Bundesrat **Drucksache** **242/20**

13.05.20

Antrag
des Freistaates Bayern

Entschließung des Bundesrates „Für einen effektiven strafrechtlichen Schutz von kritischen Infrastrukturen gegen Cyberangriffe“

Der Bayerische Ministerpräsident München, 13. Mai 2020

An den
Präsidenten des Bundesrates
Herrn Ministerpräsidenten
Dr. Dietmar Woidke

Sehr geehrter Herr Präsident,

gemäß dem Beschluss der Bayerischen Staatsregierung wird die als Anlage beigefügte

> Entschließung des Bundesrates „Für einen effektiven strafrechtlichen Schutz von kritischen Infrastrukturen gegen Cyberangriffe“

mit dem Antrag übermittelt, dass der Bundesrat diese fassen möge.

Es wird gebeten, die Vorlage gemäß § 36 Absatz 2 GO BR auf die Tagesordnung der 989. Sitzung am 15. Mai 2020 zu setzen und anschließend den zuständigen Ausschüssen zur Beratung zuzuweisen.

Mit freundlichen Grüßen
Dr. Markus Söder

Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln
Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0720-2946

Entschließung des Bundesrates

„Für einen effektiven strafrechtlichen Schutz von kritischen Infrastrukturen gegen Cyberangriffe“

Angesichts besonders gefährlicher und verwerflicher Cyberattacken auf kritische Infrastrukturen in der Corona-Krise muss auch das Cyber-Strafrecht besser aufgestellt werden, damit derartige kriminelle Handlungen konsequent geahndet werden können.

Mitten in der sich ausbreitenden Corona-Pandemie legte im März 2020 ein Cyberangriff den Betrieb eines Krankenhauses in der tschechischen Stadt Brünn lahm, welches eines der größten Corona-Testlabore des Landes betreibt. Die IT-Sicherheitsorganisationen von Bund und Ländern beobachten eine Zunahme von Cyberangriffen mit Bezug zum Corona-Virus. Solche Angriffe auf Krankenhäuser oder andere Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen können zu erheblichen Störungen der öffentlichen Sicherheit und des öffentlichen Lebens, zu Versorgungsengpässen oder zu anderen dramatischen Folgen führen und im Extremfall – etwa beim Ausfall von Beatmungsgeräten – sogar den Verlust von Menschenleben fordern.

Um dieser wachsenden Bedrohungslage entgegenzuwirken, müssen weitere gesetzgeberische Schritte unternommen werden, damit die für solche Angriffe verantwortlichen Täter zügig ermittelt und schuldangemessen bestraft werden können. Dies ist gerade auch in der aktuellen Krisensituation dringend geboten – nicht zuletzt um andere potentielle Täter abzuschrecken, Menschenleben zu schützen und die Funktionsfähigkeit des staatlichen Gemeinwesens aufrechtzuerhalten.

1. Vor diesem Hintergrund hat sich der Bundesrat mit der wachsenden Bedrohung durch Cyberangriffe auf kritische Infrastrukturen, insbesondere auf Krankenhäuser, Atomkraftwerke, Telekommunikationsnetze, Flughäfen oder andere Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, befasst. Solche Cyberangriffe können zu erheblichen Störungen der öffentlichen Sicherheit und des öffentlichen Lebens, zu Versorgungsengpässen oder zu

anderen dramatischen Folgen führen und im Extremfall sogar den Verlust von Menschenleben fordern.

2. Der Bundesrat stellt fest, dass das derzeitige materielle Strafrecht insbesondere für Fälle von schwerwiegenden Cyberangriffen auf kritische Infrastrukturen mit gravierenden Folgen nicht durchweg ausreichend schuld- und tatangemessene Sanktionen ermöglicht, um andere potentielle Täter abzuschrecken und dadurch die Gesellschaft und das Funktionieren des staatlichen Gemeinwesens zu schützen.

3. Der Bundesrat stellt weiter fest, dass das derzeitige Strafprozessrecht den Strafverfolgungsbehörden in Fällen von Cyberangriffen auf kritische Infrastrukturen nicht durchweg die notwendigen technischen Ermittlungsbefugnisse einräumt, um die Täter zu ermitteln und vor einem Gericht zur Verantwortung ziehen zu können.

4. Der Bundesrat fordert daher das Bundesministerium der Justiz und für Verbraucherschutz auf, den gesetzgeberischen Handlungsbedarf in Strafgesetzbuch und Strafprozessordnung in Bezug auf einen effektiven strafrechtlichen Schutz von kritischen Infrastrukturen zu prüfen und den erforderlichen gesetzgeberischen Vorschlag zeitnah vorzulegen.

Begründung:

Mitten in der sich ausbreitenden Corona-Pandemie legte im März 2020 ein Cyberangriff den Betrieb eines Krankenhauses in der tschechischen Stadt Brünn lahm. Das Krankenhaus betreibt eines der größten Corona-Testlabore des Landes. Dem Krankenhausleiter zufolge wird es Wochen dauern, den vollen Betrieb wieder herzustellen. Cyberangriffe auf Krankenhäuser oder andere kritische Infrastrukturen, bei denen teilweise auch Verschlüsselungstrojaner (sog. Ransomware) in die IT-Infrastruktur einschleust werden, sind längst keine Seltenheit mehr. Auch ein Klinikum in Fürth wurde im Dezember 2019 Opfer eines Angriffs auf das IT-System, wodurch der Betrieb stark eingeschränkt wurde. Angriffe dieser Art können verheerende Folgen haben und erlangen in der aktuellen Krisensituation eine besondere Brisanz. Die Bedeutung der ungestörten, garantierten Funktionsfähigkeit der IT-Strukturen, insbesondere von Krankenhäusern sowie gerade auch den Einrichtungen der kommunalen Daseinsvorsorge (insbesondere Strom- und Wasserversorgung), darf nicht unterschätzt werden. Das Gemeinwesen kann sich die Verwundbarkeit dieser kritischen Infrastrukturen durch Cyberangriffe in Fällen einer Pandemie nicht leisten, denn es steht der Verlust von Menschenleben zu befürchten.

Hier ist es auch Aufgabe des Strafrechts, die für solche Angriffe verantwortlichen Personen zügig zu ermitteln und schuldangemessen zu bestrafen - nicht zuletzt um andere potentielle Täter abzuschrecken, die Gesellschaft und Menschenleben zu schützen und das Vertrauen in die staatliche Handlungsfähigkeit zu erhalten. Diese Aufgabe, die sich in Zeiten der Corona-Krise umso dringlicher stellt, kann das Strafrecht derzeit jedoch nur bedingt erfüllen.

Der materiell-strafrechtliche Schutz von Einrichtungen kritischer Infrastrukturen vor Delikten aus dem Phänomenbereich der Cyberkriminalität, der gegenwärtig im Wesentlichen durch die §§ 202a ff., 303a f. StGB gewährt wird, ist unzureichend. Kritische Infrastrukturen sind nach der allgemeinen Definition der KRITIS-Strategie der Bundesregierung "Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden". Damit sind nicht nur die Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen erfasst, sondern auch die Sektoren Staat und Verwaltung sowie Medien und Kultur. Kritische Infrastrukturen können also zum Beispiel nicht nur Krankenhäuser, Kernkraftwerke, Flughäfen oder Banken, sondern auch Regierungs-, Verwaltungs- oder Justizbehörden, der Deutsche Bundestag oder Rundfunkeinrichtungen sein. Diese Infrastrukturen sind besonders schutzwürdig, da sie aufgrund der fortschreitenden Digitalisierung in hohem Maße und gerade in Zeiten einer krisenhaften Zuspitzung wie in einer Pandemie auf informationstechnische Systeme angewiesen sind und unberechtigte Zugriffe auf diese Systeme schwerwiegende Folgen auch für die Allgemeinheit haben können.

Der Bedeutung dieser kritischen Infrastrukturen wird die aktuelle Rechtslage nicht gerecht. Dies zeigt sich an den im unteren Bereich angesiedelten Strafrahmen und den fehlenden Qualifikationstatbeständen, Regelbespielen und Erfolgsqualifikationen. Gerade für Cyberangriffe auf kritische Infrastrukturen im Besonderen bedeutet dies, dass es keine erhöhten Strafdrohungen (mit Ausnahme der Computersabotage nach § 303b StGB) gibt. Damit kann auf diese schwerwiegenden Taten mit einem gesteigerten Unrechtsgehalt auch in der derzeitigen Lage der besonderen Verwundbarkeit von kritischer Infrastruktur nicht tat- und schuldangemessen reagiert werden. Konkret gibt es z.B. keine Erfolgsqualifikation für den Fall, dass der Täter durch eine Computersabotage wenigstens leichtfertig den Tod oder eine schwere Gesundheitsschädigung eines anderen Menschen verursacht (etwa weil lebenserhaltende Geräte wie Beatmungsmaschinen in einem Krankenhaus ausfallen). Angesichts der schweren Tatfolgen ist beim Verlust von Menschenleben und bei schweren Gesundheitsschädigungen eine im Mindestmaß erhöhte Strafdrohung unbedingt erforderlich und auch sachgerecht, um eine schuldangemessene Bestrafung zu gewährleisten und general- wie spezialpräventiven Strafbedürfnissen gerecht zu werden.

Ferner macht die Strafverfolgungspraxis seit Jahren nachdrücklich geltend, dass die Täter, die es mit ihren Taten auf kritische Infrastrukturen und damit indirekt auf Menschenleben abgesehen haben, derzeit nicht mit Erfolgsaussichten ermittelt werden können und hat Änderungen im Strafprozessrecht angemahnt. Beim Verdacht einer Straftat nach den §§ 202a ff., 303a f. StGB können die Täter häufig nicht ermittelt und überführt werden, weil den Strafverfolgungsbehörden die strafprozessualen Befugnisse für erfolgversprechende Ermittlungen in der digitalen Welt nicht oder nur eingeschränkt zur Verfügung stehen. So ist eine Überwachung der Telekommunikation in Form der „Serverüberwachung“ oder eine Online-Durchsuchung zur Identifizierung der Täter, zur Aufhellung der verwendeten Infrastruktur und zum Führen des Tatnachweises mangels Vorliegens einer Katalogtat nach § 100a Absatz 2 bzw. § 100b Absatz 2 StPO derzeit rechtlich nicht zulässig. Die Erhebung von Verkehrsdaten ist de lege lata nur eingeschränkt nach § 100g Absatz 1 Satz 1 Nummer 2 StPO zulässig, mangels Vorliegens einer Katalogtat aber nicht nach § 100g Absatz 1 Satz 1 Nummer 1 oder § 100g Absatz 2 StPO. Diese technischen Ermittlungsmaßnahmen stellen aber oftmals den einzig erfolgversprechenden Ermittlungsansatz dar, da die Delikte der Cyberkriminalität in den allermeisten Fällen auch oder ausschließlich unter Zuhilfenahme von Telekommunikationsdiensten begangen werden.

Angesichts dieser Analyse, die einen offensichtlichen Handlungsbedarf zeigt, sollten die notwendigen gesetzgeberischen Schritte im Bundesrecht, für die bereits zahlreiche Vorschläge vorliegen, zeitnah ergriffen werden. Das zuständige Bundesministerium der Justiz und für Verbraucherschutz soll insofern vom Bundesrat aufgefordert werden, den gesetzgeberischen Handlungsbedarf in Bezug auf einen effektiven strafrechtlichen Schutz von kritischen Infrastrukturen zu prüfen und den erforderlichen gesetzgeberischen Vorschlag zeitnah vorzulegen, um so ein entsprechendes Signal zum Schutz der kritischen Infrastrukturen zu setzen.