



## Kleine Anfrage

des Abgeordneten Wolfgang Kubicki (FDP)

und

## Antwort

der Landesregierung - Innenminister

### Bekämpfung der Cyberkriminalität

Am 21. August 2013 präsentierte Innenminister Breitner Pläne gegen „Cybercrime“. Dazu wollte der Minister die Strafverfolgungsbehörden in Schleswig-Holstein personell und sachlich so ausstatten, dass sie im Internet und mit modernen Informations- und Kommunikationstechnologien kriminalistisch ebenso handlungsfähig sind wie an den Tatorten in der realen Welt unseres Alltags, so der Minister auf einer Pressekonferenz.

Der in diesem Frühjahr bekannt gewordene millionenfache Diebstahl von eMail-Konten und Passwörtern hat die Öffentlichkeit aufgeschreckt.

1. Welche Deliktsfelder ordnet die Landesregierung dem Begriff „Cyberkriminalität“ zu?

Antwort:

Der Begriff Cybercrime umfasst im internationalen als auch bundesweiten Kontext die bisherigen Begriffe Cyberkriminalität, Computerkriminalität und Informations- und Kommunikationskriminalität (IuK-Kriminalität) und wird wie folgt definiert:

*"Cybercrime umfasst die Straftaten, die sich gegen das Internet, weitere Datennetze, informationstechnische Systeme oder deren Daten richten (Informationstechnologie als Tatobjekt [Variante 1]).*

*Cybercrime umfasst auch solche Straftaten, die mittels dieser Informationstechnik begangen werden. (Informationstechnologie als Tatmittel [Variante 2])."*

Dem Bereich der 1. Variante (auch „Cybercrime im engeren Sinne“) werden folgende Straftaten zugeordnet:

- Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen gem. §§ 202 a, 202 b und 202 c StGB
- Computerbetrug nach § 263 a StGB
- Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei der Datenverarbeitung nach §§ 269, 270 StGB
- Falschbeurkundung / Urkundenunterdrückung im Zusammenhang mit der Datenverarbeitung gem. §§ 271, 274 I Nr. 2, 348 StGB
- Datenveränderung, Computersabotage nach §§ 303 a, 303 b StGB

Diese Delikte können z.B. begangen werden durch

- so genannte DDos-Attacken
- Accountübernahmen/Diebstahl digitaler Identitäten
- Angriffe auf das Online-Banking

Der größere Anteil im Deliktsbereich Cybercrime entsteht allerdings durch Straftaten der 2. Variante.

Dazu gehören insbesondere:

- Kinderpornografie
- Warenbetrug
- Warenkreditbetrug

2. In welchen Dienststellen und an welchen Dienstorten ist die Bekämpfung dieser Deliktsform angesiedelt und wo fließen Informationen zusammen?

Antwort:

Die polizeilichen Ermittlungen und Zentralstellentätigkeiten in der Bekämpfung von Cybercrime sind in Schleswig-Holstein wie folgt organisiert:

|                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LKA SH Kiel                                                  | <ul style="list-style-type: none"> <li>• Projekt „Zentrale Organisationseinheit Cybercrime (ZOEK)“</li> <li>• Zentrale Ansprechstelle für Dienststellen des Landes und des Bundes, der Wirtschaft sowie öffentlicher und nicht-öffentlicher Einrichtungen</li> <li>• Ermittlungen zur Bekämpfung von Delikten der „qualifizierten Cybercrime“<sup>1</sup></li> <li>• Zentrale IT-Beweissicherung – für das LKA und die Landesebene</li> <li>• Ansprechstelle Kinderpornografie</li> </ul> |
| Bezirkskriminalinspektionen Kiel, Lübeck, Flensburg, Itzehoe | <ul style="list-style-type: none"> <li>• Regionale IT-Beweissicherung (rITB) – für den Bereich der Landgerichtsbezirke</li> </ul>                                                                                                                                                                                                                                                                                                                                                         |

<sup>1</sup> Qualifizierte Delikte der Cybercrime sind Delikte, bei denen die Elemente der IT in den Tatbestandsmerkmalen enthalten sind **und** bei denen für die Sachbearbeitung eine spezielle informations-technische Qualifikation erforderlich ist.

|                                            |                                                                                                                                                                                                                  |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Kriminalpolizeistellen/-außenstellen in SH | <ul style="list-style-type: none"> <li>• Alle Delikte, die nicht der „qualifizierten Cybercrime“ zugeordnet werden sowie u. a.</li> <li>• Waren-/Warenkreditbetrügereien</li> <li>• Kinderpornografie</li> </ul> |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Im Bereich der Staatsanwaltschaften werden die Delikte der Informations- und Kommunikationskriminalität durch Sonderdezernenten der örtlichen Staatsanwaltschaften bearbeitet. Zu ihrer Unterstützung ist bei der Behörde des Generalstaatsanwalts des Landes Schleswig-Holstein eine Zentralstelle „Informations- und Kommunikationskriminalität“ eingerichtet. Ergänzend wird auf die Ausführungen zu Punkt 5. „Informations- und Kommunikationskriminalität (IuK)“ (Seiten 35, 36) der Jahrespresseerklärung des Generalstaatsanwalts vom 23. Mai 2013 Bezug genommen (vgl. Anlage).

3. Von welchen zusätzlichen Kosten - zum Beispiel für technische Einrichtungen und Geräte - geht die Landesregierung durch die Einführung des neuen Schwerpunktes „Cybercrime“ aus?

Antwort:

Auf Basis der Plandaten der mittelfristigen Finanzplanung werden bis 2018 u.a. für technische Einrichtungen, Geräte und Lizenzgebühren in der IT-Maßnahme „IT-Beweissicherung“ folgende Kosten innerhalb der Landespolizei veranschlagt:

|      |                                                                                                             |
|------|-------------------------------------------------------------------------------------------------------------|
| 2014 | ca. 388.000 € (Zuweisung einschließlich Finanzierungsvorbehalt durch das Zentrale IT-Management: 283.000 €) |
| 2015 | ca. 863.000€ <sup>2</sup>                                                                                   |
| 2016 | ca. 785.000€                                                                                                |
| 2017 | ca. 675.000€                                                                                                |
| 2018 | ca. 685.000€                                                                                                |

Außerhalb der o. a. IT-Maßnahme werden z.B. auch Finanzierungen aus dem Gesamt IT-Haushalt der Polizei über den Standard Arbeitsplatz-PC hinaus getätigt sowie für die in festgelegten Zyklen durchzuführende Reinvestition finanzielle Mittel bereitgestellt.

Nennenswerte zusätzliche Kosten entstehen auf Seiten der Staatsanwaltschaften des Landes nicht, da die Arbeitsplätze der Dezernentinnen und Dezernenten ohnehin mit internetfähigen Computern ausgestattet sind und die Polizei über die speziellen aufwendigen Auswertekomponenten verfügt.

<sup>2</sup> Für 2015 und die Folgejahre sind in den ausgewiesenen Beträgen die geplanten Kosten für die Ausstattung von zusätzlichen Arbeitsplätzen mit Hard- und Software im Bereich Cybercrime und der Auswertung von mobilen Endgeräten mit berücksichtigt.

4. Welcher konkrete Personalansatz (Soll/Ist) arbeitet in der Bekämpfung der Cyberkriminalität? Welche Qualifikationen bringen die dort tätigen Polizeivollzugsbeamtinnen und –beamte zusätzlich mit? Wo waren sie zuvor beschäftigt? Und wer füllt die durch die Übertragung der neuen Tätigkeit entstandenen Vakanzen aus?

Antwort:

Auf Ebene des LKA ist seit dem 01.02.2014 das Projekt „ZOEK“ (Zentrale Organisationseinheit Cybercrime) eingerichtet. Im Rahmen des Projektes werden die zentrale IT-Beweissicherungsgruppe des LKA, die Ermittlungen i. S. „qualifizierte Cybercrime“, die Ansprechstelle Kinderpornografie und die Zentrale Ansprechstelle Cybercrime (ZAC) zusammengefasst.

In der ZOEK sind derzeit 20 Mitarbeiter tätig, davon 17 Polizeibeamte und 1 Diplom-Informatikerin, 1 Informatiker (Universität – Mastergrad) und 1 Dipl. Wirtschaftsinformatikerin (FH).

Die hier beschäftigten Mitarbeiter werden auf Grundlage des bundeseinheitlichen geltenden Aus- und Fortbildungskonzeptes aus- und fortgebildet.

Für die ZOEK ist ein zusätzlicher Bedarf von **7 Stellen** festgestellt worden.

Dieser stellt sich gem. Stellenplan für die ZOEK des LKA SH wie folgt dar:

| <b>LKA – Projekt ZOEK</b>                 | <b>Stellenplan - Ist</b> | <b>Geplant</b> |
|-------------------------------------------|--------------------------|----------------|
| Zentralstellenaufgaben                    | 4                        | 4              |
| Ansprechstelle KiPo                       | 3                        | 3              |
| Ermittlungen und Ermittlungsunterstützung | 4                        | 6              |
| Recherche in Datennetzen                  | 0                        | 3              |
| Auswertung von Massendaten                | 0                        | 2              |
| Zentrale IT-Beweissicherung               | 9                        | 9              |
|                                           | <b>20</b>                | <b>27</b>      |

Auf der regionalen Ebene ergibt sich für die IT-Beweissicherungseinheiten bei den Bezirkskriminalinspektionen (rITBen) ein zusätzlicher Bedarf von **22 Stellen**.

| <b>rITB-Standort</b> | <b>Stellenplan - Ist</b> | <b>Geplant</b> |
|----------------------|--------------------------|----------------|
| Kiel                 | 5                        | 11             |
| Lübeck               | 5                        | 11             |
| Itzehoe              | 2                        | 7              |
| Flensburg            | 2                        | 7              |
|                      | <b>14</b>                | <b>36</b>      |

Ihre Qualifikation haben die Mitarbeiter der rITBen auf Grundlage des bundeseinheitlich geltenden Aus- und Fortbildungskonzeptes erlangt.

Die Mitarbeiter der rITBen wurden bzw. werden aus dem Personalbestand der Polizeidirektionen gewonnen.

Die jeweiligen Mehrbedarfe sind durch aufwendige polizeiinterne Arbeitsgruppen ermittelt worden. Die personelle Hinterlegung ist im Rahmen der aktuell laufenden Organisationsuntersuchungen parallel zum Stellenabbau beabsichtigt.

Auf Ebene der örtlichen Kriminalpolizeistellen und –außenstellen wird die Aufgabe zur Bekämpfung der Cybercrime von Sachbearbeitern wahrgenommen, die parallel auch mit anderen Ermittlungsaufgaben (u. a. Betrug/Einbruch) betraut sind.

Das Personal, das auf dieser Ebene Cybercrimedelikte bearbeitet, ist nicht ausgewiesen. Somit können hier auch keine Personalstärken abgebildet werden.

Sachbearbeiter, die zur Bearbeitung von Ermittlungsverfahren im Deliktsbereich Cybercrime zuständig sind, haben ihr Fachwissen durch Lehrgänge im Rahmen des IuK-Fortbildungskonzeptes SH an der Polizeidirektion für Aus- und Fortbildung (PD AFB) erworben.

5. Welche konkreten Fallzahlen können der „Cyberkriminalität“ zugeordnet werden?

Antwort:

In der Polizeilichen Kriminalstatistik (PKS) wurden folgende Fallzahlen der Cybercrime erfasst:

Cybercrime im engeren Sinne (Variante 1)

| Jahr | Fälle |
|------|-------|
| 2010 | 2.447 |
| 2011 | 2.444 |
| 2012 | 2.315 |
| 2013 | 1.510 |

Straftaten in Verbindung mit dem Tatmittel Internet (Variante 2)

| Jahr | Fälle  |
|------|--------|
| 2010 | 10.128 |
| 2011 | 9.368  |
| 2012 | 7.999  |
| 2013 | 8.741  |

Erläuternd ist hinzuzufügen, dass nach den bundesweit einheitlich geltenden Erfassungsregeln der PKS nur die Straftaten erfasst werden, deren Tatort (Handlungsort) im Inland liegt und die Tatbestandsverwirklichung hinreichend konkretisiert ist.

Außerdem wird in der PKS nur jeweils ein Fall pro Tathandlung erfasst. Das gilt auch für komplexe Ermittlungsverfahren, in denen durch dieselbe Tatausführung im Internet eine hohe Anzahl von Personen geschädigt wurde.

6. Welche konkreten Erfolge hat die Bekämpfung dieser Deliktsform bereits erzielt?

Antwort:

Die Aufklärungsquoten der PKS SH zeigen eine steigende Tendenz bei den deliktsspezifischen Ermittlungserfolgen der Landespolizei.

Variante 1

| <b>Jahr</b> | <b>bekannt gewordene Fälle</b> | <b>Aufklärungsquote</b> |
|-------------|--------------------------------|-------------------------|
| 2010        | 2.447                          | 39,7 %                  |
| 2011        | 2.444                          | 36,0 %                  |
| 2012        | 2.315                          | 38,3 %                  |
| 2013        | 1.510                          | 47,9 %                  |

Variante 2

| <b>Jahr</b> | <b>bekannt gewordene Fälle</b> | <b>Aufklärungsquote</b> |
|-------------|--------------------------------|-------------------------|
| 2010        | 10.128                         | 68,1                    |
| 2011        | 9.368                          | 68,3                    |
| 2012        | 7.999                          | 75,4                    |
| 2013        | 8.741                          | 86,5                    |

Bei den Staatsanwaltschaften wird eine Erfolgsstatistik nicht geführt.

#### 4.3 Straftaten im Zusammenhang mit Fußballspielen

Angesichts der immer wieder aktuellen Problematik von Gewalteskalationen im Zusammenhang mit Fußballspielen – insbesondere auch vor dem Hintergrund der Rivalität zwischen den „Fans“ der beiden Vereine Holstein Kiel und VfB Lübeck – ist die Zusammenarbeit zwischen Polizei und Staatsanwaltschaft auch in diesem Bereich zunehmend verbessert und intensiviert worden. Ziel ist es, neben den von der Polizei durchzuführenden Maßnahmen der Gefahrenabwehr auch umgehend und effektiv repressiv auf Gewalttaten zu reagieren.

Um Straftaten von sog. "Hooligans" wirksam entgegenzutreten, sind bei den Staatsanwaltschaften Lübeck und Kiel Sonderdezernate eingerichtet worden, in denen Verfahren wegen Straftaten im Umfeld des Fußballsports bearbeitet werden. Durch die Konzentration und Spezialisierung der Sachbearbeitung ist zugleich der reibungslose Informationsaustausch zwischen Polizei und Staatsanwaltschaft gewährleistet.

Darüber hinaus kommen bei den Heimspielen der genannten Vereine besondere Bereitschaftsdienste der Staatsanwaltschaften zum Einsatz. In Abstimmung mit der Polizei wird bei solchen Spielen mit erwarteten erhöhten Gewaltauseinandersetzungen zwischen rivalisierenden Fußballfans oder gegenüber der Polizei ein Ansprechpartner der Staatsanwaltschaft vor Ort zur sofortigen Wahrnehmung staatsanwaltlicher Ermittlungsmaßnahmen, insbesondere zur Entscheidung über die Beantragung eines Haftbefehls, abgestellt. Diesem obliegt auch die Aufgabe, als Ansprechpartner für die sog. szenekundigen Beamten der Polizei zu fungieren. Dadurch wird erforderlichenfalls eine schnelle Umsetzung von strafprozessualen Maßnahmen und die gezielte Beweissicherung für die weitere Strafverfolgung nach Ende des Fußballspiels sichergestellt.

#### 5. Informations- und Kommunikationskriminalität (IuK-Kriminalität)

Mit der Entwicklung und Verbreitung elektronischer Informations- und Kommunikationsformen hat sich zugleich in besorgniserregender Weise das Phänomen der Informations- und Kommunikationskriminalität (IuK-Kriminalität) entwickelt, die sich bei der Tatbegehung der hierbei eingesetzten elektronischen Medien, insbesondere des Internets, bedient. Das Gefahrenpotential dieser Kriminalitätsform ist besonders

hoch. Nur beispielhaft sind sog. Phishing - Fälle zu nennen, bei denen Täter rechtswidrig auf geschützte Computerzugangsdaten des Online-Banking zugreifen, um Geldbeträge vom Konto der Opfer auf eigene Konten zu schleusen. Dahinter stehen oft kriminelle Netzwerke, die für ihre Zwecke eigens entwickelte Schadensoftware einsetzen. Der zunehmenden Professionalisierung der Täter und ihrer Strategien müssen Staatsanwaltschaft und Polizei durch Spezialisierung Rechnung tragen.

Aus diesem Grunde ist bei dem Generalstaatsanwalt eine Zentralstelle „Informations- und Kommunikationskriminalität“ eingerichtet worden. Der Zentralstelle sind folgende Aufgaben zugewiesen:

- Koordinierung der Zusammenarbeit zwischen Staatsanwaltschaften und Polizeibehörden,
- Entwicklung einheitlicher Standards und Strategien für ein effizientes Ermittlungsverfahren,
- Unterstützung der Staatsanwaltschaften bei grenzüberschreitender IuK-Kriminalität,
- gegenseitiger Informationsaustausch zwischen Staatsanwaltschaften und Polizei,
- Unterstützung der Staatsanwaltschaften als Ansprechpartner bei Fragen grundsätzlicher Bedeutung,
- Durchführung von Maßnahmen zur Fortbildung der Dezernentinnen und Dezernenten der Staatsanwaltschaften,
- Stellungnahmen und Anregungen zu Gesetzgebungsvorhaben,
- Bearbeitung von Revisions- und Beschwerdesachen grundsätzlicher Bedeutung.

Darüber hinaus haben die Staatsanwaltschaften des Landes und die Generalstaatsanwälte Deutschlands im Rahmen von Arbeitsgemeinschaften geprüft, ob neue Organisationsformen der Bearbeitung erforderlich sind. Nach den Ergebnissen der jeweiligen Abschlussberichte sind ausschließliche Zuständigkeitskonzentrationen auf eine Schwerpunktstaatsanwaltschaft oder eine Schwerpunktabteilung derzeit nicht zwingend geboten. Erforderlich und ausreichend ist die Beibehaltung der Zuständigkeitskompetenz bei den örtlich zuständigen Staatsanwaltschaften, dort aber in Form von speziellen Sonderdezernaten, deren Dezernenten hier durch die beim Generalstaatsanwalt eingerichtete Zentralstelle unterstützt werden.