertation plastisch auf – kann durch marginale Änderungen und losen Einfügungen kein stimmiges Gesamtbild entstehen. Es wird Zeit, dass im Zuge einer digitalen Agenda das Strafgesetzbuch überarbeitet und im digitalen Zeitalter neu aufgestellt wird.