20. Wahlperiode

Drucksache **20/6433**

HESSISCHER LANDTAG

07. 01. 2022

Kleine Anfrage

Stefan Müller (Freie Demokraten) und Oliver Stirböck (Freie Demokraten)
vom 23.09.2021

„Cybercrime“ – Teil II

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 ope-

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

rative Zentralstelle bearbeitet die ZIT besonders aufwendige und umfangreiche Ermittlungsverfahren aus den Deliktsbereichen Kinderpornographie und sexuellem Missbrauch von Kindern mit 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 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 Internetkriminalität aufgestellt.

Diese Vorbemerkungen vorangestellt, beantworte ich die Kleine Anfrage im Einvernehmen mit der Ministerin der Justiz wie folgt:

Frage 1. Welche Aufgaben hat das HLKA im Bereich "Cybercrime" bei Angriffen auf für das Land Hessen wichtige Digital-Infrastrukturen?

Dem HLKA obliegt die Strafverfolgung bei allen herausragenden Cyberangriffen in Hessen im Auftrag der ZIT der Generalstaatsanwaltschaft Frankfurt am Main.

Frage 2. Laut dem Vorwort zur Kriminalitätsstatistik 2020 sei der Bereich der polizeilichen Prävention gestärkt worden. In den Beratungsstellen seien Cyberberater als Ansprechpartner für Bürgerinnen und Bürger installiert worden. Wie viele solcher Ansprechpartner gibt es hessenweit für Bürgerinnen und Bürger?

Der Phänomenbereich „Cybercrime“ steht im Fokus der polizeilichen Präventionsarbeit. Daher ist in jedem Flächenpräsidium und im HLKA je ein Fachberater für „Cybercrime“ implementiert, die anlassbezogen durch die Fachdienststellen zur Bekämpfung der Cybercrime unterstützt werden.

Das Hauptziel der Prävention bei Cybercrime besteht in der Sensibilisierung und Aufklärung im Innen- und Außenverhältnis für relevante Situationen und Verhaltensweisen. Um dieses Ziel zu

erreichen, wird über phänomenbezogene Vorgehensweisen der Täter und effektive Schutzmaßnahmen aufgeklärt. Hierbei werden polizeiliche Erkenntnisse über Gefahren und Risiken insbesondere im Umgang mit sensiblen Daten genutzt, um praktikable Hinweise zur sicheren Handhabung von Computern und mobilen Endgeräten zu generieren. Unmittelbare Zielgruppen der polizeilichen Präventionsarbeit sind erwachsene Personen aller Altersklassen sowie Angehörige der hessischen Polizei. Der Schwerpunkt liegt in der Aus- und Fortbildung von Multiplikatoren. Die mittelbare Zielgruppe der Kinder und Jugendlichen wird insbesondere über Lehrer und Eltern erreicht. Der hieraus resultierende Streuungseffekt führt dazu, dass eine möglichst großflächige Verbreitung der Inhalte erreicht wird.

Frage 3. Seit Februar 2021 bietet die hessische Polizei den Studienschwerpunkt Cyberkriminalistik an. 18 Kommissaranwärterinnen und -anwärter sind als neue Studiengruppe der Polizei Hessen im Februar 2021 gestartet. Wie viele von diesen belegen noch immer den Studienschwerpunkt?

Die genannte Studiengruppe, die im Februar 2021 das Bachelorstudium „Kriminalpolizei“ mit der Vertiefungsrichtung „Cyberkriminalistik“ aufgenommen hat, besteht derzeit aus insgesamt 17 Anwärterinnen und Anwärtern.

Frage 4. Wie viele Anwärterinnen und Anwärter haben im September 2021 ihr Studium mit diesem Studienschwerpunkt aufgenommen?

Im September 2021 haben insgesamt 18 Anwärterinnen und Anwärter das Bachelorstudium „Kriminalpolizei“ mit der Vertiefungsrichtung „Cyberkriminalistik“ aufgenommen.

Frage 5. Wie will die Landesregierung diesen Studienschwerpunkt weiter stärken?

Zur weiteren Stärkung der Digitalkompetenz in der hessischen Polizei soll die Vertiefungsrichtung „Cyberkriminalistik“ auch im Jahr 2022 mit jeweils einer Studiengruppe pro Semester am Studienstandort Mühlheim angeboten werden. Um genügend Bewerberinnen und Bewerber für den Studiengang zu gewinnen, bewirbt die Nachwuchsgewinnung der hessischen Polizei die Vertiefungsrichtung „Cyberkriminalistik“ mit einem zielgruppenspezifischen Werbekonzept. Der Studienstandort Mühlheim verfügt über eine äußerst attraktive und zentrale Lage im Rhein-Main-Gebiet und wurde für die Studierenden mit modernster IT-Technologie ausgestattet. Die Lehrinhalte im Studienfach „Technik, Wissenschaft, Cyberkriminalistik“ werden in der fortschrittlichen Lernumgebung von einem Team aus erfahrenen und bewährten Spezialisten vermittelt.

An der Hessischen Hochschule für Polizei und Verwaltung (ab dem 01.01.2022 Hessische Hochschule für öffentliches Management und Sicherheit) finden perspektivisch die Inhalte aus dem Bereich Informatik und Informationstechnik auch in den Studiengängen „Kriminalpolizei“, Vertiefungsrichtung „Allgemeine Kriminalistik“ sowie im Studiengang „Schutzpolizei“ sukzessive eine stärkere Berücksichtigung.

Frage 6. Wie gestaltet sich die Zusammenarbeit des HLKA mit den anderen Akteuren im Bereich „Cybercrime“ (z.B. „Hessen3C“, andere Landeskriminalämter, dem Bundeskriminalamt und der Staatsanwaltschaft)?

Das HLKA sammelt und koordiniert die polizeilichen Erkenntnisse zur Cybercrime und bildet als Zentralstelle für die Kriminalitätsbekämpfung der Polizei Hessen die Kommunikationsbrücke in das Bundesgebiet, soweit es die Polizei betrifft. Das HLKA unterhält hierzu auf unterschiedlichsten Ebenen Verbindungen und tauscht in enger Zusammenarbeit mit anderen Behörden Informationen aus. Es bestehen bundesweite Verbünde wie beispielsweise der Verbund der „Zentralen Ansprechstellen Cybercrime für die Wirtschaft“ (ZAC); gleiches gilt für den Bereich der Cybercrime-Ermittlungen und den Bereich der technischen Ermittlungsunterstützungen, bei welchen ein regelmäßiger Austausch in Form von Tagungen und Besprechungen stattfindet.

Landesspezifisch wird in einem wöchentlichen Lageaustausch zwischen Hessen3C, dem Landesamt für Verfassungsschutz Hessen (LfV) und der Zentralen Ansprechstelle Cybercrime (ZAC) im HLKA die Landeslage Cybercrime fortwährend aktualisiert und analysiert. Der institutionalisierte wöchentliche Lageaustausch zu Cyberbedrohungen, sich ständig wandelnden Formen von Cyberattacken und möglichen Schutzmaßnahmen stellt einen wesentlichen Beitrag zur Erhöhung des Resilienzniveaus gegen Cyberangriffe für die Bereiche der Landesverwaltung, Kommunen, Wirtschaftsunternehmen und Betreiber Kritischer Infrastrukturen dar.

Die von Hessen3C erstellten Lageberichte und Warnmeldungen werden dem HLKA zur Verfügung gestellt. Darüber hinaus stehen die Spezialisten des Hessen3C aus den Bereichen Cybersecurity, Cybercrime und Cyberintelligence dem HLKA bei spezifischen Fragestellungen als Ansprechpartner zur Verfügung.

Im Falle erfolgter Cyberattacken erfolgt ein anlassbezogenes und abgestimmtes Vorgehen der Polizei im Rahmen der Strafverfolgung und der möglichen Wahrnehmung von Aufgaben des Hessen3C, etwa bei Beratungsleistungen für Betroffene von Cyberangriffen oder dem Einsatz forensischer Analysewerkzeuge. Bei aller behörden- und organisationsübergreifenden Zusammenarbeit werden die rechtlichen Vorgaben berücksichtigt und gewahrt.

Besondere Bedeutung hat die Zusammenarbeit im Bereich Cybercrime mit der bei der Generalstaatsanwaltschaft Frankfurt am Main eingerichteten ZIT. Sie ist erster Ansprechpartner des Bundeskriminalamtes (BKA) für Internetstraftaten bei noch ungeklärter örtlicher Zuständigkeit in Deutschland oder bei Massenverfahren gegen eine Vielzahl von Tatverdächtigen bundesweit. Die ZIT entwickelt maßgeblich die Strafverfolgung, insbesondere Cybercrime im engeren Sinne, fort und arbeitet dafür eng mit dem HLKA zusammen.

Ergänzend wird auf die Vorbemerkung verwiesen.

Frage 7. Wie konkret erfolgt die Zusammenarbeit mit der Justiz im Bereich "Cybercrime"?

Die konkrete Zusammenarbeit der Justiz mit den Polizeibehörden erfolgt auch in Verfahren wegen Cybercrime gemäß den Regelungen in der Strafprozessordnung (StPO). Das bedeutet Folgendes: Sobald die Staatsanwaltschaft durch eine Anzeige oder auf anderem Wege von dem Verdacht einer Straftat Kenntnis erhält, hat sie zu ihrer Entschließung darüber, ob die öffentliche Klage zu erheben ist, den Sachverhalt zu erforschen. Die Staatsanwaltschaft ist befugt, von allen Behörden Auskunft zu verlangen und Ermittlungen jeder Art entweder selbst vorzunehmen oder durch die Behörden und Beamtinnen und Beamten des Polizeidienstes vornehmen zu lassen. Die Behörden und Beamtinnen und Beamte des Polizeidienstes sind verpflichtet, dem Ersuchen oder Auftrag der Staatsanwaltschaft zu genügen und in diesem Falle befugt, von allen Behörden Auskunft zu verlangen. Die Behörden und Beamtinnen und Beamte des Polizeidienstes haben daneben auch bei eigener Kenntniserlangung Straftaten zu erforschen und alle keinen Aufschub gestattenden Anordnungen zu treffen, um die Verdunkelung der Sache zu verhüten. Zu diesem Zweck sind sie befugt, alle Behörden um Auskunft zu ersuchen, bei Gefahr im Verzug auch, die Auskunft zu verlangen, sowie Ermittlungen jeder Art vorzunehmen, soweit nicht andere gesetzliche Vorschriften ihre Befugnisse besonders regeln. Die Behörden und Beamtinnen und Beamte des Polizeidienstes übersenden ihre Verhandlungen ohne Verzug der Staatsanwaltschaft.

Aufgrund der Flüchtigkeit von beweiserheblichen Daten ist in Ermittlungsverfahren wegen Cybercrime-Delikten eine schnelle und unmittelbare Kommunikation zwischen der Justiz und der Polizei erforderlich. Dies bedingt eine enge Verzahnung von staatsanwaltschaftlicher und polizeilicher Tätigkeit bei den Ermittlungen. Regelmäßige Dienstbesprechungen ZIT und der Polizei, eine enge Anbindung der ZIT an das Hessische Landeskriminalamt sowie eine 24/7-Erreichbarkeit der ZIT sorgen zudem dafür, dass die organisatorische Zusammenarbeit reibungslos verläuft.

Frage 8. Gibt es bei den Staatsanwaltschaften Dezernenten, die "Experten" für "Cybercrime" sind?

Bei den hessischen Staatsanwaltschaften sowie bei der Amtsanwaltschaft Frankfurt am Main sind seit dem Jahr 2015 jeweils Ansprechpartnerinnen und Ansprechpartner für Internetkriminalität benannt. Diese werden wiederkehrend im Rahmen von mehrtägigen Fortbildungsveranstaltungen, regelmäßigen Dienstbesprechungen und der Versendung aktueller Kurzinformationen („Newsletter“) von der ZIT geschult und stehen zum einen in ihrer jeweiligen Behörde für Nachfragen der Dezernentinnen und Dezernenten, zum anderen für den Informationsaustausch mit den polizeilichen Spezialkommissariaten im Bereich Cybercrime sowie der ZIT zur Verfügung. Zudem unterstützt die ZIT über die benannten Ansprechpartnerinnen und Ansprechpartner für Internetkriminalität die Führung von Ermittlungsverfahren der hessischen Staatsanwaltschaften sowie der Amtsanwaltschaft Frankfurt am Main durch die Bereitstellung von Vordrucken, Musterverfügungen und Ermittlungsleitfäden.

Daneben ist bereits seit dem Jahr 2010 die ZIT als „Cybercrime-Zentralstelle“ der hessischen Staatsanwaltschaften eingerichtet. Die ZIT übernimmt neben der beschriebenen koordinierenden Funktion für die hessischen Staatsanwaltschaften und die Amtsanwaltschaft Frankfurt am Main auch eigene operative Tätigkeiten und führt Ermittlungsverfahren von besonderer Schwierigkeit, besonderem Umfang oder besonderer Bedeutung. Dabei ist die ZIT erster Ansprechpartner des Bundeskriminalamtes für Internetstraftaten bei noch ungeklärter örtlicher Zuständigkeit in Deutschland oder bei Massenverfahren gegen eine Vielzahl von Tatverdächtigen bundesweit.

Zur weiteren notwendigen Spezialisierung für die effektive Strafverfolgung von Cybercrime sind in der ZIT insgesamt vier unterschiedliche Ermittlungsteams gebildet worden, die operative und administrative Aufgaben in den folgenden Themengebieten von „Cybercrime im weiteren Sinne“ bzw. „Kriminalität mit dem Tatmittel Internet“ übernehmen:

- Cyber-Kriminalität (Hackerangriffe, Datendiebstahl, Computerbetruge etc.),
- Kinderpornografie und sexueller Missbrauch von Kindern mit Bezug zum Internet,
- Darknet-Kriminalität (Handel mit Waffen, Drogen, Fälschungsgütern etc.),
- Hass-Kriminalität im Internet (Beleidigung, Bedrohung, Volksverhetzung etc.).

In diesen Ermittlungsteams werden die Dezernentinnen und Dezernenten der ZIT zudem durch zwei IT-Referenten in Fragen der technischen Ermittlungsunterstützung sowie der IT-forensischen Auswertung sichergestellter Datenträger unterstützt.

Frage 9. Welche Straftatbestände unterfallen aus Sicht der Landesregierung dem Begriff "Cybercrime", wenn sie sich darauf bezieht?

Die hessische Justiz verwendet den Begriff „Cybercrime“ in gleicher Weise wie das Bundeskriminalamt in der Polizeilichen Kriminalstatistik. Danach umfasst Cybercrime die Straftaten, die sich gegen das Internet, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne) oder die unter Nutzung von Informationstechnik begangen werden, auch als „Tatmittel Internet“ (Cybercrime im weiteren Sinne) bezeichnet.

Zu Cybercrime im engeren Sinne werden folgende Straftatbestände aus dem StGB subsumiert:

- § 202a Ausspähen von Daten,
- § 202b Abfangen von Daten,
- § 202c Vorbereiten des Ausspähens und Abfangens von Daten,
- § 202d Datenhehlerei,
- § 263a Computerbetrug,
- § 269 Fälschung beweiserheblicher Daten,
- § 270 Täuschung im Rechtsverkehr bei Datenverarbeitung,
- § 303a Datenveränderung,
- § 303b Computersabotage.

Frage 10. Welches langfristige Konzept verfolgt die Landesregierung, um dem wachsenden Kriminalitätsschwerpunkt "Cybercrime" entgegenzutreten?

Hinsichtlich der Beantwortung der Frage 10 wird auf die Vorbemerkung verwiesen.

Wiesbaden, 30. Dezember 2021

In Vertretung:
Stefan Sauer