20. Wahlperiode

Drucksache **20/6432**

HESSISCHER LANDTAG

10. 01. 2022

Kleine Anfrage

Stefan Müller (Freie Demokraten) vom 23.09.2021

„Cybercrime“ – Teil I

und

Antwort

Minister des Innern und für Sport

Vorbemerkung Fragesteller:

Daten- bzw. Cybersicherheit nimmt in den vergangenen Jahren weiter an Bedeutung zu, insbesondere vor dem Hintergrund, dass vermehrt Straftaten im digitalen Bereich erfolgen ("Cybercrime"). So verdeutlicht auch der Fünf-Jahres-Vergleich der Kriminalitätsstatistik, dass die Anzahl der erfassten Straftaten in diesem Bereich grundsätzlich steigt. Ebenso zeigen aktuelle polizeiliche Erkenntnisse und Unternehmensbefragungen, dass die deutsche Wirtschaft in einem hohen Maße von Internetkriminalität betroffen ist. Die Situation hat sich in den letzten Jahren weiter verschärft, weil die Art der Angriffe komplexer und vielfältiger geworden ist. Verdeutlicht wird dies auch durch die Auskunft des hessischen Innenministeriums, wonach 2019 insgesamt 177 Fälle von Anfragen nach Beratung und Unterstützung bei "Hessen3C" gestellt wurden, im vergangenen Jahr 920 Anfragen und in diesem Jahr 972 Anfragen, darunter 55 von kleinen und mittelständischen Unternehmen. Die wirtschaftlichen Schäden durch solche Taten sind für die Betroffenen teilweise immens. Auch deswegen ist neben präventiven Maßnahmen eine effektive Strafverfolgung im Bereich "Cybercrime" dringend notwendig.

Vorbemerkung Minister des Innern und für Sport:

Das Land richtet sein konzeptionelles Handeln gegen „Cybercrime“ an der bundesweit abgestimmten „Polizeilichen Bekämpfungsstrategie Cybercrime“ aus.

Im April 2019 wurde das Hessen CyberCompetenceCenter (Hessen3C) eröffnet, das in enger Zusammenarbeit mit Polizei und Verfassungsschutz die Cyber-Sicherheitslage analysiert, entsprechende Lagebilder erstellt, zu IT-Sicherheitsschwachstellen informiert und vor akuten Cyber-Bedrohungslagen warnt. Durch die Bündelung der fachlichen Expertise der hessischen Sicherheitsbehörden und der IT-Spezialisten des Hessen3C wurde eine Sicherheitsarchitektur geschaffen, mit der den dynamischen Herausforderungen der Cyberkriminalität zielgerichtet begegnet wird.

Die polizeiliche Bekämpfungsstrategie Cybercrime setzt den Handlungsrahmen für eine starke und nachdrückliche Prävention, Aufklärung und Verfolgung von Cybercrime. Im engen Verbund mit anderen staatlichen Akteuren trägt die hessische Polizei dazu bei, die Sicherheit im Internet und in Datennetzen zu erhöhen und das Vertrauen der Bevölkerung in Funktionsfähigkeit und Datenintegrität des Cyberraums zu stärken. Die Bekämpfung von Cybercrime wird als gesamtpolizeiliche Aufgabe wahrgenommen.

Unter Cybercrime im engeren Sinne verstehen die Sicherheitsbehörden in erster Linie Straftaten, die sich unmittelbar gegen die Infrastruktur des Internets, Datennetze, IT-Systeme oder dort gespeicherte Daten richten. Hierunter fallen z.B. das Ausspähen und Abfangen von Daten mittels Schadsoftware (Viren, Würmer, Trojanische Pferde), die betrügerische Manipulation von Überweisungen im Online-Banking oder die Computersabotage mittels sogenannter DDoS-Angriffe.

Darüber hinaus haben seit vielen Jahren Straftäter das Internet für eine Vielzahl von Delikten als ideales Tatmittel entdeckt und ihre Tatbegehungsweisen permanent angepasst. Das gilt in erster Linie insbesondere für vielfältige Betrugsvarianten. Experten sprechen in diesem Zusammenhang auch von Cybercrime im weiteren Sinne.

Eine effektive Strafverfolgung ist integraler Bestandteil von Cybersicherheit. Zwischen der Polizei und der Justiz in Hessen findet hier eine intensive und mittlerweile vielfach bewährte und erfolgreiche Zusammenarbeit, insbesondere mit der Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität (ZIT) der Generalstaatsanwaltschaft Frankfurt am Main, statt. Als operative Zentralstelle bearbeitet die ZIT besonders aufwendige und umfangreiche Ermittlungsverfahren aus den Deliktsbereichen Kinderpornographie und sexuellem Missbrauch von Kinder mit

Eingegangen am 10. Januar 2022 · Bearbeitet am 10. Januar 2022 · Ausgegeben am 13. Januar 2022
Herstellung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden · www.Hessischer-Landtag.de

Bezug zum Internet, Darknet-Kriminalität (Bekämpfung krimineller Plattformen sowie des Handels mit Waffen, Drogen und Fälschungsgütern) und Cyberkriminalität im engeren Sinne (Hackerangriffe, Datendiebstahl und Computerbetrug). Außerdem ist die ZIT hessenweit zuständig für Hass und Hetze im Internet und nimmt bundesweit Meldungen von Hatespeech im Rahmen der Kooperation #KeineMachtdemHass und der App MeldeHelden entgegen.

Die Hessische Landesregierung ist sich der großen Aufgabe einer wirksamen Strafverfolgung auch im digitalen Raum bewusst und forcierte in den letzten Jahren die Verstärkung der ZIT. Es wurden daher mit dem Haushalt 2020 zehn zusätzliche Stellen geschaffen, so dass die ZIT heute über 22 Staatsanwältinnen und Staatsanwälte verfügt. Die großen Ermittlungserfolge der ZIT (z. B. im Verfahren zur Zerschlagung der Infrastruktur der Emotet-Schadsoftware) und ihrer Vorreiterrolle in Deutschland beruhen auch auf der guten personellen Ausstattung.

Das HLKA führt im Auftrag der Staatsanwaltschaften Ermittlungen durch und bewältigt kriminalistische Herausforderungen in diesem Phänomenbereich gemeinsam mit anderen Landeskriminalämtern und dem Bundeskriminalamt. Es findet ein regelmäßiger nationaler und internationaler Informationsaustausch sowie Wissenstransfer statt. Internationale, bundesweite und länderübergreifende Fallbearbeitungen kommen verstärkt zum Einsatz. Die hessische Polizei nutzt und entwickelt innovative Bekämpfungsmethoden in den Bereichen Ermittlungen, Auswertung und Analyse durch den Einsatz und die Fortentwicklung moderner IT. Hierzu trägt unter anderem der Innovation Hub 110 mit Sitz in Frankfurt am Main bei.

Bei konkreten Cyber-Angriffen unterstützt und berät Hessen3C die Landesverwaltung, die hessischen Kommunen sowie die hessischen kleinen und mittleren Unternehmen (KMU). Ein Hauptaugenmerk der IT-Spezialisten des Hessen3C liegt auf dem Schutz der Kritischen Infrastruktur. Als zentrale Ansprechstelle stehen die Experten den Unternehmen, die der Kritischen Infrastruktur zugeordnet werden und der Wirtschaft jederzeit rund um die Uhr zur Verfügung. Mit einem Mobile Incident Response Team (MIRT) unterstützt Hessen3C bei Bedarf landesweit vor Ort. Die Spezialisten helfen bei der Analyse, dem IT-Krisenmanagement und der Schadensbegrenzung und führen im Einzelfall auch digitalforensische Datensicherungen durch. Darüber hinaus stehen Experten für Fachvorträge und Awareness-Veranstaltungen auf Anfrage kostenlos zur Verfügung.

Die Entwicklung der Cybersicherheitslage wird fortlaufend beobachtet, Cyberbedrohungen werden analysiert und notwendige Maßnahmen entsprechend umgesetzt.

Auch die Präventionsarbeit in diesem Phänomenbereich wird fortlaufend intensiviert. Die verschiedenen Adressaten werden mit phänomenologisch aktuellen und zielgruppenorientierten Präventionsaktivitäten und -maßnahmen erreicht.

Mit den in allen Polizeipräsidien und dem HLKA eingerichteten Fachkommissariaten für „Cybercrime im engeren Sinne“, den Fachberaterinnen/Fachberatern für Cybercrime-Prävention, der Zentralen Ansprechstelle Cybercrime (ZAC) im HLKA, IT-Fachpersonal und Forensikern, dem Innovation Hub 110, Hessen3C sowie der ZIT ist Hessen insgesamt sehr gut im Bereich der Internetkriminalität aufgestellt.

Diese Vorbemerkungen vorangestellt, beantworte ich die Kleine Anfrage wie folgt:

Frage 1. Im Hessischen Landeskriminalamt wurde ein Fachkommissariat zur Bekämpfung von Cyberkriminalität eingerichtet. Wie viele Mitarbeiterinnen und Mitarbeiter gibt es beim HLKA im Bereich "Cybercrime" (bitte aufschlüsseln nach Aufgabenbereichen)?

Im Hessischen Landeskriminalamt ist die Thematik „Cybercrime im engeren Sinne“ in einem Hauptsachgebiet verortet. Hierunter werden Straftaten gefasst, die sich gegen das Internet, weitere Datennetze, informationstechnische Systeme oder deren Daten richten.

Der Bereich zur Bekämpfung von Cyberkriminalität setzt sich aus den folgenden Sachgebieten zusammen:

- 1. Sachgebiet:
  Aufgabenmanagement und Zentrale Ansprechstelle Cybercrime für die Wirtschaft (ZAC)
- 2. Sachgebiet:
  Technische Ermittlungsunterstützung, OSINT-Recherchen, Recherchen in Datennetzen
- 3. Sachgebiet:
  Ermittlungen in herausragenden Verfahren von Cybercrime im engeren Sinne und Bearbeitung der Ersuchen i. Z. m. Kryptowährungen für alle hessischen Polizeidienststellen.

Insgesamt stehen den drei Sachgebieten Polizeivollzugsbeamtinnen/-beamte im zweistelligen Bereich zur Verfügung. Aus polizeitaktischen Gründen kann eine detaillierte Darstellung der personellen Strukturierung innerhalb der Sachgebiete nicht erfolgen.

Darüber hinaus befassen sich zwei weitere Sachgebiete mit den Phänomenen Kinderpornografie / Jugendpornografie, sexueller Missbrauch von Kindern / sexueller Missbrauch von Jugendlichen. Die Sachgebiete sind aktuell der BAO FOKUS zugeordnet.

Wie in der Vorbemerkung bereits erwähnt, arbeiten bei den Ermittlungsverfahren mehrere Akteure im Verbund zusammen. Neben Ermittlerinnen/Ermittlern, die sich behördenübergreifend unterstützen, sind dies Informatikerinnen/Informatiker und Spezialisten des Hessen3C.

Frage 2. Wie viele Mitarbeiterinnen und Mitarbeiter in den einzelnen Polizeipräsidien sind mit dem Thema „Cybercrime“ beschäftigt?

In den Flächenpräsidien ist die Thematik „Cybercrime im engeren Sinne“ bei den Zentralen Kriminalinspektionen (ZKI) und im PP Frankfurt am Main in der Kriminalinspektion 30 (K 30) verortet.

Für das Führen von Ermittlungsverfahren in Fällen von „Cybercrime im engeren Sinne“ stehen in den einzelnen Polizeipräsidien insgesamt Mitarbeiterinnen und Mitarbeiter im mittleren zweistelligen Bereich zur Verfügung.

Wie in der Vorbemerkung ausgeführt, gibt es darüber noch „Cybercrime im weiteren Sinne“, also Straftaten, bei denen die Informations- und Kommunikationstechnik zur Planung, Vorbereitung und Ausführung für „klassische“ Straftaten eingesetzt wird. Der Schwerpunkt liegt hier im Betrugsbereich. Diese Delikte werden – je nach Schwere des Deliktes – in den jeweiligen Betrugskommissariaten der Kriminal- und Polizeidirektionen, aber auch in den Dezentralen Ermittlungsgruppen aller Polizeireviere und -stationen bearbeitet.

Aus polizeitaktischen Gründen kann eine detaillierte Darstellung der personellen Strukturierung innerhalb der Präsidien nicht erfolgen. Es wird zudem auf die Vorbemerkung sowie die Beantwortung der Frage 1 verwiesen

Frage 3. Gibt es in den Polizeipräsidien zusätzlich Informatiker?

Frage 4. Wenn ja: Wie viele?

Auf Grund des Sachzusammenhangs werden die Fragen 3 und 4 gemeinsam beantwortet.

Informatikerinnen und Informatiker sowie weiteres IT-Fachpersonal zur Bekämpfung der „Cybercrime“ werden in den ZKI und im K 30 des PP Frankfurt am Main vorrangig im Bereich der Digitalen Forensik eingesetzt. Die Mitarbeiterinnen und Mitarbeiter führen keine eigenen Ermittlungsverfahren, sondern unterstützen technisch die Ermittlerinnen und Ermittler. Weiterhin fungiert die Digitale Forensik auch als Servicedienststelle für sämtliche Fachkommissariate, deren originäre Delikte mittels Informationstechnik begangen wurden (Cybercrime im weiteren Sinne).

Insgesamt stehen in den einzelnen Polizeipräsidien Mitarbeiterinnen und Mitarbeitern im mittleren zweistelligen Bereich zur Verfügung.

Aus polizeitaktischen Gründen kann eine detaillierte Darstellung der personellen Strukturierung innerhalb der Präsidien nicht erfolgen. Es wird zudem auf die Vorbemerkung sowie die Beantwortungen der Fragen 1 und 2 verwiesen.

Frage 5. Wird derzeit diesbezüglich auf (weitere) externe Fachkompetenz zurückgegriffen bzw. ist ein solcher Rückgriff geplant?

Im Bereich der Cybercrime-Ermittlungen wird aus ermittlungstaktischen und rechtlichen Gründen in der Regel nicht auf externe Fachkompetenz zurückgegriffen. In der Digitalen Forensik hingegen werden anlassbezogen externe Firmen beauftragt, vor allem für Extraktions- und Dekodierungstätigkeiten an Smartphones oder mobilen Endgeräten. Zudem kommt es im Rahmen von Forschungsprojekten zu Kooperationen mit Universitäten, Hochschulen und Instituten.

Darüber hinaus stehen die Spezialisten von Hessen3C aus den Bereichen Cybersecurity, Cybercrime und Cyberintelligence dem HLKA bei spezifischen Fragestellungen als Ansprechpartner für Beratungen zur Verfügung.

Frage 6. Wie werden Fälle im Bereich "Cybercrime" in den polizeilichen Erfassungssystemen registriert? (z.B. durch Listen etc.)?

Der Phänomenbereich Cybercrime wird – wie alle anderen Straftaten auch – im hessischen Vorgangsbearbeitungssystem ComVor erfasst und über Datenschnittstellen weiterverarbeitet. So auch im sogenannten „einheitlichen Fallbearbeitungssystem“ (eFBS), welches zur kriminalpolizeilichen Auswertung und Fallbearbeitung zur Verfügung steht.

Die statistische Erfassung wird durch die „Polizeiliche Kriminalstatistik“ (PKS) abgebildet. Da sich die „digitale Gesellschaft“ in der gesamten Kriminalität widerspiegelt, setzte sich nach Gremienbefassung die Abbildung eines Überbegriffs „Computerkriminalität“, künftig „Cybercrime“, zur Abbildung von Cybercrime durch. Hier wird die Gesamtheit der Delikte subsumiert, die die Eigenschaft „Tatmittel Internet und/oder IT-Geräte“ aufweisen.

Frage 7. Hält die Landesregierung es für notwendig, dass Fälle im Bereich "Cybercrime" gesondert abgebildet werden?

Die Computerkriminalität wurde in der PKS bisher mit Hilfe mehrerer Sonderkenner abgebildet. Für eine übersichtlichere Abbildbarkeit wird der Bereich Cybercrime zukünftig unter dem Überbegriff „Cybercrime“ mit Hilfe eines Sonderkenners (Tatmittel Internet und/oder IT-Geräte) abgebildet. Diese gesonderte Abbildung wird als erforderlich erachtet, um einen noch umfassenderen Überblick über die Anzahl der angezeigten Straftaten im Bereich Cybercrime zu erlangen.

Frage 8. Wie viele Fälle von "Cybercrime" konnten durch das HLKA in den letzten fünf Jahren jeweils erfolgreich gelöst werden?

Cybercrime umfasst alle Delikte, die als Kenner das Tatmittel Internet und/oder IT-Geräte aufweisen, wie z.B. Betrug oder Angriff auf Datennetze. Die Bearbeitung erfolgt in den Sachgebieten im HLKA und zu einem weit überwiegenden Teil hessenweit in den Fachkommissariaten. Darüber hinaus wird das HLKA in einer Vielzahl von Ermittlungsverfahren ermittlungsunterstützend und -beratend tätig.

Vor dem Hintergrund ist eine genaue Bezifferung der Fälle, die das HLKA erfolgreich gelöst hat, nicht möglich.

Frage 9. Wie schätzt die Landesregierung die Dunkelziffer der ungelösten Fälle ein?

Nach der Einschätzung des Bundeskriminalamtes im Bundeslagebild 2020 ist im Bereich Cybercrime das Dunkelfeld weit überdurchschnittlich ausgeprägt. Gründe hierfür liegen u.a. darin, dass eine große Anzahl strafbarer Handlungen im Internet aufgrund zunehmender technischer Sicherungseinrichtungen meist nicht über das Versuchsstadium hinauskommt und von den Geschädigten nicht bemerkt wird. Ferner werden Straftaten durch Betroffene oftmals nicht angezeigt, insbesondere dann, wenn noch kein finanzieller Schaden entstanden ist. Eigene wissenschaftliche Studien liegen der Hessischen Landesregierung aktuell nicht vor.

Frage 10. Wie hoch schätzt die Landesregierung die wirtschaftlichen Schäden, die aus der lnternetkriminalität resultieren, für die hessische Wirtschaft ein?

Der Hessischen Landesregierung liegen zu dieser Frage keine Erhebungen vor.

Wiesbaden, 30. Dezember 2021

In Vertretung:
Stefan Sauer