Cyber-Kriminalität

Susanne Reindl-Krauskopf[*]

Abstract

Schon seit geraumer Zeit beschäftigen sich der Europarat und die Europäische Union mit dem Phänomen der Cyberkriminalität. Während der Europarat versucht, diese Kriminalitätsform in einem einzigen Rechtsakt, nämlich der Cybercrime-Konvention vom 23.11.2001 inkl. Zusatzprotokoll, zu erfassen, behandelt die Europäische Union die verschiedenen Ausprägungen des Cybercrime in unterschiedlichen Rechtsakten. Der folgende Beitrag konzentriert sich auf das materielle Cyber-Strafrecht. Neben einem allgemeinen Vergleich, der auch die Durchsetzung der Konventions- bzw. der europarechtlichen Pflichten beleuchtet, erfolgt weiter eine Detailbetrachtung anhand ausgewählter Beispiele. Diese behandelt das Strafensystem sowie den Vergleich einzelner Tatbestände, z. B. des widerrechtlichen Zugangs zu Systemen. Diskutiert werden dabei die Bestimmungen der Art. 2, 5 und 13 der Cybercrime-Konvention, Art. 2 und Art. 3 des Rahmenbeschlusses des Rates vom 24.2.2005 über Angriffe auf Informationssysteme (ABl. 2005 L 69/67) sowie die Art. 3, 4, 7 und 9 der Richtlinie des Europäischen Parlaments und des Rates vom 12.8.2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates (ABl. 2013 L 218/8). Der vorliegende Beitrag arbeitet Überschnei-

[*] Univ.-Prof. Dr., die Autorin ist Inhaberin des Lehrstuhls für Strafrecht, Strafprozessrecht und Kriminologie an der Universität Wien.

dungen, Gemeinsamkeiten und Unterschiede zwischen diesen Rechtsakten heraus. Im Zuge dessen werden auch die relevanten Entwicklungen in der europäischen Gesetzgebung dargestellt.

I. Einleitung

1. Allgemeines

Welche Instrumente gibt es im Europarat und in der Europäischen Union? Welche Überschneidungen und welche Abweichungen bestehen inhaltlicher Natur? Ich bin gebeten worden, diesen Fragen nachzugehen und ein entsprechendes Bild des Status quo im Vergleich zwischen den beiden europäischen Ebenen im Bereich der Cyber-Kriminalität zu zeichnen.

Aber was ist eigentlich Cyber-Kriminalität? Mit dieser Frage muss der Vergleich im Grunde beginnen. Denn die Cybercrime Konvention des Europarates vom 23.11.2001[1] (im Folgenden: CyCC) erfasst unter diesem Titel materielles Cyberstrafrecht (Art. 2-13 CyCC) und prozessuale Instrumente, wie etwa die Kommunikationsüberwachung oder Datensicherung (Art. 14-22 CyCC) und internationale Zusammenarbeit (Art. 23-35 CyCC). Schon dabei zeigt sich ein erster wesentlicher Unterschied darin, wie der Europarat einerseits und die Europäische Union anderseits an dieses Phänomen herangehen. Denn selbstverständlich gibt es in allen drei Bereichen auch auf Unionsebene einschlägige Rechtsakte: Denken Sie nur etwa an das Übereinkommen über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der EU vom 29.5.2000,[2] das sich in seinen Art. 17-22 mit Fragen der Telekommunikationsüberwachung beschäftigt, oder an den Rahmenbeschluss über die Vollstreckung von Entscheidungen über die Sicherstellung von Vermögensgegenständen oder Beweismitteln in der Europäischen Union

[1] ETS Nr. 185; zur Entstehungsgeschichte, die bis in die 1990er Jahre zurückreicht, siehe den Erläuternden Bericht zur CyCC, Rz. 7 ff.; *E. Hilgendorf/B. Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, 38 ff.; *D. Krutisch*, Strafbarkeit des unberechtigten Zugangs zu Computerdaten und -systemen, in: M. Maiwald, Schriften zum Strafrecht und Strafprozessrecht, Bd. 72, 2004, 48 ff.; *O. Plöckinger*, Internet und materielles Strafrecht – Die Convention on Cyber-Crime, in: O. Plöckinger/D. Duursma/G. Helm, Aktuelle Entwicklungen im Internet-Recht, 2002, 113 f.; *S. Reindl*, E-Commerce und Strafrecht, 2003, 19 f.; *D. Schuh*, Computerstrafrecht im Rechtsvergleich – Deutschland, Österreich, Schweiz, 2012, 35 ff.; *C. Schwarzenegger*, Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime vom 23. November 2001, in: FS S. Trechsel, 2002, 308 ff.

[2] ABl. 2000 C 197/1.

vom 22.7.2003,[3] der – wie der Name schon sagt – u. a. die grenzüberschreitende Sicherstellung von Beweismitteln regelt. Doch handelt es sich eben um einzelne Rechtsinstrumente und nicht um einen einzigen umfassenden Rechtsakt vergleichbar der CyCC. Um die Gegenüberstellung anschaulicher zu machen, werde ich mich in der Folge allerdings auf das materielle Recht beschränken.

2. Materielles Cyberstrafrecht

Die Cybercrime Konvention des Europarates wird meines Erachtens zu Recht als wichtigste europäische und völkerrechtliche Rechtsgrundlage auf diesem Gebiet bezeichnet;[4] und zwar nicht zuletzt deshalb, weil sie auch im materiellen Recht versucht, möglichst viele der eben angesprochenen Bereiche abzudecken: Neben den Angriffen auf Daten und Systeme (Art. 2-6 CyCC) finden sich auch Vorgaben zur "Computerbezogenen Fälschung" (Art. 7 CyCC), zum "Computerbezogenen Betrug" (Art. 8 CyCC), zur Kinderpornographie (Art. 9 CyCC) und zu Urheberrechtsverletzungen (Art. 10 CyCC).

Die Rechtsinstrumente auf Ebene der Europäischen Union beschäftigen sich zwar ebenfalls mit vielen dieser Aspekte. Doch sind diese typischerweise in unterschiedlichen einzelnen Rechtsakten geregelt: Angriffe auf Daten und Systeme sind z. B. Gegenstand des Rahmenbeschlusses über Angriffe auf Informationssysteme[5] und nunmehr der Richtlinie über Angriffe auf Informationssysteme und zur Ersetzung des genannten Rahmenbeschlusses auf Angriffe gegen Daten und Systeme.[6] Der Kampf gegen die Kinderpornographie, die in Art. 9 CyCC angesprochen ist, findet auf Unionsebene Widerhall im Rahmenbeschluss zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornographie[7] bzw. in der Richtlinie zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeu-

[3] RB 2003/577/JI, ABl. 2003 L 196/45.

[4] So explizit die Mitteilung der Kommission an das Europäische Parlament, den Rat und den Ausschuss der Regionen (Eine allgemeine Politik zur Bekämpfung der Internetkriminalität), KOM(2007) 267 endg. vom 22.5.2007.

[5] RB 2005/222/JI des Rates vom 24.2.2005 über Angriffe auf Informationssysteme, ABl. 2005 L 69/67.

[6] RL 2013/40/EU des Europäischen Parlaments und des Rates vom 12.8.2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates, ABl. 2013 L 218/8.

[7] RB 2004/68/JI des Rates vom 22.12.2003 zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornografie, ABl. 2004 L 13/44.

tung von Kindern sowie der Kinderpornographie sowie zur Ersetzung des genannten Rahmenbeschlusses.[8] Als letztes Beispiel sei noch der Rahmenbeschluss zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln[9] genannt, dessen Art. 3 starke Überschneidungen mit dem computerbezogenen Betrug nach Art. 8 CyCC aufweist.

3. Zwischenergebnis

Als erstes Ergebnis des Vergleichs zeigt sich somit, dass die Vertragsparteien der CyCC versucht haben, einen möglichst umfassenden Rechtsrahmen für das Phänomen der Cyber-Kriminalität zu erarbeiten. Damit wurde die Konvention zu einer ganz wesentlichen Grundlage in diesem Bereich, auf der gut aufgebaut werden kann[10] und die eine Reichweite über die EU, ja selbst über die Europaratsstaaten hinaus besitzt. So können nämlich nicht nur Mitgliedstaaten des Europarates Vertragspartei sein, sondern auch andere Staaten, die sich an der Verhandlung beteiligt haben (Art. 36 CyCC), und solche, die zum Beitritt eingeladen werden (Art. 37 CyCC). So ist die CyCC bislang auch z. B. für Australien, die Dominikanische Republik, Japan und die USA in Kraft getreten.[11]

Damit zeigt sich aber auch ein entscheidender Nachteil der CyCC: Sie ist gerade für ein Themengebiet wie die Cyber-Kriminalität, die sich in technischer Hinsicht und damit auch betreffend die Art der Angriffe und die Modi Operandi relativ rasch weiterentwickelt hat, ein relativ altes Vertragswerk; stammt sie doch schon aus 2001. Anpassungen an die veränderte

[8] RL 2011/93/EU des Europäischen Parlaments und des Rates vom 13.12.2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates, ABl. 2011 L 335/1.

[9] RB 2001/413/JI des Rates vom 28.5.2001 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln, ABl. 2001 L 149/1.

[10] So explizit u. a. der Vorschlag für einen Rahmenbeschluss des Rates über Angriffe auf Informationssysteme vom 19.4.2002, KOM(2002) 173 endg., 10; RB 2005/222/JI, Erwägungsgrund 7; Mitteilung des Rates der Europäischen Union an die Presse über die 2827. Tagung des Rates Justiz und Inneres vom 8. und 9.11.2007 zur Bekämpfung der Internetkriminalität, 14617/07 (Presse 253), Punkt 4 der Schlussfolgerungen zur Bekämpfung der Internetkriminalität; RL 2013/40/EU, Erwägungsgrund 15. Stets hielten die europäischen Institutionen die Mitgliedstaaten auch dazu an, die Ratifizierung der CyCC voranzutreiben (siehe u. a. Mitteilung der Kommission an das Europäische Parlament, den Rat und den Ausschuss der Regionen [Eine allgemeine Politik zur Bekämpfung der Internetkriminalität], KOM[2007] 267 endg. vom 22.5.2007, 7).

[11] Für einen Überblick über den Stand der Unterschriften, Ratifikationen und des In-Krafttretens siehe: <http://www.conventions.coe.int>.

Kriminalitätswirklichkeit wären notwendig. Solche Überarbeitungen und Anpassungen an neue Herausforderungen sind jedoch schwierig, weil sie auf ein Aufschnüren des Gesamtpakets mit langwierigen Verhandlungen hinauslaufen würden. Rasche Adaptierungen sind daher wenig realistisch. Je mehr Staaten am Vertragswerk beteiligt sind, umso schwieriger wird es auch, alle – womöglich gegenläufigen – Interessen zu koordinieren. Das hat sich schon während der Verhandlungen zur CyCC gezeigt. Gab es ursprünglich noch Bestrebungen, bei den inhaltsbezogenen Delikten neben der Kinderpornographie auch rassistische und fremdenfeindliche Inhalte aufzunehmen, so scheiterte dies rasch an den widerstreitenden Interessen der verhandelnden Staaten.[12] Zuletzt wurde der Kompromiss erzielt, diese Inhalte über ein Zusatzprotokoll[13] zu regeln, das allerdings bei weitem nicht die vergleichbare Schärfe wie die Stammkonvention aufweist, sondern eine Fülle von Vorbehalten bei den einzelnen Regelungen vorsieht.[14]

Demgegenüber muss man zwar erst alle einschlägigen Rechtsakte zusammenstellen, wenn man sich über den Rechtsrahmen für die Cybercrime-Bekämpfung auf Unionsebene ähnlich umfassend informieren will, wie er in der CyCC abgebildet ist. Doch ergibt sich durch die einzelnen spezifischen Rechtsakte i. d. R. eine größere Flexibilität hinsichtlich Änderungen, die aufgrund rechtlicher Fragen, des technischen Fortschritts oder wegen neuer krimineller Erscheinungsformen notwendig werden.

Im Übrigen unterscheiden sich die Mechanismen zur Durchsetzung der Konventions- bzw. europarechtlichen Pflichten wesentlich: Im Europarat besteht im Grunde bei Nichtumsetzung der Vertragspflichten nur die Möglichkeit, das Stimmrecht eines Mitgliedstaates zu suspendieren bzw. ihn nach Art. 8 i. V. m. Art. 3 des Statutes des Europarates auszuschließen. Praktisch gesehen sind solche Sanktionen aber aus politischen Gründen eher unwahrscheinlich.[15]

Auf Unionsebene war die Umsetzungskontrolle im Zusammenhang mit Rahmenbeschlüssen nur schwach ausgebildet; die Kommission hatte näm-

[12] Vgl dazu etwa *F. Zeder*, Internet und Strafrecht, in: WiR - Studiengesellschaft für Wirtschaft und Recht, Internet und Recht, 2002, 73 (87).

[13] Zusatzprotokoll zum Übereinkommen über Cyberkriminalität betreffend die Kriminalisierung mittels Computersystemen begangener Handlungen rassistischer und fremdenfeindlicher Art, ETS Nr. 189 vom 28.1.2003. Zum Vergleich könnte man hier im Übrigen den RB 2008/913/JI des Rates vom 28.11.2008 zur strafrechtlichen Bekämpfung bestimmter Formen und Ausdrucksweisen von Rassismus und Fremdenfeindlichkeit vom 28.11.2008, ABl. 2008 L 328/55.

[14] Von den vier Artikeln, die sich mit inhaltlichen Vorgaben für Straftatbestände beschäftigen, sehen drei Vorbehaltsmöglichkeiten vor.

[15] Zu diesem Kontrollmechanismus näher *P. Fischer/H. F. Köck/M. M. Karollus*, Europarecht, 4. Aufl. 2002, Rz. 163.

lich keine Handhabe.[16] Doch seit dem Vertrag von Lissabon werden nunmehr auch die strafrechtlichen Regeln insbesondere in Form von Richtlinien (Art. 83 AEUV) erlassen. Wird ein Mitgliedstaat bei der Umsetzung einer Richtlinie säumig, so kann die Kommission ein Vertragsverletzungsverfahren gegen diesen Mitgliedstaat anstrengen (Art. 258 AEUV), was bis zur Verhängung von Pauschalbeträgen oder Zwangsgeldern gegenüber säumigen Mitgliedstaaten durch den EuGH führen kann (Art. 260 AEUV) und den Druck zur Umsetzung doch wesentlich erhöht.

II. Detailvergleich anhand ausgewählter Beispiele

Im Folgenden werde ich anhand des klar umgrenzten Bereichs der Angriffe auf Daten und Systeme auf Unterschiede bzw. Überschneidungen zwischen CyCC und dem Unionsrecht eingehen. Dabei geht es um Art. 2-6 CyCC einerseits und die Richtlinie über Angriffe auf Informationssysteme (im Folgenden: Richtlinie) anderseits. Soweit zwischen dem vorangegangenen Rahmenbeschluss über Angriffe auf Informationssysteme (im Folgenden: Rahmenbeschluss)[17] und der Richtlinie nennenswerte Unterschiede bestehen, werde ich auch den Rahmenbeschluss einbeziehen.

1. Strafensystem

Bevor ich einige Tatbestände vergleiche, darf ich auf die allgemeine Frage der vorgesehenen Strafen eingehen. Art. 13 CyCC spricht von der Pflicht, wirksame, verhältnismäßige und abschreckende Sanktionen, einschließlich Freiheitsstrafen vorzusehen. Damit greift die Europaratskonvention weniger intensiv in gewachsene Rechtssysteme ein als die Rechtsinstrumente auf

[16] Siehe dazu nur u. a. *F. Zeder*, Der Rahmenbeschluss als Instrument der EU-Rechtsangleichung im Strafrecht am Beispiel des Rahmenbeschlusses gegen Geldfälschung, ÖJZ 2001, 81 (82 f); *R. Feik*, in: H. Mayer, Kommentar zu EU- und EG-Vertrag, Bd. I, 2006, Art. 35 EUV, Rz. 2.

[17] Siehe zur Vorgeschichte zum Rahmenbeschluss u. a. die Empfehlung 7 der Strategie "Prävention und Bekämpfung der organisierten Kriminalität. Eine Strategie der Europäischen Union für den Beginn des neuen Jahrtausends", ABl. 2000 C 124/1, die Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen (eEurope 2002), KOM(2000) 890 endg. vom 26.1.2001, 8 ff. und 17 sowie die Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen (Sicherheit der Netze und Informationen: Vorschlag für einen europäischen Politikansatz), KOM(2001) 298 endg. vom 6.6.2001, 10 ff.

Unionsebene. Die Richtlinie verlangt zwar ebenso wirksame, angemessene und abschreckende Strafen (Art. 9 RL 2013/40/EU).[18] Doch wird durch die Richtlinie eine Verpflichtung zur Einführung einer ganzen Reihe von Mindesthöchststrafen vorgesehen:

- Als allgemeine Regel werden Freiheitsstrafen im Höchstmaß von mindestens zwei Jahren verlangt, wenn kein leichter Fall vorliegt (Art. 9 Abs. 2 RL 2013/40/EU),
- Freiheitsstrafen im Höchstmaß von mindestens drei Jahren bei Eingriffen in Systeme und Daten (Art. 4, 5 RL 2013/40/EU), falls eine beträchtliche Anzahl von Informationssystemen unter Verwendung bestimmter Tatwerkzeuge beeinträchtigt wird (Art. 9 Abs. 3 RL 2013/40/EU) und
- Freiheitsstrafen im Höchstmaß von mindestens fünf Jahren bei Eingriffen in Systeme und Daten (Art. 4, 5 RL 2013/40/EU), falls die Tat
    - im Rahmen einer kriminellen Vereinigung begangen wurde,
    - einen schweren Schaden verursacht hat oder
    - gegen ein Informationssystem einer kritischen Infrastruktur verübt wurde (Art. 9 Abs. 4 RL 2013/40/EU).

Wenngleich das Bestreben der Kommission nachvollziehbar sein mag, durch ausreichend hohe Sanktionen die reibungslose Anwendbarkeit der Rechtshilfeinstrumente zu garantieren,[19] so stellt die Verpflichtung zu solchen Mindesthöchststrafen die Mitgliedstaaten mitunter vor wesentliche Schwierigkeiten: Jeder Mitgliedstaat verfügt entsprechend seiner Rechtstradition über eine Rangordnung der Rechtsgüter, die sich auch im strafrechtlichen Sanktionensystem widerspiegelt. So wird die Verletzung als hochwertig beurteilter Güter strenger bestraft als die solcher, die für weniger schützenswert angesehen werden. Typischerweise wird etwa das menschliche Leben als wichtigstes Gut bewertet, weshalb in den Strafgesetzen für vorsätzliche Tötung die höchsten Strafen vorgesehen sind. Verpflichtende Mindesthöchststrafen können solche gewachsenen und in sich schlüssigen Systeme beeinträchtigen. Beispielsweise kann jemand, der einen anderen vorsätzlich leicht am Körper verletzt, in Österreich mit Freiheitsstrafe bis zu einem Jahr bestraft werden. Obwohl es um das Rechtsgut Leib und Leben geht, wäre die Höchststrafe geringer als die Mindesthöchststrafe von zwei Jahren, die die Richtlinie z. B. für das Eindringen in ein fremdes Informationssystem unter Verletzung von Sicherheitsvorkehrungen verlangt, wenn kein leichter Fall vorliegt. Will der nationale Gesetzgeber ein ausgewogenes und dem Stellenwert der Rechtsgüter Rechnung tragendes Sanktionensystem

[18] So auch schon Art. 6 RB 2005/222/JI.
[19] Impact Assessment zum Richtlinienvorschlag, SEC (2010) 1122 endg., 15, 46.

erhalten, müsste er wohl früher oder später auch die Strafen für andere Rechtsgutsverletzungen anheben. Die Verpflichtung zur punktuellen Schaffung von Mindesthöchststrafen in Richtlinien hat somit das wenig wünschenswerte Potenzial, eine Strafbarkeitsspirale nach oben hin zu immer strengeren Strafen zu schaffen und auch Strafrechtsbereiche zu beeinflussen, die von der jeweiligen Richtlinie überhaupt nicht geregelt werden sollten.

Einer solchen Herausforderung stehen die Vertragsstaaten bei der CyCC hingegen nicht gegenüber, denn wirksame, verhältnismäßige und abschreckende Strafen i. S. d. Art. 13 CyCC lassen sich auch jenseits eines Systems zwingender Mindesthöchststrafen in nationalen Rechtssystemen verwirklichen.

2. Einzelne Tatbestände im Vergleich

Im Allgemeinen sind sich die Tatbestände der CyCC, des Rahmenbeschlusses und der Richtlinie sehr ähnlich.[20] Das verwundert auch nicht weiter, baut doch schon der Rahmenbeschluss auf der CyCC auf.[21] Allerdings verzichtete er darauf, zwei in der CyCC vorgesehene Regelungen, nämlich das Abfangen von Daten (Art. 3 CyCC) und die Bestimmungen über spezielle Tatwerkzeuge (Art. 6 CyCC), zu übernehmen. Die Richtlinie enthält nunmehr diesbezügliche Tatbestände (Art. 6 bzw. Art. 7 RL 2013/40/EU).

a) "Hacking" – Zugang zu Systemen

Nach Art. 2 CyCC ist der vorsätzliche unbefugte Zugang zu einem Computersystem als Ganzem oder einem Teil davon als Straftat zu umschreiben. Als Grundsatz soll somit jeglicher vorsätzliche unbefugte Zugang erfasst werden. Allerdings sieht Art. 2 CyCC Möglichkeiten zur Einschränkung der Strafbarkeit vor: Die Vertragsparteien können nämlich als Voraussetzung für die Strafbarkeit vorsehen, dass die Tat

- unter Verletzung von Sicherheitsmaßnahmen,
- in der Absicht, Computerdaten zu erlangen,
- in einer anderen unredlichen Absicht oder

[20] Ein grundsätzlicher Unterschied liegt darin, dass die CyCC an Computersystemen, der Rahmenbeschluss und die Richtlinie hingegen am Informationssystem anknüpfen. Für die weitere Betrachtung kann dieser Unterschied aber vernachlässigt werden.

[21] In diesem Sinne z. B. Erwägungsgrund 7 des RB 2005/222/JI; KOM(2002) 173 endg., 9 ff.

- in Zusammenhang mit einem Netzwerk erfolgt.

Demgegenüber war der vorsätzliche unbefugte Zugang zu einem Informationssystem als Ganzem oder einem Teil davon nach Art. 2 RB 2005/222/JI unter Strafe zu stellen, wenn kein leichter Fall vorliegt. Zusätzlich sah der Rahmenbeschluss dann noch die Möglichkeit vor, die Strafbarkeit auf jene Fälle zu beschränken, in denen der Täter eine Sicherheitsmaßnahme bei der Tat verletzt hat (Art. 2 Abs. 2 RB 2005/222/JI). Anders als nach der CyCC griff die Strafverpflichtung von Vornherein nur jenseits leichter Fälle. Art. 3 RL 2013/40/EU baut darauf auf: Nach der Richtlinie muss jeder vorsätzliche unbefugte Zugang zu einem System als Ganzem oder zu einem Teil davon strafbar sein, wenn dieser Zugang durch Verletzung einer Sicherheitsmaßnahme erfolgt. Auch nach Art. 3 RL 2013/40/EU greift die Verpflichtung zur Sanktionierung nur jenseits leichter Fälle.

Von zentraler Bedeutung für die Strafbarkeit ist nach diesen europarechtlichen Instrumenten demnach, wann kein leichter Fall vorliegt. Was darunter zu verstehen ist, definieren leider weder der Rahmenbeschluss noch die Richtlinie. Insofern würde es naheliegen, die Möglichkeiten zur Strafbarkeitsbeschränkung der zeitlich und inhaltlich vorangegangenen CyCC als Orientierungshilfe heranzuziehen. Umso überraschender sind vor diesem Hintergrund aber die Ausführungen im Bericht der Kommission an den Rat über den Umsetzungsstand des Rahmenbeschlusses.[22] Danach haben vier Mitgliedstaaten die nicht leichten Fälle durch zusätzliche Tatbestandsmerkmale umschrieben:

- Österreich sah einen erweiterten Vorsatz auf Datenspionage, Verwertung der Daten und Vorteilserlangung bzw. Schädigung durch diese Verwertung vor;
- die Tschechische Republik verlangte die anschließende Datenbeschädigung oder deren Missbrauch;
- Finnland setzte die Gefährdung der Daten voraus und
- Lettland eine erhebliche Schädigung.

Nach Art. 2 CyCC sind diese Strafbarkeitseinschränkungen allesamt unproblematisch. Die Kommission fand allerdings, dass diese Umschreibungen der Bedingung des Rahmenbeschlusses "wenn kein leichter Fall vorliegt" nicht angemessen Rechnung tragen.[23] Darüber hinaus hat die Kommission die Mitgliedstaaten aufgefordert, nunmehr beim Tatbestand des

[22] Bericht der Kommission an den Rat auf der Grundlage von Art. 12 des Rahmenbeschlusses des Rates vom 24.2.2005 über Angriffe auf Informationssysteme, KOM(2008) 448 endg. vom 14.7.2008, 4 f.

[23] KOM(2008) 448 endg., 5.

"Hackings" keine über den Richtlinientext hinausgehenden Tatbestandsmerkmale zur Umschreibung des nicht leichten Falles vorzusehen.[24] Wie die Mitgliedstaaten die nicht leichten Fälle aber verlässlich definieren sollen, wenn nicht unter Rückgriff auf solche zusätzlichen Tatbestandsmerkmale, bleibt bedauerlicherweise offen.

Im Vergleich zeigt sich insgesamt, dass Art. 2 CyCC zweifellos als Grundlage für Rahmenbeschluss und Richtlinie dient. Diese europäischen Instrumente gehen aber über Art. 2 CyCC hinaus, indem sie die Strafbarkeit schon auf Tatbestandsebene wesentlich weiter ziehen und keine Strafbarkeitsbeschränkungen, die nach Art. 2 Abs. 2 CyCC noch zulässig wären, mehr vorsehen.

b) Eingriff in Systeme

Die Regeln über unbefugte vorsätzliche Eingriffe in Systeme sehen in allen drei Rechtsakten (Art. 5 CyCC, Art. 3 RB 2005/222/JI, Art. 4 RL 2013/40/EU) Strafen für jene Täter vor, die beispielsweise durch Eingabe großer Datenmengen oder durch Datenmanipulationen Computer- bzw. Informationssysteme in ihrer Funktionalität schwer stören oder beeinträchtigen. Hinsichtlich solcher Angriffe waren Art. 5 CyCC und Art. 3 RB 2005/222/JI im Grunde deckungsgleich. Strafbar sollte nach der CyCC jeder schwere Eingriff und nach dem Rahmenbeschluss jeder nicht leichte Fall sein. Auch die jeweils genannten Tathandlungen waren fast identisch: Eine kleine Abweichung lag darin, dass die CyCC auch das Beeinträchtigen von Computerdaten nannte, während sich im RB stattdessen das Verstümmeln und Unzugänglichmachen von Daten fand. Nennenswerte Unterschiede zwischen CyCC und RB lagen nur in der Frage der Versuchsstrafbarkeit und der Gestaltung der Sanktion. Zwar soll der Versuch nach Art. 11 CyCC grundsätzlich strafbar sein, doch ist dies nicht obligatorisch (Art. 11 Abs. 3 CyCC). Demgegenüber statuierte Art. 5 Abs. 2 RB 2005/222/JI zwingend die Strafbarkeit des Versuchs. Hinsichtlich der Sanktion sahen Art. 6 und 7 RB 2005/222/JI – anders als die CyCC – bereits Mindesthöchststrafen vor.[25]

Art. 4 RL 2013/40/EU baut wieder auf dieser Grundlage auf und übernimmt auch die Tathandlung des Beeinträchtigens aus Art. 5 CyCC. Die

[24] Vorschlag für eine Richtlinie über Angriffe auf Informationssysteme, KOM(2010) 517 endg. vom 30.9.2010, 8.

[25] Und zwar von einem bis zu drei Jahren Freiheitsstrafe, wenn kein leichter Fall vorliegt, und von zwei bis zu fünf Jahren bei Tatbegehung im Rahmen einer kriminellen Vereinigung.

wesentliche Weiterentwicklung liegt im bereits geschilderten System der Mindesthöchststrafen, das – je nach Szenario – abgestuft Mindesthöchststrafen von bis zu zwei, drei und fünf Jahren Freiheitsstrafe vorsieht (Art. 9 Abs. 2-4 RL 2013/40/EU).

Auch für dieses Deliktsfeld gilt somit: Die CyCC war das klare Vorbild, auf dem aufgebaut wurde. Zwischenzeitig erkannte neue Risken, z. B. Botnetzwerke und Anschläge auf kritische Infrastrukturen,[26] wurden in die Überlegungen zu den späteren Rechtsakten miteinbezogen, aber – anders als beim Hacking – nicht auf Tatbestandsebene, sondern bei den Strafrahmen berücksichtigt.

c) Tatwerkzeuge im Vergleich

Art. 6 CyCC sieht unter dem Titel "Missbrauch von Vorrichtungen" die Strafbarkeit für Vorbereitungshandlungen vor. So soll etwa schon derjenige strafbar sein, der mit dem Vorsatz auf rechtswidrigen Zugang zu einem Computersystem ein Spionageprogramm herstellt oder besitzt. Auch das Beschaffen eines Computerpasswortes mit demselben Vorsatz wäre nach Art. 6 CyCC strafrechtlich zu erfassen. Bemerkenswerterweise hat der Rahmenbeschluss diese Bestimmung weder in ihrer ursprünglichen noch in einer ähnlichen Form übernommen.[27]

Die Richtlinie greift dieses Vorfelddelikt wieder auf. Abgesehen von der Mindesthöchststrafe von bis zu zwei Jahren Freiheitsstrafe weicht die Richtlinie in folgenden wesentlichen Punkten von Art. 6 CyCC ab:

- Verpönte Tatwerkzeuge sind nach der Richtlinie Computerprogramme und Zugangsdaten, nicht aber auch andere Vorrichtungen z. B. Hardware-Tools, mit deren Hilfe man die Computerstraftaten begehen könnte.
- Die Pflicht zur Bestrafung greift nach Art. 7 RL 2013/40/EU erst, wenn kein leichter Fall vorliegt, während nach Art. 6 CyCC der Missbrauch der Tatwerkzeuge grundsätzlich strafbar ist; die Vertragsstaaten können aber nach Art. 6 Abs. 3 CyCC weitreichende Vorbehalte erklären.
- Eine Strafbarkeit wegen bloßen Besitzes verpönter Tatwerkzeuge ist in Art. 7 RL 2013/40/EU nicht vorgesehen, während die CyCC auch den Besitz erfasst. Die Vertragsstaaten können die Strafbarkeit allerdings da-

[26] KOM(2010) 517 endg., 4; RL 2013/40/EU, Erwägungsgrund 4.

[27] Die Gründe dafür können dem Vorschlag für den Rahmenbeschluss KOM(2002) 173 endg., ebenso wenig entnommen werden wie den Erwägungsgründen.

von abhängig machen, dass der Täter eine bestimmte Anzahl dieser Tatmittel besitzt.

Auch im Vorfeldbereich baut die RL eindeutig auf der CyCC auf, bleibt aber auf den ersten Blick dahinter zurück. Berücksichtigt man freilich die weitreichende Vorbehaltsmöglichkeit nach Art. 6 CyCC, relativiert sich dieses Bild.

III. Schlussfolgerungen und Ausblick

Insgesamt bestätigt sich der Eindruck, dass die CyCC eine wesentliche Grundlage für den Rahmenbeschluss ebenso wie für die Richtlinie über Angriffe auf Informationssysteme ist. Diese Rechtsakte bauen auf der CyCC auf und gehen teilweise über sie hinaus. Das ist vor allem bei der Richtlinie nicht überraschend, liegen doch einige Jahre technischer Entwicklung zwischen der CyCC und der Richtlinie. Letztere betont auch selbst, dass sogar der Rahmenbeschluss den Fokus noch auf andere kriminelle Phänomene gelegt hat und später auftretende Erscheinungsformen daher nicht in gebotenem Maße berücksichtigen konnte; als Beispiel für neue Herausforderungen nennt die Kommission dabei etwa den Umgang mit Botnetzwerken und den Schutz kritischer Infrastruktur.[28] Im Ergebnis liegt somit allen Rechtsinstrumenten dasselbe abgestimmte Grundkonzept zugrunde. Die nunmehrige Richtlinie etabliert aber unter anderem aufgrund der Berücksichtigung der technischen Weiterentwicklung, vor allem aber auch wegen des weiter ausgebauten Systems der Mindesthöchststrafen ein – regional begrenzt – strengeres Strafrechtsregime innerhalb des Anwendungsbereiches der CyCC.

Größeren Herausforderungen als im materiellen Recht werden wir meines Erachtens aber bei der Entwicklung sinnvoller Ermittlungsmaßnahmen im grenzüberschreitenden Raum gegenüberstehen. Fragen der Beweissicherung in der so genannten Cloud ebenso wie das Einfrieren von Daten zur Beweissicherung oder der Umgang mit verschlüsselter Kommunikation bzw. verschlüsseltem Beweismaterial bedürfen wohl ebenso gemeinsamer internationaler Antworten. Es wäre erfreulich, wenn Europarat und Europäische Union auch im Bereich der Prävention und Verfolgung von Cybercrime, insbesondere auch bei neu auftretenden Gefahren, eine ebenfalls in den wesentlichen Grundzügen abgestimmte Rechtslage erreichen könnten.

[28] KOM(2010) 517 endg., 4; RL 2013/40/EU, Erwägungsgrund 4.