Hochschule für Wirtschafts-,

Rechts- und Sozialwissenschaften

Die Problematik der grenzüberschreitenden Strafverfolgung von Cybercrime

---

Masterarbeit

vorgelegt von:

Yaelle Häring

Burggrabenstrasse 31a

8266 Steckborn

yaelle.haering@student.unisg.ch

11 607 868

Referent:

Prof. Dr. Marc Forster

Vorgelegt am: 16. November 2015

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abs.	Absatz
akt.	aktualisiert
A.M.	andere(r) Meinung
Art.	Artikel
AS	amtliche Sammlung des Bundesrechts
aStGB	altes StGB: Schweizerisches Strafgesetzbuch vom 21.12.1937 (wurde am 07.03.2014 per 01.07.2014 durch Bundesbeschluss geändert)
Aufl.	Auflage
BBl	Bundesblatt
Bd.	Band
bearb.	bearbeitet
BGE	Bundesgerichtsentscheid / Amtliche Sammlung der Entscheidungen des Schweizerischen Bundesgerichts (www.bger.ch)
BGer	Bundesgericht
BJ	Bundesamt für Justiz
BSK	Basler Kommentar
bspw.	beispielsweise
BstGer	Bundesstrafgericht
BÜPF	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs vom 01.07.1998, SR 780.1
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18.04.1999, SR 101
bzw.	beziehungsweise
CCC	Übereinkommen über Cyberkriminalität vom 23.11.2001, SR 0.311.43
CoE	Council of Europe
d.h.	das heisst

Diss.	Dissertation
Ds.	Drucksache
DuD	Datenschutz und Datensicherheit, Wiesbaden
E.	Erwägung
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EMRK	Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 04.01.1950 (Europäische Menschenrechtskonvention, EMRK), SR 01.101
erw.	erweitert
et al.	et alii, et aliae, et alia
etc.	et cetera
f. / ff.	folgend(e) / fortfolgend(e)
fedpol	Bundesamt für Polizei
Fn	Fussnote
gem.	gemäss
GwÜ	Übereinkommen über Geldwäscherei sowie Ermittlungen, Beschlagnahme und Einziehung von Erträgen aus Straftaten vom 08.11.1990, SR 0.311.53
Habil.	Habilitation
Hrsg.	Herausgeber
HSSR	Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht
i.d.R.	in der Regel
i.e.S.	im engeren Sinne
INTERPOL	Internationale kriminalpolizeiliche Organisation
IRS	Internal Revenue Services
IRSG	Bundesgesetz über internationale Rechtshilfe in Strafsachen (Rechtshilfegesetz) vom 20.03.1981, SR 351.1
IRSV	Verordnung über internationale Rechtshilfe in Strafsachen (Rechtshilfeverordnung) vom 24.02.1982, SR 351.11

ISO	Internationale Organisation für Normung
ISSS	Information Security Society Switzerland
ISTR	Internationales Strafrecht
i.S.v.	im Sinne von
i.w.S.	im weiteren Sinne
Jg	Jahrgang
Kap.	Kapitel
KMU	Kleine und mittlere Unternehmen
KOBIK	Nationale Koordinationsstelle zur Bekämpfung der Internetkriminalität
lit.	litera (Buchstabe)
Mm.	Medienmitteilung
m.w.H.	mit weiteren Hinweisen
N	Note
No./Nr.	Nummer
NZZ	Neue Zürcher Zeitung (Zürich)
PK	Praxiskommentar
Rs.	Rundschreiben
Rz.	Randziffer
s.	siehe
S.	Seite
sog.	sogenannte(r)
SR	systematische Sammlung des Bundesrechts
StGB	Schweizerisches Strafgesetzbuch vom 21.12.1937, SR 311.0
StPO	Schweizerische Strafprozessordnung (Strafprozessordnung, StPO) vom 5.10.2007, SR 312.0
SZ	Süddeutsche Zeitung
überarb.	überarbeitet

URG	Bundesgesetz über das Urheberrecht und verwandte Schutzrechte vom 09.10.1992, SR 231.1
vgl.	vergleiche
vollst.	vollständig
VÜPF	Verordnung über die Überwachung des Post- und Fernmeldeverkehrs vom 31.10.2001, SR 780.11
z.B.	zum Beispiel
Zf.	Zusammenfassung
Ziff.	Ziffer
zit.	zitiert
ZSR	Zeitschrift für Schweizerisches Recht, Basel
ZStrR	Schweizerische Zeitschrift für Strafrecht, Bern

Quellenverzeichnis

BALTISSER ANNINA, Datenbeschädigung und Malware im Schweizer Strafrecht – Der Tatbestand des Art. 144bis StGB im Vergleich mit den Vorgaben der Cybercrime Convention und der deutschen Regelung (Diss.), Zürich, Basel, Genf 2013. [zit.: BALTISSER, S.]

BREYER PATRICK, Die Cyber-Crime-Konvention des Europarats, in: Datenschutz und Datensicherheit (DuD), Jg. 25/2001, Ausgabe 10/2001, S. 592ff., Wiesbaden. [zit.: BREYER, DuD, S.]

CAPUS NADJA, Strafrecht und Souveränität: Das Erfordernis der beidseitigen Strafbarkeit in der internationalen Rechtshilfe in Strafsachen (Habil.), Bern 2010. [zit.: CAPUS, S.]

DONATSCH ANDREAS / HEIMGARTNER STEFAN / MEYER FRANK / SIMONEK MADELEINE, Internationale Rechtshilfe – unter Einbezug der Amtshilfe im Steuerrecht, 2. Aufl., Zürich, Basel, Genf 2015. [zit.: DONATSCH et al., S.]

FABBRI ALBERTO / FURGER ANDREA, Geheime Überwachungsmassnahmen in der internationalen Kooperation in Strafsachen: Ermittlungserfolg im Ausland versus Rechtsgüterschutz in der Schweiz, in: Schweizerische Zeitschrift für Strafrecht (ZStrR), Jg. 128, Heft 04/10, S. 394ff., Bern 2010 [zit.: FABBRI/FURGER, ZStrR, S.]

FORSTER MARC, Marksteine der Bundesgerichtspraxis zur strafprozessualen Überwachung des digitalen Fernmeldeverkehrs – Probleme der grenzüberschreitenden Strafverfolgung bei Delikten über soziale Netzwerke und den mobilen Internetverkehr, in: GSCHWEND LUKAS / HETTICH PETER / MÜLLER-CHEN MARKUS / SCHINDLER BENJAMIN / WILDHABER ISABELLE (Hrsg.), Festgabe zum Schweizerischen Juristentag 2005 in St. Gallen, S. 615ff., Zürich 2015. [zit.: FORSTER, S.]

GLESS SABINE, Internationales Strafrecht – Grundriss für Studium und Praxis, 2., vollst. überarb. Aufl., Basel 2015. [zit.: GLESS, Rz.]

GISIN MARKUS, Phishing und Skimming – Die Strafbarkeit aktueller Deliktformen im elektronischen Zahlungsverkehr (Masterarbeit), Luzern 2007. [zit.: GISIN, S.]

GSTÖHL CAROLINE, Geheimnisschutz im Verfahren der internationalen Rechtshilfe in Strafsachen, Bern 2008. [zit.: GSTÖHL, S.]

HEIMGARTNER STEFAN, Die Internationale Dimension von Internetstraffällen – Strafhoheit und internationale Rechtshilfe in Strafsachen, in: SCHWARZENEGGER CHRISTIAN /ARTER OLIVER / JÖRG FLORIAN S. (Hrsg.), Internet-Recht und Strafrecht – 4. Tagungsband 2004, S. 117ff., Bern 2005. [zit.: HEIMGARTNER, S.]

HEIMGARTNER STEFAN / NIGGLI MARVEL ALEXANDER (Hrsg.), Basler Kommentar: Internationales Strafrecht IRSG/GwÜ, Basel 2015. [zit.: BSK ISTR – AUTOR/IN, Art. IRSG N]

HILGENDORF ERIC / VALERIUS BRIAN, Computer- und Internetstrafrecht – Ein Grundriss, 2. Aufl., Berlin 2012. [zit.: HILGENDORF/VALERIUS, Rz.]

HILGENDORF ERIC / FRANK THOMAS / VALERIUS BRIAN, Computer- und Internetstrafrecht – Ein Grundriss, Berlin 2005. [zit.: HILGENDORF et al., Rz.]

KRONIG PHILIPPE / BOLLMANN EVA, Die Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK), in: SCHWARZENEGGER CHRISTIAN /ARTER OLIVER / JÖRG FLORIAN S. (Hrsg.), Internet-Recht und Strafrecht – 4. Tagungsband 2004, S. 19ff., Bern 2005. [zit.: KRONIG/BOLLMANN, S.]

MARBETH-KUBICKI ANETTE, Computer- und Internetstrafrecht, München 2005. [zit.: MARBETH-KUBICKI, N]

POPP PETER, Grundzüge der internationalen Rechtshilfe in Strafsachen, Basel 2001. [zit.: POPP, Rz.]

REINDL-KRAUSKOPF SUSANNE, Computerstrafrecht im Überblick, 2., überarb. Aufl., Wien 2009. [zit.: REINDL-KRAUSKOPF, S.]

SCHMID NIKLAUS, Das neue Computerstrafrecht, in: Schweizerische Zeitschrift für Strafrecht (ZStrR), Jg. 113 (1995), Heft 01/95, S. 22ff., Bern 1995. [zit.: SCHMID, ZStrR, S.]

SCHUH DANIEL, Computerstrafrecht im Rechtsvergleich: Deutschland, Österreich, Schweiz (Diss.), in: Schriften zum Strafrecht, Heft 228, Berlin 2012. [zit.: SCHUH, S.]

SCHWARZENEGGER CHRISTIAN, Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime vom 23. November 2001, in: DONATSCH ANDREAS / FORSTER MARC / SCHWARZENEGGER CHRISTIAN (Hrsg.), Strafrecht, Strafprozessrecht und Menschenrechte – Festschrift für STEFAN TRECHSEL zum 65. Geburtstag, S. 305ff., Zürich, Basel, Genf 2002. [zit.: SCHWARZENEGGER, S.]

SCHWARZENEGGER CHRISTIAN, Die Internationalisierung des Wirtschaftsrechts und die schweizerische Kriminalpolitik: Cyberkriminalität und das neue Urheberstrafrecht,

in: Zeitschrift für Schweizerisches Recht (ZSR), Jg. 127 (2008) II, Heft 2, S. 399ff., Basel 2008. [zit.: SCHWARZENEGGER, ZSR, S.]

Springer Fachmedien Wiesbaden (Hrsg.), Kompakt-Lexikon – Wirtschaftsinformatik: 1'500 Begriffe nachschlagen, verstehen, anwenden, Wiesbaden 2013. [zit.: Springer Fachmedien Wiesbaden, S.]

STRATENWERTH GÜNTER / JENNY GUIDO / BOMMER FELIX, Schweizerisches Strafrecht, Besonderer Teil I: Straftaten gegen Individualinteressen, 7., ergänzte und überarb. Aufl., Bern 2010. [zit.: STRATENWERTH et al., § N]

STRATENWERTH GÜNTER / WOHLERS WOLFGANG, Schweizerisches Strafgesetzbuch – Handkommentar, 3. Aufl., Bern 2013. [zit.: STRATENWERTH/WOHLERS, Art. StGB N]

TRECHSEL STEFAN / PIETH MARK (Hrsg.), Schweizerisches Strafgesetzbuch – Praxiskommentar, 2. Aufl., Zürich, St. Gallen 2013. [zit.: StGB PK – AUTOR/IN, Art. StGB N]

VATIS MICHAEL A., The Council of Europe Convention on Cybercrime, in: STEINBRUNER JOHN D. / BELLOVIN STEVEN M. / DYCUS STEPHEN / ECKERT SUE / GOLDSMITH III JACK L. / JERVIS ROBERT / LODAL JAN M. / VENABLES PHILIP (Hrsg.), Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, S. 207ff., Washington D.C. 2010. [zit.: VATIS, S.]

VETTER JAN, Gesetzeslücken bei der Internetkriminalität (Diss.), in: Schriftenreihe – Strafrecht in Forschung und Praxis, Bd. 27, Hamburg 2003. [zit.: VETTER, S.]

Materialverzeichnis

Botschaft über die Änderung des Schweizerischen Strafgesetzbuches und des Militärstrafgesetzes (Strafbare Handlungen gegen das Vermögen und Urkundenfälschung) sowie betreffend die Änderung des Bundesgesetzes über die wirtschaftliche Landesversorgung (Strafbestimmungen) vom 24. April 1991, in: BBl 1991 II 969, S. 969ff. [zit.: BBl 1991 II 969, S.]

Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18. Juni 2010, in: BBl 2010 4697, S. 4697ff. [zit.: BBl 2010 4697, S.]

Botschaft zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 27. Februar 2013, in BBl 2013 2683, S. 2683ff. [zit.: BBl 2013 2683, S.]

Botschaft zur Genehmigung des Übereinkommens des Europarats zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch (Lanzarote-Konvention) sowie zu seiner Umsetzung (Änderung des Strafgesetzbuches) vom 04. Juli 2012, in: BBl 2012 7571, S. 7571ff. [zit.: BBl 2012 7571, S.]

Bundesamt für Justiz (BJ), Die internationale Rechtshilfe in Strafsachen, Wegleitung, 2009, abgerufen am 12.11.2015 von: <http://www.rhf.admin.ch/etc/medialib/data/rhf.Par.0085.File.tmp/wegl-str-d-2009.pdf>. [zit.: Wegleitung, S.]

Bundesamt für Justiz, Rundschreiben Nr. 2: Cyber Crime Convention, vom 31. Oktober 2012, abgerufen am 12.11.2015 von: <http://www.rhf.admin.ch/etc/medialib/data/rhf/recht.Par.0025.File.tmp/kreisschreiben-cyber-crime-convention-d.pdf>. [zit.: BJ, Rs. Nr. 2, S.]

Bundesbeschluss über die Genehmigung und die Umsetzung des Übereinkommens des Europarats über die Cyberkriminalität vom 18. März 2011, in: AS 2011 6293, S. 6293ff. [zit.: AS 2011 6293, S.]

Bundesbeschluss über die Genehmigung und Umsetzung des Übereinkommens des Europarats zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch (Lanzarote-Konvention) vom 27. September 2013, in: AS 2014 1159 (BBl 2013 7395). [zit.: AS 2014 1159]

Council of Europe (CoE), Convention on Cybercrime – Explanatory Report, vom 8. November 2001, Budapest 2001. [zit.: ETS No. 185, Ziff.]

Council of Europe (CoE), Zusatzprotokoll zum Übereinkommen über Computerkriminalität betreffend die Kriminalisierung mittels Computersystemen begangener Handlungen rassistischer und fremdenfeindlicher Art, vom 28. Januar 2003, Strassburg 2003. [zit.: CoE, Zusatzprotokoll vom 28.01.2003]

Eidgenössisches Justiz- und Polizeidepartement (EJPD) / Bundesamt für Justiz (BJ), Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens zum erläuternden Bericht und zum Vorentwurf über die Änderungen des Schweizerischen Strafgesetzbuches und des Rechtshilfegesetzes, Genehmigung und Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität, vom 10. April 2010, abgerufen am 12.11.2015 von: <https://www.bj.admin.ch/dam/data/bj/sicherheit/gesetzgebung/archiv/cybercrime-europarat/ve-res-d.pdf>. [zit.: EJPD/BJ, Zf. Vernehmlassungsverfahren, S.]

Gesetzesentwurf der Bundesregierung: Entwurf eines Gesetzes zu dem Übereinkommen des Europarats vom 23. November 2001 über Computerkriminalität, Deutscher Bundestag, 16. Wahlperiode, Drucksache 16/7218, 16.11.2007. [zit.: Deutscher Bundestag, Ds. 16/7218]

Rahmenbeschluss 2005/222/JI des Rates vom 24.02.2005 über Angriffe auf Informationssysteme, in: Amtsblatt der Europäischen Union, vom 16.03.2005, abgerufen am 12.11.2015 von: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:00 71:DE:PDF>. [zit.: Rahmenbeschluss 2005/222/JI]

Internetverzeichnis

Eidgenössisches Justiz- und Polizeidepartement (EJPD), Medienmitteilungen vom 14.11.2001: Gemeinsam die Cyber-Kriminalität bekämpfen - Bundesrat genehmigt Konvention des Europarates, abgerufen am 12.11.2015 von: <https://www.bj.admin.ch/bj/de/home/aktuell/news/2001/67.html>. [EJPD, Mm. vom 14.11.2001]

Eidgenössisches Justiz- und Polizeidepartement (EJPD), Medienmitteilungen vom 13.03.2009: Die Cyberkriminalität über die Grenzen hinweg bekämpfen – Vernehmlassung zur Umsetzung der Europaratskonvention eröffnet, abgerufen am 12.11.2015 von: <https://www.bj.admin.ch/bj/de/home/aktuell/news/2009/ref_2009-03-13.html>. [zit.: EJPD, Mm. vom 13.03.2009]

Eidgenössisches Justiz- und Polizeidepartement (EJPD), Medienmitteilungen vom 18.06.2010: Die Cyberkriminalität über die Grenzen hinweg verstärkt bekämpfen – Bundesrat verabschiedet Botschaft zur Ratifikation der Europaratskonvention, abgerufen am 12.11.2015 von: <https://www.bj.admin.ch/bj/de/home/aktuell/news/2010/ref_2010-06-181.html>. [zit.: EJPD, Mm. vom 18.06.2010]

Der Bundesrat, Medienmitteilungen vom 15.09.2011: Die Cyberkriminalität verstärkt bekämpfen – Europaratskonvention tritt für die Schweiz am 1. Januar 2012 in Kraft, abgerufen am 12.11.2015 von: <https://www.bj.admin.ch/bj/de/home/aktuell/news/2011/ref_2011-09-15.html>. [zit.: Der Bundesrat, Mm. vom 15.09.2011]

Der Bundesrat, Medienmitteilung vom 07.03.2014: Freier von 16- bis 18-jährigen Prostituierten werden künftig bestraft, abgerufen am 12.11.2015 von: <http://www.ejpd.admin.ch/ejpd/de/home/aktuell/news/2014/2014-03-070.html>. [zit.: Der Bundesrat, Mm. vom 07.03.2014]

ERDI, Transbonder data access: Strong critics on plans to extend CoE Cybercrime Treaty, in: ERDI (Hrsg.), Protecting Digital Freedom, Artikel vom 05.06.2013, abgerufen am 12.11.2015 von: <https://edri.org/edrigramnumber11-11transborder-data-access-cybercrime-treaty/>. [zit.: ERDI, Protecting Digital Freedom]

Handelszeitung, Hacker haben Konten von Schweizer KMU im Visier, in: Handelszeitung, Ausgabe vom 02.02.2015, abgerufen am 12.11.2015, von: <http://www.handelszeitung.ch/unternehmen/hacker-haben-konten-von-schweizer-kmu-im-visier-734074>. [zit.: Handelszeitung, 02.02.2015]

HERZOG FELIX, Straftaten im Internet, Computerkriminalität und die Cybercrime Convention, abgerufen am 12.11.2015 von: <http://www.politicacriminal.cl/n_08/d_1_8.pdf>. [zit.: HERZOG, S.]

HIRSTEIN ANDREAS, Rechtshilfe gegen Internetkriminalität im Internet – Der Bund will die Cyber-Konvention umsetzen. Dagegen wehrt sich die Wirtschaft. Sie fürchtet um das Bankgeheimnis, in: Neue Zürcher Zeitung, Nr. 43, S. 72, vom 25.10.2009, abgerufen am 12.11.2015 von: <http://www.nzz.ch/rechtshilfe-gegen-kriminalitaet-im-internet -1.3918996>. [zit.: HIRSTEIN, NZZ]

Information Security Society Switzerland (ISSS), Vernehmlassung zum Entwurf des Bundesbeschlusses über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität (ECC), Bern 2009, abgerufen am 12.11.2015, von: <https://www.isss.ch/fileadmin/publ/sigccc/ECC-Vernehmlassung-ISSS.pdf>. [zit.: ISSS[1], S.]

Information Security Society Switzerland (ISSS), Pressemitteilung: Beitritt der Schweiz zur Europaratskonvention über die Cyberkriminalität nicht ohne Anpassung des Schweizer Strafrechts an die aktuellen Formen der Computer- und Netzwerkkriminalität, Thalwil 2009, abgerufen am 12.11.2015, von: <https://www.isss.ch/fileadmin/publ/sigccc/Pressemitteilung-ECC-der-ISSS.pdf>. [zit.: ISSS[2], S.]

Internationale Organisation für Normung (ISO), Information technology – Vocabulary, abgerufen am 11.11.2015 von: <https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en>. [zit.: ISO/IEC 2382:2015]

Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK), KOBIK, abgerufen am 12.11.2015, von: <https://www.cybercrime.admin.ch/kobik/de/home/ueberuns/kobik.html>. [zit.: KOBIK[1]]

Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK), Warnmeldungen 2015, abgerufen am 12.11.2015 von: <https://www.cybercrime.admin.ch/kobik/de/home/warnmeldungen/2015.html>. [zit.: KOBIK[2]]

Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK), Zuständigkeiten der Kantone und des Bundes, abgerufen am 12.11.2015 von: <https://www.cybercrime.admin.ch/kobik/de/home/ueberuns/zustaendigkeit_.html>. [zit.: KOBIK[3]]

Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK), Jahresbericht 2014, Bern 2015, abgerufen am 2.11.2015 von: <https://www.cybercrime.admin.ch/dam/data/kobik/Berichte/2015-03-26/jb-2015-d.pdf>. [zit.: KOBIK, Jahresbericht 2014, S.]

Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK), Jahresbericht 2013, Bern 2014, abgerufen am 12.11.2015 von: <https://www.cybercrime.admin.ch/dam/data/kobik/Berichte/2014-18/rechenschaftsbericht-2013-d.pdf>. [zit.: KOBIK, Jahresbericht 2013, S.]

Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK), Jahresbericht 2012, Bern 2013, abgerufen ab 12.11.2015 von: <https://www.cybercrime.admin.ch/dam/data/kobik/Berichte/2008-12/rechenschaftsbericht-2012-d.pdf>. [zit.: KOBIK, Jahresbericht 2012, S.]

LEHMANN BEAT, European Cybercrime Convention (ECC – ETS 185) – Ein Werkstattbericht aus der Tätigkeit der für die Ausarbeitung einer Vernehmlassung zur Umsetzung des ECC in das schweizerische Recht im Sommer 2009 eingesetzten Special Interest Group der ISSS, St. Gallen 2010, abgerufen am 12.11.2015 von: <https://www.isss.ch/fileadmin/events/2010/StGallerTagung/ISSS_StGallerTagung2010_ECC_Lehmann.pdf>. [zit.: LEHMANN, S.]

NZZ, Bundesanwaltschaft führt Pilotverfahren gegen Kreditkartenbetrüger, in: Neue Zürcher Zeitung, Ausgabe vom 10.05.2015, abgerufen am 12.11.2015 von: <http://www.nzz.ch/wirtschaft/newsticker/bundesanwaltschaft-fuehrt-pilotverfahren-gegen-kreditkartenbetrueger-1.18539495>. [zit.: NZZ, 10.05.2015]

NZZ, CNN – Russische Hacker attackieren Computer des Weissen Hauses, in: Neue Zürcher Zeitung, Ausgabe vom 08.04.2015, abgerufen am 12.11.2015 von: <http://www.nzz.ch/newsticker/russische-hacker-attackieren-offenbar-computer-des-weissen-hauses-1.18517902>. [zit.: NZZ, 08.04.2015]

NZZ, Computernetzwerk des Pentagons – Hackerangriffe aus Russland, in: Neue Zürcher Zeitung, Ausgabe vom 24.04.2015, abgerufen am 12.11.2015 von: <http://www.nzz.ch/international/amerika/hackerangriff-aus-russland-1.18529018>. [zit.: NZZ, 24.04.2015]

NZZ, USA – Grossangelegte Cyber-Attacke auf Steuerbehörde, in: Neue Zürcher Zeitung, Ausgabe vom 27.05.2015, abgerufen am 12.11.2015 von: <http://www.nzz.ch/international/grossangelegte-cyber-attacke-auf-us-steuerbehoerde-1.18549639>. [zit.: NZZ, 27.05.2015]

SEIDL ALEXANDER / FUCHS KATHARINA, Die Strafbarkeit des Phishing nach Inkrafttreten des 41. Strafrechtsänderungsgesetzes, in: Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht (HSSR), Jg. 11, Ausgabe 2/2010, S. 85ff., abgerufen am 12.11.2015 von: <http://www.hrr-strafrecht.de/hrr/archiv/10-02/hrrs-2-10.pdf>. [zit.: SEIDL/FUCHS, HSSR, S.]

Süddeutsche Zeitung (SZ), Cyberangriff – Sicherheitsfirma Kaspersky Lab gehackt, in: Süddeutsche Zeitung, Ausgabe vom 10.06.2015, abgerufen am 12.11.2015 von: <http://www.sueddeutsche.de/digital/cyberangriff-sicherheitsfirma-kaspersky-lab-gehackt-1.2514908>. [zit.: SZ, 10.06.2015]

Tagesanzeiger, 200 Millionen Schaden wegen Internetkriminalität, in: Tagesanzeiger, Ausgabe vom 06.05.2015, abgerufen am 12.11.2015 von: <http://www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/200-Millionen-Franken-Schaden-wegen-Internetkriminalitaet/story/14113297>. [zit.: Tagesanzeiger, 06.05.2015]

WEBER AMALIE M., The Council of Europe's Convention on Cybercrime, Berkeley Technology Law Journal, Vol. 18, Iss. I, Art. 28, Berkeley 2003, abgerufen am 12.11.2015 von: <http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1416&context=btlj>. [zit.: WEBER, S.]

1 Einleitung

1.1 Problematik

„Das grösste Problem mit dem Fortschritt ist –

auch die Nachteile entwickeln sich weiter."

(ERNST FERSTL, Schriftsteller, *1955)

Innerhalb der letzten Jahre erlebte das Internet grosse technologische Fortschritte. Mit diesen einher ging die Entwicklung einer Vielzahl von neuen Kommunikationsmöglichkeiten. Wie die klassischen Kommunikationsmittel können auch diese für illegale Zwecke und zur Begehung von Straftaten missbraucht werden. Eine entsprechende Entwicklung ist deutlich erkennbar. So weist das Thema der Cyberkriminalität heute eine grosse Aktualität auf. Immer wieder wird man im Alltag mit dem Thema der Internetkriminalität konfrontiert. Vor allem in der ersten Hälfte des Jahres 2015 häuften sich in diversen Zeitungen die Meldungen über kriminelle Handlungen im Internet. Kaum ein Tag verging, an welchem nicht wieder über neue und noch grössere Fälle der Internetkriminalität berichtet wurde. Zu denken ist etwa an die Cyberattacke auf das Computersystem der US-Steuerbehörde IRS, bei welcher rund 100'000 Daten von Steuerzahlern gestohlen wurden,[1] die Ermittlungen der Schweizerischen Bundesanwaltschaft wegen des Diebstahls von Kreditkartendaten über das Internet,[2] oder aber auch an den Angriff russischer Hacker auf ein als nicht geheim eingestuftes Computernetzwerk des amerikanischen Verteidigungsministeriums.[3] Potentielle Ziele von Cyberattacken sind neben staatlichen Behörden auch Einzelpersonen oder KMUs, wie bspw. der Cyberangriff auf die russische Sicherheitsfirma Kaspersky Lab,[4] die Hacking-Attacken auf Konten von Schweizer KMUs[5] oder die immer wieder veröffentlichten Warnmeldungen auf der Internetseite von KOBIK verdeutlichen[6]. Die durch Cyberkriminalität verursachten Schäden werden von den Betroffenen allzu oft unterschätzt. Allein im Jahr 2014 wird

1 Vgl. NZZ, 27.05.2015.
2 Vgl. NZZ, 10.05.2015.
3 Vgl. NZZ, 24.04.2015.
4 Vgl. SD, 10.06.2015.
5 Vgl. Handelszeitung, 02.02.2015.
6 Vgl. KOBIK².

der durch die Internetkriminalität verursachte Schaden der Schweizerischen Volkswirtschaft auf rund CHF 200 Mio. geschätzt.[7]

Die Anzahl der im Internet ausgeübten Delikte nimmt jährlich zu. Wie einer Statistik der nationalen Meldestelle KOBIK[8] entnommen werden kann, gingen in der Schweiz allein im Jahr 2014 mehr als 10'200 Verdachtsmeldungen zur Internet- und Computerkriminalität ein. Dies entspricht einer Zunahme von mehr als 10 Prozent gegenüber dem Vorjahr. Über 87 Prozent der eingegangenen Verdachtsmeldungen wiesen dabei eine strafrechtliche Relevanz auf. Die gemeldeten Delikte hatten dabei nicht nur nationale, sondern auch internationale Auswirkungen.

Unter den Begriff der Cyberkriminalität sind viele Delikte subsumierbar. Der entscheidende Unterschied zu den sog. „klassischen" Straftaten des StGB liegt in der kaum wahrnehmbaren Überwindung von Landesgrenzen und den damit einhergehenden Problemen der Strafverfolgung der Täter. Während Landesgrenzen für Kriminelle in der Ausübung eines Internetdeliktes problemlos überschritten werden können, stellen sie für die hoheitliche Ermittlungskompetenz der nationalen Strafverfolgungsbehörden eine massgebliche Barriere dar. Nur dank Instrumenten der internationalen Rechtshilfe, welche das Überwinden der Grenzen für die Strafverfolgung durch die Zusammenarbeit der Strafverfolgungsbehörden der betroffenen Staaten ermöglichen, können Internettäter verfolgt werden.

Computer- und Internetdelikte betreffen i.d.R. die Rechtsordnungen zahlreicher Staaten. Eine wirksame und flächendeckende internationale Strafverfolgung von Cybercrime kann jedoch nur erfolgen, wenn sich möglichst viele Staaten an der grenzüberschreitenden Strafverfolgung beteiligen. Das „Übereinkommen über Computerkriminalität" des Europarates vom 23. 11. 2001 (CCC) bezweckt als ergänzendes Abkommen, neben den bereits bestehenden Verträgen zur internationalen Zusammenarbeit in Strafsachen, die länderübergreifende Kooperation im Bereich Cyberkriminalität zu optimieren. Mittels bindender Bestimmungen soll durch das CCC auf internationaler Ebene eine verstärkte, effiziente und gut funktionierende Bekämpfung von Cybercrime etabliert werden.

---

7 Vgl. Tagesanzeiger, 06.05.2015.
8 Vgl. KOBIK, Jahresbericht 2014, S. 2f.

1.2 Vorgehensweise

Die vorliegende Arbeit befasst sich mit der internationalen Zusammenarbeit im Bereich Cyberkriminalität und möchte insbesondere auf die Schwierigkeiten der grenzüberschreitenden Strafverfolgung eingehen. Schwerpunkt der Arbeit bilden die Instrumente des CCC zur internationalen Zusammenarbeit sowie das Zusammenspiel jener mit dem Tatbestandskatalog des CCC. Dabei soll untersucht werden, inwiefern das CCC seine eigenen Zielen umsetzen kann und ob es zu einer effektiv verbesserten Bekämpfung der Cyberkriminalität beitragen kann.

Im folgenden Kapitel werden für das Verständnis der Arbeit notwendige Begriffe definiert. Anschliessend soll die Frage beantwortet werden, was sich hinter dem Begriff der internationalen Rechtshilfe verbirgt, was deren Grundsätze sind und wie sich der Ablauf eines Rechtshilfeverfahrens aus Schweizer Sicht gestaltet. Im vierten Kapitel wird das CCC vorgestellt. Dabei wird auf die Ziele des Abkommens eingegangen, weiter werden die Entstehung und Umsetzung der Konvention in der Schweiz dargelegt und zum Schluss dessen Aufbau veranschaulicht. Im anschliessenden Kapitel fünf werden die einzelnen Straftatbestände der Konvention vorgestellt und deren Umsetzung im Schweizerischen Recht erläutert. Dabei soll ein Überblick über das gemäss der Konvention zu kriminalisierende, delinquente Verhalten geschaffen werden. Das sechste Kapitel befasst sich mit den Instrumenten der internationalen Zusammenarbeit, welche durch das CCC neu geschaffen wurden. Auch hier soll wieder eine Verbindung zur Umsetzung im Schweizerischen Recht hergestellt werden. Ein spezieller Fokus wird zudem auf die neuen Instrumente der internationalen Zusammenarbeit gelegt. Im siebten Kapitel wird der Mehrwert des CCC für die Schweiz analysiert, indem mittels Beizug von statistischem Material die tatsächliche Anwendung des Abkommens in der Schweiz überprüft wird. Des Weiteren wird auf einzelne Kritikpunkte und deren Berechtigung eingegangen und hinterfragt, inwiefern das CCC seinen eigenen Ziele gerecht wird. Im Schlusswort werden abschliessend die wichtigsten Erkenntnisse der Arbeit zusammengefasst.

2 Begriffliches und Grundlagen zu Cybercrime

Für das Grundverständnis der vorliegenden Arbeit kann auf die Definition einzelner Begriffe nicht verzichtet werden. Im Folgenden werden neben dem zentralen Begriff „Cybercrime" auch weitere Begriffe aus dem Bereich der Internet- und Computerkriminalität erläutert. Die Definition erfolgt dabei in Anlehnung an die Begriffsbestimmung des CCC, des StGB und des VÜPF.

2.1 Cybercrime bzw. Internetkriminalität

Der Begriff „Cybercrime" bezeichnet ganz allgemein Vergehen bzw. Verbrechen, welche mit Hilfe von Computern oder dem Internet begangen werden.[9] Im engeren Sinn kann der Begriff „Cybercrime" unter verschiedenen Gesichtspunkten definiert werden. Dabei taucht eine Vielzahl von Begriffen auf wie „Internet-" und „Computerkriminalität", „Online-Delikte", „IT-Kriminalität", „virtuelle Kriminalität" u.a. Vor allem die Begriffe „Computer-" und „Internetkriminalität" werden gerne als Synonyme verwendet, in der breiten Lehre wird i.d.R. aber eine wesentliche Unterscheidung dieser beiden Begriffe vorgenommen. Die Unterscheidung der beiden Begriffe ist aber nicht einheitlich; sie werden je nach Kontext mit unterschiedlichen und sich teilweise widersprechenden Inhalten belegt. Um der vorliegenden Arbeit ein einheitliches Verständnis der verwendeten Begrifflichkeiten zugrunde zu legen, werden die Begriffe „Internet-" und „Computerkriminalität" im Folgenden näher betrachtet. Der Definition liegt die Unterscheidung zu Grunde, ob die Straftaten ausschliesslich mit dem Computer begangen werden können, wie dies bei den Tatbeständen des Computerstrafrechts der Fall ist oder ob der Computer lediglich als Medium bzw. Instrument benutzt wird, um die Straftaten im Internet auszuüben.[10] In ersterem Fall wird in dieser Arbeit der Begriff „Computerkriminalität", in

---

9 Vgl. Springer Fachmedien Wiesbaden, S. 33.

10 Vgl. KRONIG/BOLLMANN, S. 22f; SCHWARZENEGGER, ZSR, S. 409ff.; Für Beispiele einer anderen Aufteilungen vgl. zudem: BALTISSER, Fn 240 und 242 mit weiteren Beispielen; KRONIG/BOLLMANN, S. 23f. zur Kategorisierung der Delikte gemäss der Bundespolizei; REINDL-KRAUSKOPF, S. 8f. zu einer Unterteilung in drei Kategorien: Angriffe auf Daten und Systeme, verbotene Inhalte und Vermögensschädigungen; SIEBER (S. 87ff.) seinerseits nimmt sogar eine Einteilung in fünf Kategorien vor: er unterscheidet die Delikte nach solchen, welche „sich gegen Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Computersystemen richten, traditionelle Computerdelikte, inhaltsbezogene Delikte, Delikte im Zusammenhang mit Urheberrechtsverletzungen und Datenschutzdelikte" in: BALTISSER, Fn 242; Springer Fachmedien Wiesbaden, S. 28 bzgl. Aufteilung in Computerkriminalität i.e.S. und Computerkriminalität i.w.S.; Auch WIDMER/BÄHLER (S. 292ff.) nehmen eine Dreiteilung vor. Sie unterscheiden zwischen Meinungsäusserungsdelikten, Computerdelikten und Urheberrechteverletzungen im Internet, in: BALTISSER, Fn 240.

letzterem der Begriff „Internetkriminalität i.e.S." verwendet. Ist gleichzeitig von Internetkriminalität i.e.S. und Computerkriminalität die Rede, werden jeweils die Oberbegriffe Internet- bzw. Cyberkriminalität verwendet.

2.1.1 Internetkriminalität i.e.S.

Unter den Begriff der „Internetkriminalität i.e.S." werden all jene Straftatbestände subsumiert, bei welchen die Existenz eines Computersystems nicht zwingend vorausgesetzt wird. Es handelt sich hier um Kriminalitätstatbestände, bei welchen das Computersystem als reines Medium und Tatwerkzeug benutzt wird, um Kriminalitätsphänomene ins Internet zu übertragen.[11] Das Internet selbst fungiert als Tatmittel bzw. Tatobjekt,[12] indem dessen Technik zur Begehung der Straftaten missbraucht wird.[13] Der Charakter der strafrechtlichen Handlung liegt somit nicht im Missbrauch automatischer Datenverarbeitungsanlagen, sondern in der delinquenten Nutzung von Datennetzen.[14] Die Erscheinungsformen der Internetkriminalität i.e.S. sind sehr vielfältig. In der Schweiz fallen darunter u.a. Straftaten wie die Darstellung von Gewalt (Art. 135 StGB), der Betrug (Art. 146 StGB), Ehrverletzung (Art. 173ff. StGB), harte Pornografie (Art. 197), Rassendiskriminierung (Art. 261bis StGB), Urheberrechtsverletzungen (Art. 67 URG) und Verletzungen des Fabrikations- oder Geschäftsgeheimnisses (Art. 12 StGB).[15]

2.1.2 Computerkriminalität

Der Begriff der „Computerkriminalität" ist bis heute, trotz vieler Definitionsversuchen in der Vergangenheit, nicht präzise kriminologisch bestimmbar.[16] Gewöhnlich wird der Begriff der „Computerkriminalität" weit ausgelegt, um möglichst alle kriminellen Verhaltensnormen zu erfassen, welche unmittelbar oder mittelbar im Zusammenhang mit einer elektronischen Datenverarbeitungsanlage stehen.[17]

Gemäss dem hier zugrunde liegenden Verständnis fasst der Begriff „Computerkriminalität" jene Straftaten zusammen, welche mittels eines Computers oder unter Einsatz einer elektronischen Datenverarbeitung[18] begangen werden, wobei ein Internetzugang nicht

11 Vgl. KRONIG/BOLLMANN, S. 23.
12 Vgl. SCHUH, S. 28f.; HILGENDORF et al., Rz. 123; HERZOG, S. 1.
13 Vgl. Springer Fachmedien Wiesbaden, S. 92f.
14 Vgl. VETTER, S. 4.
15 Vgl. KOBIK[3].
16 Vgl. VETTER, S. 3; siehe auch: SCHUH, S. 28.
17 Vgl. VETTER, S. 3; siehe auch: HILGENDORF et al., Rz. 123: SCHUH, S. 28.
18 Vgl. HERZOG, S. 1; HILGENDORF/VALERIUS, Rz. 7.

zwingend vorausgesetzt wird.[19] Die Tatbestände der Computerkriminalität charakterisieren sich dadurch, dass für die Begehung die Existenz eines Computernetzwerkes Voraussetzung ist,[20] dieses somit entweder als zwingend erforderliches Tatmittel oder als Tatobjekt der deliktischen Handlung zum Einsatz kommt.[21] In der Schweiz werden unter den Begriff der Computerkriminalität die Delikte des Computerstrafrechts subsumiert.[22] Diese sind im Einzelnen unbefugte Datenbeschaffung (Art. 143 StGB), unbefugtes Eindringen in ein Datenverarbeitungssystem (Art. 143bis StGB), Datenbeschädigung (Art. 144bis StGB), betrügerischer Missbrauch einer Datenverarbeitungsanlage (Art. 147 StGB) und Erschleichung einer Leistung einer Datenverarbeitungsanlage, der sog. „Zeitdiebstahl" (Art. 150 Abs. 3 StGB).[23]

2.2 Weitere Begriffe aus den Bereichen Computer und Internet

2.2.1 Computersystem

In Art. 1 lit. a CCC wird der Begriff „Computersystem" als eine Vorrichtung oder eine Gruppe miteinander verbundener Vorrichtungen definiert, welche einzeln oder zu mehreren auf der Grundlage eines Programms automatisch Datenverarbeitungen durchführen.[24] Anders ausgedrückt sind Computersysteme technische Einrichtungen, welche Informationen in nicht direkt lesbarer, meist kodierter Form empfangen, mittels Programm automatisiert bearbeiten und anschliessend wiedergeben.[25] Entscheidend ist, dass dabei immer ein Datenaustausch über das Netzwerk stattfindet.[26]

Die Verbindung[27] von zwei oder mehr Computersystemen bildet ein Netzwerk.[28] Ein Netzwerk kann geographisch auf ein kleines Gebiet beschränkt sein (lokales Netzwerk) oder ein grosses Gebiet umfassen (Globalnetzwerk). Ein Beispiel für ein globales Netzwerk ist das Internet, welches aus vielen verbundenen Netzwerken besteht, die alle

---

19 Vgl. Springer Fachmedien Wiesbaden, S. 92.
20 Vgl. KRONIG/BOLLMANN, S. 23.
21 Vgl. SCHUH, S. 28.
22 Vgl. KOBIK[3].
23 Die einzelnen Tatbestände des Computerstrafrechts stellen kein Neuland dar, sondern sind, mit Ausnahme von Art. 143bis StGB, Abwandlungen der klassischen Vermögensstraftatbestände, vgl. SCHMID, ZStrR, S. 23.
24 Art. 1 lit. a CCC.
25 Vgl. STRATENWERTH/WOHLERS, Art. 143bis StGB N 1; ETS No. 185, Ziff. 23.
26 Vgl. ETS No. 185, Ziff. 24.
27 Eine solche Verbindung kann erdgebunden (z.B. mittels Draht oder Kabel), drahtlos (z.B. Funk, Infrarot oder Satellit) oder eine Kombination von beidem sein, vgl. ETS No. 185, Ziff. 24.
28 Vgl. ETS No. 185, Ziff. 24.

dasselbe Protokoll benutzen. Neben diesem existieren auch andere Arten von Netzwerken, welche Daten auch ohne Internetverbindung untereinander übermitteln können.[29]

2.2.2 Computerdaten

Der Begriff „Computerdaten" umfasst gemäss Art. 1 lit. b CCC jede Darstellung von Tatsachen, Informationen oder Konzepten in einer für die Verarbeitung in einem Computersystem geeigneten Form, einschliesslich eines Programms, das die Ausführung einer Funktion durch ein Computersystem auslösen kann.[30] Anders ausgedrückt handelt es sich bei Daten um alle Informationen in immaterieller Form,[31] welche Gegenstand menschlicher Kommunikation sein können.[32]

Der Ausdruck „für die Verarbeitung geeignet" bedingt, dass die Daten in eine Form gebracht werden, in welcher sie direkt von einem Computersystem weiterverarbeitet werden könne. Es kann sich dabei sowohl um elektronische Daten als auch um Daten in einer anderen Form handeln, welche die direkte Weiterverarbeitung ermöglichen.[33] Computerdaten können sowohl Ziel einer der Straftatbestände des CCC sein, als auch Gegenstand einer Ermittlungsmassnahme in Form von Beweismitteln darstellen.[34] Die Definition des CCC beruht auf der ISO-Definition für Computerdaten,[35] welche den Begriff „Daten" als eine Darstellung von Informationen in einer formalisierten Art und Weise für die Kommunikation, Interpretation und Verarbeitung umschreibt.[36]

2.2.3 Dienstanbieter/Service Provider

Als Dienstanbieter gilt laut CCC einerseits jeder öffentliche oder private Anbieter, der Nutzern seines Dienstes die Übertragung von Daten mit Hilfe eines Computersystems ermöglicht.[37] Andererseits wird unter „Dienstanbieter" auch jede andere Person verstanden, die für einen solchen Kommunikationsdienst oder für dessen Nutzer Computerdaten verarbeitet oder speichert.[38] Für die Qualifikation als Dienstanbieter ist irrele-

---

29 Vgl. ETS No. 185, Ziff. 24; Als weitere Netzwerke kommen bspw. firmeninterne Netzwerke in Frage, welche zur Übermittlung von Daten keinerlei Internetverbindung benötigen.
30 Art. 1 lit. b CCC.
31 Vgl. BALTISSER, S. 61.
32 Vgl. STRATENWERTH/WOHLERS, Art. 143 StGB N 2; STRATENWERTH et al., § 14 N 25; StGB PK – TRECHSEL/CRAMERI, Art. 143 StGB N 3; BSK StGB – WEISSENBERGER, Art. 143 StGB N 8.
33 Vgl. BALTISSER, S. 62; BBl 1991 II 969, S. 986f.; ETS No. 185, Ziff. 25; SCHMID, ZStrR, S. 24.
34 Vgl. ETS No. 185, Ziff. 25.
35 Vgl. ETS No. 185, Ziff. 25.
36 Vgl. ISO/IEC 2382:2015, 2121272.
37 Art. 1 lit. c i CCC.
38 Art. 1 lit. c ii CCC; Vgl. zudem: ETS No. 185, Ziff. 26f.; Für eine ausführlichere Definition des Begriffs „Provider" vgl. HILGENDORF/VALERIUS, Rz. 178; Springer Fachmedien Wiesbaden, S. 93f.

vant, ob die Benutzer eine geschlossene Gruppe[39] bilden oder ob das Angebot der Öffentlichkeit zur Verfügung steht, sei es kostenlos oder gegen Gebühr.[40]

Nicht unter den Begriff „Dienstanbieter" fallen Inhalts-Anbieter von bloss „qualifizierten Inhalten,"[41] solange diese nicht gleichzeitig auch Übermittlungen von Daten oder eine damit zusammenhängende Verarbeitung der Daten anbieten.[42]

2.2.4 Verkehrsdaten

Der Begriff „Verkehrsdaten" umfasst alle Computerdaten die von einem Computersystem innerhalb einer Kommunikationskette generiert werden und aus denen der Ursprung, das Ziel, der Weg, die Uhrzeit, das Datum, der Umfang, die Dauer der Kommunikation und die Art des für die Kommunikation benutzten Dienstes[43] entnommen werden kann.[44]

Die Auslegung des Begriffs „Verkehrsdaten" im CCC ist nicht deckungsgleich mit jener der VÜPF.[45] Letztere beschreibt Verkehrsdaten als „Informationen, die von den Anbietern über den Post- oder Fernmeldeverkehr von Teilnehmerinnen und Teilnehmern aufgezeichnet werden, um Tatsachen der Postsendung oder der Kommunikation und die Rechnungsstellung zu belegen."[46] Indem die VÜPF neben dem elektronischen Datenverkehr auch jenen des Postverkehrs und Informationen zur Rechnungsstellung unter den Begriff „Verkehrsdaten" zusammenfasst, ist der Begriff „Verkehrsdaten" in der VÜPF weiter gefasst als im CCC. Mit Blick auf die praktische Anwendung sind die Begriffsbeschreibungen aber weitgehend deckungsgleich.[47]

Grundsätzlich werden Verkehrsdaten von Computern innerhalb einer Kommunikationskette erhoben, um eine Kommunikation von ihrem Ursprung bis zu ihrem Bestimmungsort zu verfolgen. Gleichzeitig fungieren sie auch als Unterstützung der Kommuni-

---

39 Als Beispiel einer geschlossenen Gruppe führt das CCC die Kommunikation von Arbeitnehmern über ein firmeninternes Netzwerk auf, vgl. ETS No. 185, Ziff. 26.

40 Vgl. ETS No. 185, Ziff. 26.

41 Inhalts-Anbieter, auch Content-Provider genannt, halten eigene Informationen auf Servern oder Online-Diensten, um diese im Internet anzubieten, vgl. HILGENDORF/VALERIUS, Rz. 180; Springer Fachmedien Wiesbaden, S. 30.

42 Vgl. ETS No. 185, Ziff. 27.

43 „Zugrundeliegende Services" bedeutet: Dienstleistungen, welche innerhalb des Netzwerkes benutzt werden, z.B. Datentransfer, E-Mail etc., vgl. ETS No. 185, Ziff. 30.

44 Art. 1 lit. d CCC; Die Aufzählung der Verkehrsdaten, welche u.U. eruiert werden dürfen, ist abschliessend, vgl. EST No. 185, Ziff. 30.

45 Vgl. BBl 2010 4697, S. 4703.

46 Vgl. Anhang zu Art. 2 VÜPF, Ziff. 7.

47 Vgl. BBl 4697, S. 4702f.; BSK ISTR – BÖHI, Art. 18b IRSG N 4; FABBRI/FURGER, ZStrR, Fn 58.

kation.[48] Im Falle einer Strafuntersuchung wegen Cyberkriminalität werden Verkehrsdaten vor allem zur Ermittlung der Quelle der Kommunikation benötigt. Gleichzeitig dienen Verkehrsdaten auch als Ausgangspunkt für die Erhebung weiterer Beweise.[49] Da Verkehrsdaten überwiegend nur über einen relativ kurzen Zeitraum hinweg gespeichert werden, ist es wichtig, deren umgehende Sicherung und Weitergabe anordnen zu können.[50] Das Sammeln und Abspeichern von Verkehrsdaten wird dadurch gerechtfertigt, dass diese, im Gegensatz zu Inhaltsdaten, keinerlei Auskunft über den Inhalt der Kommunikation geben und deren Abspeicherung somit weniger in die Privatsphäre des Benutzers eingreift.[51] In der Schweiz sind die Provider in diesem Zusammenhang verpflichtet, die für die Teilnehmeridentifikation notwendigen Verkehrs- und Rechnungsdaten während 6 Monaten aufzubewahren.[52]

48 Vgl. ETS No. 185, Ziff. 28.
49 Vgl. ETS No. 185, Ziff. 29.
50 Vgl. ETS No. 185, Ziff. 29; FABBRI/FURGER, ZStrR, S. 409.
51 Vgl. ETS No. 185, Ziff. 29; A.M. HERZOG, S. 7.
52 Art. 15 Abs. 3 BÜPF.

3 Internationale Rechtshilfe in Strafsachen

3.1 Allgemeines: Was ist internationale Rechtshilfe?

Unter den Begriff der internationalen Rechtshilfe, bzw. der „Rechtshilfe i.w.S.“, fallen alle Handlungen, welche ein Staat (der ersuchte Staat) unternimmt, um einem anderen Staat (dem ersuchenden Staat) die Verfolgung und Bestrafung von Straftaten zu erleichtern.[53] Rechtshilfe i.w.S. umfasst verschiedenste Arten der zwischenstaatlichen Zusammenarbeit, welche alle die Durchsetzung eines Strafanspruchs mittels gegenseitiger Hilfe und damit die Umsetzung kriminalpolitischer Ziele anstreben.[54] Sie beruht auf dem Grundsatz des Territorialitätsprinzips. Dieses verbietet einem Staat grundsätzlich, auf dem Hoheitsgebiet eines anderen Staates eigene Strafverfolgungsmassnahmen vorzunehmen.[55] Deshalb ist für die Erlangung von Personen, Objekten und Informationen auf dem Gebiet eines anderen Staates zwingend die Hilfe des jeweils betroffenen Staates notwendig, um welche über die internationale Rechtshilfe ersucht werden kann.[56]

In der internationalen Rechtshilfe in Strafsachen gilt es zwischen den einzelnen Rechtsinstituten zu unterscheiden.[57] Im Mittelpunkt dieser Arbeit steht das Institut der „kleinen Rechtshilfe.“ Dieses umfasst sämtliche Massnahmen, welche ein Staat zur Unterstützung eines Strafverfahrens des ersuchenden Staates auf seinem eigenen Territorium vornimmt.[58] Im Folgenden bezieht sich der Begriff „Rechtshilfe“ immer auf die „kleine Rechtshilfe.“[59]

3.2 Prinzipien der Rechtshilfe

Das Leisten von Rechtshilfe hängt massgeblich davon ab, ob gewisse Grundsätze der internationalen Zusammenarbeit eingehalten und im konkreten Fall gegeben sind. Einer

---

53 Vgl. Wegleitung, S. 5.

54 Vgl. BSK ISTR – HEIMGARTNER/NIGGLI, Einführung N 11.

55 Vgl. BGer 1B_344/2014 E. 5.3; BBl 2013 2683, S. 2689; Capus, S. 192ff.; DONATSCH et al., S. 4; HEIMGARTNER, S. 120ff. und S. 135.

56 Vgl. BGer 1B_344/2014 E. 5.3; BSK ISTR – HEIMGARTNER/NIGGLI, Einführung N 3 und N 19; FORSTER, S. 616f.

57 Art. 1 Abs. 1 IRSG: Die einzelnen Rechtsinstitute der internationalen Rechtshilfe sind die Auslieferung (Art. 32ff. IRSG), die akzessorische, „andere“ bzw. kleine Rechtshilfe (Art. 63ff. IRSG), die stellvertretende Strafverfolgung (Art. 85ff. IRSG) und die Vollstreckung ausländischer Strafentscheide (Art. 94ff. IRSG).

58 Vgl. BSK ISTR – HEIMGARTNER/NIGGLI, Einführung N 29; Als entsprechende Massnahmen kommen die Befragung von Zeugen, Auskunftspersonen oder Beschuldigten, die Herausgabe oder Sicherstellung von Beweis- oder Schriftstücken, Hausdurchsuchungen und Beschlagnahme, die Gegenüberstellung, die Herausgabe von Vermögenswerten und die Zustellung von Vorladungen, Urteilen und anderen Gerichtsakten in Betracht, vgl. Art. 63 Abs. 1 bis 3 IRSG; Vgl. zudem: GSTÖHL, S. 95; Wegleitung, S. 5.

59 Bezieht sich die Verwendung des Begriffs auf die Rechtshilfe i.w.S., wird in der Arbeit von nun an ausdrücklich darauf hingewiesen.

der klassischen Grundsätze des Rechtshilferechts ist das Prinzip der beidseitigen Strafbarkeit.[60] Dieses besagt, dass ein Staat sein Gewalt- und Strafmonopol gegenüber seinen eigenen Bürgern nur insofern ausüben darf, als nach seiner souveränen Bewertung ein strafwürdiges Verhalten gegeben ist.[61] Das Prinzip der beidseitigen Strafbarkeit verlangt somit, dass die im Ersuchen geschilderte Tat einem Straftatbestand des nationalen Rechts entspricht.[62] Dabei genügt es, wenn die im Ersuchen geschilderte Handlung in beiden Staaten als Delikt geahndet wird.[63] Übereinstimmende Strafbedingungen, gleiche Sanktionsandrohungen oder der Schutz des gleichen Rechtsgutes sind nicht erforderlich.[64] Zudem muss nicht für jede einzelne im Ersuchen geltend gemachte Straftat die beidseitige Strafbarkeit gegeben sein; es genügt, wenn eines der aufgeführten Delikte dieses Erfordernis erfüllt.[65]

Sämtliches staatliche Handeln, welches in die Grundrechte von Individuen eingreift, unterliegt dem Verhältnismässigkeitsprinzip.[66] Diese gelangt auch im Rahmen der internationalen Rechtshilfe zur Anwendung.[67] Dies wird insbesondere in Art. 4 IRSG deutlich, welcher besagt, dass einem Rechtshilfeersuchen in Bagatellfällen nicht entsprochen wird.[68] Weiter verlangt das Verhältnismässigkeitsprinzip, dass die vom ausländischen Staat ersuchten Prozesshandlungen für das ausländische Verfahren erforderlich und geeignet erscheinen müssen.[69] Das im Verhältnismässigkeitsprinzip enthaltene Übermassverbot verbietet der Rechtshilfebehörde zudem, weitere als die im Rechtshilfeersuchen verlangten Massnahmen anzuordnen.[70]

---

60 Vgl. BSK ISTR – HEIMGARTNER/NIGGLI, Einführung N 44; BSK ISTR – HEIMGARTNER, Art. 64 IRSG N 1; Wegleitung, S. 27f.

61 Art. 64 Abs. 1 IRSG; Hinsichtlich der kleinen Rechtshilfe gilt das Prinzip nur bei der Anwendung von prozessualem Zwang, vgl. BSK ISTR – HEIMGARTNER/NIGGLI, Einführung N 44; BSK ISTR – HEIMGARTNER, Art. 64 IRSG N 2; CAPUS, S. 334, 347ff.; GSTÖHL, S. 102.

62 Art. 64 Abs. 1 IRSG; Vgl. zudem: BGE 132 II 81 E. 2.7.2; BGE 129 II 462; Vom Prinzip der beidseitigen Strafbarkeit ausgenommen sind Ersuche, welche sich auf die Entlastung des Verfolgten oder die Verfolgung von Taten, welche sexuelle Handlungen mit Unmündigen darstellen, stützen, vgl. Art. 64 Abs. 2 IRSG; HEIMGARTNER, S. 137; Wegleitung, S. 27f.

63 Vgl. Wegleitung, S. 28.

64 Vgl. BGer 1A.125/2006 E. 2.1 m.w.H.; BSK ISTR – HEIMGARTNER/NIGGLI, Einführung N 46; BSK ISTR – HEIMGARTNER, Art. 64 IRSG N 7; HEIMGARTNER, S. 138; Wegleitung, S. 28.

65 Vgl. Wegleitung, S. 28.

66 Art. 36 Abs. 3 BV; Vgl. zudem: POPP, Rz. 420ff.

67 Vgl. BSK ISTR – HEIMGARTNER/NIGGLI, Einführung N 42.

68 Art. 4 IRSG; Vgl. zudem: BSK ISTR – HEIMGARTNER/NIGGLI, Einführung N 42; Bagatellfälle liegen vor, wenn die Bedeutung der Tat die Durchführung eines Rechtshilfeverfahrens nicht rechtfertigt, vgl. GSTÖHL, S. 100, 111; Diese Bestimmung ist aber mit Umsicht und Zurückhaltung anzuwenden, vgl. Wegleitung, S. 21.

69 Art. 63 Abs. 1 in fine IRSG; Vgl. zudem: BSK ISTR – HEIMGARTNER/NIGGLI, Einführung N 42; HEIMGARTNER, S. 139.

70 Vgl. BSK ISTR – HEIMGARTNER/NIGGLI, Einführung N 42.

Das Spezialitätsprinzip als weiterer Grundsatz der Rechtshilfe besagt, dass die mittels Rechtshilfeverfahren übermittelten Informationen im ersuchenden Staat nur in jenem Strafverfahren verwendet werden dürfen, welches dem entsprechenden Ersuchen zugrunde liegt.[71] Damit wird dem rechtshilfeleistenden Staat die Möglichkeit gegeben, die Verwendung der zu liefernden Informationen, welche häufig schützenswert sind, im ersuchenden Staat zu kontrollieren.[72] Da das Spezialitätsprinzip aber keine absolute Geltung beansprucht, können die ersuchenden Staaten, sofern eine entsprechende Bewilligung vom ersuchten Staat erteilt wurde, die Dateien auch anderweitig verwenden.[73]

3.3 Voraussetzungen und Ablauf eines Rechtshilfeverfahrens in der Schweiz

Der Übermittlungsweg eines Rechtshilfeersuchens bestimmt sich nach der Nähe der Rechtssysteme und der geografischen Entfernung.[74] Im Normalfall geschieht die Übermittlung der Rechtshilfeersuchen über das Justizministerium. Zwischen den europäischen Staaten wird – soweit dies die jeweils anwendbaren Rechtsgrundlagen vorsehen – grundsätzlich der direkte Weg gewählt. Bestehen keine vertraglichen Beziehungen und fehlt der Direktkontakt zum jeweiligen Justizministerium, ist der diplomatische Weg zu wählen.[75] Bei Dringlichkeit oder bei vorläufig anzuordnenden Massnahmen geschieht die Übermittlung entweder über Interpol oder aber die ersuchende Behörde wendet sich direkt an die zuständige Behörde im ersuchten Staat.[76]

Ein Rechtshilfebegehren ist in Schriftform in einer der drei Amtssprachen der Schweiz zu verfassen.[77] Des Weiteren muss es Angaben zur ersuchenden Behörde, zum Gegenstand des ausländischen Verfahrens und zur Person enthalten, gegen welche sich das Verfahren richtet sowie eine rechtliche Beschreibung der Tat und des wesentlichen Sachverhalts.[78] Eine Verletzung der Formvorschriften oder die Nichteinhaltung des Übermittlungsweges hat nicht die Verweigerung der Rechtshilfe zur Folge. Vielmehr wird die ersuchende Behörde unter Fristansetzung zur Verbesserung oder Ergänzung

71 Vgl. BSK ISTR – HEIMGARTNER/NIGGLI, Einführung N 48; FABBRI/FURGER, ZStrR, S. 404; GSTÖHL, S. 111ff.
72 Vgl. Wegleitung, S. 33.
73 Vgl. BSK ISTR – HEIMGARTNER/NIGGLI, Einführung N 44; Wegleitung, S. 33.
74 Vgl. Wegleitung, S. 38.
75 Vgl. BSK ISTR – KUSTER, Art. 78 IRSG N 1; Wegleitung, S. 38f.
76 Art. 29 Abs. 2 IRSG; Vgl. zudem: BSK ISTR – HEIMGARTNER, Art. 29 IRSG N 7; Wegleitung, S. 39; Siehe auch: Anhang 9.1.
77 Art. 28 Abs. 5 IRSG; Vgl. zudem: BSK ISTR – ENGLER, Art. 28 IRSG N 3ff., 9ff., 14ff.; Wegleitung, S. 40f.
78 Vgl. Wegleitung, S. 40f.

des Ersuchens aufgefordert.[79] Eine allfällige Verbesserung oder Ergänzung des Rechtshilfeersuchens hat keinerlei Auswirkung auf vorläufig anzuordnende Massnahmen.[80]

Unter Vorbehalt der direkten Übermittlung ist in der Schweiz das Bundesamt für Justiz (BJ) für die Entgegennahme von ausländischen Ersuchen zuständig.[81] Es prüft im Rahmen seiner Weiterleitungs- und Delegationsfunktion summarisch, ob das Ersuchen den Formerfordernissen des Rechtshilfegesetzes oder der anwendbaren Staatsverträge entspricht.[82] Soweit erforderlich, kann das BJ bereits in der Phase der summarischen Prüfung vorläufige Massnamen anordnen.[83] Anschliessend wird das Ersuchen an die zuständige ausführende Behörde weitergeleitet.[84] Diese überprüft ihrerseits die gesetzlichen Erfordernisse, welche für die Gewährung von Rechtshilfe massgeblich sind.[85] Sind diese erfüllt, wird eine Eintretensverfügung erlassen und die im Ersuchen verlangten und als zulässig erachteten Rechtshilfemassnahmen angeordnet.[86] Beim Vollzug der Massnahmen ist das Gebot der raschen Erledigung zu beachten.[87]

In erster Linie fällt das ordentliche Rechtshilfeverfahren in den Zuständigkeitsbereich der kantonalen Behörden.[88] Somit ist grundsätzlich sowohl die Vorprüfung[89] als auch der Vollzug[90] der Rechtshilfemassnahmen und der Erlass der Schlussverfügung,[91] welche über die Zulässigkeit und den Umfang der Rechtshilfe Auskunft gibt, Sache der zuständigen kantonalen Behörden.[92] Ist der direkte Verkehr vorgesehen, ist die kantonale Behörde auch für die Entgegennahme des Ersuchens, die summarische Prüfung nach Art. 78 Abs. 2 IRSG und am Ende des Verfahrens für die Übermittlung der Vollzugsakten zuständig.[93]

Der Abschluss eines Rechtshilfeverfahrens erfolgt immer mit einer Schlussverfügung. Eine solche wird von der Vollzugsbehörde erlassen, wenn alle Ausführungen des Ersu-

---

79 Art. 28 Abs. 6 IRSG; Vgl. zudem: BSK ISTR – ENGLER, Art. 28 IRSG N 25; Wegleitung, S. 38.
80 Vgl. BGE 103 Ia 206, E. 7; BGE 111 Ib 242 E. 6; BGE 116 Ib 97 E. 3b; BSK ISTR – ENGLER, Art. 28 IRSG N 26. Wegleitung, S. 38.
81 Art. 78 Abs. 1 IRSG; Vgl. zudem: BSK ISTR – HEIMGARTNER, Art. 29 IRSG N 4; GSTÖHL, S. 134; Wegleitung, S. 39.
82 Art. 78 Abs. 2 IRSG; Vgl. zudem: BSK ISTR – KUSTER, Art. 78 IRSG N 3; Wegleitung, S. 45.
83 Art. 78 Abs. 5 IRSG; Vgl. zudem: BSK ISTR – KUSTER, Art. 78 IRSG N 5; Wegleitung, S. 46.
84 Vgl. Wegleitung, S. 48.
85 Art. 80 IRSG; Vgl. zudem: BSK ISTR – KUSTER, Art. 80 IRSG N 2f.; GSTÖHL, S. 137ff.; Wegleitung, S. 49.
86 Art. 80a IRSG; Vgl. zudem: BSK ISTR – KUSTER, Art. 80a IRSG N 1; Wegleitung, S. 49.
87 Art. 17a Abs. 1 IRSG; Vgl. zudem BSK ISTR – ENGLER, Art. 17a IRSG N 1; Wegleitung, S. 30 und 49.
88 Vgl. Wegleitung, S. 44.
89 Art. 80 IRSG.
90 Art. 80a IRSG.
91 Art. 80d IRSG.
92 Vgl. BSK ISTR – KUSTER, Art. 78 IRSG N 1; BSK ISTR – KUSTER, Art. 80 IRSG N 1ff.; Wegleitung, S. 44.
93 Art. 78 Abs. 1 IRSG; Vgl. zudem: BSK ISTR – KUSTER, Art. 78 IRSG N 1; GSTÖHL, S. 135; Wegleitung, S. 44.

chens, d.h. alle verlangten Beweiserhebungen getätigt wurden, abgeschlossen sind und die fallführende Rechtshilfebehörde das Ersuchen als erledigt erachtet.[94] Im Rechtshilfeverfahren ist diese Verfügung die einzige, gegen welche zusammen mit den vorangegangenen Zwischenverfügungen bei der zweiten Beschwerdekammer des Bundesstrafgerichts Beschwerde erhoben werden kann.[95] Beschwerdelegitimiert ist, wer von einer Rechtshilfemassnahme persönlich und unmittelbar betroffen ist. Ein entsprechendes schutzwürdiges Interesse muss nicht geltend gemacht werden.[96]

Beeinträchtigt das Erledigen eines Rechtshilfeersuchens die Souveränität, Sicherheit oder andere wesentliche Interessen der Schweiz, kann die Schweiz das Leisten von Rechtshilfe verweigern.[97] Ein entsprechender Entscheid obliegt dem eidgenössischen Justiz- und Polizeidepartement, welches innerhalb von 30 Tagen nach der schriftlichen Mitteilung der Schlussverfügung anzurufen ist.[98] Ebenfalls kann die Schweiz die Leistung von Rechtshilfe verweigern, wenn schwerwiegende Verfahrensmängel vorliegen.[99] Ein Rechtshilfeersuchen wird auch für unzulässig erklärt, wenn das Verfahren im Ausland lediglich zur Verfolgung oder Bestrafung einer Person wegen ihrer politischen Anschauung, ihrer Zugehörigkeit zu einer bestimmten sozialen Gruppe oder ihrer Rasse, Konfession oder Staatsangehörigkeit dient.[100]

---

94 Vgl. BSK ISTR – HEIMGARTNER/NIGGLI, Art. 80d IRSG N 1ff.; Wegleitung, S. 50.

95 Art. 80e Abs. 1 IRSG; Vgl. zudem: BSK ISTR – EYMANN, Art. 80e IRSG N 1f.; FABBRI/FURGER, ZStrR, S. 397; GSTÖHL, S. 140f.; Wegleitung, S. 55; Eine selbständige Anfechtung der Zwischenverfügung ist nur möglich, wenn die betroffenen Person einen unmittelbaren und nicht wieder gutzumachenden Nachteil beweisen kann, Art. 80e Abs. 2 IRSG; Vgl. zudem: BSK ISTR – EYMANN, Art. 80e IRSG N 3ff.

96 Vgl. FABBRI/FURGER, ZStrR, S. 396; Wegleitung, S. 41ff.

97 Art. 1a und Art. 17 IRSG; Vgl. zudem: BSK ISTR – NIGGLI/GÖHLICH, Art. 1a IRSG N 2ff. und N 20 und Art. 17 IRSG N 3 und 7f.; Wegleitung, S. 18 und S. 44.

98 Vgl. BSK ISTR – NIGGLI/GÖHLICH, Art. 17 IRSG N 8; Wegleitung, S. 18.

99 Als schwerwiegende Verfahrensmängel gelten die Verletzung der Grundsätze der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK) und des Internationalen Pakts über bürgerliche und politische Rechte (UNO-Pakt II), Art. 2 lit. a IRSG; Vgl. zudem: BSK ISTR – SUMMERS, Art. 2 IRSG N 7ff.; GSTÖHL, S. 101f.; Wegleitung, S. 18f.

100 Art. 2 lit. b und c IRSG; Vgl. zudem: BSK ISTR – SUMMERS, Art. 2 IRSG N 19ff.; Wegleitung, S. 19.

4 Das Übereinkommen des Europarates über die Cyberkriminalität

4.1 Ziele des Abkommens

Das Übereinkommen des Europarates über die Cyberkriminalität (CCC) vom 23. November 2001 ist die erste internationale Konvention, welche sich mit der Bekämpfung der Computer- und Internetkriminalität befasst.[101] Das CCC entstand aus der Notwendigkeit, die grenzüberschreitenden Straftaten der Cyberkriminalität mit der erforderlichen Schnelligkeit und Effizienz verfolgen zu können.[102] Ein formelles Rechtshilfeverfahren kann sich schnell zu einem langwierigen, komplizierten und aufwändigen Verfahren gestalten. Dies birgt die Gefahr, dass die für die Ermittlung relevanten Daten durch das langsame Verfahren verloren gehen können, da bis zur Beantwortung des rechtshängigen Ersuchens die gesetzlichen Überwachungs- und Speicherfristen – soweit vorhanden[103] – oftmals bereits abgelaufen sind. Um diesem wenig zufriedenstellenden Zustand entgegenzuwirken, wurde das CCC erlassen. Es verpflichtet die Vertragsstaaten, ihre Gesetzgebung an die Herausforderungen der neuen Informationstechnologien anzupassen und auf internationaler Ebene zu kooperieren. Denn nur damit kann eine schnelle, wirksame und umfassende Zusammenarbeit zur Bekämpfung der Cyberkriminalität zwischen den Vertragsstaaten nachhaltig gewährleistet werden.[104]

4.2 Historisches zum CCC

4.2.1 Entwicklung des CCC bis zur Vertragsunterzeichnung

Im November 1996 setzte das „European Committee on Crime Problems“ (CDCP) ein Expertenteam zur Untersuchung der Internetkriminalität ein.[105] Diese ergaben, dass nur ein bindendes internationales Abkommen die notwendige Effizienz im Kampf gegen die Internetkriminalität gewährleisten könne.[106] Gestützt auf die Ergebnisse des Expertenteams berief der Ministerrat am 4. Februar 1997 ein Gremium ein, das sog. „The Committee of Experts on Crime in Cyber-Space“ (PC-CY). Er betraute dieses mit der Aufgabe,

[101] Vgl. BBl 2010 4697, S. 4698.
[102] Vgl. ETS No. 185, N 9.
[103] Viele Staaten kennen in Bezug auf eine allfällig rückwirkende Erhebung von Randdaten des elektronischen Fernmeldeverkehrs keine oder nur verhältnismässig kurze Speicherfristen von Daten, vgl. BGer 1B_344/2014 E. 5.5.
[104] Vgl. ETS No. 185, Ziff. 16.
[105] Vgl. ETS No. 185, N 7; Entscheid CDPC/103/211196.
[106] Vgl. ETS No. 185, N 9.

das durch das Expertenteam geforderte bindende internationale Abkommen zur Bekämpfung der Internetkriminalität zu entwerfen. Im April 1997 startete das PC-CY Komitee mit seiner Aufgabe und begann mit den Verhandlungen zu einer internationalen Konvention über Internetkriminalität.[107] Ab April 2000 wurden die aktuellen Entwürfe der Konvention veröffentlicht, um einen breiten Diskurs unter den verhandelnden Staaten und allfällig interessierten Drittstaaten zu ermöglichen. Dies diente der weiteren Ausarbeitung der Konvention massgeblich, konnten dadurch doch die vielseitigen Interessen diverser Staaten berücksichtigt werden.[108] Im Juni 2001 wurden der vollendete Entwurf der Konvention und der dazugehörende erläuternde Bericht dem CDPC zur Überprüfung vorgelegt und anschliessend dem Ministerkomitee zur Annahme unterbreitet.[109]

Am 8. November 2001 wurde die Konvention und der erläuternde Bericht vom Ministerkomitee des Europarates angenommen und anschliessend am 23. November 2001 an der internationalen Konferenz über Computerkriminalität in Budapest den Staaten zur Unterzeichnung vorgelegt.[110] Bedingung für das Inkrafttreten der Konvention war deren Ratifizierung durch mindestens fünf Staaten, wobei mindestens 3 Staaten Mitglieder des Europarates sein mussten.[111] Die Konvention trat schliesslich am 1. Juli 2004 in Kraft und wurde bis heute von insgesamt 47 Staaten ratifiziert und weiteren sieben Staaten unterzeichnet.[112]

4.2.2 Ratifizierung und Umsetzung der Konvention in der Schweiz

Die Schweiz unterzeichnete das Abkommen am 23. November 2001.[113] Mit der Genehmigung des Abkommens unterstrich der Bundesrat seine Bemühungen, sich für eine verstärkte Bekämpfung der Cyberkriminalität auf internationaler Ebene einzusetzen.[114] Zwar erfüllte die Schweiz die meisten Anforderungen der Konvention bereits weitgehend, dennoch bedurfte es für deren Ratifikation und Umsetzung kleineren Änderungen

[107] Vgl. ETS No. 185, N 12.
[108] Vgl. ETS No. 185, N 14.
[109] Vgl. ETS No. 185, N 15.
[110] Vgl. ETS No. 185, N 1.
[111] Art. 36 Abs. 3 CCC.
[112] Vgl. Liste der unterzeichneten und ratifizierten Staaten, <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&CL=GER>, Stand: 11.11.2015.
[113] Vgl. BBl 2010 4697, S. 4698.
[114] Vgl. EJPD, Mm. vom 14.11.2011.

des Strafgesetzbuches und des Rechtshilfegesetzes.[115] Am 13. März 2009 eröffnete der Bundesrat schliesslich die Vernehmlassung zur Umsetzung der Europakonvention über die Cyberkriminalität. Damit gab er den Kantonen, den in der Bundesversammlung vertretenen politischen Parteien sowie den interessierten Verbänden und Organisationen die Möglichkeit, bis zum 30. Juni 2009 ihre Stellungnahme einzureichen.[116] Von dieser Möglichkeit machten 74 Interessensgruppen Gebrauch. Das Vernehmlassungsverfahren ergab einen eindeutigen Konsens aller Beteiligten zugunsten der Ratifikation des Übereinkommens und der damit einhergehenden Gesetzesänderungen.[117]

Die Botschaft zur Ratifikation der Europakonvention über die Cyberkriminalität wurde am 18. Juni 2010 vom Bundesrat verabschiedet.[118] Per 18. März 2011 erliess die Bundesversammlung einen Bundesbeschluss, durch welchen sie das Übereinkommen des Europarates unter Anbringung einiger Vorbehalte und die damit einhergehenden Gesetzesänderungen genehmigte. Gleichzeitig ermächtigte sie den Bundesrat zur Ratifizierung des Übereinkommens.[119] Ratifiziert wurde das CCC schliesslich am 21. September 2011 und trat anschliessend per 01. Januar 2012 für die Schweiz in Kraft. Zeitgleich wurden die erforderlichen Gesetzesänderungen durch den Bundesrat für verbindlich erklärt.[120]

4.3 Aufbau des CCC

Das CCC lässt sich in drei Teile gliedern.[121] Der erste Teil der Konvention setzt sich aus den allgemeinen Begriffsdefinitionen (Kap. I CCC) und materiellen Strafbestimmungen (Kap. 2 Abschnitt 1 CCC) zusammen. Mit der Vorgabe relevanter Straftatbestände bezweckt das CCC die Harmonisierung des Strafrechts zwischen den einzelnen Vertragsstaaten.[122] Das CCC verpflichtet die Vertragsmitglieder, gewisse Handlungen wie Computerbetrug, Datendiebstahl, Fälschung von Dokumenten mit Hilfe eines Computers, das Eindringen in geschützte Computersysteme und weitere Tatbestände, unter Strafe zu stellen. Weiter verpflichten sich die Vertragsmitglieder, jede Form von Kinderpornogra-

115 Im Strafgesetzbuch (StGB) wurde der Straftatbestand des unbefugten Eindringens in eine Datenverarbeitungsanlage (der sog. „Hacking"-Tatbestand) angepasst, da das CCC eine Vorverlagerung der Strafbarkeit vorsieht. Zudem wurde Art. 18b IRSG neu eingeführt, vgl. BBl 4697, S. 4698.
116 Vgl. EJPD, Mm. vom 13.03.2009; EJPD/BJ, Zf. Vernehmlassungsverfahren, S. 6.
117 Vgl. EJPD/BJ, Zf. Vernehmlassungsverfahren, S. 6.
118 Vgl. EJPD, Mm. vom 18.06.2010.
119 Vgl. AS 2011 6293.
120 Vgl. Der Bundesrat, Mm. vom 15.09.2011.
121 Vgl. auch die Aufteilung in BBl 4697, S. 4700f.
122 Vgl. BBl 2010 4697, S. 4700.

phie sowie die Verletzung von Urheberrechten und verwandten Schutzrechten im Internet strafrechtlich zu ahnden.

Der zweite Teil der Konvention beinhaltet Bestimmungen zum nationalen Strafverfahren (Kap. II Abschnitt 2 CCC). Dabei geht es vor allem um die Frage der Beweiserhebung und der Beweissicherung elektronischer Daten in einer Strafuntersuchung. Da Computerdaten durch Fernzugriff über grosse Distanzen innert Sekunden verändert werden können, werden die Vertragsstaaten verpflichtet, sicherzustellen, dass elektronische Daten während der Strafuntersuchung oder während eines laufenden Strafverfahrens authentisch zur Verfügung stehen und nicht verfälscht oder vernichtet werden können. Von zentraler Bedeutung ist dabei, dass den nationalen Untersuchungsbehörden ein rascher Zugriff auf die betreffenden Daten und deren Sicherstellung ermöglicht wird.[123]

Der dritte und umfangreichste Teil des CCC umfasst die internationale Zusammenarbeit zwischen den Mitgliedstaaten (Kap. III) und die Schlussbestimmungen zum Abkommen (Kap. IV CCC). Die Bestimmungen zur internationalen Kooperation verfolgen das Ziel einer effizienten und schnellen Zusammenarbeit zwischen den verschiedenen Staaten.[124] So kann bspw. nicht nur um die umgehende Sicherung gespeicherter Daten und deren Herausgabe ersucht werden, unter Umständen ist sogar ein unmittelbarer Zugriff auf die Daten möglich.

[123] Vgl. BBl 2010 4697, S. 4701.
[124] Vgl. BBl 2010 4697, S. 4701.

5 Strafbares Verhalten gemäss CCC und StGB

Die im ersten Teil enthaltenen Strafbestimmungen sollen durch die Entwicklung eines Mindeststandards massgeblich zur Harmonisierung des Strafrechts unter den Mitgliedstaaten beitragen. Die Vertragsparteien werden aufgefordert, gewisse Handlungen, welche in Zusammenhang mit den neuen Kommunikationstechnologien begangen werden, unter Strafe zu stellen. Dadurch soll eine verbesserte Zusammenarbeit unter den einzelnen Staaten im Hinblick auf die Bekämpfung der Cyberkriminalität verwirklicht werden.[125] Das folgende Kapitel behandelt die einzelnen Straftatbestände, welche nach den Vorgaben des CCC im Bereich des materiellen Strafrechts zu kriminalisieren sind.[126] Gleichzeitig wird eine Gegenüberstellung mit den jeweiligen Straftatbeständen des Schweizerischen Rechts vorgenommen.

5.1 Art. 2-6 CCC: Straftaten gegen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten und -systemen

5.1.1 Art. 2 CCC: Rechtswidriger Zugang

Mit Art. 2 CCC wird eine international einheitliche Kriminalisierung des „Hacking" angestrebt.[127] Die Staaten werden verpflichtet, jegliche Form des vorsätzlichen und unzulässigen Zugriffs auf Computersysteme oder Teile davon unter Strafe zu stellen. Die Vertragsstaaten können als weitere Voraussetzung für den Eintritt der Strafbarkeit vorsehen, dass eine Umgehung von Sicherheitsmassnahmen, der Vorsatz, Daten zu erhalten, ein anderer unredlicher Vorsatz oder eine Verbindung zu einem anderen Computersystem vorliegen muss.[128]

Mit dem Straftatbestand des „Hacking" wird eine Vorfeldkriminalisierung statuiert, da bereits das Eindringen in ein fremdes Computersysteme für strafbar erklärt wird.[129] Dies ist notwendig, da schon mit dem blossen Eindringen in ein Computersystem die

[125] Vgl. BBl 2010 4697, S. 4700.
[126] Auf Art. 11 CCC (Versuch und Beihilfe oder Anstiftung), Art. 12 CCC (Verantwortlichkeit juristischer Personen) und Art. 13 CCC (Sanktionen und Massnahmen) wird nicht näher eingegangen, da diese kein weiteres, für diese Arbeit relevantes delinquentes Verhalten in Bezug auf die Cyberkriminalität enthalten.
[127] Vgl. BBl 2010 4697, S. 4703; SCHWARZENEGGER, S. 315.
[128] Art. 2 CCC.
[129] Vgl. HERZOG, S. 2.

Rechtssphäre des Nutzers verletzt wird.[130] Gleichzeitig wird dem „Hacking" ein massives Gefährdungspotential für weitere Rechtsgutsverletzungen zugesprochen.[131] Der Schutz vor einem rechtswidrigen Zugriff auf fremde Daten rechtfertigt sich mit dem Interesse, Computersysteme ungestört und unbefangen verwalten, bedienen und kontrollieren zu können. Unberechtigtes Eindringen als solches ist grundsätzlich illegal und soll deshalb verboten werden.[132] Das delinquente Verhalten setzt einen widerrechtlichen Zugriff voraus, weshalb der bewilligte Zugriff auf ein fremdes Computersystem vom Anwendungsbereich der Strafnorm ausgeschlossen ist.[133]

5.1.2 Umsetzung von Art. 2 CCC im „Hacking-Tatbestand" nach Art. 143bis Abs. 1 StGB

Der Straftatbestand des „Hacking" wird im Schweizerischen Strafrecht von Art. 143bis Abs. 1 StGB erfasst. Dieser kriminalisiert den unbefugten Zugriff auf ein fremdes Datenverarbeitungssystem und damit die Vorstufe der unbefugten Datenbeschaffung.[134] Strafbar macht sich demnach, wer in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem mit Vorsatz unbefugt eindringt.[135] Eine Bereicherungsabsicht oder das Verfolgen wirtschaftlicher Zwecke ist nicht erforderlich.[136] Geschütztes Rechtsgut ist die Privatsphäre des Datenverarbeitungssystems[137] und damit das Datenverfügungsrecht des Betreibers[138] und dessen Freiheit, über den Zugang zu seinem Datenverarbeitungssystem bzw. den Datenbeständen frei zu verfügen.[139]

Art. 143bis Abs. 1 StGB deckt im Wesentlichen die Anforderungen von Art. 2 CCC ab. Die Schweiz hat jedoch von der Vorbehaltsmöglichkeit in Art. 2 CCC Gebrauch gemacht, indem sie das Verletzen von Sicherheitsmassnahmen[140] als weitere Voraussetzung zur Erfüllung des Straftatbestandes vorsieht.[141]

---

130 Vgl. SCHWARZENEGGER, S. 315f.
131 Vgl. BALTISSER, S. 59; HERZOG, S. 2; SCHMID, ZStrR, S. 30; SCHWARZENEGGER, S. 307.
132 Vgl. ETS No. 185, Ziff. 44.
133 Vgl. ETS No. 185, Ziff. 47.
134 Vgl. BBl 2010 4697, S. 4703; BSK StGB – FREYTAG, Art. 143bis StGB; StGB PK – TRECHSEL/CRAMERI, Art. 143bis StGB N 1.
135 Das irrtümliche Eindringen in ein fremdes Computersystem fällt nicht unter Art. 143bis StGB, ebenso wenig das befugte Eindringen in ein fremdes Datenverarbeitungssystem,vgl. STRATENWERTH/WOHLERS, Art. 143bis StGB N 1f.; SCHMID, ZStrR, S. 3; StGB PK – TRECHSEL/CRAMERI, Art. 143bis StGB N 9.
136 Die Bereicherungsabsicht wurde mit der Revision von Art. 143bis StGB vom 01.01.2012 gestrichen, vgl. BBl 4607, S. 4708ff.; StGB PK – TRECHSEL/CRAMERI, Art. 143bis StGB N 1.
137 Vgl. StGB PK – TRECHSEL/CRAMERI, Art. 143bis StGB N 2.
138 Vgl. BBl 1991 II 969, S. 1011; BSK StGB – FREYTAG, Art. 143bis StGB.
139 Vgl. BSK StGB – WEISSENBERGER, Art. 143bis StGB N 5.
140 Als Sicherheitsmassnahmen kommen bspw. die Verwendung eines Zugangscodes, einer Verschlüsselung oder dem Einschliessen von Datenträgern in Betracht, vgl. SCHMID, ZStrR, S. 28.
141 Vgl. Vorbehalte und Erklärungen, Schweiz: Erklärung zu Art. 2 CCC.

5.1.3 Art. 3 CCC: Rechtswidriges Abfangen

Mit Art. 3 CCC wird das vorsätzliche, unrechtmässige und mit technischen Mitteln bewirkte Abfangen nicht öffentlicher Computerübertragungen einschliesslich der elektromagnetischen Abstrahlungen unter Strafe gestellt. Den Mitgliedstaaten steht es frei, zur Erfüllung des Straftatbestandes einen Vorbehalt anzubringen, welcher als weitere Voraussetzung eine unredliche Absicht verlangt, oder dass die Straftat an einem Computersystem begangen wurde, welches mit einem anderen Computersystem verbunden ist.[142] Die Bestimmung der Konvention beabsichtigt den Schutz des Rechts auf Privatsphäre beim Datenaustausch und wendet damit das Prinzip des Rechts auf Privatsphäre beim Briefverkehr aus Art. 8 EMRK auf alle Formen des elektronischen Datenaustausches an.[143]

5.1.4 Umsetzung von Art. 3 CCC in Art. 143 StGB

Art. 143 StGB stellt das unrechtmässige Beschaffen unkörperlicher Daten, und damit den Datendiebstahl, unter Strafe.[144] Damit soll das ungestörte und ausschliessliche Verfügungsrecht über die Computerdaten vor unbefugtem Zugriff geschützt werden.[145] Bestraft wird, wer sich mit Vorsatz und Bereicherungsabsicht unrechtmässig elektronische oder in vergleichbarer Weise gesicherte oder übermittelte Daten beschafft, welche nicht für ihn bestimmt und gegen seinen unbefugten Zugriff besonders gesichert sind.[146] Nicht unter diesen Tatbestand fällt demnach der unbefugte Zugriff auf nicht gesicherte Daten oder deren Verwendung.[147] Der Begriff „Datendiebstahl“ ist eine wenig passende Umschreibung der Tathandlung, da die Erfüllung des Straftatbestandes nicht das Beschaffen der Daten im Sinne von Abspeichern etc. voraussetzt; es genügt vielmehr, wenn der Täter die Verfügungsmacht über die Daten erlangt und die dabei gewonnenen Kenntnisse für seine Zwecke einsetzen kann.[148]

Da das StGB ausdrücklich eine Bereicherungsabsicht für die Erfüllung dieses Tatbestandes vorsieht, war es für die Schweiz mit der Einführung des CCC notwendig, einen entsprechenden Vorbehalt zu Art. 3 CCC anzubringen.[149]

---

142 Art. 3 CCC.
143 Vgl. ETS No. 185, Ziff. 51.
144 Vgl. BBl 1991 II 969, S. 1009; BSK StGB – FREYTAG, Art. 143 StGB.
145 Vgl. BSK StGB – WEISSENBERGER, Art. 143 StGB N 3; StGB PR – TRECHSEL/CRAMERI, Art. 143 StGB N 2.
146 Art. 143 Abs. 1 StGB.
147 Vgl. BBl 2010 4697, S. 4705.
148 Vgl. BBl 2010 4697, S. 4705; STRATENWERTH/WOHLERS, Art. 143 StGB N 3; STRATENWERTH et al., § 14 N 31; A.M. StGB PR – TRECHSEL/CRAMERI, Art. 143 StGB N 7 m.w.H.; Vgl. zudem: SCHWARZENEGGER, S. 320.
149 Vgl. Vorbehalte und Erklärungen, Schweiz: Erklärung zu Art. 3 CCC.

5.1.5 Art. 4 CCC: Eingriff in Daten

In Art. 4 CCC wird der Eingriff in Computerdaten behandelt. Die Vertragsparteien verpflichten sich, das Unbrauchbarmachen von Daten durch unbefugtes und vorsätzliches Beschädigen, Löschen, Beeinträchtigen, Verändern oder Unterdrücken von Computerdaten unter Strafe zu stellen.[150] Auch hier gewährt die Konvention eine Vorbehaltsmöglichkeit, wonach die Vertragsparteien als weitere Strafbarkeitsvoraussetzung verlangen können, dass durch den verbotenen Eingriff ein grosser Schaden für den rechtmässigen Besitzer der Computerdaten resultieren muss.[151] Die Definition eines „grossen Schadens" bleibt den einzelnen Vertragsstaaten vorbehalten. [152]

Das Ziel dieser Bestimmung ist der umfassende Schutz von Computerdaten und -programmen vor Beeinträchtigungen jeglicher Art.[153] Unbrauchbar macht Daten, wer – auch mit bloss vorübergehender Wirkung – dem Berechtigten den Gebrauch der Daten verunmöglicht.[154] Da nur unbefugtes Handeln unter diesen Straftatbestand fällt, liegt kein delinquentes Verhalten vor, wenn der Dateneingriff mit Zustimmung des Besitzers erfolgt.[155] Die in Art. 4 CCC enthaltene Regelung passt den klassischen Tatbestand der Sachbeschädigung an die Erfordernisse des Internets an.[156]

5.1.6 Art. 5 CCC: Eingriff in ein System

Art. 5 CCC stellt die unbefugte und vorsätzliche Behinderung der Funktionsweise eines Systems unter Strafe, welche durch das Eingeben von Daten, deren Übermitteln, Beschädigen, Löschen, Beeinträchtigen, Verändern oder Unterdrücken verursacht wird.[157] Eine schwerwiegende Beeinträchtigung liegt bspw. vor, wenn der Täter Daten in grosser Menge oder Frequenz versendet, um die Funktion des empfangenden Computersystems erheblich einzuschränken.[158] Nicht von der Norm erfasst wird der unaufgeforderte Massenversand von E-Mails.[159] Das geschützte Rechtsinteresse liegt im Bedürfnis der

150 Art. 4 Abs. 1 CCC.
151 Art. 4 Abs. 2 CCC.
152 Vgl. ETS No. 185, Ziff. 64.
153 Vgl. ETS No. 185, Ziff. 60; HERZOG, S. 3.
154 Vgl. BBl 2010 4697, S. 4706; ETS No. 185, Ziff. 61.
155 Vgl. ETS No. 185, Ziff. 62.
156 Vgl. HERZOG, S. 3.
157 Art. 5 CCC.
158 Vgl. BBl 2010 4697, S. 4707; ETS No. 185, Ziff. 67.
159 Vgl. BBl 2010 4697, S. 4707; ETS No. 185, Ziff. 69.

Benutzer an der einwandfreien Funktion seiner Computer- und Telekommunikationssysteme.[160]

Der Text der Konvention wurde bewusst offen formuliert, sodass jegliche Art der Funktionsbeeinträchtigung solcher Systeme vom Schutzbereich dieser Bestimmung erfasst wird.[161]

5.1.7 Umsetzung von Art. 4 und Art. 5 CCC in Art. 144bis Ziff. 1 StGB

In der Schweizerischen Rechtsordnung deckt Art. 144bis Ziff. 1 StGB neben dem Eingriff in Daten auch den Eingriff in Systeme ab. Art. 144bis Ziff. 1 StGB stellt sowohl das unrechtmässige Verändern, Löschen und Unbrauchbarmachen von elektronischen oder in vergleichbarer Weise gespeicherten oder übermittelten Daten als auch das Verhindern des Zugangs zu den eigenen Daten während einer erheblichen Zeitspanne[162] unter Strafe.[163] Soweit dabei kein grosser Schaden verursacht wird, handelt es sich bei Art. 144bis Ziff. 1 StGB um ein Antragsdelikt; resultiert hingegen ein grosser Schaden, erfolgt die Strafverfolgung von Amtes wegen.[164] Mit diesem Artikel wird die legitime Verfügungsgewalt über die Daten geschützt, denn es soll das Interesse des Verfügungsberechtigten an der ungestörten Verwendbarkeit seiner intakten Daten gewährleistet werden.[165]

5.1.8 Art. 6 CCC: Missbrauch von Vorrichtungen

Art. 6 CCC stellt das unbefugte und vorsätzliche Herstellen, Verkaufen, Verschaffen zum Gebrauch, Einführen, Verbreiten oder anderweitige Verfügbarmachen von Vorrichtungen, Computer-Programmen, Zugangscodes sowie Passwörtern, die zur Begehung einer Straftat im Sinne der vorstehenden Artikel 2-5 CCC gebraucht werden, unter Strafe.[166] Des Weiteren erklärt Art. 6 CCC den Besitz solchen Materials für strafbar, wenn es mit dem Vorsatz gehalten wird, dieses im Rahmen einer der genannten Straftaten einzusetzen.[167] Auch an dieser Stelle gewährt die Konvention den Mitgliedstaaten verschiedenste Möglichkeiten, Vorbehalte anzubringen. So kann entweder der strafbare Besitz an eine

---

160 Vgl. ETS No. 185, Ziff. 65.
161 Vgl. ETS No. 185, Ziff. 65.
162 Vgl. BBl 2010 4697, S. 4707.
163 Art. 144bis Ziff. 1 StGB; Die Aufzählung ist abschliessend, vgl. StGB PR – TRECHSEL/CRAMERI, Art. 143bis StGB N 4.
164 Art. 144bis Ziff. 1 Satz 1 und 2 StGB.
165 Vgl. BALTISSER, S. 67; BSK StGB – WEISSENBERGER, Art. 144bis StGB N 6; StGB PR – TRECHSEL/CRAMERI, Art. 144bis StGB N 2; STRATENWERTH/WOHLERS, Art. 144bis StGB N 1; Für Beispiele des Verändern, Löschen oder Unbrauchbarmachens von Daten vgl. StGB PR – TRECHSEL/CRAMERI, Art. 143bis StGB N 5ff. m.w.H sowie STRATENWERTH/WOHLERS, Art. 144bis StGB N 1.
166 Art. 6 Abs. 1 lit. a CCC.
167 Art. 6 Abs. 1 lit. b CCC; Vgl. zudem: BBl 2010 4697, S. 4707.

Mindestzahl solchen Materials gekoppelt, oder aber ein genereller Vorbehalt der Anwendbarkeit von Art. 6 CCC angebracht werden. Zwingend müssen die Vertragsstaaten aber den Verkauf, das Verbreiten und das Verfügbarmachen von Passwörtern, Codes oder ähnlichen Daten, welche einen Zugang zu einem Computersystem ermöglichen, unter Strafe stellen.[168]

Der Anwendungsbereich von Art. 6 CCC beschränkt sich auf Vorrichtungen, welche ausschliesslich zum Zweck der Begehung einer Straftat entwickelt werden.[169] Dies schliesst die Anwendung der Bestimmung bzgl. sog. „dual-use-Programme" aus, welche sowohl für kriminelle als auch legale Zwecke eingesetzt werden können.[170] Auch das Herstellen, der Verkauf, das Beschaffen zwecks Gebrauch, das Einführen, das Verbreiten oder anderweitige Verfügbarmachen oder der Besitz solchen Materials, welches nicht den Zweck der Begehung von Straftaten nach Art. 2-5 CCC umfasst, sondern bspw. für genehmigte Tests oder zum Schutz von Computersystemen gehalten wird, ist vom Anwendungsbereich des Art. 6 CCC ausgeschlossen.[171] Sicherheitstests an Computersystemen sowie die Neuentwicklung von Software zu diesem Zweck bleiben demnach straffrei, da sie entweder durch den Befugten selbst durchgeführt oder von diesem in Auftrag gegeben wurden.[172]

5.1.9 Umsetzung von Art. 6 CCC im „Viren-Tatbestand" nach Art. 144bis Ziff. 2 StGB

Art. 144bis Ziff. 2 StGB stellt selbstständige Handlungen im Zusammenhang mit Computerviren, welche auf die Beschädigung von Daten abzielen, unter Strafe.[173] Strafbar macht sich, wer Programme, von denen er weiss oder annehmen muss, dass sie zum Zweck der Datenbeschädigung oder -veränderung verwendet werden sollen, herstellt, einführt, in Verkehr bringt, anpreist, anbietet oder anderweitig zugänglich macht oder zu ihrer Herstellung Anleitung gibt.[174] Wie in Ziff. 1 wird auch bei Ziff. 2 die legitime Verfügungsgewalt über die eigenen Daten geschützt, mithin das Interesse des Verfügungsberechtigten an der ungestörten Verwendbarkeit der eigenen Daten.[175] Die Schweiz behält sich das Recht vor, Art. 6 Abs. 1 CCC nur anzuwenden, wenn das straf-

168 Art. 6 Abs. 3 CCC; Vgl. zudem: BBl 2010 4697, S. 4708; ETS No. 185, Ziff. 75ff.
169 Vgl. ETS No. 185, Ziff. 73.
170 Vgl. ETS No. 185, Ziff. 73; A.M. HERZOG, S. 4.
171 Art. 6 Abs. 2 CCC; Vgl. zudem: ETS No. 185, Ziff. 77.
172 Vgl. BBl 2010 4697, S. 4710.
173 Vgl. BSK StGB – WEISSENBERGER, Art. 144bis StGB N 4.
174 Art. 144bis Ziff. 2 StGB.
175 Vgl. BGE 129 IV 230 E. 2.1.1f.; BALTISSER, S. 71; BSK StGB – WEISSENBERGER, Art. 144bis StGB N 6.

rechtlich relevante Verhalten im Verkaufen, Verbreiten oder anderweitigen Verfügbarmachen von Mitteln gem. Art. 6 Abs. 1 lit. a Ziff. ii liegt.[176]

5.2 Art. 7 und Art. 8 CCC: Computerbezogene Straftaten

5.2.1 Art. 7 CCC: Computerbezogene Fälschung

Die Konvention erklärt in Art. 7 CCC das vorsätzlich und unbefugt vorgenommene Eingeben, Verändern, Löschen oder Unterdrücken von Computerdaten als strafbar, wenn daraus manipulierte Datenverarbeitungsergebnisse resultieren.[177] Damit wird das Erstellen von nicht-authentischen Daten, welche wie authentische Daten wirken sollen, bestraft.[178] Den Vertragsstaaten steht es frei, einen Vorbehalt anzubringen, wonach für die Erfüllung des Tatbestandes zusätzlich betrügerische oder ähnlich unredliche Absichten vorliegen müssen.[179]

Das geschützte Rechtinteresse liegt in der Sicherheit und Verlässlichkeit elektronischer Daten, deren Veränderung zu massiven Auswirkungen führen könnte. Die Autoren der Konvention beabsichtigten mit Art. 7 CCC eine analoge Bestimmung zu den traditionellen Urkundendelikten zu schaffen, welche den Verhältnissen der Datennutzung im Internet gerecht wird. Schliesslich kann die Manipulation von Computerdaten, welchen hohe Beweiskraft zukommt, die gleichen ernsthaften Konsequenzen nach sich ziehen, wie die traditionelle Urkundenfälschung, insbesondere, wenn damit die Täuschung eines Dritten beabsichtigt wird.[180]

5.2.2 Art. 8 CCC: Computerbezogener Betrug

Mit Art. 8 CCC wird das vorsätzliche und unrechtmässige Bewirken eines Vermögensverlustes zulasten einer anderen Person mit der betrügerischen oder unredlichen Absicht unter Strafe gestellt, sich oder einem anderen einen Vermögensvorteil zu verschaffen.[181] Der Vermögensverlust muss auf der Eingabe, der Änderung, der Unterdrückung oder dem Löschen von Computerdaten beruhen[182] oder durch eine andere Beeinträchtigung

[176] Vgl. Vorbehalte und Erklärungen, Schweiz: Vorbehalt zu Art. 6 Abs. 3 CCC; Vgl. zudem: BBl 2010 4697, S. 4710.
[177] Art. 7 CCC.
[178] Vgl. BBl 2010 4697, S. 4710; HERZOG, S. 4.
[179] Art. 7 CCC.
[180] Vgl. ETS No. 185, Ziff. 81.
[181] Art. 8 CCC; Vgl. zudem: BBl 2010 4697, S. 4711; HERZOG, S. 4.
[182] Art. 8 lit. a CCC.

der Funktionsweise des Computersystems[183] bewirkt werden. Dieser Tatbestand entspricht jenem klassischen Delikt der betrügerischen Kommunikationsmanipulation unter Menschen, welche mit der Absicht begangen wird, sich einen Vermögensvorteil zu Lasten eines ökonomischen oder besitzrechtlichen Vermögensverlustes eines Dritten zu verschaffen.[184]

Sowohl die Straftat als auch die Vermögensbereicherung müssen unrechtmässig erfolgen. Damit fallen legale Geschäftstätigkeiten, welche ebenfalls eine ökonomische Wertgewinnung beabsichtigen, selbstverständlich nicht unter den Anwendungsbereich dieses Artikels.[185] Indem Art. 8 CCC einen betrügerischen oder anderweitig unehrlichen Vorsatz bzgl. der Bereicherung verlangt, werden Handlungen, welche zwar einen ökonomischen Schaden des einen und einen ökonomischen Vorteil des andern verursachen, nicht von Art. 8 CCC erfasst, solange der entsprechende Vorsatz fehlt.[186]

5.2.3 Umsetzung von Art. 7 und Art. 8 CCC in Art. 147 StGB

Im Schweizerischen Strafrecht werden die Tathandlungen des computerbezogenen Betruges und der computerbezogenen Fälschung in Art. 147 StGB, dem betrügerischen Missbrauch einer Datenanlage, erfasst.[187] Dieser verbietet sowohl das vorsätzliche Einwirken auf eine Datenverarbeitungs- oder Datenübermittlungsanlage wie auch das unrichtige, unvollständige oder unbefugte Verwenden von Daten mit Bereicherungsabsicht.[188] Vorausgesetzt wird, dass das delinquente Verhalten eine Vermögensverschiebung zum Schaden eines anderen herbeiführt oder eine unmittelbar anschliessende Vermögensverschiebung verdeckt.[189] Art. 147 StGB verlangt, dass zur Vollendung des Delikts eine tatsächliche Vermögensverschiebung vorliegen muss. Nicht verlangt wird aber, dass der Täter tatsächlich einen finanziellen Vorteil erlangt.[190] Indem die Schweiz für die tatbestandsmässige Erfüllung die Absicht einer Schadensverursachung oder

183 Art. 8 lit. b CCC.
184 Vgl. ETS No. 185, Ziff. 88; Der Begriff „Vermögensverlust" umfasst demnach sowohl den Verlust von materiellen als auch immateriellen Vermögenswerten mit entsprechendem ökonomischen Wert, vgl. HERZOG, S. 4.
185 Vgl. ETS No. 185, Ziff. 89.
186 Vgl. ETS No. 185, Ziff. 90.
187 Vgl. BBl 2010 4697, S. 4711.
188 Art. 147 Abs. 1 StGB.
189 Art. 147 Abs. 1 StGB; für Beispiele zur unrichtigen, unvollständigen oder unbefugten Verwendung von Daten vgl. StGB PK – TRECHSEL/CRAMERI, Art. 147 StGB N 4ff.; STRATENWERTH/WOHLERS, Art. 147 StGB 3.
190 Vgl. BBl 2010 4697, S. 4711.

Vorteilserwirkung vorrausetzt, war das Anbringen eines entsprechenden Vorbehalts zu Art. 7 CCC notwendig.[191]

Im Unterschied zum klassischen Betrugstatbestand von Art. 146 StGB wird in Art. 147 StGB die Vermögensverschiebung nicht durch den hervorgerufenen Irrtum eines menschlichen Opfers ausgelöst, sondern rein durch die Manipulation der Daten verursacht.[192] Art. 147 StGB soll entsprechend das Vermögen der betroffenen Person als zentrales Rechtsgut schützen[193] und damit gleichzeitig eine Lücke im Strafrecht schliessen.[194]

5.3 Art. 9 CCC: Inhaltsbezogene Straftaten

5.3.1 Art. 9 CCC: Straftaten mit Bezug zu Kinderpornographie

Die Verbreitung von Kinderpornographie über das Internet wird in Art. 9 CCC kriminalisiert. Damit wird dem Problem der flutwellenartigen Verbreitung von Kinderpornographie über das Internet Rechnung getragen.[195] Bestraft wird, wer Kinderpornographie zum Zweck ihrer Verbreitung über ein Computersystem herstellt, anbietet oder verfügbar macht, verbreitet oder übermittelt, für sich selbst oder einen anderen über ein Computersystem beschafft oder Kinderpornographie in einem Computersystem oder auf einem Computerdatenträger besitzt.[196]

Der Begriff „Kinderpornographie“ umfasst visuelle Darstellungen einer minderjährigen Person bei eindeutig sexuellen Handlungen, visuelle Darstellungen einer Person mit dem Erscheinungsbild einer minderjährigen Person bei eindeutig sexuellen Handlungen oder visuelle Darstellungen real erscheinender Bilder, die eine minderjährige Person bei eindeutig sexuellen Handlungen zeigen.[197] Als „minderjährige Personen“ gelten in Übereinstimmung mit der UN-Konvention für die Rechte der Kinder[198] alle Personen, welche

191 Vgl. Vorbehalte und Erklärungen, Schweiz: Erklärung zu Art. 7 CCC; Vgl. zudem: BBl 2010 4697, S. 4710.
192 Vgl. BGE 129 IV 315 E. 2.1; BBl 2010 4697, S. 4771; SCHMID, ZStrR, S. 35f.
193 Vgl. BSK StGB – FIOLKA, Art. 147 StGB N 7; SCHMID, ZStrR, S. 35.
194 Vgl. BEG 129 IV 315 E. 2.1; StGB PK – TRECHSEL/CRAMERI, Art. 147 StGB N 1; STRATENWERTH/WOHLERS, Art. 147 StGB N 1.
195 Vgl. HERZOG, S. 4.
196 Art. 9 Abs. 1 CCC; Vgl. zudem: BBl 2010 4697, S. 4711.
197 Art. 9 Abs. 2 CCC.
198 Art. 1 UN-Convention on the Right of the Child; Vgl. zudem: ETS No. 185, Ziff. 104.

das 18. Lebensjahr noch nicht vollendet haben.[199] Da einzelne Staaten in ihrer Rechtsordnung eine tiefere Altersgrenze bzgl. Kinderpornographie festhalten, sieht die Konvention die Möglichkeit vor, einen entsprechenden Vorbehalt anzubringen, wobei das Alter von 16 Jahren nicht unterschritten werden darf.[200] Weiter gibt Art. 9 CCC die Möglichkeit, die Anwendbarkeit gewisser Teile des Artikels durch Abgabe einer entsprechenden Erklärung auszuschliessen.[201]

5.3.2 Umsetzung von Art. 9 CCC in Art. 197 Abs. 4 und Abs. 5 StGB

In der Schweiz werden die entsprechenden Tathandlungen aus Art. 9 CCC und insbesondere auch der Besitz oder das Herunterladen von kinderpornographischem Material auf elektronischen Datenträgern in Art. 197 Abs. 4 und Abs. 5 StGB unter Strafe gestellt.[202] Das Verbot soll die ungestörte Entwicklung von Kindern und Jugendlichen ermöglichen. Gleichzeitig sollen erwachsene Verbraucher vor einer Nachahmung abgehalten werden.[203]

Das Alter der sexuellen Mündigkeit lag in der Schweiz zum Zeitpunkt der Ratifizierung des Abkommens bei 16 Jahren,[204] weshalb damals eine entsprechende Erklärung abgeben wurde.[205] Mit der Ratifizierung der Lanzarote-Konvention[206] und der damit einhergehenden Änderung des StGB per 01. Juli 2014[207] ist diese Erklärung hinfällig geworden. Zwar liegt das Alter der sexuellen Mündigkeit nach Art. 187 StGB noch immer bei 16 Jahren, jedoch geniessen Personen unter dem Begriff „Minderjährige“ bis zum vollendeten 18. Lebensjahr unter Art. 197 Abs. 4 und Abs. 5 StGB einen strafrechtlichen Schutz vor der zwangsweisen Mitwirkung bei sexuellen Darbietungen.[208] Mit dieser Gesetzes-

---

199 Art. 9 Abs. 3 CCC; Das Etablieren eines einheitlichen internationalen Standards bzgl. des Alters galt innerhalb der Diskussionen rund um die „Konstruktion“ des Artikels als zentrales politisches Thema. Während der politischen Debatte musste aber festgestellt werden, dass einzelne Staaten in ihrem Recht eine tiefere Altersgrenze bezüglich Kinderpornographie festhalten, weshalb in der Endfassung der Konvention den Parteien die Freiheit belassen wurde, ein tieferes Mindestalter vorzusehen, wobei 16 Jahre nicht unterschritten werden dürfen. An dieser Stelle ist darauf hinzuweisen, dass sich das Alter der Kinder auf deren Missbrauch als Sexualobjekt und nicht auf das Alter einer Zustimmung zu einer sexuellen Beziehung. Vgl. ETS No. 185, Ziff. 104.

200 Art. 9 Abs. 3 CCC; Vgl. zudem: ETS No. 185, Ziff. 104.

201 Art. 9 Abs. 4 CCC.

202 Art. 197 Abs. 4 und Abs. 5 StGB; In BBl 2010 4697, S. 4711 ist noch die Rede von Art. 197 Ziff. 3 und 3bis aStGB.

203 BGE 131 IV 16 E. 1.2; BSK StGB – MENG, Art. 197 StGB N 22.

204 Art. 187 StGB.

205 Vgl. Vorbehalte und Erklärungen, Schweiz: Erklärung zu Art. 9 Abs. 3 CCC.

206 Vgl. AS 2014 1159.

207 Vgl. EJPD, Mm. vom 07.03.2014.

208 Vgl. BBl 2012 7571, S. 7617.

änderung kommt das Schweizerische Strafrecht den Anforderungen von Art. 9 Abs. 3 CCC bzgl. Alter vollumfänglich nach.

Die Schweiz hat die Anwendbarkeit von Art. 9 Abs. 2. lit. b CCC hinsichtlich der Kriminalisierung von visuellen Darstellungen einer Person mit dem Erscheinungsbild einer minderjährigen Person bei eindeutig sexuellen Handlungen mittels Vorbehalt ausgeschlossen.[209] Damit beseitigt sie Unstimmigkeiten bzgl. der Interpretation des Ausdrucks „Erscheinungsbild einer minderjährigen Person." Denn sollte dieser dahingehend ausgelegt werden, dass nicht erkennbar ist, ob es sich tatsächlich um eine minderjährige Person handelt, wären neben den Minderjährigen auch Erwachsene, welche wie Minderjährige aussehen, zu schützen. Eine Ausweitung des Straftatbestandes in diese Richtung erscheint gem. Bundesrat nicht angebracht.[210]

5.4 Art. 10 CCC: Straftaten in Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte

5.4.1 Art. 10 CCC: Verletzung des Urheberrechts und verwandter Schutzrechte

Art. 10 CCC befasst sich mit der Verletzung des geistigen Eigentums und Urheberrechten durch Downloads (Herunterladen von Daten) im Internet. Bestraft wird, wer vorsätzlich, in gewerbsmässigem Umfang und mittels Computersystemen Urheberrechtsverletzungen oder Verletzungen verwandter Schutzrechte begeht, wie sie im nationalen Recht der jeweiligen Vertragspartei aufgrund deren Verpflichtungen aus einzelnen internationalen Übereinkünften festgehalten sind.[211] Den Parteien erwachsen dabei nur aus jenen völkerrechtlichen Übereinkommen Verpflichtungen, welche sie auch ratifiziert haben.[212] Diese erfahren allenfalls Beschränkungen, wenn die jeweilige Vertragspartei zu einzel-

[209] Vgl. Vorbehalte und Erklärungen, Schweiz: Vorbehalt zu Art. 9 Abs. 4 CCC.
[210] Vgl. BBl 2010 4697, S. 4711f.
[211] Art. 20 Abs. 1 und 2 CCC; Die massgebenden Verträge in Bezug auf die Urheberrechtsverletzung sind (Abs. 1): die Pariser Fassung der Berner Übereinkunft zum Schutz von Werken der Literatur und Kunst vom 24. Juli 1971 (SR 0.231.15), das Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums (SR 0.632.20 Anhang 1.C) und der WIPO-Urheberrechtsvertrag (SR 0.231.151). Die massgebenden Verträge in Bezug auf die Verletzung verwandter Schutzrechte sind (Abs. 2): Das internationale Abkommen über den Schutz der ausübenden Künstler, der Hersteller von Tonträger und der Sendeunternehmen (Abkommen von Rom; SR 0.231.171), das Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums und der WIPO-Vertrag über Darbietungen und Tonträger (SR 0.231.171.1).
[212] Vgl. BBl 2010 4697, S. 4713; ETS No. 185, Ziff. 110.

nen Bestimmungen Vorbehalte oder Erklärungen abgegeben hat.[213] Soweit die internationalen Verpflichtungen aus den völkerrechtlichen Übereinkünften nicht beeinträchtigt werden, können sich die Vertragsparteien das Recht vorbehalten, bei einer begrenzten Anzahl von Fällen[214] von einer strafrechtlichen Verantwortlichkeit nach Abs. 1 und Abs. 2 abzusehen, sofern andere wirksame Abhilfen wie bspw. Bestimmungen aus dem Zivil- oder dem öffentlichen Recht zur Verfügung stehen.[215]

Die Definition von Urheberrecht und verwandter Schutzrechte untersteht dem nationalen Recht der Mitgliedstaaten, weshalb diese stark variieren kann. Art. 10 CCC selbst schützt nur Rechtsgutsverletzungen des geistigen Eigentums aus den im Artikel genannten Abkommen. Nicht in den Schutzbereich von Art. 10 CCC fallen somit bspw. patent- oder marktrechtliche Verletzungen.[216]

5.4.2 Umsetzung von Art. 10 CCC in Art. 67-69a URG

Die Schweiz hat sämtliche völkerrechtliche Abkommen aus Art. 10 Abs. 1 und Abs. 2 CCC ratifiziert und die in den internationalen Übereinkommen vorgesehenen Rechte im Urheberrechtsgesetz anerkannt. Die entsprechenden Verletzungen des Urheberrechts und der verwandten Schutzrechte sind in den Art. 67-69a URG als Straftatbestände enthalten.[217] Sie kriminalisieren u.a. das vorsätzliche und gewerbsmässige Verletzen von Urheberrechten und verwandten Schutzrechten mit Hilfe eines Computersystems.[218] Indem im URG nicht gewerbsmässige Verletzungen auf Antrag verfolgt werden können, geht dieses über die Anforderungen von Art. 10 CCC hinaus.[219]

213 Vgl. ETS No. 185, Ziff. 110.
214 So z.B. bei Parallel-Importen oder dem Mietrecht, vgl. ETS No. 185, Ziff. 116.
215 Art. 10 Abs. 3 CCC.
216 Vgl. ETS No. 185, Ziff. 109.
217 Vgl. BBl 2010 4697, S. 4713.
218 Vgl. SCHWARZENEGGER, ZSR, S. 462f.
219 Vgl. BBl 2010 4697, S. 4714.

6 Die Instrumente des CCC zur internationalen Zusammenarbeit

Das folgende Kapitel widmet sich den besonderen Bestimmungen des CCC zur internationalen Zusammenarbeit. Insbesondere werden die neuen Instrumente zur internationalen Strafverfolgung und Zusammenarbeit aus Kap. III, Abschnitt 2 CCC[220] vorgestellt. Gleichzeitig wird, wo notwendig und verfügbar, auf die entsprechenden Schweizerischen Bestimmungen aus dem IRSG eingegangen.

6.1 Art. 29 und Art. 30 CCC: Rechtshilfe bei vorläufigen Massnahmen

In Art. 29 und 30 CCC sind vorläufige Massnahmen enthalten, welche einem formellen Rechtshilfeersuchen vorausgehen. Sie sind notwendig, da oftmals erst durch sie wichtige und grundlegende Informationen für das Stellen eines Rechtshilfeersuchens gewonnen werden können.

6.1.1 Art. 29 CCC Umgehende Sicherung gespeicherter Computerdaten

Art. 29 CCC ermöglicht mittels Ersuchen die umgehende Sicherung gespeicherter Computerdaten. Gestützt auf diesen Artikel kann eine Vertragspartei eine andere Vertragspartei vor der Durchführung eines ordentlichen Rechtshilfeverfahrens um die Anordnung oder anderweitige Bewirkung der umgehenden Sicherung von Daten ersuchen, welche mittels eines Computersystems im Hoheitsgebiet der anderen Vertragspartei gespeichert sind. Für die umgehende Sicherung gespeicherter Daten wird vorausgesetzt, dass die ersuchende Vertragspartei beabsichtigt, ein Rechtshilfeersuchen betreffend Durchsuchung oder ähnlichen Zugriff, Beschlagnahme oder ähnliche Sicherstellung oder Weitergabe der Daten zu stellen.[221] Beim Instrument nach Art. 29 CCC handelt es sich somit um eine vorläufige und zeitlich begrenzte Massnahme. Sie bezweckt die Daten bis zur Behandlung und Erledigung des langwierigen Rechtshilfeersuchens verfügbar zu halten.[222] Nach Eingang eines Ersuchens um umgehende Sicherung gespeicherter Computerdaten hat die ersuchte Vertragspartei alle geeigneten Massnahmen zur Sicherung der bezeichneten Daten in Übereinstimmung mit ihrem innerstaatlichen Recht vorzunehmen. Das Vorliegen der beidseitigen Strafbarkeit wird vom CCC zu diesem Verfah-

[220] Auf Art. 35 CCC wird nicht näher eingegangen, da dieser lediglich Aussagen über das Netzwerk 7/24 macht, auf welches im Rahmen dieser Arbeit nicht eingegangen wird.
[221] Art. 29 Abs. 1 CCC.
[222] Vgl. BBl 2010 4697, S. 4731; ETS No. 185, Ziff. 282; HEIMGARTNER, S. 144f.

renszeitpunkt grundsätzlich noch nicht vorausgesetzt.[223] Die gesetzliche Frist, während derer der ersuchte Staat zur Sicherung der Daten verpflichtet ist, beträgt 60 Tage.[224] Wird das in Aussicht gestellte formelle Rechtshilfeersuchen der ausländischen Behörde nicht innerhalb dieser Frist eingereicht, darf die vorgenommene Sicherungskopie vernichtet werden.[225] Geht ein formelles Rechtshilfeersuchen innert der gesetzlichen Frist ein, dürfen die gesicherten Daten nicht mehr gelöscht werden, bis über das Ersuchen entschieden wurde.[226]

Die Massnahme nach Art. 29 CCC wirkt schneller als ein ordentliches Rechtshilfeverfahren und stellt gleichzeitig auch einen geringeren Eingriff in die Rechte der Betroffenen dar.[227] Deren Rechte auf Achtung der Privatsphäre werden gewahrt, indem zum Zeitpunkt dieses Verfahrensstadiums noch keine Herausgabe der Daten verlangt wird, sondern lediglich der Verwahrer der Daten[228] durch die ersuchte Vertragspartei zur Sicherung der entsprechenden Daten aufgefordert wird. Die Weitergabe der Daten erfolgt erst, wenn alle Kriterien für eine vollständige Offenlegung erfüllt sind.[229]

Das CCC setzt zu diesem Verfahrenszeitpunkt zwar noch keine beidseitige Strafbarkeit voraus, es bietet aber jenen Vertragsstaaten, welche die beidseitige Strafbarkeit als Voraussetzung für die Erledigung eines Rechtshilfeersuchens um Durchsuchung oder ähnlichen Zugriff, Beschlagnahme oder ähnliche Sicherstellung oder Weitergabe gespeicherter Computerdaten verlangen, die Möglichkeit, einen entsprechenden Vorbehalt anzubringen.[230] Demnach können Ersuche um die umgehende Sicherung gespeicherter Computerdaten abgelehnt werden, wenn sich diese auf andere Straftaten als jene in den Art. 2-11 CCC beziehen und Grund zur Annahme besteht, dass die Voraussetzungen der beidseitigen Strafbarkeit im Zeitpunkt der Weitergabe der Daten nicht erfüllt werden kann.[231] Weitere allfällige Ablehnungen eines Sicherungsgesuches sind an strenge Voraussetzungen geknüpft. Laut Art. 29 Abs. 5 CCC kann ein Sicherungsersuchen nur abgelehnt werden, wenn dessen Durchführung die Souveränität, Sicherheit, öffentliche Ordnung oder andere wesentliche Interessen des ersuchten Staates beeinträchtigt, oder

223 Art. 29 Abs. 3 CCC; Vgl. zudem: ETS No. 185, Ziff. 285.
224 Art. 29 Abs. 7 CCC.
225 Vgl. BBl 2010 4697, S. 4732; Vgl. zudem: GSTÖHL, S. 175f., 199ff., zu vorsorglichen Massnahmen allgemein; GSTÖHL, S. 235ff., zu Zwangsmassnahmen im Post- und Fernmeldeverkehr.
226 Art. 29 Abs. 7 CCC.
227 Vgl. BBl 2010 4697, S. 4731f.
228 Häufig sind dies Dienstanbieter oder andere Drittparteien.
229 Vgl. BBl 2010 4697, S. 4732; ETS No. 185, Ziff. 283.
230 Vgl. ETS No. 185, Ziff. 286.
231 Art. 29 Abs. 4 CCC.

wenn der ersuchte Staat die Straftat als politische oder mit einer solchen zusammenhängenden Straftat ansieht.[232]

Die Schweiz hat von der Vorbehaltsmöglichkeit aus Art. 29 Abs. 4 CCC Gebrauch gemacht.[233] Dies zurecht, erscheint es doch sinnlos, eine vorläufige Sicherung der Daten vorzunehmen, wenn bereits beim Ersuchen um die vorläufige Sicherung der Daten feststeht, dass einem späteren Rechtshilfeersuchen um deren Herausgabe aufgrund der mangelnden beidseitigen Strafbarkeit nicht entsprochen werden kann.[234] Weiter empfiehlt der Bundesrat allgemein die Ablehnung eines Ersuchens, wenn zum Zeitpunkt der Entscheidung über die Anordnung der vorläufigen Massnahme fest steht, dass einem später folgenden Rechtshilfeersuchen um die Herausgabe der gespeicherten Daten nicht entsprochen werden kann. Der Bundesrat stützt seine Empfehlung dabei auf Art. 31 CCC, welcher die Verweigerung eines Rechtshilfeersuchens gestützt auf das geltende innerstaatliche Recht und die anwendbaren Verträge ermöglicht.[235]

6.1.2 Umsetzung der umgehenden Datensicherung in Art. 18 IRSG

Den Anforderungen von Art. 29 CCC an das nationale Recht entspricht in der Schweiz Art. 18 IRSG. Dieser sieht unter dem Titel „vorläufige Massnahmen“ unter anderem vor, dass auf ausdrückliches Ersuchen eines anderen Staates die zuständige Behörde vorläufige Massnahmen zur Erhaltung des bestehenden Zustandes, zur Wahrung bedrohter rechtlicher Interessen oder zur Sicherung gefährdeter Beweismittel anordnen kann.[236] Ist Gefahr im Verzug, können vorsorgliche Massnahmen auch ohne entsprechendes Ersuchen durch das BJ angeordnet werden, sofern ein solches vom ersuchenden Staat angekündigt wird.[237] Dabei genügt es, wenn sich die Ankündigung auf das Stellen eines Rechtshilfeersuchens bezieht; die Ankündigung eines Ersuchens um vorläufige Massnahmen ist dann nicht mehr nötig. In einem solchen Fall prüft die zuständige Behörde selbst, welche Massnahmen in der betreffenden Situation erforderlich sind.[238]

Mit Art. 18 IRSG wird die Anordnung vorläufiger Massnahmen zur Unterstützung eines ausländischen Strafverfahrens ermöglicht. Ein Ersuchen für die Anordnung vorläufiger Massnahmen trifft meist zu einem Zeitpunkt ein, in welchem der ersuchende Staat

---

232 Art. 29 Abs. 5 CCC.
233 Vgl. Vorbehalte und Erklärungen, Schweiz: Vorbehalt zu Art. 29 Abs. 4 CCC.
234 Vgl. auch: ISSS[1], S. 27.
235 Vgl. BBl 2010 4697, S. 4733.
236 Art. 18 Abs. 1 IRSG.
237 Art. 18 Abs. 2 IRSG; Vgl. zudem: DONATSCH et al., S. 133; GLESS, Rz. 303.
238 Vgl. DONATSCH et al., S. 133.

(noch) nicht in der Lage ist, ein Rechtshilfeersuchen zu stellen. Zur Anordnung der vorläufigen Massnahmen nach Art. 18 IRSG genügt die blosse Möglichkeit eines zukünftigen Rechtshilfeersuchens. Unerheblich ist, ob ein Rechtshilfeersuchen zu einem späteren Zeitpunkt tatsächlich eingereicht wird.[239]

Die vorläufigen Massnahmen nach Art. 18 bezwecken wie Art. 29 CCC die Sicherung des gegenwärtigen Zustandes während des Rechtshilfeverfahrens,[240] die Wahrung bedrohter rechtlicher Interessen bzw. die Sicherung gefährdeter Beweismittel.[241] Deshalb bleiben die vorläufigen Massnahmen grundsätzlich bis zum definitiven Entscheid über die Rechtshilfeleistung bestehen.[242] Für die Zulässigkeit von vorsorglichen Massnahmen ist entscheidend, dass die allgemeinen Voraussetzungen der Rechtshilfe prima facie erfüllt sind.[243]

Ein Ersuchen um die Anordnung vorläufiger Massnahmen nach Art. 18 IRSG unterliegt grundsätzlich der Vorprüfung durch das BJ. Die Weiterleitung des Ersuchens an die ausführende Behörde entscheidet sich nach der Zulässigkeit der Rechtshilfe. Die ausführende Behörde tritt schliesslich mittels Eintretensverfügung auf das Ersuchen ein.[244] Die Anordnung vorläufiger Massnahmen erfolgt durch die ausführende Behörde mittels Erlass einer Zwischenverfügung.[245] In Fällen des direkten Verkehrs laufen die Ersuche über die Meldestelle KOBIK.[246]

6.1.3 Art. 30 CCC: Umgehende Weitergabe gesicherter Verkehrsdaten

Wurde ein Ersuchen zur umgehenden Sicherung gespeicherter Computerdaten nach Art. 29 CCC eingereicht, ermöglicht Art. 30 CCC die umgehende Weitergabe gesicherter Verkehrsdaten. Vorausgesetzt wird, dass die ersuchte Vertragspartei bei der Erledigung eines Ersuchens nach Art. 29 CCC feststellt, dass ein Dienstanbieter in einem anderen Staat an der Übermittlung der Kommunikation beteiligt war.[247] In diesem Fall gibt die ersuchte Vertragspartei umgehend Verkehrsdaten in ausreichender Menge an die ersu-

239 Vgl. BSK ISTR – AEPLI, Art. 18 IRSG N 11.
240 Vgl. DONATSCH et al., S. 132; GLESS, Rz. 303.
241 Vgl. BSK ISTR – AEPLI, Art. 18 IRSG N 26; POPP, Rz. 491.
242 Vgl. Wegleitung, 61; Davon ausgenommen sind die vorsorglichen Massnahmen nach Art. 18 Abs. 2 Satz 2 IRSG, vgl. GLESS, Rz. 303.
243 Vgl. DONATSCH et al., S. 133; POPP, Rz. 493 m.w.H.; Wegleitung, S. 60.
244 Vgl. BSK ISTR – AEPLI, Art. 18 IRSG N 1f.
245 Vgl. BSK ISTR – AEPLI, Art. 18 IRSG N 2; GLESS, Rz. 303; GSTÖHL, S. 146.
246 KOBIK, Jahresbericht 2014, S. 23.
247 Art. 30 Abs. 1 CCC.

chende Vertragspartei weiter, sodass der entsprechende Dienstanbieter und der Übermittlungsweg der Kommunikation festgestellt werden können.[248]

Von der Weitergabe der gesicherten Verkehrsdaten darf nur abgesehen werden, wenn die ersuchte Vertragspartei der Ansicht ist, dass die Erledigung des Ersuchens geeignet ist, ihre Souveränität, Sicherheit, öffentliche Ordnung oder andere wesentliche Interessen zu beeinträchtigen oder wenn der ersuchte Staat die im Ersuchen betreffende Straftat als politische oder mit einer solchen zusammenhängenden Straftat ansieht.[249]

Durch die schnelle Übermittlung gewonnener Informationen wird eine wirksamere Bekämpfung der Computerkriminalität ermöglicht. Eine umgehende Sicherung und Übermittlung der Verkehrsdaten verhindert, dass diese geändert oder gelöscht und wegen ihrer Kurzlebigkeit nutzlos werden.[250]

6.1.4 Umsetzung von Art. 30 CCC in Art. 18b IRSG

Den Voraussetzungen aus Art. 30 CCC wird im Schweizerischen Recht Art. 18b IRSG gerecht. Dieser wurde mit dem Inkrafttreten des CCC zur Umsetzung von Art. 30 und Art. 33 CCC neu in das Gesetz aufgenommen.[251] Art. 18b IRSG statuiert zwei Fälle, in welchen die umgehende Weitergabe von gesicherten Verkehrsdaten gestützt auf ein entsprechendes Ersuchen vor Ablauf des Rechtshilfeverfahrens ermöglicht wird:[252] Abs. 1 lit. a sieht vor, dass eine umgehende Weitergabe von gesicherten Verkehrsdaten nur erfolgen darf, wenn die vorläufigen Massnahmen zeigen, dass sich der Ursprung der Kommunikation, welche Gegenstand des Ersuchens ist, in einem anderen Staat befindet. Abs. 1 lit. b gestattet zudem die umgehende Übermittlung von gesicherten Verkehrsdaten, wenn diese von der Vollzugsbehörde aufgrund der Anordnung einer bewilligten Echtzeitüberwachung nach Art. 269-281 StPO ohnehin erhoben werden. Für die Zulässigkeit der rechtshilfemässigen Übermittlung von Verkehrsdaten wird ein ausdrückliches Ersuchen eines anderen Staates[253] und durch die Verweise in Abs. 1 lit. b auf die

248 Art. 30 Abs. 1 CCC; Vgl. zudem: ETS No. 185, Ziff. 290; HEIMGARTNER, S. 145 m.w.H.
249 Art. 30 Abs. 2 CCC; Vgl. zudem: ETS No. 185, Ziff. 291.
250 Vgl. BBl 2010 4697, S. 4733; FABBRI/FURGER, ZStrR, S. 409.
251 Vgl. BSK ISTR – BÖHI, Art. 18b IRSG N 1.
252 Art. 30 Abs. 1 lit. a und lit. b CCC; Vgl. zudem: BBl 2010 4697, S. 4734f.; BSK ISTR – BÖHI, Art. 18b IRSG N 3 und N 10.
253 Vgl. BstGer, 11.2.2011, RR.2009.234, E. 4.2; BSK ISTR – BÖHI, Art. 18b IRSG N 7.

Bestimmungen von Art. 269-281 StPO zusätzlich auch ein dringender Tatverdacht vorausgesetzt.[254]

Um eine Strafuntersuchung im Ausland nicht zu gefährden, muss die Übermittlung von Verkehrsdaten notwendigerweise ohne die vorherige Einholung einer Zustimmung der betroffenen Person erfolgen. Somit geschieht sowohl die Überwachung als auch die Übermittlung der erhobenen Daten an die ersuchende Behörde ohne Wissen der betroffenen Person und folglich auch ohne die Möglichkeit derselben, sich dagegen zu wehren.[255] Da dies einen schwerwiegenden Eingriff in die Rechte der betroffenen Personen darstellt, sieht das Gesetz an dieser Stelle eine Reihe von Schutzmassnahmen vor:[256] Die Überwachungsmassnahmen müssen einerseits von einem unabhängigen Gericht nach Art. 272 StPO genehmigt werden. Die übermittelten Daten dürfen weiter vor Abschluss des Rechtshilfeverfahrens nur zu Fahndungs- bzw. Ermittlungszwecken und nicht als Beweismittel verwendet werden. Zuletzt unterliegt die Übermittlung der Verkehrsdaten der unverzüglichen Kontrolle durch das BJ. Darüber hinaus findet vermehrt eine doppelte Prüfung des Ersuchens durch die Vollzugsbehörde und das BJ statt. Zudem muss die Behörde, welche für die Genehmigung des Ersuchens zuständig ist, die Erfüllung einer Reihe von Kriterien überprüfen, welche materiell weitgehend mit jenen des Rechtshilfeverfahrens übereinstimmen.[257]

Sobald es die Situation erlaubt, spätestens jedoch vor Abschluss der Strafuntersuchung oder der Einstellung des Verfahrens, muss der Betroffene über die erfolgte Übermittlung der Daten an das Ausland informiert werden. Anschliessend hat die betroffene Person die Möglichkeit, mittels einer Beschwerde gegen die Schlussverfügung an das Bundesstrafgericht zu gelangen. Bei Gutheissung der Beschwerde ist die ausländische Behörde verpflichtet, die Informationen aus ihren Akten zu entfernen und eine entspre-

---

254 Da nach Art. 64 IRSG in einem Rechtshilfeersuchen lediglich die strafbaren Handlungen in tatsächlicher Hinsicht dargelegt werden müssen, die Verdachtsgründe aber weder zu beschreiben noch zu belegen sind, ist das strenge Erfordernis des dringenden Tatverdachtes problematisch. Aus diesem Grund wird in der Lehre der Ansatz vertreten, dass bei der Erhebung von elektronischen Verkehrsdaten im Rahmen der internationalen Rechtshilfe die Anforderungen an den Nachweis des dringenden Tatverdachts nicht zu hoch angesetzt werden dürfen. Vgl. hierzu: BSK ISTR – BÖHI, Art. 18b IRSG N 8; FABBRI/FURGER, ZStrR, S. 399.

255 Vgl. BBl 2010 4697, S. 4735; BSK ISTR – BÖHI, Art. 18b IRSG N 19.

256 Art. 18b IRSG; Vgl. zudem: BBl 2010 4697, S. 4735; BSK ISTR – BÖHI, Art. 18b IRSG N 20ff.; FABBRI/FURGER, ZStrR, S. 406 und S. 409.

257 Vgl. BBl 2010 4697, S. 4735. Zu diesen Kriterien gehört die beidseitige Strafbarkeit (Art. 3 BÜPF), die Verhältnismässigkeit (Subsidiarität der Massnahmen: Art. 3 Abs. 1 lit. a-c BÜPF) sowie die Aussonderung von Dokumenten (Art. 8 BÜPF), vgl. BBl 4697, S. 4735, Fn 199.

chende Bescheinigung den Schweizer Behörden zuzustellen.[258] Mit diesen Massnahmen werden einerseits die Erfordernisse der Strafverfolgung erfüllt, andererseits werden aber auch weiterhin die berechtigten Interessen der betroffenen Person angemessen gewahrt.[259]

Die Arbeitsgruppe der Information Security Society Switzerland (ISSS) bezeichnet die Massnahmen des sog. erweiterten Rechtsschutzes, welche die Rechte der betroffenen Personen wahren sollte, als wenig griffig. Insbesondere bei der Massnahme, nach welcher der ersuchende Staat die erhaltenen Daten bis zum Abschluss eines ordentlichen Rechtshilfeverfahrens nicht als Beweismittel verwenden darf, stellt sich die Frage, wie die Einhaltung durch den ersuchten Staat überprüft, ein allfälliger Missbrauch verhindert und die Streichung der Daten bei der Ablehnung eines Ersuchens durchgesetzt werden kann.[260] In der Praxis wird diesen gerechtfertigten Befürchtungen Rechnung getragen, indem die vorzeitige Übermittlung von gesicherten Verkehrsdaten von der Unterzeichnung einer Garantieerklärung abhängig gemacht wird. Damit soll die Einhaltung der Auflagen so weit als möglich gewährleistet werden.[261] Zudem ist es Aufgabe des BJ für die Einhaltung des Gesetzes zu sorgen. Es hat die Möglichkeit bei einer missbräuchlichen Anwendung oder Missachtung der Bestimmung sowohl bei den Schweizerischen als auch bei den ausländischen Behörden zu intervenieren.[262]

Weder im CCC noch im geltenden Schweizerischen Recht lassen sich Vorbehalte zur Pflicht der umgehenden Weitergabe gesicherter Verkehrsdaten vor Einleitung und ausserhalb eines Rechtshilfeverfahrens finden. Die Arbeitsgruppe der ISSS vertritt in ihrem Bericht zur Vernehmlassung die Ansicht, dass sich Art. 30 CCC, anders als Art. 29 CCC, nicht lediglich auf Verkehrsdaten im Zusammenhang mit Art. 2-11 CCC beziehen würde, sondern auf Verkehrsdaten sämtlicher Delikte der Cyberkriminalität Anwendung fände. Damit würde sich eine wesentliche Ausweitung des Anwendungsbereiches von Art. 30 CCC ergeben.[263] Dieser Ansicht ist zu widersprechen. Indem die vorgängige Übermittlung von Verkehrsdaten nach Art. 30 CCC auf die Erledigung eines Ersuchens nach Art. 29 CCC angewiesen ist, kommen die Vorbehaltsmöglichkeiten von Art. 29 CCC auch bei der Anwendung von Art. 30 CCC zum Tragen. Eine umfassende Pflicht zur Übertragung

258 Vgl. BBl 2010 4697, S. 4735; BSK ISTR – BÖHI, Art. 18b IRSG N 25ff.
259 Vgl. BBl 2010 4697, S. 4736.
260 Vgl. ISSS[1], S. 28; ebenfalls kritischer Ansicht: FABBRI/FURGER, ZStrR, S. 413f.; Allgemein zur Durchsetzung von Rechtshilfebeschränkungen vgl. GSTÖHL, S. 382ff.
261 Vgl. BSK ISTR – BÖHI, Art. 18b IRSG N 22; FABBRI/FURGER, ZStrR, S. 406.
262 Vgl. BBl 4697, S. 4735.
263 Vgl. ISSS[1], S. 28.

von Verkehrsdaten nach Art. 30 CCC ergibt sich somit lediglich bei Ersuchen nach Art. 29 CCC, welche sich auf Art. 2-11 CCC stützen. In den übrigen Fällen bedingt die Erfüllung eines Ersuchens um vorläufige Datensicherung und gestützt darauf die allfällige Übermittlung von Verkehrsdaten das Vorliegen der beidseitigen Strafbarkeit. Ist diese nicht gegeben, wird ein Ersuchen nach Art. 29 CCC abgelehnt, womit es auch zu keiner vorzeitigen Übermittlung von Verkehrsdaten nach Art. 30 CCC kommen kann.

Die rechtshilfeweise Erhebung von Verkehrsdaten und deren Übermittlung an das Ausland sind Aufgaben der zuständigen kantonalen Staatsanwaltschaft bzw. in Fällen der Bundesgerichtbarkeit,[264] der Bundesanwaltschaft. Die zuständige Behörde erlässt eine Eintretensverfügung, holt beim zuständigen Zwangsmassnahmengericht die allenfalls erforderlichen Genehmigungen nach Artikel 272 StPO ein und ordnet die gewünschten Überwachungsmassnahmen an. In der selben Verfügung oder einer separaten Zwischenverfügung entscheidet die Vollzugsbehörde zudem über die vorzeitige, an Bedingungen geknüpfte Übermittlung der aufgrund der Überwachungsanordnung erhobenen Daten. Die Verfügungen der Vollzugsbehörde und der Entscheid des Zwangsmassnahmengerichts, sprich die Anordnung und die Überwachung der Übermittlung, sind dem BJ unverzüglich zu übermitteln. Bei Nichteinhaltung der gesetzlichen Voraussetzung kann dieses Beschwerde einlegen.[265]

6.2 Art. 31-34 CCC: Rechtshilfe in Bezug auf Ermittlungsbefugnisse

6.2.1 Art. 31 CCC: Rechtshilfe beim Zugriff auf gespeicherte Computerdaten

In Art. 31 CCC wird die Rechtshilfe beim Zugriff auf gespeicherte Computerdaten geregelt. Der Artikel hält fest, dass eine Vertragspartei eine andere Vertragspartei um die Anordnung einer Durchsuchung oder ähnlichen Zugriff, einer Beschlagnahme oder ähnliche Sicherstellung und die Weitergabe der Daten ersuchen kann, welche mittels eines Computersystems im Hoheitsgebiet der ersuchten Vertragspartei gespeichert sind. Ebenfalls kann die ersuchende Partei gestützt auf Art. 31 CCC um die Weitergabe von Dateien ersuchen, welche nach Art. 29 CCC gesichert wurden.[266] Die ersuchte Vertragspartei erledigt entsprechende Ersuche unter Anwendung der in Art. 23 genannten völkerrechtlichen Übereinkünften, sonstigen Übereinkünften und Rechtsvorschriften, so-

[264] Art. 23ff. StPO.
[265] Vgl. BBl 2010 4697, S. 4736; BSK ISTR – Böhi, Art. 18b IRSG N 11ff.
[266] Art. 31 Abs. 1 CCC; Vgl. zudem: ETS No. 185, Ziff. 292.

wie unter Einhaltung der einschlägigen Bestimmungen aus Kap. III CCC.[267] Die ersuchte Partei hat ein Rechtshilfeersuchen nach Art. 31 CCC umgehend zu erledigen, wenn entweder Gründe zur Annahme bestehen, dass bei den einschlägigen Daten eine besondere Gefahr des Verlustes oder der Veränderung besteht,[268] oder wenn die in Abs. 2 bezeichneten Übereinkünfte und Rechtsvorschriften eine umgehende Zusammenarbeit vorsehen.[269]

Die Rechtshilfeleistung nach Art. 31 CCC beschränkt sich nicht nur auf Delikte nach Art. 2-11 CCC, sondern kann bei jeglichem Zugriff auf gespeicherte Computerdaten ersucht werden. Die Arbeitsgruppe des ISSS äusserte ihre Bedenken diesbezüglich, dass durch die neue Regelung bestehende Bestimmungen ihrem Sinn enthoben und umgangen werden könnten.[270] Dass Art. 31 CCC keine Möglichkeit vorsieht, einen Vorbehalt anzubringen und auch selbst die Anwendbarkeit nicht auf einzelne Delikte beschränkt, ist entgegen der Befürchtungen der Arbeitsgruppe des ISSS nicht als problematisch zu bewerten.[271] Indem sich die Zusammenarbeit aus Art. 31 CCC nach den in Art. 23 CCC genannten Übereinkommen, weiteren völkerrechtlichen Verträgen und innerstaatlichen Rechtsvorschriften richtet, findet automatisch eine Beschränkung der Rechtshilfemöglichkeiten entlang der geltenden Bestimmungen und Grundsätze statt.

6.2.2 Art. 32 CCC: Grenzüberschreitender Zugriff auf gespeicherte Computerdaten mit Zustimmung oder wenn diese öffentlich zugänglich sind

Mit Art. 32 CCC wurde ein neues Instrument der internationalen Strafverfolgung etabliert, welches den ermittelnden Behörden die Befugnis zur grenzüberschreitenden Strafverfolgung einräumt, ohne den förmlichen Rechtshilfeweg über die Art. 29-31 CCC beschreiten zu müssen.[272] Damit wird ein nicht abgesprochenes Vorgehen eines Staates ermöglicht, ohne die Souveränität eines anderen Staates zu beeinträchtigen.[273] Art. 32 CCC erlaubt einer Vertragspartei den Zugriff auf Computerdaten im Ausland unabhängig von einer Genehmigung einer anderen Vertragspartei, wenn es sich bei diesen Daten

267 Art. 31 Abs. 2 CCC; ETS No. 185, Ziff. 292.
268 Art. 31 Abs. 3 lit. a CCC.
269 Art. 31 Abs. 3 lit. b CCC.
270 Als Beispiel wird der Steuer- und Wirtschaftsbereich genannt, in welchem Daten vermehrt in elektronisch lesbarer Form abgelegt und auch von den Untersuchungsbehörden in dieser Form erhoben werden, vgl. ISSS[1], S. 28f.
271 Vgl. BBl 4697, S. 4737.
272 Vgl. BGer 1B_344/2014 E 4.3.11.
273 Vgl. BBl 2010 4697, S. 4737.

entweder um öffentlich zugängliche gespeicherte Daten handelt[274] oder um Daten, zu welchen die freiwillige Zustimmung der zur Weiterleitung rechtmässig befugten Person vorliegt.[275]

Aus dem erläuternden Bericht zu Art. 32 CCC lässt sich entnehmen, dass diese Bestimmung zu vielen Diskussionen unter den Autoren führte. Relativ schnell wurde klar, dass zur Zeit des Verfassens der Konvention noch nicht der richtige Zeitpunkt für den Erlass einer umfassenden, rechtsverbindlichen Regelung war. Dies lässt sich einerseits auf die fehlende Erfahrung im Umgang mit solchen Ermittlungsmöglichkeiten zurückführen. Andererseits war man sich damals aber schon bewusst, dass die besten Lösungen erst anhand spezifischer Gegebenheiten innerhalb eines konkreten Falles entwickelt werden können. Zugunsten des Abkommens einigten sich die Autoren auf einen minimalen Konsens und entschieden gleichzeitig, keine weiteren Anwendungsfälle vorzusehen, bis entsprechende Erfahrungswerte gesammelt werden können.[276] Andere unilaterale Zugriffsmöglichkeiten – wie jene aus Art. 32 CCC – werden durch das Abkommen nicht autorisiert. Eine anderweitige Datenerhebung oder rückwirkende Überwachung muss somit über den ordentlichen Rechtshilfeweg beantragt werden.[277]

Der grenzüberschreitende Zugriff auf öffentlich gespeicherte und zugängliche Daten ist unabhängig von ihrem geographischen Speicherort erlaubt.[278] Art. 32 lit. a CCC verhindert somit, dass eine Vertragspartei vorab die Zustimmung für das Abrufen und Verwenden von ohnehin öffentlich zugänglichen Daten von jenem Staat einholen muss, in welchem die Daten gespeichert sind.[279]

Der grenzüberschreitende Zugriff auf nicht öffentlich zugängliche Daten durch ein Computersystem im Inland ist gemäss Art. 32 lit. b CCC nur möglich, wenn eine freiwillige[280] und rechtmässige Zustimmung einer Person vorliegt. Diese muss befugt sein, entsprechende Daten an die ermittelnde Behörde weiterzugeben. Im erläuternden Bericht zum CCC wird an dieser Stelle als Beispiel für eine rechtmässig zustimmungsberechtigte Person eine Person aufgeführt, deren E-Mails von einem Internetservice-Provider im

274 Art. 32 lit. a CCC.
275 Art. 32 lit. b CCC.
276 Vgl. ETS No. 185, Ziff. 293.
277 Vgl. BGer 1B_344/2014 E 5.12; BBl 2010 4697, S. 4737, Fn 208.
278 Art. 32 lit. a CCC.
279 Vgl. BBl 2010 4697, S. 4737f.
280 Die Zustimmung zur grenzüberschreitenden Datenbeschaffung muss ausdrücklich freiwillig erfolgen. Dabei genügt auch eine konkludente Zustimmung, wenn die zustimmungsberechtigte Person bspw. gefolgt auf eine Anfrage die entsprechenden Daten herausgibt, vgl. BGer 1B_344/2014 E 5.10.

Ausland gespeichert werden, oder eine Person, welche ihre Daten bewusst im Ausland speichert.[281] Liegt die Zustimmung einer solchen Person vor, kann die Vertragspartei, ohne den ordentlichen Weg der Rechthilfe einschlagen zu müssen, auf im Hoheitsgebiet einer anderen Vertragspartei gespeicherte Computerdaten zugreifen, oder diese empfangen.[282] Wer im konkreten Fall eine zustimmungsberechtigte Person sein kann, wird im erläuternden Bericht zum CCC offen gelassen. Dies ergebe sich aus den tatsächlichen Umständen, der Person selbst und dem anwendbaren nationalen Recht des Staates, in welchem die betreffende Person handelt.[283]

Der Botschaft zum CCC kann in Bezug auf die zustimmungsberechtigte Person eine weitere Voraussetzung entnommen werden. Demnach bedarf es für den befugten Zugriff nicht der Zustimmung einer beliebigen Person, sondern einer Person im Inland, welche rechtmässig zur Weiterleitung der Daten an eine inländische Strafverfolgungsbehörde befugt ist.[284] Eine solch enge Auslegung der Bestimmung sei notwendig, um der Gefahr eines Missbrauchs durch die Umgehung der Rechtshilfe oder der damit verbundenen Verletzung der Privatsphäre Dritter entgegenzuwirken.[285]

Im Leitentscheid vom 14. Januar 2015 widerspricht das Bundesgericht dieser Auffassung.[286] Es führt aus, dass eine solche Voraussetzung dem Sinn und Zweck des internationalen Abkommens widersprechen und die Hauptanliegen des CCC unterlaufen würde. Zudem liesse weder der Wortlaut noch die einschlägigen Materialien des Übereinkommens eine entsprechende Interpretation zu. Die Zustimmungsvoraussetzungen würden den Anwendungsbereich der Bestimmung genügend einschränken, so dass es einer weiteren Voraussetzung, wie dem Erfordernis der Zustimmung einer inländischen Person, nicht bedarf. Das Bundesgericht ist der Ansicht, dass es mit dieser Voraussetzung kaum noch möglich wäre, über Art. 32 lit. b CCC auf ausländische E-Mail-Konten oder Accounts von sozialen Netzwerken zuzugreifen, da nur in äusserst seltenen Fällen bei im Ausland gespeicherten Daten eine zustimmungsberechtigte Person im Inland gefunden werden könnte, die darüber hinaus auch noch freiwillig ihre Zustimmung zur Datener-

281 Vgl. ETS No. 185, Ziff. 294.
282 Vgl. BGer 1B_344/2014 E 4.3.11.
283 Vgl. ETS No. 185, N 294; Zur Frage des anwendbaren Rechts vgl. BGer 1B_344/2014 E 5.10; BBl 2010 4697, S. 4738.
284 Vgl. BBl 2010 4697, S. 4738; Eine ähnliche Auslegung lässt sich auch in einem von der deutschen Bundesregierung erlassenen Entwurf eines Gesetzes zum Übereinkommen des Europarates vom 23. November 2001 über Computerkriminalität finden, Deutscher Bundestag, Ds. 16/7218, S. 55.
285 Vgl. BBl 2010 4697, S. 4738.
286 Vgl. BGer 1B_344/2014; Vgl. zudem: FORSTER, S. 619.

hebung erteilen würde.[287] Unter Berücksichtigung der Argumente des Bundesgerichts, welche die Notwendigkeit klar verdeutlichen, dass für die Anwendung von Art. 32 lit. b CCC nicht lediglich auf die Zustimmung von inländischen Personen gezählt werden darf, erscheint die durch die Botschaft zusätzlich vorgesehene Voraussetzung und die damit einhergehende Einschränkung der Anwendbarkeit von Art. 32 lit. b CCC nicht nachvollziehbar. Die im Leitentscheid des Bundesgerichts vertretene Auffassung ist zu begrüssen.

Von einem grenzüberschreitenden Zugriff nach Art. 32 lit. b CCC sind jegliche Daten ausgenommen, bei welchen es sich um vertrauliches Datenmaterial einer Drittperson handelt, welche ebenfalls einer Offenlegung zustimmen müsste und dies nicht getan hat, da es in diesem Fall an einer Befugnis i.S.v. Art. 32 lit. b CCC fehlt.[288]

6.2.3 Art. 33 CCC: Rechtshilfe bei der Erhebung von Verkehrsdaten in Echtzeit

Die Rechtshilfe bei der Erhebung von Verkehrsdaten in Echtzeit richtet sich nach Art. 33 CCC. Die Vertragsstaaten verpflichten sich in diesem Artikel zur gegenseitigen Rechtshilfeleistung. Die Rechtshilfe unterliegt dabei den im innerstaatlichen Recht vorgesehenen Bedingungen und Verfahren.[289] Gemäss Abs. 2 sind die Vertragsstaaten verpflichtet, zumindest in jenen Fällen gegenseitig Rechtshilfe zu leisten, in denen die Erhebung von Verkehrsdaten in Echtzeit in einem inländischen Verfahren möglich wäre.[290] Eine Einschränkung für die Anwendung von Überwachungsmassnahmen hinsichtlich der Schwere der Straftat ist in Art. 33 CCC nicht vorgesehen.[291]

Eine Erhebung von Verkehrsdaten in Echtzeit ist notwendig, da die Ermittler häufig nicht gewährleisten können, dass eine Kommunikation, gestützt auf die Aufzeichnungen früherer Übermittlungen, bis zu ihrem Ursprung zurückverfolgt werden kann. Die Ursache liegt darin, dass Dienstanbieter wesentliche Verkehrsdaten in der Übertragungskette möglicherweise automatisch löschen, bevor diese gesichert werden können.[292]

---

287 Vgl. BGer 1B_344/2014 E 5.9.
288 Vgl. BBl 2010 4697, S. 4738.
289 Art. 33 Abs. 1 CCC; Neben den nationalen Bestimmungen und Verfahren hat sich die Rechtshilfe auch an den Verträgen und Rechtsvorschriften über die Rechtshilfe in Strafsachen zu orientieren, vgl. BBl 2010 4697, S. 4738; ETS No. 185, Ziff. 295.
290 Art. 33 Abs. 2 CCC.
291 Vgl. BBl 2010 4697, S. 4739.
292 Vgl. BBl 2010 4697, S. 4738; ETS No. 185, Ziff. 295.

6.2.4 Umsetzung der Echtzeitüberwachung von Verkehrsdaten in Art. 18b IRSG

Die Echtzeitüberwachung von Verkehrsdaten über das Rechtshilfeverfahren wird in der Schweiz in Art. 18b IRSG geregelt. Wie bereits in Kap. 6.1.4 erwähnt, ermöglicht dieser eine unverzügliche Übermittlung von Daten an das Ausland, ohne vorgängigen Erlass einer Verfügung an die in der Schweiz wohnhafte betroffene Person.[293] Es liegt in der Natur der Sache, dass überwachte Personen über Massnahmen zur Echtzeitüberwachung nicht informiert werden sollten. Dieses Erfordernis lässt sich jedoch nur schwerlich mit den Grundsätzen des IRSG vereinbaren. Diese verlangen, dass keine Informationen aus dem Geheimbereich einer Person ohne deren Kenntnis und Möglichkeit, sich dagegen zu wehren, an das Ausland übermittelt werden dürfen.[294] Die Arbeitsgruppe des ISSS weist an dieser Stelle zurecht darauf hin, dass bei der Umsetzung des CCC dem Umstand Rechnung getragen werden muss, dass die Garantien und Grundrechte der Bürger aus der Schweizerischen Gesetzgebung gewahrt werden müssen.[295] Aus diesem Grund wird für die Anordnung einer Echtzeitüberwachung elektronischer Verkehrsdaten die vorgängige Genehmigung eines Zwangsmassnahmengerichts zwingend vorausgesetzt.[296]

Im Schweizerischen Recht ist die Echtzeitüberwachung von Verkehrsdaten gemäss Art. 273 StPO bei einem Verbrechen, Vergehen oder einer Übertretung nach Art. 179septies StGB, unter Beachtung der Voraussetzungen von Art. 269 Abs. 1 lit. b und c StPO gestattet.[297] Auch wenn Art. 33 CCC selbst keine Einschränkung für die Echtzeitüberwachung hinsichtlich der Schwere der Tat kennt, kann die Schweiz, gestützt auf den Grundsatz der Verhältnismässigkeit, ein Ersuchen um Rechtshilfe bei der Erhebung von Verkehrsdaten in Echtzeit ablehnen, wenn der Tatbestand im Schweizerischen Recht als Übertretung eingestuft wird. [298]

6.2.5 Art. 34 CCC: Rechtshilfe bei der Erhebung von Inhaltsdaten in Echtzeit

Art. 34 CCC regelt die Frage der Rechtshilfe bei der Erhebung von Inhaltsdaten in Echtzeit. Da das Abfangen von Inhaltsdaten stark in die Privatsphäre der betroffenen Person eingreift, wird die Verpflichtung zur Rechtshilfeleistung bei einer Echtzeiterhebung von

---

293 Art. 80m IRSG; Vgl. zudem: BBl 2010 4697, S. 4738f.
294 Vgl. BBl 2010 4697, S. 4736; FABBRI/FURGER, ZStrR, S. 395.
295 Vgl. ISSS[1], S. 29.
296 Vgl. BSK ISTR – BÖHI Art. 18b IRSG N 9; siehe auch Art. 273 Abs. 2 StPO.
297 Art. 273 StPO; Vgl. zudem: BBl 2010 4697, S. 4739; FORSTER, S. 620.
298 Einzige Ausnahme bildet die in Art. 273 StPO ausdrücklich festgehaltenen Übertretung nach Art. 179septies StGB, vgl. BBl 2010 4697, S. 4739.

Inhaltsdaten eingeschränkt.[299] Die Vertragsstaaten sind nur insoweit zur Leistung von Rechtshilfe verpflichtet, als dies in den jeweils anwendbaren Verträgen und dem innerstaatlichen Recht vorgesehen ist.[300]

6.2.6 Umsetzung der Echtzeiterhebung von Inhaltsdaten in der Schweiz

Die Schweiz leistet in Bezug auf die Übermittlung von Inhaltsdaten in Echtzeit vor Abschluss eines ordentlichen Rechtshilfeverfahrens keine Rechtshilfe. Die mit Inkrafttreten der Konvention einhergehende Revision des IRSG beschränkte sich darauf, den Anforderungen an das nationale Recht aus Art. 33 CCC zu genügen. Art. 18b IRSG berücksichtigt lediglich die Erhebung von Verkehrsdaten in Echtzeit, nicht aber jene von Inhaltsdaten. Der Schweiz fehlt somit eine umfassende gesetzliche Regelung zur Durchführung von Überwachungsmassnahmen im Rahmen der Rechtshilfe, welche sowohl die Erhebung von Verkehrs-, als auch jene von Inhaltsdaten beinhaltet.[301]

In der Lehre wird teilweise die Meinung vertreten, das Einholen einer Garantieerklärung vor der Übermittlung von Inhaltsdaten in Echtzeit genüge, um die Interessen der betroffenen Person und die Rechtsstaatlichkeit zu wahren.[302] Dieser Ansicht widerspricht BÖHI zurecht.[303] Denn würde man dieser Argumentation folgen, wäre Art. 18b IRSG obsolet. Art. 18b IRSG lässt nur unter Einhaltung einschränkender Voraussetzungen die Übermittlung von Verkehrsdaten zu. Aus diesem Grund darf eine Übermittlung von Inhaltsdaten nur bei Vorliegen einer genügenden gesetzlichen Grundlage erfolgen. Fehlt eine solche, würde mit der Übermittlung von Inhaltsdaten vor Abschluss eines Rechtshilfeverfahrens das Gebot von Art. 36 BV verletzt.[304] Dieses besagt, dass Einschränkungen von Grundrechten neben weiteren Voraussetzungen immer auch einer genügenden gesetzlichen Grundlage bedürfen.[305]

---

299 Vgl. ETS No. 185, Ziff. 297.
300 Art. 34 CCC.
301 Vgl. BBl 2010 4697, S. 4736.
302 Vgl. FABBRI/FURGER, ZStrR, S. 410, 416.
303 Vgl. BSK ISRT – BÖHI, Art. 18b IRSG N6.
304 Vgl. BSK ISRT – BÖHI, Art. 18b IRSG N6; A.M. FABBRI/FURGER, ZStrR, S. 409f.
305 Art. 36 BV.

7 Mehrwert des CCC für die Schweiz

Im folgenden Kapitel wird nach einer Analyse der tatsächlichen Anwendung des CCC in der Schweiz untersucht, inwiefern das CCC seiner eigenen Zielsetzung gerecht wird. Insbesondere wird auf die Ziele der Harmonisierung und der Verbesserung der internationalen Zusammenarbeit eingegangen. Gleichzeitig wird eine Auseinandersetzung mit der am häufigsten geäusserten Kritik zum Abkommen vorgenommen.

7.1 Wie oft kommen die Bestimmungen des CCC zur Anwendung?

KOBIK ist seit Eingliederung in die Bundeskriminalpolizei im Jahr 2009 für die Koordination des internationalen kriminalpolizeilichen Informationsaustausches im Bereich der Internetkriminalität zuständig. Neben der Unterstützung der Kantone in ihrer Strafverfolgung bildet KOBIK zudem die Schnittstelle zwischen den Kantonen und den internationalen Organisationen wie INTERPOL und Europol in Sachen Cybercrime. [306]

Seit Inkrafttreten der Cybercrime-Konvention kann jährlich eine Zunahme der Meldeeingänge und -ausgänge über KOBIK festgestellt werden.[307] Während im letzten Quartal 2011 vor Inkrafttreten der Konvention noch lediglich 49 Meldungen vom Ausland kamen und 27 an das Ausland gingen, wurden im letzten Quartal 2012 (nach Inkrafttreten der Konvention) bereits 128 Meldungen aus dem Ausland (Zunahme von 161% gegenüber dem Quartal aus dem Vorjahr) und 254 Meldungen an das Ausland vermerkt (Zunahme um mehr als das 9-fache).[308] Gesamthaft liefen im Jahr 2012 483 Meldungen aus dem Ausland und 561 Meldungen an das Ausland über KOBIK.[309]

Bereits im Folgejahr wurde wiederum eine markante Zunahme der Meldungen verzeichnet. So gingen im Jahr 2013 bei KOBIK 739 Meldungen zum Anwendungsbereich des CCC aus dem Ausland ein. Dies entspricht einem Anstieg von über 53% gegenüber dem Vorjahr. An das Ausland[310] liefen über KOBIK insgesamt 946 Meldungen. Dies entspricht einem Anstieg von über 68% gegenüber den Meldungen des Vorjahres.[311] Zum ersten Mal wurde im Jahr 2013 die Meldungen nach Art. 29ff. CCC in einer separaten Statistik festgehalten, gemäss welchen die Untersuchungsbehörden auf dem polizeilichen Weg unter in Aussichtstellung eines Rechtshilfeersuchens die umgehende Datensi-

306 Vgl. KOBIK, Jahresbericht 2014, S. 23.
307 Siehe auch: Anhang 9.2.
308 Vgl. KOBIK, Jahresbericht 2012, S. 20.
309 Vgl. KOBIK, Jahresbericht 2012, S. 20.
310 Interpol und Europol.
311 Vgl. KOBIK, Jahresbericht 2013, S. 24.

cherung veranlassen können. In diesem Zusammenhang hat KOBIK aus dem Inland acht und aus dem Ausland vier Ersuche weitergeleitet.[312]

Im Jahr 2014 nahmen die Meldungen im Bereich des Übereinkommens nochmals zu. So sind über die verschiedenen Kanäle insgesamt 1314 Meldungen aus dem Ausland eingegangen, was einem Anstieg von 77,8% gegenüber dem Vorjahr entspricht. 1285 Meldungen leitete KOBIK im Jahr 2014 an das Ausland weiter, was einem Anstieg von 35,8% im Vergleich zum Vorjahr entspricht.[313] Auch im Jahr 2014 wurden die Anfragen zu Art. 29ff. CCC bezüglich der Sicherstellung von Daten über den polizeilichen Weg unter in Aussichtstellung eines Rechtshilfeersuchens in einer separaten Statistik aufgeführt. So gingen im Jahr 2014 bei KOBIK 15 Ersuche aus den Kantonen an ausländische Behörden und 11 Ersuche aus dem Ausland ein.[314]

Der Umstand, dass weder das Bundesamt für Statistik noch das BJ statistische Erhebungen zur Anwendbarkeit der CCC vornehmen, verdeutlicht, wie wichtig die Zusammenarbeit der Strafverfolgungsbehörden über den direkten Weg ist. Der offizielle Weg über die Justizministerien ist zumindest in der Schweiz nur von geringer Relevanz. Während ein Mitarbeiter des BJ aus eigenen Erfahrungen lediglich von schätzungsweise ein bis zwei Fällen aus dem Anwendungsbereich von Art. 18b IRSG zu berichten wusste, ist beim zuständigen Mitarbeiter der Schweizerischen Botschaft in Rom, bis heute kein Ersuchen um Rechtshilfe eingegangen. Beide verweisen bezüglich der Anwendbarkeit der CCC auf die Meldestelle KOBIK, was die im oberen Teil bereits aufgezeigte Relevanz der polizeilichen Zusammenarbeit und damit des direkten Verkehrs in diesem Bereich verdeutlicht. Gemäss Aussage des Mitarbeiters des BJ geht es rechtshilfeweise überwiegend nur noch um die Herausgabe der vorsorglich sichergestellten Daten nach Art. 29ff. CCC.

7.2 Wird das CCC den internationalen Anforderungen und seiner eigenen Zielsetzung gerecht?

Das wichtigste Ziel des CCC ist die erfolgreiche Bekämpfung der Cyberkriminalität mittels einer schnellen, wirksamen und umfassenden Zusammenarbeit auf internationaler Ebene. Die Umsetzung dieses Ziels wird nicht nur durch entsprechende Instrumente der

312 Vgl. KOBIK, Jahresbericht 2013, S. 25.
313 Vgl. KOBIK, Jahresbericht 2014, S. 23.
314 Vgl. KOBIK, Jahresbericht 2014, S. 23.

internationalen Kooperation erreicht, sie ist auch stark von der Grundlage eines jeden Rechtshilfeverfahrens abhängig, das dem Ersuchen zugrunde liegende Delikt. Fehlt es an der beidseitigen Strafbarkeit, erfolgt i.d.R. auch keine Rechtshilfeleistung. Die gegenseitige Beeinflussung von Straftat und Rechtshilfeleistung wird im Folgenden genauer untersucht, um aufzuzeigen, inwiefern sich diese effektiv auf die internationale Zusammenarbeit auswirkt und ob dazu geäusserte Kritiken tatsächlich angebracht sind.

7.2.1 Wie wirken sich die Vorbehaltsmöglichkeiten auf die Harmonisierung aus?

Mit der Vorgabe einzelner Straftatbestände in Art. 2-11 CCC werden die Vertragsstaaten zur Anpassung ihrer nationalen Bestimmungen an die Herausforderungen neuer Informationstechnologien verpflichtet. Mit der Harmonisierung der unterschiedlichen nationalen Rechtsordnungen wird eine wichtige Grundlage für die Rechtshilfe und die internationale Zusammenarbeit geschaffen. Die Möglichkeit, an etlichen Stellen des Straftatenkatalogs des CCC Vorbehalte und Erklärungen anzubringen, verhindert die vollständige gegenseitige Anpassung. So können die Vertragsparteien nicht nur die Anwendbarkeit gewisser Abschnitte einzelner Artikel ausschliessen, sie können auch weitere Voraussetzungen an das Erfüllen des Straftatbestandes knüpfen. Beides wirkt einer umfassenden Harmonisierung unter den nationalen Rechtsordnungen entgegen. Die individuelle Abänderbarkeit gewisser Teile des Tatbestandkatalogs birgt die Gefahr, dass ein ersuchter Staat aufgrund der fehlenden beidseitigen Strafbarkeit ein Rechtshilfeersuchen ablehnen kann, sich aber dennoch vertragskonform verhält.

Dies wirft berechtigterweise die Frage auf, ob mit diesen Vorbehaltsmöglichkeiten das Ziel der Harmonisierung des materiellen Strafrechts gar unterlaufen wird. Einige Autoren[315] sind der Meinung, die Konvention lasse den nationalen Gesetzgebern zu viel Spielraum in Bezug auf die Umsetzung der Vorgaben. Andere[316] vertreten die Ansicht, die Vorbehalte dienen jenen Staaten als Schlupflöcher, deren Recht nicht im Einklang mit dem Recht der anderen Staaten steht. So würden die Vorbehaltsmöglichkeiten den jeweiligen Parteien gestatten, ihr existierendes Recht zu bewahren und damit die Harmonisierung zu untergraben. WEBER ist gar der Meinung, dass eine gemeinsame Basis einer Cybercrime-Strafgesetzgebung erst erreicht werden kann, wenn alle Parteien dem

315 Vgl. BALTISSER, S. 149; HILGENDORF, S. 270.
316 Vgl. VATIS, S. 220; WEBER, S. 443f.

Abkommen ohne Vorbehalte beigetreten sind.[317] Dieser Ansicht kann, wie sogleich dargelegt wird, nicht gefolgt werden.

Das Leisten von Rechtshilfe tangiert immer das Territorium des ersuchten Staates. Aus diesem Grund ist es wichtig, dass dieser Rechtshilfeersuchen ablehnen kann, wenn die Voraussetzungen des nationalen Rechts zur Gewährung von Rechtshilfe nicht erfüllt sind. Es darf nicht Ziel eines Abkommens sein, die Souveränität eines Staates zugunsten der Strafverfolgung in einem anderen Staat in schwerwiegender Weise zu beschneiden. Dies hätte nicht nur negative Auswirkungen auf den Abschluss eines Abkommens, sondern auch auf potentielle Neubeitritte. Ein Abkommen, welches keinerlei Vorbehalte zulässt, würde einem „Welt-Recht" gleichkommen, dessen Annahme und Akzeptanz gerade auf diesem Gebiet fraglich erscheint. Indem Mitgliedstaaten sich gewisse Rechte bei der Umsetzung des Straftatenkatalogs vorbehalten können, wird die Wahrscheinlichkeit neuer Beitritte gefördert, was wiederum zur Verbesserung der internationalen Zusammenarbeit beiträgt. Die Einschränkung der Harmonisierung durch die Vorbehalte zugunsten der Souveränität der Mitgliedstaaten ist deshalb für die Umsetzbarkeit des Abkommens in Kauf zu nehmen.

7.2.2 Ist der Tatbestandskatalog des CCC unvollständig?

Immer wieder äussern Autoren[318] die Kritik, der Tatbestandskatalog des Abkommens umfasse nicht alle delinquenten Handlungen bzgl. Cyberkriminalität. Um die Frage zu beantworten, inwiefern das CCC alles deliktische Verhalten im Zusammenhang mit einem Computernetzwerk oder dem Internet abdeckt und ob die vorgebrachte Kritik angebracht ist, wird auf die eingangs vorgenommene Unterscheidung zwischen Computerkriminalität und Internetkriminalität i.e.S. zurückgegriffen.[319] Grundsätzlich wird demnach unterschieden, ob ein Computersystem oder ein Netzwerk explizit Angriffsziel und Tatobjekt ist, oder ob die Tathandlung in einer klassischen Straftat besteht, welche auch über das Internet begangen werden kann. Legt man diese Begriffsdefinitionen dem Tatbestandskatalog des CCC zugrunde, wird deutlich, dass in diesem vor allem die Kriminalisierung von Handlungen aus dem Bereich der Computerkriminalität verlangt wird. Dies zeigt sich auch bei der Gegenüberstellung des Straftatbestandskatalogs mit dem Schweizerischen Computerstrafrecht, lassen sich doch mit Ausnahme des „Zeit-

317 Vgl. WEBER, S. 444.
318 Vgl. HERZOG, S. 5f.; ISSS[1], S. 5; WEBER, S. 444.
319 Vgl. Kapitel 2.1.

diebstahls“[320] alle Tatbestände des Computerstrafrechts im CCC wiederfinden. Aus dem Bereich der Internetkriminalität i.e.S. verlangt das CCC einzig die Kriminalisierung von Kinderpornographie (Art. 9 CCC) und der Schutz vor Urheberrechtsverletzungen und Verletzungen verwandter Schutzrechte (Art. 10 CCC). Weitere Delikte der Internetkriminalität i.e.S. werden im Straftatbestandskatalog des CCC nicht aufgeführt. Dies weist grundsätzlich auf die Unvollständigkeit des Tatbestandskatalogs des CCC hin, womit die Kritik als angebracht erscheint.

Auch im erläuternden Bericht zum CCC lassen sich an einigen Stellen Hinweise auf die Unvollständigkeit des Tatbestandskatalogs finden. Gerade in Bezug auf Urheberrechtsverletzungen und Verletzungen verwandter Schutzrechte wird ausdrücklich darauf hingewiesen, dass bspw. markt- und patentbezogene Verletzungen nicht unter den Schutz des CCC fallen.[321] Vom Schutzbereich der Konvention umfasst werden nur die in Art. 10 Abs. 1 und Abs. 2 CCC ausdrücklich genannten Abkommen. Andere Verträge sind vom Anwendungsbereich der Konvention ausgeschlossen. Zudem erwachsen für die Vertragsparteien nur aus jenen Verträgen Verpflichtungen, welche sie unterzeichnet haben. Allfällige Vorbehalte bei den einzelnen Verträgen schränken die Anwendbarkeit weiter ein. Mit anderen Worten besteht die Gefahr, dass Massnahmen aus dem CCC wie z.B. Art. 29ff. CCC im Bereich der Urheberrechtsverletzung nur zur Anwendung gelangen, sofern die jeweiligen Vertragsparteien sowohl Mitglied des CCC als auch der entsprechenden Verträge aus Art. 10 Abs. 1 und Abs. 2 CCC sind.

Es ist somit theoretisch denkbar, dass eine Vertragspartei der Konvention im Bereich der Urheberrechtsverletzung keine Rechtshilfe leisten muss, wenn sie die entsprechenden Verträge aus Art. 10 Abs. 1 und Abs. 2 CCC nicht ratifiziert hat. Weshalb sich die Autoren der Konvention mit Art. 10 CCC lediglich auf die bis dahin existierenden Verträge beschränkten und keinen weiter gefassten Schutzbereich formulierten, welcher auch zukünftige Verträge und Entwicklungen berücksichtigt hätte, ist aus heutiger Sicht nicht nachvollziehbar. Damit wurden dem Schutzbereich unnötigerweise Grenzen gesetzt, welche nachträglich nur mit entsprechenden Anpassungen der Konvention an neue Erscheinungsformen der Urheberrechtsverletzung überwunden werden könnten. Die damit einhergehende Einschränkung der Wirkung des CCC steht klar im Widerspruch

---

320 Art. 150 Abs. 4 StGB erklärt die unbefugte Beanspruchung fremder Computeranlagen, deren Dienstleistung einem grösseren Publikum nur gegen Entgelt angeboten wird, für strafbar, vgl. BSK StGB – FREYTAG, Art. 150 StGB; BSK StGB – WEISSENBERGER, Art. 150 StGB N 3; SCHMID, ZStrR, S. 37f.

321 Vgl. ETS No. 185, Ziff. 109; Siehe auch Kapitel 5.4.1.

zum Ziel, eine effiziente internationale Zusammenarbeit zur Bekämpfung von Cyberkriminalität zu etablieren, da sich die Anwendbarkeit von Art. 10 CCC auf den Stand von 2001 beschränkt. Für die Durchsetzung neuer internationaler Verträge im Bereich der Urheberrechtsverletzung bedarf es einer möglichst umfassenden Teilnahme, um allenfalls auf die besonderen Instrumente der internationalen Zusammenarbeit des CCC zurückgreifen zu können.

Weitere Bereiche, welche vom Tatbestandskatalog des Übereinkommens nicht erfasst werden, lassen sich bspw. bei HERZOG finden. So bemängelt er, dass weder der Missbrauch von elektronischen Handelsplattformen im Internet noch das sog. „Phishing" vom Anwendungsbereich des CCC erfasst werden würde.[322] Neben diesen Taten sind unzählige weitere Delikte im Internet denkbar, welche unter den Begriff der Internetkriminalität i.e.S. subsumiert werden können. Diesen Delikten ist gemeinsam, dass sie als „klassische" Straftaten auch im Internet begangen werden können. Da sie i.d.R. über die bereits bestehenden internationalen Verträge und die nationalen Rechtsordnungen als Straftaten kriminalisiert werden, hat ihre Absenz im Tatbestandskatalog des CCC kaum Auswirkung auf die Anwendbarkeit der Instrumente zur internationalen Strafverfolgung.

Die Anwendbarkeit der eigentlichen Rechtshilfeinstrumente des CCC (Art. 31, Art. 33 und Art. 34 CCC) beschränkt sich nicht auf die Delikte des Tatbestandskataloges. Sind die Voraussetzungen für die Rechtshilfeleistung erfüllt, wird einem entsprechenden Ersuchen aus dem Bereich der Cyberkriminalität grundsätzlich entsprochen, unabhängig davon, ob es sich um Computerkriminalität oder Internetkriminalität i.e.S. handelt. Auch die Anwendbarkeit der Massnahmen nach Art. 32 CCC ist unabhängig von einer allfälligen Auflistung des Deliktes im Tatbestandskatalog des CCC gegeben.

Einzig die Massnahmen nach Art. 29 und Art. 30 CCC nehmen direkten Bezug auf die Art. 2-11 CCC. So kann sich ein Staat das Recht vorbehalten, von einer vorsorglichen Massnahme abzusehen, wenn sich das entsprechende Ersuchen auf andere Straftaten als jene in Art. 2-11 CCC bezieht und Grund zur Annahme besteht, dass einem späteren Rechtshilfeersuchen aufgrund der fehlenden beidseitigen Strafbarkeit nicht entsprochen werden kann. Wie bereits umfassend ausgeführt,[323] erübrigt sich in diesem Fall eine vorsorgliche Datensicherung. Die Datensicherung ist wie die eigentliche Herausgabe der

[322] Vgl. HERZOG, S. 5f.
[323] Vgl. Kapitel 6.1.1f.

gesicherten Daten über ein ordentliches Rechtshilfeersuchen zu beantragen. Die Problematik liegt dabei im Charakter der Daten, um deren Sicherung vorsorglich ersucht wird, da diese in den meisten Fällen äusserst kurzlebig sind. Dies hat zur Folge, dass bis zur Erledigung eines ordentlichen Rechtshilfeverfahrens essentielle Daten unbrauchbar werden oder sogar verloren gehen können. Wie erwähnt, kommt das CCC ergänzend zu den bereits bestehenden internationalen Rechtshilfeabkommen und dem nationalen Recht zur Anwendung, welche die Kriminalisierung der meisten „klassischen" Delikte verlangen. Die Wahrscheinlichkeit, dass einem Ersuchen nach Art. 29 CCC nicht entsprochen wird, ist somit relativ gering. Damit erübrigt sich eine Erweiterung des Tatbestandskataloges um die Delikte der Internetkriminalität i.e.S., auch in Bezug auf das sog. „Phishing" und den Missbrauch von elektronischen Handelsplattformen.[324]

Die Ausweitung des Tatbestandkataloges erübrigt sich nicht nur allein wegen der fehlenden Notwendigkeit, sondern auch aufgrund der mangelnden Durchsetzbarkeit. Die Kritik, dass das schwerfällige Änderungsverfahren von internationalen Verträgen eine dauerhafte Fixierung des Rechts riskiert, kann bei jedem internationalen Abkommen aufgeführt werden und trifft auch auf das Vorliegende zu. Zudem ist es unmöglich, jegliches deliktische Verhalten zu erfassen. Bereits heute ist eine Fülle an strafbaren Handlungen denkbar, welche über das Internet begangen werden können. Es liegt in der Natur von Cyberkriminalität, stets laufenden Veränderungen unterworfen zu sein, weshalb sich in regelmässigen Abständen eine erneute Anpassung des Abkommens aufdrängen würde. Dies ist weder erstrebenswert noch praktikabel.

Eine denkbare Lösung in Bezug auf zukünftig auftauchende Kriminalitätsphänomene könnte im Erlass von Zusatzprotokollen[325] und Rahmenbeschlüssen[326] bestehen. Mit diesen könnten allenfalls auftretende Lücken des CCC geschlossen oder sich noch zeigende Fehler behoben werden. Dieser Lösungsansatz ist aber nur begrenzt zufriedenstellend, da die Wirksamkeit der einzelnen Zusatzverträge doch wiederum von der Unterzeichnung und Ratifizierung möglichst vieler Staaten abhängig ist.

---

324 Vgl. GISIN, S. 5ff.; A.M. BALTISSER, S. 151; Zum deutschen Recht vgl. SEIDL/FUCHS, HSSR, S. 85ff.
325 Vgl. z.B. CoE, Zusatzprotokoll vom 28.01.2003.
326 Vgl. z.B. Rahmenbeschluss 2005/222/JI.

7.2.3 Braucht es bei den internationalen Instrumenten zur Zusammenarbeit auch Vorbehaltsmöglichkeiten?

Im Gegensatz zu den Straftatbeständen können die Mitgliedstaaten im Teil zur internationalen Zusammenarbeit kaum Vorbehalte und Erklärungen anbringen. Es stellt sich die Frage, ob es hier überhaupt Vorbehaltsmöglichkeiten braucht. In Anbetracht der Zielsetzung, die internationale Zusammenarbeit effizienter zu gestalten, ist fraglich, ob Vorbehaltsmöglichkeiten dieses Ziel nicht sogar unterlaufen würden.

Einem Rechtshilfeverfahren liegt immer eine Straftat zugrunde. Ob eine solche jeweils gegeben ist, können die Staaten dank der Vorbehaltsmöglichkeiten im ersten Teil der Konvention stark beeinflussen. Bei fast jedem Straftatbestand kann die Anwendung teilweise ausgeschlossen oder die Erfüllung an weitere Voraussetzungen geknüpft werden. Fehlt es an der beidseitigen Strafbarkeit, wird einem entsprechenden Rechtshilfeersuchen i.d.R. nicht entsprochen. Die Vorbehaltsmöglichkeiten aus dem ersten Teil haben also direkte Auswirkungen auf die Anwendbarkeit des dritten Teils. In diesem zusätzliche Möglichkeiten vorzusehen, welche das Ablehnen eines Ersuchens erlauben, erscheint deshalb überflüssig.

Ein weiteres Argument, welches gegen zusätzliche Vorbehaltsmöglichkeiten spricht, ist die fehlende Notwendigkeit. Immer wieder wird verdeutlicht, dass das CCC ergänzend zu den bereits bestehenden internationalen Verträgen und Abkommen zur Anwendung gelangt. Die allgemeinen Grundsätze der Rechtshilfe finden demnach auch auf dieses Abkommen Anwendung.[327] Ist die Grundlage für die Rechtshilfeleistung einmal gegeben, sollte von einer solchen nur noch abgesehen werden dürfen, wenn die Erledigung des Ersuchens die staatliche Souveränität etc.[328] gefährdet. Dieser Grundsatz beansprucht innerhalb der Rechtshilfe eine umfassende Wirkung, weshalb weitere als die im Abkommen ohnehin vorgesehenen spezifischen Vorbehalte überflüssig sind. Auf das Anbringen von Vorbehaltsmöglichkeiten bei den Rechtshilfemassnahmen (Art. 31, Art. 33 und Art. 34 CCC) kann damit verzichtet werden. Auch bei den vorsorglichen Massnahmen nach Art. 29f. CCC bedarf es keiner weiteren als der bereits verankerten Vorbehaltsmöglichkeit. In Art. 29 Abs. 4 CCC können sich die Mitgliedstaaten das Recht vorbehalten, hinsichtlich weiterer Tatbestände als Art. 2-11 CCC die Anordnung der vorsorglichen Datensicherung vom Vorliegen der beidseitigen Strafbarkeit abhängig zu machen.

---

[327] Vgl. Art. 25 Abs. 4 CCC.
[328] Vgl. z.B. Art. 29 Abs. 5 CCC, Art. 31 Abs. 2 CCC.

Indem sich das vorsorgliche Überliefern von Verkehrsdaten nach Art. 30 CCC auf ein Ersuchen nach Art. 29 CCC stützt, gilt für diesen, auch wenn im Gesetzestext nicht explizit formuliert, die gleiche Einschränkung wie bei Art. 29 CCC. Somit erübrigt sich auch hier die Forderung nach weiteren Vorbehaltsmöglichkeiten. Einzig bei Art. 32 lit. b CCC würde sich eine Vorbehaltsmöglichkeit rechtfertigen. Dies aber vor allem aus Datenschutzgründen.[329]

Die Forderung nach weiteren Vorbehaltsmöglichkeiten im Teil zur internationalen Zusammenarbeit ist zuletzt auch deshalb nicht nachvollziehbar, da solche den Sinn und Zweck des Abkommens gänzlich unterlaufen würden. Nachdem es den Vertragsmitgliedern gestattet ist, die Grundlage der internationalen Rechtshilfe mit etlichen Vorbehalten und Erklärungen dem jeweiligen nationalen Recht entsprechend anzupassen, würde das ganze Konstrukt der Rechtshilfe in Frage gestellt werden, wenn zusätzliche Vorbehalte vorgebracht werden könnten. Dies würde nur zu einer unnötigen Anhäufung von Vorbehalten führen, welche die Umsetzung des Abkommens massiv erschweren, wenn nicht sogar verunmöglichen. Die Kritik, im Gegensatz zum Straftatenkatalog lassen sich im Kapitel zur internationalen Zusammenarbeit kaum Vorbehaltsmöglichkeiten finden, ist somit unbegründet.

7.2.4 Exkurs: Kritik zu Art. 32 lit. b CCC aus datenschutzrechtlicher Sicht

Art. 32 lit. b CCC erlaubt den Zugriff auf nicht öffentlich zugängliche Daten, wenn die freiwillige Zustimmung einer berechtigten Person vorliegt. Dies ist grundsätzlich unproblematisch, solange die zustimmungsberechtigte Person gleichzeitig die Inhaberin der Daten ist und damit auch die Weitergabe derselben direkt beeinflussen kann. Neben den Dateninhabern kommen aber auch Serviceprovider als zustimmungsberechtigte Personen in Frage, wenn sich diese in ihren allgemeinen Nutzungsbedingungen ein entsprechendes Weiterleitungsrecht an in- und ausländische Strafverfolgungsbehörden vorbehalten.[330] In diesem Fall entzieht sich die Zustimmungsbefugnis der betroffenen Person bereits zu jenem Zeitpunkt, in welchem sie sich mit den Nutzungsbedingungen einverstanden erklärt. Der angefragte Serviceprovider kann somit ohne Kenntnis der betroffenen Person einer Datenübermittlung an in- und ausländische Strafverfolgungsbehörden zustimmen.

---

329 Mehr dazu sogleich: Kap. 7.2.4.

330 Vgl. BGer 1B_344/2014 E. 5.10; FORSTER, S. 618f.; Kritisch dazu: HEIMGARTNER, S. 146f.

Die Herausgabe oder der Abruf von Daten nach Art. 32 CCC geschieht, ohne dass ein Gericht vorgängig über deren Zulässigkeit entschieden hat. Die Abwägung zwischen den Interessen des Privaten am Schutz seiner Daten und jenen der Öffentlichkeit an der Strafverfolgung obliegt somit einer Privatperson, ohne dass eine zusätzliche Überprüfung durch eine staatliche Institution vorgenommen werden kann. Die Problematik liegt weniger darin, dass die Daten an eine Strafverfolgungsbehörde weitergeleitet werden, sondern dass die Weiterleitung an eine Behörde im Ausland erfolgt und sich damit die Kontrolle der inländischen Behörden über die Daten faktisch entzieht. Auch wenn die ausländischen Behörden an die Einhaltung gewisser Grundsätze gebunden sind, kann sich eine nachträgliche Anfechtung bzgl. der Herausgabe der Daten äusserst schwierig gestalten. Da eine datenschutzrechtliche Würdigung des Abkommens nicht Inhalt dieser Arbeit ist und dies auch nur wenig zur Frage der verbesserten internationalen Zusammenarbeit beiträgt, wird auf weitere Ausführungen zu diesem Thema verzichtet.

7.2.5 Wie wirkt sich die fehlende Beteiligung wichtiger Staaten auf die Umsetzbarkeit des CCC aus?

Bis heute wurde die Konvention des Europarates zur Bekämpfung der Cyberkriminalität nicht von allen Staaten ratifiziert. Wie bei jedem internationalen Übereinkommen wird auch beim hier thematisierten die Wirksamkeit massgeblich durch die Anzahl der beteiligten Vertragsparteien beeinflusst. Neben einigen Mitgliedern des Europarates wie Russland, Irland und Schweden, fehlen auch Länder wie Argentinien, China und Südafrika.[331] Am auffälligsten ist die Absenz von Ländern wie Russland und China, wo der Ursprung vieler ernsthafter Cyberattacken der letzten Jahre vermutet wird.

Eine erfolgreiche Umsetzung der Konvention kann nur erreicht werden, wenn der Beitritt nahezu universell ist.[332] Ohne eine weltweite Beteiligung der Staaten besteht die Gefahr, dass die Durchführung von Cyberdelikten in Länder ausserhalb des Einflussbereiches der Konvention verlagert wird. Zudem können sich Täter durch die Verschleierung ihrer Tathandlung einer Strafverfolgung entziehen, indem sie ihre Onlineaktivitäten über Länder ausserhalb der Konvention führen. Damit in solchen Fällen eine Strafverfolgung dennoch möglich ist, sind die betroffenen Staaten wieder gezwungen, für die Aufklärung der Straftat den ordentlichen Rechtshilfeweg über die Justizministerien zu beschreiten, sofern ein entsprechendes Abkommen zwischen den Staaten besteht. Fehlt

331 Vgl. Liste der unterzeichneten und ratifizierten Staaten, <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&CL=GER>, Stand: 11.11.2015.

332 Siehe auch: HEIMGARTNER, S. 147; WEBER, S. 444; VATIS, S. 220.

ein solches, ist auf den diplomatischen Weg auszuweichen. Umso geringer die Beziehungen zwischen den Staaten sind, umso höher ist die Wahrscheinlichkeit, dass keine Zusammenarbeit bei der Strafverfolgung von Internettätern zustande kommt. Einerseits besteht damit das Risiko, dass die ersuchten Länder generell von der Rechtshilfeleistung absehen, da bspw. das entsprechende Verhalten in ihrem Land keiner strafrechtlichen Verfolgung unterliegt, oder aber die nötigen nationalen Prozessbestimmungen zur effektiven Strafverfolgung und Beweiserhebung fehlen. Andererseits können bis zur Erledigung des Ersuchens wichtige Daten verloren gehen. Dies verdeutlicht einmal mehr die Wichtigkeit einer möglichst universellen Beteiligung, um eine schnelle, wirksame und umfassende Zusammenarbeit zur Bekämpfung der Cyberkriminalität zu gewährleisten. Mit diesem Problem hat jedoch nicht nur das vorliegende Abkommen zu kämpfen: Grundsätzlich ist es für die Umsetzung von völkerrechtlichen Verträgen immer wünschenswert, dass sich möglichst viele Staaten beteiligen.

Gründe, weshalb einige Staaten von der Ratifikation der Konvention absehen, sind viele denkbar. So wird immer wieder auf den fehlenden Datenschutz hingewiesen[333] und auch das Defizit in Bezug auf die Wahrung der Grundrechte[334] – insbesondere der Schutz der Privatsphäre – wird genannt. Teilweise wurden auch Befürchtungen geäussert, dass Mitgliedstaaten, welche sich nicht den gleichen rechtsstaatlichen Garantien verpflichten wie die westeuropäischen Demokratien, die Pflicht zur umfassenden Leistung von Rechtshilfe ausnutzen würden, um an die Herausgabe von schützenswerten Daten zu gelangen.[335] Diese Kritik scheint zwar angebracht, bei näherer Betrachtung der Liste aller Mitgliedstaaten zeigt sich aber, dass nicht Länder mit entwickelten Demokratien und Grundrechten die Ratifikation unterlassen, sondern überwiegend jene, in welchen der Schutz derselben nicht als oberstes Ziel erklärt wird. Ungeachtet dessen muss es weiterhin Ziel des Abkommens sein, möglichst universelle Anwendung zu erlangen. Allein die stetig zunehmenden Zahlen an Anfragen in der Schweiz im Bereich der Strafverfolgung von Cybercrime belegen die Relevanz des Abkommens. Bei steigender Teilnehmerzahl wird nicht nur die internationale Zusammenarbeit verbessert, gleichzeitig kann auch dank der effizienteren Bekämpfung die Cyberkriminalitätsrate gesenkt werden.

---

333 Vgl. BREYER, DuD, S. 592ff.; EDRI, Protecting Digital Freedom, S. 1ff.

334 BALTISSER, S. 149 m.w.H.; EJPD/BJ, Zf. Vernehmlassungsverfahren, S. 7; ISSS[1], S. 9; LEHMANN, S. II-3; MARBERTH-KUBICKI, N 37f. m.w.H.

335 ISSS[1], S. 9.

8 Schlusswort

Die vorliegende Arbeit verdeutlicht, wie wichtig das CCC für die internationale Bekämpfung der Cyberkriminalität ist. Es hilft die Ländergrenzen, welche von den nationalen Strafverfolgungsbehörden nicht überschritten werden dürfen, dank internationaler Rechtshilfeinstrumente zu überwinden. Ohne ein solches bindendes Abkommen wäre die strafrechtliche Verfolgung grenzüberschreitender Internetdelikte innert nützlicher Frist kaum denkbar.

Im Gegensatz zur hoheitlichen Ermittlungskompetenz endet der Wirkungsbereich eines Cyberdeliktes nicht an der Staatsgrenze. Vielmehr öffnet sich durch die neuen Kommunikationstechnologien ein beträchtlicher Wirkungsbereich für Internetdelikte, welcher weit über die Landesgrenzen hinausgeht. Um diesen neuen kriminologischen Phänomen erfolgreich entgegen zu treten, bedarf es einer effizienten und wirksamen internationalen Zusammenarbeit. Diese kann nur erfolgreich sein, wenn bindende Bestimmungen vorliegen, auf welche sich die einzelnen Staaten bei der Strafverfolgung berufen können. Ohne diese Verpflichtungen ist es ungewiss, ob überhaupt und in welchem Umfang Rechtshilfe von den betroffenen Staaten geleistet wird. Darüber hinaus birgt ein langwieriges Verfahren in sich die Gefahr, dass bis zur Erledigung eines Rechtshilfeersuchens wichtige Daten unbrauchbar werden oder gar verloren gehen. Ein Abkommen, welches diesen Missständen entgegenwirkt, ist deshalb essentiell.

Diesen Anforderungen versucht das CCC gerecht zu werden. Das vom Europarat initiierte Abkommen entstand aus der Erkenntnis, dass nur die internationale Gemeinschaft den Anforderungen der neuen Informationstechnologien und den damit neu auftretenden Kriminalitätsphänomenen gewachsen ist. Bis heute wurde das Abkommen von 47 Staaten ratifiziert und von weiteren 7 Staaten unterzeichnet. Für die Schweiz trat das CCC per 01. Januar 2012 in Kraft. Für die Umsetzung des Abkommens bedurfte es kleineren Anpassungen des Strafgesetzbuches und des Gesetzes zur internationalen Rechtshilfe, welche zeitgleich mit dem CCC für rechtsgültig erklärt wurden.

Das CCC verpflichtet seine Mitgliedstaaten zur Anpassung der materiellen und prozessrechtlichen Bestimmungen an die Herausforderungen der neuen Informationstechnologien. Mit der Harmonisierung der nationalen Rechtsordnungen wird eine wichtige Grundlage für das gegenseitige Leisten von Rechtshilfe geschaffen. An etlichen Stellen des Straftatbestandskataloges bietet das CCC die Möglichkeit, bei der Umsetzung der

Konvention Vorbehalte und Erklärungen anzubringen. Die individuelle Abänderbarkeit einzelner Bestimmungen wirkt jedoch der vollständigen Harmonisierung der nationalen Rechtsordnungen entgegen. Gleichzeitig fördern die Vorbehaltsmöglichkeiten aber die Wahrscheinlichkeit neuer Beitritte, was wiederum die internationale Zusammenarbeit verbessert. Aus diesem Grund ist die Beschränkung der Harmonisierung zugunsten der Souveränität bestehender und potentieller Mitgliedsstaaten in Kauf zu nehmen.

Die Auseinandersetzung mit dem Straftatbestandskatalog des CCC verdeutlicht, dass dieses vor allem Delikte der Computerkriminalität unter Strafe stellt. Darüber hinaus verlangt das CCC aus dem Bereich der Internetkriminalität i.e.S. lediglich die Kriminalisierung von Kinderpornographie und den Schutz vor Urheberrechtsverletzungen und Verletzungen verwandter Schutzrechte. Der Kritik, der Straftatbestandskatalog sei nicht vollständig, was zur Unterlaufung der Ziele des CCC führen würde, ist zu widersprechen. Da das CCC subsidiär zu bereits bestehenden internationalen Abkommen zur Anwendung gelangt, ist ein weites Feld an Delikten, welche vor allem unter den Begriff der Internetkriminalität i.e.S. subsumiert werden können, strafrechtlich erfasst. Eine Ausweitung des Tatbestandskatalogs des CCC erübrigt sich damit. Zudem würde eine Anpassung des Tatbestandskatalogs an der fehlenden Durchsetzbarkeit in den beteiligten Staaten scheitern.

Im CCC werden allgemeine klassische Rechtshilfeinstrumente aufgeführt, welche die Staaten verpflichten, in Bezug auf die Herausgabe von gespeicherten Computerdaten und die Erhebung von Verkehrsdaten in Echtzeit gegenseitig Rechtshilfe zu leisten. Darüber hinaus werden mit dem CCC auch neue Instrumente zur internationalen Strafverfolgung im Bereich der Cyberkriminalität, wie die Anordnung vorsorglicher Massnahmen, eingeführt. Gerade diese tragen massgeblich dazu bei, der Gefahr von Datenverlusten durch die lange Dauer eines ordentlichen Rechtshilfeverfahrens entgegen zu wirken. So kann einerseits gemäss Art. 29ff. CCC unter in Aussichtstellen eines entsprechenden Ersuchens bereits die vorsorgliche Sicherung von Computerdaten beantragt werden. Darüber hinaus können im Rahmen eines solchen Ersuchens noch vor Eingang eines Rechtshilfeersuchens Verkehrsdaten an den ersuchenden Staat geliefert werden, wenn sich herausstellt, dass ein Dienstanbieter im Ausland an der Kommunikation beteiligt war. Die Kritik, die Übermittlung solcher Daten unterlaufe die Schutzwirkungen eines ordentlichen Rechtshilfeverfahrens, ist ungerechtfertigt, unterliegt die vorzeitige

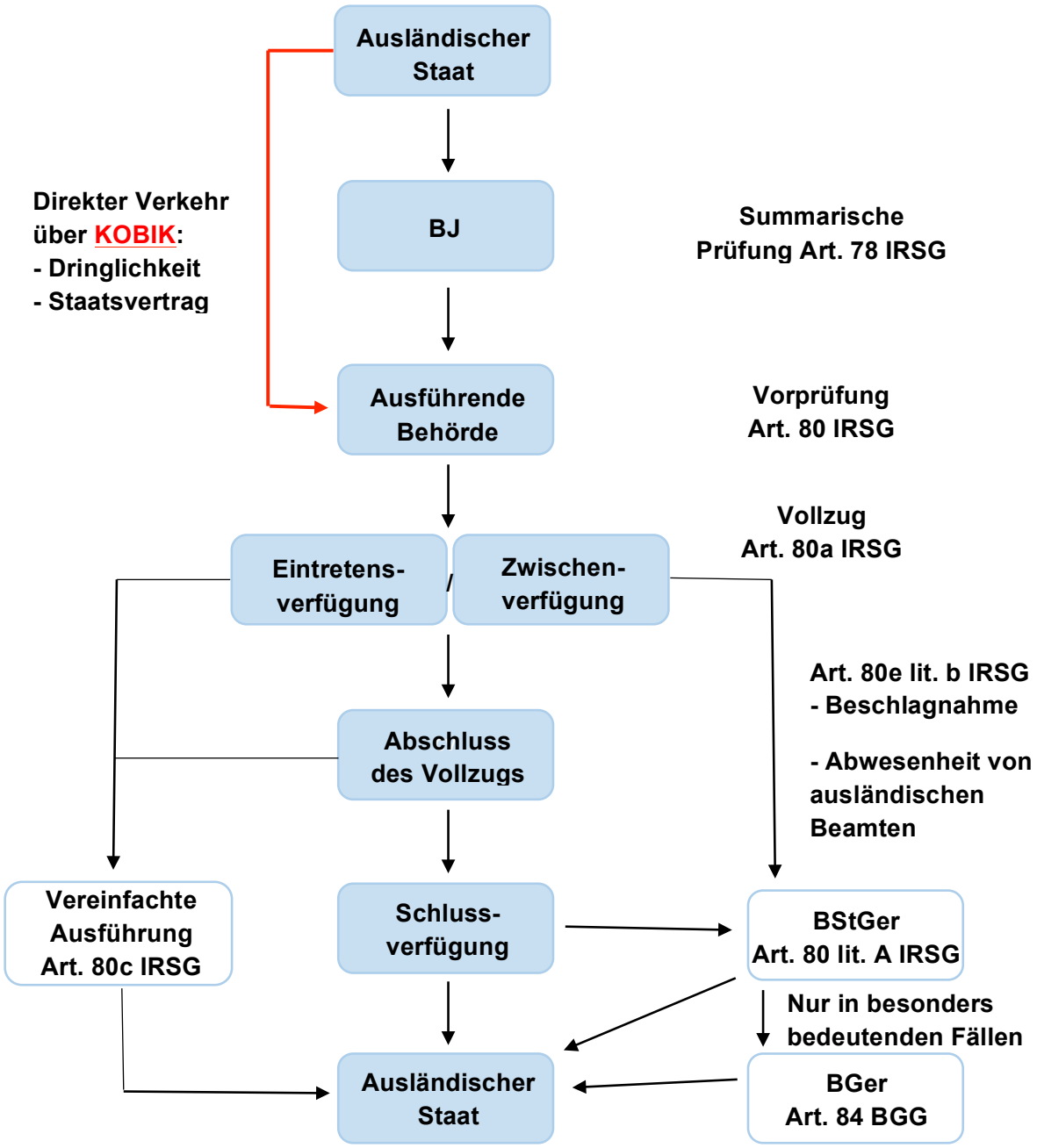
Übermittlung von Verkehrsdaten schliesslich einer strengen Überprüfung, welche jener eines ordentlichen Rechtshilfeverfahrens gleich kommt.

Art. 32 CCC erlaubt neben dem Zugriff auf öffentlich zugängliche Daten auch den direkten Zugriff auf nicht öffentliche Daten, sofern die freiwillige Zustimmung einer berechtigten Person vorliegt. Diese muss dabei nicht von einer inländischen Person erfolgen. Grundsätzlich trägt auch dieses Instrument massgeblich zur Beschleunigung der grenzüberschreitenden Strafverfolgung bei. Liegt die Zustimmungsberechtigung bei einem Service-Provider ist dieses Instrument jedoch kritisch zu hinterfragen. Schliesslich liegt in diesem Fall die Entscheidung über die Herausgabe der Daten an eine ausländische Strafverfolgungsbehörde bei einer Privatperson, ohne dass vorher eine staatliche Instanz über deren Zulässigkeit entscheiden konnte.

Abschliessend bleibt zu sagen, dass trotz der aufgezeigten Mängel, welche im CCC an einigen Stellen auftreten, die Instrumente der internationalen Zusammenarbeit sehr wohl geeignet sind, die Bekämpfung der Internetkriminalität zu ermöglichen und zu verbessern. Schon allein die Tatsache, dass die Vertragsparteien die vorsorgliche Sicherung von Daten verlangen können, trägt massgeblich dazu bei, dem Verlust wichtiger Daten entgegenzuwirken. Auch wenn das CCC grundsätzlich als Ergänzung zu bereits bestehenden Verträgen aus dem Bereich der Rechtshilfe zur Anwendung gelangt, gilt es dennoch die Besonderheit hervorzuheben, dass das CCC neben den „klassischen“ Rechtshilfeinstrumenten auch andere, vorsorgliche und sogar rechtshilfeunabhängige Massnahmen beinhaltet. Auch die klaren Aussagen, in welchen Bereichen Rechtshilfe zu leisten ist, schafft für die Vertragsparteien eine Grundlage, auf welche sie sich im Rahmen der internationalen Zusammenarbeit stützen können. Das Zusammenspiel all dieser Massnahmen ermöglicht schliesslich die Umsetzung des Ziels, eine effizientere, umfassendere und wirksamere Bekämpfung von Cyberkriminalität zu gewährleisten.

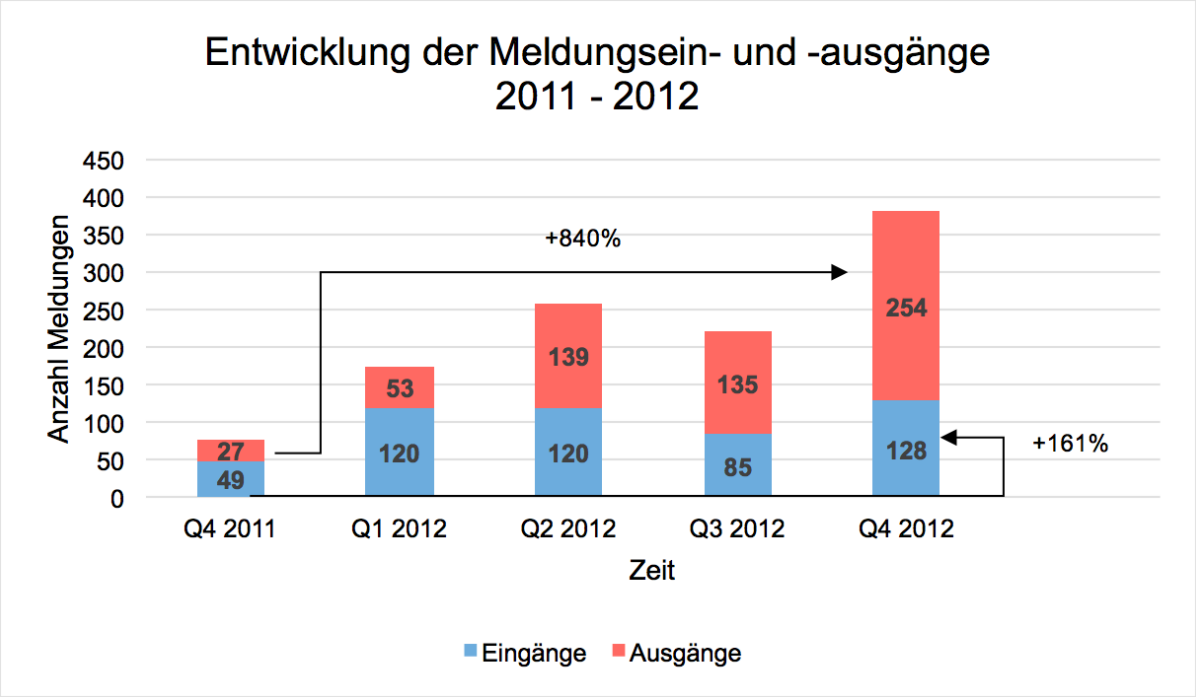
9 Anhang

9.1 Ablauf eines Rechtshilfeverfahrens

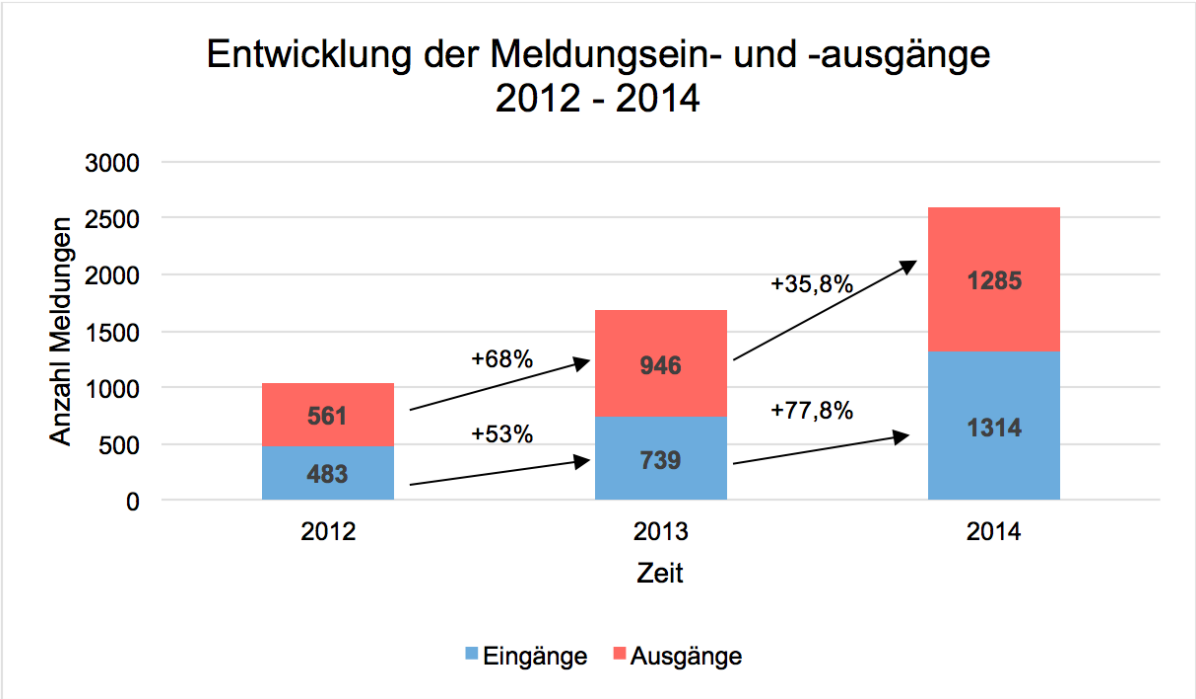


Quelle: Eigene Darstellung in Anlehnung an: Wegleitung, S. 90.

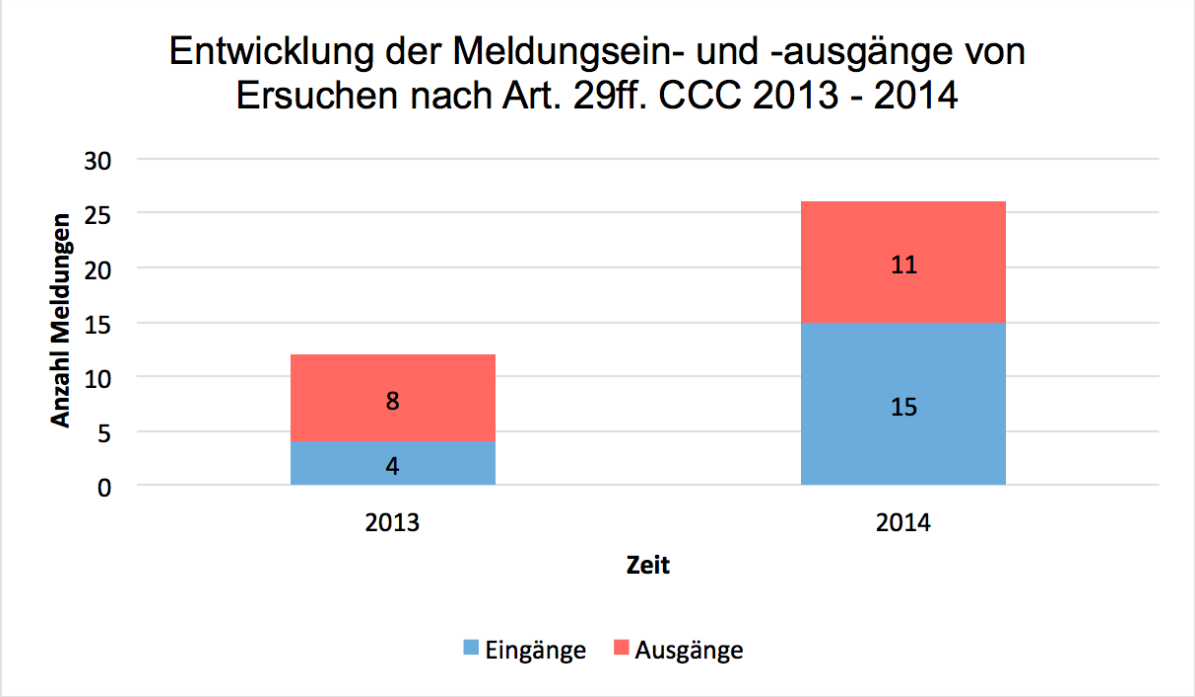
9.2 Entwicklung der Meldungsein- und -ausgängen bei KOBIK betreffend Cyberkriminalität vor und nach Inkrafttreten des CCC



Quelle: Eigene Darstellung in Anlehnung an: KOBIK, Jahresbericht 2012-2014.



Quelle: Eigene Darstellung in Anlehnung an: KOBIK, Jahresbericht 2012-2014.



Quelle: Eigene Darstellung in Anlehnung an: KOBIK, Jahresbericht 2012-2014.

Eigenständigkeitserklärung

"Ich erkläre hiermit,

- dass ich die vorliegende Arbeit selbstständig ohne fremde Hilfe und ohne Verwendung anderer als der angegeben Hilfsmittel verfasst habe;
- dass ich sämtliche verwendeten Quellen erwähnt und gemäss gängigen wissenschaftlichen Zitierregeln korrekt zitiert habe;
- dass das Thema, die Arbeit oder Teile davon nicht bereits Gegenstand eines Leistungsnachweises einer anderen Veranstaltung oder Kurses war; sofern dies nicht ausdrücklich mit dem/der Dozierenden im Voraus vereinbart wurde;
- dass ich ohne schriftliche Zustimmung der Universität keine Kopien dieser Arbeit an Dritte aushändigen oder veröffentlichen werde, wenn ein direkter Bezug zur Universität St. Gallen oder ihrer Dozierenden hergestellt werden kann;
- dass ich mir bewusst bin, dass meine Arbeit elektronisch auf Plagiate überprüft werden kann und ich hiermit der Universität St. Gallen laut Prüfungsordnung das Urheberrecht soweit einräume, wie es für die Verwaltungshandlungen notwendig ist."

Steckborn, 16. November 2015

Yaelle Häring