Rat der
Europäischen Union

Brüssel, den 19. Mai 2017
(OR. en)

7159/1/17
REV 1 DCL 1

GENVAL 20
CYBER 36

FREIGABE

des Dokuments	7159/1/17 REV 1 RESTREINT UE/EU RESTRICTED
vom	2. Mai 2017
Neuer Status:	Öffentlich zugänglich
Betr.:	Evaluierungsbericht zur siebten Runde der gegenseitigen Begutachtungen "Praktische Umsetzung und Durchführung europäischer Strategien zur Verhütung und Bekämpfung von Cyberkriminalität" – Bericht über Deutschland

Die Delegationen erhalten in der Anlage die freigegebene Fassung des obengenannten Dokuments.

Der Wortlaut dieses Dokuments ist mit dem der vorherigen Fassung identisch.

Rat der
Europäischen Union

Brüssel, den 2. Mai 2017
(OR. en)

7159/1/17
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 20
CYBER 36

BERICHT

Betr.:	Evaluierungsbericht zur siebten Runde der gegenseitigen Begutachtungen "Praktische Umsetzung und Durchführung europäischer Strategien zur Verhütung und Bekämpfung von Cyberkriminalität" – Bericht über Deutschland

ANLAGE

Inhalt

1. ZUSAMMENFASSUNG 5
2. EINLEITUNG 8
3. ALLGEMEINE FRAGEN UND STRUKTUREN 11
3.1. Nationale Cyber-Sicherheitsstrategie 11
3.2. Nationale Prioritäten in Bezug auf die Cyberkriminalität 13
3.3. Statistiken über die Cyberkriminalität 15
3.3.1. Wichtigste Trends, die die Cyberkriminalität fördern 15
3.3.2. Zahl der gemeldeten Cyber-Straftaten 17
3.4. Innerstaatliche Haushaltsmittel zur Prävention und Bekämpfung von Cyberkriminalität sowie Unterstützung durch EU-Haushaltsmittel 20
3.5. Fazit 23
4. NATIONALE STRUKTUREN 25
4.1. Justiz (Strafverfolgungen und Gerichte) 25
4.1.1. Interne Struktur 25
4.1.2. Fähigkeit zur und Hemmnisse für eine erfolgreiche Strafverfolgung 27
4.2. Strafverfolgungsbehörden 35
4.3. Sonstige Behörden/Einrichtungen/öffentlich-private Partnerschaften 41
4.4. Zusammenarbeit und Koordinierung auf nationaler Ebene 44
4.4.1. Rechtliche oder politische Verpflichtungen 44
4.4.2. Mittel für die Verbesserung der Zusammenarbeit 50
4.5. Fazit 52
5. RECHTLICHE ASPEKTE 55
5.1. Materielles Strafrecht im Bereich Cyberkriminalität 55
5.1.1. Übereinkommen des Europarats über Computerkriminalität 55
5.1.2. Beschreibung der nationalen Rechtsvorschriften 55
A/ Rahmenbeschluss 2005/222/JI des Rates über Angriffe auf Informationssysteme und Richtlinie 2013/40/EU über Angriffe auf Informationssysteme 55
B/ Richtlinie 2011/93/EU zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie 62
C/ Online-Kartenbetrug 67
D/ Sonstige Phänomene der Cyberkriminalität 70
5.2. Verfahrensfragen 72
5.2.1. Ermittlungstechniken 72

5.2.2. Forensik und Verschlüsselung 76
5.2.3. Elektronische Beweismittel 82
5.3. Schutz der Menschenrechte/Grundfreiheiten 86
5.4. Gerichtliche Zuständigkeit 88
5.4.1. Grundsätze für die Ermittlungen bei Cyberkriminalität 88
5.4.2. Regeln für das Vorgehen bei Kompetenzkonflikten und Befassung von Eurojust 89
5.4.3. Gerichtliche Zuständigkeit für in der "Cloud" begangene Cyberstraftaten 90
5.4.4. Auffassung Deutschlands zum Rechtsrahmen zur Bekämpfung der Cyberkriminalität 90
5.5. Fazit 92
6. OPERATIVE ASPEKTE 95
6.1. Cyberangriffe 95
6.1.1. Art der Cyberangriffe 95
6.1.2. Mechanismen zur Abwehr von Cyberangriffen 96
6.2. Maßnahmen gegen Kinderpornografie und sexuellen Missbrauch von Kindern im Internet 99
6.2.1. Datenbank-Software zum Ausfindigmachen von Opfern und Maßnahmen zur Vermeidung einer erneuten Viktimisierung 99
6.2.2. Maßnahmen zur Bekämpfung der sexuellen Ausbeutung bzw. des sexuellen Missbrauchs im Internet, der Verbreitung sexueller Inhalte über das Internet oder Mobiltelefone (Sexting) und des Cyber-Mobbing 101
6.2.3. Präventionsmaßnahmen gegen Sextourismus, pornografische Darbietungen von Kindern und Sonstiges 103
6.2.4. Akteure und Maßnahmen gegen Websites, die Kinderpornografie enthalten oder verbreiten 108
6.3. On-line-Kartenbetrug 114
6.3.1. Online-Meldung 114
6.3.2. Rolle der Privatwirtschaft 115
6.4. Sonstige Phänomene der Cyberkriminalität 117
6.5. Fazit 118

7. INTERNATIONALE ZUSAMMENARBEIT 121
7.1. Zusammenarbeit mit EU-Agenturen 121
7.1.1. Formelle Anforderungen für die Zusammenarbeit mit Europol/EC3, Eurojust und ENISA 121
7.1.2. Bewertung der Zusammenarbeit mit Europol/EC3, Eurojust und ENISA 121
7.1.3. Operative Leistung von JIT und Cyberpatrouillen 125
7.2. Zusammenarbeit zwischen deutschen Behörden und Interpol 126
7.3. Zusammenarbeit mit Drittstaaten 127
7.4. Zusammenarbeit mit der Privatwirtschaft 128
7.5. Instrumente der internationalen Zusammenarbeit 130
7.5.1. Rechtshilfe 130
7.5.2. Instrumente der gegenseitigen Anerkennung 133
7.5.3. Überstellung/Auslieferung 133
7.6. Fazit 136
8. AUS- UND FORTBILDUNG, SENSIBILISIERUNG UND PRÄVENTION 140
8.1. Spezifische Aus- und Fortbildung 140
8.2. Sensibilisierungsmaßnahmen 174
8.3. Prävention 182
8.3.1. Nationale Rechtsvorschriften/politische Maßnahmen und andere Maßnahmen 182
8.3.2. Öffentlich-private Partnerschaften (ÖPP) 185
8.4. Fazit 187
9. SCHLUSSBEMERKUNGEN UND EMPFEHLUNGEN 189
9.1. Vorschläge Deutschlands 189
9.2. Empfehlungen 189
9.2.1. Empfehlungen an Deutschland 190
9.2.2. Empfehlungen an die Europäische Union, ihre Organe und Einrichtungen sowie an die anderen Mitgliedstaaten 192
9.2.3. Empfehlungen an Eurojust/Europol/ENISA 194
ANHANG A: Programme for the on-site visit 195
ANHANG B: Persons interviewed/met 202
ANHANG C: List of abbreviations/glossary of terms 208

1. ZUSAMMENFASSUNG

Die Begutachtung der Bundesrepublik Deutschland wurde im Zeitraum 24.-27. Mai 2016 durchgeführt und umfasste Treffen mit Verantwortlichen der Arbeitsfelder Prävention und Bekämpfung von Cyberkriminalität sowie Umsetzung und Durchführung europäischer Strategien (Bundesministerium der Justiz und für Verbraucherschutz, Bundesministerium des Innern, Bundesministerium für Wirtschaft und Energie, Bundesministerium für Familie, Senioren, Frauen und Jugend, Bundeskriminalamt (BKA), Bundesamt für Sicherheit in der Informationstechnik (BSI), German Competence Centre against Cybercrime, Bitkom (Digitalverband Deutschlands)).

Zudem wurde ein Besuch bei der Generalstaatsanwaltschaft Celle organisiert, an dem Staatsanwälte und Polizeibeamte aus Celle, Verden, Berlin, Köln, Bamberg und Lüneburg teilgenommen haben und bei dem sich der Gutachterausschuss einen Eindruck darüber verschaffen konnten, wie sich das Vorgehen gegen die Cyberkriminalität aus der Sicht der Praktiker darstellt.

Allgemein hat der Gutachterausschuss festgestellt, dass Deutschland die Cyberkriminalität sehr entschlossen bekämpft und dafür gut ausgestattet ist. Zu diesem Zweck hat Deutschland eine Reihe von Initiativen, bewährten Praktiken und Maßnahmen eingeführt, an denen sich andere Mitgliedstaaten orientieren könnten.

In Anbetracht der föderalen Struktur der Bundesrepublik erfordert die Verhütung und Bekämpfung der Cyberkriminalität eine enge Zusammenarbeit zwischen Bund und Ländern. Es wird darauf hingearbeitet, diese beiden Ebenen zu vernetzen und eine reibungslose Kommunikation und Koordinierung zu gewährleisten.

Die nationalen Prioritäten bei der Bekämpfung der Cyberkriminalität sind mit den Projekten zu den EMPACT-Prioritäten verknüpft, die im Rahmen des EU-Politikzyklus entwickelt wurden: Prävention, Kapazitätsaufbau, internationale und nationale Zusammenarbeit, Europäische Strategie. Deutschland verfügt über eine robuste nationale Cyber-Sicherheitsstrategie, die 1991 eingeführt wurde, sowie seit 2009 über eine polizeiliche Bekämpfungsstrategie Cybercrime, die zuletzt 2015 überarbeitet wurde.

Die meisten Bundesländer verfügen entweder über Schwerpunktstaatsanwaltschaften zur Bekämpfung der Cyberkriminalität oder haben bei den Staatsanwaltschaften Sonderabteilungen bzw. Ansprechpartner für Cyberkriminalität geschaffen bzw. benannt.

Was die Polizeibehörden anbelangt, so hat die Mehrheit der Länder bei den jeweiligen Landeskriminalämtern Sonderdezernate zur Bekämpfung von Cyberkriminalität eingerichtet. Die Sonderdezernate verfügen über Personal mit fundierten IT-Kenntnissen und spezieller informationstechnischer Sachkunde. Im Bundeskriminalamt besteht außerdem eine für Cyberkriminalität zuständige Organisationseinheit (Gruppe SO4).

Was die Rechtsvorschriften anbelangt, so hat Deutschland das Übereinkommen des Europarats über Cyberkriminalität ratifiziert; zudem wurden die Richtlinie 2011/93/EU zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie und die Richtlinie 2013/40/EU über Angriffe auf Informationssysteme in innerstaatliches Recht umgesetzt.

Die Zusammenarbeit mit dem Privatsektor ist als sehr gut zu bezeichnen. Deutschland hat eine zuverlässige und äußerst strukturierte öffentlich-private Partnerschaft auf Bundes- und Länderebene eingerichtet. Das BKA hat eine Vereinbarung mit dem German Competence Centre against Cybercrime (G4C) geschlossen, einem von mehreren Banken getragenen Verein. Zudem besteht eine gute Zusammenarbeit mit dem BITKOM und der Deutschen Telekom.

Was die Abwehr von Cyber-Angriffen anbelangt, so ist das BSI (CERT) zuständig für das IT-Netz der öffentlichen Verwaltung, und es besteht eine sehr gute Zusammenarbeit mit verschiedenen anderen Einrichtungen (aktive Unterrichtung, Austausch bewährter Praktiken, gemeinsame Bewältigung von Vorfällen). Bei kritischen Infrastrukturen besteht eine eingeschränkte gesetzliche Verpflichtung, dem BSI IT-Vorfälle zu melden; die Polizei ist allerdings bemüht, zu einer möglichst umfassenden Meldung von Vorfällen zu ermutigen.

Bei der Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern im Internet wenden die Bundesbehörden das "Konzept der Zugangssperre" nicht an, da sie die "Löschung von Inhalten" als den effizienteren Ansatz betrachten.

Deutschland kann eine sehr gute internationale Zusammenarbeit bei der Bekämpfung von Cyberkriminalität innerhalb von Europol/EC3 und Eurojust vorweisen; Gleiches gilt für Interpol und andere Dritte. Während des Evaluierungsbesuchs wurden einige Schwierigkeiten gemeldet, die bei der Zusammenarbeit mit Drittstaaten aufgetreten sind.

Deutschland betreibt mehrere Sensibilisierungs- und Präventionsprogramme, um die Öffentlichkeit und die Unternehmen über die Risiken der Cyberkriminalität zu unterrichten und zu einem sicheren Umgang mit dem Internet zu ermutigen. Die Polizeien auf Bundes- und Landesebene sind an diesen Präventionskampagnen umfassend beteiligt.

Das BKA hat mehrere Aus- und Fortbildungsprogramme zum Thema Cyberkriminalität aufgestellt, einschließlich im Bereich der IT-Forensik. Auf Länderebene werden verschiedene Schulungsinitiativen umgesetzt, beispielsweise in Nordrhein-Westfalen, wo eine gemeinsame Fortbildungsveranstaltung für Spezialisten der Landespolizei und niedersächsische Staatsanwälte organisiert wird. Der Gutachterausschuss betrachtet dies als bewährte Vorgehensweise.

2. EINLEITUNG

Mit der Gemeinsamen Maßnahme 97/827/JI vom 5. Dezember 1997[1] wurde ein Mechanismus für die Begutachtung der einzelstaatlichen Anwendung und Umsetzung der zur Bekämpfung der organisierten Kriminalität eingegangenen internationalen Verpflichtungen geschaffen. Im Einklang mit Artikel 2 der Gemeinsamen Maßnahme hatte die Gruppe "Allgemeine Angelegenheiten einschließlich Bewertungen" (GENVAL) am 3. Oktober 2013 beschlossen, dass die siebte Runde der gegenseitigen Begutachtungen die praktische Umsetzung und Durchführung europäischer Strategien zur Verhütung und Bekämpfung von Cyberkriminalität zum Gegenstand haben soll.

Die Wahl der Cyberkriminalität zum Thema der siebten Runde der gegenseitigen Begutachtungen ist von den Mitgliedstaaten begrüßt worden. Aufgrund der Vielzahl unterschiedlicher Straftaten, die unter den Begriff Cyberkriminalität fallen, ist allerdings vereinbart worden, dass sich die Begutachtung vor allem auf die Straftaten konzentrieren soll, denen die Mitgliedstaaten besondere Aufmerksamkeit widmen möchten. Daher ist die Begutachtung auf drei spezifische Bereiche – Cyberangriffe, sexueller Missbrauch von Kindern bzw. Kinderpornografie im Internet und Online-Kartenbetrug – ausgerichtet und sollte eine umfassende Untersuchung der rechtlichen und praktischen Aspekte der Bekämpfung von Cyberkriminalität, der grenzübergreifenden Zusammenarbeit und der Zusammenarbeit mit den einschlägigen EU-Agenturen ermöglichen. Von besonderer Bedeutung sind in diesem Kontext die Richtlinie 2011/93/EU zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie[2] (Umsetzungsfrist 18. Dezember 2013) und die Richtlinie 2013/40/EU über Angriffe auf Informationssysteme[3] (Umsetzungsfrist 4. September 2015).

1 Gemeinsame Maßnahme 97/287/JI vom 5. Dezember 1997 (ABl. L 344 vom 15.12.1997, S. 7-9).
2 ABl. L 335 vom 17.12.2011, S. 1.
3 ABl. L 218 vom 14.8.2013, S. 8.

Zudem wird in den Schlussfolgerungen des Rates zur Cybersicherheitsstrategie vom Juni 2013[4] das Ziel der baldigen Ratifizierung des Übereinkommens des Europarates über Computerkriminalität (Übereinkommen von Budapest)[5] vom 23. November 2001 bekräftigt und in den Erwägungsgründen betont, dass "die EU keine neuen internationalen Rechtsinstrumente für Cyberangelegenheiten fordert". Das Übereinkommen über Computerkriminalität wird durch ein Zusatzprotokoll betreffend die Kriminalisierung mittels Computersystemen begangener Handlungen rassistischer und fremdenfeindlicher Art[6] ergänzt.

Die Erfahrungen aus früheren Begutachtungen zeigen, dass sich die Mitgliedstaaten hinsichtlich der Durchführung einschlägiger Rechtsakte in unterschiedlichen Positionen befinden, und mit der aktuellen Begutachtungsrunde könnte auch ein nützlicher Beitrag für diejenigen Mitgliedstaaten geleistet werden, die möglicherweise noch nicht alle Aspekte der unterschiedlichen Instrumente umgesetzt haben. Dennoch soll sich die Begutachtung, die breit und fachübergreifend angelegt ist, nicht nur auf die Umsetzung der verschiedenen Instrumente zur Bekämpfung der Cyberkriminalität konzentrieren, sondern vielmehr auf die operativen Aspekte in den Mitgliedstaaten.

Daher wird hierbei auch berücksichtigt werden, wie die Polizeibehörden mit Eurojust, ENISA und Europol/EC3 zusammenarbeiten, wie Rückmeldungen der betreffenden Akteure an die zuständigen Polizei- und Sozialdienste übermittelt werden und wie sich die Zusammenarbeit mit den Strafverfolgungsbehörden gestaltet. Die Begutachtung richtet sich vor allem auf die Umsetzung einzelstaatlicher Strategien zur Bekämpfung von Cyberangriffen, Betrug und Kinderpornografie. Des Weiteren wird die operative Praxis in den Mitgliedstaaten in Bezug auf die internationale Zusammenarbeit sowie die Unterstützung für die Opfer der Cyberkriminalität begutachtet.

---

4 Dok. 12109/13 POLGEN 138 JAI 612 TELECOM 194 PROCIV 88 CSC 69 CIS 14 RELEX 633
JAIEX 55 RECH 338 COMPET 554 IND 204 COTER 85 ENFOPOL 232 DROIPEN 87 CYBER 15 COPS 276 POLMIL 39 COSI 93 DATAPROTECT 94.

5 Sammlung der Europaratsverträge Nr. 185; es wurde am 23. November 2001 zur Unterzeichnung aufgelegt und trat am 1. Juli 2004 in Kraft.

6 Sammlung der Europaratsverträge Nr. 189; es wurde am 28. Januar 2003 zur Unterzeichnung aufgelegt und trat am 1. März 2006 in Kraft.

Die Gruppe "Allgemeine Angelegenheiten einschließlich Bewertungen" hat am 1. April 2014 die Reihenfolge der Besuche in den Mitgliedstaaten festgelegt. Deutschland ist der (dritte) Mitgliedstaat, der in dieser Begutachtungsrunde begutachtet wurde. Im Einklang mit Artikel 3 der Gemeinsamen Maßnahme hat der Vorsitz eine Liste der Experten für die durchzuführenden Begutachtungen aufgestellt. Die Mitgliedstaaten haben nach einem schriftlichen Ersuchen, das der Vorsitzende der Gruppe am 28. Januar 2014 an die Delegationen übermittelt hat, Experten benannt, die über eingehende praktische Kenntnisse in Bezug auf den Begutachtungsgegenstand verfügen.

Die Gutachterausschüsse setzen sich aus drei nationalen Experten zusammen, die von zwei Bediensteten des Generalsekretariats des Rates sowie Beobachtern unterstützt werden. Für die siebte Runde der gegenseitigen Begutachtungen hat die Gruppe "Allgemeine Angelegenheiten einschließlich Bewertungen" dem Vorschlag des Vorsitzes zugestimmt, dass die Europäische Kommission, Eurojust, ENISA und Europol/EC3 als Beobachter eingeladen werden sollten.

Die mit der Begutachtung Deutschlands beauftragten Experten waren Herr Pierrick Buret (Frankreich), Herr Sven Kivvistik (Estland) und Herr Timo Piiroinen (Finnland). Drei Beobachter waren ebenfalls beteiligt: Frau Daniela Buruiana (Eurojust), Frau Claudia Warken (Europäische Kommission) und Herr Alexander Gutwin (Europol), begleitet von Herrn Steven Cras und Frau Carmen Necula vom Generalsekretariat des Rates.

Dieser Bericht ist vom Gutachterausschuss mit Unterstützung des Generalsekretariats des Rates ausgehend von den Ergebnissen des Besuchs in Deutschland vom 23. bis 27. Mai 2016 und von den ausführlichen Antworten Deutschlands auf den Fragebogen zusammen mit den ausführlichen Antworten auf Folgefragen erstellt worden.

3. ALLGEMEINE FRAGEN UND STRUKTUREN

3.1. Nationale Cyber-Sicherheitsstrategie

Die Bundesrepublik Deutschland verfügt über eine nationale Cyber-Sicherheitsstrategie. Sie kann hier eingesehen werden:
http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber_eng.pdf;jsessionid=A7CACE6B709E665A39AB488C5A406778.2_cid364?__blob=publicationFile
Die Cyber-Sicherheitsstrategie umfasst zehn Bereiche:

- Schutz kritischer Informationsinfrastrukturen
- Sichere IT-Systeme in Deutschland
- Stärkung der IT-Sicherheit in der öffentlichen Verwaltung
- Nationales Cyber-Abwehrzentrum
- Nationaler Cyber-Sicherheitsrat
- Wirksame Kriminalitätsbekämpfung auch im Cyber-Raum
- Effektives Zusammenwirken für Cyber-Sicherheit in Europa und weltweit
- Einsatz verlässlicher und vertrauenswürdiger Informationstechnologie
- Personalentwicklung der Bundesbehörden
- Instrumentarium zur Abwehr von Cyber-Angriffen

Daneben existiert seit 2009 eine polizeiliche Bekämpfungsstrategie Cybercrime, die zuletzt 2015 überarbeitet wurde. Sie enthält Handlungsfelder und -empfehlungen in folgenden Bereichen:

- Lagedarstellung
- Polizeiliche Zusammenarbeit
- Recht
- Zusammenarbeit zwischen Polizei und Justiz
- Bekämpfungsmethoden

- Kooperation mit Dritten (Outreach)
- Aus- und Fortbildung
- Personalentwicklung
- Organisationsentwicklung
- Prävention
- Technik und Logistik

Daneben bestehen auch auf Landesebene zum Teil eigene Strategien und Konzepte zur Bekämpfung und Prävention der Cyberkriminalität.

Angesichts der großen Bandbreite von Cyberstraftaten kann es keine allgemein bewährten Verfahren oder Methoden zur Ermittlung solcher Taten geben. Jeder Fall liegt anders, die Ermittlungsverfahren und -methoden müssen sich am konkreten Einzelfall und den jeweils vorhandenen Ermittlungsansätzen orientieren. Einer der wichtigsten Ermittlungsansätze ist sicher der Rückgriff auf Datenspuren im Netz bei der Kommunikation in Form der Personenauskunft zu verwendeten IP-Adressen, in Form der Verkehrsdatenauskunft oder – soweit eine Katalogstraftat vorliegt – auch eine Überwachung der Internetkommunikation. Weitere wichtige Quellen sind die Beschlagnahme und Auswertung von Datenträgern und E-Mail-Postfächern. Sofern die Cyberstraftat ein Vermögensdelikt beinhaltet, sind zudem Bank- und Kontoauskünfte unabdingbar, um den Weg des Geldes nachzuvollziehen. Insbesondere beim Phishing im Zusammenhang mit Online-Banking wird bei den Finanzagenten angesetzt und mittels verdeckter Maßnahmen versucht, den bandenmäßig begangenen Computerbetrug beweissicher nachzuweisen.

Sind Ermittlungen auf technischem Wege nicht möglich, müssen verdeckte personale Ermittlungen geführt werden. Solche verdeckten polizeilichen Ermittlungen durch den Einsatz von sogenannten "NoeP" (nicht offen ermittelnde Polizeibeamte), der auf Grundlage der polizeilichen Generalklausel möglich ist, erfolgt zumeist bei Ermittlungen in Foren und Boards. Allerdings sind solche Ermittlungen nur dann erfolgversprechend, wenn sie langfristig angelegt sind.

Im Land Brandenburg wird ein Videochatsystem betrieben, das durch die Nutzer nach Anmeldung – unter Angabe eines Namens und der E-Mail-Adresse – mit einem User Account genutzt werden kann.

Der Dienst bietet die Möglichkeit, an Gruppenchats teilzunehmen, bei denen eine Bildübertragung in Echtzeit erfolgt. Werden auf dieser Videochatplattform Straftaten begangen, z. B. Abbildungen des erigierten männlichen Geschlechtsteils gezeigt, wird dieses durch den Betreiber zeitnah dokumentiert. Dieser ermittelt die serverseitig gespeicherte IP-Adresse und übermittelt diese per Telefax an die Staatsanwaltschaft. Dort wird beschleunigt ein Ermittlungsverfahren eingeleitet, der Internetdienstanbieter anhand der IP-Adresse ermittelt und – sofern dieser Verkehrsdaten für einen relevanten Zeitraum speichert – per Telefax gemäß § 100j Abs. 1 Satz 1, Abs. 2 StPO zu einer Auflösung zu einem Anschlussinhaber aufgefordert.

3.2. Nationale Prioritäten in Bezug auf die Cyberkriminalität

Prävention

Die präventiven Aktivitäten sind sowohl an die Bürgerinnen und Bürger als auch die Wirtschaft gerichtet. Sowohl auf Bundes- als auch auf Landesebene bestehen vielfältige Maßnahmen, um auf aktuelle Erscheinungsformen von Cyberkriminalität hinzuweisen und die Bevölkerung zu sensibilisieren. So werden auf Veranstaltungen und über die Internetauftritte der zuständigen Behörden Präventionstipps und Sicherheitshinweise angeboten.

Darüber hinaus besteht mit dem "German Competence Centre against Cyber Crime e.V." eine institutionalisierte öffentlich-private Partnerschaft des Bundeskriminalamts (BKA) und des Bundesamts für Sicherheit und Informationstechnik (BSI) mit (bisher) drei Finanzinstituten und einem Hersteller von Antivirussoftware (Hintergrundinformationen s. http://www.g4c-ev.org/). Ziel ist der Erfahrungsaustausch zu aktuellen Modi operandi (welche oft auf Sicherheitslücken beruhen) und Täterstrukturen sowie die Entwicklung geeigneter Gegenmaßnahmen.
Sofern bestimmte Formen der Cyberkriminalität die Interessen des Verbraucherschutzes berühren (können), informieren die zuständigen Behörden die Bevölkerung hierüber und geben gezielte Hinweise. In diesem Zusammenhang wird aktiv Öffentlichkeitsarbeit betrieben.

Kapazitätsaufbau:
Cyberkriminalität (im engeren Sinne) stellt sowohl auf Bundesebene als auch in den Ländern einen besonderen Schwerpunkt in der Kriminalitätsbekämpfung dar und gewinnt weiter an Bedeutung.

Die Bundesregierung hat sich zum Ziel gesetzt, die sachliche und personelle Ausstattung der Sicherheitsbehörden weiter zu verbessern und die technischen und rechtlichen Kompetenzen an ihre neuen Aufgaben anzupassen. Die Kompetenzen des BKA und der Bundespolizei sollen im Bereich Cybercrime, Cyberspionage und Cybersecurity gestärkt werden. Im BKA wird das Cybercrime Center, das die Auswertung und Ermittlung in diesem Phänomenbereich bündelt, weiter ausgebaut.

Schulungen:
Schulungsangebote von Bildungsträgern unterschiedlicher Art Bundeskriminalamt (BKA), andere Bundesländer, Bund deutscher Kriminalbeamter, Hochschulen, Europol) werden den Mitarbeitern unterschiedlicher Professionen – je nach Ausbildungsstand und Fortbildungsbedarf – angeboten. In Bezug auf Richter und Staatsanwälte wird auf die Ausführungen unter 10 B 1 (Seite 109 f.) verwiesen.

Internationale und nationale Zusammenarbeit:

Die internationale Kooperation, z. B. mit der Europäischen IT-Sicherheitsagentur ENISA und dem Europol-Cybercrime-Center, soll gestärkt werden. Die internationale Zusammenarbeit erfolgt grundsätzlich über das BKA, im Einzelfall auch direkt durch die zuständigen Behörden. Die Cybercrime-Zentralstellen des Bundes und der Länder sind miteinander gut vernetzt. Auf der Plattform des Nationalen Cyber-Abwehrzentrums wird das arbeitsteilige Zusammenwirken der fachlich spezialisierten Behörden auf Bundesebene verbessert.

Europäische Strategie:

Die nationalen Prioritäten entsprechen den strategischen Zielvorgaben und den operativen Aktionsplänen der EU für die Bekämpfung der Cyberkriminalität. Entsprechend dem EU-Politikzyklus 2014-2017 wurde Cybercrime für Deutschland als eine der Prioritäten festgelegt, wobei eine Unterteilung in drei Unterprojekte vorgenommen wurde:

- Kreditkartenbetrug
- Sexueller Missbrauch von Kindern im Internet
- Cyber-Angriffe.

3.3. Statistiken über die Cyberkriminalität

3.3.1. Wichtigste Trends, die die Cyberkriminalität fördern

Cyberkriminalität ist ein wachsendes gesellschaftliches Problem. Mit dem verstärkten Einzug der IT in nahezu alle Lebensbereiche ist auch eine Steigerung der Angriffsmöglichkeiten für Cyberkriminelle verbunden. Die technischen Möglichkeiten zur Durchführung von Cyberangriffen/Cyberstraftaten werden durch ein professionelles Angebot von cyberkriminellen Dienstleistungen in der Untergrundökonomie ("Cybercrime as a Service") auch für Kriminelle ohne eigene technische Expertise nutzbar.

Im Jahr 2014 wurden 246 925 Fälle erfasst, die unter Nutzung des Tatmittels Internet ("Computer as a tool") begangen wurden. Das waren überwiegend Betrugsdelikte (74,2 %), darunter vor allem Warenbetrug (29,2 %). Weiterhin wurden 49 925 Fälle von Cybercrime im engeren Sinne[7] ("Computer as a target") registriert, darunter 11 887 Fälle (23,8 %) des Ausspähens und Abfangens von Daten einschließlich Vorbereitungshandlungen sowie 5 661 Fälle (11,3 %) von Datenveränderung und Computersabotage. Die Aufklärungsquote bei Cyberkriminalität im engeren Sinne beträgt 29,3 %, im Teilbereich Datenveränderung und Computersabotage jedoch nur 17,7 %. Außerdem gab es 23 670 Fälle von Betrug mittels rechtswidrig erlangter Debitkarten mit PIN.

Für diese Fallzahlen und Aufklärungsquoten ist aufgrund geänderter Vorgaben für die statistische Erfassung kein Vergleich zum Vorjahr möglich. Außerdem ist zu berücksichtigen, dass hier nur solche Fälle enthalten sind, deren Tathandlungsort in Deutschland lag und die polizeilich abschließend bearbeitet sind. Einzelne bzw. besonders relevante Phänomene, wie z. B. Phishing im Bereich Onlinebanking, Erpressungshandlungen im Zusammenhang mit gezielten DDoS-Attacken oder auch die vielfältigen anderen Erscheinungsformen der digitalen Erpressung (z. B. mittels "Ransomware"), werden in der Polizeilichen Kriminalstatistik (PKS) nicht unter dem Begriff Cyberkriminalität, sondern vielmehr unter den PKS-Schlüsseln der einzelnen Straftatbestände erfasst. Insofern finden diese deliktischen Ausprägungen an dieser Stelle keine Berücksichtigung.

Auch 2014 wurden Schäden lediglich bei den Delikten Computerbetrug und Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten registriert. Diese belaufen sich im Jahr 2014 auf rund 39,4 Mio. EUR, wovon mit rund 36,9 Mio. EUR der Großteil auf Computerbetrug entfällt.

[7] Cyberkriminalität im engeren Sinne umfasst alle Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (konkret die Delikte: Computerbetrug (PKS 517500), Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten (PKS 517900), Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung (PKS 543000), Datenveränderung/Computersabotage (PKS 674200) sowie Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen (PKS 67800).

Weitere Einzelheiten können dem Bundeslagebild Cybercrime entnommen werden, welches unter folgender Internetadresse abgerufen werden kann:
http://www.bka.de/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime__node.html?__nnn=true

Das Phänomen Cyberkriminalität nimmt in der polizeilichen Aufgabenwahrnehmung eine immer größere Rolle ein. Das Internet ermöglicht allen Formen von Kriminalität eine Zunahme.

3.3.2. Zahl der gemeldeten Cyber-Straftaten

Die Basis für die Erhebung der Straftaten im Bereich Cyberkriminalität bildet die Polizeiliche Kriminalstatistik (PKS) der Bundesrepublik Deutschland. In der PKS werden die von der (Kriminal-) Polizei bearbeiteten Verbrechen und Vergehen einschließlich der mit Strafe bedrohten Versuche gemäß eines definierten Straftatenkataloges und die dazu von der Polizei ermittelten Tatverdächtigen erfasst. Die statistische Erfassung eines Falles erfolgt nach Abschluss der polizeilichen Ermittlungen durch die für die Endbearbeitung zuständige Polizeidienststelle und bei Abgabe des Vorganges an die Staatsanwaltschaft oder das Gericht. Das Bundeskriminalamt fasst die angelieferten Einzeldatensätze zur Jahresstatistik der PKS der Bundesrepublik Deutschland zusammen. Daten privater Einrichtungen finden nur in einigen wenigen Einzelfällen zur Beschreibung aktueller Phänomene Berücksichtigung.

Der Polizei bekannt gewordene Fälle werden nach dem Tatortprinzip erfasst. Jeder Tatverdächtige wird für den Berichtszeitraum unabhängig von der Zahl der abgeschlossenen Ermittlungsvorgänge nach bestimmten Erfassungsgrundsätzen nur einmal gezählt. Wenn beispielsweise eine tatverdächtige Person in einem Statistikbereich mehrere Straftaten, die verschiedenen Schlüsselzahlen zuzuordnen sind, begangen hat, wird sie zu jeder Schlüsselzahl und zu der (den) jeweils nächst höheren Gruppe(n) sowie bei der Gesamtzahl nur einmal gezählt (Tatverdächtigenechtzählung).

Unabhängig von der Entwicklung der reinen Fall- bzw. Schadenszahlen haben die Intensität der kriminellen Aktivitäten im Bereich Cyberkriminalität und das für jeden Internetnutzer bestehende Gefährdungspotenzial weiter zugenommen. Diese Entwicklung lässt sich nicht zuletzt an der gestiegenen Professionalität der eingesetzten Schadsoftware sowie der festgestellten zunehmenden Spezialisierung und Professionalisierung der Täter ableiten.

Cyberkriminalität wird in der Polizeilichen Kriminalstatistik (PKS) darüber hinaus nicht vollständig abgebildet. Die Fälle von Cyberkriminalität werden unter verschiedenen Straftatenschlüsseln ausgewiesen. Fälle, bei denen der Geschädigte in Deutschland wohnt, der Ort der strafbaren Handlung aber im Ausland liegt oder liegen kann, werden beispielsweise nicht erfasst. Die Abbildung von Straftaten der Cyberkriminalität in der PKS wird zurzeit überarbeitet. Ziel ist es, Entwicklungen dieses Phänomenbereiches umfassender darstellen zu können.

Die PKS ist eine Ausgangsstatistik; die von der Polizei bearbeiteten Fälle werden nach Abschluss der Ermittlungen bei Abgabe an die Staatsanwaltschaft erfasst.

Vergleiche mit der Justizstatistik (siehe unten zu Frage 1.6) mit der PKS sind nicht möglich, weil zwischen den Erfassungszeitpunkten (PKS-Abgabe an die Justiz; rechtskräftige Entscheidung) zum Teil erhebliche Zeitspannen liegen, die Erfassungsgrundsätze und die rechtliche Würdigung abweichen.

Für den Bereich der Strafjustiz kann über die Anzahl der Abgeurteilten und Verurteilten berichtet werden (vgl. unten stehende Tabelle). Diese werden in der Strafverfolgungsstatistik erfasst. "Abgeurteilte" sind Angeklagte, gegen die Strafbefehle erlassen wurden bzw. Strafverfahren nach Eröffnung des Hauptverfahrens durch Urteil oder Einstellungsbeschluss rechtskräftig abgeschlossen worden sind. Ihre Anzahl setzt sich zusammen aus den Verurteilten und aus Personen, bei denen die andere Entscheidungen (z. B. Einstellung, Freispruch) getroffen wurden. "Verurteilte" sind Angeklagte, gegen die nach allgemeinem Strafrecht Freiheitsstrafe, Strafarrest oder Geldstrafe (auch durch einen rechtskräftigen Strafbefehl) verhängt worden ist, oder deren Straftat nach Jugendstrafrecht mit Jugendstrafe, Zuchtmittel oder Erziehungsmaßregeln geahndet wurde. Die Strafverfolgungsstatistik orientiert sich an den strafrechtlichen Vorschriften.

Einige Vorschriften des Strafgesetzbuchs können als Computerdelikte im engeren Sinne bezeichnet werden, während andere Delikte sowohl mittels Computer bzw. Internet als auch auf andere Weise verwirklicht werden können, ohne dass insoweit statistisch differenziert werden könnte. Deshalb wird in der unten stehenden Tabelle zwischen "Computerdelikten im engeren Sinne" und "sonstigen Delikten" unterschieden. Dies wirkt sich auch auf den Anteil der Verurteilungen wegen Cyberkriminalität an der Gesamtzahl aller Verurteilungen aus.

Legt man insoweit den engeren Begriff von Computerdelikten zugrunde, beträgt der Anteil im Jahr 2013 0,3 % (2 728 von 755 938 Verurteilungen), bei einem weiteren Verständnis 0,7 % (5 788 von 755 938 Verurteilungen). Ein Vergleich dieser Anteile mit den polizeilichen Zahlen (siehe oben 1.4) kommt aus verschiedenen Gründen nicht in Betracht, unter anderem schon deshalb, weil die Polizeiliche Kriminalstatistik anders als die Strafverfolgungsstatistik keine Straßenverkehrsdelikte erfasst. Hinsichtlich der Entwicklung der Verurteilungszahlen in den letzten Jahren (2011-14) kann keine wesentliche Veränderung festgestellt werden (siehe Tabelle unten).

Anzumerken bleibt, dass der Straftatbestand der Datenhehlerei nach § 202d Strafgesetzbuch (StGB) erst im Dezember 2015 in Kraft getreten ist, sodass es diesbezüglich noch keine statistische Erfassung gibt.

Abgeurteilte und Verurteilte wegen Computerdelikten

	2011		2012		2013		2014	
Straftatbestand (§§ StGB)	**Abgeurteilte**	**Verurteilte**	**Abgeurteilte**	**Verurteilte**	**Abgeurteilte**	**Verurteilte**	**Abgeurteilte**	**Verurteilte**
Computerdelikte i.e.S.								
202a Ausspähen von Daten	80	48	73	41	64	30	***84***	***48***
202b Abfangen von Daten	2	1	5	2	3	2	***1***	***1***
202c Vorbereiten des Ausspähens u. Abfangens von Daten	2	2	2	2	1	1	***4***	***1***
263a Computerbetrug	3.439	2.797	3.393	2.777	3.252	2.645	***3.241***	***2.628***
303a Datenveränderung	50	27	59	36	53	32	***46***	***24***
303b Computersabotage	18	10	28	15	26	18	***22***	***12***
Computerdelikte i.e.S. insgesamt	**3.591**	**2.885**	**3.560**	**2.873**	**3.399**	**2.728**	***3.398***	***2.714***
sonstige Delikte								
184 Verbreitung pornographischer Schriften	150	116	195	154	213	158	***282***	***222***
184a Verbreitung gewalt- o. tierpornograph. Schriften	17	11	9	9	10	9	***13***	***11***
184b Verbreitung, Erwerb, Besitz kinderpornograph. Schr.	1.716	1.611	1.892	1.788	1.795	1.679	***2.170***	***2.022***
184c Verbreitung, Erwerb, Besitz jugendpornograph. Schr.	109	90	112	100	125	101	***158***	***133***
184d Verbreitung pornograph. Darbietungen durch Medien	14	12	13	11	18	13	***15***	***9***
130 Abs. II Nr. 1 und 2 Volksverhetzung	67	53	49	39	32	25	***57***	***43***
131 Gewaltdarstellung	15	6	15	12	16	12	***22***	***9***
266b Missbrauch von Scheck- und Kreditkarten	61	40	52	39	41	28	***42***	***20***
269, 270* Fälschung beweiserheblicher Daten	996	845	1.033	864	1.218	1.035	***1.371***	***1.159***
Sonstige Delikte insgesamt	**3.145**	**2.784**	**3.370**	**3.016**	**3.468**	**3.060**	***4.130***	***3.628***
Computerdelikte insgesamt	**6.736**	**5.669**	**6.930**	**5.889**	**6.867**	**5.788**	***7.528***	***6.342***

* § 270 StGB wird in der Strafverfolgungsstatistik nicht gesondert ausgewiesen

Quelle: Statistisches Bundesamt, Fachserie 10 Reihe 3 (Strafverfolgung)

Hinsichtlich der polizeilichen Daten wird auf die Polizeiliche Kriminalstatistik (PKS) verwiesen, die auch in englischer Sprache unter folgender Adresse verfügbar ist:
http://www.bka.de/DE/Publikationen/PolizeilicheKriminalstatistik/pks__node.html

Darauf basieren auch die Bundeslagebilder Cybercrime, die hier abrufbar sind:
http://www.bka.de/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime__node.html?__nnn=true

Wegen der oben bereits genannten Änderungen in der statistischen Erfassung von Cyberkriminalität ist auf Basis der Zahlen von 2014 auch innerhalb einer Veröffentlichungsreihe leider kein Vergleich zu vorhergehenden Jahren möglich.

3.4. Innerstaatliche Haushaltsmittel zur Prävention und Bekämpfung von Cyberkriminalität sowie Unterstützung durch EU-Haushaltsmittel

Die Mittelzuweisung für die Strafverfolgungsbehörden zur Bekämpfung der Cyberkriminalität (präventiv wie auch repressiv) erfolgen auf Basis der festgelegten Landes- und Bundeshaushalte. Weitere externe Finanzquellen stehen den Polizeibehörden in der Regel nicht zur Verfügung. Lediglich in Ausnahmefällen, z. B. zur Finanzierung von internationalen (europaweiten) Forschungsvorhaben bzw. im Rahmen von EMPACT-Maßnahmen, kann eine Unterstützung durch Mittel der EU erfolgen.

Das Bundeskriminalamt (BKA) erhält aktuell EU-Mittel zur Bekämpfung der Cyberkriminalität im Rahmen des (zwischenzeitlich ausgelaufenen) EU-Förderprogramms "ISEC" ("Internal Security", Laufzeit von 2007 bis 2013). Hier führt das BKA gemeinsam mit den Niederlanden und Schweden das Projekt "Cyber-OK – Ausmaß und Ausprägungen in ausgewählten EU-Mitgliedsstaaten" mit einer Laufzeit vom 1. April 2014 bis 31. März 2016 und einem Projektvolumen von rund 500 000 EUR durch. Das Projekt ist abgeschlossen; der Abschlussbericht kann online unter folgender Adresse eingesehen werden: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/PolizeiUndForshung/1_50_Cyber-OCScopeandManifestationsInSelectedEUMemberStates.html.
Im Jahr 2014 bestand wieder die Möglichkeit, Vorhaben, die der Verhütung und der Bekämpfung der Cyberkriminalität innerhalb der Europäischen Union dienen, durch die Beantragung von Fördermitteln der EU teilfinanzieren zu lassen. Dazu stellte die EU-Kommission im Programm "Internal Security Fund – Police" (ISF-zentral) ca. 5 Mio. EUR zur Verfügung. Eine Beantragung von Projekten ist erst nach gesonderten Aufrufen zur Einreichung von Projektvorschlägen ("calls for proposals") möglich.

In den Ländern erfolgt die Mittelzuweisung im Rahmen der allgemeinen Aufgabenwahrnehmung. Vereinzelt werden zusätzliche Stellen oder überplanmäßige Ausgaben bewilligt. EU-Mittel wurden – soweit bekannt – durch die Länder bislang nicht beantragt. An der Finanzierung des polizeilichen Präventionsprogramms ProPK sind die Länder gemäß des Königsteiner Schlüssels[8] beteiligt. Die Erstellung und Entwicklung von Medien unter anderem zur Prävention von Cyberkriminalität erfolgen hier bundesweit. Die Materialien werden entsprechend abgerufen und genutzt.

Deutschland verfügt über eine robuste nationale Cyber-Sicherheitsstrategie, die 1991 eingeführt wurde, sowie seit 2009 über eine polizeiliche Bekämpfungsstrategie Cybercrime, die zuletzt 2015 überarbeitet wurde.

Daneben bestehen auch auf Landesebene zum Teil eigene Strategien und Konzepte zur Bekämpfung und Prävention im Phänomenbereich Cyberkriminalität.

[8] Im Königsteiner Schlüssel ist festgelegt, wie die einzelnen Länder der Bundesrepublik Deutschland an gemeinsamen Finanzierungen zu beteiligen sind. Der Anteil, den ein Land danach tragen muss, richtet sich zu zwei Dritteln nach dem Steueraufkommen und zu einem Drittel nach der Bevölkerungszahl.

Das Ziel der nationalen Strategie besteht darin, in Deutschland für ein gebührendes Maß an Cyber-Sicherheit entsprechend den Erfordernissen der Verwaltung und der Wirtschaft zu sorgen. In der Cyber-Sicherheitsstrategie für Deutschland werden zehn vorrangige Ziele und Maßnahmen aufgeführt:

- Schutz kritischer Infrastrukturen
- Sichere IT-Systeme in Deutschland
- Stärkung der IT-Sicherheit in der öffentlichen Verwaltung
- Nationales Cyber-Abwehrzentrum
- Nationaler Cyber-Sicherheitsrat
- Wirksame Maßnahmen gegen Cyberkriminalität
- Effektives Zusammenwirken für Cyber-Sicherheit in Europa
- Einsatz verlässlicher und vertrauenswürdiger Informationstechnologie
- Angemessener Ausbau der personellen Kapazitäten und der Fähigkeiten der Bundesbehörden
- Instrumentarium zur Abwehr von Cyber-Angriffen

Die Notwendigkeit eines harmonisierten Schutzniveaus bei der IT-Sicherheit wurde ebenso hervorgehoben wie die Tatsache, dass Wirtschaftsunternehmen Sicherheitsmaßnahmen im IT-Bereich ergreifen sollten.

Es wurden folgende Elemente benannt, die weitere Überlegungen erfordern:

- Abschreckung böswilliger Akteure
- Prüfung der militärischen Aspekte innerhalb der Strategie
- Einführung des Konzepts der aktiven Cyber-Abwehr
- Verbesserung der Widerstandsfähigkeit der Infrastruktur durch den Einsatz von Netzen, die vom Internet getrennt sind
- Verbesserung der Zusammenarbeit zwischen Behörden und Wirtschaftsunternehmen, um Angriffen besser entgegenwirken zu können
- Wirksamer Schutz der Privatsphäre und der informationellen Selbstbestimmung im europäischen Binnenmarkt

3.5. Fazit

- **Deutschland verfügt über zwei Cyber-Sicherheitsstrategien, eine auf Bundesebene und eine spezifischere Strategie auf BKA-Ebene. Zudem haben einige Bundesländer eigene Cyber-Sicherheitsstrategien. Die nationale Cyber-Sicherheitsstrategie deckt einen weiten Bereich von Themen ab, und in Deutschland sind zwei Einrichtungen mit der Cyber-Sicherheit befasst (das Nationale Cyber-Abwehrzentrum und der Nationale Cyber-Sicherheitsrat).**

- **Die Regierung hat den Privatsektor (Wirtschaft, Industrie, Bitkom usw.) in die Ausgestaltung der nationalen Cyber-Sicherheitsstrategie einbezogen. Allerdings ist der Gutachterausschuss der Auffassung, dass weitere wichtige Akteure, beispielsweise die Generalstaatsanwaltschaft oder die Strafverfolgungsbehörden, in größerem Maße einbezogen werden könnten.**

- **Die Strategie ist an einen Umsetzungsplan mit genau festgelegten Fristen gebunden. Das Handlungsfeld Cyber-Sicherheit wird von der deutschen Polizei als die wichtigste Herausforderung für die nächsten 10-15 Jahre betrachtet.**

- **Der Schutz kritischer Infrastrukturen betrifft staatliche Einrichtungen, die Gesellschaft und die Wirtschaft. Am Nationalen Cyber-Sicherheitsrat beteiligen sich Vertreter zuständiger öffentlicher Verwaltungen, die mit Wirtschaftsvertretern zusammenarbeiten. Das BSI arbeitet gut mit ENISA zusammen.**

- **Die nationalen Prioritäten sind auf die wichtigsten Aspekte des Phänomens ausgerichtet – z. B. Prävention, Kapazitätsaufbau, Aus- und Fortbildung, internationale und innerstaatliche Zusammenarbeit – und entsprechen dem EU-Politikzyklus 2014-2017.**

- **In Deutschland werden die polizeilichen Kriminalstatistiken vom BKA erstellt, wobei Cybercrime-Straftaten unterschiedlichen Straftatbeständen zugeordnet werden oder in der Kriminalstatistik nicht erfasst werden, wenn die Straftäter keinen Wohnsitz in Deutschland haben (auch wenn die Opfer in Deutschland wohnen). Allerdings wird die BKA-Kriminalstatistik derzeit überarbeitet, um die Erfassung auszuweiten. Die Polizeiliche Kriminalstatistik kann nicht mit den Justizstatistiken verglichen werden, da die Erhebungszeiträume nicht übereinstimmen (Straftaten werden erst erfasst, wenn die polizeilichen Ermittlungen abgeschlossen sind und die betreffenden Fälle an die Staatsanwaltschaft oder das Gericht weitergeleitet werden können), die Erfassungsmodalitäten und Daten sich unterscheiden und im Einzelfall das Gericht eine andere strafrechtliche Einordnung vornehmen kann. Daher ergibt sich durch eine Zusammenführung der Kriminal- und der Justizstatistik kein zusätzlicher Nutzen.**

- **Sowohl die Bundes- auch die Länderhaushalte sehen Mittelzuweisungen für die Bekämpfung der Cyberkriminalität vor. Zudem hat das BKA von der EU Fördermittel für einige Projekte erhalten, z. B. "Cyber OC - Scope and manifestations in selected EU Member States".**

4. NATIONALE STRUKTUREN

4.1. Justiz (Strafverfolgungen und Gerichte)

4.1.1. Interne Struktur

In Deutschland sind insbesondere folgende Behörden und Dienststellen für die Verhütung, Auswertung und Bekämpfung von Cyberkriminalität zuständig:

- Die Staatsanwaltschaften der Länder (zum Beispiel die Zentralstelle zur Bekämpfung der Internetkriminalität "ZIT" bei der Generalstaatsanwaltschaft Frankfurt am Main),
- das Bundeskriminalamt (BKA) (insbesondere die Gruppe SO 4),
- Kriminalpolizeidienststellen der Länder,
- das Bundesamt für Verfassungsschutz (BfV) ,
- die Landeskriminalämter (LKÄ)
- die Landesämter für Verfassungsschutz
- die Bundespolizei (BPOL)
- das Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie
- das Zollkriminalamt (ZKA).

Die Bekämpfung von Cyberkriminalität erfordert eine enge Zusammenarbeit auf Bundes- und Landesebene. Hierfür stehen sowohl im BKA als auch in den Ländern zentrale Ansprechpartner zur Verfügung. In ihrer Arbeit mit den zuständigen Bundesbehörden (BKA, BSI, BPOL, BfV, ZKA) haben sich die jeweiligen *Single Points of Contact* und gemeinsame Fachtagungen bewährt und zum Aufbau eines engen Informationsnetzwerkes geführt.

Die Strafverfolgung ist Ländersache. Die meisten Länder haben bei den Staatsanwaltschaften entweder Schwerpunktstaatsanwaltschaften zur Bekämpfung von Cyberkriminalität (so die Länder Brandenburg (Staatsanwaltschaft Cottbus), Thüringen (Staatsanwaltschaft Mühlhausen) und Mecklenburg-Vorpommern (Schwerpunktstaatsanwaltschaft für Informations- und Kommunikationskriminalität (IuK) in Rostock) oder Sonderdezernate bzw. Ansprechpartner für Cybercrime bei den Staatsanwaltschaften geschaffen (so die Länder Baden-Württemberg, Bayern, Berlin, Bremen, Hamburg, Mecklenburg-Vorpommern, Niedersachen, Rheinland-Pfalz, Saarland, Sachsen, Sachsen-Anhalt und Schleswig-Holstein).

Baden-Württemberg hat 2011 bei der Generalstaatsanwaltschaft Stuttgart eine Zentralstelle für die Bekämpfung der Informations- und Kommunikationskriminalität (ZIK) eingerichtet. Für Niedersachsen besteht bei der Generalstaatsanwaltschaft Celle eine zentrale Koordinierungs- und Unterstützungsstelle (ZOK = Zentrale Stelle Organisierte Kriminalität und Korruption).

Die ZOK, deren Aufgabengebiet den Bereich der Internetkriminalität bzw. der Kriminalität auf dem Gebiet der Informations- und Kommunikationstechnik (IuK-Kriminalität) umfasst, fungiert für den Bereich "Cybercrime" als Koordinator und zentraler Ansprechpartner u. a. für die drei niedersächsischen Schwerpunktstaatsanwaltschaften zur Bekämpfung der IuK-Kriminalität (Staatsanwaltschaften Göttingen, Osnabrück und Verden). Darüber hinaus kommen der ZOK Schulungs- und Beratungsfunktionen zu. Rheinland-Pfalz hat auf Seiten der Staatsanwaltschaft zum 1. Oktober 2014 die Landeszentralstelle Cybercrime (LZC), die landesweit für die Verfolgung von Cyberkriminalität zuständig ist, geschaffen. Zum 1. Januar 2015 hat Bayern bei der Generalstaatsanwaltschaft Bamberg eine Zentralstelle zur Bekämpfung der Computer- und Internetkriminalität (Zentralstelle Cybercrime Bayern- ZCB) eingerichtet. Am 15. März 2016 hat Sachsen bei der Generalstaatsanwaltschaft Dresden eine Zentralstelle für die Bekämpfung von Cyberkriminalität eingerichtet, die als Ansprechstelle sowohl für die Staatsanwaltschaften in Sachsen als auch für die Zentralstellen anderer Bundesländer bei Cyberkriminalitätsverfahren dient. Sie koordiniert auch die Aus- und Fortbildung sächsischer Staatsanwälte auf dem Gebiet der Cyberkriminalität. Ferner ermittelt die Zentralstelle in schweren und komplexen Fällen von Cyberkriminalität auch selbst, zusammen mit dem sächsischen Cybercrime Competence Center (SN4C) des Landeskriminalamtes.

Am 11. April 2016 hat das Land Nordrhein-Westfalen eine Zentral- und Ansprechstelle Cybercrime bei der Staatsanwaltschaft Köln eingerichtet. Die Stelle führt Cybercrime-Ermittlungsverfahren von herausgehobener Bedeutung, dient als zentrale Ansprechstelle für Polizei, Justiz, Wirtschaft und Wissenschaft und ist an regionalen und überregionalen Aus- und Fortbildungsprogrammen beteiligt. Schleswig-Holstein hat bei der Generalstaatsanwaltschaft eine Zentralstelle für die Koordinierung der Ermittlungen bei Cyberkriminalität eingerichtet.

Die Ermittlung von Cyberstraftaten ist in Mecklenburg-Vorpommern durch Dienstanweisung des Generalstaatsanwalts seit dem 1. Juli 2012 der Schwerpunktstaatsanwaltschaft für Informations- und Kommunikationskriminalität (IuK) in Rostock übertragen worden. Die Schwerpunktgruppe setzt sich derzeit aus einem Gruppenleiter und drei Dezernenten zusammen. Das Land Hessen hat bei der Generalstaatsanwaltschaft Frankfurt am Main eine Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) geschaffen. Schleswig-Holstein hat bei der Generalstaatsanwaltschaft eine Zentralstelle eingerichtet, die die Verfolgung von Cybercrime-Straftaten koordiniert.

In den meisten Bundesländern bestehen keine speziellen Zuständigkeiten der Gerichte. In Nordrhein-Westfalen besteht am Landgericht Köln jedoch eine spezielle Strafkammer als Ergänzung zu der Zentral- und Ansprechstelle Cybercrime bei der Staatsanwaltschaft Köln.

4.1.2. Fähigkeit zur und Hemmnisse für eine erfolgreiche Strafverfolgung

In Bund und Ländern wurden eigene Organisationseinheiten zur Bekämpfung von Cyberkriminalität aufgebaut. Teilweise wurden auch in den Flächendienststellen der Landespolizeien spezielle Arbeitsbereiche bei den für die Kriminalitätsbekämpfung zuständigen Dienststellen für die Bearbeitung der Cyberkriminalität geschaffen.

Auf Bundesebene wie auf Landesebene werden die sachliche und personelle Ausstattung der Sicherheitsbehörden weiter verbessert und die technischen und rechtlichen Befähigungen den jeweiligen Aufgaben angepasst.

Die Kompetenzen des Bundeskriminalamtes (BKA) und der Bundespolizei sollen im Bereich Cybercrime gestärkt werden. Das Cybercrime Centre im BKA soll ausgebaut werden und die Bearbeitung phänomenübergreifender Internetaktivitäten zusammengefasst werden.

Auf der Plattform des Nationalen Cyber-Abwehrzentrums soll das arbeitsteilige Zusammenwirken der fachlich spezialisierten Behörden verbessert werden.
Durch das am 18. Dezember 2015 in Kraft getretene Gesetz wurde der Straftatbestand der Datenhehlerei geschaffen.

Im Hinblick auf die Bundesländer wurden – ohne Anspruch auf Vollständigkeit – folgende Informationen gemeldet:

Baden-Württemberg:
Zur Intensivierung der Bekämpfung der Cyberkriminalität und zur Optimierung der IuK-Einsatz- und Ermittlungsunterstützung im Bereich der digitalen Spuren wurden zum Jahresbeginn 2012 bestehende Einheiten des Landeskriminalamts Baden-Württemberg (LKA BW) zu einer neuen Abteilung "Cybercrime und Digitale Spuren zusammengeführt". Die Abteilung wurde in den folgenden Jahren personell verstärkt, zuletzt im Rahmen der Umsetzung der Polizeireform zum 1. Januar 2014, und hat derzeit einen Personalstamm von 98 Mitarbeiterinnen und Mitarbeitern.

Im Rahmen der Umsetzung der Polizeireform wurden zudem die Kriminalinspektionen 5 (Cybercrime, Digitale Beweismittel) bei den regionalen Polizeipräsidien eingerichtet. Diese Inspektionen nehmen spiegelbildlich die Aufgaben der Abteilung Cybercrime und Digitale Spuren (Abteilung 5) im LKA BW wahr. Ausnahmen hiervon sind landesweite Servicedienstleistungen wie der Betrieb des Telekommunikationsüberwachungs (TKÜ)-Zentrums, die Mobilfunkaufklärung oder die Netzwerkforensik sowie die Internetrecherche und die Ansprechstelle Kinderpornografie. Diese Aufgaben werden ausschließlich im LKA BW wahrgenommen.

Neben der Einrichtung einer neuen Abteilung wurden neue landesweite Gremien wie der Steuerungskreis Cybercrime/Digitale Spuren sowie Arbeitskreise für die einzelnen Themenbereiche wie Ermittlungen, Digitale Spuren und Datenanalyse initiiert.

Die polizeiliche Schwerpunktsetzung bei der Bekämpfung von Cyberkriminalität, insbesondere seit Gründung der Abteilung 5 im LKA BW, führt dazu, dass nicht nur Cyberkriminalität im engeren Sinne stärker in das Bewusstsein aller Kolleginnen und Kollegen gerückt ist, sondern auch die Bekämpfung der Internetkriminalität (Cyberkriminalität mit dem Internet als Tatmittel) insgesamt. Insofern ist in der Gesamtschau eine deutliche Verbesserung der Bekämpfung von Cyberkriminalität im ganzen Land festzustellen.

Berlin:

Bei der Berliner Polizei sind folgende Dienststellen mit dem Thema Cybercrime befasst:
Landeskriminalamt (LKA) 75: Forensische Informations- und Kommunikationstechnik (IuK), einschließlich der Patenschaft für die Hotspots in den örtlichen Direktionen

LKA 72: Zentralstelle Internet (Ermittlungsunterstützung der Sachbearbeitung bei Ermittlungen im Internet, welche über das übliche Tätigkeitsfeld eines Sachbearbeiters hinaus reichen).

LKA 33: Ermittlungen führende Dienststelle mit den Zuständigkeiten der Datendelikte (§§ 202 a bis 202c StGB sowie §§ 303a, 303b StGB und §§ 269, 270, 271, 274 Absatz 1 Nummer 2, 348 StGB) sowie Phishing im Zusammenhang mit Geldwäsche (§ 263a sowie § 261 StGB).

LKA 33 vertritt den Themenbereich "Cybercrime" bei der Leitertagung Cybercrime des Bundes und der Länder. Die Zentrale Ansprechstelle Cybercrime (ZAC) für die Wirtschaft beim LKA Berlin ist hier angesiedelt. Beide Aufgaben erfordern eine Zusammenarbeit mit den anderen Bundesländern. Die ZAC leistet Netzwerkarbeit in Berlin und ist per se Ansprechpartner in allen Fragen der Cyberkriminalität.

Im Bereich der Cyberkriminalität im weiteren Sinne ist eine Vielzahl von Dienststellen – abhängig vom Delikt – zuständig. Exemplarisch sind dabei zu nennen:

LKA 13 – Kinderpornografische Abbildungen im Internet

LKA 23/25 – Verstöße gegen das Urheberrecht (im Internet)

LKA 33 – (Online-) Waren- und Leistungsbetrug.

LKA Präv. – Steuerung, Koordinierung und – in ausgesuchten Fällen – Initiierung von Präventionsmaßnahmen.

Brandenburg

Die Bekämpfung des Phänomens "Cybercrime" innerhalb des Polizeipräsidiums (PP) erfolgt dreistufig auf Ebene der Fachdirektion Landeskriminalamt (FD LKA), der Kriminalpolizei der Polizeidirektionen (PD) sowie der Kriminalkommissariate der Inspektionen (KKI).
Durch das PP wurde ein "Netzwerk gegen Cybercrime" – u. a. unter Mitwirkung der Schwerpunktstaatsanwaltschaft "zur Bekämpfung der Computer und Datennetzkriminalität sowie Gewalt darstellender, pornografischer und sonstiger jugendgefährdender Schriften" eingerichtet.
Weiterhin wird eine enge nationale und internationale Zusammenarbeit angestrebt, bspw. durch Teilnahme am Nordverbund "Cybercrime", der Kooperation mit anderen Polizeidienststellen des Bundes und der Länder (u. a. Hospitationen, Erfahrungsaustausche), um eine Zusammenarbeit mit anderen Behörden und Einrichtungen auszubauen.

Saarland

Die Zuständigkeiten für den Bereich Cyberkriminalität verteilen sich im Landeskriminalamt auf das Dezernat LPP 222 Cybercrime (Zentralstelle) und auf neun Kriminaldienste/ Polizeiinspektionen.
Das Dezernat LPP 222 Cybercrime ist die Cybercrime-Zentralstelle der saarländischen Polizei im Sinne des Gesetzes über das Bundeskriminalamt (BKA) und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKAG). Die Dienststelle ist damit Bindeglied zwischen den Dienststellen der saarländischen Polizei und den LKÄ bzw. dem BKA.
Durch das Fachdezernat werden im Rahmen der Funktion "Zentrale Ansprechstelle Cybercrime für die Wirtschaft und sonstige öffentliche und nichtöffentliche Stellen" Kontakte zu Unternehmen und Verbänden, zur Wissenschaft und sonstigen Stellen aufgebaut und gepflegt.

Sachsen

Für die Bekämpfung von Cyberkriminalität sind in der sächsischen Polizei für den Freistaat Sachsen sowohl die Polizeidirektionen als auch das Landeskriminalamt (LKA) zuständig.

Das Landeskriminalamt bearbeitet Cybercrime-Fälle unter anderem auf Anordnung des Sächsischen Staatsministeriums des Innern, auf Zuweisung des Bundeskriminalamtes an den Freistaat Sachsen, sofern das sächsisches Innenministerium (SMI) keine andere Polizeidienststelle für zuständig erklärt, oder auf Zuweisung der Generalstaatsanwaltschaft bzw. Ersuchen einer Staatsanwaltschaft.

Darüber hinaus kann das Landeskriminalamt die vollzugspolizeiliche Ermittlungstätigkeit übernehmen, wenn direktionsübergreifende Ermittlungen erforderlich sind und eine einheitliche Verfolgung zweckmäßig erscheint oder eine andere Polizeidienststelle wegen des Umfangs, der Überörtlichkeit oder der hohen Öffentlichkeitswirksamkeit darum ersucht.

Kernelement der Neuausrichtung der Bekämpfung von Cyberkriminalität in der sächsischen Polizei ist die Einrichtung eines Cybercrime-Competence Centers (SN4C) im LKA am 10. Juni 2014. Im SN4C wird der bisher in verschiedenen Abteilungen "verstreute" Informations- und Kommunikationstechnik (IuK)-Sachverstand unter einheitlicher Führung in einer Organisationseinheit konzentriert.

Schleswig-Holstein

Die Ermittlungen und Zentralstellentätigkeiten in Sachen Cyberkriminalität und für Delikte im Zusammenhang mit Kinderpornografie werden in Schleswig-Holstein auf unterschiedlichen polizeilichen Ebenen vorgenommen:

Landeskriminalamt:

- Projekt "Zentrale Organisationseinheit Cybercrime (ZOEC)"
- Zentralstelle (Zentrale Ansprechstelle für Dienststellen des Landes und des Bundes, der Wirtschaft sowie öffentlicher und nicht-öffentlicher Einrichtungen)
- Ermittlungen zur Bekämpfung von Delikten der "qualifizierten Cybercrime"
- Zentrale IT-Beweissicherung – für das (Landeskriminalamt) LKA und die Landesebene
- Ansprechstelle Kinderpornografie

Bezirkskriminalinspektionen:

- Regionale IT-Beweissicherung (rITB) – für die Landgerichtsbezirke

Kriminalinspektionen/ Kriminalpolizeistellen

- Alle Delikte, die nicht der "qualifizierten Cybercrime" zugeordnet werden können sowie u. a.
- Waren-/Warenkreditbetrügereien
- Kinderpornografie

Darüber hinaus findet derzeit eine Betrachtung des Ist-Zustandes der Landespolizei durch die "AG Bekämpfungskonzeption Cybercrime" hinsichtlich organisatorischer und inhaltlicher Erfordernisse zur effektiven Bekämpfung von Cyberkriminalität statt.

Auf Ebene des Landeskriminalamts (LKA) ist seit dem 1. Februar 2014 das Projekt "ZOEC" (Zentrale Organisationseinheit Cybercrime) eingerichtet. Im Rahmen des Projektes werden die zentrale IT-Beweissicherungsgruppe des LKA, die Ermittlungen in Sachen "qualifizierte Cybercrime", die Ansprechstelle Kinderpornografie und die Zentrale Ansprechstelle Cybercrime (ZAC) zusammengefasst.

Thüringen

Bei der Thüringer Polizei sind die Einrichtungen zur Verhütung, Bekämpfung und forensischen Auswertung/Begutachtung im Bereich Cyberkriminalität organisatorisch getrennt.
Die Verhütung von Cyberkriminalität fällt aufgrund der verschiedenen beteiligten Themenbereiche in den Wirkungskreis diverser staatlicher und nichtstaatlicher Stellen. Neben Polizei und Justiz sind hier insbesondere die Bildungseinrichtungen zu nennen. Die Zusammenarbeit besteht anlassbezogen, eine Koordinierung zwischen den Institutionen erfolgt derzeit nicht.

Ermittlungsverfahren im Bereich der Cyberkriminalität wurden/werden sowohl durch das Landeskriminalamt (LKA) Thüringen als auch die örtlichen zuständigen Dienststellen je nach Deliktsbereich bearbeitet.

Im LKA Thüringen wurde am 1. September 2014 zur Effektivierung der Bekämpfung von Cyberkriminalität das Dezernat 64 (Cybercrime) gegründet. Dieses gliedert sich in die Bereiche Auswertung, Bekämpfung von Cyberkriminalität und ZASt (Zentrale technische Auswertestelle zur Bekämpfung der Kinder- und Jugendpornografie). Im LKA Thüringen werden besondere Fälle der Cyberkriminalität, Ermittlungsverfahren im Zusammenhang mit der Verbreitung von Kinder- und Jugendpornografie sowie Ermittlungsverfahren wegen des Verdachts des sexuellen Missbrauchs von Kindern, bei denen die Tathandlung in der Herstellung von kinderpornografischen Schriften besteht, bearbeitet.

Alle anderen Delikte im Bereich Cyberkriminalität werden durch die örtlich zuständigen Dienststellen in den Landespolizeiinspektionen bearbeitet.

Eine Sicherung und Aufbereitung der in Cybercrimeverfahren festgestellten Daten zur Auswertung durch den Sachbearbeiter erfolgt sowohl durch das Dezernat 43 im LKA Thüringen als auch durch die Regionalen Beweissicherungseinheiten, die den einzelnen Landespolizeiinspektionen angegliedert sind. In Fällen, in denen eine technisch aufwändige Auswertung notwendig ist, erfolgt die gesamte Auswertung der Daten durch Mitarbeiter des Dezernates 43. Auch werden Gutachten ausschließlich in diesem Bereich gefertigt. In den Regionalen Beweissicherungseinheiten und dem Dezernat 43 sind spezielle IT-Untersuchungsbeamte tätig.

Das Dezernat 33 des LKA Thüringen realisiert die Technische Einsatz- und Ermittlungsunterstützung für Thüringen (z. B. Schaltung von Telekommunikationsüberwachungs (TKÜ) -Maßnahmen).

Ein Erfahrungs- und Wissensaustausch der beteiligten Bereiche erfolgt in Fachtagungen. Das Dezernat 64 steht den Landespolizeibehörden bei Fachfragen in Bezug auf Cyberkriminalität als Ansprechpartner zur Verfügung.

Nach der durch das Grundgesetz vorgesehenen Kompetenzverteilung zwischen Bund und Ländern ist die Ausübung staatlicher Befugnisse und die Erfüllung staatlicher Aufgaben Sache der Länder, soweit das Grundgesetz keine andere Regelung trifft oder zulässt. Diesem Grundsatz entsprechend obliegt die Strafverfolgung grundsätzlich den Strafverfolgungsbehörden der Länder, namentlich den Staatsanwaltschaften und ihren Ermittlungspersonen. In besonders geregelten Fällen, namentlich im Bereich des Staatschutzes, bestehen Zuständigkeiten des Generalbundesanwaltes und des Bundeskriminalamtes. Im Bundeskriminalamt besteht eine für Cyberkriminalität zuständige Organisationseinheit (Gruppe SO4). Präventionsprogramme werden von der Projektleitung "Polizeiliche Kriminalprävention der Länder und des Bundes" erarbeitet, diese richten sich je nach Deliktsfeld im Phänomenbereich Cyberkriminalität an unterschiedliche Adressaten.

Die Mehrheit der Länder hat bei den jeweiligen Landeskriminalämtern Sonderdezernate zur Bekämpfung von Cyberkriminalität eingerichtet. Die Sonderdezernate verfügen über Personal mit fundierten IT-Kenntnissen und spezieller informationstechnischer Sachkunde.

4.2. Strafverfolgungsbehörden

Im Hinblick auf die Bundesländer wurden – ohne Anspruch auf Vollständigkeit – folgende Informationen gemeldet:

Berlin:
In Berlin werden Cyberstraftaten im engeren Sinne (keine Online-Kartendelikte) bei der Polizei im Landeskriminalamt (LKA) LKA 33, konkret LKA 336 (Phishing im Zusammenhang mit Online-Banking) sowie LKA 335 (Datendelikte sowie Computersabotage) bearbeitet. Darüber hinaus gibt es eine Reihe von Dienststellen, die Cyberkriminalität im weiteren Sinne bearbeiten. Der gegenständliche Einsatz von Zahlungskarten (einschl. Skimming) wird bei LKA 36 bearbeitet. Die Zuständigkeit für die betrügerische Erlangung von Leistungen und Waren mittels Zahlungskartendaten obliegt LKA 37. LKA 13 ist zuständig für den im Internet abgebildeten Missbrauch von Kindern (Kinderpornografie).

Diese Dienststellen sind im Rahmen ihrer Aufgabenwahrnehmung auch für die Prävention zuständig. Sofern bei Dienststellen der Berliner Polizei Unterstützungsbedarf in Fragen der Internet-Ermittlung (einschl. Live-Forensik) gegeben ist, steht LKA 722 als Zentralstelle Internet verfahrensbegleitend zur Verfügung. Die forensische Auswertung von sichergestellten Datenträgern oder deren Duplikaten ist Aufgabe von LKA 75. In den Flächendirektionen (Direktion 1 -6) sind Sachgebiete zur Informations- und Kommunikationstechnik (IuK)-Ermittlungsunterstützung bei den Ref VB eingerichtet worden. Neben der Auswertung von Handys sind diese mit einer Reihe von verfahrensunterstützenden IuK-Fragestellungen befasst (z. B. Anpassung von Datenformaten von Überwachungskameras zur fallbezogenen Auswertung).

Mecklenburg-Vorpommern

Die Bearbeitung von Cybercrime-Straftaten erfolgt in Mecklenburg-Vorpommern (MV) grundsätzlich entsprechend dem Grunddelikt durch die Kriminalkommissariate, die Kriminalpolizeiinspektionen in den Fachkommissariaten 5 (Wirtschaft, Umwelt und Cybercrime) oder das Landeskriminalamt MV.

Die Kriminalpolizeiinspektionen sind darüber hinaus zuständig für Straftaten gegen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten und -systemen (insbesondere §§ 202a-d, 263a, 303a, b StGB) sowie andere Delikte, deren Bearbeitung eine spezielle informationstechnische Sachkunde erfordert.

Das Landeskriminalamt MV ist darüber hinaus zuständig, wenn der Sachverhalt eine zentrale Sachbearbeitung erfordert, weil beispielsweise tiefergehende IT-Kenntnisse, spezielle informationstechnische Sachkunde und/oder erheblicher nationaler oder internationaler Koordinierungsaufwand notwendig ist.

Mit Wirkung vom 1.März 2011 wurde im Landeskriminalamt MV das Dezernat 45/ Cybercrime eingerichtet. Das Dezernat 45 gliedert sich in die Arbeitsbereiche Grundsatz/Auswertung; Ermittlungen; Ermittlungsunterstützung und die Ansprechstelle Kinderpornografie. Das Dezernat 45 fungiert zugleich auch als Zentrale Ansprechstelle Cybercrime und unterstützt die Kriminalkommissariate und Kriminalpolizeiinspektionen bei den Ermittlungen.

Sachsen-Anhalt

Grundsätzlich werden die Delikte von den örtlich zuständigen Polizeidienststellen bearbeitet. Die Zuständigkeit des Landeskriminalamts (LKA) begründet sich bei Ermittlungen in Fällen der Cyberkriminalität im engeren Sinn (strafrechtliche Handlungen gegen staatliche Institutionen und Einrichtungen oder herausragende Personen des öffentlichen Lebens) und beispielsweise bei neu auftretenden Modi Operandi, insbesondere dann, wenn durch die Straftaten Schäden in erheblichem Ausmaß bei einer Vielzahl von Personen oder mittleren und größeren Wirtschaftsunternehmen bereits eingetreten oder zu erwarten sind. In Einzelfällen wird die Bearbeitungszuständigkeit zwischen dem LKA bzw. der jeweilig zuständigen Polizeidirektion abgestimmt.

Die Bereiche der Informations- und Kommunikationstechnik (IuK)-Forensik werden im LKA und in den drei Polizeidirektionen, organisatorisch getrennt von den Ermittlungsbereichen, vorgehalten.

Wie zuvor bereits erwähnt, wurde zur Bekämpfung der Cyberkriminalität am 1. Juni 2012 im LKA das 4C eingerichtet. Es besteht aus den Bereichen IuK-Forensik (EDV-Beweissicherung und -auswertung, Sachverständige für Kryptologie, Mobilgeräteforensik, forensische IuK), IuK-Ermittlungsunterstützung (Telekommunikationsüberwachung, Technische Einsatzgruppe, IT-Ermittlungsunterstützung) sowie Cybercrime-Ermittlungen mit der Auswertungs- und Koordinierungsstelle Kinder- und Jugendpornografie.

Thüringen

Auf allen Ebenen ist spezialisiertes Personal eingesetzt. Die zentrale Präventionsstelle des Landes liegt in der Zuständigkeit der Landespolizeidirektion, SG 12/Kriminalitätsbekämpfung. In jeder Landespolizeiinspektion steht eine kriminalpolizeiliche Beratungsstelle, in jeder Dienststelle zwei Mitarbeiter Prävention zur Verfügung.

Sowohl das Bundeskriminalamt (BKA) (Gruppe SO4) als auch die 16 Landeskriminalämter (LKÄ) der Bundesländer verfügen über Spezialdienststellen zur Bekämpfung der Cyberkriminalität oder sind in der konkreten Vorbereitung zur Einrichtung solcher Dienststellen. Die Strukturen der einzelnen Dienststellen sind aufgrund der föderalen Struktur Deutschlands sehr heterogen. Darüber hinaus werden forensischen Spezialdienststellen unterhalten, die bei der Beweissicherung und -auswertung hinzugezogen werden. Jede Kriminalpolizeiliche Dienstelle hat eine IT-Beweisauswerteeinrichtung.
Im Hinblick auf die Bundesländer wurden – ohne Anspruch auf Vollständigkeit – folgende Informationen gemeldet:

Baden-Württemberg:

In Baden-Württemberg wurden, um die Strafverfolgung im Bereich Cyberkriminalität zu verstärken, zum Jahresbeginn 2012 bestehende Inspektionen des Landeskriminalamt Baden-Württemberg (LKA BW) zu einer neuen Abteilung Cybercrime und Digitale Spuren zusammengeführt. Diese Abteilung wurde in den folgenden Jahren personell verstärkt und hat derzeit einen Personalstamm von 98 Mitarbeiterinnen und Mitarbeitern.

Im Rahmen der Polizeireform wurden außerdem die Kriminalinspektionen 5 bei den regionalen Polizeipräsidien eingerichtet. Sie nehmen spiegelbildlich die Aufgaben der Abteilung 5 des LKA BW wahr. Ausnahmen hiervon sind landesweite Servicedienstleistungen wie der Betrieb des Telekommunikationsüberwachungs-Zentrums, die Mobilfunkaufklärung oder die Netzwerkforensik sowie die Internetrecherche und die Ansprechstelle Kinderpornografie. Diese Aufgaben werden ausschließlich im LKA BW wahrgenommen.

Neben dem Aufgabenbereich "Ermittlungen" sind sowohl im LKA BW als auch in den örtlichen Kriminalinspektionen speziell ausgebildete Mitarbeiter mit Aufgaben im Bereich IT-Forensik betraut. Mit Einführung einer Sonderlaufbahn Cyberkriminalist im Jahr 2014 (Einstellung von studierten Informatikern/Ingenieuren und anschließender verkürzter Polizeiausbildung) soll die Kompetenz weiter gesteigert werden.

Berlin

Die forensische Untersuchung von digitalen Beweismitteln ist Aufgabe des Landeskriminalamtes Berlin (LKA 75). Ein Teil der dort beschäftigten Mitarbeiter verfügt über eine (abgeschlossene) Ausbildung zum Sachverständigen. Die anderen Mitarbeiter verfügen ebenfalls über einen großen Sachverstand. Zudem sind in dieser Dienststelle mehrere Informatiker beschäftigt. LKA 72 u. a. "Zentralstelle Internet" verfügt ebenfalls über eine Reihe sehr sach- und fachkundiger Mitarbeiter. Auch sie "untersuchen" im weitgefassten Wortsinn Cyberkriminalität. Ihnen obliegt u. a. die Aufgabe der Netzwerkforensik. Einzelne Mitarbeiter von LKA 33 untersuchen in ausgesuchten Fällen sichergestellte Beweismittel bzw. nehmen Datensicherungen und Auswertungen nach forensischen Grundsätzen vor. Diese führen auch Ermittlungsverfahren.

Brandenburg

Die Bekämpfung des Phänomens "Cybercrime" ist innerhalb des Polizeipräsidiums Brandenburg dreistufig strukturiert. Darüber hinaus ist die Bekämpfung des Kriminalitätsphänomens "Cybercrime" Aufgabe von jedem Polizeibediensteten im Sinne eines "Ersteinschreiters". Um den wachsenden Herausforderungen der Bekämpfung von Cyberkriminalität auch zukünftig ausreichend begegnen zu können, stellte die Brandenburger Polizei IT-Fachpersonal ein und bietet diesen – je nach Qualifikation – gesonderte Entwicklungs- und Karrieremöglichkeiten.

Mecklenburg-Vorpommern

Das Dezernat 55 "Forensische IuK und Spezialfotografie" des Landeskriminalamtes MV ist Phänomen übergreifend für die forensischen Untersuchungen von digitalen Beweismitteln zuständig. Im Dezernat 45 ist darüber hinaus die deliktsbezogene forensische Untersuchung möglich. Im Dezernat 55 Forensische IuK gibt es entsprechende Dienstposten als Sachverständiger Forensische IuK.

Saarland

Im Saarland ergibt sich die Zuständigkeit für Dezernat Landespolizeipräsidium LPP 222 Cybercrime. Dabei handelt es sich um die Zentralstelle der saarländischen Vollzugspolizei für den Bereich Cybercrime 6 als Ansprechstelle für IT-Ermittlungsunterstützung für die Dienststellen der saarländischen Polizei, zuständig für Ermittlungen in herausragenden Fällen der Cyberkriminalität, aber auch als Zentrale Ansprechstelle Cybercrime für die Wirtschaft und sonstige öffentliche und nichtöffentliche Stellen (ZAC). Als besondere Posten für forensische IT-Untersuchungsbeamte wurden beim Dezernat LPP 222 Cybercrime zwei Informatiker-Stellen sowie bei LPP 4.7 IT-Forensik Posten für IT-Forensik-Sachverständige eingerichtet.

Sachsen

In Sachsen werden in Abhängigkeit von dem Ziel der Untersuchung, von der Auftragslage der zuständigen Staatsanwaltschaft und von der zeitlichen Umsetzung (forensische) Untersuchungen im Bereich Cyberkriminalität an externe Firmen zur Auswertung bzw. Aufbereitung übergeben. Im Einzelfall werden Untersuchungen direkt im SN4C oder im kriminaltechnischen Institut des Landeskriminalamtes durchgeführt.

Bayern

Auf polizeilicher Seite steht seit 1.Januar 2014 beim Bayerischen Landeskriminalamt (BLKA) mit dem Dezernat 54 eine spezielle Dienststelle zur Untersuchung von Cyberkriminalität zur Verfügung. Sie besteht aus dem Sachgebiet 541 "Zentralstelle Cybercrime – ZAC", dem Sachgebiet 542 mit mehreren Ermittlungskommissionen sowie dem Sachgebiet 543 für die Netzwerkfahndung. Daneben sind spezielle Ermittlungsabteilungen bei den Polizeipräsidien München und Mittelfranken eingerichtet, die alle über spezialisierte Ermittler mit IT-Ausbildung (sog. Cybercops) verfügen. Weiter ist im Sachgebiet 633 "Kompetenzzentrum TKÜ-BY" im BLKA die Umsetzung von Ermittlungsmaßnahmen im Bereich der Telekommunikation (TKÜ, Verkehrsdatenerhebung, IMSI-Catcher usw.) konzentriert.

Zusätzlich bestehen bei allen Flächenpräsidien Arbeitsbereiche zur Cybercrime- Bekämpfung sowie regionale Beweissicherungs- und Auswertungsstellen (RBA) für die Durchführung forensischer Auswertungen und die Koordinierung von TKÜ-Maßnahmen. Daneben besteht mit dem Sachgebiet 210 "Forensische IuK" im BLKA eine weitere Dienststelle für Auswertungen von sichergestellten Unterlagen zur Verfügung.

Hamburg

Die Polizei Hamburg verfügt über eine spezielle Dienststelle, in der sowohl Ermittlungsbeamte als auch Computerforensiker für Untersuchungsaufgaben zusammengezogen worden sind (LKA 54 – Cybercrime). Sowohl im Ermittlungsbereich als auch im Bereich der Forensik sind Polizeivollzugsbeamte parallel zu Angestellten ("Informatikern") tätig.

Thüringen

Die zukünftige Struktur des neu installierten Dezernates 64 im Landeskriminalamt Thüringen (TLKA) wurde bereits unter Punkt 1.3 (Anlage 1) erläutert.

Im Bereich der forensischen IuK in Thüringen existiert in jeder der sieben Landespolizeiinspektionen eine "Regionale Beweissicherungseinheit" (RBE), welche für ihren Zuständigkeitsbereich elektronische Daten sichert, für die Sachbearbeitung aufbereitet und einfache IT-Probleme bearbeitet.

Im TLKA nimmt das Dezernat 43 FIuK diese Aufgaben wahr. Weiterhin gehören zur Arbeit des Dezernates 43 die Koordinierung von Schulungsmaßnahmen, die Erstellung von Gutachten und die Bearbeitung schwierigerer Fälle. Dazu erfolgte eine Spezialisierung im Dezernat 43.

4.3. Sonstige Behörden/Einrichtungen/öffentlich-private Partnerschaften

Verfassungsschutzbehörden des Bundes und der Länder

Die Verfassungsschutzbehörden des Bundes und der Länder nehmen bestimmte, gesetzlich definierte Aufgaben wahr. Die Kernaufgabe besteht darin, bestimmte als "Bestrebungen" bezeichnete Verhaltensweisen zu beobachten. Gegenstand der Beobachtung sind gemäß § 3 Absatz 1 Bundesverfassungsschutzgesetz:

- Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind,
- eine ungesetzliche Beeinträchtigung der Amtsführung der Verfassungsorgane des Bundes oder eines Landes oder ihrer Mitglieder zum Ziel haben,
- sicherheitsgefährdende oder geheimdienstliche Tätigkeiten im Geltungsbereich dieses Gesetzes für eine fremde Macht,
- Bestrebungen im Geltungsbereich des Bundesverfassungsschutzgesetzes, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden, oder
- Bestrebungen, die gegen den Gedanken der Völkerverständigung (Artikel 9 Abs. 2 des Grundgesetzes), insbesondere gegen das friedliche Zusammenleben der Völker gerichtet sind.

Aktivitäten, die keinen derartigen Hintergrund haben, so schädlich sie für den einzelnen, die Gesellschaft oder den Staat auch sind, werden von der gesetzlichen Aufgabenzuweisung nicht erfasst. Die breite Palette der Cyberkriminalität ist daher nur dann für den Verfassungsschutz von Bedeutung, wenn Bestrebungen der beschriebenen Art damit im Zusammenhang stehen. Der Verfassungsschutz verfügt über keine exekutiven Befugnisse. Die Abwehr konkreter Gefahren und die Strafverfolgung liegen somit nicht in seiner Zuständigkeit.

Bundesamt für Sicherheit in der Informationstechnik

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde am 1. Januar 1991 gegründet und gehört zum Geschäftsbereich des Bundesministeriums des Innern. Das BSI ist zuständig für die Sicherung der IT der Bundesverwaltung sowie der Kritischen Infrastrukturen in Deutschland und nimmt darüber hinaus als neutrale Stelle Beratungs-, Warnungs- und Informationsaufgaben zu Fragen zur IT-Sicherheit in der Informationsgesellschaft wahr. Derzeit sind dort ca. 600 Informatiker, Physiker, Mathematiker und andere Mitarbeiter beschäftigt. Weiterer Personalaufwuchs ist geplant. Seinen Hauptsitz hat das BSI in Bonn.

Zu den Aufgaben des BSI gehören nach dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) in der Informationstechnik des Bundes (BSI-Gesetz) unter anderem:

- Schutz der Netze des Bundes, Erkennung und Abwehr von Angriffen auf die Regierungsnetze
- Prüfung, Zertifizierung und Akkreditierung von IT-Produkten und -Dienstleistungen
- Zentrale Stelle für die IT-Sicherheit in der Informationstechnik Kritischer Infrastrukturen
- Warnung vor Schadprogrammen oder Sicherheitslücken in IT-Produkten und -Dienstleistungen
- IT-Sicherheitsberatung für die Bundesverwaltung und andere Zielgruppen
- Information und Sensibilisierung der Bürger für das Thema IT- und Internet-Sicherheit
- Entwicklung einheitlicher und verbindlicher IT-Sicherheitsstandards
- Entwicklung von Kryptosystemen für die IT des Bundes.

Cyber-Abwehrzentrum

Unter der Federführung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bilden das Bundesamt für Verfassungsschutz (BfV), das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), das Bundeskriminalamt (BKA), die Bundespolizei (BPol), das Zollkriminalamt (ZKA), der Bundesnachrichtendienst (BND) und die Bundeswehr das Cyber-Abwehrzentrum (Cyber-AZ).

Alle Behörden arbeiten unter strikter Wahrung ihrer jeweiligen gesetzlichen Aufgaben und Befugnisse kooperativ zusammen. Das Cyber-AZ ist mit den Lagezentren und entsprechenden Einrichtungen der beteiligten Behörden vernetzt, in denen die operative Arbeit geleistet wird.

Im Cyber-AZ werden alle Informationen zu Cyber-Angriffen, die Behörden im Rahmen ihrer Zuständigkeiten eruieren, zusammengeführt. So bewertet das BSI einen Cyber-Angriff aus technischer Sicht, das BfV befasst sich mit der Frage, ob der Angriff möglicherweise von einem ausländischen Nachrichtendienst ausgegangen ist, und das BBK bewertet die Auswirkungen von möglichen Angriffen auf Infrastrukturen. Die darüber hinaus mitwirkenden Behörden fügen ihre Erkenntnisse über neue Angriffswege und Angriffswerkzeuge ein, dadurch liegt innerhalb kürzester Zeit ein aktuelles, umfassendes Lagebild vor.

Die Koordinierung der Bekämpfung der Cyberkriminalität auf polizeilicher Ebene erfolgt bundesweit auf dem Gremienweg der Bund-Länder-Zusammenarbeit, insbesondere durch die AG Kripo und deren nachgeordnete Kommission Kriminalitätsbekämpfung (repressiv) sowie der Kommission Polizeiliche Kriminalprävention (präventiv). Neben den bereits genannten Gremien befasst sich auch die Kommission Staatsschutz (K-ST) im Rahmen einer BLAG "Politisch motivierte Cybercrime" mit diesem Thema.
Darüber hinaus findet zweimal jährlich die Leitertagung "Cybercrime" im Bundeskriminalamt (BKA) statt. Teilnehmer sind die entscheidungsbefugten Dienststellenleiter der Zentralstellen "Cybercrime" der Bundesländer sowie des BKA.

In den Ländern erfolgt die Koordinierung nach den landesrechtlichen Organisationsregelungen.

4.4. Zusammenarbeit und Koordinierung auf nationaler Ebene

4.4.1. Rechtliche oder politische Verpflichtungen

Mit dem am 25. Juli 2015 in Kraft getretenen Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) wurden die IT-Sicherheitsanforderungen an Betreiber kritischer Infrastrukturen verschärft und eine Verpflichtung eingeführt, bestimmte IT-Sicherheitsvorfälle zu melden.

Insbesondere werden den Betreibern bei Sicherheitsvorfällen, die IT einer Kritischen Infrastruktur betreffen, Meldepflichten auferlegt. Diese Meldepflichten sollen unter anderem im Falle eines Angriffs die schnellere Erstellung eines vollständigen Lagebildes und die schnellere Ergreifung gezielterer Gegenmaßnahmen ermöglichen.

Die abschließende Bestimmung derjenigen Anlagen, Einrichtungen oder Teile hiervon, die eine Kritische Infrastruktur im Sinne dieses Gesetzes sind, soll nach Artikel 1 Nummer 2 des IT-Sicherheitsgesetzes durch Rechtverordnung erfolgen.

Soweit die Betreiber Kritischer Infrastrukturen bereits Spezialgesetzen wie dem Gesetz über die Elektrizitäts- und Gasversorgung (EnWG) oder dem Gesetz über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren (AtG) unterfallen, werden die Pflichten dieser Betreiber dort gesondert geregelt.

Die Meldepflichten von Telekommunikationsdiensteanbietern werden im Einklang mit den neuen Vorschriften für Kritische Infrastrukturen dahingehend erweitert, dass diese der Bundesnetzagentur auch Beeinträchtigungen melden müssen, die zu beträchtlichen Sicherheitsverletzungen führen können. Bisher war eine Meldung lediglich vorgesehen, wenn eine Sicherheitsverletzung bereits eingetreten war. Außerdem wird die Meldepflicht auf Störungen erstreckt, die zu einer Einschränkung der Verfügbarkeit oder zu einem unerlaubten Zugriff auf die Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können. Soweit die gemeldeten Sicherheitsverletzungen die Informationstechnik betreffen, erfolgt nun immer eine Weitergabe der Informationen durch die Bundesnetzagentur an das BSI. Die Erweiterung der Meldepflichten ermöglicht eine bessere und genauere Einschätzung von Angriffen auf Telekommunikationsnetze und -dienste.

Darüber hinaus werden die Telekommunikationsunternehmen verpflichtet, Nutzer zu benachrichtigen, soweit ihnen Störungen bekannt werden, die von Systemen der Nutzer ausgehen. Dies betrifft insbesondere Bot-Netze, die sich auf den Rechnern der Nutzer installiert haben. Die Informationspflicht greift jedoch nur, wenn der Telekommunikationsanbieter den Nutzer bereits kennt.

Die Bewältigung von schweren Cyberangriffen wird durch die IT-Krisenmanagement-Strukturen übernommen.

Das IT-Krisenmanagement in Deutschland findet im Kern im Nationalen IT-Krisenreaktionszentrum (IT-KRZ) beim Bundesamt für Sicherheit in der Informationstechnik (BSI) statt. Das IT-KRZ wächst dabei stufenlos aus dem Nationalen IT-Lagezentrum und Computer Emergency Response Team des Bundes (CERT-Bund) auf. Damit kann lageangemessen durch Heranziehen relevanter Experten und Unterstützungskräfte des BSI über einen skalierbaren Ansatz die sog. "Besondere Lage" bzw. IT-Krise bewältigt werden. Im IT-KRZ werden über ein Stabs-Zellen-Modell, analog zu allgemeinen Krisen- und Katastrophenschutzstäben, alle relevanten Personen zusammengeführt, um organisatorische wie fachliche Aufgaben zu bewältigen. Es finden einsatztaktische/fachliche Aufgaben wie Lageerfassung, -bewertung, Priorisierung und Maßnahmenempfehlungen statt. Fachexperten aus dem gesamten BSI werden lageangemessen eingebunden und sorgen für eine breite fachliche Expertise. Über die Stabszellen wird die Kommunikation mit den Zielgruppen des BSI, z. B. Behörden sowie Unternehmen aus den Kritischen Infrastrukturen, sichergestellt und eine geeignete Koordinierung von Krisenmanagementprozessen durchgeführt.

Pressearbeit und Justiziariat sind ebenso eingebunden wie ggf. Verbindungspersonen zu anderen Behörden, z. B. dem Bundeskriminalamt (BKA), in ihren jeweiligen Aufgabenbereichen. Dies schließt insbesondere Vertreter des Nationalen Cyber-Abwehrzentrums ein, mithilfe derer der Kontakt zu den deutschen Sicherheitsbehörden gehalten wird. Unterstützt wird das IT-KRZ durch die organisatorischen Stabsaufgaben wie Personalmanagement, Logistik und Innerer Dienst.

Sofern neben dem fachlichen Krisenpotential auch eine Ausweitung auf andere Teilgebiete des öffentlichen Lebens bzw. eine politische Komponente hinzukommt, wird der Krisenstab des Bundesministeriums des Innern (BMI) aktiviert. Dieser Stab ist für die allgemeine Bewältigung von Krisen zuständig und damit zusätzlich zu den IT-Krisenaspekten auch noch für weitere möglicherweise davon in Folge von Interdependenzen betroffene Teilbereiche des öffentlichen Lebens, z. B. im Sinne des Bevölkerungsschutzes (Versorgungssicherheit) oder der Terrorabwehr (Täterermittlung). Für das IT-bezogene ministerielle Krisenmanagement ist innerhalb des BMI-Krisenstabes ein eigener Stabsbereich zuständig. Dieser bereitet die IT-Lage, die im IT-Krisenreaktionszentrum des BSI erarbeitet und erstellt wird, ministeriell auf und stellt diese im BMI-Krisenstab dar. Der Stabsbereich dient in seiner grundsätzlichen Ausrichtung als Schnittstelle zwischen dem allgemeinen, strategisch-administrativen Stab im BMI und dem operativ-taktischen (Stab/) IT- KRZ im BSI.

Zur Vervollständigung des Lagebildes ist dabei der Austausch zwischen IT-Lagezentrum des BSI, dem BMI-Lagezentrum und dem Gemeinsamen Melde- und Lagezentrum des Bundes und der Länder (GMLZ) selbstverständlich. Weitere Lagezentren werden lageabhängig eingebunden.

Vor allem durch das IT-KRZ findet zudem eine Kommunikation und Kooperation mit Fachcommunities im nationalen wie im internationalen Bereich statt. Weltweit haben sich CERT-Verbünde gebildet, deren Ziel die Zusammenarbeit bei IT-Vorfällen ist, einschließlich der gegenseitigen Unterstützung bei der Bewältigung von IT-Lagen. CERT-Verbünde sind mit teils homogener Ausrichtung, z. B. Regierungs-/Behörden-CERTs, vorhanden, teils mit sehr heterogener Zusammenstellung, z. B. mit Teams aus Wirtschaft, Wissenschaft und Behörden.

Die unterschiedliche Ausrichtung der Teams und ihrer teils multidisziplinären Zusammenstellung ist explizit als Vorteil zu verstehen, um auf breite Expertise zurückgreifen zu können. Durch die Internationalität wird dies noch unterstützt. Neben dem Tagesgeschäft dienen diese Verbünde auch dem IT-Krisenmanagement, was in diesen Kreisen regelmäßig geübt wird.

Die zivil-militärische Zusammenarbeit im Bereich der IT-Vorfallsbearbeitung und bei CERT-Aufgaben wird auf nationaler Ebene zwischen dem BSI und der Bundeswehr seit Jahren erfolgreich praktiziert. Das BSI ist bei der NATO als National Cyber-Defence Authority gelistet und im Fall eines größeren Cyberangriffs mit staatlichem Hintergrund primäre Kontaktstelle für Deutschland. Das CERT-Bundeswehr ist auf den Schutz der eigenen militärischen Netze ausgerichtet und arbeitet dazu mit den anderen internationalen militärischen CERTs zusammen.

Das IT-KRZ verfügt über langjährig etablierte und geübte Krisenmanagementkanäle in die öffentliche Verwaltung, insbesondere die Bundesverwaltung, und zu den deutschen Unternehmen der Kritischen Infrastrukturen. Über diverse Mechanismen und Kooperationen des BSI kann ein breites Spektrum und das Gros der deutschen Wirtschaft aber auch der Bürger erreicht werden.

Im Bereich Online-Kartenbetrug erfolgt die Zusammenarbeit des Bundeskriminalamtes (BKA) mit der Privatwirtschaft auf vielfältige Art und Weise. Beispielhaft sind hier die Zusammenarbeit mit dem Arbeitskreis Sicherheit "Debit- und Kreditkarten in Deutschland" und die Nationale Kooperationsstelle Cybercrime, insbesondere die "institutionalized Public-Private-Partnership" (**iPPP**) zu nennen. Im Zusammenhang mit der Erhöhung der Sicherheit beim Zahlungskarteneinsatz erfolgt eine Kooperation mit Wirtschaftsunternehmen in den Bereichen Verhinderung der Manipulation von POS-Terminals und Geldausgabeautomaten sowie im Zusammenhang mit dem Wechsel von Magnetstreifen- auf Chiptechnologie.

Daneben arbeiten auch die Strafverfolgungsbehörden der Länder zur Bekämpfung und Aufklärung von Straftaten des Online-Kartenbetrugs mit Unternehmen, insbesondere mit Banken, auf vielfältige Art und Weise zusammen. Beispielhaft – ohne Anspruch auf Vollständigkeit – wird die Zusammenarbeit der Strafverfolgungsbehörden mit Unternehmen in den Ländern Brandenburg und Sachsen-Anhalt geschildert:

Im Bundesland **Brandenburg** wurde bei dem Polizeipräsidium Fachdirektion Landeskriminalamt (FD LKA) die Zentrale Ansprechstelle Cybercrime für Unternehmen, Einrichtungen und Bürger eingerichtet. Sie ist zugleich Single Point of Contact (SPoC).

Die FD LKA nimmt u. a. regelmäßig an Veranstaltungen der Industrie- und Handelskammern des Landes Brandenburg teil, um auf diesem Wege Erkenntnisse zu polizeilich bekannt gewordenen Cybercrime-Phänomenen mitzuteilen, Kontakte zu Partnern aus der Wirtschaft und IT-Branche zu knüpfen bzw. Erfahrungen zur IT-Sicherheit in Unternehmen auszutauschen.

Im Bundesland **Sachsen-Anhalt** arbeitet die Polizei im Rahmen der Ermittlungen bei der Bekämpfung von Straftaten in diesem Deliktsfeld eng mit der Firma EURO-Kartensysteme GmbH als Gemeinschaftsunternehmen (Service- und Kompetenzzentrum) im Bereich des kartengestützten Zahlungsverkehrs der deutschen Kreditwirtschaft zusammen. Anfragen werden aber auch an die einzelnen Kreditkartenunternehmen gerichtet. Eine Beantwortung seitens der Kreditkartenunternehmen erfolgt jedoch nicht in jedem Fall.

Einmal jährlich führt der Arbeitskreis Sicherheit der Kartenorganisationen in Deutschland eine praxisbezogene Fachtagung zum Thema Zahlungskartenkriminalität durch, bei der zeitnah neue Modi Operandi und Sicherheitsstrategien vermittelt werden. Zum Teilnehmerkreis gehören neben Ermittlungsbeamten der Fachdienststellen der Kriminalpolizei der Länder und des BKA auch Vertreter der Kartenindustrie sowie Sicherheitsunternehmen. Des Weiteren findet quartalsweise auf freiwilliger Basis mit dem o. g. Teilnehmerkreis ein Stammtisch zum Zwecke des Informationsaustausches statt.

Seitens der Polizei und den Vertretern der Kartenindustrie sowie den Geldautomaten-/Terminalherstellern besteht ein intensiver Informationsaustausch. Speziell ausgebildete oder geschulte Mitarbeiter der Kreditkarteninstitute entwickeln eigene Sicherheitskonzepte. Sie arbeiten eng mit der Polizei zusammen und sind für die Polizeibehörden jederzeit ansprechbar. Die Öffentlichkeit wird seitens der Polizei mit entsprechendem Präventionsmaterial sensibilisiert. Beispielsweise soll durch die Veröffentlichung von Kurzfilmen das Sicherheitsbewusstsein verstärkt werden. Auf Anfragen führen Polizeibeamte Schulungen in Geldinstituten durch. Die europaweite Einführung der EMV-Chiptechnologie sowie die grundsätzliche Deaktivierung der Magnetstreifen auf Debitkarten seitens der Geldinstitute erhöhten die Sicherheit im Zusammenhang mit Skimmingangriffen auf deutsche Geldautomaten enorm. Dadurch werden die Einsatzmöglichkeiten gefälschter Karten zunehmend erschwert.

Auf die Genehmigung von Online-Transaktionen haben die Strafverfolgungsbehörden keinen Einfluss. Auch hier wird im Rahmen der Prävention auf den sensiblen Umgang beim Bezahlen im Internet hingewiesen. Grundsätzlich verhalten sich die Banken bei der Anzeigenerstattung relativ restriktiv, zumal die Schäden durch die missbräuchliche Verwendung von Kartendaten nur einen Bruchteil des Gesamtumsatzes ausmachen.

Es besteht eine Verpflichtung zur Herausgabe von Beweismitteln nach Maßgabe der Strafprozessordnung. Die Unterstützung und Verbesserung der Zusammenarbeit mit der Privatwirtschaft werden durch Schaffung einer entsprechenden institutionalisierten Zusammenarbeit der Privatwirtschaft mit der öffentlichen Verwaltung/Strafverfolgung (z. B. zwischen BKA/BSI und verschiedenen Einrichtungen aus dem Privatsektor im sogenannten "German Competence Centre against Cybercrime e.V." (G4C)) realisiert. Vergleichbare Bestrebungen sind aufgrund des föderalen Aufbaus der Polizei in Deutschland auch in den Bundesländern feststellbar. Deutschland hat die Vorgaben der e-Commerce-Richtlinie zur Verantwortlichkeit von Internet-Diensteanbietern in den §§ 7 bis 10 des Telemediengesetzes (TMG) umgesetzt. Grundsätzlich ist zunächst der jeweilige Content-Provider, der Inhalte im Internet verfügbar macht, für seine eigenen Inhalte strafrechtlich verantwortlich. Nach den §§ 7 bis 10 TMG sind Anbieter von Telemediendiensten grundsätzlich für fremde Informationen, die sie für ihre Nutzer übermitteln oder speichern, nicht verantwortlich und auch nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen anlasslos zu überwachen oder nach Anhaltspunkten für rechtswidrige Tätigkeiten zu überprüfen. Dabei sieht § 10 TMG vor, dass Host-Provider, die fremde Informationen für ihre Nutzer speichern, für diese Informationen nicht verantwortlich sind, sofern sie

- keine Kenntnis von einer rechtswidrigen Handlung oder Information haben oder
- unverzüglich tätig werden, um rechtswidrige Inhalte zu entfernen oder zu sperren, sobald sie hiervon Kenntnis erlangt haben.

Weisungen der Polizei (in der Regel Zuständigkeit der Landespolizei) kommen die Diensteanbieter in der Regel mit dem entsprechenden Entfernen der Inhalte umgehend nach. Ergreift ein Host-Provider keine entsprechenden Maßnahmen, bestimmt sich seine Verantwortlichkeit für die jeweiligen rechtswidrigen Inhalte nach den allgemeinen Vorschriften. Eine unmittelbare strafrechtliche Verantwortlichkeit von Internet-Providern ergibt sich aus den Vorschriften des TMG jedoch nicht.

4.4.2. Mittel für die Verbesserung der Zusammenarbeit

Von den meisten Ländern wurde die technische und personelle Ausstattung der Strafverfolgungsbehörden als zufriedenstellend empfunden. Schwierigkeiten bestehen hier vor allem bei der Auswertung von Datenträgern mit großen Datenmengen. In vielen Verfahren werden inzwischen auf Rechnern von Beschuldigten Daten im Bereich von Terabyte sichergestellt. Die hier notwendige Auswertung ist einerseits technisch sehr aufwändig und benötigt andererseits häufig eine längere Zeit, sodass es hier zu Verzögerungen im Verfahrensabschluss kommen kann.

Das entsprechende Fachwissen wird Staatsanwälten und Richtern im Rahmen zahlreicher Fortbildungsveranstaltungen vermittelt.

Für die Ausbildung im Bereich Cyberkriminalität stehen derzeit im Bundeskriminalamt ca. 200 000 EUR pro Jahr zur Verfügung. Diese Kosten setzen sich aus Dozentenhonoraren, Reisekosten und der Beschaffung von Hard- und Software zusammen.

Die Tagungsstätte der Deutschen Richterakademie in Trier wendete 2014 allein 151 844 EUR zur Bezahlung der Referentenhonorare auf; hinsichtlich der Tagungsstätte der Deutschen Richterakademie in Wustrau betrugen die Ausgaben allein für die Referentenhonorare im Jahr 2014 178 591 EUR.

Im Hinblick auf die Bundesländer wurden – ohne Anspruch auf Vollständigkeit – folgende Informationen gemeldet:

Baden-Württemberg:

etwa 20 000 EUR pro Jahr aus Fortbildungsmitteln des Justizhaushalts für Schulungen der Staatsanwältinnen und Staatsanwälte.

Brandenburg:

ca. 7 000 EUR - 10 000 EUR.

Saarland:

etwa 20 000 EUR.

Sachsen-Anhalt:

ca. 40 000 EUR.

Bayern:

ca. 10 000 EUR.

Bremen:

ca. 10 000 EUR Jahr.

Hamburg:

Die externen Schulungskosten werden auf ca. 15 000 EUR pro Jahr geschätzt. Das Gesamtbudget beträgt im Schnitt rund 180 000 EUR pro Jahr.

Hessen:

Für die von der Hessischen Justizakademie ausgerichteten Tagungen werden jährlich ca. 15 000 EUR aufgewendet.

Niedersachsen:

etwa 10 000 EUR (staatsanwaltschaftlichen Ausbildungsangebote).

Rheinland-Pfalz:

im Jahr ca. 10 000 EUR (für Fortbildungsmaßnahmen auf polizeilicher Ebene).

Thüringen:

2013 ca. 20 000 EUR und 2014 ca. 36 000 EUR.

4.5. Fazit

- **Deutschland hat mit 16 Bundesländern eine föderale Struktur. Nach der durch das Grundgesetz vorgesehenen Kompetenzverteilung zwischen Bund und Ländern ist die Ausübung staatlicher Befugnisse und die Erfüllung staatlicher Aufgaben Sache der Länder, soweit das Grundgesetz keine andere Regelung trifft oder zulässt. Diesem Grundsatz entsprechend obliegt die Strafverfolgung grundsätzlich den Strafverfolgungsbehörden der Länder, namentlich den Staatsanwaltschaften und ihren Ermittlungspersonen. In besonders geregelten Fällen (z. B. Staatsschutz) bestehen Zuständigkeiten des Generalbundesanwaltes und des Bundeskriminalamtes.**

- **Es gibt verschiedene nationale Strukturen, die für die Verhütung, Auswertung und Bekämpfung von Cyberkriminalität zuständig sind: Staatsanwaltschaften der Länder, Polizei auf Bundes- und Länderebene, die Ämter für Verfassungsschutz auf Bundes- und Länderebene, das Zollkriminalamt und das Bundesamt für Sicherheit in der Informationstechnik.**

- **Die meisten Bundesländer verfügen entweder über auf die Bekämpfung der Cyberkriminalität spezialisierte Staatsanwälte oder haben in den Staatsanwaltschaften eigens hierzu Abteilungen eingerichtet oder Kontaktpersonen benannt.**

- **Was die Polizeibehörden anbelangt, so hat die Mehrheit der Länder bei den jeweiligen Landeskriminalämtern Sonderdezernate zur Bekämpfung von Cyberkriminalität eingerichtet. Die Sonderdezernate verfügen über Personal mit fundierten IT-Kenntnissen und spezieller informationstechnischer Sachkunde. Im Bundeskriminalamt besteht außerdem eine für Cyberkriminalität zuständige Organisationseinheit (Gruppe SO4).**

- **Es gibt ferner unter der Federführung des BSI ein bundesweites Cyber-Abwehrzentrum (Cyber-AZ), das aus verschiedenen Behörden besteht, die für Cyber-Abwehr zuständig sind. Es koordiniert die Abwehr von Cyber-Angriffen, wobei der Schwerpunkt auf Angriffen gegen Infrastrukturen liegt, und leistet außerdem operative Arbeit.**

- **Die Koordinierung der Bekämpfung von Cyberkriminalität erfolgt durch die für Cyberkriminalität zuständige Abteilung des Bundeskriminalamts, die Landeskriminalämter, die Bundespolizei und weitere Gremien wie die Kommission Kriminalitätsbekämpfung, die Kommission Polizeiliche Kriminalprävention und die Kommission Staatsschutz.**

- **Auf Bundesebene gibt es eine "institutionalized Public-Private-Partnership" (iPPP) im Bereich Cyberkriminalität mit der Bezeichnung "German Competence Centre against Cyber Crime" (G4C). Darüber hinaus haben die Strafverfolgungsbehörden bei der Bekämpfung von Straftaten des Online-Kartenbetrugs sehr gute Beziehungen zum Finanzsektor. Der Gutachterausschuss ist der Auffassung, dass die Zusammenarbeit und die Koordinierung auf Bundesebene gut verlaufen.**

- **Die Polizei hat ihre eigene Cyber-Abwehrstrategie eingeführt und Kontaktstellen für die Wirtschaft im Falle von Cyberkriminalität, einen Koordinierungsmechanismus und eine einheitliche Anlaufstelle für den Informationsaustausch eingerichtet. Ferner gibt es eine Kooperationsplattform mit der Wirtschaft. Die Strategie umfasst 11 Maßnahmenbereiche einschließlich Maßnahmen, die von privaten Akteuren zu treffen sind.**

- **Einige Praktiker haben dem Gutachterausschuss erläutert, dass die Aufteilung der Zuständigkeiten zwischen den Sonderstellen für die Bekämpfung der Cyberkriminalität von Fall zu Fall nach informeller Absprache zwischen den Verfolgungsdiensten erfolgt. Dabei wird auch der Rechtskategorie der Straftat Rechnung getragen; im Falle einer schweren Straftat liegt die Zuständigkeit für die Ermittlungen bei den Behörden für die Bekämpfung schwerer Cyberkriminalität.**

- **Dem Bundeskriminalamt stehen jedes Jahr Finanzmittel für Schulungen im Bereich Cyberkriminalität zur Verfügung und einige Länder berichteten, dass sie ebenfalls über zugewiesene Finanzmittel für Schulungszwecke verfügen.**

5. RECHTLICHE ASPEKTE

5.1. Materielles Strafrecht im Bereich Cyberkriminalität

5.1.1. Übereinkommen des Europarats über Computerkriminalität

Deutschland hat das Übereinkommen am 23. November 2001 unterzeichnet und am 9. März 2009 ratifiziert. Es ist in Deutschland am 1. Juli 2009 in Kraft getreten.

5.1.2. Beschreibung der nationalen Rechtsvorschriften

A/ Rahmenbeschluss 2005/222/JI des Rates über Angriffe auf Informationssysteme und Richtlinie 2013/40/EU über Angriffe auf Informationssysteme

Straftaten, die nur über Informationssysteme möglich sind, insbesondere solche, die mit Cyber-Angriffen zusammenhängen: §§ 202a, 202b, 202c, 202d, 303a, 303b des Strafgesetzbuches (StGB).

– Nach § 202a StGB macht sich strafbar, wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft. Dies wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

– In § 202a Absatz 2 StGB werden Daten als solche definiert, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

– Gemäß § 202b StGB macht sich strafbar, wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft. Dies ist mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bedroht.

– Nach § 202c StGB macht sich strafbar, wer eine Straftat nach § 202a oder § 202b StGB vorbereitet, indem er Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten ermöglichen, oder Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder zugänglich macht. Dies wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

– Gemäß § 202d StGB macht sich strafbar, wer Daten, die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen. Dies ist mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bedroht, wobei die Strafe aber nicht schwerer sein darf, als die für die Vortat angedrohte Strafe (§ 202d Absatz 2 StGB). Für Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen, ist eine Ausnahme vorgesehen.

– Gemäß § 303a StGB wird bestraft, wer Daten löscht, unterdrückt, unbrauchbar macht oder verändert. Dies ist mit Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe bedroht.

– Nach § 303b StGB wird bestraft, wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er eine Tat nach § 303a Absatz 1 StGB begeht, Daten in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert. Dies ist mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bedroht.

– Strafbar ist bei allen Delikten nur das vorsätzliche Handeln, § 15 StGB.

– Erschwerende/mildernde Umstände: Handelt es sich bei § 303b StGB um eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist (§ 303b Absatz 2 StGB), ist die Tat mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bedroht. In besonders schweren Fällen können Freiheitsstrafen von sechs Monaten bis zu zehn Jahren verhängt werden. Ein besonders schwerer Fall (§ 303b Absatz 4 StGB) liegt beispielsweise vor, wenn der Täter einen Vermögensverlust großen Ausmaßes herbeiführt, wenn der Täter gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat, oder wenn durch die Tat die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt wird.

– Wiederholungstaten: Dies ist ein Gesichtspunkt der Strafzumessung (§ 46 StGB). Handelt der Täter gewerbsmäßig, so liegt ein besonders schwerer Fall nach § 303b Absatz 4 StGB vor. Gewerbsmäßig handelt, wer sich aus wiederholter Tatbegehung eine nicht nur vorübergehende, nicht ganz unerhebliche Einnahmequelle verschaffen will.

– Der Versuch ist in den Fällen von §§ 303a, 303b StGB strafbar (vgl. § 303a Abs.2 StGB, § 303b Absatz 3 StGB). Nach § 202c StGB ist in den Fällen von §§ 202a und 202b, § 303a Absätze 1 und 2 sowie § 303b Absätze 1 und 5 StGB die Vorbereitung unter Strafe gestellt.

– Anstiftung und Beihilfe sind unter den Voraussetzungen von §§ 26, 27 StGB strafbar.

Straftaten, bei denen Computer und Informationssysteme entweder Hauptinstrument oder Hauptziel sind: §§ 263a, 269, 270 StGB

– Der Computerbetrug nach § 263a StGB ist mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bedroht. Eine Straftat nach § 263a StGB liegt vor, wenn der Täter, in der Absicht sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, dass er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten oder sonst durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflusst.

– Gemäß § 269 StGB wird mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft, wer zur Täuschung im Rechtsverkehr beweiserhebliche Daten so speichert oder verändert, dass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder derart gespeicherte oder veränderte Daten gebraucht.

– Die Taten müssen vorsätzlich begangen worden sein. Die fahrlässige Begehungsweise steht nicht unter Strafe.

– Erschwerende/mildernde Umstände: Ein besonders schwerer Fall des Computerbetrugs nach § 263a Absatz 2 in Verbindung mit § 263 Absatz 3 Satz 2 StGB liegt vor, wenn der Täter den Betrug gewerbsmäßig oder als Mitglied einer Bande begangen hat, ein Vermögensverlust großen Ausmaßes herbeigeführt wurde oder der Täter in der Absicht gehandelt hat, durch fortgesetzte Begehung von Betrug eine große Zahl von Menschen in die Gefahr des Verlustes von Vermögenswerten zu bringen, eine Person in wirtschaftliche Not gebracht wurde, der Täter seine Befugnisse oder seine Stellung als Amtsträger missbraucht oder einen Versicherungsfall vorgetäuscht hat, nachdem er oder ein anderer zu diesem Zweck eine Sache von bedeutendem Wert in Brand gesetzt oder ein Schiff zum Sinken gebracht hat. Mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren, in minder schweren Fällen mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren wird bestraft, wer die Straftat als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Straftaten nach den §§ 263 bis 264 oder 267 bis 269 verbunden hat, gewerbsmäßig begeht. In den gleichen Fällen liegen besonders schwere Fälle vor für die Fälschung beweiserheblicher Daten gemäß § 269 Absatz 3 in Verbindung mit § 267 Absatz 3 StGB. Für besonders schwere Fälle sieht das Gesetz eine Freiheitsstrafe von 6 Monaten bis zu 10 Jahren vor.

– Wiederholungstaten: Dies ist ein Gesichtspunkt der Strafzumessung (§ 46 StGB). Nach § 263a Absatz 2 StGB in Verbindung mit § 263 Absätze 3 bis 5 StGB sowie § 269Absatz 3 in Verbindung mit § 267 Absätze 3 und 4 StGB liegt ein besonders schwerer Fall vor, wenn der Täter gewerbsmäßig handelt. Gewerbsmäßig handelt, wer sich aus wiederholter Tatbegehung eine nicht nur vorübergehende, nicht ganz unerhebliche Einnahmequelle verschaffen will.

– Der Versuch ist strafbar: § 263a Absatz 2 StGB in Verbindung mit § 263 Absatz 2 StGB, § 269 Absatz 2 StGB. Mit einer Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird nach § 263a Absatz 3 StGB bestraft, wer einen Computerbetrug vorbereitet, indem er Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überlässt.

– Anstiftung und Beihilfe sind unter den Voraussetzungen von §§ 26, 27 StGB strafbar.

Anleitung zur Begehung einer schweren staatsgefährdenden Gewalttat (§ 91 StGB)

– Nach § 91 Absatz 1 StGB ("Anleitung zur Begehung einer schweren staatsgefährdenden Gewalttat") macht sich strafbar, "wer 1. eine Schrift (§ 11 Absatz 3), die nach ihrem Inhalt geeignet ist, als Anleitung zu einer schweren staatsgefährdenden Gewalttat (§ 89a Absatz 1) zu dienen, anpreist oder einer anderen Person zugänglich macht, wenn die Umstände ihrer Verbreitung geeignet sind, die Bereitschaft anderer zu fördern oder zu wecken, eine schwere staatsgefährdende Gewalttat zu begehen, 2. sich eine Schrift der in Nummer 1 bezeichneten Art verschafft, um eine schwere staatsgefährdende Gewalttat zu begehen". Den "Schriften" stehen nach § 11 Absatz 3 StGB Ton- und Bildträger, Datenspeicher, Abbildungen und andere Darstellungen gleich.

– Das Strafmaß des § 91 StGB ist Freiheitsstrafe bis zu drei Jahren oder Geldstrafe. Bei geringer Schuld kann von Strafe abgesehen werden (§ 91 Absatz 3 StGB).

– Es handelt sich um ein Vorsatzdelikt (§ 15 StGB).

– Der Versuch ist nicht strafbar (§ 23 Absatz 1 StGB).

– Die Strafbarkeit von Anstiftung und Beihilfe richtet sich nach den allgemeinen Vorschriften (§§ 26, 27 StGB).

Die oben genannten Straftaten können nur von natürlichen Personen begangen werden. Gegen Verbände (juristische Personen und Personengesellschaften) kann eine Geldbuße von bis zu zehn Millionen Euro festgesetzt werden, wenn eine Leitungsperson eine unternehmensbezogene Straftat oder Ordnungswidrigkeit begangen hat (§§ 30, 130 OWiG). Das Höchstmaß der Verbandsgeldbuße für Straftaten und Aufsichtspflichtverletzungen (die zu einer Straftat führen) wurde 2013 von einer Million auf bis zu zehn Millionen Euro angehoben (§§ 30 Absatz 2 Satz 1, 130 Absatz 3 Satz 3 OWiG). Diese Höchstgrenze kann überschritten werden, wenn sie zur Abschöpfung des aus der Tat erlangten wirtschaftlichen Vorteils nicht ausreicht (§§ 30 Absatz 3, 17 Absatz 4 OWiG).

Kriterien wie zum Beispiel die Schadenshöhe werden auch im Rahmen der Strafzumessung nach § 46 StGB berücksichtigt.

Leichte Fälle können von den Staatsanwaltschaften nach §§ 153 Absatz 1, 153 a Strafprozessordnung (StPO) eingestellt werden. Im Falle des § 153a Absatz 1 StPO muss der Täter eine Auflage erfüllen, bevor das Verfahren endgültig eingestellt wird.

Pläne für konkrete Gesetzgebungsmaßnahmen zur Cyberkriminalität liegen derzeit nicht vor.

Es gibt Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV). Diese Richtlinien sind vornehmlich für den Staatsanwalt bestimmt. Einige Hinweise wenden sich aber auch an den Richter. Nach Nummer 208 RiStBV hat der Staatsanwalt bei Verfahren betreffend staatsgefährdende Schriften das Bundeskriminalamt (BKA) zu benachrichtigen. Das BKA gibt nach Nummer 224 RiStBV Auskunft darüber, ob eine Schrift (§ 11 Absatz 3 StGB) bereits Gegenstand eines Strafverfahrens nach §§184, 184a, 184b, 184c StGB gewesen ist. Um voneinander abweichende Entscheidungen zu verhindern, sind bei pornografischen Schriften bei den Ermittlungen Grundsätze nach Nummer 224 Absatz 2 RiStBV zu beachten. Stellt ein Gericht in einer rechtskräftigen Entscheidung fest, dass eine Schrift einen der in §§ 184, 184a und 184b StGB bezeichneten Inhalt hat, so übersendet nach Nummer 228 RiStBV die Zentralstelle eine Ausfertigung dieser Entscheidung der Bundesprüfstelle für jugendgefährdende Medien zur Aufnahme der Schrift in die Liste der jugendgefährdenden Medien nach § 18 Absatz 5 Jugendschutzgesetz (JuSchG).

Durch das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) wurde das BKA für alle Straftaten nach §§ 202a, 202b, 202c, 263a, 303a und 303b des Strafgesetzbuches (StGB), die sich gegen Behörden richten, zuständig. Die Staatsanwaltschaft kann die Ermittlungen auf eine andere Behörde übertragen (vgl. § 4 Gesetz über das BKA und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKAG)). Nummer 30 Absatz 1 RiStBV regelt hierzu, dass der Staatsanwalt, dem ein Sachverhalt bekannt wird, der den Verdacht einer der in § 4 Absatz 1 Satz 1 BKAG bezeichneten Straftaten begründet, unverzüglich, erforderlichenfalls fernschriftlich oder fernmündlich, das BKA und das Landeskriminalamt unterrichtet.

Verfassungsfeindliche Sabotage (§ 88 Absatz 1 Nummer 2 StGB)

– In Hinblick auf "Straftaten, die nur über Informationssysteme möglich sind, insbesondere solche, die mit Cyberangriffen zusammenhängen" (Kategorie 1 der Anlage 2 des Fragebogens) kommt § 88 Absatz 1 Nummer 2 StGB ("Verfassungsfeindliche Sabotage") in Betracht. Demnach macht sich strafbar, "[w]er als Rädelsführer oder Hintermann einer Gruppe oder, ohne mit einer Gruppe oder für eine solche zu handeln, als einzelner absichtlich bewirkt, dass im räumlichen Geltungsbereich dieses Gesetzes durch Störhandlungen […] Telekommunikationsanlagen, die öffentlichen Zwecken dienen, […] ganz oder zum Teil außer Tätigkeit gesetzt oder den bestimmungsmäßigen Zwecken entzogen werden, und sich dadurch absichtlich für Bestrebungen gegen den Bestand oder die Sicherheit der Bundesrepublik Deutschland oder gegen Verfassungsgrundsätze einsetzt".

– Das Strafmaß ist Freiheitsstrafe bis zu fünf Jahre oder Geldstrafe. Es handelt sich um ein Vorsatzdelikt, § 15 StGB.

– Der Versuch ist strafbar (§ 88 Absatz 2 StGB).

– Die Strafbarkeit von Anstiftung und Beihilfe richtet sich nach den allgemeinen Vorschriften (§§ 26, 27 StGB).

Die Gesetzeslage in Deutschland erfüllte bereits nahezu alle Vorgaben der Richtlinie 2013/40/EU über Angriffe auf Informationssysteme. Es war lediglich eine Anhebung der Strafobergrenze für den Straftatbestand des Vorbereitens des Ausspähens und Abfangens von Daten (§ 202c StGB) von einem Jahr auf zwei Jahre Freiheitsstrafe erforderlich, welche mit dem am 26. November 2015 in Kraft getretenen Gesetz zur Bekämpfung der Korruption erfolgt ist.

B/ Richtlinie 2011/93/EU zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie

Die Richtlinie 2011/93/EU zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie ist von Deutschland mit dem 49. Gesetz zur Änderung des Strafgesetzbuches (Umsetzung europäischer Vorgaben zum Sexualstrafrecht) in deutsches Recht umgesetzt worden; das Gesetz ist am 27. Januar 2015 in Kraft getreten. **Sexueller Missbrauch von Kindern (§ 176 StGB)**

– Nach § 176 Absatz 1 StGB wird bestraft, wer sexuelle Handlungen an einer Person unter 14 Jahren (Kind) vornimmt oder an dem Kind vornehmen lässt. Ebenso wird bestraft, wer ein Kind dazu bestimmt, dass es sexuelle Handlungen an einem Dritten vornimmt oder von einem Dritten an sich vornehmen lässt (§ 176 Absatz 2 StGB). Gemäß § 176 Absatz 4 StGB wird mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren bestraft, wer sexuelle Handlungen vor einem Kind vornimmt (Nummer 1), ein Kind dazu bestimmt, dass es sexuelle Handlungen vornimmt, soweit die Tat nicht nach Absatz 1 oder Absatz 2 mit Strafe bedroht ist (Nummer 2), auf ein Kind durch Schriften (§ 11 Absatz 3 StGB) oder mittels Informations- oder Kommunikationstechnologie einwirkt, um das Kind zu sexuellen Handlungen zu bringen, die es an oder vor dem Täter oder einer dritten Person vornehmen oder von dem Täter oder einer dritten Person an sich vornehmen lassen soll (Nummer 3 Buchstabe a) oder um eine Tat nach § 184 Absatz 1 Nummer 3 (Herstellung kinderpornografischer Schriften) oder nach § 184b Absatz 3 (Erwerb und Besitz kinderpornografischer Schriften) zu begehen (Nummer 3 Buchstabe b) oder auf ein Kind durch Vorzeigen pornografischer Abbildungen oder Darstellungen, durch Abspielen von Tonträgern pornografischen Inhalts, durch Zugänglichmachen pornografischer Inhalte mittels Informations- oder Kommunikationstechnologie oder durch entsprechende Reden einwirkt (Nummer 4). Nach § 176 Absatz 5 StGB wird mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren bestraft, wer ein Kind für eine Tat nach den Absätzen 1 bis 4 (§ 176 StGB) anbietet oder nachzuweisen verspricht oder wer sich mit einem anderen zu einer solchen Tat verabredet.

- Begriffsbestimmungen: Gemäß § 184h Nummer 1 StGB sind sexuelle Handlungen nur solche, die im Hinblick auf das jeweils geschützte Rechtsgut von einiger Erheblichkeit sind. Sexuelle Handlungen vor einer anderen Person sind gemäß § 184h Nummer 2 StGB nur solche, die vor einer anderen Person vorgenommen werden, die den Vorgang wahrnimmt. Gemäß § 11 Absatz 3 StGB stehen den Schriften Ton- und Bildträger, Datenspeicher, Abbildungen und andere Darstellungen gleich. Der Begriff der Pornografie ist gesetzlich nicht definiert, sondern wird von der Rechtsprechung bestimmt (zu Kinder- und Jugendpornografie siehe nachstehend § 184b Absatz 1 Nummer 1 und § 184c Absatz 1 Nummer 1 StGB).
- Strafbar ist nur vorsätzliches Handeln, § 15 StGB.
- Erschwerende/mildernde Umstände: Erschwerungsgründe: § 176a (Schwerer sexueller Missbrauch von Kindern), § 176b StGB (Sexueller Missbrauch von Kindern mit Todesfolge).
- Strafrahmen: Freiheitsstrafe von sechs Monaten bis zu zehn Jahren (§ 176 Absätze 1 und 2 StGB); Freiheitsstrafe von drei Monaten bis fünf Jahren (§ 176 Absätze 4 und 5 StGB); Freiheitsstrafe von einem Jahr bis fünfzehn Jahre (§ 176a Absatz 1 StGB); Freiheitsstrafe von zwei Jahren bis fünfzehn Jahre (§ 176a Absatz 3 StGB), lebenslange Freiheitsstrafe oder Freiheitsstrafe von zehn bis fünfzehn Jahren (§ 176b StGB).
- Wiederholungstaten: Gemäß § 176a Absatz 1 StGB wird der sexuelle Missbrauch von Kindern in den Fällen des § 176 Abs. 1 und 2 mit Freiheitsstrafe nicht unter einem Jahr bestraft, wenn der Täter innerhalb der letzten fünf Jahre wegen einer solchen Straftat rechtskräftig verurteilt worden ist.
- Anstiftung und Beihilfe sind unter den Voraussetzungen von §§ 26, 27 StGB strafbar.
- Der Versuch ist gemäß § 176 Absatz 6 StGB mit Ausnahme der Straftaten nach § 176 Absatz 4 Nummer 3 und 4 und § 176 Absatz 5 StGB strafbar.

Verbreitung, Erwerb und Besitz kinderpornografischer Schriften (§ 184b StGB)

– Gemäß § 184b Absatz 1 StGB wird mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren bestraft, wer eine kinderpornografische Schrift verbreitet oder der Öffentlichkeit zugänglich macht (Nummer 1, 1. Halbsatz) oder wer es unternimmt, einer anderen Person den Besitz an einer kinderpornografischen Schrift, die ein tatsächliches oder wirklichkeitsnahes Geschehen wiedergibt, zu verschaffen (Nummer 2) oder wer eine kinderpornografische Schrift, die ein tatsächliches Geschehen wiedergibt, herstellt (Nummer 3) oder wer eine kinderpornografische Schrift herstellt, bezieht, liefert, vorrätig hält, anbietet, bewirbt oder es unternimmt, diese Schrift ein- oder auszuführen, um sie oder aus ihr gewonnene Stücke zu verwenden oder einer anderen Person eine solche Verwendung zu ermöglichen, soweit die Tat nicht nach Nummer 3 mit Strafe bedroht ist (Nummer 4). Gemäß § 184b Absatz 3 StGB macht sich strafbar, wer es unternimmt, sich den Besitz an einer kinderpornografischen Schrift, die ein tatsächliches oder wirklichkeitsnahes Geschehen wiedergibt, zu verschaffen, oder wer eine solche Schrift besitzt.

– Begriffsbestimmungen: Gemäß § 184b Absatz 1 Nummer 1, 2. Halbsatz StGB ist eine pornografische Schrift (§ 11 Absatz 3 StGB – s.o.) kinderpornografisch, wenn sie a) sexuelle Handlungen von, an oder vor einer Person unter vierzehn Jahren (Kind) oder b) die Wiedergabe eines ganz oder teilweise unbekleideten Kindes in unnatürlich geschlechtsbetonter Körperhaltung oder c) die sexuell aufreizende Wiedergabe der unbekleideten Genitalien oder des unbekleideten Gesäßes eines Kindes zum Gegenstand hat. Gemäß § 184d Absatz 1 Satz 1 StGB wird nach §§ 184 bis 184c StGB auch bestraft, wer einen pornografischen Inhalt mittels Rundfunk oder Telemedien einer anderen Person oder der Öffentlichkeit zugänglich macht. Gemäß § 184d Absatz 2 Satz 1 StGB wird nach § 184b Absatz 3 StGB auch bestraft, wer es unternimmt, einen kinderpornografischen Inhalt mittels Telemedien abzurufen.

– Strafbar ist nur vorsätzliches Handeln, § 15 StGB.

– Erschwerende/mildernde Umstände: § 184b Absatz 2 StGB sieht eine Strafschärfung vor, wenn der Täter in den Fällen des Absatzes 1 gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung solcher Taten verbunden hat, und wenn die Schrift in den Fällen des § 184b Absatz 1 Nummer 1, 2 und 4 ein tatsächliches oder wirklichkeitsnahes Geschehen wiedergibt.

– Strafrahmen: Verbreiten, Herstellen, Besitz, Verschaffen etc. (§ 184b Absätze 1 und 2): Freiheitsstrafe von drei Monaten bis zu fünf Jahren. Qualifikation für Absatz 1 (§ 184b Absatz 2): Freiheitsstrafe von sechs Monaten bis zehn Jahren. Unternehmen des Sichverschaffens und Besitz (§ 184b Absatz 3): Freiheitsstrafe bis zu drei Jahren oder Geldstrafe.

– Wiederholungstaten: Dies ist ein Gesichtspunkt der Strafzumessung (§ 46 StGB).

– Anstiftung und Beihilfe sind unter den Voraussetzungen von §§ 26, 27 StGB strafbar.

– Der Versuch ist gemäß § 184b Absatz 4 StGB strafbar; dies gilt nicht für Taten nach § 184b Absatz 1 Nummern 2 und 4 sowie Absatz 3. Soweit das Gesetz jedoch in § 184b Absatz 1 Nummer 2 sowie Absatz 3 StGB von dem Unternehmen einer Tat spricht, wird gemäß § 11 Absatz 1 Nummer 6 deren Versuch und deren Vollendung erfasst.

– Sonstiges: Gemäß § 184b Absatz 5 StGB gelten § 184b Absatz 1 Nummer 2 und Absatz 3 StGB nicht für Handlungen, die ausschließlich der rechtmäßigen Erfüllung von staatlichen Aufgaben dienen oder die sich aus einer Vereinbarung mit einer zuständigen staatlichen Stelle ergeben (Nummer 2) oder die der Erfüllung dienstlicher oder beruflicher Pflichten dienen (Nummer 3).

Verbreitung, Erwerb und Besitz jugendpornografischer Schriften (§ 184c StGB)

– Gemäß § 184c Absatz 1 StGB wird bestraft, wer eine jugendpornografische Schrift verbreitet oder der Öffentlichkeit zugänglich macht (Nummer 1, 1. Halbsatz) oder es unternimmt, einer anderen Person den Besitz an einer jugendpornografischen Schrift, die ein tatsächliches oder wirklichkeitsnahes Geschehen wiedergibt, zu verschaffen (Nummer 2) oder eine jugendpornografische Schrift, die ein tatsächliches Geschehen wiedergibt, herstellt (Nummer 3) oder eine jugendpornografische Schrift herstellt, bezieht, liefert, vorrätig hält, anbietet, bewirbt oder es unternimmt, diese Schrift ein- oder auszuführen, um sie oder aus ihr gewonnene Stücke zu verwenden oder einer anderen Person eine solche Verwendung zu ermöglichen, soweit die Tat nicht nach Nummer 3 mit Strafe bedroht ist (Nummer 4). Gemäß § 184c Absatz 3 StGB macht sich strafbar, wer es unternimmt, sich den Besitz an einer jugendpornografischen Schrift, die ein tatsächliches Geschehen wiedergibt, zu verschaffen, oder wer eine solche Schrift besitzt.

– Begriffsbestimmungen: Gemäß § 184c Absatz 1 Nummer 1, 2. Halbsatz StGB ist eine pornografische Schrift (§ 11 Absatz 3 StGB – s. o.) jugendpornografisch, wenn sie a) sexuelle Handlungen von, an oder vor einer vierzehn, aber noch nicht achtzehn Jahre alten Person oder b) die Wiedergabe einer ganz oder teilweise unbekleideten vierzehn, aber noch nicht achtzehn Jahre alten Person in unnatürlich geschlechtsbetonter Körperhaltung zum Gegenstand hat. Gemäß § 184d Absatz 1 Satz 1 StGB wird nach §§ 184 bis 184c StGB auch bestraft, wer einen pornografischen Inhalt mittels Rundfunk oder Telemedien einer anderen Person oder der Öffentlichkeit zugänglich macht. Gemäß § 184d Absatz 2 Satz 2 StGB wird nach § 184c Absatz 3 StGB auch bestraft, wer es unternimmt, einen jugendpornografischen Inhalt mittels Telemedien abzurufen.

– Strafbar ist nur vorsätzliches Handeln, § 15 StGB.

– Erschwerende/mildernde Umstände: § 184c Absatz 2 StGB sieht eine Strafschärfung vor, wenn der Täter in den Fällen des Absatzes 1 gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung solcher Taten verbunden hat und wenn die Schrift in den Fällen des § 184c Absatz 1 Nummer 1, 2 und 4 ein tatsächliches oder wirklichkeitsnahes Geschehen wiedergibt.

– Verbreiten, Herstellen, Besitz, Verschaffen etc. (§ 184c Absätze 1 und 2): Freiheitsstrafe bis zu drei Jahren oder Geldstrafe. Qualifikation für Absatz 1 (§ 184c Absatz 2): Freiheitsstrafe von drei Monaten bis fünf Jahren. Unternehmen des Sichverschaffens und Besitz (§ 184c Absatz 3): Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

– Wiederholungstaten: Dies ist ein Gesichtspunkt der Strafzumessung (§ 46 StGB).

– Anstiftung und Beihilfe sind unter den Voraussetzungen von §§ 26, 27 StGB strafbar.

– Der Versuch ist gemäß § 184c Absatz 5 StGB strafbar; dies gilt nicht für Taten nach § 184c Absatz 1 Nummern 2 und 4 sowie Absatz 3. Soweit das Gesetz jedoch in § 184c Absatz 1 Nummer 2 und 4 sowie in Absatz 3 StGB von dem Unternehmen einer Tat spricht, wird gemäß § 11 Absatz 1 Nummer 6 StGB deren Versuch und deren Vollendung erfasst.

– Sonstiges: Gemäß § 184c Absatz 4 StGB sind § 184c Absatz 1 Nummer 3, auch in Verbindung mit Absatz 5, und Absatz 3 nicht anzuwenden auf Handlungen von Personen in Bezug auf solche jugendpornografische Schriften, die sie ausschließlich zum persönlichen Gebrauch mit Einwilligung der dargestellten Person hergestellt haben. Gemäß § 184c Absatz 6 StGB gilt § 184b Absatz 5 StGB entsprechend.

C/ Online-Kartenbetrug

Die Bürger melden im Regelfall, wenn sie Opfer von Kartenbetrug im Internet geworden sind. Private Unternehmen melden es nicht immer und die Betreiber der Karten melden es fast nie. Gründe dafür sind folgende:

Der Bürger stellt fest, dass von seinem Kreditkartenkonto/Girokonto unberechtigte Transaktionen durchgeführt wurden; um dies zu klären, setzt er sich im Regelfall als erstes mit seinem Geldinstitut in Verbindung. Im Regelfall wird der Bürger dann von der Bank aufgefordert, eine Anzeige zu erstatten. Zusätzlich sieht der Bürger den Missbrauch seiner Daten subjektiv als eine sehr schwere und ernsthafte Bedrohung an.

Private Unternehmen zeigen den Kartenbetrug bedeutend weniger an, weil sie im Regelfall nur mittelbar von dem Kartenbetrug betroffen sind. Bei ihnen werden Waren und Leistungen mittels widerrechtlich erlangter Kartendaten bestellt. Da sie oftmals von den Kreditkartengesellschaften entschädigt werden, liegt kein besonderes Interesse an einer Strafverfolgung vor. Verluste die trotzdem gemacht werden, sind genauso eingepreist wie die Diebstähle in einem normalen Ladengeschäft.

Die Betreiber der Karten, ob Banken oder die Gesellschaften selbst, erstatten fast nie Anzeigen. Jede Anzeige würde ein negatives Image der Kreditkarte bedienen, was nicht im Interesse der Banken und Gesellschaften liegt.

Über das Dunkelfeld liegen in diesem Phänomenbereich keine fundierten Kenntnisse vor; allerdings besagt eine regionale Studie in Niedersachsen, dass im gesamten Phänomenbereich "Cybercrime" lediglich 9% der Straftaten angezeigt werden.
Gründe dafür, dass keine Meldung des Betrugsopfers erfolgt, könnten sein:
• Kauf von Zugängen zu illegalen oder pornografischen Inhalten
• Kauf von illegalen Waren (z. B. Drogen, apothekenpflichtige Medikamente)
• Geringfügigkeit des Betrages
• Angst vor Prestigeverlust bei Privatunternehmen

Im Bereich Online-Kartenbetrug erfolgt die Zusammenarbeit des Bundeskriminalamtes (BKA) mit der Privatwirtschaft auf vielfältige Art und Weise. Beispielhaft sind hier die Zusammenarbeit mit dem Arbeitskreis Sicherheit "Debit- und Kreditkarten in Deutschland" und die Nationale Kooperationsstelle Cybercrime, insbesondere die "institutionalized Public-Private-Partnership" (**iPPP**) zu nennen. Im Zusammenhang mit der Erhöhung der Sicherheit beim Zahlungskarteneinsatz erfolgt eine Kooperation mit Wirtschaftsunternehmen in den Bereichen Verhinderung der Manipulation von POS-Terminals und Geldausgabeautomaten sowie im Zusammenhang mit dem Wechsel von Magnetstreifen- auf Chiptechnologie.

Daneben arbeiten auch die Strafverfolgungsbehörden der Länder zur Bekämpfung und Aufklärung von Straftaten des Online-Kartenbetrugs mit Unternehmen, insbesondere mit Banken, auf vielfältige Art und Weise zusammen. Beispielhaft – ohne Anspruch auf Vollständigkeit – wird die Zusammenarbeit der Strafverfolgungsbehörden mit Unternehmen in den Ländern Brandenburg und Sachsen-Anhalt geschildert:

Im Bundesland **Brandenburg** wurde bei dem Polizeipräsidium Fachdirektion Landeskriminalamt (FD LKA) die Zentrale Ansprechstelle Cybercrime für Unternehmen, Einrichtungen und Bürger eingerichtet. Sie ist zugleich Single Point of Contact (SPoC).

Die FD LKA nimmt u. a. regelmäßig an Veranstaltungen der Industrie- und Handelskammern des Landes Brandenburg teil, um auf diesem Wege Erkenntnisse zu polizeilich bekannt gewordenen Cybercrime-Phänomenen mitzuteilen, Kontakte zu Partnern aus der Wirtschaft und IT-Branche zu knüpfen bzw. Erfahrungen zur IT-Sicherheit in Unternehmen auszutauschen.

Im Bundesland **Sachsen-Anhalt** arbeitet die Polizei im Rahmen der Ermittlungen bei der Bekämpfung von Straftaten in diesem Deliktsfeld eng mit der Firma EURO-Kartensysteme GmbH als Gemeinschaftsunternehmen (Service- und Kompetenzzentrum) im Bereich des kartengestützten Zahlungsverkehrs der deutschen Kreditwirtschaft zusammen. Anfragen werden aber auch an die einzelnen Kreditkartenunternehmen gerichtet. Eine Beantwortung seitens der Kreditkartenunternehmen erfolgt jedoch nicht in jedem Fall. Einmal jährlich führt der Arbeitskreis Sicherheit der Kartenorganisationen in Deutschland eine praxisbezogene Fachtagung zum Thema Zahlungskartenkriminalität durch, bei der zeitnah neue Modi Operandi und Sicherheitsstrategien vermittelt werden.

Zum Teilnehmerkreis gehören neben Ermittlungsbeamten der Fachdienststellen der Kriminalpolizei der Länder und des BKA auch Vertreter der Kartenindustrie sowie Sicherheitsunternehmen. Des Weiteren findet quartalsweise auf freiwilliger Basis mit dem o. g. Teilnehmerkreis ein Stammtisch zum Zwecke des Informationsaustausches statt. Seitens der Polizei und den Vertretern der Kartenindustrie sowie den Geldautomaten-/Terminalherstellern besteht ein intensiver Informationsaustausch.

Speziell ausgebildete oder geschulte Mitarbeiter der Kreditkarteninstitute entwickeln eigene Sicherheitskonzepte. Sie arbeiten eng mit der Polizei zusammen und sind für die Polizeibehörden jederzeit ansprechbar. Die Öffentlichkeit wird seitens der Polizei mit entsprechendem Präventionsmaterial sensibilisiert. Beispielsweise soll durch die Veröffentlichung von Kurzfilmen das Sicherheitsbewusstsein verstärkt werden. Auf Anfrage führen Polizeibeamte Schulungen in Geldinstituten durch. Die europaweite Einführung der EMV-Chiptechnologie sowie die grundsätzliche Deaktivierung der Magnetstreifen auf Debitkarten seitens der Geldinstitute erhöhten die Sicherheit im Zusammenhang mit Skimmingangriffen auf deutsche Geldautomaten enorm. Dadurch werden die Einsatzmöglichkeiten gefälschter Karten zunehmend erschwert. Auf die Genehmigung von Online-Transaktionen haben die Strafverfolgungsbehörden keinen Einfluss. Auch hier wird im Rahmen der Prävention auf den sensiblen Umgang beim Bezahlen im Internet hingewiesen. Grundsätzlich verhalten sich die Banken bei der Anzeigenerstattung relativ restriktiv, zumal die Schäden durch die missbräuchliche Verwendung von Kartendaten nur einen Bruchteil des Gesamtumsatzes ausmachen.

D/ Sonstige Phänomene der Cyberkriminalität

Von den meisten Ländern wurde die technische und personelle Ausstattung der Strafverfolgungsbehörden als zufriedenstellend empfunden. Schwierigkeiten bestehen hier vor allem bei der Auswertung von Datenträgern mit großen Datenmengen. In vielen Verfahren werden inzwischen auf Rechnern von Beschuldigten Daten im Bereich von Terabyte sichergestellt. Die hier notwendige Auswertung ist einerseits technisch sehr aufwändig und benötigt andererseits häufig eine längere Zeit, sodass es hier zu Verzögerungen im Verfahrensabschluss kommen kann.

Das Bundeskriminalamt (BKA) versucht, Hindernisse bei der grenzübergreifenden Zusammenarbeit, insbesondere beim Thema Online-Kartenbetrug, durch die Intensivierung der bilateralen internationalen Kooperationen sowie die Einbindung von Zentralstellen (INTERPOL/Europol) zu reduzieren.

In Sachsen-Anhalt und in anderen Ländern erfolgt die Zusammenarbeit mit ausländischen Polizeibehörden grundsätzlich im Rahmen der internationalen Rechtshilfe. Daneben erhebt das "Sicherheitsmanagement Zahlungskarten" der EURO-Kartensysteme GmbH alle Daten zu europaweit angegriffenen Geldautomaten/POS-Terminals und stellt diese den Ermittlungsbehörden zur Verfügung.

Das Land Hessen berichtete, dass sich als probates Mittel zur grenzüberschreitenden Beweissicherung in den letzten Jahren erwiesen hat, in den Fällen, in denen Hinweise aus dem Ausland auf Straftaten, bei denen Geschädigte auch im Inland vorhanden sind, ein "Parallel-Ermittlungsverfahren" einzuleiten, die beweissichernden Erstmaßnahmen zu treffen und dann im Wege des § 61a IRG zur Vorbereitung eines Rechtshilfeersuchens die hier gewonnenen Informationen zeitnah an die ausländischen Ermittlungsbehörden zu übermitteln.

Da sich der Weg der förmlichen Rechtshilfe oftmals trotzdem als zu schwerfällig erwiesen hat, um wirksame Strafverfolgung betreiben zu können, haben sich in den letzten Jahren bilaterale Kooperationen (insbesondere JITs (Joint-Investigation-Teams)) als weiteres wirksames Mittel zur grenzübergreifenden Bekämpfung des Online-Kartenbetrugs erwiesen.

Ferner ist Deutschland in diesem Zusammenhang an einigen europäischen und internationalen Projekten beteiligt. Dies sind unter anderem:

– die Europäische Agentur für Netz- und Informationssicherheit (ENISA) zur Förderung einer verstärkten Zusammenarbeit und eines verbesserten Informationsaustauschs zwischen den Mitgliedsstaaten zu Themen der Netz- und Informationssicherheit
– das Programm der Europäischen Kommission AGIS zur Unterstützung der EU-Staaten und Kandidatenländer (Angehörige von Rechtsberufen, Strafverfolgungsbehörden und Vertreter von Stellen, die mit der Unterstützung der Opfer befasst sind) beim Aufbau europaweiter Netzwerke und dem Austausch von Informationen und bewährten Praktiken
– die Interpol European Working Party on IT-Crime (EWPITC), eine Plattform für den Erfahrungsaustausch zur Bekämpfung von IT-Kriminalität.

5.2. Verfahrensfragen

5.2.1. Ermittlungstechniken

Folgende Ermittlungstechniken sind zulässig:

- Durchsuchung und Beschlagnahme eines Informationssystems bzw. von Computerdaten

Die Durchsuchung und Beschlagnahme von Gegenständen, auf denen Daten gespeichert sind (z. B. Festplatten oder Server) sind gemäß §§ 94 ff., 102 ff., 110 Strafprozessordnung (StPO) möglich, soweit es sich bei diesen Gegenständen um Beweismittel in einem Ermittlungsverfahren handelt.

- Abfangen bzw. Sammeln von Verkehrs- bzw. Inhaltsdaten in Echtzeit

Im Rahmen einer Telekommunikationsüberwachung nach §§ 100a, 100b StPO ist eine Ausleitung der Verkehrs- bzw. Inhaltsdaten in Echtzeit möglich. Dies setzt allerdings voraus, dass der Verdacht einer der in § 100a Absatz 2 StPO aufgezählten schweren Straftaten vorliegt und die Überwachung gemäß § 100b StPO nach dem üblichen Verfahren richterlich angeordnet wurde. Verkehrsdaten wie etwa die Nummern oder Kennungen der beteiligten Anschlüsse oder der Endgeräte sowie Standortdaten eines Mobiltelefons können ferner gemäß § 100g StPO erhoben werden. Voraussetzung ist hier die Begehung einer Straftat von auch im Einzelfall erheblicher Bedeutung, wozu insbesondere die in § 100a Absatz 2 StPO genannten Straftaten zählen, oder die Begehung einer Straftat mittels Telekommunikation.

Bezieht sich die Maßnahme auf Verkehrsdaten, die nach dem am 18. Dezember 2015 in Kraft getretenen Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten von den Telekommunikationsunternehmen über einen bestimmten Zeitraum verpflichtend gespeichert werden müssen, ist die Erhebung nur bei besonders schweren Straftaten im Sinne der in § 100g Absatz 2 StPO aufgezählten Straftaten zulässig. Eine richterliche Anordnung ist in allen Fällen der Erhebung von Verkehrsdaten regelmäßig erforderlich.

- Sicherung von Computerdaten

Gespeicherte Daten können durch die Beschlagnahme der Speichermedien gesichert werden. Dies setzt gemäß §§ 94, 98 StPO einen Straftatverdacht und in der Regel eine richterliche Anordnung voraus. Zudem ist zu begründen, dass die Daten als Beweismittel für die Untersuchung von Bedeutung sein können. Bei Gefahr in Verzug kann die Anordnung der Beschlagnahme auch durch die Staatsanwaltschaft und die Polizei erfolgen (§ 98 Absatz 1 Satz 1 StPO). Eine Erhebung im Wege der sogenannten "Online-Durchsuchung", d. h. ein Zugriff auf die gespeicherten Daten unter Nutzung der Kommunikationsnetze durch Infiltrieren des Zielsystems mittels einer speziellen Spähsoftware, ist für Zwecke der Strafverfolgung nicht zulässig.

- Anordnung auf Sicherung der gespeicherten Verkehrs- bzw. Inhaltsdaten

Nach § 100b, 101a StPO können Maßnahmen nach §§ 100a, 100g StPO nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden. Bei Gefahr im Verzug kann die Anordnung auch durch die Staatsanwaltschaft getroffen werden. Dies gilt jedoch nicht für den Abruf verpflichtend gespeicherter Verkehrsdaten (§ 101a Absatz 1 Satz 2 StPO). Soweit die Anordnung nicht binnen drei Werktagen von dem Gericht bestätigt wird, tritt sie außer Kraft.

- Anordnung auf Sicherung der Nutzerinformationen

Die Erhebung von Nutzerinformationen in Form von Bestandsdaten, zu denen etwa Name und Anschrift eines Anschlussinhabers sowie zugteilte Rufnummern und Anschlusskennungen gehören, bei Telekommunikationsunternehmen ist zulässig, soweit dies für die Erforschung des Sachverhalts oder Ermittlung des Aufenthaltsortes eines Beschuldigten erforderlich ist (§ 100j StPO). Voraussetzung ist – wie bei allen strafprozessualen Maßnahmen – das Vorliegen des Anfangsverdachts einer Straftat; eine richterliche Anordnung ist nicht erforderlich.

Im Rahmen der rechtlichen Möglichkeiten werden die in Frage kommenden polizeilichen Ermittlungsmaßnahmen (verdeckte und/oder offene Maßnahmen) durchgeführt.

Folgende besondere Ermittlungsmethoden werden eingesetzt:

- Ermittlung von Bestandsdaten und Verkehrsdaten bei Providern (dies ist eine der häufigsten eingesetzten Ermittlungsmethoden),
- Telekommunikationsüberwachung (Überwachung des Datenverkehrs von Internet-Access-Rechnern oder Servern im Internet),
- klassische Telefonüberwachung,
- E-Mail-Beschlagnahme beim Serviceprovider,
- IP-Tracking (z. B. Skype und andere Messenger-Dienste),
- Open-Source-Recherchen im Internet,
- Ermittlungen in Foren sowie Personalisierung von Nicknames sowie
- Sicherung von Daten von Datenträgern und aus dem Internet (Web-Seiten, Log-Dateien).

Es ist zunehmend festzustellen, dass umfangreiche Server-Überwachungen oder individuell programmierte Überwachungsmaßnahmen nötig sind, um Cyberstraftaten erfolgreich verfolgen zu können. Allerdings umfasst eine erfolgreiche Ermittlungsstrategie immer eine Vielzahl unterschiedlicher, auch klassischer, Ermittlungsmaßnahmen.

Im Bereich der Bekämpfung der Kinderpornografie dürften die häufigsten Ermittlungsmethoden die anlassunabhängige Recherche in Filesharingnetzwerken zur Ermittlung von Personen, die Kinderpornografie verbreiten und herunterladen, aber auch das Auswerten von Login-Daten zur Ermittlung der Nutzer kinderpornografischer Webseiten sowie die Auswertung der Kontakte bereits ermittelter Täter sein.

Weitere Ermittlungsansätze für die Strafverfolgungsbehörden ergeben sich beispielsweise aus Recherchen im Internet, erlangten Beweismitteln aus Durchsuchungsmaßnahmen, verdeckten Maßnahmen bzw. aus Vernehmungen von Beschuldigten oder Zeugen.

Angesichts der großen Bandbreite von Cyberstraftaten kann es keine allgemein bewährten Verfahren oder Methoden zur Ermittlung solcher Taten geben. Jeder Fall liegt anders, die Ermittlungsverfahren und -methoden müssen sich am konkreten Einzelfall und den jeweils vorhandenen Ermittlungsansätzen orientieren. Einer der wichtigsten Ermittlungsansätze ist sicher der Rückgriff auf Datenspuren im Netz bei der Kommunikation in Form der Personenauskunft zu verwendeten IP-Adressen, in Form der Verkehrsdatenauskunft oder – soweit eine Katalogstraftat vorliegt – auch eine Überwachung der Internetkommunikation. Weitere wichtige Quellen sind die Beschlagnahme und Auswertung von Datenträgern und E-Mail-Postfächern. Sofern die Cyberstraftat ein Vermögensdelikt darstellt, sind zudem Bank- und Kontoauskünfte unabdingbar, um den Weg des Geldes nachzuvollziehen. Insbesondere beim Phishing im Zusammenhang mit Online-Banking wird bei den Finanzagenten angesetzt und mittels verdeckter Maßnahmen versucht, den bandenmäßig begangenen Computerbetrug beweissicher nachzuweisen.

Sind Ermittlungen auf technischem Wege nicht möglich, müssen verdeckte personale Ermittlungen geführt werden. Solche verdeckten polizeilichen Ermittlungen durch den Einsatz von sogenannten "NoeP" (nicht offen ermittelnde Polizeibeamten), der auf Grundlage der polizeilichen Generalklausel möglich ist, erfolgt zumeist bei Ermittlungen in Foren und Boards. Allerdings sind solche Ermittlungen nur dann erfolgversprechend, wenn sie langfristig angelegt sind.

Im Land Brandenburg wird ein Videochatsystem betrieben, das durch die Nutzer nach Anmeldung – unter Angabe eines Namens und der E-Mail-Adresse – mit einem User Account genutzt werden kann. Der Dienst bietet die Möglichkeit, in Gruppenchats mittels einer Bildübertragung in Echtzeit miteinander zu kommunizieren. Werden auf dieser Videochatplattform Straftaten begangen, z. B. Abbildungen des erigierten männlichen Geschlechtsteils gezeigt, wird dieses durch den Betreiber zeitnah dokumentiert. Dieser ermittelt die serverseitig gespeicherte IP-Adresse und übermittelt diese per Telefax an die Staatsanwaltschaft. Dort wird beschleunigt ein Ermittlungsverfahren eingeleitet, der Provider anhand der IP-Adresse ermittelt und – sofern dieser Verkehrsdaten für einen relevanten Zeitraum speichert – per Telefax gemäß § 100j Abs. 1 Satz 1, Abs. 2 StPO zu einer Auflösung zu einem Anschlussinhaber aufgefordert.

5.2.2. Forensik und Verschlüsselung

Beispielsweise erfolgt die Untersuchung einer beschlagnahmten Festplatte elektronisch. Die Analyse eines beschlagnahmten E-Mail-Postfaches erfolgt über eine Internetverbindung und kann somit als "ferngesteuerte forensische Untersuchung" eingestuft werden. Nicht praktiziert wird in Deutschland derzeit die Überwachung der computerunterstützten Telekommunikation (z. B. über Smartphones) im Wege eines zuvor eingeschleusten Trojaners.

Die heutzutage genutzten Computersysteme sind mit neuester Hard- und Software sowie stetig anwachsenden Speichermedien ausgestattet. Um diese Geräte auf unterschiedlichste Informationen wie SMS-Nachrichten, E-Mails, Dokumente, Fotos, Videos, Anrufprotokolle und gelöschte Daten hin analysieren zu können, werden für die forensische, polizeiliche Analyse und Untersuchung von Datenträgern und Speichersystemen ebenfalls hochwertige Soft- und Hardwaresysteme eingesetzt. Dem wachsenden Marktanteil von mobilen Endgeräten, wie Smartphones, Tablets und Laptops, kommt auch bei der Sicherung von Beweismitteln und der forensischen Begutachtung aus polizeilicher Sicht eine stetig ansteigende Bedeutung zu. Ein zentraler Aspekt der IT-Forensik ist die elektronische Untersuchung der digitalen Daten, die gemäß dem in Punkt 2 B Ziffer 4 erläuterten Prozess forensisch gesichert wurden. Die Untersuchung erfolgt durch einen federführenden Sachbearbeiter, wobei jeder Schritt dokumentiert wird und Manipulationen an den Quelldaten ausgeschlossen sind. Ferngesteuerte Untersuchungen im Wortsinn erfolgen nicht, jedoch werden je nach Erfordernis u.U. auch Sicherungen von entfernten Datenquellen (z. B. Cloud-Daten, Websites) vorgenommen. Dies erfolgt stets unter verantwortlicher Steuerung des Sachbearbeiters bzw. der (z. B. durch Rechtshilfeersuchen) beauftragten Stelle. Im Rahmen der Netzwerkforensik können durch Täter im Internet bei professionellen Anbietern angemietete Root-Servern überwacht werden. Die Root-Server werden von den Tätern i.d.R. als sog. "drop zones" genutzt, d. h. zur Entgegennahme von auf Opferrechnern ausgespähten Daten (Bankdaten etc.).

Verschlüsselung sollte nicht nur als Problem verstanden werden: Unter Abwägung sämtlicher Notwendigkeiten fördert die Bundesregierung auch aktiv den breiteren Einsatz von "Verschlüsselungs- und anderen Schutzmechanismen". In der "Digitalen Agenda" lautet der Auftrag:

"Wir unterstützen mehr und bessere Verschlüsselung. Wir wollen Verschlüsselungs-Standort Nummer 1 auf der Welt werden. Dazu soll die Verschlüsselung von privater Kommunikation in der Breite zum Standard werden."

"Wir fördern Geschäftsmodelle, die Anonymisierungs- und Pseudonymisierungsverfahren verwenden."

Die Bundesregierung unterstützt daher den Gebrauch von Verschlüsselungstechniken durch die Bürger und beabsichtigt nicht, diesen einzuschränken. Die Verfügbarkeit von sicheren und vertrauenswürdigen Verschlüsselungstechnologien ist sowohl für den Schutz der Privatsphäre der Bürger als auch für einen effektiven Datenschutz eine wesentliche Voraussetzung. Denn die Vertraulichkeit von Kommunikation im Internet kann nach derzeitigem Stand nur durch den Einsatz von Verschlüsselungstechnologien gesichert werden. Ihr Einsatz ist daher für die Wahrung der Privatsphäre im digitalen Raum unverzichtbar. Allerdings kann insbesondere im Bereich der schweren und organisierten Kriminalität der Einsatz von Verschlüsselung die Strafverfolgung erheblich erschweren.

Der Zugriff auf ermittlungsrelevante Informationen wird durch unbewussten oder gezielten Einsatz von Verschlüsselung erschwert oder vollständig verhindert. Im Bereich der schweren und organisierten Kriminalität stellen Maßnahmen zur Telekommunikationsüberwachung regelmäßig die einzig erfolgversprechenden Ermittlungsmaßnahmen dar. Fehlt diese Möglichkeit, können zahlreiche schwere und schwerste Straftaten nicht verfolgt werden.

Die Kryptierung von Telekommunikation hat im Zusammenhang mit der dynamischen Entwicklung und Verbreitung von Informations- und Kommunikationstechnologien weiter an Bedeutung gewonnen, u. a. weil der Einsatz von Verschlüsselungstechnik heute ohne Fachwissen von jedermann durch den Einsatz von kostenloser Software realisiert werden kann. Neben der aktiven Verschlüsselung von Daten und Verbindungen durch den Nutzer (z. B. Einsatz von Verschlüsselungstools für E-Mail oder VoIP) erfolgt diese häufig auch vom Nutzer unbewusst durch die Verwendung von Produkten, bei welchen eine Verschlüsselung des Datenstroms bereits integraler Bestandteil ist (z. B. Skype, Google Mail). Es ist zu erwarten, dass die Implementierung von Verschlüsselungsmechanismen bei neuen Telekommunikationsdiensten künftig obligatorisch sein wird. Im Rahmen der Untersuchung und Auswertung aufgezeichneter Telekommunikationsdaten stellt nicht selten bereits die Erkennung verschlüsselter Telekommunikation ein Problem dar, da die hohe Marktdynamik ständig neue bzw. veränderte Telekommunikationsdienste hervorbringt, die zunächst einer zumeist sehr aufwändigen manuellen Untersuchung bedürfen, bevor eine automatisierte Verarbeitung und Klassifizierung möglich sind. Auch bei tatrelevanten Datenträgern ist zunehmend zu beobachten, dass diese von den Tätern verschlüsselt werden, um den Strafverfolgungsbehörden Beweismittel zu entziehen.

Anonymisierung und Kryptierung werden teilweise gezielt eingesetzt, um Ermittlungen bzw. die Strafverfolgung zu erschweren oder zu verhindern. Eine Herausforderung ist dabei u. a., verschlüsselte Inhalte zu erkennen, da diese zum Teil nicht als solche gekennzeichnet sind. Zum Beispiel ist es möglich, innerhalb einer mit TrueCrypt verschlüsselten Datei weitere Inhalte verborgen und verschlüsselt zu speichern (sog. "hidden container"). Das Erschließen der Inhalte verschlüsselter Dateien auf rein technischem Wege gestaltet sich schwierig, äußerst aufwendig und mit sehr begrenzter Aussicht auf Erfolg.
Verschlüsselung gilt heute unter der Voraussetzung, dass Algorithmen sorgfältig ausgewählt und implementiert werden, als wirksames Schutzmittel zur Sicherung von Vertraulichkeit und Integrität. Es gibt nicht für alle Verschlüsselungen vorhandene Angriffsmechanismen. Die Entwicklung solcher Angriffsmechanismen ist enorm zeitintensiv. Ein "Brute-force"-Angriff – also das Ausprobieren aller möglichen Schlüssel – auf starke Verschlüsselung ist wegen der immensen zeitlichen Dauer in nahezu allen Fällen sinnlos. Selbst sogenannte Wörterbuchangriffe mit erstellten Begriffen zur Passwortsuche können über Monate bzw. Jahre dauern. Einige Verschlüsselungsmethoden sind derzeit nicht zu decodieren.

Eine Standardlösung gibt es weder für verschlüsselte Daten noch für verschlüsselte Kommunikation. Nach Prüfung des Einzelfalles werden ggf. gezielte Maßnahmen, wie besondere Maßnahmen zur Telekommunikationsüberwachung oder Dekryptierungsmaßnahmen eingesetzt.

Ob diese Lösungen zum Ziel führen, hängt im Allgemeinen vom Umgang des Täters mit der Verschlüsselungssoftware ab. Nur wenn dieser die Möglichkeit der Software nicht vollumfänglich nutzt, könnten die Sicherheitsbehörden auf Inhaltsdaten zuzugreifen. Andernfalls bleibt bei Kommunikationsvorgängen nur die sog. Rohdaten- bzw. Metadaten-Analyse, die technisch anspruchsvoll ist und IT-Spezialwissen voraussetzt. Bei vollverschlüsselten Datenträgern sind u. U. keine weiteren Ansätze möglich. In vielen Arbeitsbereichen ist es daher noch nicht möglich, das Problem der Verschlüsselung effektiv zu lösen.

Durch den Einsatz von spezialisierten Informatikern ist es in einigen Fällen gelungen, von den Tätern vorgenommene Verschlüsselungen zu decodieren. Zur effektiveren Bearbeitung von Wörterbuchangriffen können leistungsfähige Server mit Hochleistungsgrafikkarten zur Dekryptierung hilfreich sein.

Durch Intensivierung der Forschung und Entwicklung, gute Kooperation unter den Behörden und Entwicklung neuer Methoden können die durch Verschlüsselung entstehenden Herausforderungen teilweise kompensiert werden. So kann auf ermittlungstaktischer Ebene unter strenger Wahrung der strafprozessualen Vorgaben und des Verhältnismäßigkeitsgrundsatzes die Kryptierung von Datenträgern z. B. umgangen werden, sofern ein Zugriff bei laufenden Rechnern erfolgt und eine Sicherung des Arbeitsspeichers vorgenommen wird.

Im Zusammenwirken mit Polizeibehörden des Bundes und der Länder erfolgt anlassbezogen die Zusammenarbeit bei der Problemlösung sowie der Bereitstellung von Erkenntnissen zur Überwindung von Verschlüsselungsmechanismen.

Durch gemeinsame Gremien, Arbeits- und Projektgruppen werden auf Landes- und Bundesebene grundsätzliche Lösungsansätze für problematische Themen wie die Verschlüsselung von ermittlungsrelevanter Kommunikation und Daten erarbeitet. Da alle Strafverfolgungsbehörden bzgl. des Themas Kryptierung vor ähnlichen Herausforderungen stehen, hat sich innerhalb Deutschlands ein Informations- und Erkenntnistausch unter Beteiligung von Experten entwickelt, der vom BKA koordiniert wird und im Rahmen eines jährlichen "Sachbearbeitertreffens Kryptoanalyse" institutionalisiert wurde. Auf diesem Workshop werden die jeweils aktuellen Probleme diskutiert und nach praktikablen Ansätzen gesucht, Erfahrungen (Angriffsmechanismen) ausgetauscht und gegenseitige Hilfe – falls möglich – geleistet.

Eine Zusammenarbeit findet über die polizeilichen Gremien hinaus in diversen etablierten und institutionalisierten Fachtagungen und Expertentreffen statt. Ein regelmäßiger Informationsaustausch erfolgt über eine elektronische Kooperationsplattform (Wiki-TKÜ). Auf Bundesebene besteht zudem eine Forschungskooperation.

Im Bundeskriminalamt und zum Teil in den Ländern bestehen entsprechende Kompetenzzentren oder sind im Aufbau. Das Bundeskriminalamt (BKA) beschäftigt sich aktuell intensiv mit dem Thema Kryptoanalyse. Als spezialisierte Einrichtungen im weiteren Sinne sind alle Berechtigten Stellen zu bezeichnen, die mit der Durchführung von Telekommunikationsüberwachungsmaßnahmen betraut sind. Ebenso sind die Hersteller und Anbieter von Telekommunikationsanlagen und von Spezialsoftware sowie spezialisierte Forschungseinrichtungen (z. B. Universitäten, Fraunhofer-Institute) zu diesem Kreis zu zählen.

In der Regel wird die Entschlüsselung nicht in Zusammenarbeit mit Privatunternehmen durchgeführt. In Einzelfällen ist die Vergabe an externe Firmen theoretisch möglich. Ob eine Entschlüsselung an Privatunternehmen vergeben wird, obliegt der Entscheidung der verfahrensführenden Staatsanwaltschaft. Es existieren vereinzelt kommerzielle Anbieter, die Entschlüsselungen kostenpflichtig anbieten – jedoch ohne Erfolgsgarantie. Eine Beauftragung von Privatunternehmen seitens des Bundeskriminalamts (BKA) erfolgt derzeit nicht. Im Bereich der Telekommunikationsüberwachung kommen auch Softwareprodukte privater Unternehmen zum Einsatz, eine Entschlüsselung in Zusammenarbeit mit oder durch solche Unternehmen findet gleichwohl nicht statt.

Entschlüsselungen sind in jedem Fall sehr aufwendig, weshalb bei starker Kryptografie mit sachgerechter Anwendung eine effektive Lösung nicht möglich ist. Am Markt werden verschiedene Verschlüsselungsprogramme angeboten, die derzeit eine sichere Verschlüsselung gewährleisten. Vor dem Hintergrund der erhöhten Sensibilität rücken diese Programme immer stärker in den Blick der Öffentlichkeit, sodass sensible Bürger Daten und Kommunikation immer häufiger mit solchen Anwendungen vor unbefugtem Zugriff schützen.

Diese Entwicklung hat in einigen Fällen dazu geführt, dass auch Straftäter ihre inkriminierten oder beweiserheblichen Daten mit diesen Programmen dem Zugriff der Strafverfolgungsbehörden entziehen. Problembehaftet ist die Untersuchung von Daten, welche unter Anwendung anerkannt sicherer Krypto-Verfahren verschlüsselt wurden. Auch die Auswahl von Passwörtern hat Auswirkungen auf die Lösung der bestehenden Probleme.

Sofern in der Durchführung der klassischen Ermittlungen (Durchsuchung Umfeld Rechnerstandort, Abklärung soziales Umfeld des Beschuldigten, Vernehmungen) oder im Rahmen der Durchführung von Live-Forensik (Arbeitsspeichersicherung und Auswertung) keine konkreten Hinweise auf Passwörter oder Passwortfragmente erlangt werden können, ist eine erfolgreiche Dekryptierung in der Regel nicht oder nur in wenigen Einzelfällen und dann mit hohem Zeitansatz durchführbar. Entscheidend hierbei ist die Rechenleistung des verwendeten Dekryptierungssystems, wobei Passwörter einer bestimmten Länge und Komplexität zu einem exorbitanten Zeitansatz (von Monaten und Jahren) führen können. Hierzu gibt es keine bekannte Standardlösung.

Für Kommunikationsvorgänge können die Sicherheitsbehörden grundsätzlich auf die Ausgleichsmaßnahme Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) zurückgreifen.

Ausgehend davon, dass sich die Sicherheitsbedenken auf den möglichen Verlust verfahrensrelevanter Informationen durch entsprechende Verschlüsselung beziehen, verfolgen die zuständigen Behörden grundsätzlich folgende Ansätze zur Problemlösung:

– Intensivierung der Forschung und Entwicklung in diesem Bereich
– Experten-Austausch, Methoden-Austausch
– Ausbau der technischen Fähigkeiten
– Ausweitung der Kooperationen zwischen den Sicherheitsbehörden

Konkrete Problemlösungsansätze im Bereich Kryptierung werden in folgenden Maßnahmen gesehen:

– Ausbau der behördlichen Dekodier- und Analysekompetenz,
– Erforschung, (Weiter-)Entwicklung und flexibler Einsatz innovativer Methoden zur Umgehung von Kryptierung bzw. zur Erfassung von Telekommunikationsdaten, z. B. im Wege der Quellen-TKÜ und anderer spezieller Formen der Telekommunikationsüberwachung,
– Gewinnung von Meta-/Verkehrsdaten verschlüsselter Telekommunikation, um zumindest die näheren Umstände der Telekommunikation in Erfahrung zu bringen, wenn der Telekommunikationsinhalt nicht erschlossen werden kann,
– Intensivierung behördenübergreifender Zusammenarbeit, Kompetenzbündelung, Kooperation mit externen Instituten.

5.2.3. Elektronische Beweismittel

Verkehrsdaten sind gemäß § 3 Nummer 30 Telekommunikationsgesetz (TKG) Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Bestandsdaten sind nach § 3 Nummer 3 TKG solche Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden.

Gemäß § 202a Absatz 2 StGB sind Daten nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

Gemäß § 184b Absatz 1 Nummer 1, 2. Halbsatz StGB ist eine pornografische Schrift (§ 11 Absatz 3 StGB – s.o.) kinderpornografisch, wenn sie a) sexuelle Handlungen von, an oder vor einer Person unter vierzehn Jahren (Kind) oder b) die Wiedergabe eines ganz oder teilweise unbekleideten Kindes in unnatürlich geschlechtsbetonter Körperhaltung oder c) die sexuell aufreizende Wiedergabe der unbekleideten Genitalien oder des unbekleideten Gesäßes eines Kindes zum Gegenstand hat.
Nach § 184c Absatz 1 Nummer 1, 2. Halbsatz StGB ist eine pornografische Schrift (§ 11 Absatz 3 StGB – s. o.) jugendpornografisch, wenn sie a) sexuelle Handlungen von, an oder vor einer vierzehn, aber noch nicht achtzehn Jahre alten Person oder b) die Wiedergabe einer ganz oder teilweise unbekleideten vierzehn, aber noch nicht achtzehn Jahre alten Person in unnatürlich geschlechtsbetonter Körperhaltung zum Gegenstand hat.

Die übrigen Begriffe sind in Deutschland nicht legal definiert.

Nach § 110 Absatz 3 StPO darf die Durchsicht eines elektronischen Speichermediums bei dem von der Durchsuchung Betroffenen auch auf hiervon räumlich getrennte Speichermedien, soweit auf sie von dem Speichermedium aus zugegriffen werden kann, erstreckt werden, wenn andernfalls der Verlust der gesuchten Daten zu befürchten ist. Die Regelung dient dazu, den Verlust beweiserheblicher Daten zu vermeiden, die von dem durchsuchten Computer aus zwar zugänglich sind, sich aber auf einem räumlich getrennten Speichermedium, wie etwa dem Server im Intra- oder Internet, befinden. Dazu gehören auch E-Mails, die auf dem Server des Providers gespeichert sind. Die Durchsicht ist zulässig, wenn ansonsten ein Daten- und Beweismittelverlust zu befürchten ist, wenn also das externe Speichermedium nicht rechtzeitig sichergestellt werden kann. Werden verfahrensrelevante Daten gefunden, dürfen diese nach § 110 Absatz 3 Satz 2 StPO gesichert werden.

Als elektronische Beweismittel werden alle Beweise, die mittels Digitaltechnik erzeugt oder gespeichert werden, eingestuft. Es kommen alle Gegenstände infrage, auf denen potenziell verfahrensrelevante digitale Daten gespeichert sein können, z. B. Computer, Laptops, externe Datenträger, Handys/Smartphones, Spielekonsolen, aber auch z. B. Datenbanken und E-Mail-Bestände im Unternehmenskontext sowie Daten im Netzwerk, auf Cloud-Speichern oder im Internet (z. B. Foren etc.). Diese werden unter Sachleitung der Staatsanwaltschaft nach §§ 94, 98 StPO sichergestellt bzw. beschlagnahmt. Ist ein Verlust der gesuchten Daten zu befürchten (weil sie sich z. B. räumlich getrennt in einem Cloud-Speicher befinden, dessen Verbindung bei Sicherstellung des Asservats unterbrochen werden würde), können diese nach § 110 Absatz 3 StPO zunächst vorläufig sichergestellt werden, um eine Durchsicht (auch auf entfernten Datenspeichern) hinsichtlich verfahrensrelevanter Daten durchzuführen.
Auf technischer Ebene werden die digitalen Daten gesichert, um die Beweismittelkette zu wahren und jedwede Manipulation auszuschließen. Durch die zuständigen Polizeibehörden wird von eingehenden originalen Untersuchungsdaten (u. a. Asservate wie Log-Dateien, komplette Festplatten-Images) eine Datensicherung gefertigt. Elektronische Beweismittel werden dabei gemäß anerkannten Standards IT-forensisch gesichert. Dazu wird eine bitweise 1:1-Kopie der Daten samt forensischer Prüfsummen in einem standardisierten Format erzeugt, wobei ein eigens für diesen Prozess eingesetztes Schreibschutzmodul sicherstellt, dass auf die Quelldaten stets nur lesend zugegriffen wird. Im Anschluss an diesen Duplikationsprozess (sog. "Imaging") findet eine weitere Verifikation anhand der gespeicherten Prüfsummen statt. Die Integrität der gesicherten Daten wird dabei über die Berechnung einer kryptografischen Checksumme sichergestellt.

Auf diese Weise wird eine gerichtsverwertbare forensische Datensicherung erstellt, die als Basis aller weiteren Untersuchungen dient. Diese finden ausschließlich auf den forensischen Kopien und nie auf den Originaldaten statt.

Die Kopie der Untersuchungsdaten wird forensisch aufbereitet. Die inhaltliche Auswertung der forensisch aufbereiteten Datenträger erfolgt durch die ermittelnde polizeiliche Sachbearbeitung.

Da nur mit Kopien der auszuwertenden Daten gearbeitet wird, ist immer nachvollziehbar, dass die zu untersuchenden Daten nicht von Mitarbeitern des Landeskriminalamts (LKA) oder der Polizei manipuliert werden. Sofern sie für das Strafverfahren von Bedeutung sind, erfolgt auch die sachgerechte Aufbewahrung des Speichermediums bzw. des Duplikats. Sie stehen den Gerichten bzw. der Staatsanwaltschaft zur Verfügung. Zur Übermittlung von Daten werden je nach Datenmenge CD/DVD oder externe Festplatten verwendet. Die Entscheidung, welche Teilmenge der gesicherten Daten letztlich Verwendung in einem Verfahren finden, obliegt der Staatsanwaltschaft bzw. den Ermittlern, die die Daten einer inhaltlichen Bewertung unterziehen.

In Deutschland gibt es keine Sondervorschriften bezüglich der Beweisführung in Hinblick auf "elektronische Beweismittel". Der Begriff "elektronischer Beweis" ist rechtlich nicht definiert. Die Strafprozessordnung (StPO) in Deutschland beinhaltet keine expliziten Regelungen für elektronische Beweismittel. Es gelten die allgemeinen Regeln. Gespeicherte Daten werden in der Regel auf ein weiteres Speichermedium (z. B. DVD, Festplatte) kopiert (gespiegelt) und der Staatsanwaltschaft und dem Gericht in dieser Form zur Verfügung gestellt. Zudem werden lesbare Daten (z. B. Textnachrichten) oder Bilddateien ausgedruckt und zumindest zusätzlich in Papierform zur Verfügung gestellt. Nach derzeitiger Rechtslage ist eine unmittelbare Verlesung elektronischer Dokumente zum Zwecke der Beweisaufnahme über ihren Inhalt nicht möglich, da sie nicht als "Urkunden" bzw. als "Schriftstück" gelten. Sie müssen daher zunächst ausgedruckt werden. Im Rahmen eines aktuellen Gesetzgebungsvorhabens soll durch Änderung der entsprechenden Vorschrift eine unmittelbare Verlesung auch elektronischer Dokumente ermöglicht werden.

5.3. Schutz der Menschenrechte/Grundfreiheiten

Die im Grundgesetz verbürgten Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht. Nach Artikel 1 Absatz 3 Grundgesetz (GG) ist die Ausübung jeder staatlichen Gewalt an die Grundrechte gebunden. Soweit nach dem Grundgesetz ein Grundrecht durch Gesetz oder auf Grund eines Gesetzes eingeschränkt werden kann, muss das Gesetz dem Grundsatz der Verhältnismäßigkeit entsprechen. Das Gesetz muss allgemein und nicht nur für den Einzelfall gelten. Außerdem muss das Gesetz das Grundrecht unter Angabe des Artikels nennen. In keinem Falle darf ein Grundrecht in seinem Wesensgehalt angetastet werden. Die Grundrechte gelten auch für inländische juristische Personen, soweit sie ihrem Wesen nach auf diese anwendbar sind. Wird jemand durch die öffentliche Gewalt in seinen Rechten verletzt, so steht ihm der Rechtsweg offen. Das Unionsrecht entfaltet gemäß den Bestimmungen der Verträge und im Rahmen der durch Artikel 23 GG gezogenen Schranken innerstaatliche Wirkung.

Für die Erhebung von internetbezogenen Daten, insbesondere Bestandsdaten und Verkehrsdaten, enthalten das Telekommunikationsgesetz, die Strafprozessordnung (StPO) sowie die jeweiligen Polizeigesetze Vorschriften, die konkrete materielle und verfahrensrechtliche Vorgaben enthalten. Die Erhebung von Kommunikationsinhalten ist nur im Rahmen von Telekommunikationsüberwachungsmaßnahmen aufgrund einer richterlichen Anordnung zulässig.

Grundrechte können in der Regel aufgrund von allgemeinen Gesetzen, zu denen die Befugnisnormen im Ermittlungsverfahren zählen, eingeschränkt werden, solange der Grundsatz der Verhältnismäßigkeit gewahrt bleibt. Dies trifft sowohl auf das Recht auf informationelle Selbstbestimmung, als auch auf das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (vgl. jeweils Artikel 2 Absatz 1 i.V.m. Art. 1 Absatz 1 Grundgesetz (GG)), das Grundrecht der Meinungsfreiheit (Artikel 5 Absatz 1 und 2 GG) und das Grundrecht auf Gewährleistung des Telekommunikationsgeheimnisses (Artikel 10 GG) zu.

Beispielsweise findet nach Artikel 5 Absatz 2 Grundgesetz die Meinungsfreiheit ihre Schranken in den Vorschriften der allgemeinen Gesetze, den gesetzlichen Bestimmungen zum Schutze der Jugend und in dem Recht der persönlichen Ehre. Die Vorschriften des Ermittlungsverfahrens können allgemeine Gesetze und Jugendschutzgesetze im Sinne dieser Vorschriften darstellen. So können zur Verfolgung der Verbreitung kinderpornografischer Schriften (§ 184b StGB) Datenträger, z. B. Festplatten und Server, mit deren Hilfe die Verbreitung über das Internet stattfand, als Beweismittel nach §§ 94, 110 Strafprozessordnung (StPO) beschlagnahmt werden, obwohl die Handlungen des Betroffenen gegebenenfalls in den Schutzbereich des Grundrechts auf Meinungsfreiheit fallen könnten.

5.4. Gerichtliche Zuständigkeit

5.4.1. Grundsätze für die Ermittlungen bei Cyberkriminalität

Ein Einschreiten deutscher Strafverfolgungsbehörden setzt voraus, dass deutsches Strafrecht zur Anwendung kommt. Dies bestimmt sich nach den §§ 3 bis 9 Strafgesetzbuch (StGB). Das deutsche Strafrecht ist immer anwendbar auf Taten, die im Inland begangen werden (Territorialitätsprinzip, § 3 StGB). § 9 StGB zufolge ist eine Tat an jedem Ort begangen, an dem der Täter gehandelt hat oder im Falle des Unterlassens hätte handeln müssen oder an dem der zum Tatbestand gehörende Erfolg eingetreten ist oder nach der Vorstellung des Täters eintreten sollte.

Unabhängig vom Recht des Tatorts gilt das deutsche Strafrecht auch für Taten, die auf einem Schiff oder in einem Flugzeug begangen werden, das berechtigt ist, die Bundesflagge oder das Staatszugehörigkeitszeichen der Bundesrepublik Deutschland zu führen (Flaggenprinzip, § 4 StGB). Wenn die im Ausland begangene Tat dort mit Strafe bedroht ist oder der Tatort keiner Strafgewalt unterliegt, gilt das deutsche Strafrecht zudem sowohl für jede an (passives Personalitätsprinzip, § 7 Absatz 1 StGB) oder von einem deutschen Staatsangehörigen (aktives Personalitätsprinzip, § 7 Absatz 2 Nummer 1 StGB) im Ausland begangene Tat. Darüber hinaus sieht § 7 Absatz 2 Nummer 2 StGB vor, dass das deutsche Strafrecht auch auf Auslandstaten von Ausländern anwendbar ist, wenn die Tat am Tatort mit Strafe bedroht ist oder keiner Strafgewalt unterliegt und der Täter im Inland angetroffen wird; weitere Voraussetzung ist, dass der Täter, obwohl das IRG seine Auslieferung je nach der Art der Tat zuließe, nicht ausgeliefert wird (sei es weil ein Auslieferungsersuchen innerhalb angemessener Frist nicht gestellt oder abgelehnt wird oder die Auslieferung nicht durchführbar ist).

Zudem gilt das deutsche Strafrecht gemäß§ 5 StGB für Auslandstaten mit besonderem Inlandsbezug, unabhängig vom Recht des Tatorts. Darüber hinaus enthält § 6 StGB einen Katalog von Auslandstaten gegen international geschützte Rechtsgüter, für die unabhängig vom Recht des Tatorts ebenfalls das deutsche Strafrecht anwendbar ist (Weltrechtsprinzip) beispielsweise die Verbreitung kinderpornografischer Schriften (§ 184b Absatz 1 bis 3 StGB in § 6 Nummer 6 StGB).

5.4.2. Regeln für das Vorgehen bei Kompetenzkonflikten und Befassung von Eurojust

Eine zwingende rechtlich verbindliche Vorgabe für die Lösung von Kompetenzkonflikten gibt es in Deutschland nicht.

Maßgabe zum Umgang mit grenzüberschreitenden Kompetenzkonflikten ist das Verbot der mehrfachen Strafverfolgung, wie es sich u. a. in Artikel 54 Schengener Durchführungsübereinkommen (SDÜ) und Artikel 50 EU-Grundrechtecharta findet.

Wesentlich bei Straftaten, bei denen die Möglichkeit konkurrierender Verfolgungszuständigkeiten besteht, ist eine Information des anderen beteiligten Staates.

Sofern der Fall mehrerer konkurrierender Gerichtsbarkeiten erkannt wurde, kann dieser auf unterschiedlichste Art gelöst werden. Wenn eines der Verfahren offensichtlich das umfassendere und zielführendere ist, werden die anderen Staaten ihre Verfahren im Hinblick auf dieses Leitverfahren entweder aussetzen oder einstellen können. Dies kann in Deutschland nach u. a. §§ 153, 154 ff. StPO erfolgen. Sofern keiner der Staaten bereit ist, die Führung des Verfahrens zu übernehmen oder mehrere Staaten die Führung des Verfahrens übernehmen wollen, bietet sich ein konsensualer Verfahrenstransfer an. Dieser ist für Deutschland nicht verbindlich geregelt, ergibt sich aber als naheliegende Lösung zum Beispiel aus dem Rahmenbeschluss 2009/948/JI des Rates vom 30. November 2009 zur Vermeidung und Beilegung von Kompetenzkonflikten in Strafverfahren.

Sofern eine Verständigung darüber, wo ein Verfahren zu führen ist, nicht möglich ist, können sich die deutschen Behörden (wie auch die Behörden der anderen Mitgliedsstaaten) an Eurojust wenden. Eurojust kommt hier die Rolle eines Mediators zu, ohne jedoch eine verbindliche Entscheidung treffen zu dürfen.

Die rechtshilferechtlichen Entscheidungen im EU-Bereich sind auf die Bundesländer übertragen. Daher haben die Bundesbehörden im Zusammenhang mit Fällen von Cyberkriminalität keine praktischen Erkenntnisse in Bezug auf den Rahmenbeschluss 2009/948/JI des Rates vom 30. November 2009 zur Vermeidung und Beilegung von Kompetenzkonflikten in Strafverfahren beizusteuern. Eine amtliche Statistik zur sonstigen Rechtshilfe wird seitens des Bundes nicht geführt.

5.4.3. Gerichtliche Zuständigkeit für in der "Cloud" begangene Cyberstraftaten

Beim Zugriff der Strafverfolgungsbehörden auf in der "Cloud" gespeicherte Daten stellt sich das praktische Problem, dass häufig unklar ist, auf welchem Staatsgebiet die Daten gespeichert sind, mit der Folge, dass der Adressat eines ggf. zu stellenden Rechtshilfeersuchens an den Staat des Datenspeicherortes nicht ermittelt werden kann.

5.4.4. Auffassung Deutschlands zum Rechtsrahmen zur Bekämpfung der Cyberkriminalität

Im Hinblick auf die Frage der Anwendbarkeit deutschen Strafrechts betrachten die staatlichen Behörden das bestehende Regelwerk angesichts der Vielfältigkeit der Regelungen (Territorialitäts-, Flaggen-, passives/aktives Personalitätsprinzip, Taten mit besonderem Inlandsbezug und Weltrechtsprinzip) als ausreichend.

Die Befugnisse deutscher Strafverfolgungsbehörden sind bei Ermittlungsmaßnahmen wie dem Zugriff auf Daten nach dem Souveränitätsprinzip grundsätzlich auf das Territorium der Bundesrepublik Deutschland beschränkt. Allerdings erweist sich das das normale Rechtshilfeverfahren, wie es im Regelfall angewendet wird, oftmals als zu langwierig, um erfolgversprechend zu sein. Ein direkter grenzüberschreitender Datenzugriff, wie er etwa gemäß Artikel 32 des Übereinkommens über Computerkriminalität zulässig ist, erweist sich daher als regelmäßig einzig erfolgversprechender Weg. Im Übrigen ist im Wege der internationalen Rechtshilfe vorzugehen. Zu den praktischen Herausforderungen gehört, dass z. B. nach Artikel 31 Absatz 1 des Übereinkommens über Computerkriminalität der Staat des Datenspeicherortes als Adressat eines Rechtshilfeersuchens vorgesehen ist. Dieser ist jedoch oft gar nicht bekannt, oder weicht vom Staat des Providersitzes ab.

Eine verbesserte internationale polizeiliche und justizielle Rechtshilfe kann nur durch eine internationale über die EU hinausgehende Regelung auf der Grundlage des Übereinkommens über Computerkriminalität erreicht werden. Hilfreich wäre außerdem v. a. eine Verbesserung und Beschleunigung der Kommunikation zwischen den zuständigen Rechtshilfebehörden. Darüber hinaus können sich aufgrund unterschiedlichen nationalen Strafrechts Schwierigkeiten durch etwaige Anforderungen an die beiderseitige Strafbarkeit ergeben.

5.5. Fazit

- **Deutschland hat 2009 das Übereinkommen des Europarates über Computerkriminalität ratifiziert.**

- **Der Rahmenbeschluss 2005/222/JI des Rates über Angriffe auf Informationssysteme und die Richtlinie 2013/40/EU über Angriffe auf Informationssysteme sind in nationales Recht umgesetzt worden.**

- **Auch die Richtlinie 2011/93/EU zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie ist in nationales Recht umgesetzt worden.**

- **Das Strafgesetzbuch ist jüngst geändert worden, um das Übereinkommen von Lanzarote und die Richtlinie 2011/93/EU vollständig umzusetzen. Dabei wurde § 176 Absatz 4 Nummer 3 StGB verbessert, unter den das "Grooming" fällt.**

- **Auf dem gleichen Gebiet wurde jüngst ein Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme angenommen. Es gibt neue Bestimmungen über die Vorratsdatenspeicherung hinsichtlich der Verpflichtung der Internetdiensteanbieter, Verkehrsdaten für 10 Wochen und Standortdaten für 4 Wochen aufzubewahren, wobei strenge Auflagen (aufgelistete schwere Straftaten) gelten, die dem Schutz der Privatsphäre der Bürger dienen. Das neue Gesetz wurde im Dezember 2016 nach dem Evaluierungsbesuch verabschiedet; die Speicherpflicht wird 2017 in Kraft treten.**

- **Die Datenaufbewahrung ist aber nach wie vor ein Thema für die Praktiker, und die diesbezügliche Zusammenarbeit mit anderen Ländern ist problematisch. Eine Lösung sollte wohl auf EU-Ebene gefunden werden.**

- **Einige Praktiker berichteten von praktischen Problemen in Bezug auf § 202a StGB; ihres Erachtens gibt es keine geeigneten rechtlichen Instrumente für Ermittlungen in diesen Fällen. Sie äußerten die Überlegung, dass diese Bestimmung geändert werden sollte, damit erschwerende Umstände beim Besitz riesiger Mengen an gestohlenen Daten gegeben sind. Andererseits erklärten Vertreter des Justizministeriums, dass sie diese Frage geprüft hätten und es ihres Erachtens nicht angemessen sei, derzeit Änderungen an der Rechtslage vorzunehmen.**

- **Der bloße Besitz von Schadsoftware oder Anmeldedaten ist nicht strafbar. Diese Sachverhalte sind nach dem nationalen Recht nur strafbewehrt, wenn sie von einer Person in der Absicht der Selbstbereicherung, der Bereicherung eines Dritten oder der Schädigung eines Dritten begangen werden.**

- **Was das Verfahrensrecht anbelangt, so ermöglicht die deutsche Strafprozessordnung Ermittlungsmaßnahmen. Elektronische Beweismittel werden beschrieben als viele verschiedene Typen von Daten, die mittels Digitaltechnik erzeugt oder gespeichert werden.**

- **Illegal beschaffte Beweismittel werden nicht a priori abgelehnt, sondern vor Gericht bewertet.**

Nach deutschem Recht ist der Direktzugang deutscher Behörden zu ausländischen Anbietern zur Erlangung von Informationen über Teilnehmer zulässig und hängt davon ab, inwieweit dies nach dem Recht des Staates, in dem der Anbieter seinen Sitz hat, zulässig ist; dies funktioniert sehr gut. Einige Praktiker äußerten jedoch den Wunsch nach einem harmonisierten Mechanismus für den Austausch von Informationen über Teilnehmer und für neue Ansätze auf EU-Ebene zur Festlegung der gerichtlichen Zuständigkeit.

- **Betont wurden Probleme bei der Beschaffung von Beweismitteln in der Cloud, und es wurde der Wunsch geäußert, dass dies auf EU-Ebene angegangen wird.**

- **Andere Herausforderungen in Bezug auf Verschlüsselung und grenzüberschreitenden Zugriff auf Daten wurden angesprochen. Die Entschlüsselung ist sehr zeitaufwändig (Monate, gelegentlich sogar Jahre), und bei einer starken Verschlüsselung gibt es keine wirkliche Lösung.**

- **Was die Ermittlungen bei Botnetzen anbelangt, so wurde die Auffassung vertreten, dass einige rechtliche Bestimmungen bestehen sollten, die den Justizbehörden die Befugnis verleihen, in das Botnetz einzudringen, um Beweismittel zu erlangen und anschließend das Netz auszuschalten. Die Möglichkeit der Überwachung des Datenverkehrs von Botnetzen reicht nicht aus, um Cyberkriminalität wirksam zu bekämpfen.**

- **Einigen Praktikern zufolge ist es notwendig, rechtliche Bestimmungen in die Strafprozessordnung aufzunehmen, um den Einsatz von Instrumenten für den Zugang zu krimineller Infrastruktur ("Hacking") zuzulassen. Die Polizeibeamten vertreten die Auffassung, dass die Straftäter ihnen immer einen Schritt voraus sind.**

- **Ferner wurde betont, dass sichere Wege für den Austausch von Informationen, insbesondere auf dem Gebiet der Computerkriminalität, erforderlich sind.**
  In Deutschland sind 18 Kontaktstellen des EJN mit gesicherten E-Mail-Adressen ausgestattet.

6. OPERATIVE ASPEKTE

6.1. Cyberangriffe

6.1.1. Art der Cyberangriffe

Der BSI-Lagebericht aus dem Jahr 2014 zeigt folgende Parameter auf:

Schwachstellen:

- 2014 gab es rund 700 kritische Schwachstellen in den meistverbreiteten Softwareprodukten.
- Für die Gruppe der weit verbreitet genutzten Produkte muss mit einer Erkennung von durchschnittlich zwei kritischen Schwachstellen pro Tag gerechnet werden.
- 2014 gab es bis Juli fünf bekannt gewordene Zero-Day-Schwachstellen.

Schadprogramme:

- Die Gesamtzahl der PC-basierten Schadprogrammvarianten liegt bei mehr als 250 Millionen.
- Die Zahl der Schadprogrammvarianten steigt täglich um rund 300 000.
- In Deutschland kommt es jeden Monat zu mindestens 1 Million Infektionen durch Schadprogramme.
- Betroffen ist mit etwa 95 Prozent vorwiegend Windows.
- Die Anzahl der Schadprogramme für Smartphones und Tablets beträgt mindestens drei Millionen.
- 98 Prozent davon betreffen das Betriebssystem Android.

Botnetze:

- In Deutschland sind mehr als eine Million Internetrechner Teil eines Botnetzes.

Identitätsdiebstahl:

- Millionenfälle im Januar und April: Insgesamt wurden 34 Millionen Identitäten gestohlen.
- Jeden Tag werden mehrere Tausend digitale Identitäten gestohlen.
- Die Anzahl der Schadprogramme für ID-Diebstahl steigt kontinuierlich an. Das BSI analysiert monatlich 11 000 Schadprogramme mit Bezug zu Identitätsdiebstahl in Deutschland.

DDoS:

- 2014 gab es allein in Deutschland über 32 000 DDoS-Angriffe.
- Mehr als ein Drittel der Unternehmen war in den letzten drei Jahren Ziel eines DDoS-Angriffes auf ihre Webseiten.
- Ein Viertel der Unternehmen war von DDoS-Angriffen auf die Netzinfrastruktur betroffen.

Regierungsnetze/Bundesverwaltung:

- Täglich gibt es tausende ungezielte Angriffe auf das Regierungsnetz.
- Durch spezielle Sicherheitsmaßnahmen werden monatlich zusätzlich bis zu 60 000 verseuchte E-Mails in den Netzen der Bundesverwaltung abgefangen.
- 2014 wurden täglich etwa 15 bis 20 hochwertige Angriffe auf das Regierungsnetz entdeckt.
- Durchschnittlich ein gezielter Angriff pro Tag hat einen nachrichtendienstlichen Hintergrund.

6.1.2. Mechanismen zur Abwehr von Cyberangriffen

Die Bewältigung von schweren Cyberangriffen wird durch die IT-Krisenmanagement-Strukturen übernommen.
Das IT-Krisenmanagement in Deutschland findet im Kern im Nationalen IT-Krisenreaktionszentrum (IT-KRZ) beim Bundesamt für Sicherheit in der Informationstechnik (BSI) statt. Das IT-KRZ wächst dabei stufenlos aus dem Nationalen IT-Lagezentrum und Computer Emergency Response Team des Bundes (CERT-Bund) auf. Damit kann lageangemessen durch Heranziehen relevanter Experten und Unterstützungskräfte des BSI über einen skalierbaren Ansatz die sog. "Besondere Lage" bzw. IT-Krise bewältigt werden. Im IT-KRZ werden über ein Stabs-Zellen-Modell, analog zu allgemeinen Krisen- und Katastrophenschutzstäben, alle relevanten Personen zusammengeführt, um organisatorische wie fachliche Aufgaben zu bewältigen.

Es finden einsatztaktische/fachliche Aufgaben wie Lageerfassung, -bewertung, Priorisierung und Maßnahmenempfehlungen statt. Fachexperten aus dem gesamten BSI werden lageangemessen eingebunden und sorgen für eine breite fachliche Expertise. Über die Stabszellen wird die Kommunikation mit den Zielgruppen des BSI, z. B. Behörden sowie Unternehmen aus den Kritischen Infrastrukturen, sichergestellt und eine geeignete Koordinierung von Krisenmanagementprozessen durchgeführt. Pressearbeit und Justiziariat sind ebenso eingebunden wie ggf. Verbindungspersonen zu anderen Behörden, z. B. dem Bundeskriminalamt (BKA), in ihren jeweiligen Aufgabenbereichen. Dies schließt insbesondere Vertreter des Nationalen Cyber-Abwehrzentrums ein, mithilfe derer der Kontakt zu den deutschen Sicherheitsbehörden gehalten wird. Unterstützt wird das IT-KRZ durch die organisatorischen Stabsaufgaben wie Personalmanagement, Logistik und Innerer Dienst.

Sofern neben dem fachlichen Krisenpotential auch eine Ausweitung auf andere Teilgebiete des öffentlichen Lebens bzw. eine politische Komponente hinzukommt, wird der Krisenstab des Bundesministeriums des Innern (BMI) aktiviert. Dieser Stab ist für die allgemeine Bewältigung von Krisen zuständig und damit zusätzlich zu den IT-Krisenaspekten auch noch für weitere möglicherweise davon in Folge von Interdependenzen betroffene Teilbereiche des öffentlichen Lebens, z. B. im Sinne des Bevölkerungsschutzes (Versorgungssicherheit) oder der Terrorabwehr (Täterermittlung). Für das IT-bezogene ministerielle Krisenmanagement ist innerhalb des BMI-Krisenstabes ein eigener Stabsbereich zuständig. Dieser bereitet die IT-Lage, die im IT-Krisenreaktionszentrum des BSI erarbeitet und erstellt wird, ministeriell auf und stellt diese im BMI-Krisenstab dar. Der Stabsbereich dient in seiner grundsätzlichen Ausrichtung als Schnittstelle zwischen dem allgemeinen, strategisch-administrativen Stab im BMI und dem operativ-taktischen (Stab/) IT-KRZ im BSI.

Zur Vervollständigung des Lagebildes ist dabei der Austausch zwischen IT-Lagezentrum des BSI, dem BMI-Lagezentrum und dem Gemeinsamen Melde- und Lagezentrum des Bundes und der Länder (GMLZ) selbstverständlich. Weitere Lagezentren können lageabhängig eingebunden werden.

Vor allem durch das IT-KRZ findet zudem eine Kommunikation und Kooperation mit Fachcommunities im nationalen wie im internationalen Bereich statt. Weltweit haben sich CERT-Verbünde gebildet, deren Ziel die Zusammenarbeit bei IT-Vorfällen ist, einschließlich der gegenseitigen Unterstützung bei der Bewältigung von IT-Lagen. CERT-Verbünde sind mit teils homogener Ausrichtung, z. B. Regierungs-/Behörden-CERTs, vorhanden, teils mit sehr heterogener Zusammenstellung, z. B. mit Teams aus Wirtschaft, Wissenschaft und Behörden. Die unterschiedliche Ausrichtung der Teams und ihrer teils multidisziplinären Zusammenstellung ist explizit als Vorteil zu verstehen, um auf breite Expertise zurückgreifen zu können. Durch die Internationalität wird dies noch unterstützt. Neben dem Tagesgeschäft dienen diese Verbünde auch dem IT-Krisenmanagement, was in diesen Kreisen regelmäßig geübt wird.

Die zivil-militärische Zusammenarbeit im Bereich der IT-Vorfallsbearbeitung und bei CERT-Aufgaben wird auf nationaler Ebene zwischen dem BSI und der Bundeswehr seit Jahren erfolgreich praktiziert. Das BSI ist bei der NATO als National Cyber-Defence Authority gelistet und im Fall eines größeren Cyberangriffs mit staatlichem Hintergrund primäre Kontaktstelle für Deutschland. Das CERT-Bundeswehr ist auf den Schutz der eigenen militärischen Netze ausgerichtet und arbeitet dazu mit den anderen internationalen militärischen CERTs zusammen.

Das IT-KRZ verfügt über langjährig etablierte und geübte Krisenmanagementkanäle in die öffentliche Verwaltung, insbesondere die Bundesverwaltung, und zu den deutschen Unternehmen der Kritischen Infrastrukturen. Über diverse Mechanismen und Kooperationen des BSI kann ein breites Spektrum und das Gros der deutschen Wirtschaft aber auch der Bürger erreicht werden.

Die zur Verfügung stehenden internationalen Kommunikationswege (INTERPOL, Europol, G7, sowie zahlreiche bilaterale Kontakte) werden genutzt. Bei justiziellen Ersuchen wird der formelle Rechtshilfeweg beschritten, der allerdings im dynamischen Phänomen Cybercrime aufgrund der formalen Vorgaben in aller Regel nicht praktikabel und zielführend ist, insbesondere aufgrund der zeitlichen Aufwände und der Erledigungsdauer. Hier erweist sich das G7-24/7 Kontaktpunktnetzwerk als vorteilhaft. Es ist aber nicht geeignet, alle Defizite der Rechtshilfewege zu kompensieren. Daher existieren entsprechende Bestrebungen, den schnellen Informationsaustausch auf polizeilicher Ebene entsprechend auf justizieller Ebene durch direkte Zusammenarbeit der zuständigen Staatsanwaltschaften zu übertragen.

6.2. Maßnahmen gegen Kinderpornografie und sexuellen Missbrauch von Kindern im Internet

6.2.1. Datenbank-Software zum Ausfindigmachen von Opfern und Maßnahmen zur Vermeidung einer erneuten Viktimisierung

Das Bundeskriminalamt betreibt im Rahmen der Zentralstellenfunktion bei der Bekämpfung des sexuellen Missbrauchs von Kindern und Jugendlichen und der Herstellung und Verbreitung von kinder-/jugendpornografischem Bild-/Videomaterial eine nationale Bildvergleichssammlung, um die in diesen Deliktsbereichen anfallenden Informationen zu sammeln und auszuwerten. Neben der nationalen Bildvergleichssammlung, die vom BKA unterhalten wird, nutzt das BKA als nationales Zentralbüro der Bundesrepublik Deutschland auch die "internationale Datenbank über die sexuelle Ausbeutung von Kindern" (ICSE-DB), die vom Generalsekretariat von Interpol unterhalten wird,

Die Bildvergleichssammlung ermöglicht

- die Zuordnung von identifizierten Tätern zu dem von ihnen gefertigten Bild-/Videomaterial mit kinder-/jugendpornografischem Inhalt
- die Abgrenzung zu pornografischen Abbildungen mit Jugendlichen bzw. jungen erwachsenen Darstellern
- den Abgleich von gespeichertem Bild-/Videomaterialmit mit neu sichergestelltem Material
- die Vermeidung von Mehrfachermittlungen aufgrund der Identifizierung von bereits bekannten Tätern bzw. Opfern des sexuellen Missbrauchs
- eine Unterstützung der Beweisführung durch Einführung von bereits früher sichergestelltem Material in ein aktuelles Verfahren

Über einen Abgleich mit dem bereits bekannten kinder-/jugendpornografischen Bildmaterial kann festgestellt werden, inwieweit eine minderjährige Personen als Opfer einer Sexualstraftat bereits bekannt geworden ist.
Zur Vermeidung einer erneuten Viktimisierung werden jugendgefährdende Medien von der Bundesprüfstelle für jugendgefährdende Medien (BPjM) in den Index jugendgefährdender Medien aufgenommen. Die Entscheidung, eine Internetseite in den Index aufzunehmen, ergeht in einem Verfahren, das einem Gerichtsverfahren ähnelt. Zu dem Verfahren gehört eine nichtöffentliche Anhörung vor einem aus 12 Personen bestehenden Gremium. Jede von der Entscheidung unmittelbar betroffene Person (beispielsweise der Herausgeber, Autor oder Verleger) erhält Gelegenheit, teilzunehmen und ihren Standpunkt zu erläutern.

Die BPjM leitet das Verfahren ein (wie oben beschrieben) und nimmt die Internetseite in die Liste bzw. den Index auf, wenn sie als jugendgefährdend eingestuft wird.
Das Jugendschutzgesetz sieht vor, dass indizierte ausländische Internetseiten von nutzerautonomen Filterprogrammen gefiltert werden. Zur Erfüllung dieses gesetzlichen Auftrags nutzt die BPjM das BPjM-Modul. Das BPjM-Modul enthält die indizierten URL, die von anderen Ländern aus verbreitet werden. Es ist kein eigenständiges Filterprogramm, lässt sich jedoch in nutzerautonome Filterprogramme als Filtermodul (Blacklist) für den Jugendschutz integrieren. Die BPjM stellt in Kooperation mit der Freiwilligen Selbstkontrolle (FSM) Herstellern nutzerautonomer Filterprogramme das BPjM-Modul zur Verfügung. Das Modul ermöglicht die Filterung der von der BPjM indizierten ausländischen Internetseiten beispielsweise in Schulen.

Die großen Suchmaschinenbetreiber, die in Deutschland ihren Dienst anbieten, haben sich selbst verpflichtet, indizierte Internetseiten nicht in den Suchergebnissen anzuzeigen. Sie erfüllen diese Selbstverpflichtung bereits seit einigen Jahren.

6.2.2. Maßnahmen zur Bekämpfung der sexuellen Ausbeutung bzw. des sexuellen Missbrauchs im Internet, der Verbreitung sexueller Inhalte über das Internet oder Mobiltelefone (Sexting) und des Cyber-Mobbing

Im Hinblick auf die Bundesländer wurden – ohne Anspruch auf Vollständigkeit – folgende Informationen gemeldet:

Berlin:

Die Anschrift, Telefonnummer und die E-Mailanschrift des Landeskriminalamts (LKA) 13 ist zusammen mit einem Flyer über das Verhalten beim Auffinden von Kinderpornografie im Internet veröffentlicht.

Das Dezernat für Sexualdelikte führt regelmäßig Präventionsveranstaltungen zum sexuellen Missbrauch in Schulen und Kindergärten durch. Die Polizei Berlin verfügt außerdem über eine Internetwache, bei der jederzeit Hinweise und Anzeigen erstattet werden können.

Auch hier gehen häufig Hinweise wegen möglicher Kinderpornografie im Internet ein. Dazu bietet die Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) auf ihrer Internetseite www.polizei-beratung.de diverse Informationshilfen an. Zu nennen wären dazu der Filmspot: "Chatten. *Aber sicher*!" Er weist Kinder auf Sicherheitsregeln beim Chatten hin. Zum anderen bietet der Filmspot "Surfen. Aber sicher!" einen weiteren Baustein zu der Aktion "Kinder sicher im Netz". Der TV-Moderator Rudi Cerne gibt Eltern Tipps, wie sie ihre Kinder vor den Gefahren des Internets schützen können. Beide Spots gibt es sowohl als DVD für den Einsatz vor Ort als auch als Internet-Content. Das comic-artige Heft "Hallo – jetzt reicht's" stellt in kindgerechter Art lebensweltliche Erfahrungen von Kindern, insbesondere zu Gewalt, Mobbing, Erpressung, Sachbeschädigung sowie Chatten im Internet dar und vermittelt dazu Verhaltensregeln. Die Zielgruppe sind Grundschüler/innen.

In dem Faltblatt "Das Netz vergisst nichts" wird in einer Comicgeschichte geschildert, weshalb man von sich und anderen so wenig persönliche Daten wie möglich im Internet preisgeben sollte. Die Zielgruppe sind Kinder und Jugendliche. Das Internetportal "time4teen" unter der Internetadresse www.time4teen.de richtet sein Informationsangebot speziell an junge Menschen. Es enthält Hinweise zu Kriminalitätsgefahren verschiedenster Art, darunter Kindesmisshandlung, Mobbing und sexuelle Gewalt. Weitere Informationshilfen können unter der genannten Internetseite abgefragt werden.

Brandenburg

Die Bereiche Prävention der Polizeiinspektionen führen u. a. Veranstaltungen zum Thema "Neue Medien" für Schüler(innen) der 6. bis 7. Klasse und deren Eltern sowie Lehrkräfte durch. Im Rahmen dieser Präventionsmaßnahme sollen die Adressaten über potenzielle Gefahren im Umgang mit den "Neuen Medien" informiert und zur kritischen sowie verantwortungsvollen Auseinandersetzung mit den Angeboten und Möglichkeiten des Internets befähigt werden. Dabei sollen auch Opfervermeidungsstrategien oder die Täterstrategien, insbes. beim Cybergrooming, thematisiert werden. Innerhalb dieser Veranstaltungen werden auch verschiedene Medien der bundesweiten Programms Polizeiliche Kriminalprävention genutzt.

Mecklenburg-Vorpommern

Im Jahr 2001 wurde erstmals in Mecklenburg-Vorpommern die Onlineplattform "Initiative Sicheres Internet" in Zusammenarbeit mit dem Datenverarbeitungszentrum MV geschaffen. Im Jahr 2010 wurde die Plattform weiterentwickelt und steht seitdem unter www.netzverweis.de als Meldeportal u. a. für Verdachtsfällte der Kinderpornografie und Computerkriminalität zur Verfügung. Dadurch wurde eine direkte Kontaktmöglichkeit zum Dezernat 45/ Cybercrime des Landeskriminalamts (LKA) MV geschaffen.

6.2.3. Präventionsmaßnahmen gegen Sextourismus, pornografische Darbietungen von Kindern und Sonstiges

Durch zwei Gesetzesänderungen in den Jahren 1993 und 1998 wurden die Voraussetzungen dafür geschaffen, dass der durch deutsche Täter im Ausland begangene sexuelle Missbrauch ausländischer Kinder und Jugendlicher in Deutschland bestraft werden kann, selbst wenn die Handlung im betreffenden Staat nicht mit Strafe bedroht ist. Hierzu wurden bestimmte Formen des sexuellen Missbrauchs von Kindern (1993) und Jugendlichen (1998) in den Katalog des § 5 StGB ("Auslandstaten mit besonderem Inlandsbezug") aufgenommen. Somit liegen die Grundvoraussetzungen für eine umfassende Strafverfolgung zumindest deutscher Tatverdächtiger vor, die Sexualstraftaten zum Nachteil von Kindern (gleich welcher Nationalität und ohne Berücksichtigung des Rechtes am Tatort) begehen.

Die Arbeitsgruppe zur Umsetzung des Verhaltenskodexes gegen Kindersextourismus nimmt sich unter Federführung des Deutschen ReiseVerbands e.V. (DRV) und unter maßgeblicher Beteiligung von ECPAT Deutschland (Arbeitsgemeinschaft zum Schutz der Kinder vor sexueller Ausbeutung; NGO), dieser besonderen Erscheinungsform des sexuellen Missbrauchs von Kindern und Jugendlichen seit einiger Zeit an. Bereits vor Jahren entwickelte sie ein gemeinsames Faltblatt zur Sensibilisierung von Urlaubern, das über die Polizei und die in dieser Arbeitsgruppe vertretenen Kooperationspartner weltweit zur Verteilung kommt.

Eine ergänzende Initiative dieser Arbeitsgruppe im Jahr 2010 bestand darin, einen Videospot zur Sensibilisierung der deutschsprachigen Bevölkerung zu veröffentlichen, mit dem Privat- und Geschäftsreisende angesprochen werden sollen, die aufgrund ihres Reiseziels Beobachtungen über Verdachtsfälle machen könnten oder sogar Zeuge von Fällen des sogenannten Kindersextourismus werden, die in Überprüfungen durch die Polizei des betroffenen Landes und ggf. in konkrete Ermittlungsverfahren münden.

Insbesondere ECPAT Deutschland hat sich darum bemüht, dass auch in Deutschland (analog Österreich und der Schweiz) seitens der Bundesbehörden eine zentrale Online-Meldestelle für Urlauber im Ausland eingerichtet und öffentlichkeitswirksam beworben wird, um Meldungen über derartige Fälle entgegenzunehmen und die weitere Bearbeitung im jeweiligen ausländischen Staat zu veranlassen bzw. zu fördern. Zur Erleichterung der Meldung über entsprechende Beobachtungen/Verdachtsfälle wurde – zeitgleich zur Veröffentlichung des Videospots der Arbeitsgemeinschaft zur Umsetzung des Verhaltenskodexes gegen Kindersextourismus anlässlich des Welttourismustages 2010 – beim Bundeskriminalamt (BKA) im September 2010 eine zentrale E-Mailadresse zur Entgegennahme von entsprechenden Hinweisen eingerichtet. Ergänzend wurde ein Kontaktformular auf der Internetseite des BKA (www.bka.de) unter der Rubrik Bürgerkontakt zum Kindersextourismus eingerichtet. Das Formular ist bei Eingabe einschlägiger Begriffe in Suchmaschinen leicht auffindbar und bietet den Vorteil, dass der Meldende "geleitet" wird und so wichtige Angaben nicht vergisst.

Auf europäischer Ebene wurde am 5. März 2014 im Rahmen der Internationalen Tourismusbörse (ITB) die Europäische Meldeplattform geschaltet, welche Reisenden die Möglichkeit bietet, Hinweise von sexuellem Missbrauch an die zuständigen nationalen Stellen weiterzugeben. Die entsprechende deutsche Meldeplattform ist mit dieser ebenfalls verlinkt bzw. direkt unter "www.nicht-wegsehen.net" erreichbar. Eine Verlinkung der Infoseite zum Kindersextourismus des Bundeskriminalamtes und dem dortigen Kontaktformular besteht ebenfalls.

Die Überprüfung der auf der zentralen E-Mailadresse wie auch auf dem Kontaktformular des BKA eingehenden Hinweise erfolgt beim BKA im 24/7-Dienst, um ggf. im Einzelfall erforderliche Sofortmaßnahmen einleiten zu können.

Die Maßnahmen zur Bekämpfung pornografischer Abbildungen von Kindern in Echtzeit richten sich nach den einschlägigen gesetzlichen Grundlagen der Strafprozessordnung bzw. im Einzelfall nach den Rechtsgrundlagen des Telekommunikationsgesetzes bzw. Telemediengesetzes zur Erhebung von Bestandsdaten bei den Internet-Service-Providern.

Im Zuge der anlassunabhängigen Internetrecherche ist es polizeilich möglich, kinder- und jugendpornografische Inhalte im Internet (Chatforen, Tauschbörsen etc.) aufzuspüren und die dafür verantwortlichen Personen ggf. mit Hilfe der Internet-Service-Provider zu ermitteln.

Darüber hinaus können Anhaltspunkte zum sexuellen Missbrauch von Kindern und Jugendlichen bzw. zur Verbreitung kinder- und jugendpornografischer Schriften auch bei der Durchführung sonstiger strafprozessualer Maßnahmen (z. B. Telekommunikationsüberwachung, Durchsuchungen) erlangt und weiterverfolgt werden.

Der Arbeitsbereich Internetrecherche des Landeskriminalamtes Baden-Württemberg verfügt über selbstprogrammierte Software, um in Filesharing-Plattformen das Verbreiten und Downloaden von kinderpornografischen Inhalten verfolgen und beweissicher dokumentieren zu können.

Durch automatisierte Prozesse ist es möglich, bei den Providern sehr zeitnah eine IP-Anfrage zu stellen, sodass es in einer Vielzahl von Fällen möglich ist, die Beschuldigten zu identifizieren.

Deutschland hat drei Hotlines:
Jugendschutz.net (länderübergreifende Stelle für den Jugendmedienschutz)
eco e.V. (Verband der Internetwirtschaft e.V.)
fsm e.V. (Freiwillige Selbstkontrolle deutscher Multimedia-Diensteanbieter)
Alle drei Hotlines sind Mitglieder von INHOPE.
Meldungen an die drei Hotlines und an die Polizei können anonym und online erfolgen.

Zahlreiche Maßnahmen sind ergriffen worden, um einen hohen Bekanntheitsgrad der Hotlines in Deutschland zu erreichen. Dazu gehören Internetseiten, Flyer, Broschüren, Pressemitteilungen, Jahresberichte, Präsentationen über die Arbeit der Hotlines auf nationaler und internationaler Ebene und die Förderung durch den Projektkoordinator Klicksafe.

Führen Internetnutzer eine Suche mit Begriffen im Zusammenhang mit dem sexuellen Missbrauch von Kindern durch, so meldet Google dies den Hotlines der FSM und von Jugendschutz.net.

Bei Inhalten im Zusammenhang mit Kindesmissbrauch, die einer der drei Hotlines gemeldet werden, wird gemäß einer Vereinbarung zwischen dem BKA und den Hotlines wie folgt verfahren:
a) Die Hotline erhält Informationen von der Öffentlichkeit oder von Partnerhotlines über Darstellungen von Kindesmissbrauch.
b) Die Hotline prüft den Inhalt und stellt fest, ob er illegal ist oder nicht.
c) Kommt die Hotline zu dem Schluss, dass das Material strafrechtlich relevant ist, so erstellt sie einen Bericht über den Inhalt (mit Links) und sendet ihn per Email an das BKA.
d) Ist das Material in Deutschland gehostet, so darf die Hotline einen Anbieter, der Mitglied der Hotline ist, erst kontaktieren, nachdem sie dem BKA den Inhalt gemeldet hat. Mit dieser Abfolge werden Risiken für die strafrechtlichen Ermittlungen vermieden. Erforderlichenfalls beschlagnahmt das BKA den einschlägigen Inhalt für die Zwecke des Strafverfahrens.
e) Ist das Material im Ausland gehostet, so wird die Hotline zugleich eine Meldung an den passenden INHOPE-Partner machen, damit das Material so schnell wie möglich entfernt wird. Die Hotlines können darüber hinaus direkt an einen ausländischen Anbieter herantreten, wenn die Meldung auf dem polizeilichen Weg und an die INHOPE-Hotline nicht zum Entfernen des einschlägigen Materials geführt hat.
f) Beim BKA gehen alle Meldungen der drei Hotlines und von nationalen Polizeistellen und außerdem direkt von der Öffentlichkeit ein.

g) Das BKA überprüft bei allen eingehenden Meldungen, ob der Inhalt illegal und nach wie vor online ist.

h) Ist der Inhalt illegal, online und in Deutschland gehostet, so wird wie folgt verfahren, um das Entfernen des Inhalts zu veranlassen:

- Der entsprechende Diensteanbieter wird vom BKA unterrichtet und aufgefordert, den Inhalt zu entfernen, die Nutzerdaten desjenigen mitzuteilen, der den Inhalt hochgeladen hat, usw.
- Das BKA prüft täglich die Verfügbarkeit von Inhalten, die in Deutschland gehostet sind, und tritt an den verantwortlichen Diensteanbieter heran, um das Entfernen des Inhalts zu veranlassen.
- Durchschnittliche Bearbeitungszeit für deutsche Inhalte im Jahr 2014: 1,88 Tage (Erhalt der Meldung durch das BKA bis zum Entfernen des Inhalts durch den Diensteanbieter).

i) Ist der Inhalt illegal, online und im Ausland gehostet, so wird wie folgt verfahren, um das Entfernen des Inhalts zu veranlassen:

aa) Die nationale Polizei des Landes, in dem der Inhalt gehostet ist, wird vom BKA über das 24/7-Netzwerk unterrichtet, damit sie in eigener Zuständigkeit Maßnahmen zum Entfernen ergreift.

bb) Parallel dazu werden alle Inhalte im Ausland über die deutschen Hotlines auch an die INHOPE-Hotline des entsprechenden Landes weitergemeldet.

cc) Das BKA prüft nach der Meldung drei Wochen lang jede Woche die Verfügbarkeit gemeldeter Inhalte und sendet der Polizei des entsprechenden Landes eine Erinnerung, wenn das Material noch abrufbar ist. Ist das Material nach vier Wochen noch abrufbar, so versucht das BKA, mit der Stelle im Ausland einen persönlichen Kontakt herzustellen (beispielsweise telefonisch), um den Fall zu erörtern.

dd) Die Hotlines können einen ausländischen Anbieter direkt kontaktieren, wenn die Meldung auf dem polizeilichen Weg und an die INHOPE-Hotline nicht zum Entfernen des einschlägigen Materials geführt hat.

6.2.4. Akteure und Maßnahmen gegen Websites, die Kinderpornografie enthalten oder verbreiten

Deutschland ist bestrebt, für das prompte Entfernen von Darstellungen des sexuellen Missbrauchs von Kindern zu sorgen. Nach deutschem Recht sind Zugangsanbieter und Anbieter von Hostdiensten nicht verpflichtet, Filter für kinderpornografisches Material anzuwenden. Eine solche Verpflichtung stünde nicht im Einklang mit Artikel 15 der Richtlinie 2000/31/EG.

Zugangsanbieter, Cacheanbieter und Anbieter von Hostdiensten sind in der Regel nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen (§ 7 Absatz 2 des Telemediengesetzes). Ist jedoch ein Anbieter von Hostdiensten über illegale Inhalte, die bei seinem Dienst gespeichert sind, unterrichtet, so kann er für illegale Inhalte zur Verantwortung gezogen werden, wenn er nicht unverzüglich Maßnahmen zum Entfernen solcher Inhalte ergreift. Das Meldesystem nach Abschnitt 5.A.5 beruht auf diesem Mechanismus.

Das Bundeskriminalamt hat im Jahr 1995 die "Zentralstelle Kinderpornografie" eingerichtet, um bundesweit und koordiniert kinderpornografische Inhalte auszuwerten. Der Deliktsbereich sexueller Missbrauch von Kindern sowie Besitz, Verbreitung und Herstellung von Kinderpornografie ist seit dem Jahr 2009 deliktisch-phänomenologischer Schwerpunkt des Bundeskriminalamts, was dazu führte, dass die ursprüngliche "Zentralstelle Kinderpornografie" von einem Sachgebiet in ein Referat mit rund 20 Polizeibeamten umgewandelt wurde.

Parallel zur Einrichtung der "Zentralstelle Kinderpornografie" im Bundeskriminalamt richteten die Bundesländer "Ansprechstellen Kinderpornografie" bei den jeweiligen Landeskriminalämtern ein, um zum einen dem Phänomen aufgrund fortschreitender Technisierung durch Spezialisierung Rechnung zu tragen, zum anderen um den direkten und umfassenden Informationsaustausch auf nationaler Ebene zu gewährleisten. Unterhalb der "Ansprechstellen Kinderpornografie" bei den Landeskriminalämtern sind die jeweiligen Fachdienststellen bei den örtlichen Polizeipräsidien angesiedelt, welche ebenfalls auf die Bearbeitung entsprechender Ermittlungsverfahren spezialisiert sind.
Ohne Anspruch auf Vollständigkeit wurde von den Ländern Folgendes berichtet:

Baden-Württemberg:

Im Bereich der Staatsanwaltschaften sind in jeder Behörde einige Beamte schwerpunktmäßig, aber nicht ausschließlich mit der Bearbeitung von Kinderpornografie befasst. Bei einer Staatsanwaltschaft besteht entsprechend Nummer 223 RiStBV eine Sonderzuständigkeit insbesondere für die Verfahren wegen des Besitzes und der Verbreitung kinderpornografischer Schriften, die in der Jugendabteilung in zwei Dezernaten (jeweils hälftig mit wechselseitiger Vertretung) angesiedelt ist. Für diese Spezialzuständigkeit sind jeweils etwa 30 bis 40 Prozent des Arbeitskraftanteils zu veranschlagen. Bei einer anderen Staatsanwaltschaft ist für Fälle der Kinderpornografie ausschließlich ein spezielles Dezernat zuständig. Dort werden aber darüber hinaus auch sonstige Sexualstraftaten zum Nachteil von Kindern und Jugendlichen sowie Umweltdelikte und Straftaten nach dem Tierschutzgesetz bearbeitet. Die staatsanwaltschaftlichen Dezernenten dieser Sonderdezernate verfügen jeweils über die allgemeinen Befugnisse eines Staatsanwalts. Bei der Generalstaatsanwaltschaft Stuttgart ist die Zentralstelle zur Bekämpfung gewaltdarstellender, pornografischer und sonstiger jugendgefährdender Schriften eingerichtet.

Beim Landeskriminalamt (LKA) Baden-Württemberg werden regelmäßig Operationen zur Bekämpfung von Kinderpornografie im Internet von spezialisierten Beamten der Inspektion 510 durchgeführt. Zudem ist dort eine Ansprechstelle Kinderpornografie eingerichtet. Bei einem Kriminalkommissariat ist derzeit ein Kriminalbeamter ausschließlich mit der Bearbeitung von Verfahren aus dem Bereich der Kinderpornografie befasst. Er wird zeitweise unterstützt durch weitere Beamte des zuständigen Dezernates. Die Sicherung der bei Durchsuchungen beschlagnahmten Speichermedien und das Überspielen der Dateien auf zur Auswertung geeignete Datenträger wird jedoch durch ein gesondertes Dezernat ("ITB") innerhalb der Kriminalinspektion 5 einer Kriminalpolizei vorgenommen. Dieses Dezernat besteht aus insgesamt elf Personen. Es ist jedoch nicht nur für solche Delikte zuständig, sondern generell für die Auswertung von Speichermedien.

Derzeit liegt die Dauer, die für diese Auswertung benötigt wird, bei ca. sieben Monaten. Auch bei der einer anderen Staatsanwaltschaft zuarbeitenden Polizei gibt es eine korrespondierende Spezialzuständigkeit der Kriminalpolizei im Dezernat für Sexualdelikte, bei der nach der aktuellen Polizeireform vier Kriminalbeamte (drei Vollzeitkräfte und eine Halbtagskraft) für den Bereich des gesamten Polizeipräsidiums zuständig sind. Daneben gibt es bei der dortigen Kriminalpolizei für die Auswertung von Datenträgern einen Fachbereich "ITB – Internet / Beweissicherung", bei der ein Kriminalhauptkommissar vorrangig für den Bereich Kinderpornografie zuständig ist.

Bayern:

Spezialisierte Einheiten, die ausschließlich mit Kinderpornografie befasst sind, bestehen nicht. Soweit Ermittlungen mit Internetbezug aber besondere rechtliche und technische Schwierigkeiten aufwerfen, werden derartige Verfahren durch die seit 1. Januar 2015 neu geschaffene Zentralstelle Cybercrime Bayern (ZCB) bei der Generalstaatsanwaltschaft Bamberg bearbeitet.
Für eine Staatsanwaltschaft werden die Delikte der Kinderpornografie bei einem speziellen Dezernat des Polizeipräsidiums bearbeitet, das aus ca. 15 Ermittlungsbeamten besteht und darüber hinaus auch für sonstige Sexualstraftaten zum Nachteil von Kindern, Jugendlichen und Erwachsenen zuständig ist.

Berlin:

Das Landeskriminalamt Berlin verfügt über ein Kommissariat, das ausschließlich mit der Bearbeitung von Ermittlungsverfahren wegen Kinder- und Jugendpornografie und des dokumentierten sexuellen Missbrauchs von Kindern und Jugendlichen sowie der Verbreitung von Pornografie zuständig ist. Derzeit besteht das Kommissariat aus 23 Mitarbeitern
(18 Kriminalbeamte, 1 Verwaltungsbeamter und 4 Tarifbeschäftigte. Bei der Staatsanwaltschaft Berlin werden Straftaten nach den §§ 184 bis 184d StGB in einer Spezialabteilung verfolgt.

Bremen:

Bei der Staatsanwaltschaft Bremen gibt es zwei Sonderdezernate für die Bekämpfung von Kinderpornografie. Bei der Polizei Bremen besteht eine Sonderzuständigkeit beim Kommissariat für Sexualdelikte. Dort werden Ermittlungsverfahren im Bereich von Kinderpornografie von vier Polizeibeamten bearbeitet, die jedoch zusätzlich auch noch allgemeine Sexualdelikte bearbeiten.

Hamburg:

Beim Landeskriminalamt Hamburg besitzt das Fachkommissariat LKA 541 (Cybercrime, Ermittlungen) u. a. die zentrale Zuständigkeit für Straftaten der Verbreitung von Kinderpornografie. Das LKA 541 fungiert als zentrale Ansprechstelle für Kinderpornografie (mit Melde und Auswertungsaufgaben) sowie als Ermittlungseinheit für die kriminalpolizeiliche Sachbearbeitung. Für diese Aufgabe stehen sechs Kriminalbeamte und eine Angestellte zur Verfügung.

Die Schwerpunktabteilung der Staatsanwaltschaft Hamburg ist auch für die Bearbeitung der Verfahren im Zusammenhang mit der Bekämpfung von Kinderpornografie zuständig.

Hessen:

Spezialisierte Einheiten, die sich ausschließlich der Bekämpfung der Kinderpornografie widmen, sind in Hessen nicht vorhanden. Allerdings verfügt jede Staatsanwaltschaft über einen oder mehrere Sonderdezernenten, die als Teil ihres Dezernates die sog. Jugendmedienschutzverfahren bearbeiten.

Darüber hinaus wird in der Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) eine Vielzahl sogenannter Umfangsverfahren aus dem Bereich der Kinderpornografie bearbeitet. Die Zentralstelle ist in diesen Umfangsverfahren als unmittelbarer Ansprechpartner des Bundeskriminalamtes tätig und wird in diesen Verfahren als "Identifizierungs-Staatsanwaltschaft" tätig. Nach Täterermittlung gibt sie die Verfahren gegen außerhessische Beschuldigte an die örtlich zuständigen Staatsanwaltschaften ab. Insgesamt wurden in der Zentralstelle seit dem Tätigwerden im Jahre 2010 mehrere tausend Verfahren gegen Beschuldigte wegen Besitzes und Verbreitung kinderpornografischer Schriften eingeleitet. Auch Fahndungsmaßnahmen zur Identifizierung von Opfern und Tätern sexuellen Missbrauchs, der in kinderpornografischen Schriften dargestellt wird, ist regelmäßige Aufgabe der ZIT. So wurden im Rahmen von Fahndungsmaßnahmen, insbesondere Öffentlichkeitsfahndungen, eine Reihe von Missbrauchstätern identifiziert. In der Zentralstelle wurden seit dem Tätigwerden im Jahre 2010 mehrere tausend Verfahren gegen Beschuldigte wegen Besitzes und Verbreitung kinderpornografischer Schriften geführt.

Mecklenburg-Vorpommern:

Im Bereich der Justiz des Landes Mecklenburg-Vorpommern sind keine spezialisierten Einheiten zur ausschließlichen Verfolgung von Kinderpornografie eingerichtet. Ermittlungs- und Strafverfahren, welche den Vorwurf des Herstellens, Besitzens oder Verbreitens von Kinderpornografie zum Gegenstand haben, werden als Jugendschutzdelikte in den Jugendabteilungen der Staatsanwaltschaften in gesonderten Dezernaten bearbeitet. Sofern im Zusammenhang mit der Verbreitung über das Internet besondere Kenntnisse der Computertechnik erforderlich sind, leistet die Schwerpunktstaatsanwaltschaft IuK Ermittlungsunterstützung.

Niedersachsen:

Die landesweit zuständige Zentralstelle zur Bekämpfung gewaltdarstellender, pornografischer oder sonst jugendgefährdender Schriften, die bei der Staatsanwaltschaft Hannover angesiedelt ist, befasst sich neben den Verfahren wegen des Besitzes u. a. auch mit Verfahren wegen strafbarer Verbreitung allgemeiner Pornografie (§ 184 StGB), Gewalt- und Tierpornografie (§ 184a StGB) und Gewaltdarstellung (§ 131 StGB). Der Schwerpunkt der Tätigkeit liegt allerdings eindeutig auf der Verfolgung von Straftaten wegen Besitzes und Verbreitung von kinder- und jugendpornografischen Schriften. Die Verfahren aus dem Bereich der Kinderpornografie werden in der Zentralstelle für ganz Niedersachsen bearbeitet. Hier sind die üblichen Zentralstellenbefugnisse geben. Die Zentralstelle verfügt über einen Abteilungsleiter und fünf Dezernenten, welche allerdings nur zur Hälfte der Zentralstelle zugeordnet sind und mit der anderen Hälfte der Arbeitskraft Sexualstrafsachen bearbeiten. Im Jahr 2013 wurden in der Zentralstelle mehr als 3 500 Verfahren gegen namentlich bekannte Tatverdächtige bearbeitet. Bei den Verfahren handelte es sich ganz überwiegend um Straftaten wegen des Verdachts des Besitzes und Verbreitung von kinder- und jugendpornografischen Schriften.

Rheinland-Pfalz:

Bei allen Staatsanwaltschaften des Landes sind Sonderdezernate eingerichtet. Die damit befassten Dezernentinnen und Dezernenten bearbeiten in der Regel noch andere Sachgebiete. So werden teilweise Verfahren wegen Kinderpornografie (im Internet) von den Dezernentinnen und Dezernenten des Sonderdezernats "Sexualstraftaten/ Pornografie" bearbeitet, in deren Zuständigkeit daneben sämtliche Straftaten gegen die sexuelle Selbstbestimmung fallen.

Bei der Generalstaatsanwaltschaft Koblenz ist außerdem die Zentralstelle des Landes Rheinland-Pfalz zur Bekämpfung jugendgefährdender Schriften eingerichtet worden. Der hierfür zuständige Dezernent nimmt ebenfalls noch weitere Aufgaben wahr. Die Zentralstelle führt keine eigenen Ermittlungen durch, sondern nimmt Prüfaufgaben von übergeordneter Bedeutung, die Sammlung von Entscheidungen und eine gewisse Koordinierungsfunktion zwischen den Staatsanwaltschaften wahr.

Auch die Polizei des Landes Rheinland-Pfalz verfügt über keine spezialisierte Einheit, die sich ausschließlich mit dem Phänomen Kinderpornografie beschäftigt. Im Rahmen der Zentralstellenfunktion ist im Dezernat 44 des Landeskriminalamtes Rheinland- Pfalz (Gewaltdelikte/Delikte gegen Frauen und Kinder) die Ansprechstelle Kinderpornografie eingerichtet. Im Dezernat 44 werden ferner Gewalt-, Tötungs-, Waffen- und Sexualdelikte, Gewalt in engen sozialen Beziehungen, Stalking sowie Gewalt gegen Polizeibeamtinnen und Polizeibeamte bearbeitet, sowie die Verbunddatei "vermisste und unbekannte Tote" betreut.

Darüber hinaus werden dem Bereich der Kinderpornografie zuzuordnende Delikte bei den regionalen Kriminalinspektionen der Polizei des Landes Rheinland-Pfalz in den dortigen Kommissariaten 2 (Sexualdelikte/Delikte gegen Frauen und Kinder) bearbeitet.

Sachsen:

Bei den Staatsanwaltschaften werden Verfahren, die Kinderpornografie zum Gegenstand haben, durch mehrere Dezernentinnen und Dezernenten bearbeitet. Deren Anzahl ist abhängig vom Verfahrensaufkommen und umfasst je nach Staatsanwaltschaft zwischen ein und drei Dezernentinnen und Dezernenten. Diese haben jeweils keine ausschließliche Zuständigkeit für die Verfolgung der Kinderpornografie, sondern sind auch für andere Ermittlungsverfahren zuständig.

Sachsen-Anhalt:

Das Ministerium für Justiz und Gleichstellung hat eine zentrale Dienststelle zur Bekämpfung der Darstellung von Gewalt, Pornografie und anderen jugendgefährdenden Inhalten in den Medien eingerichtet, die der Staatsanwaltschaft Halle (Saale) angegliedert ist. Diese Dienststelle ist für das gesamte Bundesland zuständig.

Thüringen:

Im Landeskriminalamt (LKA) Thüringen befindet sich im Dezernat 64 die Zentrale technische Auswertestelle zur Bekämpfung der Kinder- und Jugendpornografie (ZASt). Diese ist mit 6 Dienstposten unterlegt. Im Fachkonzept der Thüringer Polizei zur Bekämpfung von Delikten der Kinder- und Jugendpornografie im Freistaat Thüringen sind die Befugnisse und Zuständigkeiten geregelt.

6.3. On-line-Kartenbetrug

6.3.1. Online-Meldung

Die Bürger melden im Regelfall, wenn sie Opfer von Kartenbetrug im Internet geworden sind. Private Unternehmen melden es nicht immer und die Betreiber der Karten melden es fast nie.

Gründe dafür sind folgende.
Der Bürger stellt fest, dass von seinem Kreditkartenkonto/Girokonto unberechtigte Transaktionen durchgeführt wurden; um dies zu klären, setzt er sich im Regelfall als erstes mit seinem Geldinstitut in Verbindung. Im Regelfall wird der Bürger dann von der Bank aufgefordert, eine Anzeige zu erstatten. Zusätzlich sieht der Bürger den Missbrauch seiner Daten subjektiv als eine sehr schwere und ernsthafte Bedrohung an.

Private Unternehmen zeigen den Kartenbetrug bedeutend weniger an, weil sie im Regelfall nur mittelbar von dem Kartenbetrug betroffen sind. Bei ihnen werden Waren und Leistungen mittels widerrechtlich erlangter Kartendaten bestellt. Da sie oftmals von den Kreditkartengesellschaften entschädigt werden, liegt kein besonderes Interesse an einer Strafverfolgung vor. Verluste die trotzdem gemacht werden, sind genauso eingepreist wie die Diebstähle in einem normalen Ladengeschäft.

Die Betreiber der Karten, ob Banken oder die Gesellschaften selbst, erstatten fast nie Anzeigen. Jede Anzeige würde ein negatives Image der Kreditkarte bedienen, was nicht im Interesse der Banken und Gesellschaften liegt.

Über das Dunkelfeld liegen in diesem Phänomenbereich keine fundierten Kenntnisse vor; allerdings besagt eine regionale Studie in Niedersachsen, dass im gesamten Phänomenbereich "Cybercrime" lediglich 9 % der Straftaten angezeigt werden.

Gründe dafür, dass keine Meldung des Betrugsopfers erfolgt, könnten sein:

- Kauf von Zugängen zu illegalen oder pornografischen Inhalten
- Kauf von illegalen Waren (z. B. Drogen, apothekenpflichtige Medikamente)
- Geringfügigkeit des Betrages
- Angst vor Prestigeverlust bei Privatunternehmen

6.3.2. Rolle der Privatwirtschaft

Im Bereich Online-Kartenbetrug erfolgt die Zusammenarbeit des Bundeskriminalamtes (BKA) mit der Privatwirtschaft auf vielfältige Art und Weise. Beispielhaft sind hier die Zusammenarbeit mit dem Arbeitskreis Sicherheit "Debit- und Kreditkarten in Deutschland" und die Nationale Kooperationsstelle Cybercrime, insbesondere die "institutionalized Public-Private-Partnership" (**iPPP**) zu nennen. Im Zusammenhang mit der Erhöhung der Sicherheit beim Zahlungskarteneinsatz erfolgt eine Kooperation mit Wirtschaftsunternehmen in den Bereichen Verhinderung der Manipulation von POS-Terminals und Geldausgabeautomaten sowie im Zusammenhang mit dem Wechsel von Magnetstreifen- auf Chiptechnologie.

Daneben arbeiten auch die Strafverfolgungsbehörden der Länder zur Bekämpfung und Aufklärung von Straftaten des Online-Kartenbetrugs mit Unternehmen, insbesondere mit Banken, auf vielfältige Art und Weise zusammen. Beispielhaft – ohne Anspruch auf Vollständigkeit – wird die Zusammenarbeit der Strafverfolgungsbehörden mit Unternehmen in den Ländern Brandenburg und Sachsen-Anhalt geschildert:

Im Bundesland **Brandenburg** wurde bei dem Polizeipräsidium Fachdirektion Landeskriminalamt (FD LKA) die Zentrale Ansprechstelle Cybercrime für Unternehmen, Einrichtungen und Bürger eingerichtet. Sie ist zugleich Single Point of Contact (SPoC).

Die FD LKA nimmt u. a. regelmäßig an Veranstaltungen der Industrie- und Handelskammern des Landes Brandenburg teil, um auf diesem Wege Erkenntnisse zu polizeilich bekannt gewordenen Cybercrime-Phänomenen mitzuteilen, Kontakte zu Partnern aus der Wirtschaft und IT-Branche zu knüpfen bzw. Erfahrungen zur IT-Sicherheit in Unternehmen auszutauschen.

Im Bundesland **Sachsen-Anhalt** arbeitet die Polizei im Rahmen der Ermittlungen bei der Bekämpfung von Straftaten in diesem Deliktsfeld eng mit der Firma EURO-Kartensysteme GmbH als Gemeinschaftsunternehmen (Service- und Kompetenzzentrum) im Bereich des kartengestützten Zahlungsverkehrs der deutschen Kreditwirtschaft zusammen. Anfragen werden aber auch an die einzelnen Kreditkartenunternehmen gerichtet. Eine Beantwortung seitens der Kreditkartenunternehmen erfolgt jedoch nicht in jedem Fall. Einmal jährlich führt der Arbeitskreis Sicherheit der Kartenorganisationen in Deutschland eine praxisbezogene Fachtagung zum Thema Zahlungskartenkriminalität durch, bei der zeitnah neue Modi Operandi und Sicherheitsstrategien vermittelt werden. Zum Teilnehmerkreis gehören neben Ermittlungsbeamten der Fachdienststellen der Kriminalpolizei der Länder und des BKA auch Vertreter der Kartenindustrie sowie Sicherheitsunternehmen. Des Weiteren findet quartalsweise auf freiwilliger Basis mit dem o. g. Teilnehmerkreis ein Stammtisch zum Zwecke des Informationsaustausches statt. Seitens der Polizei und den Vertretern der Kartenindustrie sowie den Geldautomaten-/Terminalherstellern besteht ein intensiver Informationsaustausch. Speziell ausgebildete oder geschulte Mitarbeiter der Kreditkarteninstitute entwickeln eigene Sicherheitskonzepte. Sie arbeiten eng mit der Polizei zusammen und sind für die Polizeibehörden jederzeit ansprechbar. Die Öffentlichkeit wird seitens der Polizei mit entsprechendem Präventionsmaterial sensibilisiert. Beispielsweise soll durch die Veröffentlichung von Kurzfilmen das Sicherheitsbewusstsein verstärkt werden.

Auf Anfragen führen Polizeibeamte Schulungen in Geldinstituten durch. Die europaweite Einführung der EMV-Chiptechnologie sowie die grundsätzliche Deaktivierung der Magnetstreifen auf Debitkarten seitens der Geldinstitute erhöhten die Sicherheit im Zusammenhang mit Skimmingangriffen auf deutsche Geldautomaten enorm. Dadurch werden die Einsatzmöglichkeiten gefälschter Karten zunehmend erschwert. Auf die Genehmigung von Online-Transaktionen haben die Strafverfolgungsbehörden keinen Einfluss. Auch hier wird im Rahmen der Prävention auf den sensiblen Umgang beim Bezahlen im Internet hingewiesen. Grundsätzlich verhalten sich die Banken bei der Anzeigenerstattung relativ restriktiv, zumal die Schäden durch die missbräuchliche Verwendung von Kartendaten nur einen Bruchteil des Gesamtumsatzes ausmachen.

6.4. Sonstige Phänomene der Cyberkriminalität

Von den meisten Ländern wurde die technische und personelle Ausstattung der Strafverfolgungsbehörden als zufriedenstellend empfunden. Schwierigkeiten bestehen hier vor allem bei der Auswertung von Datenträgern mit großen Datenmengen. In vielen Verfahren werden inzwischen auf Rechnern von Beschuldigten Daten im Bereich von Terabyte sichergestellt. Die hier notwendige Auswertung ist einerseits technisch sehr aufwändig und benötigt andererseits häufig eine längere Zeit, sodass es hier zu Verzögerungen im Verfahrensabschluss kommen kann.

Konkrete Maßnahmen des Bundeskriminalamtes sind u. a. die Zusammenarbeit mit den Herstellern bzw. Betreibern von Zahlungsterminal (POS und GAA).

Im Saarland werden im konkreten Fall an alle saarländischen Banken über den Genossenschaftsverband der saarländischen Bank sog. Bankenwarnungen veranlasst. Auch werden die zuständigen saarländischen Dienststellen aufgrund der Zentralstellenfunktion dieser Dienststelle über bundesweite Erkenntnisse in diesem Bereich informiert und sensibilisiert.

6.5. Fazit

- **Die deutschen Behörden haben zu Cyber-Angriffen mitgeteilt, dass die Bedrohung durch Ransomware in Deutschland sehr hoch ist. Es kommt zu großangelegten Angriffen, bei denen Spam, Exploit-Kits und die Schwachstellen von Servern insbesondere bei Anbietern mobiler Dienste genutzt werden. Etwa 60 % der Unternehmen waren in den vergangenen Jahren Opfer von Cyber-Angriffen.**

- **Das BSI (CERT) bietet einen Dienst, der an sieben Tagen rund um die Uhr zur Verfügung steht, und weitere Meldewege (Telefon, Email, Fax, Webseiten).**

- **Das BSI (CERT) ist zuständig für das IT-Netz der öffentlichen Verwaltung, und es besteht eine sehr gute Zusammenarbeit mit verschiedenen anderen Einrichtungen (aktive Unterrichtung, Austausch bewährter Praktiken, gemeinsame Bewältigung von Vorfällen).**

- **Das BSI unterrichtet das BKA auf freiwilliger Basis über Vorfälle, die Straftaten der Cyberkriminalität darstellen könnten; das BKA und/oder die LKÄ ist/sind dann gesetzlich verpflichtet, Ermittlungen einzuleiten.**

- **Das BKA und das BSI haben mit privaten Partnern aus dem Bankensektor und der Antivirus-Branche eine iPPP mit der Bezeichnung G4C eingerichtet, um die Cyberkriminalität zu bekämpfen.**

- **Beim BKA ist rund um die Uhr Personal in Bereitschaft, um im Falle von Cyberangriffen/-vorfällen im Zusammenhang mit kritischen Infrastrukturen und/oder Bundeseinrichtungen rasch reagieren zu können.**

- **Alle zwei Jahre wird eine bundesweite Cyber-Übung zu spezifischen Themen organisiert. Die Polizei kann als Beobachter an diesen Cyber-Übungen teilnehmen.**

- **Unternehmen in Deutschland sind bisweilen zurückhaltend, wenn es um die Meldung von Vorfällen der Cyberkriminalität an die Polizei geht, da sie einen Vertrauens- oder Prestigeverlust befürchten. Um zu Meldungen anzuregen, betonen die Polizeibehörden, dass die Ermittlungen geheim geführt und gute Ergebnisse erzielt werden können, ohne dass der Ruf der Unternehmen geschädigt wird.**

- **Im Bereich des Online-Kartenbetrugs existiert eine informelle Gruppe, die sich auf persönliche Kontakte stützt und mit verschiedenen einschlägigen Akteuren (BKA, private Partner) praxisbezogene Treffen durchführt.**

- **Bei der Bekämpfung von Darstellungen von Kindesmissbrauch im Internet wendet Deutschland nicht das Konzept der Zugangssperre an. Die Löschung wird als der effizientere Ansatz befürwortet. Dem Bundestag wird alljährlich ein Bericht über die Effizienz der Löschung von Internetseiten, die Darstellungen von Kindesmissbrauch enthalten, vorgelegt.**

- **Im Hinblick auf Maßnahmen zur Vermeidung einer erneuten Viktimisierung erklärten die deutschen Behörden, dass es eine Vereinbarung über Hotlines für die Bekämpfung der sexuellen Ausbeutung von Kindern gibt.**

- **Mit einem bundesweiten Datenbankprojekt wird insbesondere auf das Dunkelfeld im Deliktsbereich sexueller Missbrauch von Kindern abgezielt. Das Projekt stützt sich auf Hotlines und darüber hinaus auf eine Zusammenarbeit auch mit der Privatwirtschaft.**

- **Die deutschen Behörden nutzen Schlüsselwörter für die automatische Bilderkennung, um Darstellungen von Kindesmissbrauch zu erkennen. Ein aktuelles Projekt, das in zwei Jahren abgeschlossen werden soll, wird es ermöglichen, geschlechtsbetonte Körperhaltungen zu erkennen, nicht jedoch die Person selbst (die Identität), wobei jedoch eine Überprüfung in der Interpol-Datenbank und mit der Privatwirtschaft erfolgt.**

- **Als gute Praxis sollte Folgendes hervorgehoben werden: Wenn die Polizei das Opfer nicht anhand der Datenbank identifizieren kann, jedoch hinsichtlich der möglichen Identität eines Kindes einen begründeten Verdacht hat, so gibt sie ein oder zwei Fotos des Opfers zur Identifizierung an Schulen weiter.**

- **Eine Zentralstelle für die Prävention von Kindersextourismus organisiert außerdem Sensibilisierungskampagnen.**
  Im Jahr 2010 wurde ein Projekt unter Beteiligung von Nichtregierungsorganisationen, Strafverfolgungsbehörden und Vertretern der Tourismusbranche aus AT, DE, IT, FR, NL, PL und der Schweiz entwickelt, damit ein grenzüberschreitender Koordinierungsmechanismus zur Verfügung steht. Ein bundesweites Netzwerk ermöglicht einen Informationsaustausch zwischen wichtigen Akteuren (BKA, Tourismusverbände) und Sensibilisierungsmaßnahmen.

- **Auf der Website des BKA steht ein Link zur Verfügung, unter dem Fälle von Sextourismus gemeldet werden können.**

- **Sensibilisierungskampagnen zum Thema sexueller Missbrauch von Kindern werden darüber hinaus vom Bundesministerium für Familie, Senioren, Frauen und Jugend und vom Bundesministerium für Bildung und Forschung organisiert.**

- **Eine weitere vorbildliche Vorgehensweise ist, dass Polizeibeamte anonym oder in Gruppensitzungen eine psychologische oder ähnliche Beratung in Anspruch nehmen können. Alle Bewerber werden bewertet, bevor sie zu Fachbeamten für die Bekämpfung sexuellen Missbrauchs von Kindern werden; es gibt jährliche psychologische Tests und es sind Strategien für die spezifischen Stressfaktoren entwickelt worden.**

7. INTERNATIONALE ZUSAMMENARBEIT

7.1. Zusammenarbeit mit EU-Agenturen

7.1.1. Formelle Anforderungen für die Zusammenarbeit mit Europol/EC3, Eurojust und ENISA

Die Zusammenarbeit von nationalen Behörden und Eurojust bei der Ermittlung von Cyberstraftaten erfolgt auf der Grundlage des Gesetzes zur Umsetzung des Beschlusses (2002/187/JI) des Rates vom 28. Februar 2002 über die Errichtung von Eurojust zur Verstärkung der Bekämpfung der schweren Kriminalität auf die gleiche Weise wie bei der Zusammenarbeit zur Ermittlung von anderen Straftaten. Formelle Anforderungen oder besondere Verfahren zur Zusammenarbeit mit Eurojust sind nach dem innerstaatlichen Recht nicht vorgesehen.

Grundsätzlich kann sich jede Staatsanwaltschaft, jedes Gericht und jede Polizeibehörde, die/das Fragen im Zusammenhang mit der Bearbeitung einer Strafsache mit internationalem Bezug hat, unmittelbar – und selbstverständlich in deutscher Sprache – an den deutschen Tisch bei Eurojust wenden. Dies kann per Telefon, Fax, E-Mail, auf dem Postweg oder auch persönlich erfolgen.

7.1.2. Bewertung der Zusammenarbeit mit Europol/EC3, Eurojust und ENISA

Eurojust war bereits mehrfach bei der Bearbeitung von grenzübergreifenden Ermittlungen als Koordinierungsstelle eingebunden:

So wurde Eurojust von der Hessischen Zentralstelle zur Bekämpfung der Internetkriminalität in einem Verfahren beteiligt und hat daraufhin koordinierende Unterstützung geleistet, die dazu geführt hat, dass an einem Tag weltweit aufeinander abgestimmte prozessuale Maßnahmen durchgeführt werden konnten (http://www.eurojust.europa.eu/press/PressReleases/Pages/2014/2014-05-19.aspx).

Hierfür hat Eurojust drei Koordinierungstreffen organisiert. Die Zusammenarbeit mit Eurojust war insgesamt vorbildlich. Weiterhin wurde Eurojust unterstützend in einem Verfahren einer deutschen Staatsanwaltschaft tätig (Ermittlungsverfahren wegen Betrugs durch Versenden von Phishing Mails), in dem bei einem Koordinierungstreffen unter Beteiligung des EC3 die weitere Zusammenarbeit sowie die Frage, wer gegen welchen Beschuldigten weiter ermitteln wird, geklärt wurde. In einem weiteren Fall (Ermittlungsverfahren wegen Betruges mittels Ransomsoftware/Banking Trojaner) koordinierte Eurojust eine Vielzahl von Rechtshilfeersuchen. Zudem wurde hier die Möglichkeit der Bildung einer gemeinsamen Ermittlungsgruppe besprochen.

In Baden-Württemberg wurden in drei derzeit laufenden Verfahren Daten mit Europol bzw. dem dort angesiedelten "European Cybercrime Centre" (EC3) ausgetauscht, wobei es zu verfahrensbezogenen Besprechungen mit entsprechendem Informations- und Datenaustausch kam, nachdem über sog. "Cross-Match-Reports" Zusammenhänge zwischen einzelnen Verfahren festgestellt werden konnten. In einem Verfahren wurde eine gemeinsame Ermittlungsgruppe bzw. ein Joint Investigation Team (JIT) geführt.

In dem bundesweiten Sammelverfahren der "Ermittlungsgruppe Nerd" des Landeskriminalamtes Niedersachsen haben insgesamt drei jeweils vom EC3 organisierte Treffen zum europaweiten Problem von Ransomware stattgefunden. An diesen Treffen haben Polizeibedienstete und Staatsanwälte der Staaten teilgenommen, die von dem Phänomen betroffen waren. Darüber hinaus nahmen Vertreter von Wirtschaftsunternehmen sowie Mitarbeiter von staatlichen und privaten Institutionen, die sich mit Internetsicherheit beschäftigen, teil.

Durch das EC3 wurde der erfolgte Erfahrungsaustausch mit Blick auf die Ermittlungen analysiert, bewertet und den Teilnehmern als schriftlichen Report zur Verfügung gestellt. Neben diesen Arbeitsgesprächen bei Europol ist ein weiteres Treffen bei Eurojust zwischen spanischen und deutschen Ermittlern initiiert worden. Bei diesem Gespräch wurde der aktuelle Ermittlungsstand beider Länder bezüglich gewonnener Tätererkenntnisse ausgetauscht.

Die Zusammenarbeit der deutschen Strafverfolgungsbehörden mit dem EC3 erfolgt sowohl in operativen wie strategischen Bereichen. Eine fallbezogene operative Zusammenarbeit erfolgt anlassbezogen und seit 1.September 2014 im Rahmen der vom EC3 initiierten J-CAT (Joint Cybercrime Action Task Force).

Das EC3 wird als aktiver Partner wahrgenommen. Seine Einrichtung hat einen Mehrwert für die Cybercrimebekämpfung erbracht. Es gilt den eingeschlagenen Weg fortzusetzen und konsequent weiter zu entwickeln. (siehe auch Antwort zu Frage 8.A.2.). Eurojust genießt in der deutschen Strafverfolgungspraxis hohes Ansehen. Da Cyberstraftaten in aller Regel internationale Ermittlungsbezüge aufweisen, ist der Beitrag von Europol/EC3 und Eurojust regelmäßig wertvoll. Vor allem bei der Organisation multinationaler Operationen, aber auch beim Austausch von Informationen ist die Einbindung dieser Einrichtungen unverzichtbar.

Die Erfahrung in **Baden-Württemberg** zeigt, dass Hospitationen bei Europol durch eigene Mitarbeiter zu einem besseren Verständnis der Prozesse bei Europol führen und damit auch die Ermittlungsmöglichkeiten präziser eingesetzt werden können. Ferner sprach sich Baden-Württemberg für eine Einbindung der Einrichtungen in die Ermittlungen aus. Derzeit fungieren die Einrichtungen nur als supranationale Koordinierungsstellen.

Das Land **Hessen** gab folgende Empfehlung ab:
Diese Einrichtungen sollten intensiver auf die untere Ebene der Landesjustizverwaltungen zugehen, d. h. sie sollten aktiv an die Staatsanwaltschaften herantreten, um ihre Funktionen und den Mehrwert ihrer Einbindung begreiflich zu machen.

Das Land **Niedersachsen** gab folgende Empfehlung ab:
Der Zugang zu der Analysestelle des EC3 sollte vereinfacht und den Landesbehörden direkt zugänglich gemacht werden. Maßgeblich ist hier die Vernetzung von EC3 und Eurojust, damit neben der Koordination der Strafverfolgungsbehörden gleichzeitig auch eine umfassende europaweite Datenanalyse angeboten werden kann. Sinnvoll wäre zudem, das EC3 verstärkt als forensischen Dienstleister auszubauen, z. B. zum Test neuer Schadsoftwarevarianten, Wirkungsweise in bestimmten Betriebssystemumgebungen, Funktionsweise und Erkennbarkeit.

Hinsichtlich Eurojust wäre hilfreich, hier noch verstärkt auf eine Synchronisierung von Ermittlungshandlungen hinwirken zu können. Z. B. ist es nach wie vor praktisch unmöglich, zeitgleich in mehreren Mitgliedstaaten Serverüberwachungen zu fahren. Eurojust wäre aber die richtige Stelle, die verschiedenen Erfordernisse der Nationalstaaten entsprechend zu berücksichtigen und fallbezogen ein Kompetenznetzwerk in den Mitgliedstaaten zu schaffen, welche der ermittelnden Strafverfolgungsbehörde im Einzelfall direkt zuarbeiten können, z. B. nach Vorfeldbewilligung der angedachten Maßnahmen durch die national zuständigen Stellen.

Das Land **Rheinland-Pfalz** gab folgende Empfehlung ab:
Die Einbindung von Europol durch die sachbearbeitende Dienststelle bereits zu Beginn der Ermittlungsverfahren ermöglicht die Nutzung der relevanten Analysedatei (AWF) zu einem frühen Zeitpunkt. Für den weiteren Verfahrensverlauf hat dies jedoch eine entsprechende Nachlieferung der im Verfahren erhobenen Daten wie beispielsweise Personen-, Fahrzeugdaten, Sachverhalten, Telefonnummern oder Nicknames durch die sachbearbeitende Dienststelle mit dem damit verbundenen Arbeitsaufwand zur Folge. Parallel dazu sollte eine konsequente Eingabe der Personalien von Tatverdächtigen im Europol-Informationssystem (EIS) erfolgen. Dadurch könnte der Mehrwert sowohl des EIS als auch der AWF, unter anderem aufgrund einer hieraus resultierenden bzw. erhöhten Trefferwahrscheinlichkeit, erheblich gesteigert werden.
Zu den EUCTF-Tagungen wird ein Vertreter des Bundeskriminalamts (BKA) entsandt.

7.1.3. Operative Leistung von JIT und Cyberpatrouillen

Die Staatsanwaltschaft Stuttgart, die sich an einem JIT beteiligt hatte, berichtete hierzu, dass die Erfahrungen nicht zufriedenstellend waren, da der weitere beteiligte Mitgliedstaat die zur Überführung eines Täters notwendigen Beweise aus letztlich nicht nachvollziehbaren Gründen nicht zur Verfügung gestellt habe. Dagegen hätte die ZIK (Zentralstelle für die Bekämpfung der Informations- und Kommunikationskriminalität bei der Generalstaatsanwaltschaft Stuttgart) in **Baden-Württemberg** durchaus positive Erfahrungen mit dem Instrument der gemeinsamen Ermittlungsgruppe gemacht.

Vom Land **Hessen** wurde von positiven Erfahrungen berichtet. Die Gründe, die zur Einrichtung dieses Instituts geführt haben, hätten sich bestätigt. Die Verfahren wurden beschleunigt und hätten effektiver geführt werden können.
Auch in **Sachsen** sind die Generalstaatsanwaltschaft und die meisten Staatsanwaltschaften bereits an gemeinsamen Ermittlungsgruppen beteiligt, hauptsächlich bei Ermittlungen zur organisierten Kriminalität. Ihre Erfahrungen mit international koordinierten Ermittlungen, die bei der wirksamen Verfolgung von Cyberkriminalität nützlich sein können, waren weitgehend positiv.

Die anderen Bundesländer haben bislang keine Erfahrung mit einer gemeinsamen Ermittlungsgruppe.
Das Land Baden-Württemberg berichtete, dass die Übersetzungs- und Reisekosten für die gemeinsamen Treffen in Den Haag für das JIT getragen worden seien. Von Hessen wurde berichtet, dass EU-Mittel bereitgestellt wurden, um bei Coordination Meetings bei Eurojust Reisekosten abzudecken.

Es liegen keine Erfahrungen hinsichtlich gemeinsamer Cyberpatrouillen vor.

Um die internationale Zusammenarbeit zu verbessern, hat Deutschland über das Bundeskriminalamt (BKA) im Rahmen des EMPACT Operational Action Plans "Cyber Attacks" im Jahr 2014 die Gründung einer internationalen Koordinierungsgruppe initiiert. Ziel dieser Koordinierungsgruppe ist die Schaffung einer Plattform, um den Erfahrungsaustausch zwischen den Recherchedienststellen der Teilnehmerländer zu verbessern, die Kontaktaufnahme zu vereinfachen und bei möglichen künftigen gemeinsamen Maßnahmen effektiver zusammenarbeiten zu können.

7.2. Zusammenarbeit zwischen deutschen Behörden und Interpol

Die internationale Bilddatenbank (ICSE DB) befindet sich seit März 2009 beim Generalsekretariat von Interpol in Lyon im Wirkbetrieb. Die Abfrage und Bestückung der Datenbank erfolgt online durch die jeweiligen nationalen Zentralbüros der IKPO-Interpol. Für Deutschland ist dies das Bundeskriminalamt. Über die Abfrage in der Datenbank kann festgestellt werden, ob es sich um neues oder bereits bekanntes und ggf. bereits identifiziertes kinderpornografisches Material handelt. Abgefragte Bilder werden in der Regel in der Datenbank mit den relevanten Falldaten gespeichert und stehen so unmittelbar für zukünftige Abfragen aller anderen Staaten bereit.

Der potenzielle Mehrwert der ICSE DB wächst somit stetig mit der Anzahl der teilnehmenden Staaten und deren aktiven Nutzung der Datenbank. Das Bundeskriminalamt verfügt seit Wirkbetrieb der ICSE DB über einen Online-Zugang. Die Abfragen wie auch Bestückung der ICSE DB werden für Deutschland zentral durch das Bundeskriminalamt durchgeführt. Die ICSE DB ist ein unverzichtbarer Bestandteil bei der sogenannten "Täter-Opferidentifizierung".

Die Zusammenarbeit des Bundeskriminalamtes mit Drittstaaten verläuft ggf. auf dem INTERPOL-Kanal. Die Erwartungshaltung gegenüber dem bei INTERPOL im Aufbau befindlichen INTERPOL Digital Crime Center als zentrale Kontaktstelle Cybercrime innerhalb des INTERPOL Global Complex for Innovation (IGCI in Singapur) ist hoch.

Nach Mitteilung des Landes Sachsen-Anhalt verläuft die Zusammenarbeit zufriedenstellend. Zur Erlangung von verfahrenstechnisch verwertbaren Bestands- und Verbindungsdaten von IP-Adressen oder E-Mail-Account-Daten ist bei einer Vielzahl von Staaten ein förmliches Rechtshilfeersuchen auf justizieller Ebene erforderlich.

7.3. Zusammenarbeit mit Drittstaaten

Bei Hinweisen auf Ermittlungsansätze im Ausland werden die bestehenden bilateralen Kontakte genutzt. Sollten keine solchen Kontakte verfügbar sein, werden die Standardkommunikationswege (Europol, INTERPOL, G7) für den polizeilichen Informationsaustausch genutzt. Sofern erforderlich, werden gerichtsverwertbare, benötigte Informationen im Rahmen des regulären Rechtshilfeweges erhoben.

Im Bereich der Bekämpfung von Kinderpornografie, welche bei Europol -EC3- als Cyberkriminalität behandelt wird, liegen positive Erfahrungen im Kontext international zu koordinierender Ermittlungen vor. Auch bei der Bekämpfung von klassischer Cyberkriminalität erweist sich das Zusammenspiel Drittstaaten, Europol / EC3 sowie Mitgliedstaaten als hilfreich.

In **Baden-Württemberg** werden in einem laufenden Ermittlungsverfahren derzeit erste Erfahrungen mit EC3 gesammelt. Über EC3 konnten für ein Verfahren des Landeskriminalamts Baden-Württemberg (LKA BW) über sog. "Cross-Match-Reports" Verbindungen zu Verfahren in anderen Mitgliedsländern hergestellt werden. Es wird derzeit angestrebt, einen Informationsaustausch mit diesen Ländern durchzuführen. Um die Zusammenarbeit mit Europol auszubauen, wurde ein Beamter zu einer dreimonatigen Hospitation nach Den Haag zu Europol entsandt. Eine weitere dreimonatige Hospitation fand Anfang 2015 statt.

Das Land **Hessen** nahm Bezug auf folgenden Link:
http://www.eurojust.europa.eu/press/PressReleases/Pages/2014/2014-05-19.aspx
Ferner berichtete das Land Hessen, dass die Vertreter der LEA der USA an allen Coordination Meetings teilgenommen hätten. Eurojust und Europol/EC3 seien der ideale Partner, um Drittstaaten in laufende Ermittlungsverfahren einzubinden.

Nach dem Bericht des Landes **Niedersachsen** hat es einen Mehrwert erbracht. Insbesondere sei die Einbindung der USA über Eurojust in einem Fall hilfreich und in bestimmten Punkten kooperativer als im bilateralen Verhältnis gewesen.

7.4. Zusammenarbeit mit der Privatwirtschaft

Die Niederlassungen der ausländischen Diensteanbieter sind nach den Erfahrungen des Bundeskriminalamtes immer Vertriebs-/Marketingtöchter, die keinen Zugriff auf die Daten des Mutterunternehmens haben. Insofern hat nach hier vorliegenden Erkenntnissen keine Zusammenarbeit stattgefunden, Zwangsmaßnahmen wurden diesbezüglich auch nicht ergriffen.

Privatwirtschaftliche Unternehmen beteiligen sich an den Kosten, die im Rahmen der institutionalisierten Zusammenarbeit entstehen. Es werden beispielsweise Mittel zum Aufbau des G4C zur Verfügung gestellt.

Das Bundeskriminalamt (BKA) versucht, Hindernisse bei der grenzübergreifenden Zusammenarbeit, insbesondere beim Thema Online-Kartenbetrug, durch die Intensivierung der bilateralen internationalen Kooperationen sowie die Einbindung von Zentralstellen (INTERPOL/Europol) zu reduzieren.

In Sachsen-Anhalt und in anderen Ländern erfolgt die Zusammenarbeit mit ausländischen Polizeibehörden grundsätzlich im Rahmen der internationalen Rechtshilfe. Daneben erhebt das "Sicherheitsmanagement Zahlungskarten" der EURO-Kartensysteme GmbH alle Daten zu europaweit angegriffenen Geldautomaten/POS-Terminals und stellt diese den Ermittlungsbehörden zur Verfügung.

Das Land Hessen berichtete, dass sich als probates Mittel zur grenzüberschreitenden Beweissicherung in den letzten Jahren erwiesen hat, in den Fällen, in denen Hinweise aus dem Ausland auf Straftaten, bei denen Geschädigte auch im Inland vorhanden sind, ein "Parallel-Ermittlungsverfahren" einzuleiten, die beweissichernden Erstmaßnahmen zu treffen und dann im Wege des §§ 61a und 92c IRG zur Vorbereitung eines Rechtshilfeersuchens die hier gewonnenen Informationen zeitnah an die ausländischen Ermittlungsbehörden zu übermitteln.

Da sich der Weg der förmlichen Rechtshilfe oftmals trotzdem als zu schwerfällig erwiesen hat, um wirksame Strafverfolgung betreiben zu können, haben sich in den letzten Jahren bilaterale Kooperationen (insbesondere JITs (Joint-Investigation-Teams)) als weiteres wirksames Mittel zur grenzübergreifenden Bekämpfung des Online-Kartenbetrugs erwiesen.

Ferner ist Deutschland in diesem Zusammenhang an einigen europäischen und internationalen Projekten beteiligt. Dies sind unter anderem:

– die Europäische Agentur für Netz- und Informationssicherheit (ENISA) zur Förderung einer verstärkten Zusammenarbeit und eines verbesserten Informationsaustauschs zwischen den Mitgliedsstaaten zu Themen der Netz- und Informationssicherheit
– das Programm der Europäischen Kommission AGIS zur Unterstützung der EU-Staaten und Kandidatenländer (Angehörige von Rechtsberufen, Strafverfolgungsbehörden und Vertreter von Stellen, die mit der Unterstützung der Opfer befasst sind) beim Aufbau europaweiter Netzwerke und dem Austausch von Informationen und bewährten Praktiken
– die Interpol European Working Party on IT-Crime (EWPITC), eine Plattform für den Erfahrungsaustausch zur Bekämpfung von IT-Kriminalität.

7.5. Instrumente der internationalen Zusammenarbeit

7.5.1. Rechtshilfe

In Deutschland gibt es – abgesehen von den Regelungen in dem Übereinkommen des Europarates über Computerkriminalität (Convention on Cybercrime) – keine besondere Rechtsgrundlage für die Rechtshilfe bei der Ermittlung von Cyberkriminalität. Rechthilfe bei Ermittlungen von Cyberkriminalität erfolgt nach den gleichen Voraussetzungen und Regeln wie Rechtshilfe bei der Ermittlung von anderen Straftaten.

Die Rechtshilfe bei Cyberstraftaten erfolgt genauso wie die Rechtshilfe bei anderen Strafsachen. Grundsätzlich ist im föderalen Deutschland der Bund für die Rechtshilfe zuständig. Insoweit fungiert das Bundesamt für Justiz als Zentralstelle. Bewilligungsentscheidungen werden im Einvernehmen mit dem Auswärtigen Amt getroffen. Völkerrechtliche Vereinbarungen können in Abweichung vom diplomatischen Geschäftsweg, der eine Übermittlung von Ersuchen über das Auswärtige Amt vorsieht, den justizministeriellen Geschäftsweg zulassen.

Die Bewilligungszuständigkeit hauptsächlich im Bereich der EU-Rechtshilfe ist durch eine Vereinbarung zwischen der Bundesregierung und den Landesregierungen weitgehend auf die Landesjustizministerien übertragen worden. In der Regel haben die Justizministerien der Länder die Entscheidungszuständigkeit im Rechtshilfeverkehr mit EU-Mitgliedstaaten an die Staatsanwaltschaften delegiert.
Eilige Ersuchen um Sicherstellungsmaßnahmen können über das 24/7 Netzwerk nach Artikel 35 Convention on Cybercrime bzw. das G7-Kontaktstellennetzwerk versandt werden, dessen deutsche Kontaktstelle das Bundeskriminalamt ist.

Eine amtliche Statistik zur Rechtshilfe wird weder seitens des Bundes noch auf Länderebene geführt.

Das deutsche Recht sieht keine besonderen Verfahren oder Bedingungen vor, die in Bezug auf die verschiedenen Kategorien von Rechtshilfeersuchen bei Cyberstraftaten eingehalten werden müssen. Generell liegt dem deutschen Rechtshilferecht ein Beschleunigungsgebot zugrunde, s. Nummer 19 Absatz 1 RiVASt ("unverzüglich"; RiVASt = Richtlinien für den Verkehr mit dem Ausland in Strafrechtlichen Angelegenheiten).

Im Rahmen eines Rechtshilfeersuchens bei Cyberstraftaten kann um alle strafverfahrensrechtlich vorgesehenen Maßnahmen ersucht werden. Insoweit wird auf die Ausführungen zu Frage 2. B 2 verwiesen. Zudem darf nach § 110 Absatz 3 StPO die Durchsicht eines elektronischen Speichermediums unter bestimmten Voraussetzungen auch auf vom ursprünglichen Speichermedium räumlich getrennte Speichermedien erstreckt werden. Dies schließt die Sicherung von Daten auf dem getrennten Speichermedium ein. Allerdings gibt es insoweit komplexe Fragestellungen in Bezug auf das sogenannte "Cloud"-Computing, bei dem nicht ohne weiteres ersichtlich ist, ob die Daten physisch im In- oder Ausland (und ggf. in welchem ausländischen Staat) gespeichert sind.

Drittstaaten stellen nach den der Bundesregierung vorliegenden Informationen häufig Ersuchen wegen Computersabotage. Ausgehende Ersuchen betreffen nicht selten Betrugsstraftaten und Kinderpornografie.

In dringlichen Fällen werden Ersuchen um Vorabsicherung über das 24/7 Netzwerk nach Artikel 35 Convention on Cybercrime bzw. das G7- Kontaktstellennetzwerk kommuniziert, die aber in jedem Fall ein formelles Rechtshilfeersuchen nach sich ziehen.

In geeigneten Fällen können eine vorherige Absprache unmittelbar zwischen betroffenen Behörden oder über das Europäische justizielle Netz oder unter Einbindung von Eurojust sinnvoll sein. Dies ist insbesondere dann der Fall, wenn Ersuchen zeitgleich in verschiedenen Staaten zu erledigen sind, oder Unsicherheiten hinsichtlich der notwendigen Form und des Inhalts eines Ersuchens bestehen.

Bei Ersuchen, die auf die Sicherung und Herausgabe von Daten gerichtet sind, die in der Cloud gespeichert werden, ist oft nicht klar, an welchen Staat ein Ersuchen zu richten ist.
Die Bundesrepublik Deutschland ist Mitglied des Übereinkommens des Europarats über Computerkriminalität vom 23. November 2001 (Convention on Cybercrime). Die Convention on Cybercrime war bereits in mehreren Fällen mit Drittstaaten Grundlage für Rechtshilfeleistungen. Es handelte sich dabei um Ersuchen an die und aus den Vereinigten Staaten von Amerika und Kanada.

Die Vereinigten Staaten von Amerika stellen grundsätzlich hohe formale und inhaltliche Anforderungen an die Darlegungen insbesondere eines Zusammenhanges zwischen Straftat und konkretem Beweismittel, um dessen Übermittlung ersucht wird. Es wird versucht, durch Schulungen und durch intensive Gespräche mit dem US Department of Justice über die generelle Problematik und individuelle Fälle diese Anforderungen zu verstehen und ihnen nachzukommen. Zudem eröffnen die Regelungen des § 67 Absatz 1 des Gesetzes über die Internationale Rechtshilfe in Strafsachen (IRG) und die §§ 59 und 73 IRG für die zuständigen deutschen Behörden und Gerichte die Möglichkeit, Rechtshilfe auch ohne internationale vertragliche Grundlage zu leisten.

Die zur Verfügung stehenden internationalen Kommunikationswege (INTERPOL, Europol, G7, sowie zahlreiche bilaterale Kontakte) werden genutzt. Bei justiziellen Ersuchen wird der formelle Rechtshilfeweg beschritten, der allerdings im dynamischen Phänomen Cybercrime aufgrund der formalen Vorgaben in aller Regel nicht praktikabel und zielführend ist, insbesondere aufgrund der zeitlichen Aufwände und der Erledigungsdauer. Hier erweist sich das G7-24/7 Kontaktpunktnetzwerk als vorteilhaft. Es ist aber nicht geeignet, alle Defizite der Rechtshilfewege zu kompensieren. Daher existieren entsprechende Bestrebungen, den schnellen Informationsaustausch auf polizeilicher Ebene entsprechend auf justizieller Ebene durch direkte Zusammenarbeit der zuständigen Staatsanwaltschaften zu übertragen.

7.5.2. Instrumente der gegenseitigen Anerkennung

Deutschland hat sämtliche Rahmenbeschlüsse im Bereich der gegenseitigen Anerkennung umgesetzt. Zu Fallzahlen liegen der Bundesregierung aufgrund der Übertragung der Zuständigkeiten innerhalb der EU auf die Bundesländer grundsätzlich keine Erkenntnisse vor. Weder der Bund noch die Länder führen allgemeine Rechtshilfestatistiken. Eine Zuständigkeit des Bundes für die Anwendung des Gesetzes besteht nur hinsichtlich des Rahmenbeschlusses Geldsanktionen. Hier steht bisher die Vollstreckung von Sanktionen im Bereich des Straßenverkehrs im Vordergrund.

7.5.3. Überstellung/Auslieferung

Die Auslieferung an andere EU-Mitgliedstaaten zur Verfolgung ist im Rahmen des § 81 IRG, welcher der Umsetzung des Rahmenbeschlusses 2002/584/JI des Rates vom 13. Juni 2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten dient, nur zulässig, wenn die Tat nach dem Recht des ersuchenden Mitgliedstaats höchstens mit einer Freiheitsstrafe oder sonstigen Sanktion im Höchstmaß von mindestens 12 Monaten bedroht ist. Die Auslieferung zur Vollstreckung ist zulässig, wenn die vom ersuchenden Mitgliedstaat verhängte freiheitsentziehende Sanktion mindestens vier Monate beträgt.

Eine Überstellung oder Auslieferung erfordert keine Prüfung der beiderseitigen Strafbarkeit, wenn es sich um eine in Artikel 2 Absatz 2 des Rahmenbeschlusses des Rates vom 13. Juni 2002 über den Europäischen Haftbefehl aufgeführte Straftat handelt.

Die ausgestellten / entgegengenommenen Ersuchen um Überstellung bzw. Auslieferung ergeben sich aus der beigefügten "Bekanntmachung der Auslieferungsstatistik für das Jahr 2013" vom 14. Januar 2015, veröffentlicht am 25. Februar 2015. Die Auslieferungsstatistik für das Jahr 2014 wurde ebenfalls nach dem Evaluierungsbesuch veröffentlicht; http://www.bmjv.de/DE/Service/Statistiken/Statistiken_node.html .

Es gibt grundsätzlich keine besonderen Verfahren oder Bedingungen, die in Bezug auf die Ersuchen bei Cyberstraftaten eingehalten werden müssen. Es gilt der allgemeine Beschleunigungsapell aus Nummer 19 Absatz 1 RiVASt. Eingehende Ersuchen werden bevorzugt bearbeitet. Die Unterstützung durch das Europäische Justizielle Netzwerk, Eurojust und das 24/7 Netzwerk nach Artikel 35 Convention on Cybercrime führt zu weiterer Beschleunigung.

Es sind vorläufige Festnahmen auch zur Bekämpfung der Cyberkriminalität möglich.

Die durchschnittliche Bearbeitungsdauer wird nur bei Überstellungen auf der Grundlage des Europäischen Haftbefehls statistisch erfasst. Die Statistik differenziert nicht zwischen einzelnen Straftaten. Allgemein dauerte im Jahr 2013 die Bearbeitung der Überstellungsverfahren mit Zustimmung der verfolgten Person 15,94 Tage und ohne deren Zustimmung 38,94 Tage. Allgemein dauerte im Jahr 2014 die Bearbeitung der Überstellungsverfahren mit Zustimmung der verfolgten Person 15,15 Tage und ohne deren Zustimmung 41,74 Tage.

Im Rahmen der Zuständigkeit des Bundeskriminalamtes für die weltweite INTERPOL-Personenfahndung existieren keine besonderen Verfahren und keine besonderen Bedingungen für Cyberstraftaten. Auch bei diesem deliktischen Hintergrund wird das reguläre INTERPOL Personenfahndungsinstrumentarium genutzt. Die Rechtsgrundlage für die Übermittlung deutscher Personenfahndungsersuchen (jeglichen deliktischen Hintergrunds) an ausländische Staaten ist § 14 des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKAG), die Rechtsgrundlage für die nationale Umsetzung ausländischer Personenfahndungsersuchen (jeglichen deliktischen Hintergrunds) in Deutschland ist § 15 BKAG. Weitere Verfahrensweisen und/oder Bedingungen bei Ersuchen im Bereich der Cybercrimebekämpfung richten sich nach der Convention on Cybercrime bzw. den allgemeinen Regeln der Rechtshilfe. Über die Dauer der Abwicklung von Rechtshilfeersuchen kann keine allgemeingültige und belastbare Aussage getroffen werden.

Die ausgestellten / entgegengenommenen Ersuchen um Überstellung bzw. Auslieferung ergeben sich aus der in der beigefügten "Bekanntmachung der Auslieferungsstatistik für das Jahr 2012" vom 13. Januar 2014, veröffentlicht am 11. Februar 2014. Inzwischen wurde auch die Statistik für 2014 veröffentlicht. Typische Straftaten der Cyberkriminalität sind: § 202a StGB ("Ausspähen von Daten"), § 202b StGB, § 202c StGB ("Vorbereiten des Ausspähens und Abfangens von Daten"), § 263a StGB ("Computerbetrug"), § 269 StGB ("Fälschung beweiserheblicher Daten"), § 303a StGB ("Datenveränderung") und § 303b StGB ("Computersabotage").

Auch hier ist als Rechtsgrundlage vor allem die Convention on Cybercrime zu nennen. Im Übrigen kann die Bundesregierung auf vertragloser Basis agieren.

7.6. Fazit

- **Die Zusammenarbeit mit den EU-Mitgliedstaaten wurde als insgesamt gut bewertet, und die Praktiker nutzen alle verfügbaren Kanäle: bilaterale Beziehungen, Verbindungsbeamte und -richter oder EU-Agenturen. Die Zusammenarbeit mit Drittstaaten ist bisweilen schwierig, und bei Antworten gibt es Verzögerungen.**

- **Beim Besuch haben die Praktiker mehrmals darauf hingewiesen, dass ein sicherer Kanal für den Informationsaustausch zwischen Staatsanwaltschaften und anderen Strafverfolgungsbehörden benötigt wird.**

- **Deutschland hat Anstrengungen unternommen, um eine zuverlässige und äußerst strukturierte öffentlich-private Partnerschaft auf Bundes- und Länderebene einzurichten.**

- **Das BKA hat eine Vereinbarung mit dem German Competence Centre against Cybercrime (G4C) geschlossen, einem von mehreren Banken getragenen Verein, der insbesondere unter dem Gesichtspunkt des Online-Kartenbetrugs wichtig ist.**

- **Es wurde auch die gute Zusammenarbeit mit dem BITKOM (Digitalverband Deutschlands, der 1999 als Zusammenschluss einzelner Branchenverbände in Berlin gegründet wurde und mehr als 2300 Unternehmen der digitalen Wirtschaft vertritt) und der Deutschen Telekom betont. Diese Unternehmen bieten Software, IT-, Telekommunikations- oder Internetdienste an, stellen Hardware oder Verbraucherelektronik her und sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig.**

- **Die Deutsche Telekom muss das Fernmeldegeheimnis und die Datenschutzvorschriften einhalten. Das Unternehmen reagiert nicht auf unmittelbare Anfragen von Behörden außerhalb Deutschlands. Jede Anfrage sollte über die zuständige deutsche Behörde eingehen (Rechtshilfeverfahren). Die Deutsche Telekom ist der Auffassung, dass die grenzübergreifende Verfahren zwischen Anbietern und Strafverfolgungsbehörden harmonisiert werden sollten, weil zurzeit jedes Land unterschiedliche Anforderungen in Bezug auf die rechtmäßige Überwachung und Datenbereitstellung hat. Dies erschwere ihr das Handeln und die Einhaltung der Rechtsvorschriften.**

- **Die wichtigsten Akteure im Zusammenhang mit der internationalen Zusammenarbeit waren während des Besuchs auf Cyberkriminalität spezialisierte Staatsanwaltschaften, Generalstaatsanwaltschaften (Kontaktstellen des EJN und des ENCS), das Bundesamt für Justiz (Kontaktstellen des EJN, des ENCS und weiterer Netzwerke), das Bundeskriminalamt (BKA), das deutsche Verbindungsbüro von Europol und das deutsche Verbindungsbüro bei Eurojust. Eurojust ist den Praktikern sehr gut bekannt und wird bei Bedarf genutzt. Es wurde ein gutes Beispiel für die Nutzung von Eurojust vorgestellt, bei dem es um einen von der Staatsanwaltschaft Verden behandelten komplexen Fall von Cyberkriminalität ging. Europol ist ebenfalls bekannt und wird von den Strafverfolgungsbehörden genutzt, die sich an den Tätigkeiten der drei mit Cyberstraftaten befassten Kontaktstellen (Cyborg, Twins und Terminal) und an den im Rahmen des EU-Politikzyklus entwickelten EMPACT-Projekten beteiligen. Europol (EC3) wurde in konkreten Fällen einbezogen, und der Informationsaustausch erfolgt über die entsprechenden Kanäle (SIENA).**

Abgesehen von den Bestimmungen des Übereinkommens des Europarates über Computerkriminalität verfügt Deutschland über keinerlei gesonderte Vorschriften zur Regelung der internationalen Zusammenarbeit bei der Bekämpfung von Cyberkriminalität. Die Bestimmungen internationaler Verträge sind unmittelbar anwendbar (siehe z. B. § 1 Absatz 3 IRG [Artikel 29 des Übereinkommens von Budapest]). Die allgemeinen Vorschriften über die Rechtshilfe gelten unabhängig von der Art der Straftat für alle Ermittlungen. Dazu zählen auch Ermittlungen bei Cyberstraftaten. Grundsätzlich ist der Bund für die Rechtshilfe zuständig, insbesondere das Bundesamt für Justiz, das als Zentralstelle fungiert. Es gibt keine spezifischen Verfahren für die Beschleunigung der Erledigung von Rechtshilfeersuchen im Zusammenhang mit Ermittlungen bei Cyberstraftaten. Allerdings gibt es im deutschen Rechtshilferecht ein allgemeines Beschleunigungsgebot. Es wurde betont, dass Informationen über Teilnehmer relativ rasch erhältlich sind, wenn ein Rechtshilfeverfahren als zu langsam befunden wurde. Es besteht die große Hoffnung, dass nach den Beratungen auf EU-Ebene praktische Lösungen gefunden werden, um das Verfahren zu beschleunigen.

In einigen Fällen haben die deutschen Behörden nicht beschlossen, eine JIT einzurichten, da die Beweismittel ihres Erachtens sehr schnell auf bilateraler Ebene erlangt und ausgetauscht werden könnten.

- **Es gibt keine Statistiken über Rechtshilfeersuchen, weil sie in die Zuständigkeit der Länder fallen.**

- **Das nationale Verbindungsbüro bei Europol hat 10 Mitarbeiter, und in seiner Organisationsstruktur spiegeln sich die Bundes- und die Landesebene wider. Die nationalen Behörden haben auch die enge Zusammenarbeit mit dem EC3 hervorgehoben.**

- **Der Ausschuss wurde auch über den Plan informiert, eine Maßnahme einzuführen, die der Nacheile bei der Ermittlung von Cyberkriminalität ähnelt und den Ermittlern ermöglichen wird, in dringenden Fällen nationale Zuständigkeiten zu überschreiten und auf Daten direkt zuzugreifen.**

- **Als praktische Hilfsmittel bei der internationalen Zusammenarbeit nutzt Deutschland Eurojust, EJN und Europol (EC3) sowie das BKA als jederzeit verfügbare Ansprechstelle.**

- **Ein Beispiel für eine bewährte Vorgehensweise Deutschlands sind die Richtlinien für den Verkehr mit dem Ausland in Strafrechtlichen Angelegenheiten (RiVASt).**

- **Deutschland ist Mitglied der J-CAT, und die Arbeit dieser Gruppe wurde als sehr effizient bewertet.**

- **Deutschland begrüßt die Beratungen auf EU-Ebene über Verbesserungen bei der Strafjustiz im Cyberraum und unterstützt die Einrichtung eines Europäischen Justiziellen Netzes gegen Cyberkriminalität.**

8. AUS- UND FORTBILDUNG, SENSIBILISIERUNG UND PRÄVENTION

8.1. Spezifische Aus- und Fortbildung

Das **Bundeskriminalamt (BKA)** hat an der Erstellung verschiedener bundesweiter Aus- und Fortbildungsprogramme maßgeblich mitgewirkt. Diese decken den von Bund und Ländern formulierten Aus- und Fortbildungsbedarf ab. Gemäß dem "Bundeseinheitlichen Aus- und Fortbildungskonzept IuK-Kriminalität" erhalten Sachbearbeiter, die in "Ersteinschreiter", "Sachbearbeiter im weiteren Sinne" und "Sachbearbeiter im engeren Sinne" eingeteilt werden, entsprechend ihrer Qualifikation und Verwendungsplanung zielgruppenbezogene Lehrgänge angeboten. Dieses Konzept wurde von den Ländern nach Anpassung an die vor Ort gegebenen Umstände umgesetzt. Zur Gewährleistung der Einheitlichkeit und zur Vermeidung von Redundanzen wurden in den Ländern Multiplikatoren eingesetzt. Die Koordination dieser Multiplikatoren wird über jährliche Multiplikatoren-Fortbildungen, die das BKA organisiert und durchführt, gewährleistet.

In Zusammenarbeit mit den Fachdienststellen der Abteilung Schwere und Organisierte Kriminalität (SO) bietet die Abteilung KI aus diesem Konzept jährlich die Speziallehrgänge "Kinderpornografie in Internet", "Arzneimittelkriminalität im Tatmedium Internet" und den "Speziallehrgang für Mitarbeiter /-innen von Zentralstellen für Internetrecherchen" an. Zusätzlich ist das BKA für die zentrale Sachverständigenausbildung für Bund und Länder im Fachbereich "IuK-Forensik" zuständig. Im Rahmen der Sachverständigenausbildung ist eine Spezialisierung in den Richtungen Windows, Linux, Macintosh, Netzwerke/Internet, Mobil-Forensik und Kryptologie möglich. Alle Module der Sachverständigenausbildung werden einmal jährlich angeboten. BKA-intern wird jährlich eine aus zwei Modulen bestehende Cybercrime-Grundlagenschulung angeboten.

Kurzfristig werden dringend benötigte Lehrgänge sowohl ausschließlich für die Fachdienststellen des BKA als auch bedarfsorientierte Bund-Länder-Lehrgänge organisiert. Beispielsweise wurde im Jahr 2013 bundesweiter Bedarf an Windows 8-Forensik-Schulungen formuliert. Diesen Bedarf aufgreifend wurde im Juni 2014 eine Windows 8-Großveranstaltung durchgeführt, in deren Rahmen mehr als 50 Kolleginnen und Kollegen aus Bund und Ländern sowie der Schweiz und Luxemburg geschult wurden. Aufgrund des unverändert hohen Bedarfs wird diese Schulung im November 2014 wiederholt. Ähnliche Veranstaltungen sind für Macintosh-Forensik, Mobil-Forensik und Windows 10 geplant.

Auf der Ebene der **Deutschen Richterakademie** in Trier und Wustrau finden insgesamt 7 Tagungen bzw. Fortbildungsveranstaltungen für **Richter und Staatsanwälte aus ganz Deutschland** statt, die sich mit der Bekämpfung der Internetkriminalität befassen: die Tagung "**Ermittlungsmaßnahmen im Bereich der Telekommunikation"**, die Tagung "**Erscheinungsformen der Internetkriminalität und ihre Bekämpfung"**, die Tagung "**Strafrecht und Internet**", die Tagung "**Aktuelle Entwicklungen in Kriminalistik und Strafrechtspflege**", die Tagung "**Entwicklungen und Tendenzen im Strafrecht**", die Tagung "**Strafverfahren bei Produkt- und Markenpiraterie**" und die Tagung "**Der Kampf ums Urheberrecht im Digitalzeitalter**".

Die Tagung "**Strafverfahren bei Produkt- und Markenpiraterie**" beschäftigt sich insbesondere mit der Verletzung von Urheberrechten durch illegale Downloads im Internet. In der fünftägigen Veranstaltung sollen materiell-rechtliche Bestimmungen aus dem Marken-, Urheber- und Patentrecht sowie die einschlägigen Strafverfahrensvorschiften erörtert und Einblicke in die praktische Arbeit von Zoll und Polizei ermöglicht werden. Auch die viertägige Veranstaltung "**Der Kampf ums Urheberrecht im Digitalzeitalter**" legt den Fokus auf die Verfolgung von Urheberrechtsverstößen im Internet und beleuchtet hierzu zivil- und strafrechtliche Fragen mit besonderer Ausrichtung auf die neuen digitalen Medien. Ein Vortrag der neuntägigen Schulung "**Aktuelle Entwicklungen in Kriminalistik und Strafrechtspflege**" beschäftigt sich mit dem Thema "Identifizierung von Tätern und Opfern aus kinderpornografischen Medien – auch im Rahmen der internationalen Zusammenarbeit". Es bezieht sich somit auf einen der spezifischen Bereiche, denen die Mitgliedstaaten besondere Aufmerksamkeit widmen möchten.

Die Veranstaltung "**Ermittlungsmaßnahmen im Bereich der Telekommunikation**" dauert sechs Tage und dient unter anderem durch Vermittlung von Wissen zu Aufbau und Funktionsweise des Internets, der materiell-rechtlichen Rechtsgrundlagen und der Darstellung der praktischen Durchführung von verdeckten Ermittlungsmaßnahmen der Bekämpfung von Straftaten, die mit Mitteln der Telekommunikation begangen werden. Die Tagung "**Erscheinungsformen der Internetkriminalität und ihre Bekämpfung**", die über fünf Tage angeboten wird, beschäftigt sich mit der Frage der Anwendbarkeit des deutschen Strafrechts, mit Zuständigkeitsfragen, Rechtshilfe, Provider-Verantwortlichkeit, Fahndungsmethoden und Formen der Internetkriminalität. Ferner bietet die Deutsche Richterakademie jährlich die sechstägige Fortbildung "**Strafrecht und Internet**" an.

In dieser werden verschiedene Erscheinungsformen der Kriminalität im Zusammenhang mit dem Internet – wie Phishing, Underground Economy, Cyberwar, Urheberrechtsverletzungen und Verbreitung von Kinderpornografie in Datennetzen – und die Möglichkeiten der technischen Ermittlungen vorgestellt. Auch die im Jahresrhythmus stattfindende einwöchige Tagung "**Entwicklungen und Tendenzen im Strafrecht**" befasst sich im aktuellen Programm unter anderem mit materiell-rechtlichen Fragen der Internetkriminalität.

Die Tagungen "**Erscheinungsformen der Internetkriminalität und ihre Bekämpfung**" sowie "**Strafverfahren bei Produkt- und Markenpiraterie**" sind auch in dem Katalog des **European Judical Training Network (EJTN)** gelistet. Für die Richterinnen und Richter sowie die Staatsanwältinnen und Staatsanwälte besteht die Möglichkeit, hierüber auch an Veranstaltungen anderer europäischer Mitgliedsstaaten teilzunehmen. Über die genannten Tagungen hinaus bietet das EJTN im Jahr 2014 zwölf Fortbildungsveranstaltungen mit einem Bezug zu Cyberkriminalität an:

Fünf Veranstaltungen, ausgerichtet von **verschiedenen Ländern (Schottland, Frankreich, Portugal und Belgien)**, laufen unter dem Titel "**Cybercrime**". Hierbei handelt es sich bei vier Tagungen um Eintagesveranstaltungen; eine Veranstaltung dauert fünf Tage. Bei den drei in diesem Jahr angebotenen Tagungen "Basic training course on legal and technical aspects of cybercrime for judges and prosecutors" (jeweils zwei Tage) sollen Fertigkeiten für den Umgang mit Cyberkriminalität vermittelt werden. Die Fortbildung "Countering the Illegal Use of the Internet: Legal an policy developments at international and European level four years after Stuxnet" (zwei Tage) ist Teil einer Seminarreihe, in der es um die Bekämpfung von Internetkriminalität geht. Bei dieser Veranstaltung sollen groß angelegte Cyberangriffe, vergleichbar mit dem Computerwurm Stuxnet, behandelt und der derzeitige Stand der Möglichkeiten der Bekämpfung dargelegt werden. Bei der Zweitagesveranstaltung "Justice and Cybercrime" steht mit den Online-Bezahlsystemen eines der Hauptthemen der in der RAG GENVAL vereinbarten Bereiche im Mittelpunkt. Mit der Aussagekraft und der Zulässigkeit von elektronischen Beweisen bei Fällen von Cyberkriminalität beschäftigt sich das zweitägige Seminar "The validity and admissibility of electronic evidence in cybercrime cases". Die Tagung "Online financial crimes and fraud committed with electronic means of payment" (zwei Tage) beschäftigt sich mit Betrugsstraftaten im Internet, beispielsweise im Zusammenhang mit Internetauktionen oder "phishing".

Daneben bieten die Bundesländer intern noch folgende Fortbildungsveranstaltungen/Schulungen an:

Baden-Württemberg

In Baden-Württemberg erhalten alle Mitarbeiter der Polizei Schulungen zum Thema Cyberkriminalität als Teil ihrer Ausbildung. In der Ausbildung zum mittleren Polizeivollzugsdienst (mD) sind derzeit Lerninhalte zur Cyberkriminalität in Höhe von 41 Unterrichtsstunden enthalten. Es ist geplant, diesen Themenkomplex aufzuwerten und mit 50 Unterrichtsstunden in der Ausbildung zu verankern. Im Bereich des Studiums zum gehobenen Polizeivollzugsdienst (gD) werden an der Hochschule für Polizei (HfPol) Lerninhalte zu diesem Thema in Kriminalistik und Informatik in insgesamt gleicher Größenordnung wie in der Ausbildung mD vermittelt.

Inhaltlich werden im Rahmen der Ausbildung Grundlagen in Sachen Hardware und Software, Funktionsweisen und Aufbau des Internets, Überblick und Funktion von Schadsoftware, Begrifflichkeit und Phänomenologie, relevante Straftatbestände, Informationen zur Verdachtsgewinnung und Beweissicherung vermittelt. Je nach weiterer Verwendung der Mitarbeiter in der Organisation wird das Grundlagenwissen anschließend durch bedarfsgerechte Fortbildungsangebote sukzessive ergänzt und aufgebaut. Die Fortbildungsinhalte in Baden-Württemberg orientieren sich an der "Gesamtkonzeption Cyberkriminalität / Digitale Spuren" (Stand 22. Januar 2013) des Landeskriminalamtes Baden-Württemberg.

Der Fortbildungsrahmen gliedert sich in drei Ebenen:

– Ebene 1 – Ersteinschreiter:

Wissensniveau, welches der Streifendienstbeamte für die Bearbeitung der Thematik im "Ersten Angriff" benötigt. Dieses Wissen wird in der Ausbildung vermittelt.

– Ebene 2 – Sachbearbeiter Cybercrime:

Wissensniveau, welches der Mitarbeiter zur Sachbearbeitung der Cyberkriminalität im weiteren Sinn (Internetkriminalität), in einfachen Fällen auch für die Sachbearbeitung der Cyberkriminalität im engeren Sinn (Computerkriminalität), benötigt. Diese Sachbearbeiter fungieren weiterhin als Ansprechpartner für die Ersteinschreiter. Dieses Wissen wird im Rahmen von Fortbildungsmaßnahmen in Höhe von derzeit 26 Schulungstagen vermittelt und baut auf dem Wissenstand des Ersteinschreiters auf.

– Ebene 3 – hochspezialisierte Mitarbeiter:

Wissensniveau für Mitarbeiter, welche sich mit komplexen Sachverhalten der Cyberkriminalität beschäftigen und über umfangreiches Wissen im Bereich der Digitalen Forensik verfügen müssen. Diese Mitarbeiter sind ausschließlich in den Kriminalinspektionen 5 der Polizeipräsidien und der Abteilung 5 des LKA BW verortet.

Ziel der Schulungsmaßnahmen für die Ebenen 2 und 3 ist die Vermittlung der benötigten Wissenstiefe, um der Cyberkriminalität auf der gesamten Breite in all ihren Facetten entgegenzusteuern.

Parallel zu den Ausbildungs- und Fortbildungsmaßnahmen wird jedem Vollzugsmitarbeiter der Polizei Baden-Württemberg permanent eine elektronische Lernanwendung (eLA) zur Verfügung gestellt. In dieser sind umfangreiche Informationen zu der Thematik auf dem aktuellsten Stand zur Verfügung gestellt. Die eLA dient hierbei als Nachschlagewerk für das Themenfeld Cybercrime und zielt mit bedarfsgerechten Aktualisierungen auf einen nachhaltig hohen Wissensstand bei den Mitarbeitern.

Berlin

Für Berlin ist eine gemeinsame Fortbildungsveranstaltung Cybercrime für Spezialisten der Landespolizei und niedersächsischer Staatsanwaltschaften zu erwähnen.
Die Ersteinschreiterschulung (Stufe 1 des bundesweiten IuK Aus- und Fortbildungskonzeptes) wird im Multiplikatorenmodell vermittelt. Für Sachbearbeiter Cybercrime im weiteren Sinne (Stufe 2) bietet die Landespolizeischule einen 4-tägigen Kurs zum Thema "Ausgewählte technische Aspekte zu Ermittlungen im Internet" an. Für die Zielgruppe der Stufe 3 des IuK-Aus- und Fortbildungskonzeptes ist das Landeskriminalamt Berlin auf die Angebote anderer Anbieter (Bundeskriminalamt (BKA), andere Bundesländer) angewiesen. Im Jahr 2012 haben alle Mitarbeiter der Dienststellen LKA 335 und 336 einen zweiwöchigen Speziallehrgang besucht.

Der Lehrgang "Kinderpornografie im Internet für Polizisten, Staatsanwälte und Richter" von Dunkelziffer e.V., zweitägig, findet mehrmals im Jahr an verschiedenen Standorten in Deutschland statt. Mitarbeitern der Staatsanwaltschaft Berlin, die mit der Bearbeitung von Cyberkriminalität betreffenden Ermittlungsverfahren beauftragt sind, werden spezielle Schulungsprogramme angeboten. Ziel ist die Vermittlung spezieller technischer und rechtlicher Kenntnisse, die für die tägliche Arbeit bei Aktenbearbeitung und Sitzungsvertretung erforderlich sind. Eine entsprechende Schulung wurde kürzlich durchgeführt und beinhaltete insgesamt sechs ganztätige Fortbildungsveranstaltungen. Es wird angestrebt, hierzu jährlich Vertiefungsveranstaltungen abzuhalten.

Brandenburg

Schulungen zum Thema "Cyberkriminalität" werden grundsätzlich jedem Mitarbeiter der Polizei angeboten. Ziel ist es, ein grundständiges Basiswissen für alle Polizeivollzugsbeamten durch Ausbildung, Studium und Weiterbildung zu vermitteln. Eine E-Learning-Anwendung mit insgesamt 4 Modulen ermöglicht den Mitarbeitern, Grundlagenwissen im Selbststudium am PC zu erlernen. Inhalte dieser Module sind Themen wie Hardware, Software, Soziale Netzwerke, Cloudcomputing, Phänomenologie sowie Straf- und Strafprozessrecht. Darauf aufbauend erfolgt ein dreitägiges Präsenzseminar an der FHPol, in dem das erlernte Grundwissen nochmals praxisnah vertieft wird. Es werden weitere Aufbaumodule und Spezialmodule nach Bedarf zielgruppenorientiert angeboten. Die Inhalte aller in der Weiterbildung angebotenen Seminare sind an das bundeseinheitliche Aus- und Fortbildungskonzept zur Neuausrichtung der Kriminalpolizei angepasst.

An der Justizakademie des Landes Brandenburg finden regelmäßige Fortbildungsveranstaltungen für den höheren Justizdienst statt, in denen die Bekämpfung der Cyberkriminalität behandelt wird. So fand im Jahr 2013 eine eintägige Veranstaltung zum Thema Internetkriminalität statt, die sowohl eine Einführung in das Thema Internetkriminalität als auch einen speziellen Fortbildungsabschnitt zum Thema "Phishing und Finanzagenten" beinhaltete. Im Jahr 2014 gab es zwei eintägige Veranstaltungen, die sich vorrangig mit den technischen Grundlagen und möglichen Ermittlungsmaßnahmen im Bereich der Cyberkriminalität sowie mit der Entscheidung des Europäischen Gerichtshofs zur Vorratsdatenspeicherung befassten. Die Veranstaltungen dienten dazu, insbesondere den Richterinnen und Richtern sowie Staatsanwältinnen und Staatsanwälten, die im Bereich der Massen- und Kleinkriminalität mit dem Phänomen "Cybercrime" befasst sind, die notwendigen Grundlagen zu vermitteln.

Darüber hinaus veranstaltet das für die Fortbildung des höheren Justizdienstes zuständige Gemeinsame Juristische Prüfungsamt der Länder Berlin und Brandenburg im Rahmen des Konzepts "Fortbildung IT-Kriminalität" im Jahr 2014 eine sechstägige Spezialschulung für Spezialisten zur Bekämpfung der IT-Kriminalität, um den ständig wachsenden technischen und juristischen Anforderungen im Bereich "Cybercrime" zu begegnen. Themen sind dabei u. a. EDV-Beweissicherungsmaßnahmen, Ermittlungen in Datennetzen, auch mit Auslandsbezug, Herausforderung Massendaten und Probleme des Datenschutzes.

Im Übrigen werden (Sachbearbeiter-)Tagungen zu speziellen Themen (z. B. Webmoney) einmal jährlich durch die Fachdirektion des Landeskriminalamts veranstaltet, an denen die Dezernentinnen und Dezernenten der Schwerpunktabteilung der Staatsanwaltschaft teilnehmen.

Saarland

Im Saarland werden landesinterne Schulungen durchgeführt, die Folgendes zum Ziel haben:

- flächendeckende Grundbeschulung ("Ersteinschreiter Cybercrime")
- Spezialbeschulung der Angehörigen der Dienststellen LPP 222 Cybercrime und LPP 4.7 IT-Forensik

Themen, Häufigkeit und Dauer der Beschulungen werden bedarfsgerecht und individuell festgelegt.

Sachsen

Im Freistaat Sachsen werden zentral 81 Fortbildungskurse für die sächsische Polizei mit Bezug Cyberkriminalität angeboten. Es werden sowohl die Fortbildungskurse im Bereich Ermittlungen (IuK 0700), als auch Lehrgänge in den unterschiedlichen Servicebereichen (z. B. Mobilfunk-, Computer- und Internetnetzwerkforensik) aufgeführt. Durch die Schnittmengen (insbesondere der Informationssicherheit), die sich zum IuK-Betrieb (z. B. Betrieb der Netze und Datenbanken) ergeben, werden auch diese aufgelistet.

Durch das Landeskriminalamt Sachsen wurde bis 2012 jährlich eine viertägige "Modulare Komplexfortbildung (MKF)" organisiert, an der auch Dezernenten der Staatsanwaltschaften teilnahmen. Gegenstände der MKF waren die "Darstellung der Methoden der Ermittlungen bei IuK-Delikten, insbesondere bei Internetkriminalität", "Möglichkeiten und Grenzen der forensischen Untersuchung von Datenträgern" sowie die "Darstellung der Leistungsfähigkeit der sächsischen Polizei im Bereich der Bekämpfung der IuK-Kriminalität mit dem Ziel der sachgerechten Planung von zukünftigen Ermittlungsmaßnahmen". Die MKF wurde seit 2013 nicht mehr durchgeführt, da von Seiten der sächsischen Polizei eine grundlegende Überarbeitung des MKF-Konzeptes vorgenommen werden sollte.

Die sächsische Staatsanwaltschaft unterhält seit mehreren Jahren eine erfolgreiche Zusammenarbeit mit einem auf IT-Forensik spezialisierten Unternehmen. Dieses Unternehmen bietet jährlich eine zweitägige Schulung für bis zu zehn Teilnehmer an. Der Inhalt der Workshops orientiert sich an den aktuellen Bedürfnissen der im Bereich Cybercrimebekämpfung Tätigen. Bisher wurden u. a. die folgenden Themen behandelt: "Chat-Software-Auswertung sozialer Netzwerke", "Ermittlung von IP-Adressen", "Auswertung von Handys", "Probleme im Bereich des Cloud-Computing", "Technische Möglichkeiten und Grenzen bei der Überwachung des Internet-Datenverkehrs", "Technische Ermittlungsansätze in Fällen der Verschleierung von Telefonnummern (Spoofing)" und "Funktionsweise des Bitcoin-Bezahlsystems".

Seit dem 15. März 2016 koordiniert die sächsische Zentralstelle für die Bekämpfung von Cyberkriminalität der Generalstaatsanwaltschaft Dresden die Aus- und Fortbildung der sächsischen Staatsanwälte im Bereich Cyberkriminalität. Zu diesem Zweck hat sie ein Konzept für die Grundschulung aller sächsischen Staatsanwälte entwickelt und bietet auch fortgeschrittene Fortbildungsmaßnahmen für spezialisierte Beamte der Abteilung "Cyberkriminalität" an.

Daneben strebt die Zentralstelle zur Bekämpfung der Computer- und Internetkriminalität (Zentralstelle Cybercrime Sachsen) eine langfristige und enge Zusammenarbeit mit einer sächsischen Hochschule an. Im Rahmen dieser Zusammenarbeit sollen auch regelmäßig Fortbildungsveranstaltungen mit aktuellen IT-bezogenen Themen durchgeführt werden. Ein erster Workshop zu allgemeinen Themen der Datenauswertung fand im September 2014 statt.

Sachsen-Anhalt

Der Bereich kriminalpolizeiliche Fortbildung orientiert sich an dem bundesweiten Fortbildungskonzept der kriminalpolizeilichen Spezialfortbildung, zu der eine Bund-Länder-Projektgruppe eingerichtet wurde. Demnach werden allen Polizeibeamten Schulungen zum Thema Cyberkriminalität angeboten. Die Fortbildung gliedert sich dabei in drei Bereiche (polizeilicher Ersteinschreiter, Sachbearbeiter Cybercrime und Sachbearbeiter forensische Cybercrime). Die Häufigkeit der Lehrgangsdurchführung richtet sich nach dem von den Dienststellen gemeldeten Bedarf. Für Strafrichterinnen und Strafrichter sowie für Staatsanwältinnen und Staatsanwälte werden Schulungen im Themengebiet "Cyberkriminalität" angeboten: Das Ministerium für Justiz und Gleichstellung des Landes Sachsen-Anhalt bietet einmal jährlich eine dreitägige Fortbildungsveranstaltung zum Thema "Spezielle Ermittlungen, multimediale Kommunikation – Herausforderungen für die Strafverfolgung" an. Die Veranstaltung der Medienanstalt Sachsen-Anhalt "Jugendschutz im Internet – Ermittlung, Beweissicherung und Feststellung" (drei Tage), mit der den Teilnehmenden die Funktionsweise des Internets, internetbezogene Rechtsvorschriften, gerichtsfeste Dokumentationsmöglichkeiten und spezielle IT-Hilfsmittel zur Recherche im Internet näher gebracht werden sollen, findet seit 2004 statt. Für Bedienstete des Geschäftsbereichs mit unterschiedlichen Tätigkeitsbereichen (Systembetreuung, Behörden- und Geschäftsleitungen, Richterinnen und Richter, Rechtspfleger- und mittlerer Justizdienst, Justizangestellte) werden zum Teil mehrtägige Schulungen zum Thema "Informationssicherheit und Datenschutz" angeboten. Hierbei werden die einschlägigen Vorschriften zur Informationssicherheit sowie der sichere Umgang mit IT-Geräten und Daten vermittelt.

Schleswig-Holstein

Sachbearbeiter, die zur Bearbeitung von Ermittlungsverfahren im Deliktsbereich Cybercrime zuständig sind, erwerben ihr Fachwissen durch Lehrgänge im Rahmen des IuK-Fortbildungskonzeptes Schleswig –Holstein (SH) an der Polizeidirektion für Aus- und Fortbildung (PD AFB). Über das IT-Schulungsprogramm und das dazugehörige Teilprogramm Cybercrime ist geregelt, dass durch die PD AFB im Rahmen ihrer Laufbahnausbildung alle Auszubildenden und Studierenden die Qualifikation zum "Ersteinschreitenden Cybercrime gem. dem bundeseinheitlichen Aus- und Fortbildungskonzept Cybercrime" erlangen.

Im IT-Schulungsteilprogramm Cybercrime gibt es ein dem bundeseinheitlichem Aus- und Fortbildungsrahmen Cybercrime entsprechendes Seminarangebot, das es allen Mitarbeitern der Landespolizei Schleswig-Holstein ermöglicht, die Kompetenzen zu erlangen, die für eine Qualifikation zum Ersteinschreitenden Cybercrime erforderlich sind. Darüber hinaus existiert ein fortlaufend weiterentwickeltes, aktualisiertes und angepasstes Seminarangebot, über das die PD AFB auch weitere Zielgruppen im Deliktsfeld Cybercrime qualifiziert.

Insbesondere für die Zielgruppen der IT-Beweissicherung und der Sachbearbeitung Cybercrime im Landeskriminalamt Schleswig-Holstein werden ergänzend zum festen Seminarangebot auf Anforderung und bedarfsorientiert zusätzliche Seminare entwickelt und durchgeführt, die insbesondere die speziellen Bedürfnisse und Anforderungen befriedigen sollen. Dabei werden auch externe Referierende eingesetzt, Kooperationen mit anderen polizeilichen Fortbildungsträgern eingegangen und freie Seminarplätze über das Bundeskriminalamt veröffentlicht, um beispielsweise einen bundesweiten fachlichen Austausch zu verstärken. Das IT-Schulungsteilprogramm Cybercrime mit dem dazugehörigem u. a. im Extrapol veröffentlichten Seminarangebot wird regelmäßig durch die PD AFB überprüft, aktualisiert und den Anforderungen einer professionellen Landespolizei angepasst. CEPOL trägt insofern für die Schulung und Ausbildung bei, als dass ein Vertreter des LKA an dem diesjährigen "Cybercrime forensics & digital evidence" Kurs beim Estonian Forensic Institute teilnimmt.

Bayern

Zum Thema Cyberkriminalität fanden in Bayern für Sonderdezernenten bzw. IT-Ansprechpartner der Staatsanwaltschaften und Generalstaatsanwaltschaften erstmals 2012 besondere Schulungsmaßnahmen statt. Die durchgeführten Grund-Schulungen erstreckten sich in mehreren Teilen insgesamt über einen Zeitraum von zwei Wochen. Ziele der Schulungen waren neben technischen und ermittlungstaktischen vor allem rechtliche Problemstellungen sowie Fragen der IT-Forensik. Diese Schulungen werden durch einen mehrtägigen jährlichen Erfahrungsaustausch mit aktuellen Fragestellungen ergänzt. Diese Grundschulungen werden in einem Abstand von drei Jahren wiederholt angeboten. Daneben werden in Bayern jährlich spezielle einwöchige Schulungsmaßnahmen für Ermittlungsrichter angeboten mit dem Ziel, über technische und rechtliche Fragestellungen für Ermittlungsmaßnahmen im Bereich der Cyberkriminalität zu informieren.

Hamburg

Die Akademie der Polizei Hamburg bietet aktuell im ständigen Fortbildungskatalog vier Lehrgänge für die unterschiedlichen Zielgruppen an. Hierbei wird nach aufgabenspezifischen Anforderungen unterschieden:
I. + II. Ersteinschreiter-Lehrgänge (Einsteiger und Einsteiger-Grundkurs)

Der Einsteiger-Lehrgang dauert einen Tag. Die Lehrgangsteilnehmerinnen und -teilnehmer sollen in dem Lehrgang Computer- und Internetkompetenzen erwerben. Der Lehrgang soll sie in die Lage versetzen, sich mit den neu erworbenen Kenntnissen sicherer am Computer und im Internet zu bewegen. Der Einsteiger-Grundkurs dauert zwei Tage. Die Lehrgangsteilnehmerinnen und -teilnehmer sollen neben dem WWW-Dienst auch weitere, umfangreichere Kenntnisse zu verschiedenen Internetdiensten erwerben. Sie sollen bei der Aufnahme von Straftaten, die im Zusammenhang mit dem Internet stehen, handlungssicher werden. Sie sollen Handlungsnotwendigkeiten erkennen und die erforderlichen Maßnahmen einleiten können, den sicheren Umgang mit internetspezifischem Fachjargon erlernen und die Kompetenz und Auskunftsfähigkeit zum Thema Internet erweitern.

III. Ermittler für Sachverhalte mit standardmäßigen Cybercrime-Bezügen (Aufbaulehrgang)
Die Teilnehmerinnen und Teilnehmer des dreitägigen Aufbaulehrgangs sollen neben dem WWW-Dienst auch weitere, umfangreichere Kenntnisse zu verschiedenen Internetdiensten erwerben.

Sie sollen bei der Aufnahme von Straftaten, die im Zusammenhang mit dem Internet stehen, handlungssicher werden. Sie sollen Handlungsnotwendigkeiten erkennen und die erforderlichen Maßnahmen einleiten können, den sicheren Umgang mit internetspezifischem Fachjargon erlernen und die Kompetenz und Auskunftsfähigkeit zum Thema Internet erweitern.

IV. Spezial-Ermittler für technisch anspruchsvolle Cybercrime-Sachverhalte und Forensiker

(X-Ways)
Die Sachbearbeiter sollen während des fünf Tage dauernden Lehrgangs in die Lage versetzt werden, sichergestellte Daten mit der Anwendung X-Ways-Investigator nachvollziehbar auszuwerten und die Ergebnisse zu dokumentieren. Die Schulungen sind modular aufgebaut und können nur aufeinander aufbauend von Teilnehmern besucht werden. Die Lehrgänge werden je nach Bedarf und freien Ressourcen angeboten und durchgeführt.

Seit August 2014 werden die Auszubildenden der Akademie der Polizei Hamburg in der Grundausbildung an einem Tag zur Thematik Internet/Cybercrime beschult.

Die im Fachkommissariat Cybercrime des Landeskriminalamts Hamburg (LKA 54) beschäftigten Mitarbeiterinnen und Mitarbeiter erhalten abhängig von den persönlichen Voraussetzungen und den verfügbaren finanziellen Mitteln Schulungen. Einige Schulungsvorhaben werden den Mitarbeiterinnen und Mitarbeitern dienstlich angeboten, andere besuchen sie aus eigener Veranlassung, teils auch auf eigene Kosten. Diese Schulungen beinhalten ein breites Spektrum vom Themenbereichen der Computerforensik (von der Veranstaltung abhängige technische Tiefe) und zu unterschiedlichsten Einzelthemen (Betriebssysteme, Anwendungsprogramme, Hardware [wie "Handyforensik"] pp.). Die Schulungen reichen von Tages- über Wochenveranstaltungen hin zu langfristigen Maßnahmen, beispielsweise Studiengängen mit akademischen Abschlüssen von (Fern-) Universitäten.

Für die Hamburger Strafrichterinnen und Strafrichter sowie Staatsanwältinnen und Staatsanwälte wurde auf Landesebene zuletzt im Jahr 2012 eine Schulung zum Thema "Cyberkriminalität" angeboten. Dabei wurden insbesondere die in diesem Deliktsfeld einschlägigen Vorschriften des Strafgesetzbuchs und der Strafprozessordnung, des Telekommunikationsgesetzes und des Telemediengesetzes anhand von Fällen in ihrer speziellen Bedeutung für Straftaten im IT- Bereich erläutert.

Hessen

Seitens der Hessischen Justizakademie werden folgende Schulungen angeboten:

(1) Grundlagenschulung Internetermittlungen und Internetkriminalität

Die eintägige Veranstaltung, die erstmals 2014 in das Programm der Justizakademie aufgenommen wurde, soll Grundkenntnisse für Ermittlungen im Internet vermitteln. Dabei soll die gesamte Bandbreite der Eingriffsmaßnahmen bei Internetermittlungen eingeführt werden. Die Tagung wendet sich an Dezernentinnen und Dezernenten, die mit der Bearbeitung von Straftaten mit Internetbezug und/oder mit Jugendmedienschutzverfahren betraut oder daran interessiert sind.

(2) Internetermittlungen/Internetkriminalität

Bei der dreitägigen Veranstaltung sollen anhand von Referaten mit anschließender Diskussion die Möglichkeiten und Grenzen der Ermittlungen im Internet sowie die aktuellen materiell-rechtlichen Fragen der Internetkriminalität und des Jugendmedienschutzes (§§ 202 a ff., 263a, 131, 184 ff. StGB) erörtert werden. Dabei soll die gesamte Bandbreite der Eingriffsmaßnahmen bei Internetermittlungen dargestellt werden. Behandelt wird außerdem die Bekämpfung der Kinderpornografie im Internet unter Berücksichtigung der aktuellen Rechtsprechung und Entwicklung zur Telekommunikationsüberwachung. Die Tagung wird begleitet von Ermittlungsbeamten des Hessischen Landeskriminalamtes Wiesbaden, der Polizeipräsidien und des Bundeskriminalamts Wiesbaden, von externen Sachverständigen und von Vertretern von Internetdienstanbietern. Die Tagung, die seit 2008 regelmäßig einmal jährlich angeboten wird, wendet sich an Staatsanwältinnen und Staatsanwälte sowie Richterinnen und Richter, die mit Ermittlungsverfahren mit Internetbezug und/oder Jugendmedienschutzverfahren (einschließlich Kinderpornografie) befasst sind.

(3) Hessische Justizakademie – Internetkriminalität
Die eintägige Tagung wird regelmäßig zweimal im Jahr für Rechtsreferendarinnen und Rechtsreferendare angeboten. Sie wird auch im Rahmen der European Judicial Training Network (EJTN) ausgeschrieben. Sie ist in besonderem Maße für ausländische Teilnehmerinnen und Teilnehmer geeignet.

Niedersachsen

Es werden empfängerorientierte Angebote zu Prozessrecht, materiellem Recht und Einsatztaktik sowie Rechtshilfe gemacht. Entsprechende Schulungen werden mindestens jährlich mehrtägig abgehalten. Daneben gibt es eine Vielzahl von eng zugeschnittenen Angeboten und Austauschmöglichkeiten für Spezialkräfte. Bezüglich der Landespolizei ist das Angebot dort noch ausgeweitet und enthält in einem modular aufgebauten System ein fortlaufendes Schulungsangebot, welches in Kooperation mit den Staatsanwaltschaften teilweise auch von diesen in Anspruch genommen werden kann. Darüber hinaus wird die Thematik der Computerkriminalität als eines von mehreren Themen in weiteren Schulungen behandelt. In der von Niedersachsen angebotenen Tagung "Internationale Zusammenarbeit in strafrechtlichen Angelegenheiten" ist beispielsweise ein Referat zu "Auslandsermittlungen bei Computer- und Internetkriminalität" enthalten. Die ebenfalls von Niedersachsen organisierte Tagung "Das Opfer in der Strafrechtspflege" behandelt u. a. "Opferbedürfnisse im Bereich der Computerkriminalität".

Rheinland-Pfalz

Das Angebot der Landespolizeischule/Fachhochschule für öffentliche Verwaltung – Fachbereich Polizei – (LPS/FHöV) beinhaltet eigene Ausbildungsmodule, Module im Rahmen der Kooperation mit anderen Bundesländern und Angebote in Zusammenarbeit mit externen Anbietern. Die Ausbildungsmodule richten sich überwiegend an die Bediensteten der Polizei des Landes Rheinland-Pfalz. Hierbei werden unter anderem Schulungen zur Bedeutung digitaler Medien für die polizeiliche Sachbearbeitung, zu Internetermittlungen, zu Rechtsgrundlagen, zu Ermittlungen im Internet und web 2.0 für Ermittlungsbeamte sowie zur Cybercrime Multiplikatorenausbildung angeboten.

Darüber hinaus werden seitens der LPS/FHöV mit Unterstützung des Landeskriminalamtes Rheinland-Pfalz für Staatsanwältinnen und Staatsanwälte sowie Richterinnen und Richter der Strafgerichtsbarkeit themenspezifische Fortbildungsveranstaltungen angeboten. Diese beinhalten beispielsweise allgemeine Informationen zu Internetermittlungen, rechtliche Möglichkeiten der Internetermittlungen, Umgang mit Weblogs, Facebook, Twitter und andere, Betrugsmethoden, Manipulationsmöglichkeiten und Abo-Fallen.

Des Weiteren richtet die LPS/FHöV gemeinsame Seminare für Polizei und Justiz aus. Für das Jahr 2014 wurde das Seminar "Eingriffsrecht und Telekommunikation/ Internet" geplant. In diesem Seminar werden Datenarten, Erhebungsbefugnisse, Inhaltsüberwachung der Telekommunikation, Standortermittlungen, Ermittlungen im Internet sowie entsprechende rechtliche Grundlagen behandelt.

Die Seminare und Schulungen sind in der Regel für die Dauer von ein bis drei Tagen ausgelegt. Je nach Angebot finden die Schulungen einmal oder mehrmals jährlich statt. Die spezialisierten Mitarbeiter der forensischen IuK erhalten spezielle Schulungen zum Thema Cyberkriminalität. Das Ziel derartiger Schulungen ist es, die Mitarbeiter in die Lage zu versetzen, kompromittierte Systeme post mortem auf entsprechende digitale Spuren zu untersuchen. Schulungen im Bereich der Live-Forensik sind geplant.

Thüringen

Die Schulungsmaßnahmen der Thüringer Polizei im Bereich Cyberkriminalität orientieren sich am "Bundeseinheitlichen Aus- und Fortbildungskonzept zur Bekämpfung der IuK-Kriminalität".
Für die Zielgruppe "Ersteinschreiter" wurden die Inhalte in die Ausbildung zum mittleren Polizeivollzugsdienst (mPVD) integriert.
Aufbauend auf diese Grundkurse (GK) finden für die Zielgruppen Sachbearbeiter IuK-Kriminalität (SB IuKK) im weiteren Sinne (gelb gekennzeichnet) und SB IuKK im engeren Sinne, SB Ermittlungsunterstützung (Regionale Beweissicherung) und SB Forensische IuK (blau gekennzeichnet) weiterführende Fortbildungsveranstaltungen statt.

Beispielsweise wurden im Jahr 2013 folgende Fortbildungsveranstaltungen durchgeführt:

– 1x Seminar Betriebssystem/Anwendungen (I-510.21)

– 1 x Seminar UFED-PA (I-531.1)

– 1 x Seminar WK Internet (I-513.1)

– 1 x Windows 8 aus forensischer Sicht (I-540.1)

– 1 x GK Kryptografie (I-530.1)

– 1 x Workshop Forensisches Auswertetool Encase (I-532.1).

1. Gibt es besondere Ausbildungsmodule für forensische IT-Untersuchungsbeamte sowie für Ermittler von Cyberstraftaten?

Siehe auch Antwort zu Frage 10.B.1.

Das Bundeskriminalamt bietet unter anderem die zentrale Sachverständigenausbildung für Bund und Länder im Bereich IuK-Forensik an. Diese spezielle Ausbildung richtet sich ausschließlich an Experten. Darüber hinaus werden ad hoc bedarfsorientierte Speziallehrgänge organisiert und angeboten. Besondere Ausbildungsmodule für Cyberermittler sind die Speziallehrgänge "Kinderpornografie in Internet", "Arzneimittelkriminalität im Tatmedium Internet" und "Speziallehrgang für Mitarbeiter/-innen von Zentralstellen für Internetrecherchen". Die Cybercrimeermittler des BKA können weiterhin die Cybercrime-Grundlagenschulung als Grundausbildung besuchen.

Im Hinblick auf die Bundesländer wurden folgende Informationen gemeldet:

Baden-Württemberg

Das entsprechende Fortbildungskonzept untergliedert sich in 4 Teilbereiche, welche auf die Bedürfnisse der in der Frage 10 B 1 genannten hochspezialisierten Mitarbeiter der Ebene 3 abgestimmt sind. Jedem Teilbereich der Ebene 3 werden individuelle Fortbildungsinhalte – orientiert an den speziellen Bedarfen – vermittelt.

Brandenburg

Die angebotenen Aufbau- und Spezialmodule richten sich in erster Linie an Ermittlungsbeamte für Cyberstraftaten. Inhalte dieser Module sind Themen wie Internet, Recht, Tatortarbeit, Datensicherung, Datensichtung und Möglichkeiten der Auswertung. Seminare für speziellere Zielgruppen, zu denen auch die IT-Forensiker gehören, werden durch externe Angebote bzw. im Rahmen der bundesweiten Weiterbildung seitens des Bundeskriminalamtes abgedeckt.

Sachsen

Spezialfortbildungen und Qualifizierungen, die über den Bedarf einer zentralen Fortbildung hinausgehen, werden durch die Fachabteilungen (z. B. SN4C und Zentralstelle Cybercrime Sachsen) entweder intern oder mit externen Referenten organisiert.

Sachsen-Anhalt

Die besonderen Ausbildungsmodule für die Zielgruppe Sachbearbeiter forensische Cybercrime werden teilweise landesintern an der Fachhochschule Polizei, länderübergreifend im Rahmen der Sicherheitskooperation der Freistaaten Sachsen und Thüringen, der Länder Brandenburg, Sachsen-Anhalt und Berlin und auf Bundesebene unter Federführung des BKA angeboten.

Bayern

Von polizeilicher Seite werden über das Fortbildungsinstitut der Bayerischen Polizei spezielle mehrteilige Ausbildungsmodule für forensische IT-Untersuchungsbeamte und Ermittler von Cyberstraftaten angeboten.

Berlin

IT-Forensiker, die sich mit der Auswertung von Gerätschaften und Datenträgern beschäftigen, sind im Land Berlin bei der Polizei (LKA) angesiedelt. Nach hiesiger Kenntnis bestehen für die betreffenden Mitarbeiter entsprechende Schulungsangebote.

Hamburg

Aufgrund der Dezentralisierung der forensischen Auswertung von Datenträgern mit der Anwendung "X-Ways Investigator" wurden bzw. werden kriminalpolizeiliche Sachbearbeiterinnen und Sachbearbeiter bei der Akademie der Polizei Hamburg zur Arbeit mit dieser Anwendung in einem einwöchigen Lehrgang beschult (siehe Antwort zu Frage 10.B.1.).

Im Bereich der Computerforensik gibt es eine standardisierte Ausbildungsform zur Qualifizierung von Gutachtern, die beim BKA erfolgt. Diese wird den Mitarbeiterinnen und Mitarbeitern der Polizei Hamburg durchgängig angeboten und vor Aufnahme der eigentlichen Tätigkeit von diesen absolviert. Im Bereich der Ermittlungsbeamten existieren keine festen, stets verfügbaren und koordiniert zu absolvierenden Module. Die Inhalte werden nach Verfügbarkeit vermittelt.

Rheinland-Pfalz

Durch die LPS/FHöV werden regelmäßig eigene Ausbildungsmodule für forensische IT-Untersuchungsbeamte (z. B. im Netzwerk Forensik mit Wireshark, Virtualisierung in der Forensik) sowie für Ermittler von Cyberstraftaten (z. B. Eingriffsrecht und Telekommunikation/Internet) angeboten.

Darüber hinaus besteht für die genannten Zielgruppen im Rahmen der Kooperation mit anderen Bundesländern (über die LPS/FHöV) die Teilnahmemöglichkeit an entsprechenden Ausbildungsmodulen (z. B. digitale Forensik VI – Auswertung von Internet-Artefakten, digitale Forensik V – Live-Forensik). Weiterhin wird die Teilnahme an Veranstaltungen externer Anbieter durch die LPS/FHöV angeboten (z. B. IuK Sachverständigenausbildung – Modul 2.1.1 Wahrscheinlichkeit, Cybercrime Multiplikatorenausbildung, Grundlagenschulung "Ermittlungen Internet und web 2.0").

In Zusammenarbeit mit der Hochschule Albstadt-Sigmaringen wird zudem ein Zertifikatsprogramm im Rahmen des Projekts Open C3S angeboten. In dem aus 17 Modulen bestehenden Programm werden unter anderem Grundlagen digitaler Forensik bis hin zu speziellen Fachthemen wie z. B. Datenträger- oder Mobilfunkforensik vermittelt.

Ferner ermöglicht Rheinland-Pfalz besonders qualifizierten Polizeibeamten die Teilnahme am Masterstudiengang "Digitale Forensik" an der Hochschule Albstadt- Sigmaringen. Sie sollen künftig in ausgewählten Führungsfunktionen ab dem 4. Einstiegsamt verwendet werden.

Spezielle Ausbildungsmodule gibt es nicht. Ein Teil der Fortbildungslehrgänge wird jedoch als Vertiefungslehrgang angeboten bzw. in Kooperation mit der für Cyberkriminalität zuständigen Abteilung des Landeskriminalamts.

Thüringen

Das bundesweites Aus- und Fortbildungskonzept für Sachverständige in der FIuK ist modular aufgebaut. Im Bereich forensische IuK in Thüringen (Dezernat 43 des Landeskriminalamts Thüringen und die regionalen Beweissicherungseinheiten in den Landespolizeiinspektionen) werden jährlich Fortbildungsmaßnahmen durchgeführt, die komplexe Software-Werkzeuge der IT-Forensik schulen. Dazu zählen sowohl Lehrgänge als auch gemeinsame durch das Dezernat 43 organisierte Workshops. Sachverständige des Dezernates 43 FIuK nehmen weiterhin an Speziallehrgängen sowie jährlichen bundesweiten Fachtagungen und Workshops, wenn verfügbar, in einigen Spezialrichtungen teil.

Die Abteilung KI des Bundeskriminalamtes ist im Bereich Cyberkriminalität als Koordinierungsstelle für die Aus- und Fortbildung der Polizeibehörden des Bundes und der Länder zuständig. Die Abteilung KI kooperiert dabei eng mit nationalen und internationalen Aus- und Fortbildungsinstituten. Das Bundeskriminalamt (BKA) ist Mitglied der ECTEG und hat im Rahmen des EU-finanzierten ISEC2010-Programms drei internationale Kurse für die ECTEG entwickelt und EUROPOL zur Verfügung gestellt. CEPOL und EUROPOL (EC3) sind ebenfalls in der ECTEG vertreten, wodurch eine regelmäßige Abstimmung und ein enge Zusammenarbeit gewährleistet sind.

Im Hinblick auf die Bundesländer wurden – ohne Anspruch auf Vollständigkeit – folgende Informationen gemeldet:

Berlin

In den letzten 15 Jahren konnte ein Mitarbeiter des Landeskriminalamts (LKA) 13 einmal an einem Europol-Lehrgang zur Kinderpornografie teilnehmen. Inwieweit diese Inhalte in den Lehrgang beim Bundeskriminalamt (BKA) einfließen, kann hier nicht beurteilt werden. Schulungsangebote für Mitarbeiter der Staatsanwaltschaft und der Gerichte werden in Abstimmung mit dem Referat für organisierte Computerkriminalität durch die Senatsverwaltung für Justiz und Verbraucherschutz durchgeführt. Eine Beteiligung von EU-Organisationen fand bislang noch nicht statt.

Brandenburg

Die basisorientierte Schulung der Polizeivollzugsbeamten zur Bearbeitung von Cyberkriminalität liegt in der Zuständigkeit der Fachhochschule für Polizei (FHPol). Eine Weiterqualifizierung von Spezialisten, insbesondere im Bereich der IT-Forensik, erfolgt in Verantwortung des LKA. Für die Fortbildung des höheren Justizdienstes der Länder Berlin und Brandenburg ist seit dem 1. Januar 2005 das Gemeinsame Juristische Prüfungsamt der Länder Berlin und Brandenburg zuständig. Fortbildungsangebote von CEPOL, die über das Bundesministerium der Justiz und für Verbraucherschutz an das GJPA für Bedienstete des höheren Justizdienstes herangetragen werden, werden regelmäßig für die Bediensteten ausgeschrieben. In 2013/2014 befand sich dabei kein Fortbildungsangebot zum Thema Cybercrime.

Baden-Württemberg

Zuständig für die inhaltliche Ausgestaltung der Schulungen ist das Zentrum für interkulturelle Kompetenzen und Sprachen (ZIK), das insoweit eng mit der Abteilung 5 des LKA Baden-Württemberg zusammenarbeitet. Es ist ferner beabsichtigt, die erfolgreiche Zusammenarbeit mit der Polizei im Bereich der Grundlagenschulungen wieder aufzunehmen. Die formale Abwicklung der von dem ZIK konzipierten Schulungen erfolgt über das Justizministerium; dort werden auch die Haushaltsmittel verwaltet. Im Rahmen einer Fortbildung sind bei Europol und Eurojust tätige Kollegen als Referenten aufgetreten.

Mecklenburg-Vorpommern

Originär zuständig für Schulungen zum Thema Cyberkriminalität ist die Fachhochschule für öffentliche Verwaltung, Polizei und Rechtspflege des Landes Mecklenburg-Vorpommern in 18273 Güstrow. Fortbildungsprogramme werden im Rahmen der Sitzungen der Mitglieder der Programmkonferenz geplant. Darüber hinaus können auch vom Geschäftsbereich (Generalstaatsanwalt bzw. Oberlandesgericht) zu besonders wichtigen Themen Fortbildungen, Workshops oder Anderes angeboten werden. Fortbildungsaufgaben im Bereich der Bekämpfung der Cyberkriminalität werden von der mit einem Dezernenten besetzten Zentralstelle beim Generalstaatsanwalt wahrgenommen.

Niedersachsen

In Niedersachsen ist die Polizeiakademie (PA) zentraler Fortbildungsträger in der Landespolizei und insoweit auch für Schulungen zum Thema Cyberkriminalität zuständig. Dazu wurde von der PA im Zusammenwirken mit den polizeilichen Flächenbehörden ein modulares Aus- und Fortbildungskonzept entwickelt. Dieses ist eng an das bundeseinheitliche Aus- und Fortbildungskonzept angelehnt und wird fortlaufend aktualisiert. Daneben nehmen die Spezialisten zur Cybercrime-Bekämpfung an länderübergreifenden Fortbildungsveranstaltungen teil bzw. nutzen Angebote von Privaten, auch im Rahmen von Hospitationen. In Kooperation mit der Hochschule Emden/Leer absolvieren die Spezialisten der Cybercrime-Bekämpfung gegenwärtig ein Pilot-Webinar zu den Themen Betriebssysteme und Netzwerktechnologie. Europäische Angebote für Schulungen zum Thema Cyberkriminalität wurden bislang nicht in Anspruch genommen.

Im Bereich der Staatsanwaltschaften sind in Absprache mehrere Ebenen mit Konzeption und Durchführung von Schulungen befasst, wobei hier letztlich dem Justizministerium eine Koordinierungsfunktion zukommt.

Saarland

LPP 302 und Fachhochschule für Verwaltung, Fachbereich Polizeivollzugsdienst.

Sachsen-Anhalt

Für die zentrale Fortbildung ist die Fachhochschule Polizei zuständig. Darüber hinaus werden in den Behörden und Einrichtungen der Landespolizei schwerpunktmäßig behördenspezifische Besonderheiten in dezentralen oder im Rahmen der verfügbaren Haushaltsmittel in externen Fortbildungen in eigener Zuständigkeit durchgeführt. Die Angebote internationaler Aus- und Fortbildungseinrichtungen wie CEPOL stehen allen Polizeibeamten zur Verfügung und ergänzen die landesinternen oder nationalen Fortbildungsangebote. Eine Zuständigkeitskonzentration für Schulungen im Bereich Cyberkriminalität gibt es nicht. Die Veranstaltungen werden von dem Ministerium für Justiz und Gleichstellung (I.), der Deutschen Richterakademie (II.) beziehungsweise Judicial Institute – Scotland, Institute of Judicial Training – Brussels, Academy of European Law (ERA), Centro de Estudos Judiciários – Portugal, National Institute of Magistracy oder French National School for the Judiciary (ENM) (III.) durchgeführt.

Bayern

Die Schulungen im Bereich der Justiz werden durch das Aus- und Fortbildungsreferat im Bayerischen Staatsministerium der Justiz organisiert und koordiniert, in enger Zusammenarbeit mit dem Fachreferat für Interkriminalität in der Strafrechtsabteilung des Justizministeriums. An diesen Schulungen waren CEPOL, ECTEG und Europol/EC3 bisher nicht beteiligt.

Bremen

Polizeiliche Schulungen werden für die Bremer Polizei durch das Bundeskriminalamt (BKA) und die Landeskriminalämter angeboten. Die Staatsanwaltschaft Bremen bedient sich der Fortbildungsveranstaltungen der Richterakademie oder anderer Bundesländer.

Hessen

Für die Organisation der in Frage 10.B.1. aufgeführten Schulungen sind die Hessische Justizakademie sowie die Deutsche Richterakademie zuständig. Die genannten Organisationen auf EU-Ebene waren insoweit bislang nicht beteiligt.

Hamburg

Für den polizeilichen Bereich ist grundsätzlich die Akademie der Polizei Hamburg zuständig und erster Ansprechpartner für Schulungsmaßnahmen. Es gibt jedoch diverse Fortbildungsmaßnahmen, insbesondere Spezialistenfortbildungen, die nicht von der Akademie angeboten werden können. Die angesprochenen Organisationen der EU haben aktuell keinen oder nur sehr marginalen Einfluss auf die Schulungen.

Für Schulungen im justiziellen Bereich ist das Referat Personalentwicklung und Fortbildung der Behörde für Justiz und Gleichstellung zuständig. Derzeit findet keine Kooperation mit der Europäischen Polizeiakademie, der europäischen Gruppe für Schulung und Ausbildung in Bezug auf Cyberkriminalität oder Europol/EC3 statt.

Rheinland-Pfalz

a) Polizeiliche Ebene

Die LPS/FHöV ist für zentrale Schulungsmaßnahmen zum Thema Cybercrime zuständig. Hierbei wird in engem Kontakt mit dem Polizeipräsidium und dem LKA Rheinland-Pfalz den Bedarf ermittelt und die Ziele/Inhalte der Schulungen abgestimmt. Die Angebote der Europäischen Polizeiakademie werden landesintern durch die zentrale Koordinierungsstelle der LPS/FHöV ausgeschrieben und bedarfsorientiert besetzt. Auf die praktische Arbeit auf der Ebene der Bundesländer haben die CEPOL-Maßnahmen aufgrund der sehr geringen Zahl der zur Verfügung stehenden Teilnehmerplätze (für Deutschland in der Regel nur ein bis zwei Plätze) sowie des Umstandes, dass sie eher selten angeboten werden, im Grunde aber keinen messbaren Einfluss. Schulungsangebote von Europol oder auch der ECTEG spielten bislang keine Rolle.

b) Justizielle Ebene

Für Schulungen der Richterinnen und Richter sowie der Staatsanwältinnen und Staatsanwälte sind primär das Ministerium der Justiz und für Verbraucherschutz und sekundär die Behörden vor Ort selbst zuständig.

Sachsen

Die Organisation der Fortbildungen und das Gewinnen geeigneter Referenten obliegen der Generalstaatsanwaltschaft Dresden und dem Sächsischen Staatsministerium der Justiz. Die auf EU-Ebene eingerichteten Organisationen wie die Europäische Polizeiakademie (CEPOL), die Europäische Gruppe für Schulung und Ausbildung in Bezug auf Cyberkriminalität (ECTEG) und Europol/EC3 waren an Schulungsmaßnahmen bislang nicht beteiligt.

Thüringen

Für die Fortbildung im Bereich Cybercrime ist innerhalb der Thüringer Polizei das Bildungszentrum der Thüringer Polizei (BZThPol) zuständig.

Darüber hinaus werden jedoch durch Thüringen auch Angebote im Rahmen der Sicherheitskooperation sowie des Bundeskriminalamts (BKA) wahrgenommen. In welchem Umfang die Europäische Polizeiakademie (CEPOL), die Europäische Gruppe für Schulung und Ausbildung in Bezug auf Cyberkriminalität (ECTEG) und Europol/EC3 zu den Schulungsmaßnahmen bspw. des BKA beitragen, konnte nicht beurteilt werden.
Für die Ausbildung im Bereich Cyberkriminalität stehen derzeit im Bundeskriminalamt ca. 200 000 EUR pro Jahr zur Verfügung.
Diese Kosten setzen sich aus Dozentenhonoraren, Reisekosten und der Beschaffung von Hard- und Software zusammen.

Die Tagungsstätte der Deutschen Richterakademie in Trier wendete 2014 allein 151 844 EUR zur Bezahlung der Referentenhonorare auf; hinsichtlich der Tagungsstätte der Deutschen Richterakademie in Wustrau betrugen die Ausgaben allein für die Referentenhonorare im Jahr 2014 178 591 EUR.

Im Hinblick auf die Bundesländer wurden – ohne Anspruch auf Vollständigkeit – folgende Informationen gemeldet:

Baden-Württemberg

etwa 20 000 EUR pro Jahr aus Fortbildungsmitteln des Justizhaushalts für Schulungen der Staatsanwältinnen und Staatsanwälte.

Brandenburg:

ca. 7 000 EUR - 10 000 EUR.

Saarland:

etwa 20 000 EUR.

Sachsen-Anhalt:

ca. 40 000 EUR.

Bayern:

ca. 10 000 EUR.

Bremen:

ca. 10 000 EUR Jahr.

Hamburg:

Die externen Schulungskosten werden auf ca. 15 000 EUR pro Jahr geschätzt. Das Gesamtbudget beträgt im Schnitt rund 180 000 EUR pro Jahr.

Hessen:

Für die von der Hessischen Justizakademie ausgerichteten Tagungen werden jährlich ca. 15 000 EUR aufgewendet.

Niedersachsen:

etwa 10 000 EUR (staatsanwaltschaftlichen Ausbildungsangebote).

Rheinland-Pfalz:

im Jahr ca. 10 000 EURE (für Fortbildungsmaßnahmen auf polizeilicher Ebene).

Thüringen:

2013 ca. 20 000 EUR und 2014 ca. 36 000 EUR.

Grundsätzlich stehen die vom Bundeskriminalamt angebotenen Kurse allen (Polizei-)Beamten und Angestellten offen, die entsprechenden Aus- und Fortbildungsbedarf haben. Dies können auch Kolleginnen und Kollegen sein, die explizit mit Aufgaben der internationalen Zusammenarbeit betraut sind.

Im Hinblick auf die Bundesländer wurden folgende Informationen gemeldet:

Berlin:

Drei Mitarbeiter des Landeskriminalamts (LKA) 33 haben Seminare auf EU-Ebene besucht. Der Ort war Ryton in GB, angeboten wurde: "Advanced Network Investigators Course". Die Kurse dauerten jeweils eine Woche und sind von der EU finanziert worden.

Diese Seminare haben immer zwei Zielstellungen:

1. Netzwerkarbeit (Austausch von Infos auf Ermittlerebene, Kontakte knüpfen usw.).
2. Fachliche (inhaltliche) Fortbildung. Thema war: "Internet investigations for advanced users".

Selbige Mitarbeiter nehmen u. a. auch Aufgaben der internationalen Zusammenarbeit wahr, wenn es einen konkreten Anlass gibt. Auffrischungskurse werden zurzeit nicht angeboten.

Brandenburg:

Die an der Fachhochschule für Polizei (FHPol) angebotenen Seminare richten sich an Zielgruppen mit unterschiedlichen Aufgabengebieten. Dabei erfolgt keine Differenzierung hinsichtlich einer internationalen oder nationalen Zusammenarbeit.

Das Gemeinsame Juristische Prüfungsamt der Länder Berlin und Brandenburg hat in den Jahren 2013 und 2014 jeweils eine eintägige Fortbildungsveranstaltung zum Thema "Internationale Rechtshilfe in Strafsachen" ausgerichtet. Ein Aspekt dieser Fortbildung war auch die Zusammenarbeit mit Europol und OLAF, die u. a. gegen die grenzüberschreitende Computerkriminalität vorgehen.

Saarland:

Im Saarland wird die Grundqualifizierung Cybercrime ("Ersteinschreiterlehrgang") angeboten.

Hamburg:

Eine obligatorische Schulung der mit Rechtshilfeaufgaben betrauten Mitarbeiterinnen und Mitarbeiter der Polizei Hamburg findet in Bezug auf Cyberkriminalität nicht statt. Sollten im konkreten Fall Fragen auftreten, so stehen die Experten des Fachkommissariats Cybercrime beratend zur Verfügung.

Der Staatsanwaltschaft Hamburg stehen für den Bereich der internationalen Rechtshilfe die bundesweiten Fortbildungsangebote der Deutschen Richterakademie zur Verfügung. Diese in der Regel einwöchigen Tagungen werden zu verschiedenen Themen aus dem Bereich der internationalen Rechtshilfe (u. a. auch mit Bezug zur Cyberkriminalität) angeboten, teilweise auch mit vertiefendem Inhalt.

Niedersachsen:

Die Angebote im Bereich Cyberkriminalität sind in weiten Teilen offen für Teilnehmer aus dem genannten Kreis. Zu berücksichtigen ist, dass die Zentralstellenabteilungen ihre Rechtshilfemaßnahmen eigenständig gestalten, ihnen somit eine Doppelfunktion zukommt, zumindest hinsichtlich des verfahrensbezogenen ausgehenden Rechtshilfeverkehrs. Spezielle Angebote in Fragen der Cyberkriminalität ausschließlich für Rechtshilfedezernenten sind nicht bekannt und auch nicht vorgesehen. Allerdings werden auch im Bereich der Rechtshilfedezernate besondere Fortbildungsangebote auch von der Zentralen Stelle Organisierte Kriminalität und Korruption (ZOK) und vom EJN mitgestaltet, sodass bei Erkennen eines speziellen Bedarfs bestimmte Themen mit eingebracht werden.

Sachsen:

Es werden keine speziellen auf Cyberkriminalität bezogenen Schulungsmaßnahmen für diejenigen Dezernentinnen und Dezernenten angeboten, die Aufgaben im Rahmen der internationalen Zusammenarbeit wahrnehmen.

Sachsen-Anhalt:

Mit der thematischen Ausrichtung unter anderem zu Zuständigkeitsfragen und internationaler Rechtshilfe richtet sich die bereits beschriebene Veranstaltung "Erscheinungsformen der Internetkriminalität und ihre Bekämpfung" auch an Personen, die Aufgaben im Rahmen der internationalen Zusammenarbeit wahrnehmen. Gleiches gilt für den o.g. Vortrag zum Thema "Identifizierung von Tätern und Opfern aus kinderpornografischen Medien – auch im Rahmen der internationalen Zusammenarbeit" in der Schulung "Aktuelle Entwicklungen in Kriminalistik und Strafrechtspflege". Im Programm der Fortbildung "Strafrecht und Internet" ist mit dem Thema "Auslandsermittlungen in IuK-Verfahren" ebenfalls ein Angebot enthalten für Personen, die im Rahmen internationaler Zusammenarbeit tätig sind.

Aus Sicht des Saarlandes spielt eine Kooperation mit Exzellenzzentren für die Fortbildung der Cybercrime-Spezialdienststelle und der Forensik eine große Rolle. Eine strukturierte Zusammenarbeit mit diesen Stellen wird im Rahmen der ZAC-Funktion des Dezernats LPP 222 aufgebaut (z. B. Universität des Saarlandes, DFKI, HTW).

In der Aus- und Fortbildung im Bereich Cyberkriminalität spielen Hochschulen eine immer größere Rolle. Das Bundeskriminalamt (BKA) arbeitet eng mit verschiedenen Hochschulen zusammen. Durch den Hochschulverbund des OpenC³S-Programms besteht Kontakt zu insgesamt neun Hochschulen und Universitäten. Im Rahmen der Sachverständigenausbildung "Forensische IuK" wird die Spezialisierungsebene komplett von Hochschulen durchgeführt, die Spezialisierungsebene der Fachrichtungen Windows, Linux, Macintosh, Netzwerke/Internet und Mobile-Forensik von der Hochschule Albstadt-Sigmaringen, die Spezialisierungsebene im Bereich Kryptologie in enger Kooperation mit der Ruhruniversität Bochum.

Im gegenwärtigen Bachelor-Studiengang der Fachhochschule des Bundes für öffentliche Verwaltung – Fachbereich Kriminalpolizei wird ein Modul mit dem Titel "Kriminalität im Zusammenhang mit Informations- und Kommunikationsmedien" durchgeführt. Das Modul dauert vier Wochen und besteht u. a. aus einer technischen Einführung in informationstechnische Grundlagen. Dort werden durch externe Lehrbeauftragte Grundbegriffe und Funktionsweise des Internets vermittelt. Das "Phänomen Cybercrime" wird daneben kriminologisch und strafrechtlich bewertet und es werden den Studierenden kriminalistische und spezifische eingriffsrechtliche Instrumente des Phänomens vorgestellt. Eine Szenarien-basierte Übung zum Abschluss dient den Studierenden als Möglichkeit, die Lehrinhalte an einem fiktiven Sachverhalt mithilfe von Praktikern zu vertiefen.

Im Hinblick auf die Bundesländer wurden – ohne Anspruch auf Vollständigkeit – folgende Informationen gemeldet:

Baden-Württemberg:
Im Zuge der Polizeireform wurde der gesamte Bereich der Ausbildung, des Studiums und der Fortbildung unter dem Dach der Hochschule für Polizei (HfPol) zentralisiert. Ziel war es, den gesamten Bildungsbetrieb sowohl quantitativ als auch qualitativ aus "einer Hand" anzubieten und zu koordinieren. Die HfPol spielt damit als gemeinsamer und alleiniger Bildungsverantwortlicher in Baden-Württemberg auch eine zentrale Rolle bei der Aus- und Fortbildung im Bereich Cyberkriminalität. Für diesen Bereich wurde innerhalb des Instituts Fortbildung ein eigener "Institutsbereich Cybercrime" (IB Cybercrime) geschaffen.

Parallel zu der Aus- und Fortbildung existiert seit 2014 eine Sonderlaufbahn Cyberkriminalist, in welcher Quereinsteiger aus der IT-Branche für den gehobenen Polizeivollzugsdienst qualifiziert werden. Die Ausbildung dieser zukünftig in der Ebene 3 verwendeten Beamten läuft unter Federführung des IB Cybercrime.

Des Weiteren wurde durch Dozenten der HfPol BW im Rahmen eines Forschungssemesters geprüft, wie ein "paralleler" Studiengang mit Schwerpunkt "Cybercrime" an der HfPol BW durchführbar wäre.

Brandenburg:

Im Rahmen der Ausbildung und des Bachelorstudienganges an der FHPol werden die vorhandenen Fächer wie Kriminologie, Kriminalistik und Strafrecht um Schwerpunkte zur Thematik "Cyberkriminalität" ergänzt. Darüber hinaus wird die Thematik im Rahmen der Nutzung der E-Learning Anwendung vermittelt. Weiterhin können sich die Studenten in einem 3-wöchigen Wahlpflichtmodul "IuK-Kriminalität" – Computerkriminalität/Verfolgung von Internetstraftaten intensiv mit verschiedensten Phänomenen der Cyberkriminalität auseinandersetzen.

Mecklenburg-Vorpommern:

Durch das Dezernat 45 des Landeskriminalamts Mecklenburg-Vorpommern erfolgt eine enge Zusammenarbeit mit der Hochschule in Wismar auf der Grundlage einer Kooperationsvereinbarung. Es wurden bereits zwei E-Learning-Videos zu den Themen "Auslesen von E-Mail-Headern" und "Ermittlungen in sozialen Netzwerken" produziert. Durch Studenten der Hochschule Wismar, insbesondere aus dem Bereich Informatik, wurden Praktika im Landeskriminalamt MV durchgeführt. Darüber hinaus wurden Studenten bei der Erstellung ihrer Bachelorarbeit oder Masterthesis durch Mitarbeiter des Landeskriminalamtes MV in der Themenfindung sowie während der Erstellung der Arbeiten betreut.

Im Wintersemester 2014 wird an der Hochschule Wismar erstmals der berufsbegleitende Bachelorstudiengang "Forensik Engineering" angeboten, welcher Modulare Inhalte zur Cyberkriminalität vermittelt.

Niedersachsen:

In Kürze wird ein Rahmen-Kooperationsvertrag zwischen dem Landespolizeipräsidium Niedersachsen und der Hochschule Emden/Leer unterzeichnet, der eine Zusammenarbeit in den Bereichen Cybersicherheit und Cyberkriminalitätsbekämpfung durch konkrete Projekte in der Fortbildung, Forschung und Lehre vorsieht. Neben wechselseitigen Hospitationen, gemeinsamen Forschungsprojekten und gegenseitigen Teilnahmen an Fortbildungsveranstaltungen ist u. a. beabsichtigt, die Einführung spezieller berufsbegleitender Studiengänge an der Hochschule Emden/Leer für Bedienstete der Landespolizei zu den Themen Cyberkriminalität und Cybersicherheit zu prüfen.

Saarland:
Deutsche Hochschule der Polizei (DHPol) bietet entsprechende Fortbildungen für Führungsverantwortliche an. Die Universität des Saarlandes hat einen neuen Studiengang "Cybersicherheit" eingerichtet.

Sachsen-Anhalt:
Das Thema Cyberkriminalität ist im Lehrplan des Studiums an der Fachhochschule Polizei als Pflichtfach im Abschlussstudium mit einem Umfang von 20 Lehrveranstaltungsstunden vorgesehen. Die Studierenden lernen,

- Lagebild und Erscheinungsformen der Kriminalität im Zusammenhang mit der Informations- und Kommunikationstechnologie darstellen zu können,
- die relevanten Straftatbestände (insbes. § 148 TKG, §§ 202a ff. StGB) anwenden zu können,
- als Ersteinschreiter vor Ort und im Rahmen der Anzeigenaufnahme notwendige polizeiliche Maßnahmen im Zusammenhang mit den o.g. Erscheinungsformen der Kriminalität durchführen zu können.

Darüber hinaus wird ebenfalls im Abschlussstudium das Thema Cyberkriminalität angeboten. Hier werden in einem Umfang von vier Lehrveranstaltungsstunden aktuelle Erscheinungsformen der Internetkriminalität dargestellt und mit Bezügen zur grenzüberschreitenden Zusammenarbeit verbunden. Thematisch sind insoweit beispielhaft zu nennen: die europäische Cybercrime-Konvention, Bootnetze der DOS/DDOS-Attacken, Trojaner. Die genannten Themen sind Bestandteil des Wahlpflichtmoduls "Internationale Kriminalitätsbekämpfung".

Hamburg:
Der Fachhochschulbereich der Akademie der Polizei Hamburg ist für die grundlegende Ausbildung der Polizei Hamburg für den Bereich der Cyberkriminalität zuständig. Seit 2007 sind Erscheinungsformen der Computerkriminalität einschließlich der Vermittlung der dazugehörigen Grundlagen fester Bestandteil des Curriculums des Fachhochschulbereichs (bzw. der Vorgängerorganisation der Hoch-schule der Polizei Hamburg..
Im Grundstudium werden den Studierenden in der Lehrveranstaltung "Grundlagen der Informations- und Kommunikationstechnik" folgende Kenntnisse vermittelt:
• Aufbau von Computeranlagen und Computernetzwerken
• Technologien und wichtigste Protokolle im Internet
• Grundlagen der IT-Sicherheit und Sicherheitsrisiken
• Datensysteme der Polizei Hamburg und des Bundes.

Darauf aufbauend erhalten die Studierenden im Hauptstudium in der Lehrveranstaltung "Computerkriminalität" folgende Kompetenzen:

• Bewertung von Straftaten im Zusammenhang mit der elektronischen Datenverarbeitung

• Bewertung von elektronischen Daten als Beweismittel

• Kenntnisse über die Prinzipien der Sicherung und des Umgangs mit gesicherten elektronischen Daten und die hierbei unterstützenden Dienststellen der Polizei Hamburg.

Im Wesentlichen beinhaltet die Lehrveranstaltung folgende Themenbereiche:

• Straftaten im IuK-Bereich und unter Nutzung des Internets

• Strafverfolgung im Internet: technische Grundlagen

• Sicherung und Auswertung von Datenträgern, Netzwerkdaten und -spuren

• Computer als Strafverfolgungsinstrument.

Beide Lehrveranstaltungen haben einen Zeitansatz von 165 Stunden. Die Vermittlung dieser Schlüsselkompetenzen erfolgt fächerübergreifend durch die Disziplinen Angewandte Informatik und Rechtswissenschaft. Darüber hinaus besteht eine enge Kooperation mit dem Landeskriminalamt Hamburg, um neue Phänomene der Computerkriminalität zu erfassen und in die Lehr- und Forschungspläne aufzunehmen.

In Kooperation mit der Akademie (vormals Hochschule) der Polizei Hamburg und der Behörde für Justiz und Gleichstellung hat die Universität Hamburg im Jahre 2013 ein Symposium zur Cyberkriminalität veranstaltet, im Rahmen dessen u. a. über die Erscheinungsformen dieses Kriminalitätsfeldes, die einschlägigen Straftatbestände im deutschen Strafgesetzbuch und die Ermittlungsmethoden der Strafverfolgungsbehörden mit Fachleuten und Studentinnen und Studenten diskutiert wurde.

Sachsen:

Die Hochschule Mittweida in Sachen hat ferner den bundesweit einzigen Studiengang "Allgemeine und digitale Forensik" eingerichtet. Dort werden IT-Experten auf dem Gebiet der Computerforensik fachspezifisch ausgebildet. Der Studiengang vermittelt forensische Kenntnisse, welche für den praktischen Einsatz in Behörden, aber auch in Unternehmen konzipiert sind. Im Zentrum stehen die Computerforensik und sie umgebende Spezialgebiete, von der Kryptologie bis zur Kriminologie. Die im Rahmen dieses Studiengangs vermittelten Kenntnisse und Fähigkeiten können auch bei der Bekämpfung der Cyberkriminalität eingesetzt werden.

Thüringen:

Es existieren mehrere Hochschulen im Bundesgebiet, die eine Ausbildung zum IT-Forensiker anbieten. Im bundesweiten Sachverständigenausbildungskonzept werden spezielle Module zusammen mit Hochschulen (Bochum, Albstadt-Sigmaringen) konzipiert. In Thüringen wurde 2006 auf Initiative des Dezernates 43 des Landeskriminalamt Thüringen (TLKA) ein Grundlagenkurs Kryptografie über die TU Ilmenau konzipiert. Dieser wurde in der Vergangenheit mehrmals am Bildungszentrum der Thüringer Polizei in Meiningen für zahlreiche Teilnehmer aus verschiedenen Bundesländern durchgeführt.

An der Fachhochschule für Verwaltung FB Polizei wurde durch das Dezernat 64 des TLKA ein Seminar im Bereich Bekämpfung der Kinder- und Jugendpornografie durchgeführt.

Cyberkriminalität wird im Geschäftsbereich des Thüringer Ministeriums für Bildung, Wissenschaft und Kultur folgendermaßen definiert: unterschiedlichste kriminelle Tätigkeiten, bei denen Computer und Informationssysteme entweder Hauptinstrument oder Hauptziel sind; die Cyberkriminalität umfasst herkömmliche Straftaten (z. B. Betrug, Fälschung, Identitätsdiebstahl), inhaltsbezogene Straftaten (z. B. Verbreitung von kinderpornografischem Material über das Internet, Anstachelung zum Rassismus) und Straftaten, die nur über Computer und Informationssysteme möglich sind (z. B. Angriffe auf Informationssysteme, Überlastungsangriffe, Schadprogramme).

Die Thüringer Hochschulen bieten überwiegend keine speziellen Kurse zu dem wie vorstehend definierten Thema "Cyberkriminalität" an. Gleichwohl ist das Thema in verschiedensten Lehrveranstaltungen fest verankert, insbesondere wenn es um Fragen der IT- und Netz-Sicherheit geht wie z. B. Grundlagen, Gefährdungen, Angriffsmechanismen und kryptografische Verfahren zur Sicherung vernetzter IT-Systeme.
Das Thema "Cyberkriminalität" ist aber auch beispielsweise in den Bereichen "Mediensicherheit" und "Content Management und Web Technologien" Schwerpunkt der Forschung an der Bauhaus-Universität Weimar.

8.2. Sensibilisierungsmaßnahmen

Bedingt durch das föderale System Deutschlands wird die bundesweite polizeiliche Präventionsarbeit nicht durch eine bundesweit zentrale Stelle, sondern in ständiger Zusammenarbeit der Polizeien der Länder und des Bundes konzipiert und umgesetzt. Relevanz hat hier insbesondere das "Programm Polizeiliche Kriminalprävention der Länder und des Bundes" (ProPK), dessen Präventionsaktivitäten zum Thema Cyberkriminalität nachfolgend dargestellt werden.

Das ProPK verfolgt das Ziel, die Bevölkerung, Multiplikatoren, Medien und andere Präventionsträger über Erscheinungsformen der Kriminalität und Möglichkeiten zu deren Verhinderung aufzuklären. Dies geschieht unter anderem durch kriminalpräventive Presse- und Öffentlichkeitsarbeit und durch die Entwicklung und Herausgabe von Medien, Maßnahmen und Konzepten, die die örtlichen Polizeidienststellen und andere Einrichtungen, zum Beispiel Schulen, in ihrer Präventionsarbeit unterstützen.

ProPK hat bislang zu der Thematik Cyberkriminalität/Mediensicherheit folgende Initiativen gestartet, Medien produziert bzw. herausgegeben und bundesweit verteilt:

- Handreichung "Im Netz der Neuen Medien":
  Die Handreichung stellt eine umfassende Informationsgrundlage zum Thema Medienkompetenz von Kindern und Jugendlichen dar. Sie vermittelt grundlegendes Wissen in diesem Themenfeld u. a. auch zu Cybermobbing. Für eine tiefer gehende Beschäftigung finden sich Hinweise auf ausgewählte Materialien und Informationsquellen. Zielgruppe sind Multiplikatoren. Die Handreichung wurde aktuell überarbeitet und aktualisiert.

- Faltblattserie "Klicks-Momente":
  Die Mappe umfasst sieben Faltblätter, die jeweils einen bestimmten Aspekt bezüglich Sicherheit im Umgang mit modernen elektronischen Medien sowie von Gefahren im Internet aufgreifen. In jedem Faltblatt wird das betreffende Thema zunächst kurz und prägnant erläutert. Dann folgen Tipps, die auch weniger geübte Nutzer befolgen können. Um die strafrechtliche Relevanz einiger Inhalte zu verdeutlichen, sind auch Auszüge aus Gesetzestexten enthalten. Im Einzelnen werden in den Faltblättern folgende Themen behandelt: Soziale Netzwerke, Identitätsdiebstahl und Phishing, Persönlichkeits- und Urheberrechte im Internet, Betrug im Internet, Schadsoftware und Botnetze, Verbotene Inhalte im Internet, Smartphone und Tablet-PC.
- Filmspot "Chatten, aber sicher":
  Der Filmspot weist Kinder auf Sicherheitsregeln beim Chatten hin. Der Fußballprofi Bastian Schweinsteiger tritt dabei mit Regeln für ein sicheres Chatten auf. Siehe www.kinder-sicher-im-netz.de.
- Filmspot "Surfen, aber sicher":
  Der Videospot ist ein weiterer Baustein zu der Aktion "Kinder sicher im Netz". Der TV-Moderator Rudi Cerne gibt Eltern Tipps, wie sie ihre Kinder vor den Gefahren des Internets schützen können. Beide Spots gibt es sowohl als DVD für den Einsatz vor Ort als auch als Internet-Content.
- Internetseite "Online kaufen – mit Verstand!" (www.kaufenmitverstand.de):
  Die Internetseite bildet die virtuelle Plattform der Kampagne "Online Kaufen – mit Verstand!". Getragen wird diese Kampagne gemeinsam vom ProPK, eBay und dem Bundesverband des Deutschen Versandhandels (bvh). Ziel der Kampagne ist die Vermittlung einfacher Regeln und Informationen, mit denen sich Menschen vor betrügerischen Kaufgeschäften über das Internet schützen können. Dabei werden "7 Goldene Regeln" in den Vordergrund gestellt und näher erläutert. Auf der Internetseite besteht die Möglichkeit, die Info-Karte "Online kaufen – mit Verstand!" ("Safety Card" genannt) mit diesen sieben Regeln herunterzuladen. Des Weiteren werden ein Wissenstest, Aktionen bzw. Neuigkeiten sowie eine Presserubrik zum Thema angeboten.

- Sicherheitskompass für einen sicheren PC (http://www.polizei-beratung.de/themen-undtipps/gefahren-im-internet/sicherheitskompass.html):
  Auf der Internetseite sind die zehn wichtigsten Regeln für mehr Sicherheit im Internet zusammengefasst. Hierzu wird als Animation das Bild eines Kompasses benutzt. Anwender können je nach – von ihnen zu steuerndem – Ausschlag der Kompassnadel zwischen zehn verschiedenen Themen mit den entsprechenden Sicherheitstipps wählen. Im Einzelnen sind das: 1. Sichere Passwörter, 2. Mitbenutzer, 3. Software-Updates, 4. Firewall, 5. E-Mail und Anhänge, 6. Browser-Sicherheit, 7. Downloads, 8. Funk-Netzwerke, 9. personenbezogene Daten und 10. Hardware.
- Faltblatt "Alles, was Recht ist.":
  Das gemeinsam von ProPK, eBay und dem Bundesverband des Deutschen Versandhandels herausgegebene Faltblatt enthält Hinweise für Käufer, die Waren über das Internet bestellten, aber nicht bzw. nicht in vertragsgemäßer Form erhalten haben. Dazu werden Handlungsmöglichkeiten und Rechte für drei unterschiedliche Situationen beschrieben: a) der Artikel wurde bezahlt, aber nicht geliefert; b) der Artikel ist beim Versand verloren gegangen oder beschädigt worden; c) der gelieferte Artikel ist mangelhaft. Neben der Klärung einzelner rechtlicher Fragen sind auch die Internet-Adressen für weitergehende Informationen angegeben.
- Comic-artiges Heft "Hallo – jetzt reicht's":
  Das Heft stellt in kindgerechter Art lebensweltliche Erfahrungen von Kindern insbesondere zu Gewalt, Mobbing, Erpressung, Sachbeschädigung sowie Chatten im Internet dar und vermittelt dazu Verhaltensregeln. Zielgruppe sind Grundschulen.
- Faltblatt "... und redest selber von Respekt und Würde":
  Der Comic ist eine Initiative mit www.handysektor.de zur Stärkung von Medienkompetenz. Er beschreibt und stellt eindrücklich dar, welche schädlichen Folgen die Verbreitung von beleidigenden Inhalten über Menschen via Internet, Mobiltelefon oder Soziale Netzwerke haben kann. Zielgruppe sind Kinder und Jugendliche.

- Faltblatt "Das Netz vergisst nichts":
  Der Flyer ist auch Teil der Kooperation mit "handysektor". In einer Comicgeschichte wird hier geschildert, weshalb man von sich und anderen so wenig wie möglich persönliche Daten im Internet preisgeben sollte. Zielgruppe sind Kinder und Jugendliche.
- Opferorientiertes Faltblatt "Opfer, Schlampe, Hurensohn – gegen Mobbing":
  Im ebenfalls mit handysektor.de herausgegebenen Comic wird ein Geschehensablauf "Cybermobbing" dargestellt. Damit werden die Funktionen von Smartphones aufgezeigt und wie die mobile Einbindung in soziale Netzwerke als Mittel von "Cybermobbing" genutzt werden kann. Andererseits – und als Hauptbotschaft – wird vermittelt, Mobbing nicht hinzunehmen. Opfer von Cybermobbing können und sollten Hilfe Dritter in Anspruch nehmen. Zielgruppe sind Kinder und Jugendliche.
- Faltblatt "Apps to go":
  Das in Kooperation mit handysektor.de entwickelte Faltblatt enthält Tipps für den sicheren Umgang mit Apps auf Smartphones und Tablet-PCs. In altersgerechter Form wird dargestellt, welche Grundregeln bei der Nutzung zu beachten sind. Das Faltblatt informiert dabei über versteckte Kostenfallen, Werbung, Schutzsoftware, Zugriffsrechte oder Einstellungen im Betriebssystem.
- Medienpaket "Netzangriff":
  Das Medienpaket besteht aus einer DVD und einem beigelegten Filmbegleitheft. Es ist für den Einsatz im Schulunterricht entwickelt worden. Daneben stehen Arbeitsmaterialien (Workshop-Module) zum Download bereit. Der Film aus der Reihe Krimi.de behandelt explizit Cybermobbing. Im Film wird deutlich, dass Cybermobbing nicht nur moralisch verwerflich, sondern auch illegal ist, weil damit die Straftatbestände der Beleidigung, üblen Nachrede oder Verleumdung erfüllt sein können, mit entsprechenden strafrechtlichen Folgen. Das Medienpaket ist vergriffen. Der Film ist auf der Videoplattform YouTube eingestellt und das Begleitheft steht zum Download bereit (Quelle: http://www.youtube.com/watch?v=aHMgcmYuz2M). Zielgruppe sind Kinder und Jugendliche.

- Medienpaket "Verklickt!":

  Im März 2014 wurde das Medienpaket "Verklickt!" veröffentlicht. Es handelt sich um einen ca. 50-minütigen Spielfilm für Kinder und Jugendliche ab 12 Jahren, der ihnen sicherheitsbewusstes Verhalten in ihrer digitalen Alltagswelt vermitteln soll. Das im Medienpaket enthaltene pädagogische Begleitheft bietet Lehrern und anderen pädagogischen Fachkräften die Möglichkeit, im Rahmen von Diskussionen oder Projektarbeit die unterschiedlichen Problematiken bei der Nutzung digitaler Medien, die in dem in drei Teilen vorführbaren Film dargestellt werden, vertiefend zu behandeln. Die Inhalte des Begleithefts richten sich an der Filmhandlung aus. Thematische Schwerpunkte sind: Cybermobbing, illegale Downloads, Kostenfallen, Persönlichkeits- und Urheberrechte. Weitere Themen sind beispielweise Verhalten in Sozialen Netzwerken, jugendgefährdende Inhalte oder Passwortsicherheit.

- Info-Blatt "Gewaltvideos auf Schülerhandys":

  Das Informationsblatt beschäftigt sich mit illegalen Inhalten auf Schülerhandys. Dazu gehören insbesondere Straftaten bei Bild- und Videoaufnahmen mittels integrierter Digitalkamera, Straftaten durch den Besitz von illegalem Bildmaterial wie pornografischen Bildern/ Filmen oder Gewaltdarstellungen sowie Straftaten durch die Weitergabe von gespeicherten illegalen Inhalten. Darüber hinaus enthält das Informationsblatt Empfehlungen für Eltern, was sie beim Umgang ihrer Kinder mit Mobiltelefonen beachten bzw. wie sie sich ihren Kindern gegenüber verhalten sollten. Daneben gibt es Empfehlungen auch für Schulen bzw. Lehrer sowie Hinweise auf Internetadressen, unter denen weiterführende Informationen zu erhalten sind.

- Info-Blatt "Schleuser missbrauchen Online-Mitfahrzentralen":

  Das Informationsblatt "Schleuser missbrauchen Online-Mitfahrzentralen" beschreibt, wie Schleuser Online-Mitfahrzentralen nutzen, um Menschen unter Umgehung der gesetzlichen Einreisebestimmungen in Länder der Europäischen Union zu befördern. Nimmt ein argloser Fahrer Geschleuste mit, gerät er bei einer Kontrolle schnell unter Verdacht, als Mitglied einer Schleuserbande zu agieren. Festnahme, Vernehmungen und ein langwieriges Strafverfahren können die Folge sein.

- Info-Blatt Hardwaresicherheit:
  Das Informationsblatt gibt Hinweise, wie hochwertige Hardware (Notebooks, Computerteile und Zubehör), die in Behörden, Einrichtungen und Betrieben genutzt wird, vor Diebstahl und unbefugter Nutzung geschützt werden kann. Neben Empfehlungen zur Vorbeugung sind auch Empfehlungen enthalten, was im Fall des Diebstahls getan werden sollte.
- Internetportal "time4teen" (www.time4teen.de):
  Das Informationsangebot richtet sich gezielt an junge Menschen. Es enthält Hinweise zu Kriminalitätsgefahren verschiedenster Art, darunter Kindesmisshandlung, Mobbing und sexuelle Gewalt. In der Rubrik "Spielregeln des Lebens" finden sich Erläuterungen zu legalem wie auch strafbarem Verhalten mit Blick etwa auf Waffen, Extremismus, Computer/Internet oder Umgang mit Mobiltelefonen (Handys). Daneben werden angeboten: rechtliche Aufklärung zu den Folgen einer Straftat, Informationen über die Polizei, jugendbezogene Hilfeangebote sowie Spiele und Quizfragen. Jüngere Kinder können sich in "kids world" spielerisch über Sicherheit informieren. Dazu gehört ein interaktives Lernspiel, das von den Gefahren für Kinder im Alltag handelt und ihr Wissen dazu testet. Im Weiteren gibt es eine Rubrik zu Neuigkeiten und Veranstaltungen sowie eine Rubrik, die Serviceangebote und weiterführende Informationen enthält.
- www.polizei-beratung.de

Darüber hinaus bietet ProPK umfangreiche Informationen und Tipps auf seiner zentralen Internetseite unter http://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet.html. Seit vielen Jahren ist das Internetangebot des ProPK ein wichtiges Element der kriminalpräventiven Öffentlichkeitsarbeit. Es klärt die Bürgerinnen und Bürger über die Erscheinungsformen der Kriminalität auf und gibt gleichzeitig Tipps zum Schutz vor Kriminalität. Das Angebot wird kontinuierlich weiterentwickelt. Neue Kriminalitätsformen, wie zum Beispiel "Romance Scamming", eine Variante des Vorauszahlungsbetrugs der sog. Nigeria Connection unter Zuhilfenahme von Dating-Seiten im Internet und von sozialen Netzwerken, oder die Thematik "Finanzagenten" wurden neu aufgenommen.

Das Informationsangebot wurde 2010 grundlegend überarbeitet und zu Beginn des Jahres 2011 freigeschaltet. Nun bieten ein klar strukturierter Aufbau und eine benutzerfreundliche Menüführung einen schnellen Überblick über die vielfältigen Themen. Hierbei werden auch umfangreiche Informationen zum sicheren Umgang mit "neuen Medien" und zur Internetkriminalität bereitgestellt. Die bereitgestellten Informationen zur Aufklärung und Sensibilisierung der Bevölkerung beziehen sich auf inhaltliche Risiken (Extremismus, Pornografie/Kinderpornografie, Gewalt, Betrug usw.), kommunikationsbezogene Risiken (Cyber-Grooming, Cyber-Mobbing, Identitätsdiebstahl usw.) und technische Risiken (Hardware-Sicherheit, Viren, Würmer, Trojaner usw.).

Die Privatwirtschaft ist – wie zu den einzelnen Initiativen beschrieben – eingebunden. Nationale oder internationale Fördergelder wurden nicht in Anspruch genommen. Über die im ProPK bundesweit abgestimmten Präventionsaktivitäten hinaus gestalten die Bundesländer zumindest zum Teil eigene Präventionsangebote.

Zur Prävention verschiedener Formen von Cyberkriminalität und Risiken in Zusammenhang mit dem Internet und digitalen Medien existieren in Deutschland flächendeckend zahlreiche Projekte und Initiativen verschiedener Träger auf örtlicher, regionaler, landes- und bundesweiter Ebene. Weitere Akteure auf Bundesebene sind das Bundesamt für Sicherheit in der Informationstechnik (www.bsi.bund.de), das Bundesministerium des Innern mit der Initiative "Deutschland sicher im Netz" (www.sicher-im-netz.de/), das Bundesministerium für Familie, Senioren, Frauen und Jugend u. a. mit jugendschutz.net (www.jugendschutz.net), dem Zentrum für Kinderschutz im Internet (www.i-kiz.de/) oder auch der Initiative "Initiative SCHAU HIN! – Was Dein Kind mit Medien macht" (www.bmfsfj.de/BMFSFJ/kinder-und-jugend,did=6212.html), die Kommission für Jugendmedienschutz (KJM) der Landesmedienanstalten (www.kjmonline.de/), Klicksafe (angesiedelt bei der Landeszentrale für Medien und Kommunikation (LMK) Rheinland Pfalz; http://www.klicksafe.de/), die Stiftung Digitale Chancen (www.digitale-chancen.de/) sowie das bereits erwähnte Programm Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK; www.polizei-beratung.de).

Sensibilisierungsmaßnahmen gegen Cyberkriminalität finden in hohem Maße auch an Schulen statt, da dies der Lernort ist, an dem Kinder und Jugendliche am besten systematisch erreicht werden können. Zum Teil handelt es sich um die Materialien, die vom ProPK erstellt wurden. Generell eignen sich ein Großteil der vom ProPK (s. 10.C.1.) erstellten Materialien auch zum Einsatz in der Schule bzw. sind für diesen Einsatz konzipiert, wie zum Beispiel das Medienpaket "Verklickt!".

Im Hinblick auf die Bundesländer wurden folgende Informationen gemeldet:

Niedersachsen:

In Kooperation mit der niedersächsischen Landesschulbehörde und externen Partnern werden zwei durch die Landespolizei initiierte und unterstützend begleitete spezifische Programme zur Erhöhung der Medienkompetenz in Schulen eingesetzt. Mit den Präventionsangeboten ".comPass – Ich kenn‘ mich aus im Netz" und "Cyber-Licence – Der Medienführerschein" erhalten die Schulen die Möglichkeit, die Weiterentwicklung der Medienkompetenz ihrer Schülerinnen und Schüler zu unterstützen. Lehrerinnen und Lehrer nehmen dabei die Rolle aus Mittler/Multiplikator ein. Im Programm ".comPass" sind als weitere Zielgruppe die Erwachsenen im Bereich der Erwachsenenbildung involviert. Daneben haben sich einige regionale polizeiliche Präventionspuppenbühnen der Thematik Mediensicherheit angenommen und führen ihre Puppenspiele in den 3. und 4. Grundschulklassen ihres Zuständigkeitsbereiches auf.

Schleswig-Holstein:

In Zusammenarbeit mit dem Institut für Qualitätssicherung an Schulen Schleswig-Holstein (IQSH), dem Unabhängigen Landeszentrum für Datenschutz (ULD) und der Verbraucherzentrale (VZ) führt die Landespolizei bei Bedarf einen Medientag an Schulen mit dem Titel "Medien machen Schule" durch. Die Durchführung des kriminalpräventiven Unterrichts obliegt speziell ausgebildeten Präventionsbeamtinnen und -beamten. In Ergänzung zum Schulunterricht leistet die Polizei auf Anfrage der Schulen in allen 7. Klassen einen Beitrag zur Erhöhung des Normenbewusstseins und vermittelt Handlungssicherheit als Zeuge oder Opfer einer Straftat.

8.3. Prävention

8.3.1. Nationale Rechtsvorschriften/politische Maßnahmen und andere Maßnahmen

Das Kriminalistische Institut (Abteilung KI) des Bundeskriminalamtes befasst sich auftragsgemäß insbesondere mit kriminalistisch-kriminologischen Fragestellungen zu Cyberkriminalitätsdelikten, ist jedoch zuständigkeitshalber nicht federführend in strategische Fragestellungen der Verhütung von Cyberkriminalität in Deutschland eingebunden.

Dies fällt in die Zuständigkeit der Bundesländer. Explizite Regelungen für Prävention im Bereich Cyberkriminalität ergeben sich daraus nicht, soweit die Informationen aus den Bundesländern vorliegen. Es gibt eine bundesweite Cyber-Sicherheitsstrategie sowie bundesweite Organisationen zur Verhütung von Cyberkriminalität.

Für die Erarbeitung von Standards zum Schutz der Bundesbehörden ist das Bundesamt für die Sicherheit in der Informationstechnik (BSI) zuständig.

Im Hinblick auf die Bundesländer wurden – ohne Anspruch auf Vollständigkeit – folgende Informationen gemeldet:

Baden-Württemberg:
Die Mitarbeiter der polizeilichen Kriminalprävention besuchen gezielt Veranstaltungen, um eine möglichst breite Bevölkerungsschicht zu erreichen und durch Vorträge, Beratung und Informationsmaterialen für das Thema Cyberkriminalität zu sensibilisieren und dadurch Straftaten zu verhüten.

Brandenburg:
Bei der unter 5.A.5. dargestellten polizeilichen Präventionsarbeit im Zusammenhang mit Cyberkriminalität/Neue Medien waren im Jahr 2013 insbesondere Kinder und Jugendliche des Primarbereiches und der Sekundarstufe 1 Zielgruppen. Diese sollen zu einer sachgerechten und umsichtigen Mediennutzung befähigt werden, indem sie über potenzielle Gefahren im Umgang mit dem Internet und Neuen Medien sowie den ordnungs- und strafrechtlichen Rahmenbedingungen (z. B. Urheberrecht) informiert werden, jedoch auch entsprechende Verhaltensweisen zur Vermeidung von Opferwerdung kennen lernen.

Zu den Themen Internet und Neue Medien finden aber auch Veranstaltungen mit Erwachsenen wie Eltern oder Lehrer statt, um diese mit den Themen vertraut zu machen, sie zu einem sicherheits- und verantwortungsbewussten Umgang mit dem Internet und den Neuen Medien zu befähigen und als Multiplikatoren zu gewinnen. Zudem werden Eltern und Lehrer sensibilisiert, sich mit der Mediennutzung der Kinder und Jugendlichen auseinanderzusetzen, Handlungsempfehlungen zur Erhöhung der Medienkompetenz der Kinder und Jugendlichen zu kennen und entsprechende Hilfestellungen zu geben. Im Rahmen dieser Präventionsveranstaltungen kommen u. a. Broschüren und Medien des Programms Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK), wie z. B. die Inhalte von "Missbrauch verhindern" unterstützend zur Anwendung. Zudem wird für weitergehende Informationen auf Internetseiten wie beispielsweise "www.fragfinn.de" oder "www.bsi-fuer-buerger.de" verwiesen.

Die Fachhochschule der Polizei und des Landes Brandenburg (FHPol) beschäftigt sich im Rahmen ihrer Möglichkeit intensiv mit Aspekten der Vermittlung von Medienkompetenz, der Aufklärung über Kriminalität und deren Risiken sowie der Bedeutung polizeilicher Arbeit und Präsenz in Sozialen Medien. Neben einer Vielzahl an Fachvorträgen auf Tagungen, für andere Polizeibehörden aber auch direkt an Schulen und Jugendeinrichtungen steht insbesondere die wissenschaftliche Erforschung der kriminologischen Bedeutung von Interaktions- und Kommunikationsrisiken im digitalen Raum im Mittelpunkt der Aktivitäten. Gegenwärtig ist die FHPol zudem an zwei Forschungsprojekten mit entsprechender Ausrichtung beteiligt. In dem internationalen Forschungsprojekt "Hate Communities: A Cross-National Comparison" werden die Strukturen, Beweggründe und die Phänomenologie von Hate Crime im Netz empirisch erhoben. Die Nutzung Sozialer Medien durch die Polizei steht im Mittelpunkt des EU-Forschungsprojektes "Solving Crime through Social Media" (SOMEP).

Saarland:

Zur Aufgabe des Landespolizeipräsidiums, insbesondere des Dezernats LPP 246 – Polizeiliche Kriminalprävention und Opferschutz, gehört überwiegend die Steigerung der Medienkompetenz. Daneben auch die technische Beratung in Bezug auf die Aufbewahrung und den Verschluss von Hardware wie Notebooks, Computer, Computerteile oder Zubehör.

Die Steigerung der Medienkompetenz basiert auf drei Säulen:

- Konzepte und Medien des Programms Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK),
- AG Medienkompetenz,
- Beratung durch das Dezernat LPP 246.

(Das Dezernat LPP 246 berät Bürger, Schulen und sonstige Institutionen auf Anfrage einzelfallbezogen zum Thema, verteilt die Medien des ProPK und steht Presse, Rundfunk und Fernsehen für Interviews zur Verfügung. Anlassbezogen werden eigene Vorträge zum Themenkomplex "Gefahren des Internets/Medienkompetenz" insbesondere nach Vorkommnissen an Schulen durchgeführt.)

Thüringen:

Seit 2009 erfolgte eine Teilnahme der Thüringer Polizei an den landesweiten Multiplikatorenschulungen "Jugendmedienschutz im Internet" für Lehrer und Fachkräfte der Jugendhilfe. Die zielgruppenspezifische Präventionsmaßnahme zur Gewaltbekämpfung im Internet gliedert sich in einen Grund- und Aufbaulehrgang, an denen jeweils Polizeibedienstete aus den verschiedenen Thüringer Regionen teilgenommen haben, die als Multiplikatoren wirken.

8.3.2. Öffentlich-private Partnerschaften (ÖPP)

Vertreter von Banken (der ING-DiBa, der Commerzbank und der Hypovereinsbank) haben 2013 den Verein "German Competence Centre against Cybercrime" (G4C) gegründet. Das Bundeskriminalamt (BKA) hat mit diesem Verein eine Vereinbarung über die Kooperation im Phänomenbereich Cyberkriminalität unterzeichnet. Im Mittelpunkt der Zusammenarbeit steht die Optimierung des Schutzes vor Cyberkriminalität. Der Verein ist ein neuartiges operatives Zentrum, in dem die Mitglieder aus der Wirtschaft in Kooperation mit dem BKA Maßnahmen zum Schutz vor Cyberkriminalität entwickeln und Lösungen zu aktuellen und zukunftsorientierten Themen im Phänomenbereich Cyberkriminalität erarbeiten.

Baden-Württemberg:
Zwischenzeitlich ist die Zusammenarbeit in Form von Kooperationen zwischen Wirtschaft, Wissenschaft und öffentlichen Stellen erheblich intensiviert worden. Beispielhaft können hierfür folgende Kooperationen genannt werden, in die das Landeskriminalamt Baden-Württemberg (LKA BW) eingebunden ist:

- Sicherheitskooperation Cybercrime (Landeskriminalamt Baden- Württemberg (LKA BW), LKA Nordrhein-Westfalen (NRW), LKA Sachsen (SN), LKA Niedersachsen (NI), BITKOM-Verband),
- Allianz für Cybersicherheit in Baden-Württemberg (Innenministerium BW, Landeskriminalamt BW, Landesamt für Verfassungsschutz (LfV BW), Informatikzentrum Landesverwaltung BW(IZLBW), Ministerium für Wissenschaft, Forschung und Kunst (MWK), Ministerium für Finanzen und Wirtschaft (MFW),
- Allianz für Cybersicherheit Deutschland (BSI, BITKOM-Verband, LKA BW), Länderübergreifende Kooperation Cybercrime BW/BY/A/CH,
- Deutsches Kompetenzforum für Cybersicherheit (Microsoft, HAS, BITKOM-Verband, BLKA, Bundespolizei, LKA BW) u. a.

Niedersachsen:

Das Landeskriminalamt Niedersachsen ist nach den Landeskriminalämtern Nordrhein-Westfalen und Baden-Württemberg am 11. März 2014 der Sicherheitskooperation Cybercrime zwischen dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) beigetreten. Zu den Kooperationsfeldern der Zusammenarbeit zählen gemeinsame Aktivitäten zum Informationsaustausch und Wissenstransfer, gegenseitige Hospitationen, Dunkelfeldforschung, Konzeption und Durchführung von Präventionsmaßnahmen und Vermitteln von Experten in konkreten Einzelfällen.

In einer gemeinsamen Veranstaltung werden einmal jährlich die Kooperationsaktivitäten vorgestellt, anlassbezogen können Workshops durchgeführt werden. Vor dem Hintergrund weiterer Kooperationspartner befasst sich die Sicherheitskooperation zurzeit mit der Erarbeitung einer Geschäftsordnung. Zur Bekämpfung der Kinderpornografie im Internet wurde am 27. September 2009 durch den Niedersächsischen Innenminister für Inneres und Sport das Bündnis "White IT" ins Leben gerufen. Mittlerweile haben sich über 60 Partner aus Wirtschaft, Wissenschaft, Branchen- und Opferschutzverbänden sowie Vertretern der Heilberufe im Bündnis zusammengeschlossen, um gemeinschaftlich Aktivitäten zur Bekämpfung des sexuellen Missbrauchs von Kindern unter besonderer Berücksichtigung präventiver Aspekte voranzutreiben und hierzu Strategien und Lösungsansätze zu erarbeiten. In diesem Kontext unterstützt "White IT" das von der EU-Kommission initiierte Bündnis "Global Alliance against Child Sexual Abuse Online". Ansonsten finden im Bereich der Kinderpornografie z. B. in Niedersachsen regelmäßig Symposien statt, an denen sowohl öffentliche Strafverfolgungsbehörden als auch private Unternehmen teilnehmen.

8.4. Fazit

- **Das BKA hat verschiedene Grund- und Aufbaukurse zur Cyberkriminalität – auch auf dem Gebiet der IKT-Forensik – und bundesweit angebotene Kurse zur Schulung der Multiplikatoren (Schulung der Ausbilder in den Bundesländern) entwickelt.**

- **Die Deutsche Richterakademie bietet jährlich sieben Konferenzen und Fortbildungskurse für Richter und Staatsanwälte an.**

- **Auf Länderebene gibt es verschiedene Schulungsinitiativen. So veranstalten Nordrhein-Westfalen und Niedersachsen ein gemeinsames Trainingsprogramm für Spezialisten sowohl für die Polizeikräfte als auch für Staatsanwälte und Richter. Obwohl der Anteil der an diesen Schulungen teilnehmenden Richter nicht besonders hoch ist (nur 10 %), hält der Gutachterausschuss dies für eine sehr gute Praxis.**

- **Auch die Sensibilisierungsanstrengungen sind gut organisiert. Eine Vielfalt von Leitfäden, Faltblättern, Filmen, Websites und Informationsbögen wurden bereitgestellt, um sachdienliche Informationen in der Öffentlichkeit zu verbreiten.**

- **Die Polizei hat eine Broschüre zusammengestellt, die Empfehlungen für die Wirtschaft in Bezug darauf enthält, wie die Unternehmen sich gegen Cyberkriminalität schützen können, welche Art von Informationen sie im Hinblick auf etwaige Cyberangriffe registrieren sollten usw. Die Broschüre wurde – wie etwa auf der BKA-Jahreskonferenz – in Papierform verteilt und kann auch aus dem Internet heruntergeladen werden.**

- **Allen Polizeibeamten in Deutschland werden Grundkurse (Internet-Grundwissen) angeboten; ferner werden für die mit Cyberkriminalität befassten Polizeibeamten Schulungen zur Cyberkriminalität auf mittlerem Niveau und für Fortgeschrittene/Spezialisten abgehalten. Auch für Gerichtssachverständige werden Schulungen angeboten.**

- **Ferner sind deutsche Polizeibeamte an verschiedenen Weiterbildungskursen zusammen mit Europol, Interpol, ECTEG, CEPOL, OLAF und Academia (Netz von neun deutschen Universitäten) beteiligt.**

- **Fachschulungen zur Cyberkriminalität werden den Staatsanwälten auf Länderebene angeboten. Die Staatsanwälte sind es gewohnt, an nationalen und internationalen Weiterbildungskursen teilzunehmen.**

- **Die Richter sind nicht verpflichtet, an Schulungen zur Cyberkriminalität teilzunehmen. Es werden ihnen jedoch Weiterbildungskurse angeboten. Es ist Sache der Richter, über ihre Teilnahme an Weiterbildungskursen zu entscheiden.**

9. SCHLUSSBEMERKUNGEN UND EMPFEHLUNGEN

9.1. Vorschläge Deutschlands

Deutschland möchte folgende Verbesserungen zur Unterstützung der Bekämpfung des Phänomens der Cyberkriminalität vorschlagen:

• flächendeckende Aus- und Fortbildung bei den Strafverfolgungsbehörden und der Justiz;
• Einstellung von IT-Fachpersonal in der Polizei;
• Einführung technischer Systeme zur Bewältigung von Massendaten (Big Data).

9.2. Empfehlungen

Was die praktische Durchführung und die Anwendung des Rahmenbeschlusses und der Richtlinien anbelangt, so war der Gutachterausschuss, der die Begutachtung Deutschlands durchgeführt hat, imstande, das System in Deutschland auf zufriedenstellende Weise zu überprüfen.

Deutschland sollte 18 Monate nach der Begutachtung eine Bestandsaufnahme in Bezug auf die in diesem Gutachten enthaltenen Empfehlungen vornehmen und der Gruppe "Allgemeine Angelegenheiten einschließlich Bewertungen" (GENVAL) Bericht über die Fortschritte erstatten.

Der Gutachterausschuss hielt es für angebracht, eine Reihe von Anregungen für die deutschen Behörden zu formulieren. Darüber hinaus werden auf der Grundlage bewährter Vorgehensweisen Empfehlungen für die EU, ihre Organe, Einrichtungen, Ämter und Agenturen und insbesondere für Europol ausgesprochen.

9.2.1. Empfehlungen an Deutschland

1. Es sollte in Betracht gezogen werden, zusätzliche und leicht zu nutzende Kanäle zu schaffen, um Informationen zwischen Polizei und Staatsanwälten in den 16 Bundesländern gesichert (unter Verwendung einer Verschlüsselung) zu übermitteln;

2. es sollte in Betracht gezogen werden, den Austausch bewährter Verfahren auf dem Gebiet der Schulung der Praktiker zwischen den 16 Bundesländern weiter zu verbessern;

3. es sollte in Betracht gezogen werden sicherzustellen, dass Polizei und Strafverfolgungsbehörden an von Bundeseinrichtungen – wie etwa dem BSI – veranstalteten Übungen zur Internetsicherheit teilnehmen, um alle Möglichkeiten zur Verbesserung ihrer Arbeitsverfahren zu ermitteln;

4. die Nutzung gemeinsamer Ermittlungsgruppen (GEG) sollte weiter gefördert werden, indem beispielsweise die Praktiker, insbesondere die Staatsanwälte, mehr Informationen darüber erhalten, welche Möglichkeiten und Vorteile die GEG bieten;

5. es sollte in Betracht gezogen werden, den Abgleich der Hash-Werte von Material im Zusammenhang mit sexuellem Missbrauch von Kindern mit Material, das in öffentlich zugänglichen Quellen verfügbar ist, zuzulassen;

6. es sollte in Betracht gezogen werden, spezielle Anweisungen (Leitlinien) für die Unterstützung bei Online-Anzeigen von Cyberkriminalität, insbesondere für kleine und mittlere Unternehmen, einzuführen;

7. die Bemühungen darum, dass elektronische Beweismittel in digitaler Form vor Gericht vorgelegt werden dürfen, sollten fortgesetzt werden;

8. es sollte die Möglichkeit in Betracht gezogen werden, das Format der polizeilichen und der staatsanwaltschaftlichen Statistiken anzugleichen, um ihre Vergleichbarkeit zu ermöglichen[9].

[9] Deutschland erinnert daran, dass die Mitgliedstaaten speziell nach Artikel 14 Absatz 2 der Richtlinie 2013/40/EU nicht verpflichtet sind, ihre Erhebung und Auswertung von Statistiken auszuweiten.

9.2.2. Empfehlungen an die Europäische Union, ihre Organe und Einrichtungen sowie an die anderen Mitgliedstaaten

9. Die Mitgliedstaaten sollten sicherstellen, dass die Informationen zwischen den Praktikern – wie etwa Staatsanwaltschaften und anderen Strafverfolgungsbehörden sowie den einschlägigen europäischen Einrichtungen und Ämtern – gesichert (unter Verwendung einer Verschlüsselung) übermittelt werden können;

10. Nach dem Urteil des EuGH vom 21. Dezember 2016 (verbundene Rechtssachen C-203/15 Tele2 Sverige AB gegen Post- och telestyrelsen und C-698/15 Secretary of State for Home Department gegen Tom Watson u. a.) sollten die europäischen Organe die Auswirkungen des Urteils prüfen und darüber nachdenken, wie die Probleme bei der Zusammenarbeit zwischen Mitgliedstaaten in Bezug auf die Speicherung on Verkehrsdaten der elektronischen Kommunikation am besten gelöst werden können.

11. es sollte erwogen werden, künftig den Begriff "Kinderpornografie" durch "Darstellungen von Kindesmissbrauch" oder einen anderen geeigneten Begriff zu ersetzen;

12. die Europäische Kommission sollte die Möglichkeit, für die rechtlichen Probleme beim grenzüberschreitenden Datenzugriff Lösungen zu finden, weiter ausloten.

Der Gutachterausschuss hielt es für geboten, einige der bewährten Verfahren zu unterstreichen, die in Deutschland im Zuge der Begutachtung festgestellt wurden und als Grundlage für andere Mitgliedstaaten dienen könnten:

- in vielen Bundesländern Verfügbarkeit von Staatsanwälten und Einheiten, die auf die Bekämpfung von Cyberkriminalität spezialisiert sind;
- Möglichkeit, vorübergehende Task Forces zwischen Polizei und Staatsanwaltschaft zur Bekämpfung der Cyberkriminalität einzusetzen, was es ermöglicht, dass die gleichen Personen die Fälle bearbeiten;
- Expertentreffen zur internationalen Zusammenarbeit sowohl auf Bundes- als auch auf Länderebene;

- Einbindung verschiedener Ministerien in die Bekämpfung der Cyberkriminalität und die Koordinierung ihrer Bemühungen bei einem interministeriellen "Jour fixe" zur Cyberkriminalität; dabei treffen sich alle einschlägigen Akteure auf dem Gebiet der Verhütung und Bekämpfung der Cyberkriminalität, um sich über diesbezügliche Fragen von gemeinsamem Interesse auszutauschen und sie zu erörtern;
- Bestehen eines zentralen Ermittlungsregisters, mit dessen Hilfe schon frühzeitig Überschneidungen bei Ermittlungen festgestellt werden sollen;
- Bestehen von Hotlines zur Anzeige von Kinderpornografie;
- von Nordrhein-Westfalen organisierte gemeinsame Schulungstagungen zur Cyberkriminalität für Staatsanwälte und Richter, die zu einem gemeinsamen Sachverständnis führen und weitere Vorteile mit sich bringen können;
- Umstand, dass das mit der Bekämpfung der Kinderpornografie betraute Personal sehr gut – etwa durch das Angebot psychologischer Hilfe – betreut wird;
- die weitreichende Aufmerksamkeit und die breite Unterstützung, die die Behörden dem Schutz der KMU im Rahmen der Bekämpfung der Cyberkriminalität widmen;
- die Einrichtung des iPPP-Projekts;
- bewährte Verfahren bei der Abschaltung von Kinderpornografie-Websites und – falls die Abschaltung nicht möglich ist – Aufnahme der URL in eine schwarze Liste, die den betroffenen Personen und Organisationen – etwa Bibliotheken – übermittelt wird;
- Möglichkeit für die Privatwirtschaft, Cyberkriminalität online anzuzeigen (und die Verfügbarkeit von Leitfäden und Anlaufstellen in diesem Zusammenhang);
- aktive Teilnahme Deutschlands auf internationaler Ebene wie etwa durch J-CAT (Joint Cybercrime Action Taskforce), deren Vorsitz Deutschland seit Januar 2016 innehat, EMPACT (Europäische multidisziplinäre Plattform gegen kriminelle Bedrohungen) und die Entsendung von Verbindungsbeamten in viele Länder;
- erhöhte Zuweisung von Ressourcen zur Bekämpfung der Cyberkriminalität.
- umfassende Einbeziehung von Eurojust durch die deutschen Justizbehörden bei komplizierten grenzüberschreitenden Fällen.

9.2.3. Empfehlungen an Eurojust/Europol/ENISA

1. Die Europäische Gruppe für Schulung und Ausbildung in Bezug auf Computerkriminalität (ECTEG) sollte weiterhin Schulungen für die Strafverfolgungsbehörden in den Mitgliedstaaten in Bezug auf Cyberkriminalität anbieten und fördern.

2. Sowohl Europol als auch Eurojust sollten Überlegungen darüber anstellen, wie GEG leichter eingesetzt werden können, auch dadurch, dass der Zugang zu verfügbaren Finanzmitteln erleichtert wird, damit ihre Wirksamkeit für die Mitgliedstaaten sichergestellt ist.

ANHANG A: PROGRAMME FOR THE ON-SITE VISIT

Monday, 23 May 2016 **Arrival**	
During the day	Arrival of GENVAL Experts at Airport Berlin Tegel/ Berlin Schönefeld Hotel Titanic Comfort/ Arcotel John F.
Tuesday, 24 May 2016 **Federal Ministry of Justice and Consumer Protection (BMJV), Berlin** Room: Gustav-Radbruch-Saal (5.001)	
8:45 a.m. 9:15 a.m.	**<u>Federal Ministry of Justice and Consumer Protection</u>** • **Introductory remarks** • **Welcoming** of the Evaluation Team *by:* **Hans Georg Baumann**, Director General of the Criminal Law Directorate General in the Federal Ministry of Justice and Consumer Protection **Photo opportunity** with the Evaluation Team

9:30 a.m.	**Legal Aspects** 1. Criminalisation – 2.A. 2. Statistics (Justice) – 1 Participants: Federal Ministry of Justice and Consumer Protection, Federal Ministry of the Interior, Federal Criminal Police Office
10:45 a.m.	**Coffee break**
11:00 a.m.	**Legal Aspects (continued)** 1. Procedural issues – 2.B. 2. Jurisdiction – 2.C Participants: Federal Ministry of Justice and Consumer Protection, Federal Ministry of the Interior, Federal Criminal Police Office
12:45 a.m.	**Lunch** on invitation of the Federal Ministry of Justice and Consumer Protection
2:00 p.m.	**International cooperation** **- Tools:** • Mutual legal assistance – 7.A. • Mutual recognition – 7.B. Surrender/Extradition – 7.C. Participants: Federal Ministry of Justice and Consumer Protection, Federal Ministry of the Interior, Public Prosecutor's Office, Federal Office of Justice, Eurojust, Federal Criminal Police Office, Federal Office for Information Security (BSI)

	<u>International cooperation</u> **- partners** • Cooperation with EU Agencies – 8.A. • Participation in JITs/cyber-patrols – 8.B. Cooperation with third countries – 8.C. Participants: Federal Ministry of Justice and Consumer Protection, Federal Ministry of the Interior, Public Prosecutor's Office, Eurojust, Federal Criminal Police Office, Federal Office for Information Security
4:00 p.m.	**<u>Coffee Break</u>**
4:30 p.m.	**<u>Cooperation with the private sector</u>** – 9. Participants: Federal Ministry of Justice and Consumer Protection, Federal Ministry of the Interior, Federal Ministry of Economic Affairs and Energy, Federal Criminal Police Office, Federal Office for Information Security, German Competence Center against Cyber Crime (G4C), Bitkom (digital industry association)
6:30 p.m.	**<u>Guided tour through the Federal Ministry of Justice and Consumer Protection</u>**
7:00 p.m.	**<u>Working Dinner on invitation of the Federal Ministry of Justice and Consumer Protection</u>** Restaurant Mark Brandenburg, Mohrenstr. 30

Wednesday, 25 May 2016 **Federal Ministry of Interior (BMI), Berlin** Federal Office for Information Security (BSI) Federal Criminal Police Office (BKA) Room: C.0.435 at the Conference Center (+ Lobby)	
9:00 a.m.	**Welcoming** of the Evaluation Team by Dr. Stefan Grosse, Head of Division, General issues concerning cybercrime, cyber espionage and cyber terrorism
9:15 a.m.	**National structures** • General Matters, Cyber Security Strategies, Statistics (police) – 1 • Judiciary (prosecution and court) – 3.A • Law enforcement authorities – 3.B. • Other authorities – 3.C. Participants: Federal Ministry of Justice and Consumer Protection, Federal Ministry of the Interior, Federal Criminal Police Office
10:30 a.m.	**Coffee break**
10:45 a.m.	**Offences related to child sexual abuse online and child pornography** • Specific questions related to the act/victim – 5.A. • Filtering/Blocking of access to/Removal of content/Take down of web pages containing or disseminating child pornography – 5.B. • International cooperation – 5.C. Participants: Federal Ministry of Justice and Consumer Protection, Federal Ministry of the Interior, Federal Ministry for Family Affairs, Senior Citizens, Women and Youth, Federal Criminal Police Office

12:45 a.m.	**Lunch** on invitation of the Federal Ministry of the Interior Room: Conference Center, Lobby
2:00 p.m.	**Cyber attacks – 4.** • presentation of the BSI-situation report • regulations under the new IT Security Act, reporting obligations • CERT structures in Germany Participants: Federal Ministry of Justice and Consumer Protection, Federal Ministry of the Interior, Federal Criminal Police Office, Federal Office for Information Security (BSI)
3:00 p.m.	**Online Card Fraud** – 6. Participants: Federal Ministry of Justice and Consumer Protection, Federal Ministry of the Interior, Federal Criminal Police Office
4:00 p.m.	**Coffee Break**
4:15 p.m.	**Prevention of cybercrime, training and awareness raising activities** • Prevention – 10.A. • Training – 10.B. • Awareness Raising – 10.C Participants: Federal Ministry of Justice and Consumer Protection, Federal Ministry of the Interior, Federal Criminal Police Office, Federal Office for Information Security

5:30 p.m.	**Visit of the Tränenpalast ("Palace of the Tears" - former border crossing between "East und West" at Berlin Friedrichstraße train station)** • Guided Tour
7:00 p.m.	**Dinner on invitation of the Federal Ministry of Interior** Restaurant Zollpackhof
Thursday, 26 May 2016, Berlin **General Public Prosecution Office, Celle** Central Office Organised Crime and Corruption (ZOK)	
08:00 a.m.	**Transfer to Celle** Meeting point: in front of the hotel Titanic Comfort
11:30 a.m.	**Visit of the Central Office Organised Crime and Corruption** (Zentrale Stelle Organisierte Kriminalität und Korruption – ZOK) Participants: Federal Ministry of Justice and Consumer Protection, Federal Ministry of the Interior, Public Prosecutor's Central Offices for the Prosecution of Cybercrime of Celle, Verden, Berlin, Cologne and Bamberg, Police Officer of Lüneburg
4:00 p.m.	**Transfer to Berlin**
6:00 p.m.	Evening at free disposal

Friday, 27 May 2016 **Federal Ministry of Justice and Consumer Protection (BMJV), Berlin** **Gustav-Radbruch-Saal (5.001)**	
9:00 a.m.	**Wrap-up-session** • General observations • final remarks
12:00 am	Close of the meeting

ANHANG B: PERSONS INTERVIEWED/MET

Venue: Federal Ministry of Justice and Consumer Protection

Person interviewed/met	**Organisation represented**
OStA beim BGH Markus Busch	Federal Ministry of Justice and Consumer Protection
RiAG Nicole Fleischer	Federal Ministry of Justice and Consumer Protection
RD Dr. Garonne Bezjak	Federal Ministry of Justice and Consumer Protection
OStA Dr. Michael Sommerfeld	Federal Ministry of Justice and Consumer Protection
N.N.	Federal Ministry of the Interior
N.N.	Federal Ministry of the Interior
N.N.	Federal Criminal Police Office

Venue: Federal Ministry of Justice and Consumer Protection

Person interviewed/met	**Organisation represented**
OStA beim BGH Markus Busch	Federal Ministry of Justice and Consumer Protection
MR Dr. Katrin Brahms	Federal Ministry of Justice and Consumer Protection
OStA beim BGH Oliver Sabel	Federal Ministry of Justice and Consumer Protection
RiAG Nicole Fleischer	Federal Ministry of Justice and Consumer Protection
RiAG Michael Rothärmel	Federal Ministry of Justice and Consumer Protection
StA Christoph-Severin Haase	Federal Ministry of Justice and Consumer Protection

Frau Johanna Sprenger	Federal Ministry of Justice and Consumer Protection
Frau Kirsten Jakobs	Federal Ministry of Economic Affairs and Energy
N.N.	Federal Ministry of the Interior
N.N.	Federal Ministry of the Interior
N.N.	Federal Criminal Police Office

Meetings on

Venue: Federal Ministry of Justice and Consumer Protection

Person interviewed/met	**Organisation represented**
OStA beim BGH Markus Busch	Federal Ministry of Justice and Consumer Protection
MR Dr. Katrin Brahms	Federal Ministry of Justice and Consumer Protection
RiAG Nicole Fleischer	Federal Ministry of Justice and Consumer Protection
RiAG Michael Rothärmel	Federal Ministry of Justice and Consumer Protection
MDgt Klaus Meyer-Cabri	Eurojust
RD Dr. Holger Karitzky	Federal Office of Justice
N.N.	Federal Ministry of Interior
N.N.	Federal Ministry of Interior
N.N.	Federal Criminal Police Office
N.N.	Federal Office for Information Security
StA Christoph Lecher	General State Prosecutor

Venue: Federal Ministry of Justice and Consumer Protection

Person interviewed/met	Organisation represented
OStA beim BGH Markus Busch	Federal Ministry of Justice and Consumer Protection
RD Harald Schoen	Federal Ministry of Justice and Consumer Protection
RiAG Nicole Fleischer	Federal Ministry of Justice and Consumer Protection
N.N.	Federal Ministry of Interior
N.N.	Federal Ministry of Interior
N.N.	Federal Criminal Police Office
N.N.	Federal Office for Information Security
Frau Kirsten Jakobs	Federal Ministry of Economic Affairs and Energy
Rechtsanwalt Dr. Mark Ennulat	BITKOM e. V. (digital industry association)

Venue: Federal Ministry of Interior

Person interviewed/met	Organisation represented
RiAG Nicole Fleischer	Federal Ministry of Justice and Consumer Protection
N.N.	Federal Ministry of Interior
N.N.	Federal Ministry of Interior
N.N.	Federal Ministry of Interior
N.N.	Federal Criminal Police Office
N.N.	Federal Office for Information Security

Meetings on

Venue: Federal Ministry of Interior

Person interviewed/met	Organisation represented
MR Dr. Eberhard Schollmeyer	Federal Ministry of Justice and Consumer Protection
Frau Karla Brambati	Federal Ministry of Justice and Consumer Protection
RiAG Nicole Fleischer	Federal Ministry of Justice and Consumer Protection
N.N.	Federal Ministry of Interior
N.N.	Federal Ministry of Interior
N.N.	Federal Ministry of Interior
N.N.	Federal Ministry of Interior
N.N.	Federal Criminal Police Office
N.N.	Federal Criminal Police Office
N.N.	Federal Criminal Police Office
N.N.	Federal Ministry for Family Affairs, Senior Citizens, Women and Youth
N.N.	Federal Ministry of Economic Affairs and Energy
N.N.	Federal Review Board for Media Harmful to Minors
N.N.	jugendschutz.net (NGO)

Venue: *Federal Ministry of Interior*

Person interviewed/met	Organisation represented
MR Dr. Eberhard Schollmeyer	Federal Ministry of Justice and Consumer Protection
RiAG Nicole Fleischer	Federal Ministry of Justice and Consumer Protection
N.N.	Federal Ministry of Interior
N.N.	Federal Ministry of Interior
N.N.	Federal Criminal Police Office
N.N.	Federal Office for Information Security

Venue: *Federal Ministry of Interior*

Person interviewed/met	Organisation represented
RiAG Nicole Fleischer	Federal Ministry of Justice and Consumer Protection
N.N.	Federal Ministry of Interior
N.N.	Federal Ministry of Interior
N.N.	Federal Criminal Police Office
N.N.	Federal Office for Information Security

Venue: *Federal Ministry of Interior*

Person interviewed/met	Organisation represented
RiAG Nicole Fleischer	Federal Ministry of Justice and Consumer Protection
N.N.	Federal Ministry of Interior
N.N.	Federal Ministry of Interior
N.N.	Federal Criminal Police Office
N.N.	Federal Office for Information Security

Venue: *Central Office for Organised Crime and Corruption in Celle*

Person interviewed/met	**Organisation represented**
OStA Carsten Rosengarten	Central Office for Organised Crime and Corruption Crime in Celle
OStA Frank Lange	Public Prosecutor's Office in Verden
StA Markus Hartmann	Central Office for Cybercrime, Public Prosecutor's Office Cologne
StA Marcus Hartmann	Central Office for Cybercrime, Public Prosecutor's Office Berlin
OStA Lukas Knorr	Bavarian Central Office for the Prosecution of Cybercrime
KHK Jörn Bisping	Lüneburg Police Station
RiAG Nicole Fleischer	Federal Ministry of Justice and Consumer Protection

ANHANG C: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	GERMANY OR ACRONYM IN ORIGINAL LANGUAGE	GERMANY OR ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
	BBK		Federal Office of Civil Protection and Disaster assistance
	BfJ		Federal Office of Justice
	BKA		Federal Criminal Police Office
	BMFSFJ		Federal Ministry for Family affairs, Senior Citizens, Women and Youth
	BMI		Federal Ministry of Interior
	BMJV		Federal Ministry of Justice and Consumer Protection
	BMWI		Federal Ministry of Economic Affairs and Energy
	BPjM		Federal review Board for Media Harmful to Minors
	BPol		Federal Police
	BSI		Federal Office for Information Security
CEPOL			European Police College
	CERT-Bund		Federal Computer Emergency Response Team
CSAM			Child Sexual Abuse Material

	Cyber-AZ		National Cyberdefense Centre
	DRV		German Travel Association
EC3			European Cybercrime Centre
ECTEG			European Cubercrime Training and Education Group
EJTN			European Judicial Training Network
ENISA			European Network and Information Security Agency
EWPITC			Interpol European Working Party on IT-Crime
	FHPol		Police Academy
	G4C		German Competence Centre against Cybercrime e.V.
	GenStA		General State Prosecutor
	GMLZ		Joint Information and Situation Centre
	iPPP		Institutionalised Public-Private Partnership
ISF			Internal Security Funds
	IT-KRZ		National IT Crises response Centre

J-CAT			Joint Cybercrime Action Task
	KKB		Fight against Cyber Crime Committee
	LKAs		Criminal Police Offices of the Länder
	PCS		Police Crime Statistics
	ProPK		Federal Police Crime Prevention
	RBE		Regional Evidence Collection Unit
	RiStBV		Guidelines for criminal and monetary fine proceedings
	SN4C		Cybercrime Competence Centre
	StPO		Code of Criminal Procedure
	ZAC, StA Koln		Central Office for Cybercrime, Public Prosecutor's Office Cologne
	ZCB		Bavarian Central Office for the Prosecution of Cybercrime
	ZKA		Customs Criminal Investigation Office
	ZKI		Police Station
	ZOK		Central Office for Organised Crime and Corruption Crime