Bayerischer Landtag

17. Wahlperiode

24.03.2016 17/**10273**

Schriftliche Anfrage

des Abgeordneten **Prof. Dr. Peter Paul Gantzer SPD**
vom 13.01.2016

Cybercrime-Stellen in Bayern

Ich frage die Staatsregierung:

1. Welche Einrichtungen beschäftigen sich in Bayern mit der Bekämpfung von Cybercrime?

2. Welche Aufgabenbeschreibung und welche Eingruppierung haben die einzelnen Stellen?

3. a) Wie viele einzelne Stellen sind in diesen Einrichtungen haushaltetisch hinterlegt (insgesamt und aufgeschlüsselt nach den einzelnen Stellen)?
   b) Wie viele Stellen sind davon nicht besetzt (aufgeschlüsselt nach den einzelnen Einrichtungen)?
   c) In welcher Eingruppierung befinden sich die unbesetzten Stellen (aufgeschlüsselt nach den einzelnen Stellen)?

4. Wie hat sich die Arbeitsbelastung der einzelnen Einrichtungen seit ihrem Entstehen entwickelt?

5. Wie hat sich die personelle Ausstattung der einzelnen Einrichtungen seit ihrem Entstehen entwickelt?

6. a) Wie hoch waren die gesamten Kosten, die zur Bekämpfung von Cybercrime jährlich zur Verfügung gestellt wurden, seit 2005?
   b) Wie haben sich die Kosten für die einzelnen Einrichtungen seit ihrem Entstehen entwickelt (aufgeschlüsselt nach Personalkosten, Sachmittel)?

7. Wie ist die Arbeitsbilanz der einzelnen Einrichtungen im Bezug auf Anzeigen, Strafverfolgung, Aufklärung, Prävention?

8. Wie verläuft die Zusammenarbeit der einzelnen Einrichtungen?

Antwort

des Staatsministeriums des Innern, für Bau und Verkehr
vom 20.02.2016

1. Welche Einrichtungen beschäftigen sich in Bayern mit der Bekämpfung von Cybercrime?

Bei dem Bereich der Cyberkriminalität handelt es sich um ein äußerst komplexes und zugleich extrem dynamisches Deliktsfeld, dessen Bekämpfung die Bayerische Polizei vor neue Herausforderungen stellt.

Vor diesem Hintergrund sowie der weiter wachsenden Bedeutung des Internets in unserer Gesellschaft und den daraus entstehenden Chancen und Risiken wurden in den letzten Jahren bei der Bayerischen Polizei **umfangreiche strukturelle und organisatorische Maßnahmen** realisiert.

Um den neu entstandenen Kriminalitätsformen wirkungsvoll und konsequent entgegentreten zu können, agiert die Bayerische Polizei mit einem **mehrstufigen Aufbau**:

- Bereich der Schutzpolizei:

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 Mulitiplikatoren und Ansprechpartner bei der Anzeigenaufnahme in der Dienststelle fungieren.

- Bereich der Kriminalpolizei:

Aufgrund der quantitativen und qualitativen Entwicklung des Phänomens wurden **spezialisierte Arbeitsbereiche** bei allen Kriminalpolizeiinspektionen eingerichtet, bei denen die Bekämpfung von Cybercrime im engeren Sinn oder schwerwiegende Fälle, wie Hacking oder das Ausspähen von Daten, gebündelt werden.

Für den Bereich **Augsburg** wurde durch das Polizeipräsidium Schwaben Nord zum 01.11.2015 innerhalb der Kriminalpolizeiinspektion Augsburg ein spezielles Kommissariat 11 – Cybercrime zur Forcierung der Bekämpfung der Cyberkriminalität ausgebracht.

Das Polizeipräsidium **Mittelfranken** hat die Bekämpfung der Cybercrime-Delikte im engeren Sinn beim Kommissariat 25 des Kriminalfachdezernats 2 Nürnberg teilzentralisiert. Es werden dort alle diesbezüglichen Fälle aus dem Stadtgebiet Nürnberg bearbeitet. Außerhalb von Nürnberg übernimmt das K 25 auf Zuweisung schwerwiegende Delikte aus ganz Mittelfranken. Für einfach gelagerte Delikte wurden die Strukturen analog der Flächenpräsidien etabliert mit Cybercrime-Arbeitsbereichen in den Kriminalpolizeiinspektionen.

Beim Polizeipräsidium **München** wurde eigens ein neues Kriminalfachdezernat (KFD 12) errichtet. Das KFD 12 glie-

dert sich in ein Kommissariat 121 – Zentrale Aufgaben, ein Kommissariat 122 – Besondere Erscheinungsformen der IuK-Kriminalität sowie ein Kommissariat 123 – EDV-Beweismittelsicherung, Telekommunikationsüberwachung.

- Bayerisches Landeskriminalamt:

Das Bayerische Landeskriminalamt tritt dem stark wachsenden Kriminalitätsfeld Cybercrime mit der Einrichtung eines neuen Dezernates (Dezernat 54) entgegen, welches sich in drei Sachgebiete (Zentralstelle, Ermittlungen und Netzwerkfahndung) gliedert. Primäre Aufgabenstellung besteht in Serviceleistungen und Beratungen für andere Polizeidienststellen, insbesondere bei komplexen Ermittlungen. Dies zeigt sich auch durch die Einrichtung einer Zentralen Ansprechstelle Cybercrime (ZAC), die der Wirtschaft und sonstigen öffentlichen wie nichtöffentlichen Stellen, aber auch den Polizeiverbänden als Beratungs- und Unterstützungsorgan zur Verfügung steht.

Ferner wurde das bereits bestehende Sachgebiet „Netzwerkfahndung“ in seiner jetzigen Form mit den Fachbereichen „Anlassabhängige/-unabhängige/verdeckte Recherche“, „Soziale Netzwerke“ und „Ansprechstelle Kinderpornografie“ in das neue Dezernat Cybercrime integriert.

Großverfahren oder Straftaten mit internationalen Bezügen werden beim Bayerischen Landeskriminalamt (BLKA) bearbeitet.

- Regionale Beweismittelsicherungs- und Auswertungsstellen (RBA):

Außerdem existieren bei der Bayerischen Polizei **21** Regionale Beweismittelsicherungs- und Auswertungsstellen (RBA). Derzeit sind bei den RBAs bzw. vergleichbaren Aufgabenbereichen der Polizeipräsidien **110** Personen beschäftigt.

Die RBAs kümmern sich u. a. um alle Belange der Sicherung und Auswertung von EDV-Beweismitteln im Strafverfahren. Hierzu werten sie Datenträger aus, fertigen Datensicherungen an und vertreten ihre Feststellungen ggf. vor Gericht. Für die Tätigkeit bei den RBAs gibt es bei der Bayerischen Polizei umfangreiche Fortbildungsangebote für Polizeivollzugsbeamte. Des Weiteren werden dort auch technische Spezialisten aus verschiedenen Bereichen eingesetzt.

Die RBA sind allerdings deliktsübergreifend tätig. Demnach sind diese nicht ausschließlich für den Bereich Cybercrime, sondern auch für die Auswertung von Datenträgern im Zusammenhang mit anderen Straftaten (beispielsweise Mobiltelefone) zuständig.

Die Bekämpfung dieses Deliktsfeldes tangiert alle Ebenen polizeilichen Handelns – in unterschiedlicher Komplexität –, beginnend von Bearbeitung diesbezüglicher Straftaten bei den Schutzpolizeidienststellen bis zur Endsachbearbeitung bei speziellen Dienststellen der Kriminalpolizei sowie des Bayerischen Landeskriminalamts.

Insgesamt sind für die Bearbeitung von Cybercrime-Delikten **mehr als 200** speziell für diesen Bereich geschulte Kriminalbeamtinnen und -beamte bei den Kriminalpolizeiinspektionen der Flächenpräsidien und den Ballungsraumpräsidien sowie dem Bayerischen Landeskriminalamt eingesetzt. Bei den RBA sind darüber hinaus **110 Beamte und Arbeitnehmer** beschäftigt.

Zusätzlich hierzu sind die diesbezüglich umfangreichen Aus- und Fortbildungsmaßnahmen für Polizeibeamtinnen und Beamte anzuführen. Um diese adäquat auf dementsprechende Aufgabenstellungen vorzubereiten, wird bereits in der Ausbildung jedem Polizeivollzugsbeamten ein umfangreiches Maß an IT-Grundlagenwissen vermittelt, welches durch regelmäßige Fortbildung aktualisiert und für spezifische Aufgabenbereiche – sei es bei den RBAs oder bei den Fachdienststellen der Kriminalpolizei – vertieft wird.

2. Welche Aufgabenbeschreibung und welche Eingruppierung haben die einzelnen Stellen?

3. a) Wie viele einzelne Stellen sind in diesen Einrichtungen haushaltetisch hinterlegt (insgesamt und aufgeschlüsselt nach den einzelnen Stellen)?

b) Wie viele Stellen sind davon nicht besetzt (aufgeschlüsselt nach den einzelnen Einrichtungen)?

c) In welcher Eingruppierung befinden sich die unbesetzten Stellen (aufgeschlüsselt nach den einzelnen Stellen)?

5. Wie hat sich die personelle Ausstattung der einzelnen Einrichtungen seit ihrem Entstehen entwickelt?

Aufgrund des Sachzusammenhangs werden die Fragestellungen 2, 3 a bis 3 c sowie 5 zusammenhängend beantwortet.

Da das Deliktsphänomen Cybercrime inzwischen nahezu die gesamte Kriminalität durchdringt, beschränkt sich die Beantwortung o. g. Fragestellungen auf spezialisierte Dienststellen der Kriminalpolizei, die mit Schwerpunkt Delikte aus dem Bereich der Cyberkriminalität bearbeiten.

Hierbei handelt es sich im Bereich des Polizeipräsidiums München um das Kriminalfachdezernat (KFD) 12 – Cybercrime, im Bereich des Polizeipräsidiums Mittelfranken um das Kommissariat 25 – IuK-,Computer- und Zahlungskartenkriminalität des Kriminalfachdezernats 2 Nürnberg, das Kommissariat 11 – Cybercrime der Kriminalpolizeiinspektion (KPI) Augsburg sowie das Dezernats 54 – Cybercrime des Bayerischen Landeskriminalamts .

Die Stellenausstattung der o. g. Dienststellen mit Stand 01.01.2016 ist in der nachfolgenden Übersicht detailliert dargestellt. Daraus ersichtlich ist auch die Entwicklung der Stellensituation seit Etablierung der jeweiligen Dienststelle:

Dienststelle	Zeitpunkt der Ausbringung		01.01.2016	
	Sollstärke	Anzahl tatsächlich eingesetzte Beamte	Sollstärke	Anzahl tatsächlich eingesetzte Beamte
Bayerisches Landeskriminalamt				
Dezernat 54[1]	7	37	28	41
Polizeipräsidium München				
Kriminalfachdezernat 12[2]	30	35	41	41,65
Polizeipräsidium Mittelfranken				
Kommissariat 25 (KFD 2 Nürnberg)[3]	18	14,8	23	23,6
Polizeipräsidium Schwaben Nord				
Kommissariat 11 (KPI Augsburg)[4]	12	11,8	12	11,8

[1]Ausbringung Dezernat 54 zum 01.01.2014

[2]Ausbringung KFD 12 zum 01.04.2014; Aufnahme des Wirkbetriebs bereits ab 15.10.2013 als „Cyberfachdezernat im Aufbau“

[3]Wirkbetrieb des K 25 mit Schwerpunktbearbeitung Cybercrime am 01.08.2014

[4] Ausbringung K 11 zum 01.11.2015

Im Hinblick auf das Dezernat 54 sowie das Kriminalfachdezernat 12 des Polizeipräsidiums München ist ergänzend anzumerken, dass sich beide Dienststellen noch im Aufbau befinden und dort zukünftig noch weitere Stellenzuführungen vorgesehen sind. Die nächste Zuteilung von Stellen wurde bereits mit Wirkung zum 01.09.2016 verfügt.

Bei den vorgenannten Organisationseinheiten sind insgesamt 88 Dienstposten für Beamte der 3. und 4. Qualifikationsebene ausgebracht, die eine Besoldung nach den BesGr. A 15 (1x), A 14 (3x), A 13 (7x), A 12 (33x) und A 11 (44x) ermöglichen. Von diesen 88 Dienstposten sind aktuell 5 nicht besetzt, davon 4 im Dezernat 54 des BLKA. Die entsprechenden Besetzungs- und Auswahlverfahren sind bereits im Gange.

4. Wie hat sich die Arbeitsbelastung der einzelnen Einrichtungen seit ihrem Entstehen entwickelt?

Die Einrichtung von Arbeitsbereichen Cybercrime erfolgte sukzessive und verbandsspezifisch in den letzten Jahren, weshalb vergleichende Zeitreihen nur bedingt aussagekräftig sind. Als ein Trendmesser zur Belastungsmessung wird hier die Polizeiliche Kriminalstatistik (PKS) hinzugezogen. Anzumerken ist hierbei jedoch, dass circa 45 % der bei der Bayerischen Polizei im Jahr 2014 angezeigten Fälle aus diesem Bereich nicht zur PKS gemeldet werden können, da es sich zum Beispiel um sogenannte Auslandsdelikte handelt.

Die Anzahl erfasster Fälle im Deliktsfeld Computerkriminalität[5] hat sich im Zeitraum von 2010 (8.510) bis 2014 (11.024) erhöht. Die Aufklärungsquote ist im Vergleich zum Jahr 2005 (51,8 %) auf 34,3 % im Jahr 2014 gesunken. Die Anzahl der erfassten Fälle im Bereich der Internetkriminalität[6] ist in den vergangenen Jahren relativ konstant geblieben (2010: 22.965 Fälle und 2014: 21.261) während die Aufklärungsquote von 2010 (58,3 %) auf 46,8 % gesunken ist.

Aus Gründen der Vergleichbarkeit erfolgt eine Darstellung der Entwicklung der Computerkriminalität sowie der Internetkriminalität seit dem Jahr 2010.

[5] Der Begriff Computerkriminalität ist definiert und umfasst in der PKS folgende Delikte:

897000 – Computerkriminalität (Summenschlüssel)	
Schlüssel	Klartext
674210	Datenveränderung § 303 a Strafgesetzbuch (StGB)
674220	Computersabotage § 303 b StGB
678010	Ausspähen von Daten § 202 a StGB
678020	Abfangen von Daten gemäß § 202 b StGB
678030	Vorbereiten des Ausspähens und Abfangens von Daten gemäß § 202 c StGB
516300	Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN § 263 a StGB
517510	Computerbetrug (sonstiger) § 263 a Abs. 1 und 2 StGB
517520	Vorbereitung des Computerbetruges § 263 a Abs. 3 StGB
517900	Missbräuchliche Nutzung von Telekommunikationsdiensten § 263 a StGB
543010	Fälschung beweiserheblicher Daten § 269 StGB
543020	Täuschung im Rechtsverkehr bei Datenverarbeitung § 270 StGB
715100	Softwarepiraterie (private Anwendung z. B. Computerspiele)
715200	Softwarepiraterie in Form gewerbsmäßigen Handelns

[6] Als Internetkriminalität werden Straftaten bezeichnet, deren Tatbestandsverwirklichung unter Nutzung des Internet erfolgte.

Entwicklung des Deliktsfeldes „Computerkriminalität“ in Bayern

In nachstehender Tabelle ist die Fallentwicklung des Summenschlüssels **„Computerkriminalität“** in Bayern ersichtlich:

Jahr	Schlüssel der Tat	Straftat	erfasste Fälle		davon Versuche		aufgeklärte Fälle	
			Anzahl	Anteil in %	Anzahl	Anteil in %	Anzahl	Anteil in %
2014	897000	Computer-kriminalität	11.024	1,7	1.064	9,7	3.026	27,4
2013	897000	Computer-kriminalität	11.920	1,9	1.444	12,1	3.330	27,9
2012	897000	Computer-kriminalität	11.055	1,8	1.198	10,8	3.190	28,9
2011	897000	Computer-kriminalität	10.146	1,6	879	8,7	2.895	28,5
2010	897000	Computer-kriminalität	8.510	1,4	646	7,6	2.923	34,3

Entwicklung der Internetkriminalität in Bayern

Die PKS-Tabelle **„Internetkriminalität“** steht auswertbar erst ab dem Berichtsjahr 2010 zur Verfügung, deswegen der Auswertezeitraum 2010 bis 2014 für die Internetkriminalität in Bayern:

Jahr	Straftat	erfasste Fälle		davon Versuche		aufgeklärte Fälle	
		Anzahl	Anteil in %	Anzahl	Anteil in %	Anzahl	Anteil in %
2014	Internetkriminalität insgesamt	21.261	100	1.866	8,8	9.948	46,8
2013	Internetkriminalität insgesamt	24.292	100	3.081	12,7	10.378	42,7
2012	Internetkriminalität insgesamt	21.963	100	2.845	13	9.916	45,1
2011	Internetkriminalität insgesamt	20.609	100	1.774	8,6	10.345	50,2
2010	Internetkriminalität insgesamt	22.965	100	1.698	7,4	13.399	58,3

Entwicklung der Endsachbearbeitung von Cybercrime-Dienststellen in Bayern

In nachfolgenden Tabellen sind die Fälle, die von den Dienststellen endsachbearbeitet zur PKS gemeldet sind, dargestellt.

Das **Kommissariat 11** Augsburg wurde erst am 01.11.2015 gegründet, daraus resultierend liegen keine PKS-Daten bis einschließlich des Jahres 2014 vor.

Das **Kriminalfachdezernat 12 München** begann mit seinem Wirkbetrieb am 15.10.2013, dementsprechend liegen lediglich PKS-Daten für die Berichtsjahre 2013 und 2014 vor.

Fälle des KFD 12 Polizeipräsidium (PP) München							
Jahr	Straftat	erfasste Fälle		davon Versuche		aufgeklärte Fälle	
		Anzahl	Anteil in %	Anzahl	Anteil in %	Anzahl	Anteil in %
2014	Straftaten insgesamt	218	100	24	11	128	58,7
2013	Straftaten insgesamt	50	100	12	24	37	74

Vor dem Hintergrund, dass das **Dezernat 54** des BLKA am 01.01.2014 ausgebracht wurde, liegen nur PKS-Daten des Jahres 2014 vor.

Fälle des Dez 54 BLKA							
Jahr	Straftat	erfasste Fälle		davon Versuche		aufgeklärte Fälle	
		Anzahl	Anteil in %	Anzahl	Anteil in %	Anzahl	Anteil in %
2014	Straftaten insgesamt	1	100	0	0	0	0

Das **Kommissariat 25 Nürnberg** hat keine ausschließliche Zuständigkeit zur Bearbeitung von Cybercrime, dort werden – neben der schwerpunktmäßigen Bearbeitung von Cybercrime-Delikten – auch allgemeine Fälle von Wirtschaftskriminalität/Betrug bearbeitet. Daher sind die bearbeiteten Fälle von Cybercrime von diesem Kommissariat aus der anliegenden PKS-Tabelle nicht trennscharf herauszulesen.

Fälle des K 25 Nürnberg							
Jahr	Straftat	erfasste Fälle		davon Versuche		aufgeklärte Fälle	
		Anzahl	Anteil in %	Anzahl	Anteil in %	Anzahl	Anteil in %
2014	Straftaten insgesamt	2.604	100	146	5,6	1.221	46,9
2013	Straftaten insgesamt	2.907	100	295	10,1	1.208	41,6
2012	Straftaten insgesamt	2.017	100	198	9,8	1.045	51,8
2011	Straftaten insgesamt	2.005	100	112	5,6	1.042	52
2010	Straftaten insgesamt	1.794	100	98	5,5	732	40,8

Insgesamt resultiert daraus eine Zunahme der Arbeitsbelastung von Organisationseinheiten im Bereich der Cybercrimebekämpfung der Bayerischen Polizei.

Im Bereich der regionalen Beweismittelsicherungs- und Auswerteeinheiten (RBA) ist durch Cybercrime keine wesentliche Veränderung der Arbeitsbelastung festzustellen. Insgesamt werden dort etwa 2 bis 5 % der Arbeit für Aufträge im Bereich Cybercrime aufgewendet.

Zusammenfassend ist festzuhalten, dass es sich bei Cybercrime grundsätzlich um Straftaten handelt, die sich gegen das Internet, weitere Datennetze, informationstechnische Systeme oder deren Daten richten. Darüber hinaus umfasst der Begriff auch Straftaten, die durch Informations- oder Kommunikationstechnik begangen werden.

Weiterhin ist anzumerken, dass Cybercrime eine immer größere Rolle in den Bereichen klassischer Kriminalität, z. B. dem Waffen-, Sprengstoff- und Munitionshandel spielt, der Betäubungskriminalität und vor allem der Wirtschaftskriminalität und den Delikten zum Nachteil der sexuellen Selbstbestimmung (z. B. Kinderpornografie).

Durch Cybercrime ist in diesen Bereichen der Ermittlungsaufwand durch Verlagerung von Kommunikation der Täter und des notwendigen Erwerbs von Methodenkompetenz bei der Polizei angestiegen.

6. a) Wie hoch waren die gesamten Kosten, die zur Bekämpfung von Cybercrime jährlich zur Verfügung gestellt wurden seit 2005?

b) Wie haben sich die Kosten für die einzelnen Einrichtungen seit ihrem Entstehen entwickelt (aufgeschlüsselt nach Personalkosten, Sachmittel)?

Die insgesamt im Polizeisachhaushalt veranschlagten Haushaltsmittel stehen für die Bekämpfung sämtlicher Kriminalitätsbereiche zur Verfügung und können nicht auf einzelne Bereiche wie z. B. Cybercrime aufgeschlüsselt werden. Es obliegt grundsätzlich den jeweiligen Polizeiverbänden in welchem Deliktsbereich lageanpasst Einsatz- und Ausstattungsschwerpunkte vorgenommen werden.

Dementsprechend wurde und wird der Bereich Cybercrime jährlich bisher ausschließlich Zug um Zug über die Budgets der Polizeipräsidien finanziert. Im Rahmen des Nachtragshaushalts 2014 konnten für die Einrichtung der Cyberlabore im Bayerischen Landeskriminalamt einmalig Haushaltsmittel in Höhe von 425.000,-- € zugewiesen werden. Eine weitere Zuweisung aus zentralen Mitteln ist nicht erfolgt. Über die Höhe der von den Verbänden eigenverantwortlich festgelegten Kosten für die Ausstattung und den Betrieb von Cybercrimedienststellen kann von zentraler Stelle keine Aussage getroffen werden.

7. Wie ist die Arbeitsbilanz der einzelnen Einrichtungen im Bezug auf Anzeigen, Strafverfolgung, Aufklärung, Prävention?

Hinsichtlich der Fragen zu Anzeigen, Strafverfolgung und Aufklärung darf auf die Beantwortung der Frage 4 verwiesen werden. Für den Bereich der Prävention stellt sich die Arbeitsbilanz der einzelnen Einrichtungen wie folgt dar:

Eine gesamtgesellschaftliche Kriminalprävention ist Teil des Bayerischen Sicherheitskonzepts. Ziel der Bayerischen Polizei ist es dabei, Straftaten möglichst erst gar nicht entstehen zu lassen. Nach der Organisationsreform der Bayerischen Polizei wurden die bestehenden Regelungen zur Polizeilichen Kriminalprävention umfassend überarbeitet. Als Resultat wurde eine bayernweit verbindliche Rahmenkonzeption für die Polizeiliche Kriminalprävention in Kraft gesetzt. Den einzelnen Phänomenen wurden entsprechende Themenblätter zugeordnet, die sich auch auf die Themenfelder Internetkriminalität und Neue Medien erstrecken. Detailinformationen sind den Anlagen 1 und 2 zu entnehmen. Die Umsetzung der Präventionsmaßnahmen erfolgt durch die Polizeipräsidien. Alle diesbezüglichen Maßnahmen und Veranstaltungen werden mit dem Sachgebiet 513 – Prävention – des BLKA abgestimmt und nach Durchführung hinsichtlich Erreichen der Zielgruppe und Wirksamkeit nachbereitet. Diese Erkenntnisse werden bei zukünftigen Präventionsmaßnahmen berücksichtigt.

Über diese allgemeinen Maßnahmen hinaus werden zusätzlich folgende regionalspezifischen Präventionsmaßnahmen betrieben:

Polizeipräsidium Mittelfranken:

- **Netzwerk IT-Prävention**

Das Netzwerk IT-Prävention unterstützt in Zusammenarbeit mit der IHK Nürnberg und anderen IT-Sicherheitsexperten insbesondere gewerbliche Anwender des Mittelstandes bei der Absicherung ihrer IT-Zugänge.

- **Einzelfallberatung und Öffentlichkeitsarbeit zur Prävention von Cybercrime**

Die Präventionsbeamten der örtlichen Kriminalpolizei bieten zusammen mit dem K 34 (Kriminalpolizeiliche Prävention) auf Anfrage Einzelberatungen und Öffentlichkeitsvorträge an. Hierbei werden sie in Einzelfällen vom Fachkommissariat K 25 unterstützt.

- **Medienkompetenz bei Kindern und Jugendlichen**

Unabhängig davon existieren zahlreiche Maßnahmen und Projekte zur Verbesserung der Medienkompetenz bei Kindern und Jugendlichen. Das Spektrum reicht von „Kinder im Netz – aber sicher“, einem Projekt von K 34, in dem bereits Grundschüler mit dem richtigen Verhalten im Netz vertraut gemacht werden, bis hin zu den „Medien-Scouts“, einem Präventionskonzept der PI Fürth, bei dem Jugendliche zu Peer-Edukatoren ausgebildet werden, die an ihren (oftmals weiterführenden) Schulen Gleichaltrige zu einem adäquaten Umgang mit den neuen Medien anhalten. Im Landkreis Fürth werden bei dem „Projekt 3 x 3“ alle Mittel- und Förderschüler von Beamten der

örtlichen Polizeiinspektionen in drei aufeinanderfolgenden Jahren mit jeweils zwei Unterrichtseinheiten über die Gefahren in Zusammenhang mit neuen Medien informiert. Darüber hinaus stehen die Präventionsbeamten der Kriminalpolizei und von K 34 Schulen und Jugendzentren auf Anfrage für die Vermittlung ähnlicher Inhalte zur Verfügung.

Polizeipräsidium München:
Das Präventions- und Opferschutzkommissariat 105 des PP München bietet teilnehmerorientierte Vorträge sowie Beratungen für Eltern und Senioren zum Thema „Medienkompetenz“ an.

Des Weiteren wurde im Jahre 2015 mit „Sei gscheit im digitalen Leben, Medienkompetenz für Kinder und Jugendliche“ eine Multiplikatorenschulung für Jugendbeamte, Lehrer und Erzieher entwickelt und durchgeführt. Derzeit erfolgt in Zusammenarbeit mit der Ludwig-Maximilians-Universität München (LMU) eine Evaluation des Kurses.

Darüber hinaus bietet das K 121 (Kommissariat für Cybercrime-Delikte im Präsidiumsbereich München) folgende Präventionsmaßnahmen an:

– **Pressearbeit „Cybercrime im engeren Sinne“** offensive Öffentlichkeitsarbeit beim Auftreten neuer Kriminalitätsphänomene oder bei aktuell bestehenden Deliktsfeldern (z. B. „Service-Anrufe“/“Microsoft-Support-Anrufe“, „Fritzbox!-Hacking“, etc.) in direkter Zusammenarbeit mit der Pressestelle des PP München
– **Betreiben einer internen Telefon-Hotline** für Polizeibeamte und durch die Telefonvermittlung des PP München weitergeleitete Bürger
– **Beantwortung von Bürgeranfragen** via Kontaktformular der Bayerischen Polizei, bzw. des PP München bei deliktischer Zuständigkeit
– **Interne Fortbildung** für den Bereich Schutz- und Kriminalpolizei, u. a. in neuen Phänomen- und Ermittlungsbereichen
– **Networking** im Bereich Cybercrime mit anderen Polizeiverbänden und Polizeidienststellen sowie staatlichen Stellen und Institutionen („Infodialog Bayern – Cybercrime München“)
– **Beratungs- und Kooperationsgespräche** mit Unternehmen auf Ebene der IT-Sicherheit (z. B. BMW, etc.)
– **Vortragstätigkeiten** bei regionalen und nationalen Fachtagungen und Symposien.

Bayerisches Landeskriminalamt:
Im Dezernat 54 Cybercrime des BLKA wurde die Zentralstelle Cybercrime (ZAC) eingerichtet. Diese dient Unternehmen und Behörden als zentraler Ansprechpartner für die Bayerische Polizei. Daher nimmt die ZAC auch Anzeigen im Bereich Cybercrime auf, die von Unternehmen erstattet werden. Die weitere Sachbearbeitung erfolgt dann durch die örtlich und sachlich zuständige Dienststelle. Ein wesentlicher Teil der Arbeit der ZAC besteht darin, Prävention zu betreiben. Das geschieht, indem Unternehmen und Behörden im Rahmen von Vorträgen oder Einzelterminen Fragen zur Cybersicherheit beantwortet werden. Bei diesen Maßnahmen wird besonderer Wert darauf gelegt, die Unternehmen zielgruppengerecht zu erreichen. Daher ist die ZAC auch bei Messen wie der IT-Security Messe und Kongress (it-sa) und der CeBIT präsent.

Durch Pressearbeit, z. B. im Rahmen des Safer Internet Day am 02.02.2016, erreicht das BLKA auch größere Teile der Bevölkerung. Der Schwerpunkt liegt dabei auf der Sensibilisierung der Bevölkerung im Umgang mit internetfähigen Geräten und der eigenen Daten und internetbasierter Kommunikation. Diese Maßnahmen werden inhaltlich vom Sachgebiet 513 – Prävention – entwickelt. Die Umsetzung erfolgt nach enger Abstimmung gemeinsam vom BLKA mit den Verbänden.

8. Wie verläuft die Zusammenarbeit der einzelnen Einrichtungen?

Die Zusammenarbeit der Organisationseinheiten mit Bekämpfungsauftrag Cybercrime ist klar geregelt. Danach werden Präventionsmaßnahmen und Ermittlungen grundsätzlich bei den örtlich und sachlich zuständigen Polizei- und Kriminalfachdienststellen (K-Fachdienststellen) durchgeführt. Qualifizierte bzw. herausragende Verfahren im Bereich Cybercrime, die sich hinsichtlich der Komplexität oder des technischen Ermittlungsaufwandes deutlich von der Masse abheben und Spezialwissen erfordern, werden vom BLKA durchgeführt.

Die Verbände werden über aktuelle phänomenspezifische Entwicklungen durch den Lagebereich Cybercrime im BLKA informiert. Im **Infoportal Cybercrime** der Bayerischen Polizei können sich alle Angehörigen der Bayerischen Polizei durch laufend aktualisierte Informationen zu Phänomenen und Ansprechpartnern in den Verbänden und im BLKA informieren. Die Anwendung erreicht demnach nicht nur die Bedarfsträger der Kriminalfachdienststellen, sie ist vor allem auf die Bedürfnisse der Ersteinschreiter der Schutzpolizei ausgerichtet. Durch das Infoportal und die Möglichkeit des direkten Kontaktes wird die Cybercrime-Basisqualifikation gestärkt und die Zusammenarbeit verbessert.

In Bayern findet darüber hinaus ein regelmäßiger **Informations- und Wissensaustausch im Rahmen der Sachbearbeitertagung Cybercrime** statt. Dort liegt der Schwerpunkt auf der praktischen Ermittlungsarbeit und dem Umgang mit konkreten Fragestellungen der Ermittlungsarbeit. Anlassbezogen werden die K-Fachdienststellen durch Beratung oder Vermittlung von Methodenkompetenz vom BLKA unterstützt. Präventionsmaßnahmen werden durch Arbeitstagungen in Bayern abgestimmt. Strukturelle und organisatorische Maßnahmen werden in Bayern im Rahmen der operativen Steuerungsgruppe Cybercrime erörtert. Der ressortübergreifende Austausch innerhalb der Staatsregierung erfolgt im „Ressortkreis Strategie für Cybersicherheit“, der vom Bayerischen Staatsministerium des Innern, für Bau und Verkehr moderiert wird.

Auf **nationaler Ebene** erfolgt die polizeiliche Zusammenarbeit entweder anlassbezogen oder regelmäßig im Rahmen von Tagungen, z. B. der Zentralen Ansprechstellen Cybercrime, der Koordinationsgruppe für die anlassunabhängig im Internet recherchierenden Dienststellen oder der Expertentagung der Ansprechstellen Kinderpornografie und der Leitertagung Cybercrime.

Bei der **Generalstaatsanwaltschaft in Bamberg** wurde die **Zentralstelle Cybercrime Bayern (ZCB)** eingerichtet. Sie ist für die Bearbeitung herausgehobener Ermittlungsverfahren im Bereich der Cyberkriminalität in Bayern zuständig. Die Zusammenarbeit mit der ZCB hat sich bewährt und verläuft reibungslos.

Anlage 1

Themenfeld: Neue Medien / Internetkriminalität

Thema: Internetkriminalität

- Straftaten oder Vorbereitungshandlungen, bei denen das Internet als Tatmittel eingesetzt wird, wie z.B.:
  - Phishing, Ausspähen von Daten
  - Betrug im Zusammenhang mit Online-Handel
  - Betrug im Zusammenhang mit Sozialen Netzwerken (Romance-Scamming etc.)
  - Identitätsdiebstahl
  - Computersicherheit (in Form von Hinweisen auf notwendige Firewall und aktuellen Virenprogramm)
  - Abofallen

Fachverantwortung / Pflege:

BLKA, SG 513

Hauptzielgruppe:

- Gesamte Bevölkerung
- Eltern und Erziehungsberechtigte
- Multiplikatoren (Pädagogen etc.)

Ziele:

- Sensibilisierung bzgl. des Umgangs mit persönlichen Daten
- Sensibilisierung für die Gefahren beim Online-Handel
- Information über bekannte Vorgehensweisen (modi operandi)
- Schaffung des Bewusstseins für eine eigenverantwortliche PC-Sicherung (Firewall u. Viren)

Hilfsmittel / Medien:

- **ProPK Medien:**
  - Broschüre: „Klicks Momente“
  - Handreichung: „Im Netz der neuen Medien“
  - Interaktives Angebot: www.kaufenmitverstand.de
  - Flyer: „Alles was Recht ist – Ihre Rechte als Online-Käufer
  - Infoblatt: „Gewinnbenachrichtigungen“
  - Infoblatt: „ Hardwaresicherheit“
  - Infoblatt: „Vorauszahlungsbetrug – Nigeria-Briefe“
  - Internetangebot: Sicherheitskompass

- **Polizeiliche Medien**
  - PP SWN: Flyer „Phishing. Vorsicht Internet-Betrüger!“
  - Infothek: „Internetkriminalität“

- **Externe Medien:**
  - Bundesamt für Sicherheit in der Informationstechnik: www.bsi.de
  - Verbraucherzentrale Bundesverband: www.surfer-haben-rechte.de

Anlage 1

- Europäisches Verbraucherzentrum: www.vorsicht-im-netz.de
- BMELV: www.verbraucher-sicher-online.de
- EU-Initiative: www.klicksafe.de

Präventionsmaßnahmen / Methoden:

- Vorträge
- Schulunterrichte (an weiterführenden Schulen)
- Beratungen im Einzelfall
- Presse- und Öffentlichkeitsarbeit
- Medienverteilung

Zuständige Dienststellen:

	Flächenpräsidien			**Ballungsraumpräsidien**				
	Ndb., OBN, OBS, Ofr., Opf., SWN, SWS, Ufr.			PP Mittelfranken			PP München	
Sachgebiete / Dienststellen	PP E3 / BPFK	KPI / KPS	PI / PSt	PP E3 / BPFK	Abschn. K	PI / PSt	K 105 / BPFK	PI
verpflichtend		X			X		X	
fakultativ			X					X

Anlage 2

Themenfeld: Neue Medien / Internetkriminalität

Thema: Neue Medien

- Urheberrechtsverletzungen im Internet (Tauschbörsen, Verwendung von Bildern etc.)
- Umgang mit persönlichen (eigenen und fremden) Daten (z.B. in Sozialen Netzwerken)
- Cybermobbing
- Chatten
- Happy Slapping
- Gewalt- und pornograf. Darstellungen auf Handys u.ä.
- Jugendgefährdende Inhalte im Internet
- Ausspähen von Daten (z. B. Verändern eines Facebook-Accounts – nicht Betrug)

Fachverantwortung / Pflege:

BLKA, SG 513

Hauptzielgruppe:

- Kinder und Jugendliche an weiterführenden Schulen und in Vereinen (z.B. Jugend-Feuerwehr, Landjugendgruppen)
- Eltern und Erziehungsberechtigte
- Multiplikatoren (Pädagogen etc.)

Ziele:

- Sensibilisierung bzgl. des Umgangs mit persönlichen Daten
- Schaffung eines Unrechtsbewusstseins i. Z. mit Urheberrecht
- Sensibilisierung für die Gefahren bei der Internetnutzung
- Information über bekannte Vorgehensweisen (modi operandi)

Hilfsmittel / Medien:

- **ProPK Medien:**
  - Broschüre: „Klicks Momente“
  - Handreichung: „Im Netz der neuen Medien“
  - Hallo Heft: „Erst denken, dann klicken“
  - Infoblatt: „Gewaltvideos auf Schülerhandys“
  - DVD: „Netzangriff“
  - DVD: „Chatten aber sicher“
  - Interaktives Angebot: www.kinder-sicher-im-netz.de
  - Internetauftritt: www.time4teen.de
  - Internetangebot: Sicherheitskompass
  - Medienpaket Abseits?! DVD: „Handygewalt“

- **Polizeiliche Medien:**
  - BLKA PIT-Ordner mit Begleitfilm „Blinddate“
  - BLKA Handyflyer
  - BLKA Infobrief: „Für Dich“
  - Infothek: „Neue Medien“

- **Externe Medien:**

Anlage 2

- EU-Initiative www.klicksafe.de
- Internetauftritt: www.irights.info
- Internetauftritt: GVU
- DVD: „Blind date“ (ausleihbar bei den Fachberatern der KPI)
- BMFSFJ Flyer: „Sicher vernetzt“
- BMFSFJ Flyer: „ICQ & Co.“
- BMFSFJ Flyer „Surfen – Kinder sicher online“
- Jugendschutz.net Flyer / Broschüre: „Chatten ohne Risiko“

Präventionsmaßnahmen / Methoden:

- Vorträge
- Schulunterricht an weiterführenden Schulen
- Beratungen im Einzelfall
- Presse- und Öffentlichkeitsarbeit
- Medienverteilung

Zuständige Dienststellen:

	Flächenpräsidien			**Ballungsraumpräsidien**				
	Ndb., OBN, OBS, Ofr., Opf., SWN, SWS, Ufr.			PP Mittelfranken			PP München	
Sachgebiete / Dienststellen	PP E3 / BPFK	KPI / KPS	PI / PSt	PP E3 / BPFK	Abschn. K	PI / PSt	K 105 / BPFK	PI
verpflichtend			X		X	X	X	X
fakultativ		X						