



Ministerium der Justiz Nordrhein-Westfalen, 40190 Düsseldorf

Seite 1 von 1

Herrn Vorsitzenden
des Rechtsausschusses
des Landtags Nordrhein-Westfalen
Dr. Werner Pfeil MdL
40221 Düsseldorf

LANDTAG
NORDRHEIN-WESTFALEN
17. WAHLPERIODE

VORLAGE
17/908

A14, A09, A20

10.07.2018

Aktenzeichen
4100 - III. 274
bei Antwort bitte angeben

Bearbeiter: Herr Dr. Greier
Telefon: 0211 8792-204

nachrichtlich

Rechtsausschuss des Landtags
- Referat I 1 -
40221 Düsseldorf

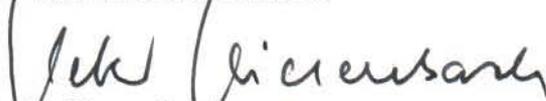
17. Sitzung des Rechtsausschusses am 04.07.2018

Öffentlicher Bericht der Landesregierung zu dem Tagesordnungspunkt
6: "Stärkung der Möglichkeiten zur Strafverfolgung von Straftaten im
Cyberraum"

Sehr geehrter Herr Vorsitzender,

als Anlage übersende ich den öffentlichen Bericht der Landesregierung
zu dem o. g. Tagesordnungspunkt zur Weiterleitung an die Mitglieder
des Rechtsausschusses.

Mit freundlichen Grüßen


Peter Biesenbach

Dienstgebäude und
Lieferanschrift:
Martin-Luther-Platz 40
40212 Düsseldorf
Telefon: 0211 8792-0
Telefax: 0211 8792-456
poststelle@jm.nrw.de
www.justiz.nrw



**Ministerium der Justiz
des Landes Nordrhein-Westfalen**

17. Sitzung des Rechtsausschusses
des Landtags Nordrhein-Westfalen
am 4. Juli 2018

Schriftlicher Bericht zu TOP 6:

„Stärkung der Möglichkeiten zur Strafverfolgung
von Straftaten im Cyberraum“

Mit dem vorliegenden Bericht der Landesregierung erfolgt die in der 10. Sitzung des Rechtsausschusses vom 18. April 2018 erbetene Unterrichtung zu dem vorbezeichneten Tagesordnungspunkt.

I.

Die in dem Beschlussantrag dargestellte zunehmende Bedeutung der Cyberkriminalität lässt sich anhand der Zahlen aus den polizeilichen Lagebildern nachvollziehen:

- Das Lagebild Cybercrime des Landeskriminalamtes Nordrhein-Westfalen zeigt für das Jahr 2016 einen Anstieg der Cyberkriminalität um 36,4% auf 22.708 Fälle.
- Aus dem Lagebild des Bundeskriminalamtes für das Jahr 2016 ergibt sich ein Anstieg um 80,5% auf 82.649 Fälle, insbesondere bedingt durch die hohe Verfahrenszahl bei Computerbetrug im Sinne des § 263a StGB. Darüber hinaus erfasste das Bundeskriminalamt im Jahr 2016 insgesamt 253.290 Fälle, in denen die Tat mittels Internet begangen wurde.

Steigende Fallzahlen zeigen auch die Studien von Wirtschaftsberatungsunternehmen und Branchenverbänden. Die Cyberkriminalität stellt sich insgesamt als ein transnationales Phänomen dar, bei dem sich aufgrund der arbeitsteiligen Vorgehensweise das Täterspektrum zunehmend erweitert.

II.

Vor diesem Hintergrund einerseits sowie der Bedeutung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme andererseits bedarf es zur effektiven Bekämpfung von Cybercrime vereinheitlichter, klar definierter und mit allen grundrechtssichernden Verfahrensregelungen ausgestatteter Eingriffsnormen und den technischen Gegebenheiten angepasster Straftatbestände.

1.

In diesem Zusammenhang erscheint die Schaffung eines Straftatbestands erforderlich, der nicht nur Datenveränderung und Computersabotage, sondern auch die unbefugte Nutzung von bzw. den unbefugten Zugang zu informationstechnischen Systemen, z. B. durch den Betrieb von Botnetzen, unter Strafe stellt. Aus Gründen der Verhältnismäßigkeit kommt dabei einer Begrenzung der Strafbarkeit auf ausgesuchte, besonders strafwürdige Konstellationen besondere Bedeutung zu. Eine Strafbarkeit sollte daher beschränkt werden etwa auf Fälle der gewerbs- oder bandenmäßigen Begehung, der Verschaffung eines Zugangs zu einer großen Anzahl informationstechnischer Systeme oder einem Handeln in der Absicht, Einrichtungen der kritischen Infrastruktur zu beeinträchtigen.

2.

Vermeehrt nutzen Straftäter zudem die Möglichkeiten der Anonymisierung, die ihnen das Internet bietet. Eine häufig genutzte Form der Anonymisierung erfolgt über das »The Onion Router« (Tor)-Netzwerk, das aus einer Vielzahl von weltweit verteilten Servern besteht, über die Datenpakete in ständig wechselnder Form geleitet werden. Beim Verbindungsaufbau wird durch das Programm eine zufällige Route über einen Teil der Server festgelegt, ohne dass Herkunft oder Ziel der Daten protokolliert werden. Durch die Verschlüsselung der Nutzerdaten und die dynamische Routenwahl wird die Feststellung von Anfangs- und Endpunkten eines Datentransfers erheblich erschwert. Insbesondere über das Tor-Netzwerk erfolgt der Zugang zum sogenannten Darknet. Zugang und Erreichbarkeit der Darknet-Angebote sind durch das Erfordernis besonderer Programme, wie des Tor-Browsers, beschränkt.

Die Angebote im Darknet umfassen neben Foren für Whistleblower oder Chatrooms für politisch Verfolgte in autoritär geführten Staaten auch Inhalte bekannter Servicebetreiber. Ebenso finden sich jedoch Angebote mit strafrechtlicher Relevanz, darunter Handel mit Betäubungsmitteln, Kinderpornographie oder Waffen, mit Schadsoftware und Ausweispapieren. Vergleichbare Angebote finden sich auch in weiteren Teilen des Internets. In technischer Hinsicht entsprechen die angebotenen Dienste denen bekannter Online-Handelsplattformen mit Vorschaubildern der angebotenen Waren, Werbung, Bewertungen für Verkäufer und Hinweisen auf weitere möglicherweise für einen Nutzer interessante Angebote. Das Kriminalitätsphänomen gewinnt in der Praxis der Strafverfolgung zunehmend an Gewicht und beschränkt sich dabei nicht auf wenige Einzelfälle. Aufgrund des ständigen Auftretens neuer Angebote und der auf Verschleierung angelegten Vorgehensweise liegen keine genauen Daten über die Anzahl einschlägiger Foren vor. Die Zentralstellen der Staatsanwaltschaften für die Verfolgung von Cybercrime der Länder haben in den vergangenen Jahren jedoch bereits zahlreiche Ermittlungsverfahren gegen die Verantwortlichen einschlägiger Foren oder Plattformen und deren Nutzer geführt. Das dort betriebene Geschäftsmodell des „*Cybercrime-as-a-Service*“ wird in der kriminellen Szene weiter ausgebaut.

Die Erfahrungen aus den geführten Ermittlungsverfahren lassen ein arbeitsteiliges Zusammenwirken von Plattformbetreibern und Nutzern der Plattform, also sowohl Händlern als auch Käufern, erkennen. Es zeigt sich zudem, dass die klassischen Organisationsdelikte und die historischen gesetzgeberischen Vorstellungen von Täterschaft und Teilnahme auf moderne, internetbasierte Täterstrukturen kaum übertragbar sind. Die Betreiber selbst stellen lediglich eine - in einigen Fällen vollautomatisierte - technische Infrastruktur zur Verfügung. Aufgrund dieser Umstände ist eine Beihilfehandlung zu einer konkreten Haupttat in der Praxis nur schwer erweislich. Auch die Zurechnung von Einzeltaten unter dem Gesichtspunkt einer bandenmäßigen Tatbegehung ist häufig nicht möglich, da in der Regel kriminelle Foren und Marktplätze der Underground Economy in amorphen Organisationsstrukturen jenseits des überkommenen Bandenbegriffs geführt werden.

3.

Den besonderen Gefahren der Cyberkriminalität und der Bedeutung informationstechnischer Systeme im täglichen Leben wird das geltende Recht nur bedingt gerecht. Die Tatbestände des Ausspähens von Daten (§ 202a StGB), des Abfangens von Daten (§ 202b StGB) und der Datenhehlerei (§ 202d StGB) weisen Höchststrafdrohungen auf, die unter denen etwa eines Diebstahls geringwertiger Sachen (§ 248a StGB) liegt. Auch für massenhaft begangene Delikte oder bei schweren Folgen sieht das Gesetz derzeit keine Qualifikationstatbestände oder strafschärfenden Regelbeispiele vor. Die Datenveränderung (§ 303a StGB) erfüllt nur bei Hinzutreten weiterer Umstände den Tatbestand der Computersabotage i. S. d. § 303b StGB, der dann eine leicht erhöhte Strafdrohung vorsieht. Die Qualifikationstatbestände der Computersabotage gemäß § 303b Absatz 2 StGB und die Regelbeispiele des § 303b Absatz 4 StGB gelten nicht für Taten gegen Privatpersonen.

4.

Ermittlungen wegen Taten aus dem Bereich des Cybercrime, deren Begehungsmodalitäten auf die Nutzung moderner Kommunikationsmethoden ausgerichtet sind, können zudem ohne Eröffnung technischer Ermittlungsmöglichkeiten kaum erfolgreich geführt werden. Aufgrund der praktischen Erfahrungen in den einschlägigen Ermittlungsverfahren befürwortet daher auch die Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW) die Ausweitung des Deliktskatalogs des § 100a StPO auf Taten, die dem Bereich der schweren Kriminalität zuzuordnen sind.

5.

Ein weiteres Anliegen der Praxis ist die Verbesserung der grenzüberschreitenden Zugriffsmöglichkeiten auf elektronische Beweismittel. Hierzu hat die EU-Kommission am 17. April 2018 Entwürfe für zwei Rechtsakte vorgelegt, die eine effektive und schnelle Sicherung von elektronischen Beweismitteln sowie einen grenzüberschreitenden Zugriff auf diese ermöglichen sollen. Ziel ist es, alle Internetdienstleister, die ihre Dienste innerhalb der EU anbieten, im Wege einer Richtlinie zu verpflichten, Zustellungsbevollmächtigte für Sicherungs- und Auskunftersuchen bezüglich elektronischer Beweismittel in Strafsachen zu benennen. Zugleich sieht der Entwurf einer Verordnung für die Ermittlungsbehörden bzw. die Strafgerichte die Möglichkeit vor, die Internetdienstleister zur vorläufigen Sicherung von Daten bzw. zu deren Herausgabe binnen kurzer Fristen zu verpflichten. Die Missachtung dieser Pflichten soll sanktioniert werden. Angesichts der wachsenden Bedeutung grenzüberschreitender Sicherung elektronischer Beweismittel sind die Vorschläge der Kommission grundsätzlich zu begrüßen. Bei den anstehenden Verhandlungen über die Ausgestaltung konkreter Einzelfragen gilt es, besonderes Augenmerk auf die Wahrung grundrechtskonformer Verfahrensstandards zu legen.

III.

Schließlich bedarf es auch im Bereich präventiv polizeilicher Maßnahmen der Schaffung klar definierter und mit allen grundrechtssichernden Verfahrensregelungen versehener Eingriffsnormen für eine effiziente Gefahrenabwehr im Cyberraum. Insbesondere eine Ermächtigungsgrundlage für die Störung von IT-Geräten im Falle eines drohenden oder erfolgten Angriffs auf inländische Einrichtungen kritischer Infrastrukturen wäre daher zu befürworten. Damit könnte eine sichere Rechtsgrundlage für Maßnahmen wie die gezielte Netztrennung des verursachenden Systems, das Ausschalten zentraler Server von Botnetzen oder das Senden eines Stopp-Befehls über den eine Störung kontrollierenden Steuerserver geschaffen werden.