

Antwort

der Landesregierung

auf die Kleine Anfrage Nr. 4223

der Abgeordneten Danny Eichelbaum (CDU-Fraktion) und Björn Lakenmacher (CDU-Fraktion)

Drucksache 6/10442

Schwerpunktstaatsanwaltschaft „Cybercrime“

Namens der Landesregierung beantwortet der Minister der Justiz und für Europa und Verbraucherschutz die Kleine Anfrage wie folgt:

Vorbemerkungen der Fragesteller

In den letzten Jahren sind Straftaten und Kriminalität, die im Internet begangen wurden bzw. Straftaten gegen Daten von Personen, Unternehmen und Behörden als neues Feld der Strafverfolgung in den Fokus gerückt. Zuletzt hat das Ausspähen von privaten Daten zahlreicher Personen des öffentlichen Lebens und deren Veröffentlichung im Internet für hohe Aufmerksamkeit gesorgt.

Im Land Brandenburg besteht seit 2016 beim LKA ein Cyber-competence-centre (CCC). Bereits im Jahr 2014 wurde die Staatsanwaltschaft Cottbus zur Schwerpunktstaatsanwaltschaft zur Bekämpfung von Computer- und Datennetzkriminalität, datenschutzrechtlicher Verstöße sowie gewaltdarstellender, pornographischer und sonstiger jugendgefährdender Schriften bestimmt.

Frage 1: Wie viele Staatsanwälte sind seit 2014 im Bereich zur Bekämpfung von Computer- und Datennetzkriminalität sowie von datenschutzrechtlichen Verstößen eingesetzt (bitte nach Jahren aufschlüsseln)?

zu Frage 1: Die Staatsanwaltschaft Cottbus wurde im Jahr 1994 zur Zentralstelle zur Bekämpfung gewaltdarstellender, pornographischer und sonstiger jugendgefährdender Schriften im Land Brandenburg bestimmt (JMBl. 1995 S. 3). Seit 2001 fungiert sie darüber hinaus als Schwerpunktstaatsanwaltschaft zur Bekämpfung der Datennetzkriminalität (JMBl. 2001 S. 5). Seit März 2014 ist sie auch zentral für die Bearbeitung datenschutzrechtlicher Verstöße zuständig (JMBl. 2014 S. 42).

Seit 2014 ist die Schwerpunktabteilung durchgängig mit einem Abteilungsleiter und sechs Dezernentinnen und Dezernenten besetzt, wovon einzelne mit einem Teil ihrer Arbeitskraft auch andere Aufgaben wahrnehmen. Seit Januar 2019 sind der Schwerpunktabteilung fünf Dezernentinnen und Dezernenten zugewiesen; eine erneute Besetzung mit sechs Staatsanwältinnen und Staatsanwälten ist zum 1. April 2019 nach einer geplanten Neueinstellung einer Staatsanwältin bei der Staatsanwaltschaft Cottbus beabsichtigt.

Eingegangen: 19.02.2019 / Ausgegeben: 25.02.2019

Frage 2: Wie sieht das Aus- und Fortbildungsangebot im Bereich Computer- und Daten- netzkriminalität aus?

- a. Sind regelmäßige Fortbildungen wiederkehrend und verpflichtend?
- b. In welchen Bereichen werden Fortbildungen angeboten (hinsichtlich des Rechts, aber auch hinsichtlich technischer Fortschritte bei Ermittlungsmethoden, Internetrecherche etc.)?

zu Frage 2: Für Staatsanwältinnen und Staatsanwälte ist die Fortbildung im Bereich der Computer- und Datennetzkriminalität - wie in allen anderen Tätigkeitsbereichen auch - grundsätzlich freiwillig. Eine fortlaufende Weiterbildung in juristischer und technischer Hinsicht erfolgt durch die regelmäßige Lektüre juristischer und IT-spezifischer Fachzeitschriften.

Darüber hinaus nimmt der Abteilungsleiter der Schwerpunktabteilung zur Bekämpfung von Computer- und Datennetzkriminalität sowie gewaltdarstellender, pornographischer und sonstiger jugendgefährdender Schriften einmal jährlich an der bundesweiten Tagung der Cybercrime-Dienststellen der Staatsanwaltschaften der Bundesländer teil. Ferner werden einschlägige Fortbildungsveranstaltungen für Staatsanwältinnen und Staatsanwälte zum einen an der landeseigenen Justizakademie in Königs Wusterhausen angeboten, beispielsweise im Jahr 2018 zweimal die Veranstaltung „Ermittlungsmaßnahmen im Internet: Recherchieren in sozialen Netzwerken und sichern von digitalen Spuren“ sowie die Veranstaltung „Ermittlungsmaßnahmen im Bereich der Telekommunikation und digitaler Kryptowährungen“. Im Jahr 2019 sind die Fortbildungsveranstaltung „Krypto-Währungen - Hintergrund und Auswirkungen auf die Gerichte und Staatsanwaltschaften“ und eine Veranstaltung zum Thema „Internetstrafrecht“ vorgesehen. Daneben besteht die Möglichkeit, an den von der Deutschen Richterakademie in Wustrau und Trier angebotenen Fortbildungsveranstaltungen teilzunehmen. Dort war das Thema Cybercrime im Jahr 2018 Bestandteil der Veranstaltungen „Aktuelle Entwicklungen im Strafrecht“, „Tatort Internet - Aktuelle Entwicklungen in Gesetzgebung und Rechtsprechung“, „Ermittlungsmaßnahmen im Bereich der Telekommunikation“, „Beweisgewinnung und Beweisverwertung bei Ermittlungen im Internet (E-Evidence)“ und „Strafrecht und Internet“. In diesem Jahr werden die Veranstaltungen „Ermittlungsmaßnahmen im Bereich der Telekommunikation“ und „Aktuelle Entwicklungen im Strafrecht“ erneut durchgeführt sowie zusätzlich die Veranstaltungen „Erscheinungsformen der Internetkriminalität und ihre Bekämpfung“ und „Cybercrime“ angeboten. Schließlich werden auch auf europäischer Ebene von der Europäischen Rechtsakademie in Trier sowie im Rahmen des europäischen Fortbildungsnetzwerks EJTN (European Judicial Training Network) vielfältige Fortbildungsveranstaltungen zu den Themen Cybercrime, E-Evidence, Computer Forensics, Web 2.0, Darknet usw. angeboten, an denen Brandenburger Staatsanwältinnen und Staatsanwälte teilnehmen können. Angaben zu den Veranstaltungen und ihren konkreten Inhalten sind im Internet unter den Webseiten <http://www.ejtn.eu> sowie <https://www.era.int> abrufbar.

Bei der Polizei des Landes Brandenburg werden die entsprechenden Aus- und Fortbildungsmaßnahmen gemäß der Konzeption „Aus- und Fortbildung Cybercrime“ der Fachhochschule der Polizei des Landes Brandenburg - als integraler Bestandteil der Strategie zur Bekämpfung und Prävention im Phänomenbereich Cybercrime (Eckpunktepapier des Ministeriums des Innern vom 31. Mai 2013) - gewährleistet.

Im Rahmen der polizeilichen Ausbildung zum mittleren und des Studiums zum gehobenen Polizeivollzugsdienst wird das Themenfeld Cybercrime insbesondere in den Pflichtfächern Kriminologie und Kriminalistik behandelt. Über das für alle Anwärtinnen und Anwärter vermittelte Grundlagenwissen hinaus bietet das Wahlpflichtmodul „Cybercrime“ im Rahmen des Studiums die Möglichkeit, sich mit der Phänomenologie und den kriminalistischen Untersuchungsmethoden von Cybercrime, aber auch mit Fragen der digitalen Polizeiarbeit, der Medienkompetenz und der Nutzung sozialer Medien intensiver auseinanderzusetzen. Eine weitere Spezialisierung auf dem Gebiet Cybercrime erfolgt im Rahmen der polizeilichen Weiterbildung durch ein modularisiertes Seminarangebot. Es gibt Basisseminare für alle Polizeibediensteten des Landes sowie Spezialfortbildungen für die Kriminalpolizei. Zur Vermittlung von Basiswissen wurde eine bereits bestehende E-Learning-Anwendung mit insgesamt sieben Lektionen überarbeitet, von denen die ersten vier kurz vor der Veröffentlichung stehen. Diese Anwendung ermöglicht es jedem Polizeibediensteten, sich Themen wie Hardware, Software, Netzwerke, Internet, Phänomenologie, Recht und Erster Angriff im Selbststudium am PC zu erschließen. Darauf aufbauend erfolgt ein dreitägiges Präsenzseminar an der Fachhochschule der Polizei, in dem das erlernte Grundwissen praxisnah vertieft wird. In den Aufbau- und Spezialmodulen, die von spezialisierten Kriminalisten und Cybercrime-Sachbearbeitern absolviert werden können, werden beispielsweise Themen wie Daten-sicherung/Tatortarbeit und Ermittlungen im Zusammenhang mit Bitcoin/Kryptowährung behandelt. Für Forensikerinnen und Forensiker werden beispielsweise die Spezialmodule „Advanced Smartphone Forensics Training“ und „iOS Forensics“ angeboten. Fortbildungen auf diesem Gebiet sind in dem Sinne nicht verpflichtend, aber gehören ggf. zum Anforderungsprofil für eine Tätigkeit in Spezialdienststellen. Darüber hinaus werden aktuelle Themen in der regelmäßig an der Fachhochschule der Polizei stattfindenden Fachtagung Cybercrime zielgruppenorientiert angeboten. Schließlich besteht im Rahmen der Sicherheitskooperation der Länder Berlin, Brandenburg, Sachsen, Sachsen-Anhalt und Thüringen eine enge Zusammenarbeit, die es Brandenburger Polizeibediensteten ermöglicht, auf ein breites Fortbildungsangebot der beteiligten Länder zurückzugreifen. Beispielsweise können hier Themen wie „Cybercrime und IT-Sicherheit“, „Ethical Hacking“ und „Medienforensik“ tiefer betrachtet werden.

Frage 3: Wie viele Verfahren im Bereich der Computer- und Datennetzkriminalität wurden seit Einrichtung der Schwerpunktzuständigkeit durchgeführt (bitte aufschlüsseln nach Jahr und Deliktsart)?

zu Frage 3: Eine valide Auskunft über die Verfahrenszahlen der Schwerpunktstaatsanwaltschaft im Bereich der Computer- und Datennetzkriminalität - aufgeschlüsselt nach Deliktsart - kann nur für den Zeitraum ab 2013 erteilt werden, da wegen Löschungs- und Aufbewahrungsfristen für einen länger als fünf Jahre zurückliegenden Zeitraum weder eine datenbankgestützte noch eine händische nachträgliche Aufschlüsselung der Verfahrenszahlen möglich ist. Die Zahlen ab 2013 ergeben sich aus der als Anlage beigefügten Tabelle.

Frage 4: Wie lang war die durchschnittliche Verfahrensdauer (bitte aufschlüsseln nach Jahren)?

zu Frage 4: Die Entwicklung der durchschnittlichen Verfahrensdauer ist der nachfolgenden Tabelle zu entnehmen. Seit 2018 werden Verfahren, die der ursprünglichen Zuständigkeit der 1994 eingerichteten Zentralstelle zur Bekämpfung gewaltdarstellender, pornographischer und sonstiger jugendgefährdender Schriften zuzuordnen sind, sowie Verfahren aus der 2001 geschaffenen Schwerpunktzuständigkeit zur Bekämpfung der Datennetzkriminalität in gesonderten Erhebungseinheiten erfasst.

Jahr	Verfahrensdauer in Monaten
2013	3,8
2014	4,4
2015	5,0
2016	6,2
2017	9,1
2018 - Schwerpunkt	12,6
2018 - Zentralstelle	1,4

Frage 5: Wie gestaltet sich die Zusammenarbeit der Schwerpunktstaatsanwaltschaft mit dem CCC? Gibt es hierbei Probleme? Wenn ja, welche und welche Lösungsvorschläge werden erwogen?

zu Frage 5: Sowohl aus polizeilicher als auch aus staatsanwaltschaftlicher Sicht gestaltet sich die Zusammenarbeit zwischen dem Landeskriminalamt Brandenburg, LKA 120 (Cyber-Competence-Center) und LKA 121 (KK Auswertung/Ermittlungen qualifizierte Cybercrime), und der Schwerpunktstaatsanwaltschaft reibungslos und vertrauensvoll. Die enge Zusammenarbeit reicht von verfahrensbezogenen Erörterungen über einen regen allgemeinen Erfahrungsaustausch bis zu der Gestaltung von gemeinsamen Schulungen in der Fachhochschule der Polizei des Landes Brandenburg. Im Rahmen dieser vertrauensvollen Zusammenarbeit erfolgen Abstimmungen zur Priorisierung von Untersuchungsaufträgen gemäß den Festlegungen der jährlichen Beratung des Polizeipräsidenten mit der Generalstaatsanwaltschaft.

Anlage/n:

1. Anlage

Anlage zur Antwort der Landesregierung auf die Kleine Anfrage 4223, Landtagsdrucksache 6/10442

Schwerpunktstaatsanwaltschaft „Cybercrime“

Deliktsbereich	2013		2014		2015		2016		2017		2018	
	Js-	UJs-										
pornografische Straftaten	409	172	299	93	346	174	317	112	356	54	695	74
Betrug, Computerbetrug	366	542	349	614	304	858	262	580	164	384	98	308
Datendelikte	243	859	172	856	159	842	87	676	105	560	96	495
sog. politische Straftaten	91	51	143	52	270	85	386	131	315	119	276	58
Datenschutzdelikte	0	4	0	25	28	26	31	19	29	21	38	33
Jugendschutzsachen	6	6	5	2	0	3	6	4	0	4	8	3
Wirtschaftsstraftaten	0	4	0	1	0	2	3	6	0	2	5	5
Persönlichkeitsrechtsverletzungen	278	31	156	220	106	64	161	62	165	65	145	59
Sonstiges	45	1780	44	622	46	402	46	449	41	330	54	342
Js-Verfahren insgesamt	1438		1168		1259		1299		1175		1415	
UJs-Verfahren insgesamt		3449		2485		2456		2039		1539		1377

Js-Verfahren: Verfahren gegen bekannte Beschuldigte
 UJs-Verfahren: Verfahren gegen unbekannt

Die vorgenannten Deliktsbereiche beinhalten im Wesentlichen folgende Straftatbestände:

pornografische Straftaten: §§ 184, 184a, 184b, 184c StGB
 Betrug, Computerbetrug: §§ 263, 263a, 269 StGB
 Datendelikte: §§ 202a ff., 303a ff. StGB
 sog. politische Straftaten: §§ 86, 86a, 111, 126, 130 StGB
 Datenschutzdelikte: Vergehen nach BDSG und BbgDSG
 Jugendschutzsachen: § 131 StGB, § 27 JuSchG, § 23 JMStV
 Wirtschaftsstraftaten: §§ 106 ff. UrhG, § 143 MarkenG
 Persönlichkeitsrechtsverletzungen: §§ 183a, 185 ff. StGB, § 33 KUG