Rat der
Europäischen Union

Brüssel, den 28. Juli 2017
(OR. en)

8185/1/17
REV 1 DCL 1

GENVAL 41
CYBER 56

FREIGABE

des Dokuments	8185/1/17 REV 1 RESTREINT UE/EU RESTRICTED
vom	18. Mai 2017
Neuer Status:	Öffentlich zugänglich
Betr.:	Evaluierungsbericht über die siebte Runde der gegenseitigen Begutachtungen "Praktische Umsetzung und Durchführung europäischer Strategien zur Verhütung und Bekämpfung von Cyberkriminalität" – Bericht über Österreich

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 18. Mai 2017
(OR. en)

8185/1/17
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 41
CYBER 56

BERICHT

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

ANLAGE

Inhaltsverzeichnis

1. ZUSAMMENFASSUNG 5

2. EINLEITUNG 9

3. ALLGEMEINE FRAGEN UND STRUKTUREN 12

3.1. Nationale Strategie für Cyber-Sicherheit 12

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 Cyberstraftaten 16

3.4. Innerstaatliche Haushaltsmittel zur Prävention und Bekämpfung von Cyberkriminalität sowie Unterstützung durch EU-Haushaltsmittel 19

3.5. Fazit 20

4. NATIONALE STRUKTUREN 22

4.1. Justiz (Strafverfolgungen und Gerichte) 22

4.1.1. Interne Struktur 22

4.1.2. Fähigkeit zur und Hemmnisse für eine erfolgreiche Strafverfolgung 23

4.2. Strafverfolgungsbehörden 25

4.3. Sonstige Behörden/Einrichtungen/öffentlich-private Partnerschaft 27

4.4. Zusammenarbeit und Koordinierung auf nationaler Ebene 29

4.4.1. Rechtliche oder politische Verpflichtungen 29

4.4.2. Mittel für die Verbesserung der Zusammenarbeit 30

4.5. Fazit 30

5. RECHTLICHE ASPEKTE 34

5.1. Materielles Strafrecht im Bereich Cyberkriminalität 34

5.1.1. Übereinkommen des Europarats über Computerkriminalität 34

5.1.2. Beschreibung der nationalen Rechtsvorschriften 34

A/ Rahmenbeschluss 2005/222/JI des Rates über Angriffe auf Informationssysteme und Richtlinie 2013/40/EU über Angriffe auf Informationssysteme 34
B/ Richtlinie 2011/93/EU zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie 36
C/ Online-Kartenbetrug 36
5.2. Verfahrensrechtliche Fragen 37
5.2.1. Ermittlungstechniken 37
5.2.2. Forensik und Verschlüsselung 47
5.2.3. Elektronische Beweismittel 48
5.3. Schutz der Menschenrechte/Grundfreiheiten 49
5.4. Gerichtliche Zuständigkeit 53
5.4.1. Grundsätze für die Ermittlungen bei Cyberkriminalität 53
5.4.2. Regeln für das Vorgehen bei Kompetenzkonflikten und Befassung von Eurojust 53
5.4.3. Gerichtliche Zuständigkeit für in der "Cloud" begangene Cyberstraftaten 54
5.4.4. Auffassung Österreichs zum Rechtsrahmen zur Bekämpfung der Cyberkriminalität 55
5.5. Fazit 55

6. OPERATIVE ASPEKTE 58
6.1. Cyberangriffe 58
6.1.1. Art der Cyberangriffe 58
6.1.2. Mechanismen zur Abwehr von Cyberangriffen 59
6.2. Maßnahmen gegen Kinderpornografie und sexuellen Missbrauch von Kindern im Internet 62
6.2.1. Datenbank-Software zum Ausfindigmachen von Opfern und Maßnahmen zur Vermeidung einer erneuten Viktimisierung 62
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 63
6.2.3. Präventionsmaßnahmen gegen Sextourismus, pornografische Darbietungen von Kindern und Sonstiges 64
6.2.4. Akteure *und Maßnahmen gegen Websites, die Kinderpornografie enthalten oder verbreiten* 66
6.3. Online-Kartenbetrug 68
6.4. Fazit 68

7. INTERNATIONALE ZUSAMMENARBEIT 72
7.1. Zusammenarbeit mit EU-Agenturen 72
7.1.1. Formelle Anforderungen für die Zusammenarbeit mit Europol/EC3, Eurojust und ENISA 72
7.1.2. Bewertung der Zusammenarbeit mit Europol/EC3, Eurojust und ENISA 72
7.1.3. Operative Leistung von JIT und Cyberpatrouillen 75

7.2. Zusammenarbeit zwischen österreichischen Behörden und Interpol 76
7.3. Zusammenarbeit mit Drittstaaten 76
7.4. Zusammenarbeit mit der Privatwirtschaft 77
7.5. Instrumente der internationalen Zusammenarbeit 78
7.5.1. Rechtshilfe 78
7.5.2. Instrumente der gegenseitigen Anerkennung 80
7.5.3. Überstellung/Auslieferung 80
7.6. Fazit 81

8. AUS- UND FORTBILDUNG, SENSIBILISIERUNG UND PRÄVENTION 83
8.1. Spezifische Aus- und Fortbildung 83
8.2. Sensibilisierungsmaßnahmen 93
8.3. Verhütung von Cyberkriminalität 94
8.3.1 Nationale Rechtsvorschriften/politische Maßnahmen und andere Maßnahmen 94
8.3.2 Öffentlich-private Partnerschaft (ÖPP) 95
8.4. Fazit 95

9. SCHLUSSBEMERKUNGEN UND EMPFEHLUNGEN 98
9.1. Vorschläge Österreichs 98
9.2. Empfehlungen 98
9.2.1. Empfehlungen an Österreich 99
9.2.2. Empfehlungen an die Europäische Union, ihre Organe und Einrichtungen sowie an die anderen Mitgliedstaaten 100

Annex A: programme for the on-site visit and persons interviewed/met 102

Annex B: Persons interviewed/met 104

Annex C: List of abbreviations/glossary of terms 107

ANNEX D: Austrian legislation 109

1. ZUSAMMENFASSUNG

Der Evaluierungsbesuch war von den österreichischen Behörden gut vorbereitet und umfasste Treffen mit den maßgeblichen Akteuren mit Zuständigkeiten in den Bereichen Verhütung und Bekämpfung von Cyberkriminalität sowie Umsetzung und Durchführung europäischer Strategien, wie etwa Bundeskanzleramt, Bundesministerium für Justiz, Bundesministerium für Inneres, Staatsanwaltschaft Wien und Polizei. Der Gutachterausschuss hatte auch Gelegenheit, mit privaten Einrichtungen zusammenzutreffen, die an der Bekämpfung und Verhütung von Cyberkriminalität in Österreich beteiligt sind, wie Saferinternet.at, der Internet-Ombudsmann, Stopline u. a.

Während des Besuchs vor Ort gaben die österreichischen Behörden ihr Bestes, um dem Gutachterausschuss vollständige Informationen und Klarstellungen zu den rechtlichen und operativen Aspekten der Verhütung und Bekämpfung von Cyberkriminalität, der grenzüberschreitenden Zusammenarbeit und der Zusammenarbeit mit EU-Einrichtungen sowie der Cyberstrategie bereitzustellen.

Die "Österreichische Strategie für Cyber-Sicherheit" (ÖSCS) bietet ein umfassendes und proaktives Konzept für den Schutz des Cyberraums und der Menschen im virtuellen Raum und gewährleistet gleichzeitig die Achtung der Menschenrechte. Sie soll die Sicherheit und Widerstandsfähigkeit der österreichischen Infrastrukturen und Dienste im Cyberraum verbessern. Es ist ein wesentliches gemeinsames Anliegen des Staates, der Wirtschaft und der Gesellschaft, Cybersicherheit in einem nationalen und internationalen Kontext zu gewährleisten.

Die Strategie wurde von den Verbindungspersonen zum Nationalen Sicherheitsrat und Cyber-Experten unter Federführung des Bundeskanzleramtes erarbeitet. Letzteres richtete auch die Cyber-Sicherheit-Steuerungsgruppe ein, die auch die Umsetzung der Strategie koordiniert und begleitet. Die Cyber-Sicherheit-Steuerungsgruppe erstellt einen jährlichen Bericht zur "Cyber-Sicherheit in Österreich" und berät die Bundesregierung in Angelegenheiten der Cybersicherheit. Es werden Durchführungspläne mit den einzelnen Schritten auf dem Weg zur Verwirklichung der Ziele der Strategie sowie Jahresberichte über Cyberkriminalität in Österreich veröffentlicht.

Die nationalen Prioritäten in Bezug auf Cyberkriminalität sind einerseits mit den Prioritäten der EU in der Bekämpfung der Cyberkriminalität sowie andererseits mit den strategischen Leitlinien der ÖSCS abgestimmt. Die Betrugsbekämpfung mittels des Mediums Internet stellt eine hohe Priorität dar. Die nationale und internationale Zusammenarbeit – allen voran mit Europol/EC3 und Eurojust – wird massiv forciert. Auf nationaler Ebene wird die enge Zusammenarbeit mit nationalen Partnern in der Wirtschaft wie dem Kreditsektor, der Wirtschaftskammer und dem Internet-Ombudsmann weiter verstärkt. Darüber hinaus ist festzustellen, dass auf der Homepage des Bundeskriminalamtes (.BK) Verhaltensregelungen bei Massenphänomenen zu finden sind.

Zudem wird derzeit im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT)/BMI ein Cyber Security Centre (CSC) aufgebaut, dessen vorrangiges Ziel die Erhöhung der Widerstandsfähigkeit gegenüber Cyberangriffen durch die operative Koordination von Cybersicherheitsvorfällen (vor allem im Bereich der kritischen Infrastrukturen samt öffentlicher Verwaltung) einerseits sowie durch Präventionsmaßnahmen andererseits (Förderung und Koordinierung von Informationsaustausch, bewusstseinsbildende Maßnahmen, Teilnahme im Bereich der Sicherheitsforschung, technische Analysen, Lagebilder) ist.

Es gibt keine eigenen Staatsanwälte oder Richter, die ausschließlich oder in erster Linie mit Fällen von Cyberkriminalität befasst sind. Österreichische Staatsanwälte und Richter sind verpflichtet, ihre Qualifikationen laufend zu verbessern und an Schulungen teilzunehmen. Österreich bietet ihnen nationale und internationale Schulungen im Bereich Cyberkriminalität an, doch aus Sicht der Gutachter sind in diesem Bereich aufgrund der Tatsache, dass es in Österreich keine auf Cyberkriminalität spezialisierten Staatsanwälte oder Richter gibt, Verbesserungen und ein größeres Schulungsangebot erforderlich.

Die Strafverfolgungsbehörden sind im Hinblick auf Cyberkriminalität gut vorbereitet, organisiert, vernetzt und ausgebildet. Die Struktur der Strafverfolgungsbehörden ist auf Bundes-, Landes- und Gemeindeebene robust. Jede regionale Abteilung hat eine Stelle zur Unterstützung im Zusammenhang mit Cyberkriminalität mit einer angemessenen Infrastruktur ("Ersteinschreiter").

Was die Gesetzgebung angeht, so wurden die europäischen Rechtsvorschriften in Bezug auf Cyberkriminalität in österreichisches Recht umgesetzt. Österreich änderte seine straf- und verwaltungsrechtlichen Vorschriften in kriminalpolizeilichen Angelegenheiten in Bezug auf Cyberkriminalität ab; es wurden Strafen eingeführt und die verschiedenen Arten von kriminellem Verhalten in Bezug auf Cyberkriminalität explizit benannt. Es sind nunmehr eigene strafrechtliche Bestimmungen in Bezug auf Cyberkriminalität und eigene Bestimmungen des Strafprozessrechts zur Regelung von Ermittlungsmaßnahmen im Bereich Cyberkriminalität zum Zweck der Erhebung von Informationen und der Sammlung von Beweismaterial von Internetdiensteanbietern in Kraft. Im österreichischen Recht ist keine Möglichkeit vorgesehen, kompromittierte Websites in Strafverfahren zu sperren. Es wird darauf hingewiesen, dass die Datenspeicherfrist für Anbieter, beispielsweise für Abrechnungszwecke, drei Monate beträgt und Österreich Legislativmaßnahmen auf EU-Ebene betreffend die Datenspeicherung abwartet, bevor es seine Vorschriften überarbeitet.

In Österreich erstellen verschiedene Einrichtungen Statistiken, es gibt jedoch keine zentrale Stelle zur Verarbeitung von Statistiken. Infolgedessen liegen der Cyber-Sicherheit-Steuerungsgruppe möglicherweise keine klaren und umfassenden statistischen Angaben zur Entwicklung der Cyberkriminalität in Österreich vor. Nach Auffassung der Gutachter wäre es zweckmäßig, eine Weiterentwicklung der bereits bestehenden und operativen statistischen Systeme in Erwägung zu ziehen, um einen Beitrag zu einem besseren Verständnis der Gefahren zu leisten, die Straftäter für jeden an der Bekämpfung der Cyberkriminalität beteiligten Akteur bedeuten.

Die ISPA, die Vereinigung der Internetdiensteanbieter Österreichs, hat 200 Mitglieder und berät Unternehmen in Fragen des Cyberraums. Sie hat eine Plattform für die Strafverfolgungsbehörden eingerichtet, um die Zusammenarbeit im Bereich der Kommunikationsüberwachung zu verbessern, und arbeitet derzeit gemeinsam mit Unternehmen, Strafverfolgungsbehörden und der Universität Wien an einer Sicherheitsstrategie. Es wird jedoch darauf hingewiesen, dass für den Finanzsektor in Österreich keine verbindliche Meldepflicht zur Information der Polizei über verdächtiges oder kriminelles Verhalten gilt – hier besteht also eine Möglichkeit für Verbesserungen, und den Gutachtern zufolge könnten in diesem Zusammenhang verbindlichere Pflichten in Erwägung gezogen werden.

Österreich führt eine Reihe von Sensibilisierungsprogrammen im Bildungsbereich durch und verfügt über mehrere Einrichtungen, die Veröffentlichungen und Webseiten auf Kinderpornografie und nationalsozialistisches Gedankengut hin überwachen, um die Entfernung solcher Inhalte zu erleichtern. Es werden auch zahlreiche Präventionsprojekte (Click & Check, Cyber.Sicher oder Cyber.Kids) durchgeführt.

Da die Cyberkriminalität eine relativ neue Erscheinung ist, sind Schulung und Entwicklung von Fachkenntnissen die wichtigsten Bereiche. Es gibt keine allgemeinen Schulungen für Richter und Staatsanwälte auf dem Gebiet Cyberkriminalität, und die Teilnahme an den verfügbaren Kursen ist nicht verpflichtend. Andererseits hat Österreich maßgeschneiderte Schulungen für die Strafverfolgungsbehörden entwickelt. Alle Verwendungsgruppen werden im Bereich Cyberkriminalität geschult (Polizeigrundausbildung, Grundausbildung für dienstführende Beamte und Grundausbildung für leitende Beamte). Es gibt keine gemeinsamen Veranstaltungen für Polizei und Justiz. Die Organisation von gemeinsamen Fortbildungsveranstaltungen für Richter und Staatsanwälte, Polizisten und IT-Fachkräfte könnte dazu beitragen, den gesamten Prozess im Zusammenhang mit einer Straftat bis zur Anklageerhebung abzudecken.

Unter Berücksichtigung des ehrgeizigen Ansatzes im Hinblick auf die Bekämpfung der Cyberkriminalität und der Bemühungen um eine ständige Stärkung der Cybersicherheit in Österreich halten die Gutachter die Lage in Österreich für vielversprechend.

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" 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 richten 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 – abgesehen von der Zusammenarbeit mit den Strafverfolgungsbehörden – auch berücksichtigt werden, wie die Polizeibehörden mit Eurojust, ENISA und Europol/EC3 zusammenarbeiten und wie Rückmeldungen der betreffenden Akteure an die zuständigen Polizei- und Sozialdienste übermittelt werden. 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 Personen, die Opfer von Cyberkriminalität werden, 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. Österreich ist der dreiundzwanzigste 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 hatte, 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 und 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.

Als Sachverständige wurden Herr Attila Kökényesi - Bartos (Ungarn), Frau Mairead Cotter (Irland) und Herr Rogério Bravo (Portugal) mit der Begutachtung von Österreich beauftragt. Zwei Beobachter waren ebenfalls beteiligt: Herr Murat Ayilmaz (Eurojust) sowie Herr Sławomir Buczma vom Generalsekretariat des Rates.

Dieser Bericht ist vom Gutachterausschuss mit Unterstützung des Generalsekretariats des Rates ausgehend von den Ergebnissen des Besuchs in Österreich vom 18. bis 20. Mai 2016 und von den ausführlichen Antworten Österreichs auf den Fragebogen zusammen mit den ausführlichen Antworten auf spätere Folgefragen erstellt worden.

3. ALLGEMEINE FRAGEN UND STRUKTUREN

3.1. Nationale Strategie für Cyber-Sicherheit

Österreich hat darauf hingewiesen, dass die nationale und internationale Absicherung des Cyberraums eine seiner obersten Prioritäten ist. Mit der "Österreichischen Strategie für Cyber-Sicherheit" (ÖSCS) wurde von der Bundesregierung am 20. März 2013 ein umfassendes und proaktives Konzept zum Schutz des Cyberraums und der Menschen im virtuellen Raum beschlossen. Die Strategie für Cyber-Sicherheit beruht auf den Prinzipien Rechtsstaatlichkeit, Subsidiarität, Selbstregulierung und Verhältnismäßigkeit. Ein offenes und freies Internet, der Schutz personenbezogener Daten, die Unversehrtheit von miteinander verbundenen Netzwerken sind Grundlage für globalen Wohlstand, Sicherheit und Förderung der Menschenrechte.

Die ÖSCS bildet das Fundament der gesamtstaatlichen Zusammenarbeit im Bereich der Cyber-Sicherheit. Mit der Strategie für Cyber-Sicherheit wird auf nationaler Ebene eine operative Cyber-Koordinierungsstruktur festgelegt. Ziel ist es, einen regelmäßigen Informationsaustausch sicherzustellen, die Situation im Cyberraum laufend zu beobachten und zu bewerten sowie gemeinsame Maßnahmen festzulegen.

Die Cyber-Sicherheit-Steuerungsgruppe ist unter Leitung des Bundeskanzleramts zuständig für die Koordination von Maßnahmen im Zusammenhang mit der Cyber-Sicherheit auf politischer Ebene, die Überwachung und Unterstützung der Umsetzung der ÖSCS, die Ausarbeitung eines jährlichen Berichts über Cyber-Sicherheit und die Beratung der Bundesregierung in allen Angelegenheiten im Zusammenhang mit der Cyber-Sicherheit. Die Steuerungsgruppe besteht aus Verbindungspersonen zum Nationalen Sicherheitsrat und Cybersicherheitsexperten der im Nationalen Sicherheitsrat vertretenen Ministerien.

Das vom Bundeskanzleramt betriebene staatliche "Computer Emergency Response Team" (CERT) fungiert bereits jetzt als zentrale Anlaufstelle bei Cyber-Vorfällen. Mit den von CERT.at und Bundeskanzleramt eingerichteten "Austrian Trust Circles" werden die Sicherheitsexperten der verschiedenen Branchen vernetzt, um so im Anlassfall sofort die richtigen Kontakte verfügbar zu haben. Die österreichische CERT-Vereinigung wird erweitert und CERT.at wird gestärkt, um die landesweite Zusammenarbeit zwischen österreichischen CERTs zu erleichtern. Dies wird einerseits zur Förderung der Einrichtung von CERTs in allen Sektoren und andererseits zur Intensivierung des Informations- und Erfahrungsaustauschs über CERT-spezifische Themen beitragen.

Die operative Koordinierungsstruktur wird vom Bundesministerium für Inneres (nach dem Modell der öffentlich-privaten Partnerschaften) koordiniert, wobei die Ministerien und die operativen Strukturen von Wirtschaft und Forschung beteiligt sind. Ziel ist die Erleichterung der laufenden Kommunikation zwischen Staat, Privatsektor und Zivilgesellschaft.

3.2. Nationale Prioritäten in Bezug auf die Cyberkriminalität

Die nationalen Prioritäten in Bezug auf Cyberkriminalität sind einerseits mit den Prioritäten der EU in der Bekämpfung der Cyberkriminalität sowie andererseits mit den strategischen Leitlinien der ÖSCS abgestimmt. Die österreichischen Behörden haben erklärt, dass die Betrugsbekämpfung mittels des Mediums Internet eine hohe Priorität darstellen. Die nationale und internationale Zusammenarbeit – allen voran mit Europol/EC3 – wird massiv forciert. Zwecks Prävention wird mit nationalen Partnern in der Wirtschaft wie dem Kreditsektor, der Wirtschaftskammer und dem Internet- Ombudsmann eng zusammengearbeitet. Auf diese Weise werden neue Phänomene unverzüglich der Öffentlichkeit zugänglich gemacht, aber auch spezielle Berufsgruppen sofort über spezifische Phänomene informiert.

Darüber hinaus ist festzustellen, dass auf der Homepage des Bundeskriminalamtes (.BK) Verhaltensregelungen bei Massenphänomenen zu finden sind. Dieses Amt, das im Innenministerium (BMI) angesiedelt ist, nimmt an der Kampagne "Gegen das Wegsehen/Don´t Look Away!" teil, an der sich sieben europäische Länder (AT, CH, DE, FR, LUX, NL, PL) im Kampf gegen den sexuellen Missbrauch von Kindern im Zusammenhang mit Tourismus beteiligen. Das .BK ist auch an der Durchführung von Vorträgen und Schulungen für Hotelmanager von ACCOR u. a. beteiligt.

Die Prioritäten des .BK/5.2 C4 – Cybercrime Competence Centre bei der Bekämpfung von Cyberkriminalität orientieren sich an den Strategiezielen des Bundeskriminalamtes (.BK) und umfassen die Ermittlungen bei Cyberstraftaten, die IT-forensische Beweissicherung und eine "Cybercrime"-Meldestelle für die Bevölkerung. Darüber hinaus deckt das C4 die Themen Ausbildung, Prävention und internationale Polizeikooperation im Kontext der Cyberkriminalität ab. Zudem unterstützt Österreich die internationalen Bestrebungen der EU zur Bekämpfung der Cyberkriminalität durch seine Teilnahme an den "EMPACT cyber attack"-Arbeitsgruppen und seine Beteiligung an den "J-CAT Operations".

Zur Zeit des Besuchs vor Ort wurde im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT)/BMI ein "Cyber Security Centre" (CSC) aufgebaut. Vorrangiges Ziel dieses Zentrums ist die Erhöhung der Widerstandsfähigkeit gegen Cyberangriffe durch die operative Koordination von Cybersicherheitsvorfällen (vor allem im Bereich der kritischen Infrastrukturen samt öffentlicher Verwaltung) einerseits sowie durch Präventionsmaßnahmen andererseits (Förderung und Koordinierung von Informationsaustausch, bewusstseinsbildende Maßnahmen, Teilnahme im Bereich der Sicherheitsforschung, technische Analysen, Lagebilder).

3.3. Statistiken über die Cyberkriminalität

3.3.1. Wichtigste Trends, die die Cyberkriminalität fördern

Ermittlungsverfahren	2011	2012	2013	2014	Gesamt
Bei den Bezirksanwaltschaften	**508**	**589**	**596**	**651**	**2 344**
118a Widerrechtlicher Zugriff auf ein Computersystem	148	95	152	190	585
119a Missbräuchliches Abfangen von Daten	18	17	22	12	69
126a Datenbeschädigung	58	71	76	67	272
126b Störung der Funktionsfähigkeit eines Computersystems	14	50	19	16	99
126c Missbrauch von Computerprogrammen oder Zugangsdaten	71	61	82	68	282
148a Betrügerischer Datenverarbeitungsmissbrauch	163	243	197	217	820
207a Pornografische Darstellungen Minderjähriger	4	2	4	3	13
208a Anbahnung von Sexualkontakten zu Unmündigen		9	3	7	19
225a Datenfälschung	32	41	41	71	185
Bei den Staatsanwaltschaften	**1 070**	**1 088**	**1 053**	**1 222**	**4 433**
118a Widerrechtlicher Zugriff auf ein Computersystem	42	51	52	71	216
119a Missbräuchliches Abfangen von Daten	12	8	9	9	38
126a Datenbeschädigung	47	47	49	42	185
126b Störung der Funktionsfähigkeit eines Computersystems	6	13	6	9	34
126c Missbrauch von Computerprogrammen oder Zugangsdaten	26	22	21	36	105
148a Betrügerischer Datenverarbeitungsmissbrauch	226	227	275	345	1073
207a Pornografische Darstellungen Minderjähriger	693	659	554	630	2536
208a Anbahnung von Sexualkontakten zu Unmündigen		50	69	66	185
225a Datenfälschung	18	11	18	14	61
Gesamt	**1 578**	**1 677**	**1 649**	**1 873**	**6 777**

Anzahl sämtlicher Ermittlungsverfahren:

Ermittlungsverfahren	2011	2012	2013	2014	Gesamt
BAZ	268 097	196 719	195 251	190 444	850 511
ST	145 549	146 110	147 300	145 164	584 123
Gesamt	**413 646**	**342 829**	**342 551**	**335 608**	**1 434 634**

Die von der Polizei in den Jahren 2012-2014 erstellten Statistiken zeigen einen Rückgang der Zahl der Cyberstraftaten gegenüber der Gesamtzahl der in Österreich gemeldeten Straftaten.

	2012	2013	2014
Anzahl sämtlicher Straftaten	548 027	546 396	527 692
Cyberkriminalität gesamt	10 308	10 051	8 966
Cyberkriminalität in %	1,9 %	1,8 %	1,7 %

3.3.2. Zahl der gemeldeten Cyberstraftaten

Die Anfall- und Erledigungszahlen der Verfahren bei den Staatsanwaltschaften und Gerichten werden in einer Datenbank der Justiz (Verfahrensautomation Justiz – VJ) erfasst und können anonymisiert ausgewertet werden. Die rechtskräftigen Verurteilungszahlen werden von dem Strafregisteramt jährlich an die Statistik Austria gemeldet, welche wiederum jährlich in der Kriminalstatistik veröffentlicht werden (www.statistik.at).

Das Bundesministerium für Inneres führt parallel zur Justiz eigene Statistiken. Die Daten zur Cyberkriminalität sind Teil der Polizeilichen Kriminalstatistik. Dabei handelt es sich um eine Anzeigenstatistik, die im Bundeskriminalamt erstellt wird. Die erforderlichen Daten werden im Protokollierungssystem der Polizei erhoben und an die Datenbank des Bundeskriminalamtes übermittelt und anschließend ausgewertet. Diese hat keine Berührungspunkte mit den Statistiken der Justizbehörden.

Die folgende Tabelle enthält Daten zu Verurteilungen und Freisprüchen:

	2011	2012	2013	2014	Gesamt
Freispruch	**45**	**51**	**68**	**50**	**214**
Landesgericht	**40**	**35**	**44**	**44**	**163**
126a Datenbeschädigung	3	1	2	1	7
148a Betrügerischer Datenverarbeitungsmissbrauch	15	9	14	20	58
207a Pornografische Darstellungen Minderjähriger	22	25	28	22	97
208a Anbahnung von Sexualkontakten zu Unmündigen				1	1
Bezirksgericht	**5**	**16**	**24**	**6**	**51**
118a Widerrechtlicher Zugriff auf ein Computersystem		2	3	1	6
126a Datenbeschädigung	2	3	7	1	13
126c Missbrauch von Computerprogrammen oder Zugangsdaten	1	1	1		3
148a Betrügerischer Datenverarbeitungsmissbrauch	1	8	10	2	21
225a Datenfälschung	1	2	3	2	8
Verurteilung	**336**	**423**	**352**	**330**	**1 441**
Landesgericht	**308**	**395**	**331**	**315**	**1 349**
118a Widerrechtlicher Zugriff auf ein Computersystem		2	1	1	4
126a Datenbeschädigung	7	5	4	3	19
126b Störung der Funktionsfähigkeit eines Computersystems	1	1			2
126c Missbrauch von Computerprogrammen oder Zugangsdaten	4			1	5
148a Betrügerischer Datenverarbeitungsmissbrauch	99	101	95	138	433
207a Pornografische Darstellungen Minderjähriger	194	286	223	167	870
208a Anbahnung von Sexualkontakten zu Unmündigen			5	1	6
225a Datenfälschung	3		3	4	10
Bezirksgericht	**28**	**28**	**21**	**15**	**92**
118a Widerrechtlicher Zugriff auf ein Computersystem	1		2		3
126a Datenbeschädigung	2	3	2		7
126b Störung der Funktionsfähigkeit eines Computersystems				1	1
126c Missbrauch von Computerprogrammen oder Zugangsdaten	2		2		4
148a Betrügerischer Datenverarbeitungsmissbrauch	20	17	12	9	58
225a Datenfälschung	3	8	3	5	19
Gesamt	**381**	**474**	**420**	**380**	**1 655**

Die von der Polizei in den Jahren 2013-2014 erstellten Statistiken zeigen einen Rückgang bei der Aufdeckung von Cyberstraftaten.

Gemeldete Fälle	2013	2014	Abweichung
Cyberkriminalität im engeren Sinn	1 737	1 754	1,0 %
Cyberkriminalität im weiteren Sinn	8 314	7 212	-13,3 %
Cyberkriminalität gesamt	10 051	8 966	-10,8 %

Abgeschlossene Fälle	2013	2014	Abweichung
Cyberkriminalität im engeren Sinn	310	316	1,9 %
Cyberkriminalität im weiteren Sinn	4 234	3 344	-21,0 %
Cyberkriminalität gesamt	4 544	3 660	-19,5 %

Abschlussquote	2013	2014	Abweichung
Cyberkriminalität im engeren Sinn	17,8 %	18,0 %	0,2
Cyberkriminalität im weiteren Sinn	50,9 %	46,4 %	-4,6
Cyberkriminalität gesamt	45,2 %	40,8 %	-4,4

Identifizierte Verdächtige	2013	2014	Abweichung
Cyberkriminalität im engeren Sinn	334	326	-2,4 %
Cyberkriminalität im weiteren Sinn	3 621	3 278	-9,5 %
Cyberkriminalität gesamt	3 955	3 604	-8,9 %

Die Gutachter haben festgestellt, dass die vom Ministerium des Inneren und vom Strafregisteramt an die Statistik Austria gemeldeten Zahlen hinsichtlich der aufgedeckten Cyberstraftaten und der durchgeführten Ermittlungen voneinander abweichen.

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

Es gibt keine spezielle Mittelzuweisung für die Verhütung und die Bekämpfung von Cyberkriminalität. Es wurden jedoch eigene Mittel für die Durchführung der in der unten stehenden Tabelle ausgewiesenen Projekte bereitgestellt.

Projektträger	**Projekttitel**	**EU-Mittel geplant**	**laufend**	**geplant**
BK Büro 5.2 Cyber Crime Competence Centre C4	Cyber.Kids	27 000,00	x	
BK Büro 1.4 Kriminalstrategie	BK-Radar	270 000,00		x
BK Büro 1.4	Neue Medien	350 000,00	x	
BK Abt. 7 Wirtschaftskriminalität	Kontrollsystem	665 660,70		x
II/BVT/3	Cyber Security Centre	1 134 000.00	x	

3.5. Fazit

- Die Bundesregierung hat am 20. März 2013 die Österreichische Strategie für Cyber-Sicherheit (ÖSCS) angenommen. Dabei handelt es sich um ein umfassendes und proaktives Konzept zum Schutz des Cyberraums, das das Fundament der gesamtstaatlichen Zusammenarbeit in diesem Bereich bildet. Sie ist Ausdruck der Vision des österreichischen Staates für die Entwicklung der Digitalwirtschaft unter Wahrung der Cyber-Sicherheit für seine Bürger.

- Die ÖSCS wurde mit Unterstützung der wichtigsten privaten Akteure, verschiedener CERTs – sowohl staatlicher (GovCERT, MilCERT) als auch privater Natur (CERTs, Banken usw.) – sowie des Cyber Crime Competence Centre (.BK Büro 5.2 C4) entworfen. Die Strategie ist eine politische Maßnahme auf höchster Ebene und wurde von der Cyber-Sicherheit-Steuerungsgruppe ausgearbeitet, die die maßgeblichen Ministerien (Justiz-, Innen-, Außen- und Verteidigungsministerium) umfasst und vom Bundeskanzleramt geleitet wird. Die Steuerungsgruppe scheint gut aufgestellt zu sein, um alle wichtigen Informationen zu sammeln und so eine fundierte Gesamtstrategie zu entwerfen sowie die wichtigsten relevanten Grundsätze festzulegen, einschließlich Rückmeldungen aus der Branche.

- Die nationalen Prioritäten in Bezug auf Cyberkriminalität sind einerseits mit den Prioritäten der EU für die Bekämpfung der Cyberkriminalität sowie andererseits mit den strategischen Leitlinien der ÖSCS abgestimmt. Die nationale und internationale Zusammenarbeit wird erheblich intensiviert. Zwecks Prävention wird mit nationalen Partnern in der Wirtschaft wie dem Kreditsektor, der Wirtschaftskammer und dem Internet- Ombudsmann eng zusammengearbeitet. Die Initiative zur Einrichtung eines Büros des Internet-Ombudsmanns ist besonders zu erwähnen, da diese Person Kunden vertritt, deren Rechte infolge von Online-Transaktionen und verdächtigem Verhalten im Internet verletzt wurden.

- In Österreich werden Statistiken von verschiedenen Einrichtungen erstellt. Die Anfall- und Erledigungszahlen der Verfahren bei den Staatsanwaltschaften und Gerichten werden in einer Datenbank der Justiz erfasst. Die Zahlen zu rechtskräftigen Verurteilungen werden von dem Strafregisteramt jährlich an die Statistik Austria gemeldet, welche wiederum jährlich in der Kriminalstatistik veröffentlicht werden.

- Das Bundesministerium für Inneres führt parallel zur Justiz eigene Statistiken. Die Daten zur Cyberkriminalität sind Teil der Polizeilichen Kriminalstatistik. Dabei handelt es sich um eine Anzeigenstatistik, die im Bundeskriminalamt erstellt wird. Die erforderlichen Daten werden im Protokollierungssystem der Polizei erhoben und an die Datenbank des Bundeskriminalamtes übermittelt.[7]

- Zudem erstellen Hotlines Statistiken aufgrund einer parallelen Meldemöglichkeit. Da in den Statistiken sowohl öffentliche als auch private Hotlines erfasst sind, könnten Mehrfachmeldungen desselben Sicherheitsvorfalls die ordnungsgemäße Erstellung von Statistiken behindern. Derzeit ist nicht bekannt, wie viele gemeldete Sicherheitsvorfälle gleichzeitig aufgenommen wurden und so möglicherweise die Zahl der Meldungen vervielfacht haben.

- Zudem unterscheiden sich die statistischen Daten von Innenministerium, Polizei und Justizministerium. Diese Unterschiede wurden nicht genauer erläutert, es wurde nur darauf hingewiesen, dass die einzelnen Organisationen bei der Definition der Basisdaten ihrer Statistiken und auch bei der Definition von Cyberkriminalität unterschiedlichen Ansätzen folgen. Die unterschiedlichen Ansätze hinsichtlich der Basisdaten ergeben sich aus den unterschiedlichen Rollen der Akteure im österreichischen System. Folglich liegen der Cyber-Sicherheit-Steuerungsgruppe unter Umständen keine klaren und umfassenden Statistiken vor, was ihre Bemühungen untergraben könnte, weil sie sich kein klares Bild von der Entwicklung der Cyberkriminalität machen kann. Nach Auffassung der Gutachter wäre es zweckmäßig, eine Weiterentwicklung der bereits bestehenden und operativen statistischen Systeme in Erwägung zu ziehen, um einen Beitrag zu einem besseren Verständnis der Gefahren zu leisten, die Straftäter im Bereich Cyberkriminalität für jeden Akteur bedeuten.

- Zudem können die Unterschiede in den Statistiken auch zu Konflikten führen, beispielsweise zwischen Polizei und Innenministerium bei der Analyse des Finanz- und Personalbedarfs der für Cyberkriminalität zuständigen Stellen der Polizei, oder sie können die internationalen bzw. die EU-Statistiken verfälschen.

- Österreich hat keine spezielle Mittelzuweisung für die Bekämpfung der Cyberkriminalität vorgenommen, doch die in dem Bericht genannten Einrichtungen erhalten ein eigenes Budget von der Regierung. Es ist jedoch darauf hinzuweisen, dass Österreich zusätzlich zum eigenen Budget für den Bereich Cyberkriminalität aktiv EU-Mittel nutzt, was eine empfohlene Vorgehensweise ist.

[7] Der Gutachterausschuss wurde beim Besuch vor Ort darüber unterrichtet, dass derzeit eine neue Berichtssoftware für die Landespolizeidirektionen entwickelt wird. Die Beschaffung aussagefähiger statistischer Daten ist ein wichtiger Aspekt dieser Arbeit. Soweit technisch und rechtlich möglich, werden mit ihr bekannte Mängel angegangen.

4. NATIONALE STRUKTUREN

4.1. Justiz (Strafverfolgungen und Gerichte)

4.1.1. Interne Struktur

Auf Basis einer rechtswirksamen Anklage ist das Hauptverfahren vor Gericht zu führen. Alle Richter, Staatsanwälte und kriminalpolizeilichen Organe haben ihr Amt unparteilich und unvoreingenommen auszuüben und jeden Anschein der Befangenheit zu vermeiden. Sie haben die zur Belastung und die zur Verteidigung des Beschuldigten dienenden Umstände mit der gleichen Sorgfalt zu ermitteln.

Kriminalpolizei und Staatsanwaltschaft sind verpflichtet, jeden ihnen zur Kenntnis gelangten Anfangsverdacht einer Straftat, die nicht bloß auf Verlangen einer hierzu berechtigten Person zu verfolgen ist, in einem Ermittlungsverfahren von Amts wegen aufzuklären. Sofern das Gesetz nichts anderes bestimmt, obliegt die Anklage der Staatsanwaltschaft, die als Leiterin des Ermittlungsverfahrens fungiert. Es wird jedoch darauf hingewiesen, dass Kriminalpolizei und Staatsanwaltschaft das Ermittlungsverfahren so weit wie möglich im Einvernehmen zu führen haben. Kann ein solches nicht erzielt werden, so hat die Staatsanwaltschaft die erforderlichen Anordnungen zu erteilen, die von der Kriminalpolizei zu befolgen sind.

Für die Verfolgung eines betrügerischen Datenverarbeitungsmissbrauchs mit besonders hohem Schaden ist die Zentrale Staatsanwaltschaft zur Verfolgung von Wirtschaftsstrafsachen und Korruption (WKStA) zuständig. Im Übrigen gelten für den Bereich Cyberkriminalität die allgemeinen Zuständigkeiten der Staatsanwaltschaften und Gerichte. Im Rahmen ihrer sachlichen Zuständigkeiten kommt der WKStA eine bundesweite Zuständigkeit zu.

Der Gutachterausschuss stellte fest, dass es insbesondere auf regionaler Ebene keine Richter oder Staatsanwälte gibt, die auf die Bekämpfung von Cyberkriminalität spezialisiert sind.

4.1.2. Fähigkeit zur und Hemmnisse für eine erfolgreiche Strafverfolgung

Auch wenn kein eigener Personalpool für den Einsatz im Bereich Cyberkriminalität besteht, wurde der Personaleinsatz im Bereich der Staatsanwältinnen und Staatsanwälte – insbesondere auch bei der Zentralen Staatsanwaltschaft zur Verfolgung von Wirtschaftsstrafsachen und Korruption (WKStA) – in den letzten Jahren deutlich erhöht. Diese Entwicklung wird von den österreichischen Behörden als positiv bewertet, auch in Bezug auf die Cyberkriminalität. Die Anzahl der Vollzeitkapazitäten bei Staatsanwältinnen und Staatsanwälten hat sich in den letzten zehn Jahres wie folgt entwickelt (tatsächlicher Einsatz, Planstellen):

StA GenProk + JBidL	SOLL	IST
04/1995	208	203,00
04/1996	208	206,00
04/1997	209	204,00
04/1998	209	207,00
04/1999	210	208,00
04/2000	220	215,00
04/2001	218	219,00
04/2002	218	216,00
10/2003	216	217,50
04/2004	213	220,50
04/2005	212	216,68
04/2006	216	218,50
04/2007	283	221,50
10/2008	340	341,50
01/2009	340	335,75
07/2010	367	363,00
07/2011	376	345,75
09/2012	382	370,75
01/2013	393	373,50
05/2014	406	380,00
04/2015	406	395,30

Zentrale Staatsanwaltschaft zur Verfolgung von Wirtschaftsstrafsachen und Korruption (WKStA)	SOLL	IST
01/2009	5	1,00
07/2009	5	5,00
01/2010	5	7,00
07/2010	7	8,00
01/2011	12	8,00
07/2011	21	10,50
01/2012	21	15,00
07/2012	21	16,00
01/2013	29	20,00
07/2013	30	21,50
01/2014	35	21,50
07/2014	40	25,50
01/2015	40	27,25
07/2015	40	30,50

Von den zuständigen Staatsanwaltschaften wurden folgende Hindernisse für ein erfolgreiche Verfolgung von Cyberstraftaten genannt:

- die internationale Dimension der Cyberkriminalität;
- die langwierige Bearbeitung von Rechtshilfeersuchen bzw. Erfolglosigkeit der Rechtshilfeersuchen;
- hohes einschlägiges Know-how der Täter, das jenes der Angehörigen der Strafverfolgungsbehörden übersteigt; ständig neue Formen der Cyberkriminalität;

- Verschleierungshandlungen der Täter durch Verwendung gefälschter Rufnummern und IP-Adressen bzw. durch Verwendung falscher Identitäten sowie durch Geldtransfers über Unternehmen wie Western Union; anonymer Internetzugang; Einsatz von Anonymisierungsprogrammen; Schwierigkeiten beim Nachweis der tatsächlichen Verwendung des Computers;
- begrenzte Möglichkeit der Einsichtnahme in soziale Netzwerke;
- große Datenvolumen =) aufgrund Überschreitung der Kapazität der Polizei ist teilweise die Bestellung von Sachverständigen erforderlich (sehr kostenintensiv);
- Probleme in Fällen, in denen Daten in der "Cloud" bzw. auf ausländischen Servern gespeichert werden;
- kurze Speicherfristen, Verbot der Vorratsdatenspeicherung;
- Vergabe von IP-Adressen im Mobilfunkbereich an mehrere Teilnehmer gleichzeitig, wodurch eine Zuordnung zu einem Gerät nicht mehr möglich ist;
- Überfrachtung aller erhebenden Beamten (Polizei, Staatsanwaltschaft) mit strafverfolgungsfremden Tätigkeiten;
- teilweise nicht im erforderlichen Ausmaß vorhandene Bereitschaft von Telekommunikationsanbietern zur Mitwirkung an den Wochenenden.

4.2. Strafverfolgungsbehörden

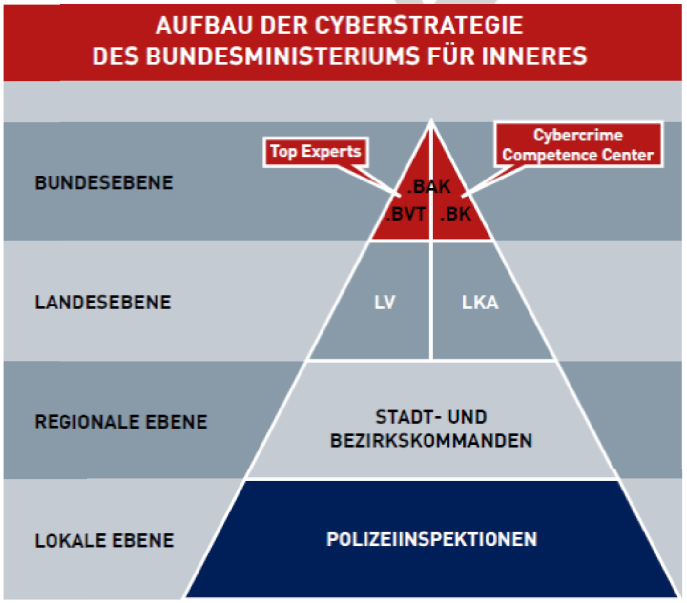
BK

Gemäß § 4 des Bundeskriminalamtsgesetzes BGBl. I Nr. 22/2002 i. d. F. von 6.2.2015 ist das .BK zuständig für die Leitung, Koordinierung und Steuerung der Arbeiten im Bereich Internetbetrug auf Bundesebene, die internationale Koordinierung und internationale Ermittlungen und die Anzeigenerstattung an die Staatsanwaltschaft. Die Leitung, Koordinierung und Steuerung auf Landesebene, die nationale Koordinierung und die nationalen Ermittlungen sowie die Anzeigenerstattung an die Staatsanwaltschaft werden von den Landeskriminalämtern (LKA) durchgeführt. Die Polizeiinspektionen sind für die Entgegennahme von Anzeigen, Ermittlungen und Anzeigenerstattung an die Staatsanwaltschaft zuständig.

Das Cybercrime Competence Centre (C4)

Das Cybercrime Competence Centre (.BK/5.2 C4) ist für alle Ermittlungen zur Bekämpfung von Cyberkriminalität im "engeren Sinn" (§§ 118a, 119a, 126a-c, 148a, 225a StGB) sowie für die Sicherung elektronischer Beweismittel zuständig. Es wurde 2011 im .BK eingerichtet. Das C4 gliedert sich in eine Meldestelle sowie in die Referate Zentrale Aufgaben, IT-Beweissicherung und Ermittlungen. Es ist die nationale und internationale Zentralstelle zur Bekämpfung von Cyberkriminalität in Österreich. Neben dem C4 auf Bundesebene bestehen in allen LKA (Landeskriminalämtern) vergleichbare Dienststellen. In diesen Organisationseinheiten sind kriminalpolizeilich und technisch ausgebildete Experten mit der Bekämpfung von Cyberkriminalität und der IT-Forensik in den jeweiligen Bundesländern befasst. Auf lokaler Ebene unterstützen Bezirks-IT-Ermittler die Polizeibeamten in den Polizeiinspektionen – die sogenannten "Ersteinschreiter". Derzeit gibt es in Österreich 300 Ersteinschreiter. Für die praktische und theoretische Ausbildung der Ersteinschreiter soll mehr Zeit vorgesehen werden. Dies wird 2017 geschehen.

Zur Illustration ist im Cyberstrategie-Organigramm der gesamte Behördenaufbau in der Bekämpfung von Cyberkriminalität dargestellt. Für die Ermittlungen zuständig ist das Referat II/BK/5.2.3 des Bundeskriminalamtes (.BK). Die IT-Forensiker des Bundeskriminalamtes sind organisatorisch im Referat II/BK/5.2.2 angesiedelt.



Zudem ist im .BK, Büro 3.2, die Meldestelle für Kinderpornografie und Kindersextourismus etabliert.

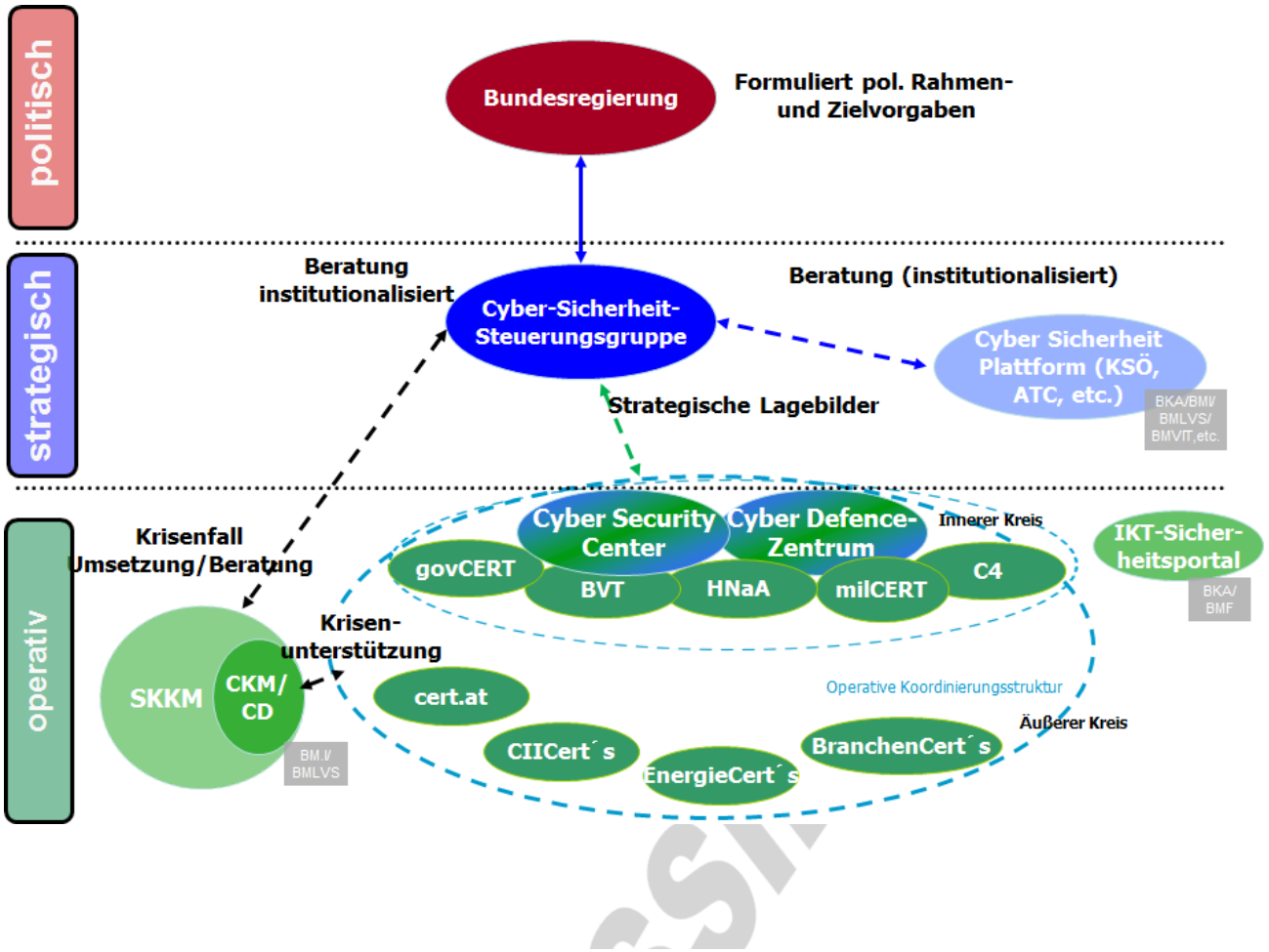
Das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung verfügt einerseits über Stellen, die die Prävention in Zusammenhang mit Cyberkriminalität zum Ziel haben, andererseits aber auch solche, die sich mit der Strafverfolgung in Zusammenhang mit begangenen Straftaten beschäftigen.

4.3. Sonstige Behörden/Einrichtungen/öffentlich-private Partnerschaft

Im Zuge der Umsetzung der Österreichischen Strategie für Cyber-Sicherheit wurde zusätzlich eine operative Koordinierungsstruktur für Cybersicherheitsvorfälle geschaffen, die relevante Stakeholder aus dem öffentlichen Dienst und der Wirtschaft zusammenführt. Den Vorsitz dieser Struktur bildet das Cyber Security Centre (CSC) (sowie im Cyberabwehrfall das Cyber Defence Centre (CDZ) im Bundesministerium für Landesverteidigung und Sport). Das CSC wurde im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT)/BMI eingerichtet, um die Widerstandsfähigkeit gegen Cyberangriffe durch die operative Koordination von Cybersicherheitsvorfällen (vor allem im Bereich der kritischen Infrastrukturen samt öffentlicher Verwaltung) einerseits sowie durch Präventionsmaßnahmen andererseits (Förderung und Koordinierung von Informationsaustausch, bewusstseinsbildende Maßnahmen, Teilnahme im Bereich der Sicherheitsforschung, technische Analysen, Lagebilder) zu erhöhen.

Aus dem öffentlichen Sektor sind folgende Einrichtungen im "inneren Kreis" vertreten: C4, GovCERT, MilCERT und das Heeres-Nachrichtenamt. Im erweiterten Kreis sollen zukünftig auch CERT.at, Branchen-CERTs und relevante Stakeholder im Bereich Cyber-Sicherheit einbezogen werden. Ziel ist eine regelmäßige Abstimmung sowie eine gemeinsame Lagebeurteilung.

Der österreichische Privatsektor hat das CERT.at eingerichtet. Die Mitglieder dieses CERT.at sind private Fachleute aus dem Cyberbereich, die vom privaten und vom öffentlichen Sektor bezahlt werden und die Cyberkriminalität bekämpfen. Es unterstützt den privaten und den öffentlichen Sektor, analysiert aktuelle Gefahren, schlägt Lösungen vor, koordiniert in Krisensituationen, ist die Anlaufstelle für den Privatsektor, veröffentlicht aktuelle Gefahrenanalysen und arbeitet mit den Internetdiensteanbietern zusammen.



Gemäß § 4 des Bundeskriminalamtsgesetzes , BGBl. I Nr. 22/2002 i. d. F. von 6.2.2015 ist das Bundeskriminalamt als übergeordnete Zentralstelle mit der nationalen Koordinierung von überregionalen und internationalen Amtshandlungen betraut. Es besteht ein Weisungsrecht gegenüber den nachgeordneten Dienststellen. Die Koordinierung bei der Bekämpfung von Cyberkriminalität erfolgt durch das Cybercrime Competence Centre C4.

Zudem gibt es ein über KIRAS finanziertes internationales Forschungsprojekt und das .BK (Büro 3.2) stellt zwei Beiräte der privaten Meldestelle "STOPLINE" (www.stopline.at). Zudem ist das Büro 3.2 ständiges Mitglied des "Runden Tischs – Ethik im Tourismus", etabliert im Bundesministerium für Wirtschaft, Familie und Jugend. Auch wird laufend an internationalen Meetings, welche von ECPAT organisiert werden, teilgenommen.

Überdies wird auf Homepages, in diversen Videospots sowie Foldern zahlreicher NGO wie ECPAT, STOPLINE (Providervereinigung) oder SAFER INTERNET ausdrücklich auf die BK-Hotline meldestelle@interpol.at hingewiesen.

Im nationalen Programm zum Schutz kritischer Infrastrukturen wurde das Modell der öffentlich-privaten Partnerschaft gewählt, um die Widerstandsfähigkeit strategisch wichtiger Unternehmen zu stärken. Dies betrifft sowohl vorbereitende Maßnahmen gegen physische Gefahren, als auch gegen Cyberkriminalität. Die Umsetzung dieser öffentlich-privaten Partnerschaft erfolgt durch die Bereitstellung von Informationsmaterial (z. B. Leitfaden für Risikomanagement), Veranstaltungen, Beratungen zu sicherheitsrelevanten Themen, ein Frühwarnsystem sowie eine ständig erreichbare Kontakt- und Meldestelle.

4.4. Zusammenarbeit und Koordinierung auf nationaler Ebene

4.4.1. Rechtliche oder politische Verpflichtungen

In Österreich ist die Privatwirtschaft derzeit nicht dazu verpflichtet, Cyberangriffe zu melden.

Die österreichischen Behörden haben eine ausreichende und effiziente Zusammenarbeit von Industrie, Banken, Privatwirtschaft und Strafverfolgungsbehörden bei der Verhinderung und Bekämpfung von Online-Kartenbetrug im Allgemeinen gemeldet. Private Unternehmen haben in der Regel keine Einwände dagegen, Zugang zu den Servern zu gewähren, wenn sie über gerichtlichen Auftrag dazu aufgefordert werden.

Im Zuge der Umsetzung der Österreichischen Strategie für Cyber-Sicherheit befindet sich ein "Cyber-Krisenmechanismus" (CKM) im Aufbau, der in den Staatlichen Krisen- und Katastrophenschutzmechanismus (SKKM) integriert werden soll.

4.4.2. Mittel für die Verbesserung der Zusammenarbeit

Das über KIRAS (Österreichisches Förderprogramm für die Sicherheitsforschung) finanzierte Forschungsprojekt 3B3M als Teil des Projekts "Social Media Crime", bei dem es sich um eine umfangreiche Untersuchung handelt, wurde zur wissenschaftlich fundierten Strukturierung von Social-Media-spezifizierten Kriminalitätsformen durchgeführt. Mittels wissenschaftlicher Recherche und Erhebungen wurde eine Analyse einzelner Social-Media-Crime-Phänomene und -Aktivitäten erstellt, die nicht nur Aufschluss über Erscheinungsformen, sondern auch über Ursachen und Folgen sowie Opfer- und Tätercharakteristika gibt. Die Ergebnisse wurden auf Basis von kriminalpolizeilichen Anforderungen strukturiert und kategorisiert. Anhand dieser Einteilung werden Präventions- und Gegenmaßnahmen, die international bereits eingesetzt bzw. angedacht sind, aufgezeigt. Aufbauend auf diesen Erkenntnissen wurden konkrete Handlungsempfehlungen generiert, die kriminalpolizeiliches Vorgehen dabei unterstützen sollen, Social-Media-Crime langfristig zu reduzieren.

Den österreichischen Behörden zufolge verfügen die Spezialeinheiten über ausreichende Ausstattung und Kompetenz. Nach Auffassung der Gutachter hat Österreich keine Haushaltsmittel speziell für die Verbesserung der Zusammenarbeit in Bezug auf Cyberkriminalität zugewiesen; allerdings verfügen die zuvor beschriebenen Stellen über Haushaltsmittel, die aus dem Regierungshaushalt stammen. Ferner wurde der Gutachterausschusses von den österreichischen Vertretern beim Besuch vor Ort darüber unterrichtet, dass für die IT-Forensik zusätzliche Mittel sowohl für technische Hilfsmittel als auch für Personal erforderlich sind.

4.5. Fazit

- Es gibt in Österreich keine spezialisierten Gerichte und Richter für Cyberkriminalität. Es gibt hierfür auch keine spezialisierten Staatsanwaltschaften oder Staatsanwälte. Die Zentrale Staatsanwaltschaft zur Verfolgung von Wirtschaftsstrafsachen und Korruption in Wien stellte einen Staatsanwalt vor, der breit angelegte internationale Ermittlungen überwacht hat und an der Zusammenarbeit im Rahmen des Einsatzes des gemeinsamen Ermittlungsteams "Mozart" beteiligt war.

- Der Gutachterausschuss erfuhr, dass die Staatsanwälte gut geschult sind und Angelegenheiten wie Kinderpornografie gut bewältigen können; dies gilt allerdings nicht für Cyberkriminalität im engeren Sinne. Nach Auffassung der Gutachter könnte eine verbesserte Schulung und Spezialisierung die Fähigkeiten der Staatsanwälte in Bezug auf Cyberkriminalität im engeren Sinne verbessern.

- Die Gutachter sind der Auffassung, dass zu Bekämpfung der Cyberkriminalität nicht nur Wissen und Verständnis hinsichtlich der Frage, wie die Straftat begangen wurde, sondern auch hinsichtlich der Frage, wie bei den verschiedenen Arten von Cyberkriminalität ermittelt werden muss, erforderlich sind. Gerade bei der Cyberkriminalität ändern sich Modus operandi sowie verwendete Software und Hilfsmittel beständig und in rascher Folge. Die Ermittlungsmethoden müssen aktualisiert werden (beispielsweise durch spezielle Ermittlungscomputersoftware), was ständige Aufmerksamkeit für diese Fragen – einschließlich der rechtlichen Auswirkungen – erfordert. Ferner erfordert die Bekämpfung der Cyberkriminalität oftmals Rechtshilfe seitens anderer Länder, was eine Vernetzung erforderlich macht. Nach Auffassung der Gutachter sollte Österreich entweder spezialisierte Staatsanwälte ernennen, die mit der Bekämpfung der Cyberkriminalität betraut sind, und/oder das Leistungsniveau und die Zahl der Fachstaatsanwälte und -richter auf diesem Gebiet erhöhen.

- Anders als bei Richtern und Staatsanwälten verfügt die Polizei über eine sehr gut ausgebaute Zentraleinheit, nämlich das für Cyberkriminalität zuständige Cybercrime Competence Centre (C4). Dieses gliedert sich in eine Meldestelle sowie in die Referate Zentrale Aufgaben, IT-Beweissicherung und Ermittlungen. Es ist die nationale und internationale Zentralstelle zur Bekämpfung von Cyberkriminalität in Österreich. Neben dem C4 auf Bundesebene bestehen in allen Landeskriminalämtern (LKA) vergleichbare Dienststellen. In diesen Organisationseinheiten sind kriminalpolizeilich und technisch ausgebildete Experten mit der Bekämpfung von Cyberkriminalität und der IT-Forensik befasst. Auf lokaler Ebene unterstützen Bezirks-IT-Ermittler die Polizeibeamten in den Polizeiinspektionen.

- Ferner wird die zentrale Struktur der Polizei auf Länderebene und auf lokaler Ebene von einer Reihe von Ersteinschreitern unterstützt, einer Belegschaft von 300 Personen, von denen in nahezu jeder lokalen Polizeidienststelle 1-3 Personen vorhanden sind. Diese Belegschaft von Ersteinschreitern verfügt über eigene Ausstattung und erhält häufig Schulungen, damit sie darauf vorbereitet sind, an Ort und Stelle Live-Forensik- oder Datenaufzeichnungsaufgaben zu erledigen. Die örtlichen Polizeibeamten erhalten eine kurze Schulung zur Cyberkriminalität (4-8 Stunden) zwecks allgemeiner Vorbereitung.

- Obwohl das C4 als disziplinübergreifendes Zentrum für Erkenntnisbeschaffung und Polizeiarbeit eingerichtet wurde, ist es anscheinend unterbesetzt und die Gutachter nahmen Kenntnis vom ausdrücklichen Wunsch nach mehr Finanzmitteln und Ressourcen. Ein anderer Aspekt ist die Notwendigkeit, für IT-Forensik – sowohl für die technische Ausstattung als auch für Personalressourcen – mehr Mittel bereitzustellen, um den Rückstand bei IT-Forensik-Prüfungen abzubauen.

- Die Polizei unterhält gute partnerschaftliche Beziehungen zu der privaten Meldestelle mit der Bezeichnung "Stopline" und auch zu den Vertretern des von der EU ko-finanzierten Projekts "Saferinternet.at". Das C4 führt auch ein eigenes, von der EU finanziertes Kriminalitätspräventionsprojekt (Cyber.Kids) durch. Bei dem Projekt wird mit Unterstützung durch Psychologen sichergestellt, dass Informationen für Minderjährige von diesen auch verstanden werden.

- Das BVT verfügt über Stellen, welche einerseits die Prävention in Zusammenhang mit Cyberkriminalität zum Ziel haben, andererseits aber auch solche, welche sich mit der Strafverfolgung in Zusammenhang mit begangenen Straftaten beschäftigen.

- Im Allgemeinen hat Österreich ein gewisses Maß an Zusammenarbeit zwischen dem öffentlichen Sektor und der Privatwirtschaft bei der Bekämpfung und Verhütung von Cyberkriminalität entwickelt. Im März 2015 wurde die Cyber-Sicherheits-Plattform ins Leben gerufen, in der unter Führung der Privatwirtschaft die öffentliche Hand und die Privatwirtschaft vertreten sind.

- Der Gutachterausschuss stellte fest, dass einige Schwierigkeiten bei der Einrichtung öffentlich-privater Partnerschaften in bestimmten Bereichen zu verzeichnen sind. Die Anforderung von Informationen von Finanzinstituten und das entsprechende Datenanforderungsverfahren beanspruchen erhebliche Zeit und sind kompliziert. Es gibt keine eindeutigen oder verbindlichen Meldepflichten für die Privatwirtschaft im Allgemeinen, was die Entscheidung, ob im Fall einer Straftat Ermittlungen oder Strafverfolgungsmaßnahmen erfolgen sollen, teilweise in der Hand der Privatwirtschaft belässt. Nach Auffassung der Gutachter wäre es sinnvoll, die Zusammenarbeit zwischen Polizei und Finanzwirtschaft im Hinblick auf bestimmte Fälle, in denen eine obligatorische Meldung erfolgen müsste, zu verstärken**.**

- Es wird die Auffassung vertreten, dass durch die Erhöhung der Ressourcen erhebliche Verbesserungen bei der täglich rund um die Uhr tätigen Kontaktstelle möglich wären, sodass sie den massiven Anstieg des Informationsdatenverkehrs bewältigen könnte.

5. RECHTLICHE ASPEKTE

5.1. Materielles Strafrecht im Bereich Cyberkriminalität

5.1.1. Übereinkommen des Europarats über Computerkriminalität

Das Übereinkommen über Computerkriminalität (SEV Nr. 185 wurde über das Strafrechtsänderungsgesetz 2002, BGBl. I Nr. 134/2002 dem Ratifizierungsprozess unterworfen.

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

Der Rahmenbeschluss 2005/222/JI über Angriffe auf Informationssysteme wurde mit dem Strafrechtsänderungsgesetz 2008, BGBl. I Nr. 109/2007, in österreichisches Recht umgesetzt. Mit den zum 1. Jänner 2016 in Kraft getretenen Bestimmungen des Strafrechtsänderungsgesetzes 2015 wird die Richtlinie 2013/40/EU über Angriffe auf Informationssysteme und zur Aufhebung des Rahmenbeschlusses 2005/222/JI umgesetzt.

In Bezug auf Cyberkriminalität gibt es im österreichischen Recht weitreichende Rechtsvorschriften[8]. Folgende Handlungen sind nach dem österreichischen Strafgesetzbuch (StGB) strafbar: widerrechtlicher Zugang auf ein Computersystem (§ 118a), Störung der Funktionsfähigkeit eines Computersystems/Datenbeschädigung (§§ 126a – 126b), missbräuchliches Abfangen von Daten (§ 119a), Missbrauch von Vorrichtungen – das Herstellen, Verbreiten, Beschaffen zwecks Gebrauchs, Einführen oder anderweitige Verfügbarmachen oder Besitzen von Instrumenten zum Missbrauch von Computern (§ 126c), betrügerischer Datenverarbeitungsmissbrauch (§ 148a), Datenfälschung (§ 225a), Verletzung des Telekommunikationsgeheimnisses (§ 119 StGB).

[8] Aufgrund der hohen Seitenzahl wurde die Beschreibung nicht in den Bericht aufgenommen. Weitere Informationen siehe Anlage D.

Widerrechtlicher Zugriff auf ein Computersystem (§ 118a StGB) und missbräuchliches Abfangen von Daten (§ 119a StGB) werden nur mit Ermächtigung des Verletzten verfolgt.

Das Versenden oder das Kontrollieren des Versands von Spam-Mails sind nicht als spezifischer Straftatbestand erfasst.

Das strafrechtliche Kompetenzpaket, BGBl. I Nr. 108/2010, sah eine Neuregelung und Schärfung der bestehenden Bestimmungen im Bereich vermögensrechtlicher Maßnahmen vor, um (hohe) Verbrechensgewinne insbesondere auch im Bereich organisierter Kriminalität effektiver zu Gunsten des Staates einziehen zu können.

Nach dem Gesetz ist bei diesen Straftaten auch der Versuch strafbar. Auch Anstiftung, Beihilfe und Versuch sind nach österreichischem Recht strafbar. Die strafrechtliche Verantwortlichkeit juristischer Personen ist im Verbandsverantwortlichkeitsgesetz (VbVG) geregelt. Juristische Personen können für die Begehung einer Straftat durch eine Person in Führungsposition (Entscheidungsträger) und für die Begehung einer Straftat durch unterstellte Personen (Mitarbeiter) strafrechtlich zur Verantwortung gezogen werden. Im letzteren Fall jedoch nur bei mangelnder Überwachung oder Kontrolle. Voraussetzung für die Strafbarkeit der juristischen Person ist, dass die Tat zu ihren Gunsten begangen wurde oder durch die Tat sie treffende Pflichten verletzt wurden. Bei Erfüllung der geschilderten Tatbestandsmerkmale ist daher auch eine strafrechtliche Verantwortlichkeit juristischer Personen für Cyberstraftaten möglich. Als Sanktion ist grundsätzlich eine Geldbuße vorgesehen, deren Höhe sich aus der Multiplikation der Anzahl der verhängten Tagessätze (von 40 bis 180) mit der Höhe des festgelegten Tagessatzes (Bemessung nach Ertrag) errechnet.

Ferner sehen die Tatbestände der "Datenbeschädigung" sowie der "Störung der Funktionsfähigkeit eines Computersystems" künftig Qualifikationen für die Herbeiführung eines schweren Schadens oder der Beeinträchtigung wesentlicher Bestandteile der kritischen Infrastruktur vor. Die Tatbegehung durch die Verwendung mehrerer Computersysteme ("Bot-Netze") erfährt Berücksichtigung seitens der österreichischen Behörden. Darüber hinaus sollen mit diesem Gesetz auch bislang strafrechtlich nicht vollständig erfasste Fälle neuer Erscheinungsformen von Computerkriminalität (etwa "Phishing" und "Skimming" im Bereich des Zahlungskartenbetrugs – § 241h StGB) einer strafrechtlichen Sanktionierung unterworfen werden. Weitere legislative Schritte sind derzeit nicht in Aussicht genommen.

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

Die materiellrechtliche Umsetzung der Richtlinie 2011/92/EU zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI, der Richtlinie 2011/36/EU zur Verhütung und Bekämpfung des Menschenhandels und zum Schutz seiner Opfer sowie zur Ersetzung des Rahmenbeschlusses 2002/629/JI und der Umsetzung von Empfehlungen der "GRETA"-Expertengruppe des Europarats betreffend die Umsetzung des Übereinkommens des Europarates zur Verhütung und Bekämpfung des Menschenhandels sowie des VN-Kinderrechtskomitees in Bezug auf das Fakultativprotokoll zum Übereinkommen über die Rechte des Kindes betreffend den Verkauf von Kindern, die Kinderprostitution und die Kinderpornografie erfolgte mit dem Sexualstrafrechtsänderungsgesetz 2013, BGBl. I Nr. 116/2013.

Unter Bezugnahme auf das Internet erfolgte die Einführung verschärfter Qualifikationen im Bereich des Delikts der "pornografischen Darstellungen Minderjähriger" sowie eines neuen Tatbestands zum "Grooming.
Derzeit sind das Herstellen, das Verbreiten oder der Besitz von Kinderpornografie mit Hilfe eines Computers (§ 207a), die Kontaktaufnahme oder das Anfreunden ("grooming") mit Kindern mit Hilfe eines Computers (§ 208a des StGB, "Anbahnung von Sexualkontakten zu Unmündigen") strafbar (siehe Anlage D).

C/ Online-Kartenbetrug

Nach österreichischem Recht sind alle betrügerischen Finanzgeschäfte strafbar. Gemäß Artikel 41h STGB (Ausspähen von Daten eines unbaren Zahlungsmittels) sind folgende Handlungen strafbar:
§ 241h. (1) Wer Daten eines Zahlungsmittels mit dem Vorsatz ausspäht,

1. dass er oder ein Dritter durch deren Verwendung im Rechtsverkehr unrechtmäßig bereichert werde oder
2. sich oder anderen eine Fälschung unbarer Zahlungsmittel (§ 241a) zu ermöglichen,

ist mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen.

(2) Wer die Tat gewerbsmäßig oder als Mitglied einer kriminellen Vereinigung begeht, ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.
(3) Der Täter ist nicht zu bestrafen, wenn er freiwillig, bevor die ausgespähten Daten im Sinne des Abs. Z oder 2 verwendet wurden, die Gefahr ihrer Verwendung durch Verständigung der Behörde, des Berechtigten oder auf andere Weise beseitigt. Besteht die Gefahr einer solchen Verwendung nicht oder ist sie ohne Zutun des Täters beseitigt worden, so ist er nicht zu bestrafen, wenn er sich in Unkenntnis dessen freiwillig und ernstlich bemüht, sie zu beseitigen.

5.2. Verfahrensrechtliche Fragen

5.2.1. Ermittlungstechniken

Nach österreichischem Recht sind folgende Ermittlungsmaßnahmen anwendbar:

Beschlagnahme (§ 115 StPO – allgemeine Regelung, keine besondere Bezugnahme auf Computerdaten, gilt daher auch für Computer, Server und alle Arten von Datenträgern):
§ 115(1) Beschlagnahme ist zulässig, wenn die sichergestellten Gegenstände voraussichtlich

1. im weiteren Verfahren als Beweismittel erforderlich sein werden,
2. privatrechtlichen Ansprüchen unterliegen oder
3. dazu dienen werden, eine gerichtliche Entscheidung auf Konfiskation (§ 19a StGB), auf Verfall (§ 20 StGB), auf erweiterten Verfall (§ 20b StGB), auf Einziehung (§ 26 StGB) oder einer anderen gesetzlich vorgesehenen vermögensrechtlichen Anordnung zu sichern, deren Vollstreckung andernfalls gefährdet oder wesentlich erschwert würde.

Über die Beschlagnahme hat das Gericht auf Antrag der Staatsanwaltschaft oder einer von der Sicherstellung betroffenen Person unverzüglich zu entscheiden. Gegebenenfalls ist die Beschlagnahme auf die dort angeführten Aufnahmen und Kopien zu beschränken. In einem Beschluss, mit dem eine Beschlagnahme zur Sicherung einer gerichtlichen Entscheidung auf Verfall (§ 20 StGB) oder auf erweiterten Verfall (§ 20b StGB) bewilligt wird, ist ein Geldbetrag zu bestimmen, in dem die für verfallen zu erklärenden Vermögenswerte Deckung finden. Wenn und sobald die Voraussetzungen der Beschlagnahme nicht oder nicht mehr bestehen oder ein nach Abs. 5 bestimmter Geldbetrag erlegt wird, hat die Staatsanwaltschaft, nach dem Einbringen der Anklage das Gericht, die Beschlagnahme aufzuheben.

Durchsuchung (§§ 119 bis 122 StPO – allgemeine Regelungen, keine besondere Bezugnahme auf Computerdaten):

§ 117(2) "Durchsuchung von Orten und Gegenständen" das Durchsuchen

a. eines nicht allgemein zugänglichen Grundstückes, Raumes, Fahrzeuges oder Behältnisses,
b. einer Wohnung oder eines anderen Ortes, der durch das Hausrecht geschützt ist, und darin befindlicher Gegenstände,

<u>Durchsuchung von Orten und Gegenständen sowie von Personen</u>

Durchsuchung von Orten und Gegenständen (§ 117 Z 2) ist zulässig, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass sich dort eine Person verbirgt, die einer Straftat verdächtig ist, oder Gegenstände oder Spuren befinden, die sicherzustellen oder auszuwerten sind.

(2) Durchsuchung einer Person (§ 117 Z 3) ist zulässig, wenn diese

1. festgenommen oder auf frischer Tat betreten wurde,
2. einer Straftat verdächtig ist und auf Grund bestimmter Tatsachen anzunehmen ist, dass sie Gegenstände, die der Sicherstellung unterliegen, bei sich oder Spuren an sich habe,
3. durch eine Straftat Verletzungen erlitten oder andere Veränderungen am Körper erfahren haben könnte, deren Feststellung für Zwecke eines Strafverfahrens erforderlich ist.

§ 120(1) Durchsuchungen von Orten und Gegenständen nach § 117 Z 2 lit. b und von Personen nach § 117 Z 3 lit. b sind von der Staatsanwaltschaft auf Grund einer gerichtlichen Bewilligung anzuordnen; bei Gefahr im Verzug ist die Kriminalpolizei allerdings berechtigt, diese Durchsuchungen vorläufig ohne Anordnung und Bewilligung vorzunehmen. Gleiches gilt in den Fällen des § 170 Abs. 1 Z 1 für die Durchsuchung von Personen nach § 117 Z 3 lit. b. Das Opfer darf jedoch in keinem Fall gezwungen werden, sich gegen seinen Willen durchsuchen zu lassen (§§ 19 Abs. 2 Z 3 und 121 Abs. 1 letzter Satz).

(2) Durchsuchungen nach § 117 Z 2 lit. a und nach § 117 Z 3 lit. a kann die Kriminalpolizei von sich aus durchführen.

§ 121(1) Vor jeder Durchsuchung ist der Betroffene unter Angabe der hierfür maßgebenden Gründe aufzufordern, die Durchsuchung zuzulassen oder das Gesuchte freiwillig herauszugeben. Von dieser Aufforderung darf nur bei Gefahr im Verzug sowie im Fall des § 119 Abs. 2 Z 1 abgesehen werden. Die Anwendung von Zwang (§ 93) ist im Fall der Durchsuchung einer Person nach § 119 Abs. 2 Z 3 unzulässig.

(2) Der Betroffene hat das Recht, bei einer Durchsuchung nach § 117 Z 2 anwesend zu sein, sowie einer solchen und einer Durchsuchung nach § 117 Z 3 lit. b eine Person seines Vertrauens zuzuziehen; für diese gilt § 160 Abs. 2 sinngemäß. Ist der Inhaber der Wohnung nicht zugegen, so kann ein erwachsener Mitbewohner seine Rechte ausüben. Ist auch das nicht möglich, so sind der Durchsuchung zwei unbeteiligte, vertrauenswürdige Personen beizuziehen.

Davon darf nur bei Gefahr im Verzug abgesehen werden. Einer Durchsuchung in ausschließlich der Berufsausübung gewidmeten Räumen einer der in § 157 Abs. 1 Z 2 bis 4 erwähnten Personen ist von Amts wegen ein Vertreter der jeweiligen gesetzlichen Interessenvertretung beziehungsweise der Medieninhaber oder ein von ihm namhaft gemachter Vertreter beizuziehen.

(3) Bei der Durchführung sind Aufsehen, Belästigungen und Störungen auf das unvermeidbare Maß zu beschränken. Die Eigentums- und Persönlichkeitsrechte sämtlicher Betroffener sind soweit wie möglich zu wahren. Eine Durchsuchung von Personen nach § 117 Z 3 lit. b ist stets von einer Person desselben Geschlechts oder von einem Arzt unter Achtung der Würde der zu untersuchenden Person vorzunehmen.

§ 122(1) Über jede Durchsuchung nach § 120 Abs. 1 erster Satz letzter Halbsatz hat die Kriminalpolizei sobald wie möglich der Staatsanwaltschaft zu berichten (§ 100 Abs. 2 Z 2), welche im Nachhinein eine Entscheidung des Gerichts über die Zulässigkeit der Durchsuchung (§ 99 Abs. 3) zu beantragen hat. Wird die Bewilligung nicht erteilt, so haben Staatsanwaltschaft und Kriminalpolizei mit den ihnen zu Gebote stehenden rechtlichen Mitteln den der gerichtlichen Entscheidung entsprechenden Rechtszustand herzustellen.

(2) Werden bei einer Durchsuchung Gegenstände gefunden, die auf die Begehung einer anderen als der Straftat schließen lassen, derentwegen die Durchsuchung vorgenommen wird, so sind sie zwar sicherzustellen; es muss jedoch hierüber ein besonderes Protokoll aufgenommen und sofort der Staatsanwaltschaft berichtet werden.
(3) In jedem Fall ist dem Betroffenen sogleich oder längstens binnen 24 Stunden eine Bestätigung über die Durchsuchung und deren Ergebnis sowie gegebenenfalls die Anordnung der Staatsanwaltschaft samt gerichtlicher Entscheidung auszufolgen oder zuzustellen.

Sicherstellung (§§ 110 bis 114 StPO – allgemeine Regelungen, keine besondere Bezugnahme auf Computerdaten, gilt daher auch für Computer, Server und alle Arten von Datenträgern):
§ 110(1) Sicherstellung ist zulässig, wenn sie
1. aus Beweisgründen,
2. zur Sicherung privatrechtlicher Ansprüche oder
3. zur Sicherung der Konfiskation (§ 19a StGB), des Verfalls (§ 20 StGB), des erweiterten Verfalls (§ 20b StGB), der Einziehung (§ 26 StGB) oder einer anderen gesetzlich vorgesehenen vermögensrechtlichen Anordnung erforderlich erscheint.

(2) Sicherstellung ist von der Staatsanwaltschaft anzuordnen und von der Kriminalpolizei durchzuführen.
(3) Die Kriminalpolizei ist berechtigt, Gegenstände (§ 109 Z 1 lit. a) von sich aus sicherzustellen,
1. wenn sie
   a) in Niemandes Verfügungsmacht stehen,
   b) dem Opfer durch die Straftat entzogen wurden,
   c) am Tatort aufgefunden wurden und zur Begehung der strafbaren Handlung verwendet oder dazu bestimmt worden sein könnten, oder
   d) geringwertig oder vorübergehend leicht ersetzbar sind,
2. wenn ihr Besitz allgemein verboten ist (§ 445a Abs. 1),

3. die im Rahmen einer Durchsuchung nach § 120 Abs. 2 aufgefunden werden oder mit denen eine Person, die aus dem Grunde des § 170 Abs. 1 Z 1 festgenommen wird, betreten wurde oder die im Rahmen ihrer Durchsuchung gemäß § 120 Abs. 1 zweiter Satz aufgefunden werden, oder
4. in den Fällen des Artikels 18 der Verordnung (EU) Nr. 608/2013 zur Durchsetzung der Rechte geistigen Eigentums durch die Zollbehörden und zur Aufhebung der Verordnung (EG) Nr. 1383/2003 des Rates, ABl. Nr. L 181 vom 29.06.2013 S. 15.

(4) Die Sicherstellung von Gegenständen aus Beweisgründen (Abs. 1 Z 1) ist nicht zulässig und jedenfalls auf Verlangen der betroffenen Person aufzuheben, soweit und sobald der Beweiszweck durch Bild-, Ton- oder sonstige Aufnahmen oder durch Kopien schriftlicher Aufzeichnungen oder automationsunterstützt verarbeiteter Daten erfüllt werden kann und nicht anzunehmen ist, dass die sichergestellten Gegenstände selbst oder die Originale der sichergestellten Informationen in der Hauptverhandlung in Augenschein zu nehmen sein werden.

§ 111(1) Jede Person, die Gegenstände oder Vermögenswerte, die sichergestellt werden sollen, in ihrer Verfügungsmacht hat, ist verpflichtet (§ 93 Abs. 2), diese auf Verlangen der Kriminalpolizei herauszugeben oder die Sicherstellung auf andere Weise zu ermöglichen. Diese Pflicht kann erforderlichenfalls auch mittels Durchsuchung von Personen oder Wohnungen erzwungen werden; dabei sind die §§ 119 bis 122 sinngemäß anzuwenden.

(2) Sollen auf Datenträgern gespeicherte Informationen sichergestellt werden, so hat jedermann Zugang zu diesen Informationen zu gewähren und auf Verlangen einen elektronischen Datenträger in einem allgemein gebräuchlichen Dateiformat auszufolgen oder herstellen zu lassen. Überdies hat er die Herstellung einer Sicherungskopie der auf den Datenträgern gespeicherten Informationen zu dulden.

(3) Personen, die nicht selbst der Tat beschuldigt sind, sind auf ihren Antrag die angemessenen und ortsüblichen Kosten zu ersetzen, die ihr durch die Trennung von Urkunden oder sonstigen beweiserheblichen Gegenständen von anderen oder durch die Ausfolgung von Kopien notwendigerweise entstanden sind.

(4) In jedem Fall ist der von der Sicherstellung betroffenen Person sogleich oder längstens binnen 24 Stunden eine Bestätigung über die Sicherstellung auszufolgen oder zuzustellen und sie über das Recht, Einspruch zu erheben (§ 106) und eine gerichtliche Entscheidung über die Aufhebung oder Fortsetzung der Sicherstellung zu beantragen (§ 115), zu informieren. Von einer Sicherstellung zur Sicherung einer Entscheidung über privatrechtliche Ansprüche (§ 110 Abs. 1 Z 2) ist, soweit möglich, auch das Opfer zu verständigen.

§ 112 (1) Widerspricht die von der Sicherstellung betroffene oder anwesende Person, auch wenn sie selbst der Tat beschuldigt ist, der Sicherstellung von schriftlichen Aufzeichnungen oder Datenträgern unter Berufung auf ein gesetzlich anerkanntes Recht auf Verschwiegenheit, das bei sonstiger Nichtigkeit nicht durch Sicherstellung umgangen werden darf, so sind diese Unterlagen auf geeignete Art und Weise gegen unbefugte Einsichtnahme oder Veränderung zu sichern und bei Gericht zu hinterlegen. Auf Antrag des Betroffenen sind die Unterlagen jedoch bei der Staatsanwaltschaft zu hinterlegen, die sie vom Ermittlungsakt getrennt aufzubewahren hat. In beiden Fällen dürfen die Unterlagen von Staatsanwaltschaft oder Kriminalpolizei nicht eingesehen werden, solange nicht über die Einsicht nach den folgenden Absätzen entschieden worden ist.

(2) Der Betroffene ist aufzufordern, binnen einer angemessenen, 14 Tage nicht unterschreitenden Frist jene Teile der Aufzeichnungen oder Datenträger konkret zu bezeichnen, deren Offenlegung eine Umgehung seiner Verschwiegenheit bedeuten würde; zu diesem Zweck ist er berechtigt, in die hinterlegten Unterlagen Einsicht zu nehmen. Unterlässt der Betroffene eine solche Bezeichnung, so sind die Unterlagen zum Akt zu nehmen und auszuwerten. Anderenfalls hat das Gericht, im Fall eines Antrags nach Abs. 1 vorletzter Satz jedoch die Staatsanwaltschaft die Unterlagen unter Beiziehung des Betroffenen sowie gegebenenfalls geeigneter Hilfskräfte oder eines Sachverständigen zu sichten und anzuordnen, ob und in welchem Umfang sie zum Akt genommen werden dürfen. Unterlagen, die nicht zum Akt genommen werden, sind dem Betroffenen auszufolgen. Aus deren Sichtung gewonnene Erkenntnisse dürfen bei sonstiger Nichtigkeit nicht für weitere Ermittlungen oder als Beweis verwendet werden.

(3) Gegen die Anordnung der Staatsanwaltschaft kann der Betroffene Einspruch erheben, in welchem Fall die Unterlagen dem Gericht vorzulegen sind, das zu entscheiden hat, ob und in welchem Umfang sie zum Akt genommen werden dürfen; Abs. 2 letzter Satz gilt. Einer Beschwerde gegen den Beschluss des Gerichts kommt aufschiebende Wirkung zu.

§ 113(1) Die Sicherstellung endet,

1. wenn die Kriminalpolizei sie aufhebt (Abs. 2),
2. wenn die Staatsanwaltschaft die Aufhebung anordnet (Abs. 3),
3. wenn das Gericht die Beschlagnahme anordnet.

(2) Die Kriminalpolizei hat der Staatsanwaltschaft über jede Sicherstellung unverzüglich, längstens jedoch binnen 14 Tagen zu berichten (§ 100 Abs. 2 Z 2), soweit sie eine Sicherstellung nach § 110 Abs. 3 nicht zuvor wegen Fehlens oder Wegfalls der Voraussetzungen aufhebt. Dieser Bericht kann jedoch mit dem nächstfolgenden verbunden werden, wenn dadurch keine wesentlichen Interessen des Verfahrens oder von Personen beeinträchtigt werden und die sichergestellten Gegenstände geringwertig sind, sich in niemandes Verfügungsmacht befinden oder ihr Besitz allgemein verboten ist (§ 445a Abs. 1). Im Fall des § 110 Abs. 3 Z 4 hat die Kriminalpolizei nach den Bestimmungen der §§ 3, 4 und 6 des Produktpirateriegesetzes 2004, BGBl. I Nr. 56/2004, vorzugehen.

(3) Die Staatsanwaltschaft hat im Fall einer Sicherstellung nach § 109 Z 1 lit. b sogleich bei Gericht die Beschlagnahme zu beantragen oder, wenn deren Voraussetzungen nicht vorliegen oder weggefallen sind, die Aufhebung der Sicherstellung anzuordnen.

(4) Im Fall einer Sicherstellung von Gegenständen (§ 109 Z 1 lit. a) findet eine Beschlagnahme auch auf Antrag nicht statt, wenn sich die Sicherstellung auf Gegenstände im Sinne des § 110 Abs. 3 Z 1 lit. a und d oder Z 2 bezieht oder der Sicherungszweck durch andere behördliche Maßnahmen erfüllt werden kann. In diesen Fällen hat die Staatsanwaltschaft die erforderlichen Verfügungen über die sichergestellten Gegenstände und ihre weitere Verwahrung zu treffen und gegebenenfalls die Sicherstellung aufzuheben.

Für die Verwahrung sichergestellter Gegenstände hat bis zur Berichterstattung über die Sicherstellung (§ 113 Abs. 2) die Kriminalpolizei, danach die Staatsanwaltschaft zu sorgen.

Die **Auskunft über Daten einer Nachrichtenübermittlung** (gemäß § 134 Z 2 StPO die Erteilung einer Auskunft über Verkehrsdaten (§ 92 Abs. 3 Z 4 TKG), Zugangsdaten (§ 92 Abs. 3 Z 4a TKG), die nicht einer Anordnung gemäß § 76a Abs. 2 unterliegen, und Standortdaten (§ 92 Abs. 3 Z 6 TKG) eines Telekommunikationsdienstes oder eines Dienstes der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes)) ist nach § 135 Abs. 2 StPO zulässig,

1. wenn und solange der dringende Verdacht besteht, dass eine von der Auskunft betroffene Person eine andere entführt oder sich sonst ihrer bemächtigt hat, und sich die Auskunft auf Daten einer solchen Nachricht beschränkt, von der anzunehmen ist, dass sie zur Zeit der Freiheitsentziehung vom Beschuldigten übermittelt, empfangen oder gesendet wird,
2. wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit einer Freiheitsstrafe von mehr als sechs Monaten bedroht ist, gefördert werden kann und der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Auskunft ausdrücklich zustimmt, oder
3. wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, gefördert werden kann und auf Grund bestimmter Tatsachen anzunehmen ist, dass dadurch Daten des Beschuldigten ermittelt werden können.
4. wenn auf Grund bestimmter Tatsachen zu erwarten ist, dass dadurch der Aufenthalt eines flüchtigen oder abwesenden Beschuldigten, der einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung dringend verdächtig ist, ermittelt werden kann.

Eine **Überwachung von Nachrichten** (gemäß § 134 Z 3 StPO das Ermitteln des Inhalts von Nachrichten (§ 92 Abs. 3 Z 7 TKG), die über ein Kommunikationsnetz (§ 3 Z 11 TKG) oder einen Dienst der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes) ausgetauscht oder weitergeleitet werden) ist nach § 135 Abs. 3 StPO zulässig,

1. in den Fällen des Abs. 2 Z 1,

2. in den Fällen des Abs. 2 Z 2, sofern der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Überwachung zustimmt,

3. wenn dies zur Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, erforderlich erscheint oder die Aufklärung oder Verhinderung von im Rahmen einer kriminellen oder terroristischen Vereinigung oder einer kriminellen Organisation (§§ 278 bis 278b StGB) begangenen oder geplanten strafbaren Handlungen ansonsten wesentlich erschwert wäre und

a) der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, oder einer Straftat gemäß §§ 278 bis 278b StGB dringend verdächtig ist, oder

b) auf Grund bestimmter Tatsachen anzunehmen ist, dass eine der Tat (lit. a) dringend verdächtige Person die technische Einrichtung benützen oder mit ihr eine Verbindung herstellen werde;

"Nachricht" im Sinne des § 92 Abs. 3 Z 7 TKG 2003 ist jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlichen Kommunikationsdienst ausgetauscht oder weitergeleitet wird. Dies schließt nicht Informationen ein, die als Teil eines Rundfunkdienstes über ein Kommunikationsnetz an die Öffentlichkeit weitergeleitet werden, soweit die Informationen nicht mit dem identifizierbaren Teilnehmer oder Nutzer, der sie erhält, in Verbindung gebracht werden können (siehe dazu gleich unten zum Begriff "Inhaltsdaten").

Die Ermittlungen werden grundsätzlich über Auftrag der Staatsanwaltschaft im Sinne der Strafprozessordnung (StPO) bzw. nach dem Sicherheitspolizeigesetz (SPG) geführt.
Methoden: Ermittlung von IP-Adressen, Überwachung der Kommunikation, Auswertung von elektronischen Beweismittel, bei Betrugsdelikten mittels des Medium Internet konsequente Verfolgung der Geldspuren. Hausdurchsuchungen und die Sicherstellung von Daten ermöglichen den Einsatz von spezieller forensischer Auswertesoftware. Dadurch besteht die Möglichkeit, Daten sichtbar zu machen und das begangene Delikt zu beweisen und bei Gericht anzuzeigen.
Die Vorratsdatenspeicherung von Verkehrsdaten für einen Zeitraum von drei Monaten durch Anbieter, beispielsweise für Abrechnungszwecke, ist zulässig.

Von den zuständigen Staatsanwaltschaften wurden folgende, am häufigsten verwendete Ermittlungsmethoden genannt:

- Auskünfte über Stamm- und Zugangsdaten,
- Auskünfte über Bankkonten und Bankgeschäfte,
- Auskünfte über Daten einer Nachrichtenübermittlung;
- Einleitung eines Auslandschriftverkehrs seitens der Polizei;
- Rechtshilfeersuchen;
- Sicherstellung und Auswertung von Datenträgern durch Polizeibeamte bzw. Sachverständige;
- Durchführung eines automationsunterstützten Datenabgleichs (Rasterfahndung).

Im Betrugsbereich hat sich folgendes Verfahren bewährt: Nach Möglichkeit, Feststellung der Kommunikationswege und deren Überwachung mit gleichzeitiger konsequenter Verfolgung der Geldspuren. Bei konkreten Ermittlungsansätzen Einsetzung von Teams, bestehend aus IT-Spezialisten, Analysten und erfahrenen Betrugsermittlern.

5.2.2. Forensik und Verschlüsselung

Die österreichischen Behörden haben mitgeteilt, dass bei der Überwachung von Servern die Verschlüsselung nach wie vor ein ungelöstes Problem darstellt. Von Experten wird immer wieder angemerkt, dass die Entschlüsselung sehr aufwendig ist und, wenn überhaupt möglich, voraussichtlich mehrere Jahre dauern würde. Eine Mitwirkung des Betroffenen (Beschuldigten) ist bis dato unvermeidlich. Verschlüsselung stellt bei der forensischen Datensicherung ein immer größer werdendes Problem dar.

Die folgenden Probleme sind im Zusammenhang mit der Verschlüsselung aufgetreten:

Die Betroffenen haben den ganzen oder Teile eines Datenträgers verschlüsselt. Dabei ist in den meisten Fällen eine Kooperationsbereitschaft mit der Behörde nicht gegeben, sodass die Daten nicht entschlüsselt werden können. In der Regel können dann nur verschlüsselte Daten gesichert werden, welche letztendlich aber keiner Auswertung zugeführt werden können. Selbst wenn der Schlüssel bekannt gegeben wird oder bekannt ist, kann meist kein physikalisches Abbild des Datenträgers erstellt werden. Dadurch können u. U. gelöschte Bereiche nur unzureichend gesichert werden. Im Rahmen der Datenübermittlung an kompetente Behörden in diesem Bereich, stellen die Datenmengen im Hinblick auf die für deren Speicherung und Lagerung erforderlichen Ressourcen immer wieder ein größeres Problem dar.

Andererseits konnten in jenen Bereichen, in denen eine sehr einfache Verschlüsselungsmethode eingesetzt wurde, einige Erfolge erzielt werden und mittels geeigneter Software konnte der Schlüssel ermittelt bzw. rückgerechnet werden. Einfache Passwörter lassen sich durch entsprechende Hardware und Tools "knacken".

Den österreichischen Behörden zufolge ist eine Zusammenarbeit zwischen den einzelnen Behörden unabdingbar, da sich nicht jede Dienststelle oder Behörde die sehr kostenintensive Hard- und Software im Bereich der Password-Recovery-Technologien leisten kann. Die Kompetenzverteilung innerhalb der Behörden sorgt dabei für Einsparungen, also auch für mehr Möglichkeiten in diesem Bereich. In Österreich ist das Bundeskriminalamt mit dem Cyber Crime Competence Centre (C4) durchaus als spezialisierte Einrichtung anzusehen. Aber auch spezielle Abteilungen innerhalb der Landesverteidigung können derartige Kompetenzen aufweisen. Generell werden in diesem Bereich aber auch Dienststellen wie Europol und Interpol als Kompetenzansprechstelle genutzt. Auf private Unternehmen wird aus rechtlichen Gründen nur über staatsanwaltschaftlichen Auftrag zugegriffen.

5.2.3. Elektronische Beweismittel

Im österreichischen Recht besteht keine spezielle Definition elektronischer Beweise bzw. keine Regelung deren Einstufung. Die Sicherung elektronischer Beweismittel erfolgt in der Regel als Assistenzdienst für die ermittelnden Organisationseinheiten im Rahmen der Strafprozessordnung (StPO). Als elektronische Beweismittel gelten alle elektronischen Daten, die im Rahmen von gerichtlichen Erhebungen relevant sein könnten. Gespeichert werden Beweismittel nur im Auftrag durch die Staatsanwaltschaft. Wurde ein derartiger Auftrag erteilt, wird eine Datensicherung und Auswertung nach den internationalen Standards durchgeführt. Die Ergebnisse werden an die ermittlungsführende Dienststelle übermittelt, welche für die Weiterleitung an die Staatsanwaltschaft zuständig ist.

Es existieren keine speziellen Zulässigkeitsvorschriften für elektronische Beweise. Sie sind daher uneingeschränkt zulässig und unterliegen der freien Beweiswürdigung. Es gelten keine anderen Zulässigkeitsvorschriften, wenn die elektronischen Beweise in einem anderen Staat erhoben werden.

5.3. Schutz der Menschenrechte/Grundfreiheiten

Jede von Zwang begleitete Ermittlungsmaßnahme ist mit einer Beeinträchtigung von Grundrechten und -freiheiten Betroffener verbunden. Daher haben die österreichischen Behörden darauf hingewiesen, dass bei derartigen Eingriffen die Gebote der Verhältnismäßigkeit, des rechtlichen Gehörs, des Rechtes auf Verteidigung, der Unschuldsvermutung und der Entscheidung binnen angemessener Frist ebenso wie die Grundsätze der Mündlichkeit und Öffentlichkeit, Unmittelbarkeit und "in dubio pro reo" zu berücksichtigen sind. Die neuerliche Verfolgung wegen derselben Tat ist unzulässig, die Strafverfolgungsbehörden sind zur Objektivität verpflichtet. Für die Einhaltung dieser Grundsätze leistet ein umfangreiches und effektives Rechtsschutzsystem Gewähr (Zitierungen aus der StPO):

Objektivität und Wahrheitserforschung

Kriminalpolizei, Staatsanwaltschaft und Gericht haben die Wahrheit zu erforschen und alle Tatsachen aufzuklären, die für die Beurteilung der Tat und des Beschuldigten von Bedeutung sind. Alle Richter, Staatsanwälte und kriminalpolizeilichen Organe haben ihr Amt unparteilich und unvoreingenommen auszuüben und jeden Anschein der Befangenheit zu vermeiden. Sie haben die zur Belastung und die zur Verteidigung des Beschuldigten dienenden Umstände mit der gleichen Sorgfalt zu ermitteln (§ 3).

Gesetz- und Verhältnismäßigkeit

Kriminalpolizei, Staatsanwaltschaft und Gericht dürfen bei der Ausübung von Befugnissen und bei der Aufnahme von Beweisen nur soweit in Rechte von Personen eingreifen, als dies gesetzlich ausdrücklich vorgesehen und zur Aufgabenerfüllung erforderlich ist. Jede dadurch bewirkte Rechtsgutbeeinträchtigung muss in einem angemessenen Verhältnis zum Gewicht der Straftat, zum Grad des Verdachts und zum angestrebten Erfolg stehen. Unter mehreren zielführenden Ermittlungshandlungen und Zwangsmaßnahmen haben Kriminalpolizei, Staatsanwaltschaft und Gericht jene zu ergreifen, welche die Rechte der Betroffenen am geringsten beeinträchtigen. Gesetzlich eingeräumte Befugnisse sind in jeder Lage des Verfahrens in einer Art und Weise auszuüben, die unnötiges Aufsehen vermeidet, die Würde der betroffenen Personen achtet und deren Rechte und schutzwürdige Interessen wahrt. Beschuldigte oder andere Personen zur Unternehmung, Fortsetzung oder Vollendung einer Straftat zu verleiten oder durch heimlich bestellte Personen zu einem Geständnis zu verlocken, ist unzulässig (§ 5).

Rechtliches Gehör

Der Beschuldigte hat das Recht, am gesamten Verfahren mitzuwirken, und die Pflicht, während der Hauptverhandlung anwesend zu sein. Er ist mit Achtung seiner persönlichen Würde zu behandeln. Jede am Verfahren beteiligte oder von der Ausübung von Zwangsmaßnahmen betroffene Person hat das Recht auf angemessenes rechtliches Gehör und auf Information über Anlass und Zweck der sie betreffenden Verfahrenshandlung sowie über ihre wesentlichen Rechte im Verfahren. Der Beschuldigte hat das Recht, alle gegen ihn vorliegenden Verdachtsgründe zu erfahren und vollständige Gelegenheit zu deren Beseitigung und zu seiner Rechtfertigung zu erhalten (§ 6).

Recht auf Verteidigung

Der Beschuldigte hat das Recht, sich selbst zu verteidigen und in jeder Lage des Verfahrens den Beistand eines Verteidigers in Anspruch zu nehmen. Der Beschuldigte darf nicht gezwungen werden, sich selbst zu belasten. Es steht ihm jederzeit frei, auszusagen oder die Aussage zu verweigern. Er darf nicht durch Zwangsmittel, Drohungen, Versprechungen oder Vorspiegelungen zu Äußerungen genötigt oder bewogen werden (§ 7).

Unschuldsvermutung

Jede Person gilt bis zu ihrer rechtskräftigen Verurteilung als unschuldig (§ 8).

Beschleunigungsgebot

Jeder Beschuldigte hat Anspruch auf Beendigung des Verfahrens innerhalb angemessener Frist. Das Verfahren ist stets zügig und ohne unnötige Verzögerung durchzuführen. Verfahren, in denen ein Beschuldigter in Haft gehalten wird, sind mit besonderer Beschleunigung zu führen. Jeder verhaftete Beschuldigte hat Anspruch auf ehest mögliche Urteilsfällung oder Enthaftung während des Verfahrens. Alle im Strafverfahren tätigen Behörden, Einrichtungen und Personen sind verpflichtet, auf eine möglichst kurze Dauer der Haft hinzuwirken (§ 9).

Mündlichkeit und Öffentlichkeit

Gerichtliche Verhandlungen im Haupt- und Rechtsmittelverfahren werden mündlich und öffentlich durchgeführt. Das Ermittlungsverfahren ist nicht öffentlich. Das Gericht hat bei der Urteilsfällung nur auf das Rücksicht zu nehmen, was in der Hauptverhandlung vorgekommen ist (§ 12).

Unmittelbarkeit

Die Hauptverhandlung bildet den Schwerpunkt des Verfahrens. In ihr sind die Beweise aufzunehmen, aufgrund deren das Urteil zu fällen ist. Im Ermittlungsverfahren sind die Beweise aufzunehmen, die für die Entscheidung über die Erhebung der Anklage unerlässlich sind oder deren Aufnahme in der Hauptverhandlung aus tatsächlichen oder rechtlichen Gründen voraussichtlich nicht möglich sein wird. Soweit ein Beweis unmittelbar aufgenommen werden kann, darf er nicht durch einen mittelbaren ersetzt werden. Der Inhalt von Akten und anderen Schriftstücken darf nur soweit als Beweis verwertet werden, als er in einer nach diesem Gesetz zulässigen Weise wiedergegeben wird (§ 13).

Freie Beweiswürdigung

Ob Tatsachen als erwiesen festzustellen sind, hat das Gericht aufgrund der Beweise nach freier Überzeugung zu entscheiden; im Zweifel stets zu Gunsten des Angeklagten oder sonst in seinen Rechten Betroffenen (§ 14).

Verbot wiederholter Strafverfolgung

Nach rechtswirksamer Beendigung eines Strafverfahrens ist die neuerliche Verfolgung desselben Verdächtigen wegen derselben Tat unzulässig. Die Bestimmungen über die Fortsetzung, die Fortführung, die Wiederaufnahme und die Erneuerung des Strafverfahrens sowie über die Nichtigkeitsbeschwerde zur Wahrung des Gesetzes bleiben hiervon unberührt (§ 17).

5.4. Gerichtliche Zuständigkeit

5.4.1. Grundsätze für die Ermittlungen bei Cyberkriminalität

Die österreichischen Strafgesetze gelten für alle Taten, die im Inland begangen worden sind.
Für andere als die in den §§ 63 und 64 bezeichneten Taten, die im Ausland begangen worden sind, gelten, sofern die Taten auch durch die Gesetze des Tatorts mit Strafe bedroht sind, die österreichischen Strafgesetze, wenn

1. der Täter zur Zeit der Tat Österreicher war oder wenn er die österreichische Staatsbürgerschaft später erworben hat und zur Zeit der Einleitung des Strafverfahrens noch besitzt;
2. der Täter zur Zeit der Tat Ausländer war, im Inland betreten wird und aus einem anderen Grund als wegen der Art oder Eigenschaft seiner Tat nicht an das Ausland ausgeliefert werden kann.

Eine mit Strafe bedrohte Handlung hat der Täter zu der Zeit begangen, da er gehandelt hat oder hätte handeln sollen; wann der Erfolg eintritt, ist nicht maßgebend. Eine mit Strafe bedrohte Handlung hat der Täter an jedem Ort begangen, an dem er gehandelt hat oder hätte handeln sollen oder ein dem Tatbild entsprechender Erfolg ganz oder zum Teil eingetreten ist oder nach der Vorstellung des Täters hätte eintreten sollen.

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

Der Rahmenbeschluss 2009/948/JI vom 30. November 2009 zur Vermeidung und Beilegung von Kompetenzkonflikten in Strafverfahren wurde von Österreich durch die §§ 59a bis 59c des Bundesgesetzes über die justizielle Zusammenarbeit in Strafsachen mit den Mitgliedstaaten der EU (EU-JZG) umgesetzt.

Österreich hat keine praktischen Erfahrungen mit Kompetenzkonflikten in Strafsachen wegen Cyberstraftaten, die österreichischen Strafverfolgungsbehörden machen jedoch auch von dem Instrument der Übertragung der Strafverfolgung bei Cyberstraftaten Gebrauch, sofern die tatverdächtige Person sich dauerhaft im Ausland aufhält und eine Strafverfolgung dort effektiver erfolgen kann. Wird die Strafverfolgung vom ersuchten Staat übernommen, hat das inländische Verfahren bis zur Mitteilung des Ergebnisses auf sich zu beruhen. Erfolgt im Ausland eine rechtskräftige Verurteilung, so ist das inländische Verfahren einzustellen, sofern die Strafe zur Gänze vollstreckt oder erlassen worden ist (§ 74 Abs. 4 ARHG).

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

Es gilt, einen entsprechenden Link, d. h. Zugang zu den Daten in einer Cloud, zu finden. Tatsächlich werden bei Sicherstellungen Links zu solchen gespeicherten Daten (Dropbox, Sendspace, u. a.) gefunden, die dann entsprechend heruntergeladen und gesichert werden. Dazu ist aber immer eine Anordnung der StA erforderlich. Die Probleme bestehen in der Praxis dadurch, dass solche Daten mit Passwort geschützt oder überhaupt verschlüsselt sind. Ohne Mitwirkung des Betroffenen ist in solchen Fällen ein Zugang nicht möglich.

Ein weiteres Problem ist, dass im Rechtshilfeverfahren mit langen Wartezeiten zu rechnen ist. In der Cloud gespeicherte Daten stellen immer wieder Probleme dar. Je nach Datenmenge und Übertragungsrate ist es nicht immer möglich, eine vollständige forensische Sicherung des Cloud-Speichers durchzuführen. Weiteres kann auf entfernte Datenspeicher meist nur logisch zugegriffen werden. Dadurch ist eine physikalische Sicherung so gut wie unmöglich, wodurch gelöschte Bereiche odgl. von einer Sicherung nicht umfasst werden können.
Ein großes Problem stellt immer wieder der zeitliche Faktor der Auswertungen dar. Meist liegt die Gültigkeit der gesuchten Daten weit unter der Zeitspanne, die notwendig ist, um sie zu finden. Besonders in der Malware-Analyse stellt dies immer wieder ein Problem dar. Die Datenmengen in diesem Bereich werden immer problematischer. Datenmengen in Terabyte-Bereich führen zu lange Auswertezeiten, was sich letztendlich wieder auf die Aktualität der Daten auswirkt.
Versteckte Dienste im Darknet stellen bei der Verfolgung immer wieder dahingehend Probleme dar, dass die technischen Möglichkeiten aufgrund der rechtlichen Rahmenbedingungen meist nicht eingesetzt werden können.

5.4.4. Auffassung Österreichs zum Rechtsrahmen zur Bekämpfung der Cyberkriminalität

Die österreichischen Behörden haben darauf hingewiesen, dass das Medium Internet ein sehr schnelllebiges Instrument ist, das schnelle polizeiliche Reaktionen erfordert. Die Identifizierung des Users ist aber aufgrund der bestehenden Rechtsnormen zum überwiegenden Teil nur mit justiziellen Rechtshilfeersuchen möglich. Die Zeitdauer der Erledigung dieser Rechtshilfeersuchen führt zu Zeitverlusten, die oft für die Aufklärung von entscheidender Bedeutung sind. Darüber hinaus führen nationale und internationale Ermittlungen aufgrund fehlender Speicherverpflichtungen (Vorratsdatenspeicherung) zu negativen Ergebnissen. Grundlegende Auskünfte über IP-Adressen und Informationen von Betroffenen wie etwa ein Auszug aus dem Headerprotokoll müssen auf dem schnellen Weg des internationalen Informationsaustausches (Amtshilfe) beschafft werden können. Leider wird hier oft auf den justiziellen Rechtshilfeweg verwiesen.

5.5. Fazit

- Österreich hat das Übereinkommen von Budapest ratifiziert. Der Rahmenbeschluss 2005/222/JI des Rates über Angriffe auf Informationssysteme wurde in österreichisches Recht umgesetzt. Die Richtlinie 2013/40/EU über Angriffe auf Informationssysteme und zur Aufhebung des Rahmenbeschlusses 2005/222/JI des Rates wurde mit dem Strafrechtsänderungsgesetz 2015 umgesetzt. Die in dem Übereinkommen und in den europäischen Rechtsvorschriften vorgesehenen Straftatbestände bestehen im nationalen Recht.

- Widerrechtlicher Zugriff auf ein Computersystem (§ 118a StGB) und missbräuchliches Abfangen von Daten (§ 119a StGB) werden nur mit Ermächtigung des Verletzten verfolgt. Dabei handelt es sich zwar um allgemeine Anforderungen, die nicht spezifisch für den rechtlichen Rahmen Österreichs sind, doch war der Gutachterausschuss der Auffassung, dass diese Anforderung zu Schwierigkeiten bei Cyberstraftaten führen kann, da die Zahl der möglichen Opfer in einem einzigen Fall bei Massendatenlecks oder anderen größeren Vorfällen für gewöhnlich sehr hoch ist, was bei der Ermittlung mit verwaltungstechnischen Schwierigkeiten einhergehen kann.

- Österreich änderte seine straf- und verwaltungsrechtlichen Vorschriften in kriminalpolizeilichen Angelegenheiten in Bezug auf Cyberkriminalität ab; es wurden Strafen eingeführt und die verschiedenen Arten von kriminellem Verhalten in Bezug auf Cyberkriminalität explizit benannt. Vor dieser Änderung war die Cyberkriminalität unter dem allgemeinen Bereich Betrug subsumiert. Österreich hat jetzt eigene strafrechtliche Bestimmungen in Bezug auf Cyberkriminalität und eigene Bestimmungen des Strafprozessrechts zur Regelung von Ermittlungsmaßnahmen im Bereich Cyberkriminalität zum Zweck der Erhebung von Informationen und der Sammlung von Beweismaterial von Internetdiensteanbietern. Infolgedessen hat Österreich strafrechtliche Vorschriften eingeführt, in denen die Verteilung der Zuständigkeiten zwischen allen, die befugt sind, Ermittlungen durchzuführen, und die Ermittlungsmaßnahmen geklärt werden.

- Die Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie wurde umgesetzt. Die Bekämpfung des Kreditkartenbetrugs ist im Strafgesetzbuch geregelt, erfolgt aber auch in Zusammenarbeit mit dem Privatsektor.

- Die österreichische Privatwirtschaft ist nicht zur Speicherung und Bereitstellung von Datenmaterial für polizeiliche Zwecke verpflichtet. Das ist besorgniserregend, wenn man bedenkt, dass möglicherweise Leben gerettet und Misshandlungen (sexueller Missbrauch von Kindern) verhindert werden könnten, was gemäß Artikel 2 und 3 der Europäischen Menschenrechtskonvention absolute Rechte sind – im Gegensatz zum Recht auf Schutz der Privatsphäre, das gemäß Artikel 8 der EMRK ein qualifiziertes Recht ist.

- Telekommunikationsdaten werden von Anbietern, beispielsweise zu Abrechnungszwecken, für einen Zeitraum von drei Monaten gespeichert. Die Tatsache, dass nach der Nichtigerklärung der Richtlinie 2006/24/EG kein europäisches Rechtsinstrument zur Regelung dieser Frage vorliegt, scheint in der gesamten EU ein Problem zu sein. Nach Auffassung der Gutachter kann dies Auswirkungen auf strafrechtliche Ermittlungen haben, und Österreich ist hier keine Ausnahme. Offensichtlich ist die Zivilgesellschaft in dieser Frage gespalten, da es aus geschichtlichen Gründen starken Widerstand gegen den Zugriff von Polizei und anderen Behörden auf den Datenverkehr gibt. Es könnte jedoch sinnvoll sein, die Debatte in der Zivilgesellschaft stärker anzustoßen, sodass der Zugriff auf den Datenverkehr als Notwendigkeit für die österreichischen Behörden und als Beitrag zu den Ermittlungen in anderen Ländern bei der weltweiten Bekämpfung von Cyberkriminalität verstanden werden kann.

- Die österreichischen Staatsanwälte haben darauf hingewiesen, dass sie sich bislang zwar noch nicht mit der Bitcoin-Frage auseinandergesetzt haben, sie jedoch der Meinung sind, dass die Suche nach Bitcoin-Vermögenswerten und deren Sicherstellung nach ihren Rechtsvorschriften möglich ist.

- Elektronische Beweismittel werden in den nationalen Rechtsvorschriften nicht definiert, sodass die allgemeinen Bestimmungen auch für diese Art von Beweismitteln gelten. Verschlüsselung wird als Herausforderung betrachtet und gilt als ungelöstes Problem bei der Überwachung von Servern. Zudem wurde von den befragten Experten immer wieder angemerkt, dass die Entschlüsselung sehr aufwendig ist und, wenn überhaupt möglich, voraussichtlich mehrere Jahre dauern würde. Eine Mitwirkung des Betroffenen (Beschuldigten) ist bis dato unvermeidlich. Verschlüsselung stellt bei der forensischen Datensicherung ein immer größer werdendes Problem dar. Der Gutachterausschuss wurde informiert, dass es keine Rechtsvorschriften gibt, nach denen Strafermittler Zugang zu fortschrittlichen Methoden der Beweisaufnahme wie etwa ferngesteuerte forensische Untersuchungen haben.

- In Bezug auf die gerichtliche Zuständigkeit Österreichs gibt es keine Sonderbestimmungen für Cyberkriminalität. Sollte es zu Zuständigkeitskonflikten kommen, so würden die Bestimmungen gelten, die auf der Grundlage des Rahmenbeschlusses 2009/948/JI des Rates vom 30. November 2009 zur Vermeidung und Beilegung von Kompetenzkonflikten in Strafverfahren in österreichisches Recht umgesetzt wurden.

6. OPERATIVE ASPEKTE

6.1. Cyberangriffe

6.1.1. Art der Cyberangriffe

Die Art und Anzahl von Cyberangriffen ergibt sich aus der folgenden Statistik:

Gemeldete Fälle	2013	2014	Abweichung
Cyberkriminalität im engeren Sinn	1 737	1 754	1,0 %
Cyberkriminalität im weiteren Sinn	8 314	7 212	-13,3 %
Cyberkriminalität gesamt	10 051	8 966	-10. 8 %

Abgeschlossene Fälle	2013	2014	Abweichung
Cyberkriminalität im engeren Sinn	310	316	1,9 %
Cyberkriminalität im weiteren Sinn	4 234	3 344	-21,0 %
Cyberkriminalität gesamt	4 544	3 660	-19,5 %

Abschlussquote	2013	2014	Abweichung
Cyberkriminalität im engeren Sinn	17,8 %	18,0 %	0,2
Cyberkriminalität im weiteren Sinn	50,9 %	46,4 %	-4,6
Cyberkriminalität gesamt	45,2 %	40,8 %	-4,4

Identifizierte Verdächtige	2013	2014	Abweichung
Cyberkriminalität im engeren Sinn	334	326	-2,4 %
Cyberkriminalität im weiteren Sinn	3 621	3 278	-9,5 %
Cyberkriminalität gesamt	3 955	3 604	-8,9 %

6.1.2. Mechanismen zur Abwehr von Cyberangriffen

Österreich ist dabei, seine Widerstandsfähigkeit gegenüber Cyberangriffen zu stärken. Im Zuge der Umsetzung der Österreichischen Strategie für Cyber-Sicherheit befindet sich ein "Cyber-Krisenmechanismus" (CKM) im Aufbau, der in den Staatlichen Krisen- und Katastrophenschutzmechanismus (SKKM) integriert werden soll.

Österreich verfügt nach eigenen Angaben über leistungsfähige Infrastrukturen, die einen hohen Grad an Sicherheit in Bezug auf die Lebensmittelversorgung, Verkehrs-, Telekommunikations-, Energie- und Finanzdienstleistungen wie auch eine gesicherte Versorgung mit Sozial- und Gesundheitsdienstleistungen gewährleisten können. Sowohl die Daseinsvorsorge für die Bevölkerung als auch die Attraktivität des Wirtschaftsstandortes beruhen auf der ständigen Verfügbarkeit und dem reibungslosen Funktionieren vielfältiger Infrastrukturen. Das ordnungsgemäße Funktionieren der Infrastrukturen ist daher zunehmend von Bedeutung.

Zu diesem Zweck hat die Bundesregierung auf der Grundlage des Programms zum Schutz kritischer Infrastrukturen aus dem Jahr 2008 am 4. November 2014 einen neuen Masterplan beschlossen. Der Masterplan APCIP 2014 dokumentiert die bereits abgeschlossenen Arbeiten und entwickelt den bisherigen Masterplan auf Basis der Erkenntnisse der letzten Jahre weiter. Der Masterplan wurde von BKA und BM.I gemeinsam erarbeitet und mit den relevanten Ressorts, Bundesländern, Interessenvertretungen und ausgewählten strategischen Unternehmen akkordiert. Der Masterplan APCIP baut auf den Prinzipien Kooperation, Subsidiarität, Komplementarität, Vertraulichkeit und Verhältnismäßigkeit auf und basiert auf einem All-hazards-Ansatz. Wesentlicher Schwerpunkt des Masterplans ist die Unterstützung von strategischen Unternehmen beim Aufbau einer umfassenden Sicherheitsarchitektur (Risikomanagement, Business Continuity Management und Sicherheitsmanagement). Dadurch wird die Resilienz und Sicherheit Österreichs gestärkt. Die Betreiber der kritischen Infrastrukturen sind zudem angehalten, ihre Anlagen auch in puncto Cybersicherheit am Stand der Technik zu halten.

Im nationalen Programm zum Schutz kritischer Infrastrukturen (Grundlage ist das Europäische Programm zum Schutz kritischer Infrastrukturen (EPCIP)) wurde festgelegt, dass Betreiber strategisch wichtiger Infrastrukturen in Zusammenarbeit mit den Behörden ausreichende und angemessene Schutzmaßnahmen implementieren sollen. Dabei handelt es sich um eine öffentlich-private Partnerschaft, gesetzliche Verpflichtungen wurden nicht vorgesehen. Es gibt – neben allfälligen Zertifizierungen, bspw. ISO 27.001 – ebenso keine allgemein gültigen Vorgaben für alle Sektoren der kritischen Infrastrukturen. Ein Problem stellt die Unmöglichkeit dar, ein großes Datenvolumen zu analysieren; darüber hinaus gibt es langwierige Verfahren, unterschiedliche Datenspeicherfristen, Sicherung von Beweismitteln, begrenzte Kenntnisse, Fähigkeiten bzw. Kompetenzen.

Im Grunde gibt es keine gesetzliche Meldepflicht für mutmaßliche Cyberangriffe auf kritische Infrastrukturen. Folglich kann der Diensteanbieter nur dann haftbar gemacht werden, wenn der Rechteinhaber auf die Rechtsverletzung hingewiesen hat und diese auch für einen juristischen Laien ohne weitere Nachforschungen offenkundig ist. Basierend auf die Vorgaben der E-Commerce-Richtlinie 2000/31/EG ist das Haftungsregime für die österreichischen Provider im E-Commerce-Gesetz geregelt. Darin sind alle Fälle aufgeführt, in denen Diensteanbieter von der Haftung befreit sind. Dies gilt für die folgenden Fälle:

1) Ein Access-Anbieter ist für die über seine Netze übermittelten Informationen nicht verantwortlich, sofern die Übermittlung nicht vom Provider veranlasst wurde, er also nicht selbst die Ausführung der Übermittlung beschlossen hat (§ 13 ECG). Grundsätzliche Voraussetzung für die Haftungsbefreiung ist, dass die übermittelten Informationen vom Nutzer des Dienstes und nicht vom Provider eingegeben werden.

2) Ein Diensteanbieter, der Nutzern eine Suchmaschine oder andere elektronische Hilfsmittel zur Suche nach fremden Informationen bereitstellt, ist für die abgefragten Informationen nicht verantwortlich, sofern er die Übermittlung der abgefragten Informationen nicht veranlasst, den Empfänger der abgefragten Informationen nicht auswählt und die abgefragten Informationen weder auswählt noch verändert (§ 14 ECG).

3) Ein Diensteanbieter, der von einem Nutzer eingegebene Informationen in einem Kommunikationsnetz übermittelt, ist für eine automatische, zeitlich begrenzte Zwischenspeicherung, die nur der effizienteren Gestaltung der auf Abruf anderer Nutzer erfolgenden Informationsübermittlung dient, nicht verantwortlich, sofern er die Information nicht verändert, die Bedingungen für den Zugang zur Information beachtet, die Regeln für die Aktualisierung der Information, die in allgemein anerkannten und verwendeten Industriestandards festgelegt sind, beachtet, die zulässige Anwendung von Technologien zur Sammlung von Daten über die Nutzung der Information, die in allgemein anerkannten und verwendeten Industriestandards festgelegt sind, nicht beeinträchtigt und unverzüglich eine von ihm gespeicherte Information entfernt oder den Zugang zu ihr sperrt, sobald er tatsächliche Kenntnis davon erhalten hat, dass die Information am ursprünglichen Ausgangsort der Übertragung aus dem Netz entfernt oder der Zugang zu ihr gesperrt wurde oder dass ein Gericht oder eine Verwaltungsbehörde die Entfernung oder Sperre angeordnet hat (§ 15 ECG).
4) Der Hosting-Provider ist nicht verantwortlich, wenn er von einem Nutzer eingegebene rechtswidrige Informationen speichert, vorausgesetzt, er hat keine tatsächliche Kenntnis von der rechtswidrigen Tätigkeit oder Information. Ferner darf sich der Provider in Bezug auf Schadenersatzansprüche auch keiner Tatsachen oder Umstände bewusst sein, aus denen eine rechtswidrige Tätigkeit oder Information offensichtlich wird. Diese Haftungsfreistellung greift nur, wenn der Provider, sobald er Kenntnis von rechtswidrigen Informationen erlangt, sofort tätig wird, um die Information zu entfernen oder den Zugang zu ihr zu sperren (§ 16 ECG).
5) Ein Diensteanbieter, der mittels eines elektronischen Verweises einen Zugang zu fremden Informationen eröffnet, ist für diese Informationen nicht verantwortlich, sofern er von einer rechtswidrigen Tätigkeit oder Information keine tatsächliche Kenntnis hat und sich in Bezug auf Schadenersatzansprüche auch keiner Tatsachen oder Umstände bewusst ist, aus denen eine rechtswidrige Tätigkeit oder Information offensichtlich wird, oder, sobald er diese Kenntnis oder dieses Bewusstsein erlangt hat, unverzüglich tätig wird, um den elektronischen Verweis zu entfernen (§ 17 ECG).

Allerdings judizieren die österreichischen Gerichte eine Verantwortlichkeit des (Host-)Providers für die Verbreitung von Persönlichkeitsrechte verletzenden Inhalten, die zu einem Unterlassungs- und einem Beseitigungsanspruch in Zivilsachen berechtigt. Dabei muss der Hostprovider den Sachverhalt kennen, der den Vorwurf gesetzwidrigen Verhaltens begründet, oder eine Prüfpflicht verletzen; diese ist allerdings auf grobe und auffallende Verstöße beschränkt.

Der Oberste Gerichtshof hat in zwei neueren Entscheidungen (4 Ob 71/14s und 4 Ob 22/15) festgehalten, dass Access-Provider den Zugang zu Websites sperren müssen, wenn diese überwiegend illegale Kopien von urheberrechtlich geschütztem Material verbreiten. Dieser Judikatur liegt eine Vorabentscheidung des Europäischen Gerichtshofs zu Art. 8 Abs. 3 der Richtlinie 2001/29/EG zugrunde: Der Europäische Gerichtshof hat in der Entscheidung in der Rechtssache C-314/12, UPC Telekabel ("kino.to") ausgesprochen, dass nach europäischem Recht Access-Provider unter gewissen Voraussetzungen verpflichtet sind, ihren Kunden den Zugriff auf Internetangebote mit rechtsverletzenden Inhalten zu verwehren.

Bis dato haben sämtliche Anbieter die geforderten Sperrmaßnahmen erst umgesetzt, nachdem sie im Wege einer einstweiligen Verfügung dazu verpflichtet wurden. Aufgrund der kino.to-Entscheidung enthalten die einstweiligen Verfügungen keine Angaben darüber, welche Art von Sperre vom Provider eingesetzt werden muss. Bei den aktuell durchgeführten Netzsperren handelt es sich um DNS-Sperren. Die österreichischen Behörden prüfen gerade, ob eine DNS-Sperre eine ausreichende Maßnahme darstellt, um den Zugang der Kunden eines Access-Anbieters zu rechtsverletzten Seiten zu verhindern.

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

In Österreich gibt es keine spezielle Datenbank-Software zum Ausfindigmachen von Opfern. Die Identifizierung von Tätern und Opfern erfolgt durch die ICSE (Datenbank, betrieben von INTERPOL). Darüber hinaus besteht bei der Opferidentifizierung eine sehr enge internationale Zusammenarbeit. An einer nationalen Datenbank zur Opferidentifizierung wird in Kooperation mit deutschen Behörden gerade gearbeitet.

Maßnahmen zur Verhinderung der erneuten Viktimisierung erfolgen hauptsächlich durch die Beratung und Betreuung der Opfer durch NGO (z. B. Weißer Ring etc.). Weiters wird wieder auf das Projekt "Click & Check" verwiesen.

In österreichischen Gerichtsverfahren werden minderjährige Zeugen/Opfer von Psychologen befragt, wobei der Verdächtige und sein Verteidiger nicht anwesend sind; sie können allerdings über den Richter erwirken, dass die Befragung fortgesetzt wird und bestimmte Fragen gestellt werden.

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

Am 1. Januar 2016 wurde mit dem Strafrechtsänderungsgesetz 2015 (BGBl. I Nr. 112/2015) der Straftatbestand der "Fortgesetzten Belästigung im Wege einer Telekommunikation oder eines Computersystems" einschließlich Cyber-Mobbing eingeführt; dieser Straftatbestand ist definiert als Handlung, die eine Person in ihrer Lebensführung unzumutbar beeinträchtigt und/oder eine Person für eine größere Zahl von Menschen wahrnehmbar an der Ehre verletzt oder Tatsachen oder Bildaufnahmen des höchstpersönlichen Lebensbereiches einer Person ohne deren Zustimmung für eine größere Zahl von Menschen wahrnehmbar macht.

Nach geltender Rechtslage stellt die Aufnahme von Nacktfotos keine Ehrverletzung dar, sodass dies nicht unter den Tatbestand der gefährlichen Drohung nach § 107 StGB subsumiert werden kann. Im Falle der Veröffentlichung von Nacktfotos liegt nach der Rechtsprechung dann eine Verletzung an der Ehre vor, wenn diese vom Opfer nicht gewollt und die Androhung damit verbunden ist, dem Opfer die gebotene achtungsvolle Behandlung zu verweigern und so sein Ansehen in der Öffentlichkeit herabzusetzen. Die Definition von "gefährliche Drohung" wurde letzthin um die Drohung mit der Bekanntgabe von Tatsachen oder der Zugänglichmachung von Bildaufnahmen des höchstpersönlichen Lebensbereiches wie folgt erweitert:
§ 74 Abs. 1 Z 5: "gefährliche Drohung: eine Drohung mit einer Verletzung an Körper, Freiheit, Ehre, Vermögen oder des höchstpersönlichen Lebensbereiches durch Zugänglichmachen, Bekanntgeben oder Veröffentlichen von Tatsachen oder Bildaufnahmen, die geeignet ist, dem Bedrohten mit Rücksicht auf die Verhältnisse und seine persönliche Beschaffenheit oder die Wichtigkeit des angedrohten Übels begründete Besorgnisse einzuflößen, ohne Unterschied, ob das angedrohte Übel gegen den Bedrohten selbst, gegen dessen Angehörige oder gegen andere unter seinen Schutz gestellte oder ihm persönlich nahestehende Personen gerichtet ist".

Darüber hinaus besteht zwischen dem österreichischen Bundeskriminalamt (.BK) und den heimischen Internetdienstanbietern eine enge Kooperation. Im Fall eines Missbrauches eines dieser Dienste kommt es zu einem raschen Datentransfer an das .BK, damit dieses entsprechende Ermittlungen zur Ausforschung der Verdächtigen einleiten kann. Das inkriminierte Bild- oder Videomaterial wird nach erfolgter Sicherstellung von den jeweiligen Anbietern entfernt.

Hierzu darf auf die enge Zusammenarbeit mit der privaten Meldestelle "STOPLINE" verwiesen werden, die zu einem merklichen Rückgang der im Internet abrufbaren Webseiten mit Darstellungen des Kindesmissbrauches führte.

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

Es sind Legislativmaßnahmen gegen die Werbung für Gelegenheiten zum Missbrauch und Kindersextourismus in Kraft, die die folgenden Tatbestände/Zuständigkeitsvorschriften des StGB umfassen:

- Ankündigung zur Herbeiführung unzüchtigen Verkehrs (eine Ankündigung, die bestimmt ist, unzüchtigen Verkehr herbeizuführen, und die nach ihrem Inhalt geeignet ist, berechtigtes Ärgernis zu erregen – § 219)
- Aufforderung zu mit Strafe bedrohten Handlungen und Gutheißung mit Strafe bedrohter Handlungen (eine Aufforderung zu einer mit Strafe bedrohten Handlung in einem Druckwerk, im Rundfunk oder sonst auf eine Weise, dass es einer breiten Öffentlichkeit zugänglich wird – § 282)

- Strafbare Handlungen im Ausland, die ohne Rücksicht auf die Gesetze des Tatorts bestraft werden (§ 64), wie etwa:

Genitalverstümmelung im Sinne von § 90 Abs. 3, erpresserische Entführung (§ 102), Überlieferung an eine ausländische Macht (§ 103), Sklavenhandel (§ 104), Menschenhandel (§ 104a), schwere Nötigung nach § 106 Abs. 1 Z 3, verbotene Adoptionsvermittlung (§ 194), Vergewaltigung (§ 201), geschlechtliche Nötigung (§ 202), sexueller Missbrauch einer wehrlosen oder psychisch beeinträchtigten Person (§ 205), schwerer sexueller Missbrauch von Unmündigen (§ 206), sexueller Missbrauch von Unmündigen (§ 207), pornografische Darstellungen Minderjähriger nach § 207a Abs. 1 und 2, sexueller Missbrauch von Jugendlichen (§ 207b), Missbrauch eines Autoritätsverhältnisses nach § 212 Abs. 1, Förderung der Prostitution und pornografischer Darbietungen Minderjähriger (§ 215a), grenzüberschreitender Prostitutionshandel (§ 217), wenn

a) der Täter oder das Opfer Österreicher ist oder seinen gewöhnlichen Aufenthalt im Inland hat,

b) durch die Tat sonstige österreichische Interessen verletzt worden sind oder

c) der Täter zur Zeit der Tat Ausländer war, sich in Österreich aufhält und nicht ausgeliefert werden kann.

Zudem wurde die Meldestelle für Kinderpornografie im Bundeskriminalamt um den Aspekt Kindersextourismus erweitert, damit Hinweise zu derartigen Straftaten erlangt werden, und ein Verbindungsbeamter des BM.I für Südostasien wurde nach Bangkok entsandt.

Durch das bestehende Projekt "Click & Check", welches für die Zielgruppe der 12- bis 14-Jährigen an Schulen und Jugendeinrichtungen umgesetzt wird, wird auch auf die Gefahr von Cyber-Grooming und die Anbahnung von strafbaren Handlungen in Chatrooms, sozialen Netzwerken und Foren hingewiesen. Allerdings besteht kein Zugriff der nationalen Behörden, wenn sich die Provider, die pornografische Darbietungen von Kindern in Echtzeit anbieten, außerhalb Österreichs befinden.

Als Präventionsmaßnahme gegen Sextourismus wurde beispielsweise eine Meldestelle für Kinderpornografie und Sextourismus (meldestelle@interpol.at) eingerichtet,

- die Informationshilfen für Kinder für die sichere Nutzung des Internets entwickelt und
- die Informationshilfen über schädliches bzw. unrechtmäßiges Verhalten im Internet entwickelt.

Zudem werden Informationsfolder zu speziellen Deliktsbereichen wie Cyber-Grooming, aber auch zu sonstigen Gefahren im Internet mit allgemeinen Tipps für Kinder, Eltern, Lehrer und Bezugspersonen erstellt. Des Weiteren wird mit dem Projekt "Click & Check" zur Bewusstseinsbildung im Umgang mit dem Internet beigetragen. Darüber hinaus wird im Rahmen der Präventionsarbeit besonderes Augenmerk auf das Thema "Sexting" und die damit verbundenen Gefahren gelegt. Eine wichtige Rolle fällt in diesem Bereich auch den in Österreich tätigen NGOs zu.

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

Im Rahmen der Vorgaben der §§ 13 bis 17 des Bundesgesetzes, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden (E-Commerce-Gesetz – ECG), BGBl. I Nr. 152/2001, ergibt sich eine Verpflichtung zur Löschung illegaler Inhalte auf Webseiten. Eine gesetzliche Möglichkeit, konkrete Internetseiten generell zu blockieren, besteht nicht. Unbeschadet dessen kann sich ein Verbot, bestimmte Inhalte im Internet zu verbreiten, aber aus einzelnen gesetzlichen Bestimmungen ergeben, so beispielsweise hinsichtlich der Verbreitung pornografischer Darstellungen Minderjähriger (§ 207a StGB) oder aus dem Verbotsgesetz 1947. Weiters besteht aufgrund der Judikatur des Europäischen Gerichtshofs zu Art. 8 Abs. 3 der Richtlinie 2001/29/EG (Rechtssache C-314/12, UPC Telekabel) ein zivilrechtlicher Anspruch von Rechteinhabern gegen Access-Provider darauf, dass Letztere ihren Kunden den Zugriff auf Internetangebote mit strukturell urheberrechtsverletzenden Inhalten verwehren. Außerdem gibt es keine Rechtsgrundlage für die Filterung von Websites nach kinderpornografischem Material.

Die Staatsanwaltschaft (§ 110 Abs. 3) kann die Sicherstellung von Servern anordnen bzw. durchführen. Die sichergestellten Server können vom Gericht auf Antrag der Staatsanwaltschaft beschlagnahmt werden (§§ 115 ff. StPO).

Es gibt zwar keine Rechtsgrundlage für die Sperre des Zugangs zum Internet, doch der Privatsektor ist in den folgenden Fällen verpflichtet, den Inhalt zu entfernen:

a) Nationale Vorgehensweise: Wenn ein Strafverfahren anhängig ist, dann wird der Host oder Provider aufgefordert, die betreffende Website mit schädlichem oder illegalem Inhalt vom Netz zu nehmen. In der Praxis reicht es in der Regel, den Provider darauf aufmerksam zu machen, dass von ihm im Netz online gehaltene Webseiten gegen die eigenen Firmenrichtlinien /-standards verstoßen. Die Gutachter stellten fest, dass notfalls das Herunternehmen von Websites auch mit richterlichem Befehl erzwungen werden kann.

b) Internationale Vorgehensweise: Ein Strafverfahren ist erforderlich, um ein internationales Rechtshilfeersuchen zu beantragen und dann über die betreffende Justiz im Ausland an den dort tätigen Provider zu übermitteln. Unmittelbare Zwangsmaßnahmen sind im Ausland nicht vorgesehen; diese können nur gemäß den nationalen Rechtsnormen von Seiten der heimischen Justiz- und Sicherheitsbehörden vorgenommen werden.

Im Büro 3.2 des Bundeskriminalamtes ist im Referat 3.2.1 (Gewaltdelikte) ein Fachbereich für die Bekämpfung der Kinderpornografie eingerichtet. Dieser Bereich besteht derzeit aus zwei Ermittlern.

Die ISPA betreibt die Stopline, die österreichische Meldestelle gegen Kinderpornografie und Nationalsozialismus im Internet. Die Stopline ist die Meldestelle im Internet, an die sich Internetnutzerinnen und -nutzer – auch anonym – einfach und unbürokratisch wenden können, wenn sie im Internet auf Webseiten mit folgenden Inhalten stoßen:

- Kinderpornografie gemäß § 207a StGB oder
- Nationalsozialismus gemäß dem österreichischen Verbots- und Abzeichengesetz u. a.

Nach Eingang ihrer Meldung bei Stopline überprüfen die Mitarbeiter, ob das Material tatsächlich illegal im Sinne der österreichischen Gesetze ist. In diesem Fall wird sofort die zuständige österreichische Exekutive, der betroffene österreichische Provider bzw. die ausländische Partner-Hotline im Rahmen von INHOPE, einem Netzwerk von Hotlines gegen illegale Inhalte im Internet, informiert, um diese Inhalte möglichst schnell zu entfernen. Dabei werden 90 % der illegalen Inhalte europaweit innerhalb von 72 Stunden entfernt.

6.3. Online-Kartenbetrug

Die österreichischen Behörden gaben an, dass Bürger und Privatunternehmen für gewöhnlich Fälle von Online-Kartenbetrug den Strafverfolgungsbehörden melden und eine ausreichende Zusammenarbeit zwischen dem Finanzsektor und den Strafverfolgungsbehörden bei der Verhinderung und Bekämpfung von Online-Kartenbetrug besteht.

Der Gutachterausschuss stellte jedoch fest, dass für die Privatwirtschaft in Österreich keine Meldepflicht gilt. Das Innenministerium teilte mit, dass sich die am 6. Juli 2016 erlassene Richtlinie zur Netz- und Informationssicherheit ("NIS-Richtlinie") auf die Lage in Österreich auswirken wird und dass nach den geplanten inländischen Rechtsvorschriften künftig für bestimmte Stellen eine Meldepflicht gelten wird.

6.4. Fazit

- Das Cyber Security Center (CSC) wird derzeit im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT)/BMI aufgebaut. Vorrangiges Ziel dieses Zentrums ist die Erhöhung der Widerstandsfähigkeit gegen Cyberangriffe durch die operative Koordination von Cybersicherheitsvorfällen (vor allem im Bereich der kritischen Infrastrukturen samt öffentlicher Verwaltung) einerseits sowie durch Präventionsmaßnahmen andererseits (Förderung und Koordinierung von Informationsaustausch, bewusstseinsbildende Maßnahmen, Teilnahme im Bereich der Sicherheitsforschung, technische Analysen, Lagebilder).

- Österreich hat eine Gruppe für Cyber-Krisenmanagement eingesetzt, bei der es sich um eine organisationsübergreifende Gruppe handelt, die sich mit allen Cyber-Notfällen befasst, mit denen Österreich möglicherweise konfrontiert ist.

- Im Allgemeinen sind Betreiber kritischer Infrastrukturen gesetzlich nicht verpflichtet, Cyber-Angriffe der Polizei zu melden. Dem Gutachterausschuss wurde jedoch mitgeteilt, dass sich dies ändern wird, sobald die NIS-Richtlinie umgesetzt worden ist. Nach Auffassung der Gutachter verlangt diese Lage nach weiteren Entwicklungen, da ohne Meldepflicht und Vertrauen in die Strafverfolgung die reale Gefahr besteht, dass die meisten entsprechenden Fälle den Behörden gar nicht erst bekannt werden. Dies kann nicht nur zur Unterlassung ordnungsgemäßer Anzeigen bei den Strafverfolgungsbehörden führen, sondern auch zu einer Fehleinschätzung auf strategischer Ebene, da bestimmte Zwischenfälle möglicherweise nicht statistisch erfasst werden.

- Die Prioritäten des .BK/5.2 C4 – Cybercrime Competence Centre bei der Bekämpfung von Cyberkriminalität orientieren sich an den Strategiezielen des Bundeskriminalamtes (.BK) und umfassen die Ermittlungen bei Cyberstraftaten, die IT-forensische Beweissicherung und eine "Cybercrime"-Meldestelle für die Bevölkerung.

- Die österreichische Polizei verfügt über eine speziell für Kinderpornografie zuständige Sondereinheit, der zwei Mitglieder angehören. Sie verfügt zudem über einen Verbindungsbeamten in Bangkok für Fälle von Kindersextourismus. Darüber hinaus entwickelt Österreich derzeit eine gemeinsame Datenbank mit Deutschland zur Feststellung der Identität der Opfer von Kinderpornografie. Die betreffende Dienststelle, die im Innenministerium (BMI) angesiedelt ist, nimmt an der Kampagne "Gegen das Wegsehen/Don't Look Away!" teil, an der sich sieben europäische Länder (Österreich, Schweiz, Deutschland, Frankreich, Luxemburg, Niederlande und Polen) im Kampf gegen den sexuellen Missbrauch von Kindern im Zusammenhang mit Tourismus beteiligen. Dahin gehend werden auch Vorträge und Schulungen für Hotelmanager von ACCOR u. a. durchgeführt.

- Nach österreichischem Recht werden minderjährige Zeugen/Opfer von Psychologen befragt, wobei der Verdächtige und sein Verteidiger nicht anwesend sind. Die Verteidigung kann allerdings über den Richter an der Anhörung mitwirken und veranlassen, dass dem Zeugen bestimmte Fragen gestellt werden. Den Gutachtern zufolge gibt es anscheinend eine gut entwickelte Regelung zur gleichzeitigen Wahrung der Rechte des Opfers und der Rechte des Beklagten.

- Es gibt keine allgemeine Vorschrift im Strafverfahren, die es den Strafverfolgungsbehörden gestatten würde, Websites, die kinderpornografisches oder nationalsozialistisches oder urheberrechtsverletzendes Material enthalten, zu sperren. In diesen Fällen gibt es einen zivilrechtlichen Anspruch darauf, dass die Anbieter ihren Kunden den Zugang zu den widerrechtlichen Inhalten verweigern.

- Die öffentliche Hand arbeitet mit NRO wie "saferinternet.at" zusammen. Diese NRO hat sich auf die Bekämpfung von Cyber-Mobbing, Schadsoftware, Internet-Betrug und Spam sowie auf Datenschutz spezialisiert. Sie wird von der EU finanziert; ihr Hauptaugenmerk gilt Schulen und der Arbeit mit Minderjährigen sowie mit Eltern und Lehrern. Sie fungiert zugleich als Melde- und als Beratungsstelle. Das Gleiche gilt für das Projekt "Cyber.Kids". Auch das von der ISPA betriebene Projekt "Stopline" als österreichische Meldestelle gegen Kinderpornografie und Nationalsozialismus im Internet sei hier aufgeführt. Nach Auffassung der Gutachter stellt die Art und Weise, wie Behörden und Privatwirtschaft bei der Bekämpfung von Kinderpornografie und Kindesmissbrauch im Internet zusammenarbeiten, ein Beispiel für vorbildliche Praxis dar.

- Der Finanzsektor ist in Österreich nicht zwingend verpflichtet, die Polizei über verdächtiges oder strafbares Verhalten zu unterrichten. Dies lässt Verbesserungen wünschenswert erscheinen, und den Gutachtern zufolge sollten auch mehr verbindlich vorgeschriebene Meldepflichten erwogen werden.

- Beim Besuch vor Ort erhielt der Gutachterausschuss Informationen über die kulturellen und geschichtlichen Gründe, aus denen die österreichische Bevölkerung sehr großen Wert auf den Schutz der Privatsphäre legt. Es wurde erklärt, dass die österreichische Bevölkerung aufgrund der tragischen Geschehnisse im Zweiten Weltkrieg, bei denen die personenbezogenen Daten der Bürger gegen diese verwendet wurden, mit großer Vorsicht reagiert, wenn die Behörden Zugriff auf Daten haben möchten. Als 1997 die Behörden die Systeme eines Telekommunikationsanbieters beschlagnahmten, um an Daten zu gelangen, gab es ein heftiges Aufbegehren in der Gesellschaft. Dies war der Auslöser für die Schaffung des Verbands der Internetdiensteanbieter Österreichs, der versucht, den ersuchenden Behörden so weit wie möglich Auskunft zu geben und gleichzeitig die Privatsphäre der Kunden zu schützen.

- Zur Erleichterung dieses Prozesses hat die österreichische Regierung ein gemeinsames System zur Weitergabe von Daten an die Strafverfolgungsbehörden geschaffen, aber die Zusammenarbeit ist auf die grundlegendsten Bedürfnisse einer Ermittlung beschränkt, die Fristen für die Vorratsdatenspeicherung sind ziemlich kurz und gelegentlich werden die gewünschten Informationen (wie etwa IP-Adressen) aus technischen Gründen (Einsatz des NAT-Verfahrens) nicht in einer gut nutzbaren Form aufbewahrt. Dies führt potenziell zu einer schwierigen Lage in Bezug auf die Identifizierung und Festnahme von Verdächtigen in Fällen von Cyberkriminalität; hier sind Verbesserungen möglich.

7. INTERNATIONALE ZUSAMMENARBEIT

7.1. Zusammenarbeit mit EU-Agenturen

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

In den österreichischen innerstaatlichen Rechtsvorschriften sind keine formellen Anforderungen oder besonderen Verfahren für die Zusammenarbeit zwischen den österreichischen Behörden und Eurojust bei der Ermittlung von Cyberstraftaten vorgesehen. Es finden die allgemeinen Regelungen für die Zusammenarbeit mit Eurojust (§§ 63 bis 68a des Bundesgesetzes über die justizielle Zusammenarbeit in Strafsachen mit den Mitgliedstaaten der EU; EU-JZG) Anwendung.

Folgendes sind die Rechtsgrundlagen für die Zusammenarbeit mit Europol: EU Polizeikooperationsgesetz; Bundesgesetz über die polizeiliche Kooperation mit den Mitgliedstaaten der Europäischen Union und dem Europäischen Polizeiamt (Europol), BGBl. I Nr. 132/2009, zuletzt geändert durch BGBl. I Nr. 161/2013 in der Umsetzung des Rahmenbeschlusses 2009/371/JI vom 6. April 2009 über die Errichtung des Europäischen Polizeiamtes (Europol): Im Mittelpunkt der Zusammenarbeit mit Europol stehen Prävention und Bekämpfung von schwerer grenzüberschreitender Kriminalität einschließlich des Terrorismus. Der Informationsaustausch mit Europol erfolgt über die Nationale Stelle Europol im Bundeskriminalamt bzw. über dessen Verbindungsbeamtenbüro in Den Haag unter der Nutzung des SIENA-Kanals.

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

Die österreichischen Behörden erklärten, dass die Unterstützung und Koordinierung seitens Europol/EC3 sowie Eurojust unerlässlich für die Erleichterung der internationalen Zusammenarbeit ist. Der umfassende Leistungskatalog besteht aus der Erstellung von Trend- und Risikoanalysen, wobei Europol sich bereits 2010 mit seinem "I-OCTA" (Internet Organised Crime Threat Assessment) mit den aus der Cyberkriminalität entstehenden Gefährdungen befasst hat. Weiters werden Frühwarnmeldungen ("early warning messages") verfasst und in Zusammenarbeit mit dem privaten Sektor (in öffentlich-privater Partnerschaft) Modelle der Kriminalprävention und strategischer Planung entwickelt.

Die operative Unterstützung durch Europol/EC3 besteht aus der operativen Analyse, forensischer Unterstützung durch neue von Microsoft entwickelte Technologien wie einer Foto-DNA zur raschen Identifikation insbesondere von Opfern von Kinderpornografie durch Abgleich von Bildern, einer raschen Reaktion auf Cybercrime Angriffe durch Einrichtung von Notfallteams, Unterstützung von Ermittlungen in Finanz- und Wirtschaftskriminalität, sowie Kinderpornografie im Internet und letztlich dem Schutz von kritischer IT-Infrastruktur in der EU innerhalb des Mandatsbereiches von Europol. Europol verarbeitet in der Erfüllung dieser Aufgaben die Informationsflüsse der Strafverfolgungsbehörden und Institutionen in der Union und auch der privaten Einrichtungen und führt sie zusammen und koordiniert ferner Aktivitäten der zuständigen Ermittlungsteams im IT-Bereich.

Österreich ist an der bei Europol eingerichteten Strategischen Gruppe der Leiter der nationalen auf Hightech-Kriminalität spezialisierten Fahndungsdienste in der Europäischen Union beteiligt. Österreich war seit der Errichtung als damaliger AWF (Analytical Work File) 2009 daran beteiligt. "Check the web" wurde im Juli 2015 in die "EU-IRU" (Europäische Meldestelle für Internetinhalte“) umgewandelt. Hier geht es jedoch um die Prävention und Bekämpfung von Terrorismus.

Österreich hat einen Verbindungsbeamten zu J-CAT bei EC3 entsendet. Seit der Errichtung von EC3 sind im Rahmen des FP "Cyborg" sechs Operationen im Laufen, wobei eine von Österreich federführend betreut wird. J-CAT (Joint Cybercrime Action Task Force) wurde im September 2014 anlässlich des JIT Mozart als ein Pilotprojekt von EC3 mit dem Ziel der vertieften Zusammenarbeit im Bereich Cyberkriminalität in Leben gerufen. Es umfasst im Wesentlichen die Bekämpfung folgender Bereiche:

- Hightech-Kriminalität (Malware, Botnets, Intrusion usw.);
- Unterstützung von Cyberkriminalität (Bulletproof-hosting, Counter Anti-Virus-Services, Leasen und Vermieten von Infrastruktur, Geldwäsche inklusive virtuelle Währungen usw.);
- Betrug im Internet (Online Zahlungssysteme, Carding, Social Engineering usw.);
- sexuelle Ausbeutung und sexueller Missbrauch, insbesondere von Kindern.

Die Zuständigkeit für diese Aufgaben liegt beim österreichischen Bundeskriminalamt. Österreich ist überzeugt, dass seine eigenen Ressourcen gebündelt und Synergien effektiv und effizient genutzt werden müssen. Eine Möglichkeit dazu bietet J-CAT, weshalb dem J-CAT-Verbindungsbeamten eine zentrale Rolle zukommt. Aufgrund bisheriger Erfahrungen ergeben sich für den J-CAT Verbindungsbeamten insbesondere folgende spezifische Anforderungen und Aufgaben:

- vertieftes fachliches Wissen in dieser sehr komplexen Materie, mit einer Vielzahl an Phänomenen, sehr umfangreichem Fachvokabular und stetiger Weiterentwicklung;
- aktueller Wissensstand zu den laufenden Ermittlungen sämtlicher J-CAT Fälle, sowie über Art und Umfang einer österreichischen Beteiligung;
- Mitwirkung an mehreren J-CAT Fällen zur gleichen Zeit mit besonderem Augenmerk auf den Österreichbezug;
- unbürokratische und rasche Abklärung dringlicher Ermittlungsschritte in beide Richtungen;
- konsequente Teilnahme an den wöchentlichen J-CAT Koordinierungsbesprechungen;
- regelmäßige Kontakte zu den J-CAT Verbindungsbeamten anderer Europol Staaten zwecks Gewährleistung einer vertrauensvollen und rechtlich korrekten Zusammenarbeit;
- direkter Kontakt zu J-CAT Mitgliedern außerhalb von Europol (z. B. USA, Kanada, Australien, Kolumbien);
- intensiverer Kontakt zum privaten Sektor, vor allem auf internationaler Ebene (z. B. Microsoft, Symantec, Kaspersky, Google, Facebook, PayPal, Ebay);
- bessere Möglichkeiten der Zusammenarbeit mit Russland durch Kontakte mit russischen IT-Sicherheitsunternehmen;
- Weitergabe von Erfahrungswerten und Erkenntnissen aus J-CAT an die nationalen Stellen;
- korrekte Zuordnung internationaler Anfragen an die maßgeblichen nationalen Stellen via SIENA;
- Entlastung nationaler Einheiten bei internationalen Ermittlungen, d. h. Einsparung von Zeit und Ressourcen.

Die österreichischen Behörden teilten mit, dass bei den Ermittlungen die Grenzen traditioneller Systeme sehr deutlich zum Vorschein gekommen seien. Wesentliche Faktoren für eine effektive Bekämpfung von Cyberkriminalität sind vor allem der permanente Wissensaustausch und die kurzen Reaktionszeiten. Während reguläre Verbindungsbeamte als verlängerter Arm verschiedener Ermittlungseinheiten agieren und dabei im Wesentlichen Administrationsaufgaben erfüllen, ist der J-CAT-Verbindungsbeamte integrativer Bestandteil der Ermittlungsorganisation. Dazu hat er sich aktiv weiterzubilden, um seine Aufgaben in der erforderlichen Qualität bewerkstelligen zu können. Begreift man den J-CAT-Verbindungsbeamten als Experten vor Ort, können operative Sitzungen auch kurzfristig einberufen werden und so manche Dienstreise kann mitunter eingespart werden. Die operativen Erfahrungen zeigen, dass ein fachkundiger J-CAT-Verbindungsbeamter jedenfalls ein wichtiger Bestandteil für die adäquate Bekämpfung der Cyberkriminalität sein sollte. Das Aufgabengebiet ist umfangreich und komplex und kann nur durch Vollzeitbeschäftigung erfüllt werden.

Die Operation "Onymous" im Rahmen von J-CAT erbrachte im Zuge einer internationalen Polizeiaktion in 15 Ländern Verhaftungen von 17 Verdächtigen, 13 Hausdurchsuchungen sowie Sicherstellung von Bitcoins und Bargeld im Wert von über einer Million US-Dollar. 414 illegale Webseiten wurden vom Netz genommen.

7.1.3. Operative Leistung von JIT und Cyberpatrouillen

Operativ wurde das gemeinsame Ermittlungsteam "MOZART" (JIT "MOZART") 2013 zur Bekämpfung des Internetbetruges gegründet. Es steht unter österreichischer Leitung und wird von Europol/Eurojust unterstützt. Neben Österreich sind folgende Staaten beteiligt: Finnland, Vereinigtes Königreich, Niederlande und Norwegen. Die Betrugshandlungen erfolgten durch Infektion des Netbanking-Systems mit Malware. Diese veranlasste das Opfer zur Autorisierung betrügerischer Geldüberweisungen. Der Ermittlungserfolg wurde durch das Offenlegen verschleierter Kommunikationswege der Täter über virtuelle private Netzwerke und Proxy-Server, die die tatsächliche IP-Adresse verbargen, erreicht. Zwischen 2013 und 2015 wurden 11 Mitglieder einer international agierenden russisch-ukrainischen OK-Gruppe eruiert sowie letztlich auch der Gründer und Kopf der Organisation im Frühjahr 2015 ausgeforscht und in den USA verhaftet. Insgesamt führten die Ermittlungen der SOKO, bzw. des gemeinsamen Ermittlungsteams "MOZART" zu 60 Festnahmen in vier verschiedenen Staaten. Der Einsatz des gemeinsamen Ermittlungsteams dauert noch an, da sich in den sichergestellten Beweismitteln Hinweise zur Klärung weiterer Straftaten weltweit finden werden.

Österreich war auch von einem anderen grenzüberschreitenden Fall betroffen, in dem eine Tätergruppe über Internet eine Malware eingesetzt hatte, die über die aktive Internetverbindung des Opfers auf dessen Konto zugriff und Überweisungen an Finanzagenten ("Money Mules") in ganz Europa tätigte. Dabei wurden Opfer in der Bundesrepublik Deutschland, im Vereinigten Königreich, in Italien, in den Niederlanden, in Finnland, in Norwegen, in den Vereinigten Staaten von Amerika und in Australien geschädigt. Die zuständige österreichische Staatsanwaltschaft hat daher ein multinationales gemeinsames Ermittlungsteam aufgestellt, das durch eine Vereinbarung zwischen Österreich, Finnland, Belgien, dem Vereinigten Königreich und Norwegen errichtet wurde. Nach Verlängerung der ursprünglich für ein Jahr anberaumten Mandatsdauer ist das Team weiterhin aktiv. Mittlerweile sind auch die Niederlande dem Team beigetreten. Der Austausch von Beweismitteln erfolgt innerhalb des JIT ohne weitere formelle Rechtshilfeersuchen; Koordinierungstreffen werden auch bei Eurojust abgehalten. Das persönliche Zusammentreffen von Ermittlern und StaatsanwältInnen aus den beteiligten Staaten erleichtert die Abstimmung der Ermittlungen und die Kontaktaufnahme im kurzen Weg. Für die Tätigkeit der JIT wurden Finanzmittel des JIT-Funding von Eurojust in Anspruch genommen.

7.2. Zusammenarbeit zwischen österreichischen Behörden und Interpol

Die Meldestelle des Bundeskriminalamts zur Bekämpfung von Kinderpornografie im Internet ist an die ICSE (Datenbank in Lyon) angeschlossen.
Die Kooperation bei Cyberkriminalität funktioniert mittels des I/24/7 Netzwerkes.

7.3. Zusammenarbeit mit Drittstaaten

Die Zusammenarbeit Österreichs mit Drittstaaten in Bezug auf Cyberkriminalität richtet sich nach der jeweils anwendbaren vertraglichen Grundlage, in Ermangelung einer solchen nach dem österreichischen Auslieferungs- und Rechtshilfegesetz (ARHG). Die Zusammenarbeit erfolgt über die NZB der IKPO INTERPOL (I-24-7-Netzwerk), bzw. auch mit den Behörden der Drittstaaten im Rahmen von Polizeikooperationsverträgen (in ca. 30 Abkommen ist die Bekämpfung von Cyberkriminalität mitumfasst).

Der Verkehr mit Drittstaaten wird prinzipiell über die Zentralstelle im Bundesministerium für Justiz abgewickelt, die Einschaltung von Eurojust erfolgt nur subsidiär, wo im Wege der Zentralstellen keine ausreichenden Kontaktmöglichkeiten bestehen. In solchen Fällen greifen die österreichischen Justizbehörden hauptsächlich auf die zwischen Eurojust und den Drittstaaten benannten Kontaktstellen zurück. Sie berichteten, dass durch die Beteiligung von Eurojust und Europol/EC3 generell eine schnellere Abwicklung von Ermittlungsfällen erfolgen kann. Europol war immer wichtiger strategischer Partner. Europol/EC3 veranstaltete Sitzungen, übernahm Reisekosten und stellte Personal bei den Einsätzen vor Ort zur Verfügung. Dies beschleunigt die Ermittlungen.

7.4. Zusammenarbeit mit der Privatwirtschaft

Die Zusammenarbeit mit der Privatwirtschaft erfolgt ausschließlich über offizielle Einrichtungen. An Facebook gerichtete Rechtshilfeersuchen werden Facebook USA zugeleitet. Gegenwärtig steht diesbezüglich nur der Rechtshilfeweg in die USA offen. Die direkte Befassung von Facebook ist derzeit mangels gesetzlicher Grundlage nicht möglich. Die betreffende Thematik wird auf EU-Ebene behandelt werden (in die neue Richtlinie über den Datenschutz im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen wurde bereits eine Regelung über die Datenübermittlung an Private in Drittstaaten aufgenommen).

Die österreichischen Behörden teilten mit, dass die Teilnahme am Global Airport Action Day (gemeinsame internationale Operationen) ein Mittel ist, um Hindernisse bei der grenzübergreifenden Zusammenarbeit, insbesondere beim Thema Online-Kartenbetrug, zu überwinden.

7.5. Instrumente der internationalen Zusammenarbeit

7.5.1. Rechtshilfe

Es gibt keine spezielle Rechtsgrundlage für die Leistung von Rechtshilfe in Bezug auf Cyberkriminalität. Die österreichischen Behörden wenden die allgemeinen Regelungen auf der Grundlage der anwendbaren Rechtsinstrumente (insbesondere EU-Rechtshilfeübereinkommen aus 2000 samt Protokoll zu diesem Übereinkommen, Europäisches Übereinkommen über die Rechtshilfe in Strafsachen samt Zusatzprotokoll, Übereinkommen über Computerkriminalität) an. Mangels vertraglicher Grundlage kann Rechtshilfe nach dem österreichischen Auslieferungs- und Rechtshilfegesetz (ARHG) auch auf der Grundlage der Gegenseitigkeit (Reziprozität) geleistet werden.

Welche Behörden für die Entgegennahme bzw. das Versenden von Rechtshilfeersuchen zuständig sind, richtet sich nach der jeweils anwendbaren vertraglichen Grundlage (diplomatischer Weg; Weg zwischen den Justizministerien; oder unmittelbarer Behördenverkehr). Für die Erledigung von Rechtshilfeersuchen sind grundsätzlich die Staatsanwaltschaften zuständig. Für Auskünfte über die Hauptverhandlung oder über die Vollstreckung von Freiheitsstrafen ist allerdings das erkennende Gericht zuständig. Entsprechendes gilt für die Vernehmung von Personen und die Übermittlung von Informationen, sofern ein Inlandsverfahren anhängig ist, in welchem bereits Anklage eingebracht wurde, und das Thema des ausländischen Rechtshilfeersuchens mit dem Gegenstand des Inlandsverfahrens in Zusammenhang steht.

Es gibt keine besonderen Verfahren oder Bedingungen, die in Bezug auf die verschiedenen Kategorien von Rechtshilfeersuchen bei Cyberstraftaten eingehalten werden müssen. Dringende Ersuchen werden als solche gekennzeichnet und vordringlich behandelt. Die durchschnittliche Beantwortung eines Ersuchens beträgt – abhängig von der begehrten Rechtshilfehandlung – etwa drei Monate.

Im Rahmen eines Rechtshilfeersuchens (auch wegen Cyberstraftaten) können alle Maßnahmen angefragt werden, die nach der österreichischen Strafprozessordnung vorgesehen sind. Die meisten Rechtshilfeersuchen in Bezug auf Cyberstraftaten betreffen die Abfrage von Stamm- und Verkehrsdaten im Bereich der Telekommunikation (wobei dieser Begriff nach österreichischem Recht auch das Internet umfasst) bzw. Bankauskünfte, wenn es um die Tatbegehung von Betrugsdelikten unter Nutzung des Internet geht.

Wenn der ersuchenden Behörde die rechtlichen und tatsächlichen Voraussetzungen für die benötigte Rechtshilfemaßnahme nicht ausreichend klar sind, werden auch vorab Konsultationen mit den Behörden des zu ersuchenden Staates geführt, wobei – neben dem direkten Verkehr – die Kontaktstellen des Europäischen Justiziellen Netzes (EJN), in Einzelfällen auch Eurojust, eingeschaltet werden können.

Aufgrund des direkten Verkehrs zwischen den EU-Mitgliedstaaten in Rechtshilfesachen ist eine zentrale Statistik aller Rechtshilfeersuchen bisher noch nicht verfügbar. Das Bundesministerium für Justiz ist aber bemüht, für die Zukunft eine statistische Auswertbarkeit des automatisierten zentralen Fallregisters zu schaffen, die es auch ermöglichen soll, Rechtshilfeersuchen nach dem zugrunde liegenden Delikt einzuordnen und statistisch zu erfassen.

Probleme bei der Erledigung/Stellung von Rechtshilfeersuchen für in der "Cloud" begangene Straftaten ergeben sich, wenn der Provider multinational wirtschaftlich tätig ist und nicht auf den ersten Blick erkennbar ist, an welchem Firmensitz in welchem Staat der Zugang zu den in der "Cloud" gespeicherten Daten zu erfolgen hat. Daher kommt es vor, dass Rechtshilfeersuchen gelegentlich an den "falschen" Staat gerichtet werden, der jedoch üblicherweise umgehend Österreich mitteilt, dass ein anderer Staat für die Rechtshilfeleistung zuständig ist.

Die Kommunikation mit Nicht-EU-MS wird zum größten Teil unter Berufung auf das Europäische Rechtshilfeabkommen vom 20. April 1959 abgewickelt. Daneben bestehen bilaterale Rechtshilfeverträge Österreichs mit einzelnen Staaten, wie Australien, Kanada und den Vereinigten Staaten von Amerika. Eingehende Ersuchen werden von den ersuchenden Staaten auch auf das Übereinkommen über Computerkriminalität vom 23. November 2001 gestützt.

In Fällen im Zusammenhang mit Cyberangriffen unter Beteiligung von Straftätern von außerhalb der EU werden von den zuständigen Staatsanwaltschaften Ersuchen um Übernahme der Strafverfolgung oder Rechtshilfeersuchen gestellt, sofern dies aussichtsreich erscheint. Mangels Erfolgsaussicht unterbleiben meist Rechtshilfeersuchen nach Afrika. Innerhalb der EU ergeben sich nach Auskunft der Staatsanwaltschaften bei Rechtshilfeersuchen an das Vereinigte Königreich Probleme.

7.5.2. Instrumente der gegenseitigen Anerkennung

Die österreichischen Behörden haben in Bezug auf die Verhütung, Ermittlung und Verfolgung der Cyberkriminalität die einschlägigen Bestimmungen der Richtlinie über die Europäische Schutzanordnung, des Rahmenbeschlusses über die Anwendung des Grundsatzes der gegenseitigen Anerkennung auf Urteile in Strafsachen, durch die eine freiheitsentziehende Maßnahme verhängt wird, und des Rahmenbeschlusses über die Anwendung des Grundsatzes der gegenseitigen Anerkennung von Geldstrafen und Geldbußen angewendet.

7.5.3. Überstellung/Auslieferung

In Artikel 2 Absatz 2 des Rahmenbeschlusses über den Europäischen Haftbefehl wird "Cyberkriminalität" allgemein als Straftat angeführt, wegen der für den Fall, dass sie nach dem Recht des Ausstellungsstaats mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht ist, (bei Vorliegen der sonstigen Voraussetzungen) die Übergabe ohne Prüfung des Vorliegens der beiderseitigen Strafbarkeit bewilligt wird. Für den Fall des Ankreuzens des betreffenden Kästchens im Formblatt "Europäischer Haftbefehl" durch die zuständige Behörde des Ausstellungsstaats ist daher von der zuständigen österreichischen Behörde das Vorliegen der beiderseitigen Strafbarkeit grundsätzlich nicht zu prüfen.
Bei Nichtanwendbarkeit des Rahmenbeschlusses über den Europäischen Haftbefehl richtet sich die Auslieferungsfähigkeit nach der anwendbaren vertraglichen Grundlage. Nach Artikel 2 Absatz 1 des Europäischen Auslieferungsübereinkommens etwa muss die dem Auslieferungsersuchen zugrundeliegende Handlung sowohl nach dem Recht des ersuchenden Staats als auch nach österreichischem Recht mit einer Freiheitsstrafe oder mit Freiheitsentziehung verbundenen vorbeugenden Maßnahme im Höchstmaß von einem Jahr oder mit einer strengeren Strafe bedroht sein. Wird um Auslieferung zur Vollstreckung einer Freiheitsstrafe ersucht, ist es erforderlich, dass deren Maß mindestens 4 Monate beträgt.

Für die Ausstellung eines Überstellungs- bzw. Auslieferungsersuchens sind die Staatsanwaltschaften bzw. – nach Einbringung der Anklageschrift – das Gericht zuständig. Für die Entscheidung über ein derartiges Ersuchen sind die Landesgerichte zuständig. Die Zuständigkeit für die Entgegennahme eines derartigen Ersuchens richtet sich nach der anwendbaren vertraglichen Grundlage (diplomatischer Weg; Weg zwischen den Justizministerien; oder unmittelbarer Behördenverkehr).

Es gibt keine besonderen Verfahren oder Bedingungen, die in Bezug auf Ersuchen bei Cyberstraftaten eingehalten werden müssen. Dringende Ersuchen werden als solche gekennzeichnet und vordringlich behandelt. Die durchschnittliche Beantwortung eines Ersuchens beträgt – abhängig davon, ob der Betroffene der Übergabe/Auslieferung zustimmt (vereinfachte Übergabe/Auslieferung) oder nicht – etwa drei bis sechs Monate.

7.6. Fazit

- Österreich arbeitet eng mit den Agenturen der EU, besonders Europol/EC3 und Eurojust, zusammen. Auf Eurojust wird in Bezug auf Cyberkriminalität häufig über das österreichische Verbindungsbüro zurückgegriffen. Die Anforderung finanzieller Unterstützung zur Finanzierung von Projekten und auch die Nutzung der Befugnisse von Eurojust zu deren Gunsten stellt nach Auffassung der Gutachter offensichtlich ein Beispiel für bewährte Praxis dar.

- Die österreichischen Behörden nehmen Europol als wichtigen strategischen Partner wahr, der zu einer rascheren Fallbearbeitung beiträgt. Europol/EC3 veranstaltete Sitzungen, übernahm Reisekosten und stellte Personal bei den Einsätzen vor Ort zur Verfügung. Dies beschleunigt die Ermittlungen.

- Österreich nimmt an einer Reihe von Einsätzen gegen die Cyberkriminalität teil und hat gute grenzübergreifende Beziehungen zu den Nachbarländern (etwa Deutschland), auch in Bezug auf bilaterale Schulung. Es herrscht die Auffassung, dass auch die CEPOL-Austauschprogramme in Betracht gezogen werden könnten.

- In Bezug auf Ermittlungen unterstützt Österreich die internationalen Bestrebungen der EU zur Bekämpfung der Cyberkriminalität durch seine Teilnahme an den "EMPACT-cyber-attack"-Arbeitsgruppen und seine Beteiligung an den "J-CAT Operations".

- Die Zusammenarbeit mit in Österreich ansässigen Unternehmen wird von den österreichischen Behörden generell als positiv eingestuft, den Gutachtern wurden aber auch von Vertretern verschiedener Akteure einige Bedenken übermittelt. Die österreichischen Behörden meldeten einige Schwierigkeiten bei der Zusammenarbeit mit Privatunternehmen mit Hauptsitz in Drittländern (beispielsweise Facebook).

- Die österreichischen Behörden verwiesen auf die Langsamkeit der Zusammenarbeit. Die Staatsanwälte äußerten Bedenken in Bezug auf Echtzeit-Übersetzungen von Inhaltsdaten, beispielsweise im konkreten Fall im Rahmen des gemeinsamen Ermittlungsteams "MOZART", bei dem es um heruntergeladene Telefongespräche/Internetkommunikation in russischer Sprache ging.

- Österreich verfügt nicht über spezielle Rechtsvorschriften für die internationale Zusammenarbeit in Bezug auf Cyberkriminalität. Die rechtliche Grundlage für diese Zusammenarbeit liegt in den internationalen Übereinkünften, denen Österreich als Partei angehört, und dem österreichischen Auslieferungs- und Rechtshilfegesetz (ARHG). Die Praktiker nutzen alle verfügbaren Kanäle: Verbindungsbeamte sowie Richter und Staatsanwälte oder EU-Agenturen.

- Die österreichischen Behörden würdigen die Zusammenarbeit mit den Mitgliedstaaten als positiv. Es wurde jedoch gemeldet, dass die Zusammenarbeit mit Drittstaaten gelegentlich schwierig war und Reaktionen möglicherweise spät erfolgen. Die Kommunikation mit Nicht-EU-Mitgliedstaaten wird zum größten Teil unter Berufung auf das Europäische Rechtshilfeabkommen von 1959 abgewickelt. Daneben bestehen bilaterale Rechtshilfeverträge Österreichs mit einzelnen Staaten, wie Australien, Kanada und den Vereinigten Staaten von Amerika.

8. AUS- UND FORTBILDUNG, SENSIBILISIERUNG UND PRÄVENTION

8.1. Spezifische Aus- und Fortbildung

Justizwesen

Schulungsmaßnahmen in Bezug auf Cyberkriminalität werden für sämtliche Vertreter der Justizbehörden (Richter und Staatsanwälte), somit auch für Personen angeboten, die Aufgaben im Rahmen der internationalen Zusammenarbeit wahrnehmen. In den letzten Jahren war das Thema Cyberkriminalität Gegenstand folgender Veranstaltungen:

- Im April 2013 fand eine (sprengelweite) Schulung des Präsidiums des Oberlandesgerichts Innsbruck mit dem Titel "Computerkriminalität – Problemfelder im Zusammenhang mit der forensischen Auswertung von Datenträgern und Ermittlungen im Internet" statt;
- im Jahr 2014 fand eine Arbeitstagung der Staatsanwälte/Staatsanwältinnen gemeinsam mit Ermittlungsleiterinnen und Ermittlungsleitern zum Thema Bekämpfung von Kinderpornografie/sexuellem Missbrauch Minderjähriger statt;
- anlässlich der RichterInnenwoche 2015 wurden Vorträge zum Thema "Medien im Zivil- und Straf(verfahrens)recht" veranstaltet, in denen nicht nur die missbräuchliche Verwendung der neuen Medien (wie Facebook oder Twitter) für die Verbreitung illegaler Inhalte, Betrugsdelikte aber auch gezielte Diffamierung aufgezeigt wurden, sondern auch die Nutzung dieser Technologien durch die Strafverfolgungsbehörden, um an relevante Informationen zu gelangen oder mit den Bürgern in Kontakt zu treten;
- 2016 finden einige wenige Veranstaltungen statt, unter anderem die Arbeitstagung für StaatsanwältInnen und ErmittlungsleiterInnen zum Thema "Bekämpfung von Kinderpornografie/sexuellem Missbrauch Minderjähriger" (9. bis 11.5.2016; gemeinsam mit dem Bundeskriminalamt), in deren Verlauf folgende Themen behandelt werden sollen: Facebook/Twitter; neue Ermittlungstools des Bundeskriminalamts; Bitcoin und andere Kryptowährungen; Darknet; Online-Ermittlungen; Problemstellungen bei Ermittlungsverfahren im Internet. Weitere Seminare über Cyberkriminalität und das Darknet finden vom 19. bis 21. September und am 10./11. November 2016 statt.

Richter und Staatsanwälte nahmen an zahlreichen Veranstaltungen der ERA, des EJTN und anderer Organisationen zum Thema Cyberkriminalität teil. Durch die für internationale Angelegenheiten zuständige Fachabteilung des BM.I (Abteilung I/4, Referat I/4/a – Attachéwesen) wird im Zusammenwirken mit der Sicherheitsakademie (Zentrum für internationale Angelegenheiten; SIAK/ZIA) bedarfsorientiert die Ausbildung der österreichischen Verbindungsbeamten (Polizeiattachés) umgesetzt.

Des Weiteren besteht eine Zusammenarbeit mit den nationalen Universitäten im Rahmen des KIRAS-Programms (Österreichisches Förderprogramm für die Sicherheitsforschung). Im Zuge einer engen Kooperation des C4 mit dem BMJ werden seit 2014 gegenseitige Aus- und Fortbildungsmaßnahmen für Richterinnen und Richter, Staatsanwältinnen und Staatsanwälte abgehalten.

Dessen ungeachtet nahmen die Gutachter zur Kenntnis, dass die Teilnahme an Schulungen für Richter und Staatsanwälte nicht verbindlich ist und die Zahl der in Österreich und im Ausland abgehaltenen Seminare, an denen sie teilgenommen haben, nicht dafür ausreicht, dass eine ausreichende Zahl von mit Strafsachen befassten Angehörigen der Fachberufe geschult wird.

Strafverfolgung

Für den Ressortbereich des Innenministeriums obliegt der Sicherheitsakademie (SIAK) die Durchführung bzw. Bereitstellung der Grundausbildungen für die Bediensteten des BMI. Für den Exekutivdienst sind durch entsprechende Verordnung

- die Grundausbildung für den Exekutivdienst (Polizeigrundausbildung);
- die Grundausbildung für die Verwendungsgruppe E 2a (dienstführende Beamte) im Exekutivdienst und
- die Grundausbildung für die Verwendungsgruppe E 1 (Leitende Beamte) im Exekutivdienst vorgesehen bzw. geregelt.

Allgemein gilt, dass die thematische/inhaltliche Ausgestaltung der jeweils vorgesehenen Lehrgegenstände in enger Zusammenarbeit mit der Generaldirektion für die öffentliche Sicherheit bzw. den jeweils zuständigen Fachabteilungen bzw. Organisationseinheiten des BMI erfolgt. Der Themenbereich "Cyberkriminalität" ist Bestandteil der Grundausbildung für den Exekutivdienst (Polizeigrundausbildung) und wird unter dem Gesichtspunkt der für das polizeiliche Einschreiten maßgeblichen Rechtsvorschriften und Handlungsanweisungen (wie insbesondere dem Strafrecht, der Strafprozessordnung, der sicherheitspolizeilichen Handlungslehre, Kriminalistik, etc.) fächerübergreifend bearbeitet. Über die Fachzirkel "Strafrecht", "Kriminalistik" und "Sicherheitspolizeiliche Handlungslehre" bzw. einschlägige Schulungen der hauptberuflich Lehrenden des Exekutivdienstes wird angestrebt, Basiswissen zum Themenbereich verstärkt in die Polizeigrundausbildung einfließen zu lassen.

Eine themenzentrierte Fokussierung ist in der Polizeigrundausbildung derzeit nicht vorgesehen (mit Ausnahme einer achtstündigen Grundschulung in Bezug auf Cyberkriminalität).

In der Grundausbildung für die Verwendungsgruppe E 2a (dienstführende Beamte) im Exekutivdienst ist im Lehrgegenstand Kriminalistik eine themenzentrierte Bearbeitung des Themenbereiches "IT-Kriminalität" vorgesehen. Inhalte bzw. Themenschwerpunkte sind unter anderem rechtliche Grundlagen und Erscheinungsformen der Computerkriminalität, Grundlagen der Sicherung elektronischer Beweismittel bzw. Möglichkeiten der Datenauswertung und -aufbereitung.

In der Grundausbildung für die Verwendungsgruppe E 1 (Leitende Beamte) im Exekutivdienst ist derzeit kein spezifisches Modul im Hinblick auf "Cyberkriminalität" bzw. "IT-Kriminalität" vorgesehen. Im Rahmen der erstmals im Jahr 2010 in die Bildungslandschaft des BM.I implementierten Fachausbildung für den Kriminaldienst (FAB-KD) sollen die Teilnehmenden die für eine professionelle Dienstverrichtung im Kriminaldienst grundlegend erforderlichen Kompetenzen bedarfsorientiert und unter Maßgabe einer konstruktiven Vernetzung mit den praktischen Anforderungen der Aufgabenerfüllung erweitern und vertiefen. Diese Schulung baut auf die Lehrinhalte der Grundausbildung für den Exekutivdienst (Polizeigrundausbildung) und der Grundausbildung für die Verwendungsgruppe E 2a (Dienstführende Beamte) im Exekutivdienst auf.

Der Themenblock "IT-Kriminalität" ist seit der erstmaligen Durchführung Bestandteil der Fachausbildung. Inhalte bzw. Themenschwerpunkte sind unter anderem rechtliche Grundlagen und Erscheinungsformen von Computer- und Netzwerkkriminalität (Cyberkriminalität im engeren bzw. im weiteren Sinne), allgemeine Grundsätze im Umgang mit elektronischem Beweismaterial, Arten der Sicherstellung von elektronischen Beweismaterial, Durchführung der Sicherstellung, Möglichkeiten der Datenauswertung und -aufbereitung, Abläufe und Vorgangsweise in der Praxis.

Im Rahmen des laufenden Zyklus der Fortbildungswoche (als standardisierte, verpflichtende Fortbildung für Angehörige des Wachkörpers Bundespolizei, die überwiegend in Uniform Dienst versehen) ist der Themenbereich "Cybercrime" bzw. "Internetkriminalität" in den Bundesländern Burgenland, Niederösterreich und Salzburg im Rahmen des Themenfeldes "Regionale Schwerpunktthemen" vorgesehen.

Die dem Prinzip des lebensbegleitenden Lernens folgende Fortbildungsstruktur des BM.I sieht schon angesichts der Komplexität und Vielschichtigkeit der Aufgaben- und Tätigkeitsbereiche der Bediensteten des Innenressorts und der mitunter doch sehr unterschiedlichen Anforderungen im Sinne der für Bildungsmaßnahmen allgemein gebotenen Bedarfs- und Zielgruppenorientierung, aber auch im Hinblick auf die allgemein wirkende Zielgruppengröße von mehr als 32.000 Bediensteten, unter anderem eine strukturierte Wechselwirkung zwischen zentralen und dezentralen Bildungsmaßnahmen vor, die unter Maßgabe der thematischen/inhaltlichen Ausrichtung, der jeweils definierten Zielgruppe, der zur Verfügung stehenden (personellen, logistischen, infrastrukturellen/räumlichen und monetären) Ressourcen sowie den wirkenden organisatorischen Rahmenbedingungen zentral für das gesamte Bundesgebiet oder dezentral innerhalb bundesländerübergreifender Fortbildungsverbände, innerhalb einer Landespolizeidirektion (regional) oder innerhalb eines Bezirks- bzw. Stadtpolizeikommandos (lokal) zu planen, zu organisieren und/oder durchzuführen sind. Zudem wird unter anderem zwischen allgemeinen und speziellen Fortbildungen unterschieden, die je nach Zuordnung unterschiedliche organisatorische und/oder strukturelle Zuständigkeiten innerhalb des BM.I bedingen.

Wenngleich der Sicherheitsakademie unter anderem die Steuerung und Koordinierung von Bildungsangeboten für die Bediensteten des Innenressorts zukommt, impliziert dies aber keineswegs, dass ihr auch die konkrete Planung, Organisation und/oder Durchführung aller Bildungsmaßnahmen innerhalb des Ressorts bzw. für sämtliche Bedienstete des Ressorts obliegt.

Spezielle Fortbildungen (im Sinne von fachbezogenen arbeitsplatz- bzw. tätigkeitsspezifischen Bildungsmaßnahmen, die angesichts ihrer thematischen/inhaltlichen Ausrichtung lediglich für einen eingeschränkten Teilnehmerkreis von Bedeutung sind) werden insbesondere vor dem Hintergrund der gebotenen Bedarfs- und Zielgruppenorientierung sowie einer möglichst effizienten Vernetzung mit den wirkenden praktischen Anforderungen der Aufgabenerfüllung bzw. Dienstverrichtung (Praxisorientierung) grundsätzlich durch die jeweils zuständige Fachabteilung bzw. Organisationseinheit des BM.I umgesetzt. Folgendes sind Beispiele für die von den zuständigen Abteilungen oder Dienststellen des BM.I angebotenen Schulungskurse zum Thema Cyberkriminalität:

- Ausbildung für Bezirks-IT-Ermittler

Auf Ebene der Polizeiinspektionen bzw. Bezirks- und Stadtpolizeikommanden wurden in den vergangenen Jahren Bezirks-IT-Ermittler eingesetzt, die unter Maßgabe ihres Ausbildungs- und Ausrüstungsstandes sowie unter fachlicher Aufsicht des jeweils eingerichteten Assistenzbereiches des Landeskriminalamtes (LKA AB 06 IT-B) IT-relevante kriminalpolizeiliche Ermittlungen sowie entsprechende Sicherungs- und Auswertetätigkeiten vornehmen. Auf Basis der aktuellen Erlasslage umfasst die Ausbildung der Bezirks-IT-Ermittler ein einwöchiges (theoretisches) Ausbildungsmodul und eine zweimonatige Praxisausbildung durch das jeweilige Landeskriminalamt. Im Zusammenwirken zwischen der für Einsatzangelegenheiten zuständigen Abteilung des BM.I (Abteilung II/2, Referat II/2/a - Exekutivdienst) und dem Bundeskriminalamt (Büro 5.2 - C4 (Cybercrime-Competence-Center) sowie Büro 1.2 (Kriminalpolizeiliche Aus- und Fortbildung) wurden in den Jahren 2012 bis 2014 in Summe 19 einwöchige Ausbildungsmodule für Bezirks-IT-Ermittler durchgeführt, an denen 276 Bedienstete teilnahmen. Inhalte dieses Ausbildungsmoduls waren unter anderem Grundlagen der Computerkriminalität, Netzwerkkriminalität und Datensicherung mit praktischer Anwendung, Grundlagen zu Auswertungen von Mobiltelefonen, Vermögensdelikte im Zusammenhang mit Internetkriminalität, Kinderpornografie im Internet, Internetkriminalität und verdeckte Ermittlungen.

- Aus- und Fortbildungen für Spezialisten auf Länderebene (LKA AB 06 IT-B)

Spezialisten auf Länderebene, konkret die Bediensteten des in den Landeskriminalämtern eingerichteten Assistenzbereiches "IT-Beweissicherung" (LKA AB 06 IT-B) werden unter organisatorischer Federführung der für Einsatzangelegenheiten zuständigen Abteilung des BMI (Abteilung II/2, Referat II/2/a – Exekutivdienst) und unter Einbindung des Bundeskriminalamtes (Büro 5.2 – C4 (Cybercrime-Competence-Center) sowie Büro 1.2 (Kriminalpolizeiliche Aus- und Fortbildung) auf Grundlage der "Kriminaldienst-Fortbildungs-Richtlinien (KDFR)" fachspezifisch fortgebildet. Eine Teilnahme der dem Assistenzbereich zuzurechnenden Bediensteten an einem der entsprechenden Seminare bzw. Workshops innerhalb eines Fortbildungszyklus (derzeit für die Jahre 2014 bis 2016) ist verpflichtend. Eine Spezialausbildung für Bedienstete, die neu mit einem Arbeitsplatz in diesem Assistenzbereich betraut wurden, besteht zur Zeit nicht.

- Aus- und Fortbildungen für Spezialisten auf Bundesebene (.BK, .BVT und .BAK)

Die Aus- und Fortbildung von Spezialisten auf Bundesebene – konkret des Bundeskriminalamtes (BK), des Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung (.BVT) und des Bundesamtes zur Korruptionsprävention und Korruptionsbekämpfung (.BAK) – wird nach individuellen Schwerpunkten und unter Nutzung entsprechender nationaler und internationaler Schulungsangebote bzw. Spezialtrainings gestaltet.
Im Rahmen der Möglichkeiten wird sowohl im Zusammenhang mit Schulungsmaßnahmen für Spezialisten auf Länderebene (LKA AB 06 IT-B), als auch für Spezialisten auf Bundesebene (BK, BVT und .BAK) auch auf entsprechende Angebote der Fachhochschulen bzw. der universitären Einrichtungen, wie z. B. der FH St. Pölten, der FH Technikum Wien und der FH Hagenberg, zum Themenbereich zurückgegriffen.
Fallweise wirken Fachhochschulen bzw. universitäre Einrichtungen, insbesondere durch die Beistellung von entsprechenden Vortragenden/Trainern, auch an ressortinternen Schulungsmaßnahmen zum Themenbereich mit.

Im Rahmen der kriminalpolizeilichen Fortbildung erfolgt wiederholt eine Ausbildung der spezialisierten IT-Ermittler auf allen Ebenen. Die Kriminaldienstfortbildungsrichtlinie (KDFR) sichert die Weiterbildung ab. Darüber hinaus notwendige Ausbildungen werden im Einzelfall geplant und durchgeführt. Eine enge Kooperation mit universitären Einrichtungen findet statt. Das BMI veranstaltet in Kooperation mit einer Fachhochschule auch einen Studienlehrgang für Wirtschaftskriminalität und Cybercrime.

In den Landeskriminalämtern erhalten Mitarbeiter des Assistenzbereichs "Informationstechnologie – Beweissicherung" im Zuge der regelmäßig stattfindenden Kriminaldienstfortbildungen Schulungen (in der Dauer von ca. 3 bis 5 Tagen für jeweils ca. 10 bis 20 Mitarbeiter; 2014 gab es diesbezüglich 8 Termine mit Inhalten aus dem Bereich von Forensikspezialistenwissen).

Auf Bezirks- und Stadtpolizeikommisariatsebene sind Bezirks-IT-Ermittler (im Bundesgebiet in Summe ca. 300) ausgebildet, welche IT-relevante kriminalpolizeiliche Ermittlungen sowie im Rahmen ihres Ausbildungs- und Ausrüstungsstandes Sicherungs- und Auswertetätigkeiten unter Aufsicht des LKA AB 06 ITB auf BPK/SPK-Ebene vornehmen. Die Ausbildung zum BezIT umfasst eine einwöchige theoretische Grundausbildung und eine zweimonatige praktische Ausbildung (in Form einer Zuteilung) sowie Fortbildungen (jährlich bis zu 2 Tage).

Im Hinblick auf die künftigen Aufgaben- und Tätigkeitsfelder der Verbindungsbeamten bzw. die für deren künftige Verwendung erforderlichen Kompetenzen werden die maßgeblichen Inhalte bzw. Themenschwerpunkte der Ausbildung unter möglichst breiter Einbindung der jeweils zuständigen Fachabteilungen und Organisationseinheiten des BM.I festgelegt. Zudem sind auch anknüpfende (thematische/inhaltliche) Inputs durch Experten des Bundesministeriums für Europa, Integration und Äußeres (BMEIA) und des Bundesministeriums für Justiz (BMJ) vorgesehen. Im Rahmen des im November 2015 begonnenen Ausbildungslehrgangs (in Form von 3 Blöcken zu jeweils 3 Wochen) wurde eine Woche speziell durch das Bundeskriminalamt gestaltet; der Themenbereich "Cyberkriminalität" war Bestandteil dieser Woche.

Im Rahmen der Möglichkeiten werden entsprechende internationale Schulungsangebote bzw. Spezialtrainings zum Themenbereich, insbesondere im Kontext mit der Aus- und Fortbildung von Spezialisten auf Länderebene (LKA AB 06 IT-B) und von Spezialisten auf Bundesebene (BK, .BVT und .BAK), genutzt.

Die ressortinterne Ausschreibung von Bildungsangeboten der Europäischen Polizeiakademie (CEPOL) erfolgt durch die Sicherheitsakademie (Zentrum für internationale Angelegenheiten; SIAK/ZIA). Im Rahmen der Kriminaldienstfortbildungsrichtlinie (KDFR) werden durch das BMI Ausbildungsverantwortliche aus den LKA (Landeskriminalämtern) bestellt, die für einen Ausbildungszyklus (aktuell 3 Jahre) ein Aus- und Fortbildungsprogramm erstellen, das für alle IT-Ermittler aus den LKA verbindlich zu absolvieren ist. Für alle IT- Ermittler aus der Bezirksebene sind jährlich Fortbildungstage in den jeweiligen Bundesländern zu absolvieren.

Eine darüber hinausgehende Grundausbildung für aktuelle und neu eintretende IT-Ermittler (die bisherige Grundausbildung wird aktuell neu gestaltet) wird inhaltlich durch das Bundeskriminalamt (Abteilungen 5 und 1) gestaltet und in Kooperation mit der Sicherheitsakademie des BMI ebenenbezogen veranstaltet. Fachbezogene Ausbildungen zu aktuellen Themen (Software, Hardware, neue Deliktsformen) werden vom Bundeskriminalamt (Abteilungen 3,5 und 7) in Kooperation mit dem Schulungsbüro des Bundeskriminalamtes geplant und durchgeführt. Im Hinblick auf die internationalen Aspekte der Ausbildung ist das Bundeskriminalamt an der "International Association for Computer Information Systems" (IACIS), einem Zusammenschluss von Forensikexperten und -expertinnen, beteiligt. Die IACIS führt Grundausbildungen und Spezialmodule im Rahmen europäischer Projekte durch. Weiters ist das Bundeskriminalamt am europäischen Schulungsprogramm "European Cybercrime Training and Education Group" (ECTEG) im Bereich High Tech Crime beteiligt. Zusätzlich finden externe, nationale Schulungen zur laufenden Fortbildung im Bereich Betriebssysteme, Auswertungssoftware, Server und Netzwerke statt. Darüber hinaus erfolgen anlassbezogene Schulungen und Workshops u. a. mit Microsoft oder dem Computer Emergency Response Team (CERT).

Für sämtliche Fortbildungsaktivitäten der Justizbehörden (Richter und Staatsanwälte) wurden im Jahr 2013 1.380.762,15 EUR aufgewendet. Dieser Betrag ergibt sich aus den Referentenhonoraren, den Kosten für die Unterbringung sowie den Reisegebühren, den Reisekostenzuschüssen und den sonstigen Kosten.

Exzellenzzentrum

Die fachlich zuständige Abteilung 5 des Bundeskriminalamtes stellt mit C4 das Exzellenzzentrum dar. Neue Entwicklungen werden evident gehalten, in Newslettern regelmäßig verbreitet und im Bedarfsfall rasch Schulungsmaßnahmen innerhalb der vorgegebenen Wege initiiert. Der vom Bundeskriminalamt (Abteilung 1) betriebene Kriminalistische Leitfaden (KLF) dient daher als Informationsplattform, auf die von allen polizeilichen Ebenen elektronisch zugegriffen werden kann. Der KLF ist immer aktuell.

Hochschulen

An der Universität Wien werden alternierend je ein Semester der Kurs "IT-Strafrecht" und der Kurs "Aktuelle Fragen des 'Cybercrime'" im Rahmen des Wahlfachkorbes "Strafjustiz und Kriminalwissenschaften" angeboten. Es gibt Zusammenstellungen optionaler Module, mit denen ein Spezialisierungsprogramm angeboten werden soll, das von den Studierenden freiwillig und zusätzlich zu den verpflichtenden Ausbildungsinhalten des rechtswissenschaftlichen Studiums absolviert werden kann.

An der Fachhochschule Wiener Neustadt wird seit März 2015 der Weiterbildungslehrgang "Wirtschaftskriminalität & Cybercrime" angeboten. Dieser Lehrgang richtet sich an Praktiker/innen, die in ihrer beruflichen Tätigkeit in Wirtschaft, Finanzen, Recht, IT, Ermittlung, Strafverfolgung und Verwaltung mit entsprechenden Herausforderungen konfrontiert sind, und wird berufsbegleitend angeboten. Der Lehrgang dauert drei Semester und schließt mit einem Master of Science in Business & Cyber Crime Control (MSc) ab.
Lehrgangsinhalte mit Bezug auf "Cyberkriminalität" sind unter anderem rechtliche Grundlagen betreffend Computerkriminalität, technische Grundlagen von Computersystemen (wie insbesondere IT-Systeme und Systemsoftware, Hardware, Datenträger, Anwendersoftware, Datenbanken, etc.), Sicherung digitaler Beweismittel, Datenanalyse und Data Mining sowie Module zu IT-Forensik, IT Security bzw. Mobile Forensic Devices.

8.2. Sensibilisierungsmaßnahmen

In Österreich wurde im Bereich "Cybersicherheit" ein "Multi-Stakeholder-Ansatz" unter Einbindung der Wirtschaft gewählt: Die Vernetzung zwischen der Wirtschaft und Vertretern der inneren Sicherheit hat mit der KSÖ-Cyber-Initiative begonnen. Daraus wurde die österreichische "Cyber-Sicherheits-Plattform", die mittlerweile der laufenden Kommunikation mit allen Stakeholdern aus Verwaltung, Wirtschaft und Wissenschaft dient.

Zusätzlich hat sich aus dieser KSÖ-Initiative das "Cyber-Security-Forum" aus Wirtschaftsvertretern entwickelt. Dabei handelt es sich um eine Kerngruppe von Unternehmen, etwa aus dem Bankensektor und der Telekommunikations- und der Technologiebranche. Diese Unternehmen tauschen sich über Cyberschwächen aus, die sonst gerne "unter Verschluss" gehalten werden, weil man etwa einen Reputationsschaden fürchtet. Auf operativer Ebene wird dabei eng und vertrauensvoll zusammengearbeitet: Informationen werden ausgetauscht, Risiken eingeschätzt und Maßnahmen diskutiert.

Für den Bereich der sogenannten Cyber Defence liegt die innerstaatliche Zuständigkeit beim Bundesministerium für Landesverteidigung und Sport. Die alljährlich vom Bundesministerium für Landesverteidigung und Sport durchgeführten IKT-Sicherheitskonferenzen (zuletzt im November 2015 in St. Pölten) dienen ebenfalls der (internen und externen) thematischen Sensibilisierung.

Das Bundeskriminalamt betreibt im Rahmen von Sensibilisierungsmaßnahmen unter anderem das Cyber Kids Präventionsprojekt für Kinder im Alter zwischen 8 und 12 Jahren sowie das Click & Check Projekt für Jugendliche, die älter als 14 Jahre sind.

8.3. Verhütung von Cyberkriminalität

Nationale Rechtsvorschriften/politische Maßnahmen und andere Maßnahmen

In der Kriminalprävention werden Themenfelder wie Eigentumsschutz, Gewaltprävention, Suchtmittelprävention und Sexualdeliktsprävention unterschieden. Obwohl sich die Cyberkriminalität in allen diesen Feldern thematisch überschneidet, wird sie erlassmäßig als eigenes Thema etabliert werden. Die Cyberkriminalität verhütenden Maßnahmen finden sich in zielgruppenorientierten Informationsoffensiven und Projekten.

Folgende Vorbeugungsmaßnahmen werden durch das Büro für Kriminalprävention im Bundeskriminalamt umgesetzt oder sind in Planung:

- periodische und anlassbezogene Veröffentlichungen zum Thema auf der Homepage, offiziellen Facebookpage und Polizeiapp.
- Projekt "Click & Check" – Programmschulung für 12-14 jährige Kinder zum Thema Social Media, Internetkriminalität, Mobbing, etc.
- Projekt "Prevention against Cybercrime – Cyber.Sicher"; E- Learning Modul für Erwachsene zum Thema Umgang mit dem Internet in Zusammenarbeit u. a. mit der Universität Wien, Wirtschaftskammer Österreich und saferinternet.at (noch nicht veröffentlicht);
- Projekt "Cyberkids": Vorbereitung für Kinder ab dem Volksschulalter im Umgang mit dem Internet (in Vorbereitung);
- "Sicher in den besten Jahren": umfassende Broschüre für die Zielgruppe der Senioren inklusive eines Kapitels zum Thema "Sicher im Internet".

Für den Bereich der sogenannten Cyber Defence liegt die innerstaatliche Zuständigkeit beim Bundesministerium für Landesverteidigung und Sport.

8.3.2 Öffentlich-private Partnerschaft (ÖPP)

Es gibt ein über KIRAS finanziertes internationales Forschungsprojekt und das .BK (Büro 3.2) stellt zwei Beiräte der privaten Meldestelle "STOPLINE" (www.stopline.at). Auch ist das Büro 3.2 ständiges Mitglied des "Runden Tischs – Ethik im Tourismus", etabliert im Bundesministerium für Wirtschaft, Familie und Jugend. Auch wird laufend an internationalen Meetings, welche von ECPAT organisiert werden, teilgenommen.

Überdies wird auf Homepages, in diversen Videospots sowie Foldern zahlreicher NGO wie ECPAT, STOPLINE (Providervereinigung) oder SAFER INTERNET ausdrücklich auf die .BK-Hotline meldestelle@interpol.at hingewiesen.

8.4. Fazit

- In den Jahren 2013-2016 wurden für Vertreter der Justiz mehrere Veranstaltungen zur Cyberkriminalität abgehalten. Die Schulung der Richter und Staatsanwälte erfolgt jedoch auf freiwilliger Grundlage. Damit ist sie auf eine begrenzte Zahl von Praktikern beschränkt, wodurch nicht gewährleistet ist, dass der mit Fällen von Cyberkriminalität und von durch den Cyberspace ermöglichter Kriminalität befasste Personenkreis über entsprechende allgemeine Kenntnisse verfügt. Richter und Staatsanwälte sind befugt, an den von externen Quellen – wie etwa ERA oder EJTN – veranstalteten Schulungsprogrammen teilzunehmen, und sie sollten aktiv ermutigt werden, die betreffenden Angebote auch zu nutzen.

- Unter Berücksichtigung der Zahl der Veranstaltungen zur Schulung der Richter und Staatsanwälte in den letzten Jahren und ihrer Teilnehmerzahl vertreten die Gutachter die Auffassung, dass das Schulungsangebot auf dem Gebiet der Cyberkriminalität nicht ausreicht. Speziell könnten mehr Finanzmittel für Staatsanwälte erwogen werden, da die Zielvision der Sicherheitsstrategieerklärung nicht erreicht werden kann, wenn die Staatsanwaltschaft sich in Fällen von Cyberkriminalität nicht erfolgreich vor Gericht durchsetzen kann.

- Weiters gibt es eine Grundausbildung für alle Kategorien von Polizeibeamten in Bezug auf ausgewählte Aspekte der Cyberkriminalität. Es gibt Kurse und Seminare für Ersteinschreiter. Derzeit gibt es in Österreich 300 Ersteinschreiter auf Bezirks- und Stadtebene. Für die praktische und theoretische Ausbildung der Ersteinschreiter soll mehr Zeit vorgesehen werden. Dies soll 2017 geschehen.

- Bei der Polizei-Grundausbildung umfasst die Anfangsphase der Ausbildung insgesamt acht Stunden. Ferner fehlt es der Polizei vor Ort an geeigneter Schulung zur angemessenen Behandlung von Fällen von Cyberkriminalität. Nach Auffassung der Gutachter sollte in Zukunft eine Verbesserung der betreffenden Ausbildungskomponenten in Betracht gezogen und speziell die für diese Polizei-Grundausbildung angesetzte Zeitdauer erhöht werden.

- In Anbetracht des beeindruckenden Niveaus der Cyberkriminalitätsschulung für die Angehörigen der Polizei vertreten die Gutachter die Auffassung, dass ein integrierter Ansatz für die gemeinsame Schulung von Richtern, Staatsanwälten und Vertretern der Strafverfolgungsbehörden als Plattform für die Erörterung der Hindernisse betreffend die Zulässigkeit von Beweismitteln und den Austausch von Erfahrungen die Widerstandsfähigkeit des österreichischen Systems der Cyberkriminalitätsbekämpfung verstärken könnte.

- Nach Auffassung der vom Gutachterausschuss gehörten Staatsanwälte sollte die Strafverfolgung über mehr IT-Forensiker und mehr spezialisierte Ermittler verfügen. Dies ist anscheinend in der ganzen EU ein Problem. Gut ausgebildete und spezialisierte Forensiker auf dem Gebiet der Cyberkriminalität sind in der Privatwirtschaft stark nachgefragt. Es ist schwierig für die öffentliche Hand, mit den von der Privatwirtschaft gebotenen finanziellen Möglichkeiten zu konkurrieren.

- Der Gutachterausschuss möchte die Zusammenarbeit zwischen C4 und den Universitäten, die darauf abzielt, neue Ermittlungswerkzeuge auf dem Gebiet der Bekämpfung der Cyberkriminalität zu entwickeln, besonders würdigen. Der Ausschuss nimmt ferner Kenntnis von den zahlreichen öffentlich-privaten Partnerschaften, die sich mit der Sensibilisierung (z. B. das Projekt "Click & Check"), der Schulung für die Strafverfolgungsbehörden und der Prävention (Prävention gegen Cyberkriminalität – Projekt "Cyber.Sicher") befassen. Nach Auffassung der Gutachter stellt diese Art der gemeinsam mit der Privatwirtschaft organisierten Zusammenarbeit ein Beispiel für vorbildliche Praxis dar.

- Österreich verfügt über eine Reihe ausgezeichneter Sensibilisierungsprogramme sowohl im Bildungsbereich als auch im Bereich der Cyber-Abwehr (Cyber Defence) sowie über mehrere Einrichtungen, die Veröffentlichungen und Webseiten auf Kinderpornografie und nationalsozialistisches Gedankengut hin überwachen, um die Entfernung solcher Inhalte zu erleichtern.

9. SCHLUSSBEMERKUNGEN UND EMPFEHLUNGEN

9.1. Vorschläge Österreichs

Nach Auffassung der österreichischen Behörden eröffnet der Cyber-Raum eine Vielzahl von Chancen und Möglichkeiten. Um die Vorteile, die unsere globalisierte Welt verspricht, nutzen zu können, muss die digitale Infrastruktur verlässlich und sicher funktionieren. Die Gewährleistung von Cybersicherheit ist daher eine zentrale gemeinsame Herausforderung für Staat, Wirtschaft und Gesellschaft.

Eine der Methoden zur Gewährleistung der Cybersicherheit besteht darin, die internationale Zusammenarbeit zu verstärken, sobald Cyberkriminalität im Spiel ist. Die Erfahrungen mit dem gemeinsamen Ermittlungsteam "MOZART" haben erwiesen, dass die Bekämpfung von Cyberkriminalität nur durch grenzüberschreitende koordinierte Zusammenarbeit erfolgen kann. Durch die in den Ermittlungen im Rahmen des gemeinsamen Ermittlungsteams "MOZART" gewonnenen Erfahrungen und Erkenntnisse konnte die Gliederung der kriminellen Struktur des Internetbetruges offengelegt und auch der Modus Operandi eruiert werden. Weltweit konnten aufgrund der Ermittlungen des JIT Mozart hunderte Fälle des Internetbetruges aufgeklärt werden. Darüber hinaus werden das Wissen und die Erkenntnisse aus der Ermittlung Bediensteten der Strafverfolgungsbehörden in Schulungen, insbesondere von Staatsanwälten, Bediensteten von Europol, FBI und des USPIS (United States Postal Inspection Service), präsentiert.

9.2. Empfehlungen

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

Österreich 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 österreichischen 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 Österreich

1. Es sollte an zuverlässigen und umfassenden statistischen Erhebungen bei den verschiedenen an der Bekämpfung der Cyberkriminalität beteiligten Akteuren (wie dem Innenministerium, dem Justizministerium, der Polizei und Meldestellen für die gleichen Berichtsthemen) gearbeitet werden, um sich einen klareren Überblick über die Entwicklung dieses Phänomens in Österreich zu verschaffen (vgl. 3.3.2 und 3.5);

2. es sollte erwogen werden, Staatsanwälte zu ernennen, die auf die Bekämpfung der Cyberkriminalität spezialisiert sind, und/oder den Kenntnisstand und die Zahl der Fachstaatsanwälte und -richter für die einzelnen Arten der Cyberkriminalität zu erhöhen, indem beispielsweise ein Netzwerk für Cyberkriminalität aufgebaut wird, in dem alle einschlägigen Informationen und bewährten Verfahren zusammengetragen werden (vgl. 4.1.1 und 4.5);

3. es sollte erwogen werden, mehr IT-Forensiker bei der Polizei einzusetzen, um eine rasche Reaktion und eine kürzere Zeitdauer für Forensik-Berichte zu gewährleisten (vgl. 4.2 und 4.5);

4. es sollte geprüft werden, ob das Erfordernis, die strafrechtliche Haftung für den illegalen Zugang zu einem Informationssystem nach Zustimmung der Geschädigten einzuführen, in umfangreichen Fällen mit einer hohen Zahl von Opfern zu Verwaltungsproblemen führen würde (vgl. 5.1.2 und 5.5);

5. es sollte dazu angeregt werden, im Anschluss an die laufenden Beratungen auf EU-Ebene an einem neuen Gesetz über die Vorratsdatenspeicherung zu arbeiten (vgl. 5.2.1 und 5.5);

6. es sollte erwogen werden, bei Strafverfahren die Möglichkeit vorzusehen, dass der Zugang zu Internetseiten mit strafrechtlich verbotenen Inhalten – beispielsweise in Fällen von Kinderpornografie, in denen Interpol eine schwarze Liste der Seiten erstellt – gesperrt wird (vgl. 6.2.4 und 6.4);

7. es sollte erwogen werden, die Zusammenarbeit mit dem Finanzsektor weiter zu verbessern, indem beispielsweise andere Methoden entwickelt werden, um sicherzustellen, dass vom Finanzsektor nicht bemerkte Cyberkriminalitätsaktivitäten an die Strafverfolgungsbehörden verwiesen und von diesen geprüft und erforderlichenfalls bearbeitet werden (vgl. 6.1.1 und 6.4);

8. es sollten die Schulungsmöglichkeiten für Richter und Staatsanwälte durch Abhaltung von mehr Veranstaltungen oder Schulungsmodulen ausgebaut werden und es sollte die Polizei-Grundausbildung ausgeweitet werden (vgl. 8.1 und 8.4);

9. es sollte erwogen werden, einen integrierten Ansatz für die gemeinsame Schulung von Richtern, Staatsanwälten und Vertretern der Strafverfolgungsbehörden als Plattform für die Erörterung der Hindernisse betreffend die Zulässigkeit von Beweismitteln und den Austausch von Erfahrungen in Bezug auf Cyberkriminalität zu schaffen (vgl. 8.1 und 8.4).

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

1. Die Mitgliedstaaten werden ermutigt, die Einrichtung eines Dienstes zur Unterstützung von geschädigten Verbrauchern in Bezug auf im Internet abgewickelte Geschäftsvorgänge oder bei anderen im Internet festgestellten verdächtigen Vorgängen entsprechend dem in Österreich entwickelten Konzept des Internet-Ombudsmanns in Betracht zu ziehen (vgl. 3.2 und 3.5);

2. die Mitgliedstaaten sollten erwägen, gut ausgebildete und gut ausgestattete Einheiten innerhalb der Strafverfolgungsbehörden einzurichten, um die Cyberkriminalität auf regionaler/lokaler Ebene wirksamer zu bekämpfen, wie dies bei den in der Polizeistruktur Österreichs eingerichteten Ersteinschreitern für Cyberkriminalität der Fall ist (vgl. 4.2 und 4.5);

3. den Mitgliedstaaten wird empfohlen, Werkzeuge und Maßnahmen für den Schutz von Kindern und Jugendlichen gegen erneute Viktimisierung bei Gerichtsverfahren zu entwickeln, wie dies bei Strafverfahren in Österreich der Fall ist, indem zur Anhörung von Opfern des sexuellen Missbrauchs von Kindern Psychologen hinzugezogen werden (vgl. 6.2.1 und 6.4);

4. den Mitgliedstaaten wird empfohlen, ihre Zusammenarbeit mit den Nachbarländern zu verbessern, um ihre Politik zur Bekämpfung der Cyberkriminalität zu verstärken, wie Österreich dies mit Deutschland oder der Schweiz praktiziert (vgl. 6.4 und 7.6);

5. den Mitgliedstaaten wird empfohlen, öffentlich-private Partnerschaften zu nutzen, um die Zusammenarbeit mit privaten Organisationen bei der Bekämpfung von Kinderpornografie und Kindesmissbrauch im Internet auf- oder auszubauen, wie dies in Österreich mit den Internetdiensteanbietern praktiziert wird (vgl. 6.2.4 und 6.4);

6. die Mitgliedstaaten werden ermutigt, auszuloten, ob häufiger auf Eurojust und das über Eurojust verfügbare Instrumentarium zurückgegriffen werden kann, um eine raschere Antwort auf Rechtshilfeersuchen oder finanzielle Unterstützung durch Eurojust zu erhalten (vgl. 7.1.3, 7.2 und 7.6);

7. die Organe und Einrichtungen der EU sollten sich so bald wie möglich mit der Frage der Vorratsdatenspeicherung befassen (vgl. 5.1.2 und 5.5).

ANNEX A: PROGRAMME FOR THE ON-SITE VISIT AND PERSONS INTERVIEWED/MET

7th Round of Mutual Evaluations ("Cybercrime")

Evaluation Visit to Austria, Vienna (18 – 20 May 2016)

Wednesday, May 18th, 2016:

10 00 – 12 30 a.m. (with coffee break): discussions of the evaluation team with representatives of the Austrian Ministry of Justice *(Ministry of Justice, Neustiftgasse 2, 1070 Vienna [Room Nr. 615]);*

12 45 – 14 15 p.m.: lunch at the *Justizcafé* (offered by the AT Ministry of Justice);

14 30 – 17 00 p.m. (with coffee break): discussions of the evaluation team with representatives of the Vienna Public Prosecutor's Office;

Thursday, May 19th, 2016:

10 00 – 12 30 a.m. (with coffee break): discussions of the evaluation team with representatives of the Austrian Ministry of the Interior *(Ministry of the Interior Minoritenplatz 9, [Room Nr. 588]);*

- *Presentation Bundeskriminalamt - C4 (Manfred PINNEGGER / Gert SEIDL)*
- *Presentation Bundesamt für Verfassungsschutz und Terrorismusbekämpfung – CSC (Philipp BLAUENSTEINER)*

12 30 – 14 30 p.m.: working lunch (offered by the AT Ministry of the Interior);

14 30 – 17 00 p.m.: (with coffee break): meeting with representatives of the Austrian Ministry of the Interior (including experts for awareness raising campaigns) and the national CERT *(Ministry of the Interior);*

- *14.30-15.00: presentation Austrian Cyber-Security Strategy (Kurt HAGER/BMI)*
- *15.00-15.30: presentation national CERT (Otmar LENDL/CERT)*
- *15.30-16.00: presentation project "Safer Internet" (Bernhard JUNGWIRTH/OIAT)*
- *16.00-16.30: presentation project "Cyberkids" (Gert SEIDL/BK)*
- *16.30-17.00: presentation on countering child abuse online by STOPLINE (tbc)*

Friday, May 20th, 2016:

10 00 – 12 00 a.m. (with coffee break): wrap-up session with representatives of the Austrian Ministry of Justice and the Austrian Ministry of the Interior *(Ministry of Justice [Room Nr. 542]);*

12 00: end of the meeting

ANNEX B: PERSONS INTERVIEWED/MET

Meetings on 18 of May, 2016

Venue: Ministry of Justice

Person interviewed/met	Organisation represented
Ms. Irene Gartner	Expert (Department for multilateral instruments on cooperation in criminal matters, including mutual recognition
Mr. Johannes Martetschläger	Expert (Department for individual cases of cooperation in criminal matters, including mutual recognition)
Mr. Clemens Burianek	Expert (Departments for Penal Law and for Criminal Procedural Law)
Ms. Sondra Fornather-Lentner	Expert (Department for training of the judiciary
Ms. Linda Mittnik	Expert (Department for Personnel)
Ms. Brigitte Süssenbacher	Expert (Department responsible for the E-Commerce-Directive)
Ms. Andrea Rohner	Expert (Department for individual cases of cooperation in criminal matters, including mutual recognition)

Venue: Vienna Public Prosecutors' Office

Person interviewed/met	Organisation represented
Ms. Maria Luise Nittel	Head of the Public Prosecutor's Office
Mr. Gerd Hermann	Department for sexual offences
Mr. Florian Kranz	Organized Crime and Terrorism
Ms. Nina Bussek	Legal Assistance Department

Meetings on 19 of May, 2016

Venue: Ministry of Interior

Person interviewed/met	Organisation represented
Mr. Philipp Blauensteiner	Expert (BVT - Federal Agency for State Protection and Counter Terrorism)
Mr. Bernhard Jungwirth	Expert and director (OIAT – Austrian Institute for Applied Telecommunications)
Mr. Otmar Lendl	Expert (cert.at – Computer Emergency Response Team)
Mr. Antonio-Maria Martino	EU policy matters and coordination (Head of Unit - Federal Ministry of the Interior)
Mr. Manfred Pinnegger	Expert (Federal Criminal Agency)
Mr. Paul Schliefssteiner	Assistant to Mr. MARTINO (Federal Ministry of the Interior)
Ms. Barbara Schloszbauer	Head of project „Stopline“ (nic.at – Austria’s domain administration)
Mr. Maximilian Schubert	Secretary General of ISPA (Internet Service Providers Austria - governing body of Austria’s Internet industry
Mr. Gert Seidl	Expert (Federal Criminal Agency)

Meetings on 20 of May, 2016

Venue: Ministry of Justice

Person interviewed/met	Organisation represented
Ms. Irene Gartner	Expert (Department for multilateral instruments on cooperation in criminal matters, including mutual recognition
Mr. Johannes Martetschläger	Expert (Department for individual cases of cooperation in criminal matters, including mutual recognition)
Mr. Clemens Burianek	Expert (Departments for Penal Law and for Criminal Procedural Law)
Mr. Gert Seidl	Expert (Federal Criminal Agency)

ANNEX C: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	AUSTRIAN OR ACRONYM IN ORIGINAL LANGUAGE	AUSTRIAN OR ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
ACSS	*ÖSCS*	Österreichische Strategie für Cyber Sicherheit	Austrian Cyber Security Strategy
APCIP	*APCIP*		Austrian Programme for Critical Infrastructure Protection
ARHG	*ARHG*		Austrian Extradition and Mutual Assistance Act
BMI	*BMI*		Federal Ministry of the Interior
BVT	*BVT*		Federal Agency for State Protection and Counter Terrorism
CKM	*CKM*		cyber crisis mechanism
CDZ	*CDZ*		Cyber Defence Centre
CSC	*CSC*		Cyber Security Centre
ECG	*ECG*		E-Commerce Act
IOCTA	*IOCTA*		Internet Organised Crime Threat Assessment
KIRAS	*KIRAS*		Austrian Security Research Programme
LKAs	*LKAs*	Landeskriminalämter	Regional Criminal Offices

SIAK	*SIAK*		The Security Academy
SKKM	*SKKM*		National Crisis and Disaster Protection Mechanism
StPO	*StPO*	Strafprozessordnung	Code of Criminal Procedure
TKG	*TKG*		Telecommunications Act
VJ	*VJ*	Verfahrensautomation Justiz	Justice department database
WKStA	*WKStA*		The Central Public Prosecutor's Office for the Prosecution of Economic Crimes and Corruption

ANNEX D: AUSTRIAN LEGISLATION

The content of the provisions cited in chapter 5.1.2

1. Illegal access to information system:

Covered by Section 118a of the Criminal Code ('Illegal access to a computer system'):

Section 118a (1) Anyone who, by overcoming a specific security measure, gains access to a computer system or to part of such a system, without being authorised to access it, or to access it alone, with the intention of:

1. procuring knowledge of personal data, for himself or another unauthorised party, thereby breaching the data subject's legitimate confidentiality interests; or

2. causing harm to another party by the use of data of which he has procured knowledge, which were saved in the system and not intended for him, shall be liable to imprisonment for a term of up to six months or to a fine of up to 360 daily rates.

(2) Anyone who commits the offence in relation to a computer system that is an essential component of critical infrastructure (point 11 of Section 74(1)) shall be liable to imprisonment for a term of up to two years.

(3) The perpetrator shall be prosecuted only if the aggrieved party has given his consent.

(4) Anyone who commits an offence under subsection (1) as a member of a criminal organisation shall be liable to imprisonment for a term of up to two years; anyone who commits an offence under subsection (2) as a member of a criminal organisation shall be liable to imprisonment for a term of up to three years.

2. Illegal system interference/illegal data interference:

Covered by Sections 126a and 126b of the Criminal Code ('Damage to data', 'Disruption of the operational capacity of a computer system):

Section 126a (1) Anyone who damages another by altering, deleting or otherwise making unusable or suppressing electronically processed, transmitted or supplied data without being authorised to access it, or to access it alone, shall be liable to imprisonment for a term of up to six months or to a fine of up to 360 daily rates.

(2) Anyone who causes damage to data exceeding EUR 5 000 by committing the offence shall be liable to imprisonment for a term of up to two years.

(3) Anyone who, by committing the offence, damages many computer systems using software, a computer password, an access code or comparable data providing access to a computer system or part thereof, if it is evident from their particular characteristics that those devices were created or adapted for the purpose, shall be liable to imprisonment for a term of up to three years.

(4) Anyone who:

1. causes damage exceeding EUR 300 000 by committing the offence;
2. damages essential components of critical infrastructure (point 11 of Section 74(1)) by committing the offence;

or

3. commits the offence as a member of a criminal organisation

shall be liable to imprisonment for a term of between six months and five years.

Section 126b (1) Anyone who severely disrupts the operational capacity of a computer system without being authorised to access it, or to access it alone, by entering or transmitting data shall be liable to imprisonment for a term of up to six months or to a fine of up to 360 daily rates, unless the offence is punishable under Section 126a.

(2) Anyone who causes long-lasting disruption to the operational capacity of a computer system by committing the offence shall be liable to imprisonment for a term of up to two years.

(3) Anyone who, by committing the offence, severely disrupts many computer systems using software, a computer password, an access code or comparable data providing access to a computer system or part thereof, if it is evident from their particular characteristics that those devices were created or adapted for the purpose, shall be liable to imprisonment for a term of up to three years.
(4) Anyone who:

1. causes damage exceeding EUR 300 000 by committing the offence;
2. commits the offence against a computer system that is an essential component of critical infrastructure (point 11 of Section 74(1)); or
3. commits the offence as a member of a criminal organisation

shall be liable to imprisonment for a term of between six months and five years.

(2a. Excursus: Critical infrastructure:
Definition in point 11 of Section 74(1) of the Criminal Code:
'critical infrastructure: establishments, facilities, systems or parts thereof, that are of significant importance for maintaining public security and national defence, for the proper functioning of public information and communication technology, for preventing or combating disasters, for the public health service, for the public water supply, energy supply or supply of essential goods, for the public waste collection system and wastewater system, or for the public transport system.')

3. Illegal interception of computer data:
Covered by Section 119a of the Criminal Code ('Illegal interception of data'):
Section 119a (1) Anyone who uses a device that has been attached to a computer system or has otherwise been enabled to receive a signal, or who intercepts electromagnetic emissions from a computer system, with the intention to procure, for himself or another unauthorised party, knowledge of data transmitted by means of that computer system and not intended for him, and, by using those data himself, making them accessible to another person for whom the data are not intended or publishing those data, to obtain a pecuniary advantage for himself or another person or to cause harm to another person, shall, unless the offence is punishable under Section 119, be liable to imprisonment for a term of up to six months or to a fine of up to 360 daily rates.
(2) The perpetrator shall be prosecuted only if the aggrieved party has given his consent.

4. Misuse of devices - production, distribution, procurement for use, import or otherwise making available or possession of computer misuse tools:

Covered by Section 126c of the Criminal Code ('Misuse of computer programs or access data'):

Section 126c (1) Anyone who produces, imports, markets, sells, otherwise makes available, procures or possesses

1. a computer program or comparable device of this nature that, given its particular characteristics, has evidently been created or adapted to commit the offence of unlawfully accessing a computer system (Section 118a), of breaching the privacy of telecommunications (Section 119), of illegal interception of data (Section 119a), of causing damage to data (Section 126a), of disruption of the operational capacity of a computer system (Section 126b) or of fraudulent misuse of data processing (Section 148a), or
2. a computer password, an access code or comparable data providing access to a computer system or a part thereof,

   with the intention of using them to commit one of the punishable acts referred to in point 1, shall be liable to imprisonment for a term of up to six months or to a fine of up to 360 daily rates.

(2) Anyone who, of their own volition, prevents the computer program referred to in subsection (1), the comparable device, or the password, the access code or the comparable data being used as described in Sections 118a, 119, 119a, 126a, 126b or 148a shall not be liable to punishment. If there is no risk of such use or if the risk was eliminated without any involvement of the perpetrator, he shall not be liable to punishment if, unaware of this fact, he made serious efforts of his own volition to eliminate the risk.

5. Computer-related production, distribution or possession of child pornography:

This comes under the general provision of Section 207a of the Criminal Code ('pornographic representations of minors'); there is no specific reference to commission of the offence by means of a computer:

Section 207a (1) Anyone who

1. produces pornographic representations of minors (subsection (4)) or
2. who offers to, obtains for, passes on to, shows to or otherwise makes available to another person such pornographic representations of minors (subsection (4)),

shall be liable to imprisonment for a term of up to three years.

(2) Anyone who produces, imports, transports or exports a pornographic representation of a minor (subsection (4)) for the purpose of dissemination or who commits an offence under subsection (1) on a commercial basis, shall be liable to imprisonment for a term of six months to five years. Anyone who commits the offence as a member of a criminal organisation or who does so in such a way that the minor suffers particularly serious harm as a result of the offence, shall be liable to imprisonment for a term of one to ten years; the same punishment shall be incurred by anyone who produces a pornographic representation of a minor (subsection (4)) using serious violence or who, when producing the representation, endangers the life of the minor depicted, either with intent or with gross recklessness (Section 6(3)).

(3) Anyone who obtains or possesses a pornographic representation of a minor who is aged over 14 but under 18 (points 3 and 4 of subsection (4)), shall be liable to imprisonment for a term of up to one year or to a fine of up to 720 daily rates. Anyone who obtains or possesses a pornographic representation of a person aged under 14 (subsection (4)) shall be liable to imprisonment for a term of up to two years.

(3a) Anyone who knowingly accesses pornographic representations of minors on the Internet shall be liable to the same punishment as provided for in subsection (3).

(4) Pornographic representations of minors are

1. realistic depictions of a sexual act on a person aged under 14 or by a person aged under 14 on themselves, on another person or with an animal,
2. realistic depictions of events involving a person aged under 14, the observation of which creates the impression, in the circumstances, that a sexual act is taking place on a person aged under 14 or is being performed by the person aged under 14 on themselves, on another person or with an animal,
3. realistic depictions

a) of a sexual act within the meaning of point 1 or of events within the meaning of point 2, but with minors aged over 14 but under 18 years, or

b) of the genitals or the genital area of minors,

to the extent that these are provocatively distorted depictions that are reduced solely to this content and are devoid of any indication of another context, which are intended to be used for the sexual arousal of the viewer;

4. images whose viewing - as a result of modification of a representation or without the use of such - creates the impression, in the circumstances, that they are depictions as described in points 1 to 3.

(5) Liability to punishment under subsections (1) and (3) shall not be incurred by anyone who

1. is in possession of a pornographic representation of a minor aged over 14 but under 18 with their consent that was produced for that minor's or the person's own use, or

1a. produces or possesses a pornographic representation of a minor aged over 14 but under 18 of themselves, or offers, procures, passes on, shows or otherwise makes available to another person such representation for their own use, or

2. produces or possesses, for their own use, a pornographic representation of a minor aged over 14 but under 18 as described in point 4 of subsection (4), as long as this act does not give rise to a risk of dissemination of the representation.

6. Computer-related solicitation or "grooming" of children:

Section 208a (1) Anyone who,

1. by means of telecommunications or using a computer system, or
2. by other means involving concealment of his or her intention,

suggests or agrees to a face-to-face meeting with a person aged under 14 and takes specific preparatory action to carry out the face-to-face meeting with that person, and does so with the intention of committing a criminal act against that person as defined in Sections 201 to 207a (1), point (1), shall be liable to imprisonment for a term of up to two years.

(1a) Anyone who establishes contact with a person aged under 14 by means of telecommunications or using a computer system, with the intention of committing a criminal act as defined in Section 207a (3) or (3a) concerning a pornographic representation (Section 207a (4)) of that person, shall be liable to imprisonment for a term of up to one year or to a fine of up to 720 daily rates.

(2) Anyone who, of their own volition and before the authority (Section 151(3)) has learned of that person's wrongdoing, renounces his intended action and confesses his wrongdoing to the authority, shall not be liable to punishment under Sections (1) and (1a).

7. Computer-related fraud or forgery

In the general definitions of fraud and forgery offences, there is no specific reference to commission of the offence using a computer. Offences the definition of which does include such a reference:

'Fraudulent misuse of data processing':

Section 148a (1) Anyone who, with the intention of unlawfully enriching himself or a third party, causes material loss to another person by influencing the results of an automated data processing operation, by means of programming; entering, altering, deleting or suppressing data; or otherwise affecting the course of the processing operation, shall be liable to imprisonment for a term of up to six months or to a fine of up to 360 daily rates.

(2) Anyone who commits the offence on a commercial basis, or causes a loss exceeding EUR 5 000 by committing the offence, shall be liable to imprisonment for a term of up to three years; anyone who causes a loss exceeding EUR 300 000 by committing the offence shall be liable to imprisonment for a term of between one and ten years.

'Falsification of data'

Section 225a Anyone who, by entering, altering, deleting or suppressing data, intentionally creates false data or falsifies genuine data for use in legal transactions to prove a right, a legal relationship or a fact, shall be liable to imprisonment for a term of up to one year.

8. Computer-related identity offences

Generally included in any case in the definition of the basic offence. General aggravating factor in identity fraud (point 8 of Section 33(1) StGB):

Section 33 (1) An aggravating factor shall be held to exist, in particular, if the offender

8. has, in the process of committing the offence, fraudulently used another person's personal data in order to gain the trust of a third party, and in so doing caused prejudice to the lawful owner of the identity.

Section 119 StGB - 'Breach of telecommunications secrecy'

Section 119 (1) Anyone who uses a device that has been attached to a telecommunications or computer system or otherwise enabled to receive a signal with the intention of procuring, for himself or for another unauthorised party, knowledge of a communication transmitted by means of that telecommunications or computer system which is not intended for him shall be liable to imprisonment for a term of up to six months or to a fine of up to 360 daily rates.

(2) The perpetrator shall be prosecuted only if the aggrieved party has given his consent.