Bayerischer Landtag

17. Wahlperiode

02.06.2017 17/16300

Schriftliche Anfrage

der Abgeordneten **Katharina Schulze**
BÜNDNIS 90/DIE GRÜNEN
vom 31.01.2017

Cybercops bei der Bayerischen Polizei II

Ich frage die Staatsregierung:

1.1 Hat die Zentralisierung der Sachbearbeitung der Delikte bei den Cybercrime-Dezernaten bzw. -Kommissariaten zu einer Überlastung der betreffenden Organisationseinheit geführt?
1.2 Welche Auslastung haben die Dienststellen zu „Regionalen Beweismittelsicherungs- und Auswertungsstellen“ (RBA) bei der Bearbeitung von „Cybercrime-Verfahren“?
1.3 Gibt es definierte und einheitliche Standards für alle Polizeipräsidien für die RBA-Dienststellen bei der Bearbeitung von „Cybercrime-Verfahren“?

2.1 Wie lange dauert im Schnitt die Bearbeitungszeit von Asservaten/Computer- und Datenträgerauswertungen?
2.2 Wie viele der Cybercops arbeiten bei den RBA (bitte nach Polizeipräsidien aufschlüsseln)?
2.3 Wie bewertet die Staatsregierung die Aufteilung in verschiedene spezialisierte Organisationseinheiten?

3.1 Sind der Staatsregierung Schnittstellenprobleme aufgrund von der verschiedenartigen organisatorischen Anbindung von Cybercrime-Ermittlungen und RBA-Aufgaben bekannt?
3.2 Wenn ja, um was für Schnittstellenprobleme handelt es sich?
3.3 Was gedenkt die Staatsregierung dagegen zu tun?

4.1 Wie viele Weiterbildungsmaßnahmen im Bereich Cybercrime gibt es bei der Bayerischen Polizei (bitte einzeln auflisten)?
4.2 Wie viele Beamtinnen und Beamte mit Führungsfunktion wurden in den letzten drei Jahren in diesem Bereich weitergebildet?
4.3 Wie viele Sachbearbeiterinnen und Sachbearbeiter wurden in den letzten drei Jahren in diesem Bereich weitergebildet?

5.1 Wie viele Beamtinnen und Beamte aus der 2. Qualifikationsebene werden zu Spezialist(inn)en ausgebildet?
5.2 Schließt der Freistaat Bayern Verträge mit Hochschulen, um dort Polizist(inn)en in spezialisierten Studiengängen ausbilden zu lassen (bitte entsprechende Hochschulen und Studiengänge namentlich aufführen)?
5.3 Welche zusätzlichen Maßnahmen werden ergriffen, dass Polizeibeamtinnen/-beamten innerhalb von Polizeiinspektionen gezielt mit dem nötigen Fachwissen ausgebildet werden?

6.1 Inwieweit sind die Ermittler bei der Bayerischen Polizei außerhalb der Spezialistenbereiche mit der Möglichkeit der spezifischen Ermittlungsinstrumente und der forensischen Spurensicherung vertraut?
6.2 Haben die Sachbearbeiter aus dem Bereich der Cybercrime-Ermittlungen bzw. der Cybercrime-RBA genug Ressourcen, um die Ermittlungsunterstützung zu leisten?
6.3 Wie viele Anfragen an die Spezialistenbereiche kamen in den letzten drei Jahren von fachfremden Polizeidienststellen (bitte nach Jahr auflisten)?

7.1 In welchen bayerischen Polizeipräsidien werden durch Cybercops anlassunabhängige bzw. eigeniniative Ermittlungen/Recherchen in nicht indexierten Bereichen des Internets (sog. Darknet bzw. Underground-Foren) durchgeführt?
7.2 In wie vielen Fällen wurden dabei in Bayern lebende bzw. behördlich gemeldete Täter identifiziert (bitte um Auflistung der entsprechenden Deliktsbereiche, z. B. Staatsschutz/Terrorismus, Bandenkriminalität, Drogen-, Waffendelikte, Carding)?
7.3 In wie vielen Fällen ermittelten Cybercops dabei als Verdeckte Ermittler (VE) i. S. d. § 110a Strafprozessordnung (StPO)?

8.1 Inwieweit erfolgt im Bereich dieser eigeniniativen Ermittlungen ein Austausch zwischen den einzelnen Polizeipräsidien bzw. Bundesländer, um Mehrfachermittlungen zu einer relevanten „virtuellen Identität“ (z. B. Nickname im Forum) zu vermeiden?
8.2 Sieht die Staatsregierung im diesem Bereich noch weiteren Koordinierungs- bzw. Handlungsbedarf?

Antwort

des Staatsministeriums des Innern, für Bau und Verkehr
vom 29.03.2017

Die Schriftliche Anfrage wird im Einvernehmen mit dem Staatsministerium der Justiz wie folgt beantwortet:

1.1 Hat die Zentralisierung der Sachbearbeitung der Delikte bei den Cybercrime-Dezernaten bzw. -Kommissariaten zu einer Überlastung der betreffenden Organisationseinheit geführt?

Cybercrime-Dezernate bzw. Cybercrime-Kommissariate bestanden bis zum 01.03.2017 nur in den Ballungsräumen München, Nürnberg und Augsburg.

Das Polizeipräsidium München und das Bayerische Landeskriminalamt verfügen über ein Kriminalfachdezernat Cybercrime (Kriminalfachdezernat (KFD) 12 beim Polizeipräsidium (PP) München, Dezernat 54 beim Bayerischen Landeskriminalamt (BLKA)), das PP Mittelfranken in Nürnberg und das PP Schwaben-Nord in Augsburg über Fachkommissariate (K 25 in Nürnberg bzw. K 11 in Augsburg) zur Bekämpfung der Internetkriminalität.

Es ist Führungsaufgabe der Präsidien, permanent die Entwicklungen in ihren Bereichen zu beobachten und darauf belastungs- und kräfteorientiert zu reagieren.

Darüber hinaus waren bislang grundsätzlich bei allen Kriminalpolizeiinspektionen spezielle Arbeitsbereiche für Cybercrime eingerichtet. Um dem rasanten und allumfassenden technischen Fortschritt im Bereich der modernen Informations- und Kommunikationstechnik und der damit eng verbundenen, schnell ansteigenden delikts- und tatmittelspezifischen Kriminalität professionelle polizeiliche Ermittlungsarbeit entgegenzusetzen, werden diese Arbeitsbereiche Cybercrime mit Beginn 01.03.2017 zu eigenständigen Kommissariaten ausgebaut. Zudem wird bei allen Kriminalpolizeiinspektionen mit Zentralaufgaben ein Kommissariat Cybercrime errichtet.

1.2 Welche Auslastung haben die Dienststellen zu „Regionalen Beweismittelsicherungs- und Auswertungsstellen“ (RBA) bei der Bearbeitung von „Cybercrime-Verfahren“?

Insgesamt sind bei der Bayerischen Polizei 21 Regionale Beweismittelsicherungs- und Auswertungsstellen (RBA) vorhanden. In den RBA werden digitale Spuren gesichert, aufbereitet und ausgewertet und die Feststellungen und Ergebnisse in Berichtsform dem Auftraggeber (endsachbearbeitende Dienststelle) zur Verfügung gestellt. Eine Endsachbearbeitung von Cybercrime-Verfahren erfolgt in den RBA-Dienststellen nicht. Die Spuren bzw. Aufträge kommen aus allen Deliktsbereichen, von der Alltagskriminalität bis hin zu Mord und Terrorismus.

Nach einer Informationserhebung bei den Verbänden ist festzustellen, dass die Labore insgesamt voll ausgelastet sind. Eine statistische Erfassung hinsichtlich der Auslastung mit Cybercrime-Delikten erfolgt nicht.

1.3 Gibt es definierte und einheitliche Standards für alle Polizeipräsidien für die RBA-Dienststellen bei der Bearbeitung von „Cybercrime-Verfahren“?

Die Bearbeitung von Aufträgen von Cybercrime-Verfahren erfolgt, wie auch die Bearbeitung der Aufträge aus anderen Deliktsbereichen, nach dem aktuellen Stand der Technik, dem wissenschaftlichen Standard der IT-Forensik und anhand der Fragestellungen der jeweiligen beauftragenden Ermittlungsdienststelle. Das Bayerische Landeskriminalamt hat für die RBA einheitliche Standards hinsichtlich der Verfahrensweise zur Auswertung und Sicherung von digitalen Spuren festgelegt. Darüber hinaus erfolgt grundsätzlich eine fallabhängige Festlegung im Einzelfall in enger Absprache mit dem kriminalpolizeilichen Sachbearbeiter.

2.1 Wie lange dauert im Schnitt die Bearbeitungszeit von Asservaten/Computer- und Datenträgerauswertungen?

Grundsätzlich wird die zeitliche Reihenfolge der Untersuchungsaufträge u. a. anhand der Deliktsqualität priorisiert, wobei die Untersuchungszeit – ungeachtet bspw. etwaiger Postlaufzeiten – in Abhängigkeit vom Untersuchungsauftrag und der Art und Anzahl der Asservate von Stunden bis zu mehreren Monaten betragen kann.

2.2 Wie viele der Cybercops arbeiten bei den RBA (bitte nach Polizeipräsidien aufschlüsseln)?

Insgesamt verrichten drei sog. Cybercops der Bayerischen Polizei ihren Dienst in einer RBA. Beim PP München wurde die RBA als Kommissariat 123 in das Kriminalfachdezernat 12 für Cybercrime eingegliedert. Hier finden zwei Cybercops ihre Verwendung. Ein weiterer Cybercop befindet sich bei der RBA-Dienststelle der Kriminalpolizeiinspektion (KPI) Würzburg, dem Kommissariat 7, im Einsatz.

Verband	Anzahl der Cybercops bei den RBA
Bayerisches Landeskriminalamt	0
PP München	2
PP Oberbayern Nord	0
PP Oberbayern Süd	0
PP Oberfranken	0
PP Mittelfranken	0
PP Unterfranken	1
PP Schwaben Süd/West	0
PP Schwaben Nord	0
PP Niederbayern	0
PP Oberpfalz	0

Tabelle 1: Anzahl bei den Verbänden in den RBA beschäftigte Cybercops

2.3 Wie bewertet die Staatsregierung die Aufteilung in verschiedene spezialisierte Organisationseinheiten?

Die Trennung in verschiedene Organisationseinheiten hat sich bisher bewährt. Die RBA sind je nach Verband als Kommissariat oder als Teil eines Kommissariats organisiert. Einige RBA sind in Cybercrime-Organisationseinheiten eingegliedert (z. B. bei dem KFD 12 des PP München, K 11 in Augsburg). Beim PP Oberfranken (KPI (Z) Oberfranken), beim PP Mittelfranken (K 36 in Nürnberg), beim PP München (K 123) und beim BLKA (SG 210) sind die RBA zentralisiert. Die unterschiedliche organisatorische Anbindung der RBA richtet sich nach den jeweiligen Bedürfnissen der Verbände und den jeweiligen organisatorischen Rahmenbedingungen. Dabei wurden insbesondere die spezifischen Gegebenheiten in den Flächenpräsidien berücksichtigt.

Die RBA ist forensischer Dienstleister für alle Dienststellen der Schutz- und Kriminalpolizei im jeweiligen Zuständigkeitsbereich. Eine Endsachbearbeitung von Verfahren erfolgt in den RBA-Dienststellen nicht, sondern in den schutz- oder kriminalpolizeilichen Organisationseinheiten nach zugewiesener sachlicher Zuständigkeit gem. eines festgelegten Rahmenkataloges „Ermittlungstätigkeit der Kriminalpolizei“.

Im Hinblick auf die Einrichtung der Cybercrime-Kommissariate bei den Kriminalpolizeiinspektionen wurde das Bayerische Landeskriminalamt vom Bayerischen Staatsministerium des Innern, für Bau und Verkehr unter Einbindung der Verbände der Bayerischen Polizei mit der Prüfung beauftragt, die organisatorische Anbindung der RBA an die Cybercrime-Dienststellen zu prüfen. Bei der Bewertung sind spezifische Gegebenheiten in den Flächenpräsidien gleichrangig mit den bestehenden Bedürfnissen der Ballungsraumpräsidien zu berücksichtigen.

3.1 Sind der Staatsregierung Schnittstellenprobleme aufgrund von der verschiedenartigen organisatorischen Anbindung von Cybercrime-Ermittlungen und RBA-Aufgaben bekannt?
3.2 Wenn ja, um was für Schnittstellenprobleme handelt es sich?
3.3 Was gedenkt die Staatsregierung dagegen zu tun?
Die RBA ist forensischer Dienstleister für alle Dienststellen der Schutz- und Kriminalpolizei. In den RBA werden digitale Spuren gesichert, aufbereitet und ausgewertet und die Feststellungen und Ergebnisse in Berichtsform dem Auftraggeber (sachbearbeitende Dienststelle) zur Verfügung gestellt. Naturgemäß ergeben sich hier Schnittstellen zu jeder beauftragenden Dienststelle. Zum einen hat sich hier eine formulargebundene Beauftragung bewährt, um alle für die Erfüllung des Untersuchungsauftrages nötigen Informationen seitens der Sachbearbeitung an die RBA zu übermitteln. Zudem erfolgen im Einzelfall direkte Absprachen zwischen dem Auftraggeber und der RBA, um die Auswertungstiefe und -richtung in umfangreichen Fällen detailliert festzulegen.

Darüber hinaus erfolgt ein reger persönlicher fachlicher Austausch zwischen Cybercops und IT-Forensiker zur Nutzung des gegenseitigen fachspezifischen Wissens.

Hinsichtlich der Prüfung einer grundsätzlichen organisatorischen Anbindung der RBA an Cybercrime-Dienststellen dürfen wir auf die Antwort zu Frage 2.3 verweisen.

4.1 Wie viele Weiterbildungsmaßnahmen im Bereich Cybercrime gibt es bei der Bayerischen Polizei (bitte einzeln auflisten)?
4.2 Wie viele Beamtinnen und Beamte mit Führungsfunktion wurden in den letzten drei Jahren in diesem Bereich weitergebildet?
4.3 Wie viele Sachbearbeiterinnen und Sachbearbeiter wurden in den letzten drei Jahren in diesem Bereich weitergebildet?
Die Bayerische Polizei misst der Fortbildung ihrer Beamtinnen und Beamten im Bereich der Informations- und Kommunikationstechnologien größte Bedeutung bei. Daher haben wir im zentralen Fortbildungsprogramm der Bayerischen Polizei auch spezielle Seminare zum Themenkreis Bekämpfung der Cyberkriminalität aufgenommen. Die angebotenen Seminare werden fortlaufend an die sich ändernden Gegebenheiten angepasst und inhaltlich fortentwickelt. Die seit 2014 zentral am Fortbildungsinstitut der Bayerischen Polizei durchgeführten Seminare sind mit deren Bezeichnung, der Anzahl der Seminare und der Teilnehmerzahl in der nachfolgenden Tabelle aufgelistet.

Eine weitere Aufschlüsselung der Teilnehmerzahlen der letzten drei Jahre nach Führungskräften bzw. Sachbearbeitern wäre nur mit einem unverhältnismäßig hohen Aufwand möglich. Hierzu müsste zusätzlich der dem jeweiligen Seminarteilnehmer zugeordnete Dienstposten einzeln betrachtet werden. Eine solche Auswertung ist in der zur Verfügung stehenden Zeit mit einem verhältnismäßigen Aufwand nicht zu leisten.

Bezeichnung des Seminars	Anzahl der Seminare / Teilnehmer insgesamt im Jahr:			Anzahl der geplanten Seminare im Jahr 2017
	2014	2015	2016	
Cybercrime - Datenauswertung Tools				1
Cybercrime - Grundlagen und Internet				8
Cybercrime - Malwareanalyse				1
Cybercrime - Manipulation	3/37	2/20	2/26	2
Cybercrime - Massendaten 1	2/24	2/19	1/14	1
Cybercrime - Massendaten 2	2/15	1/11	1/9	1
Cybercrime - Netzwerkforensik				1
Cybercrime - Recht 1	4/72	3/54	4/71	2
Cybercrime - Recht 2	2/37	2/39	2/39	1
Cybercrime - TK-Spuren 1	2/55	2/53	2/56	2
Cybercrime - Update Sb	1/24	1/23	1/23	2
Internet, Netzwerkgrundlagen	2/23	2/23	3/39	
IuK Grund Windows Client	2/20	1/11	1/13	
RBA Kryptografie, Steganografie			1/13	
RBA Live Forensik				1
RBA Mobile devices Grundlagen	1/12	1/12	1/13	2
RBA Mobile devices Tools	1/10	1/12	5/10	1
RBA Mobile Update				1
RBA Netzwerk Forensik		1/10	1/11	
RBA News	2/55	1/23	2/60	2
RBA Praktika		1/2		2
RBA Sicherung	1/13	1/10		1
RBA Update	2/24	4/74	2/22	2
RBA Virtualisierung und Cloud				1
RBA Windows Server			1/11	
RBA X-Ways 1			1/10	1
RBA X-Ways 2			1/14	4

Die Update-Seminare am Fortbildungsinstitut der Bayerischen Polizei (BPFI) Ainring und regelmäßige Arbeitstagungen des Bayerischen Landeskriminalamts bieten unseren Spezialisten zusätzlich die Möglichkeit zum aktuellen Informationsaustausch im jeweiligen Bereich.

Einzelne Experten der Bayerischen Polizei nahmen anlassbezogen z. B. an Fortbildungsveranstaltungen des Bundeskriminalamts (BKA), der Deutschen Hochschule der Polizei (DHPol), der Europäischen Polizeiakademie (CEPOL) und an Fortbildungsveranstaltungen externer Anbieter aus dem nicht-staatlichen Bereich teil.

5.1 Wie viele Beamtinnen und Beamte aus der 2. Qualifikationsebene werden zu Spezialist(inn)en ausgebildet?
Bei der Bearbeitung der Delikte aus dem Bereich „Cybercrime“ werden auch spezialisierte Sachbearbeiter der Ermittlungsgruppen bzw. der Fachkommissariate eingesetzt. Diese absolvieren entsprechend den ihnen zugewiesenen Aufgaben auch die einschlägigen zentralen Fortbildungsangebote. Im Übrigen verweisen wir auf unsere Ausführungen zu den Fragen 4.1 mit 4.3.

5.2 Schließt der Freistaat Bayern Verträge mit Hochschulen, um dort Polizist(inn)en in spezialisierten Studiengängen ausbilden zu lassen (bitte entsprechende Hochschulen und Studiengänge namentlich aufführen)?
Zwar werden interessierte Polizeibeamte an externen Hochschulen zu Computer- und Internetkriminalisten weitergebildet; zwischen dem Freistaat Bayern und den von den Beamten besuchten Hochschulen bestehen aber keine speziellen Verträge.

5.3 Welche zusätzlichen Maßnahmen werden ergriffen, dass Polizeibeamtinnen/-beamten innerhalb von Polizeiinspektionen gezielt mit dem nötigen Fachwissen ausgebildet werden?

Um dem wachsenden Bedarf an qualifizierter Fortbildung zum Thema Cybercrime zeitgerecht nachkommen zu können, hat die Bayerische Polizei mit der Nutzung des „E-Learning“ auch bei der Wissensvermittlung einen neuen Weg eingeschlagen. Ergänzend zu den zentralen Fortbildungsangeboten hat das Fortbildungsinstitut der Bayerischen Polizei die elektronischen Lernprogramme „Grundlegende Medienkompetenz“, „Erster Angriff Cybercrime“, „Soziale Netzwerke“, „Elektronischer Zahlungsverkehr“ und „Qualifizierte Anzeigenaufnahme“ entwickelt. Diese sind über die „Lernplattform der Bayerischen Polizei“ dezentral allen Beschäftigten der Bayerischen Polizei zugänglich und dienen neben der Wissensvermittlung auch als Nachschlagewerke. Damit ist sichergestellt, dass insbesondere Beamte im Wach- und Streifendienst, welche im Rahmen des sog. ersten Angriffs die erforderlichen Erst- und Sofortmaßnahmen bei Bekanntwerden einer Straftat aus dem Deliktsbereich „Cybercrime“ zu treffen haben, mit dem erforderlichen Basiswissen einleiten können.

Aufbauend auf dem vermittelten Grundlagenwissen können von unseren Beschäftigten über das „Infoportal Cybercrime“ stets aktuell Informationen zum Bereich Cyberkriminalität abgerufen werden. Das vom Bayerischen Landeskriminalamt qualitätsgesicherte Infoportal stellt ein effektives Hilfsmittel bei der Bearbeitung von Fällen aus dem vielfältigen Deliktsbereich dar.

6.1 Inwieweit sind die Ermittler bei der Bayerischen Polizei außerhalb der Spezialistenbereiche mit der Möglichkeit der spezifischen Ermittlungsinstrumente und der forensischen Spurensicherung vertraut?

Die IT-forensische Spurensicherung erfolgt bei der Bayerischen Polizei (auch aus Gründen der Gerichtsverwertbarkeit) nur durch speziell geschulte Beamte im Fachbereich Forensik oder Forensische IuK bei den RBA oder den Cybercrime-Dienststellen.

Die allgemein kriminalpolizeilichen Sachbearbeiter sind grundsätzlich nicht mit den spezifischen Ermittlungsinstrumenten zur forensischen Spurensicherung betraut. Ihre Hauptaufgabe liegt in der Ermittlungsführung. Im Rahmen des fallbezogenen Austausches zwischen Ermittler und IT-Forensiker sowie durch Fortbildungsveranstaltungen werden die Ermittler regelmäßig über die Möglichkeiten und Grenzen der IT-Forensik informiert.

6.2 Haben die Sachbearbeiter aus dem Bereich der Cybercrime-Ermittlungen bzw. der Cybercrime-RBA genug Ressourcen, um die Ermittlungsunterstützung zu leisten?

Im Falle der RBA darf auf die Beantwortung der Frage 1.2 verwiesen werden.

Hinsichtlich der Sachbearbeiter aus dem Bereich Cybercrime-Ermittlungen muss festgehalten werden, dass die Schnelllebigkeit des Internets sowie die zahlreichen Entstehungsmöglichkeiten und die Vielfalt von Internet- bzw. Netzwerkspuren Herausforderungen sind, die grundsätzlich jede Polizeibeamtin und jeder Polizeibeamte annehmen und innerhalb ihrer/seiner originären Zuständigkeit bewältigen muss. Hinsichtlich der Maßnahmen zur Fortbildung der Polizeibeamten darf auf die Beantwortung der Frage 5.3 verwiesen werden.

Die Bayerische Polizei reagiert auf die Herausforderung „Cybercrime“ mit einem mehrstufigen Konzept, um auf allen Ebenen der Sachbearbeitung Professionalität und Qualität gewährleisten zu können: Die Schutzpolizei ist einerseits bei der Aufnahme von Anzeigen und andererseits auch bei der Endsachbearbeitung von Cybercrime-Delikten in einfach gelagerten Fällen – wie z. B. Beleidigung – im Internet gefordert. Das „Tatmittel Internet“ gewinnt hier zunehmend an Bedeutung. In den Ermittlungsgruppen der Polizeiinspektionen werden speziell geschulte und fortgebildete Beamte für die Ermittlungen in diesem Bereich eingesetzt, die als sogenannte Schwerpunktsachbearbeiter Cybercrime zugleich als Multiplikatoren und Ansprechpartner bei der Anzeigenaufnahme in der Dienststelle fungieren.

Im Bereich der Kriminalpolizei sind für die Bearbeitung von Cybercrime-Delikten rund 200 speziell für diesen Bereich geschulte Ermittler eingesetzt. Bei den Regionalen Beweismittelsicherungs- und Auswertungsstellen (RBA) sind darüber hinaus rund 100 Beamte und Tarifbeschäftigte tätig.

Die speziell geschulten Ermittler für den Bereich „Cybercrime“ bei den Kriminalpolizeien und dem Bayerischen Landeskriminalamt leisten im Rahmen der vorhandenen personellen Ressourcen und der persönlichen Arbeitsbelastung regelmäßig Unterstützungs- und Beratungsleistungen durch telefonischen oder persönlichen Support für andere Dienststellen. Die Kapazitäten für die Beratung anderer Dienststellen differiert je nach Belastung des einzelnen Sachbearbeiters.

Auf die wachsende Herausforderung durch die stetige Digitalisierung der Gesellschaft und damit einhergehende stetig steigende Deliktszahlen im Bereich Cybercrime hat die Staatsregierung reagiert. Mit ihrem Sicherheitskonzept „Sicherheit durch Stärke“ hat die Staatsregierung beschlossen, die Bekämpfung der Internet- und Computerkriminalität weiter zu intensivieren, u. a. durch den Einsatz von mehr Internetpolizisten in den Polizeipräsidien. Hierzu sollen im Jahr 2017 weitere rund 70 Computer- und Internetkriminalisten eingestellt und in den Jahren 2017 und 2018 für den bayernweiten und flächendeckenden Einsatz ausgebildet werden. Dadurch werden die Dienststellen um noch mehr IT-Know-how verstärkt.

6.3 Wie viele Anfragen an die Spezialistenbereiche kamen in den letzten drei Jahren von fachfremden Polizeidienststellen (bitte nach Jahr auflisten)?

Über an die RBA-Dienststellen oder Cybercrime-Dienststellen gestellte Anfragen fachfremder Polizeidienststellen werden keine Statistiken geführt.

7.1 In welchen bayerischen Polizeipräsidien werden durch Cybercops anlassunabhängige bzw. eigeniniative Ermittlungen/Recherchen in nicht indexierten Bereichen des Internets (sog. Darknet bzw. Underground-Foren) durchgeführt?

Anlassunabhängige Recherchen im Internet (sowohl in indexierten Bereichen als auch im Darknet) sind grundsätzlich Aufgabe des SG 543 beim Bayerischen Landeskriminalamt.

Darüber hinaus steht es den Dienststellen der Bayerischen Polizei mit Aufgabenzuschnitt Cybercrime als auch in anderen tangierten Deliktsbereichen frei, neben dem Bayerischen Landeskriminalamt anlassunabhängig im Internet zu recherchieren.

7.2 In wie vielen Fällen wurden dabei in Bayern lebende bzw. behördlich gemeldete Täter identifiziert (bitte um Auflistung der entsprechenden Deliktsbereiche, z. B. Staatsschutz/Terrorismus, Bandenkriminalität, Drogen-, Waffendelikte, Carding)?

In der Polizeilichen Kriminalstatistik erfolgt keine Erfassung, auf welchen Anlassgrund die jeweiligen Ermittlungen zurückgehen, weswegen zu dieser Frage keine belastbaren Aussagen getroffen werden können.

7.3 In wie vielen Fällen ermittelten Cybercops dabei als Verdeckte Ermittler (VE) i. S. d. § 110a Strafprozessordnung (StPO)?

Bayernweit wurde bislang kein Cybercop als Verdeckter Ermittler i. S. d. §110a StPO eingesetzt.

8.1 Inwieweit erfolgt im Bereich dieser eigeniniativen Ermittlungen ein Austausch zwischen den einzelnen Polizeipräsidien bzw. Bundesländer um Mehrfachermittlungen zu einer relevanten „virtuellen Identität“ (z. B. Nickname im Forum) zu vermeiden?

Grundsätzlich kann nicht ausgeschlossen werden, dass verschiedene Dienststellen gegen dieselbe tatverdächtige Person bzw. virtuelle Identität mit Ermittlungen beginnen, insbesondere wenn diese mehrere Tathandlungen in unterschiedlichen Deliktsbereichen durchführt. Eine Zusammenführung der Erkenntnisse erfolgt über die Erfassung des Falls in den polizeilichen Datenbanken. Hierbei erfolgt ein Datenabgleich und im Trefferfall die Generierung einer Meldung an die betroffenen Dienststellen, welche zum Informationsaustausch und erforderlichenfalls zu koordinierten Maßnahmen führt. Darauf baut ein intensiver Austausch auf regionaler und nationaler Ebene auf.

8.2 Sieht die Staatsregierung im diesem Bereich noch weiteren Koordinierungs- bzw. Handlungsbedarf?

Im Hinblick auf die stetig wachsende Bedrohung durch Cyberkriminalität müssen die Eingriffsbefugnisse der Polizei zur Gefahrenabwehr und die Ermittlungsbefugnisse der Polizei zur Strafverfolgung besser an die digitale Herausforderung angepasst werden. Die Staatsregierung setzt sich für eine Verstärkung der polizeilichen nationalen wie internationalen Zusammenarbeit und der verstärkten Nutzung der Möglichkeiten des polizeilichen Datenaustauschs ein. Jede Polizistin und jeder Polizist muss nach Maßgabe der rechtlichen Rahmenbedingungen jederzeit und überall Zugriff auf diejenigen Informationen haben, welche für ihre/seine Aufgabenerfüllung erforderlich sind.

Darüber hinaus setzt sich die Staatsregierung für den Aufbau eines Europäischen Kriminalaktennachweises (EPRIS) von Polizei- und Sicherheitsbehörden ein, damit europaweit abgefragt werden kann, ob polizeiliche Akten oder Hinweise über eine Person vorliegen.

Vor dem Hintergrund der digitalen Bedrohungen werden die von der Arbeitsgruppe „Cloud Evidence“ des Cybercrime-Convention-Komitees am 16.09.2016 vorgelegten Vorschläge zur Fortentwicklung der Cybercrime-Konvention des Europarates ebenso begrüßt wie der Umstand, dass der Rat der Europäischen Union in den Ratsschlussfolgerungen „Improving Criminal Justice in Cyberspace“ (Ratsdok. 10007/16) vom 09.06.2016 insoweit die Europäische Kommission bereits mit einem Handlungsmandat ausgestattet hat. Bezogen auf diese Thematik wird seitens der Staatsregierung der Abschluss weiterer bzw. die Anpassung bereits bestehender internationaler justizieller Rechtshilfeabkommen mit anderen Staaten forciert.