Das deutsche Computerstrafrecht mit seinen europarechtlichen Bezügen

von
Dr. jur. Alexander Koch

Institut für das Recht der Netzwirtschaften,
Informations- und Kommunikationstechnologie

Gang des Vortrags

- Einführung:
  - Warum wir ein Computerstrafrecht brauchen – aber keine neue Dogmatik.
  - Cybercrime Convention.
- Aktuelle Problemstellungen:
  - Pornographie,
  - Identitätstäuschungen im E-Commerce,
  - Phishing,
  - Botnetze,
  - Angriffe auf kritische Infrastrukturen.

Warum wir ein Computerstrafrecht brauchen – aber keine neue Dogmatik

- Strafrecht ist in besonderem Maße auf Klarheit der Vorschriften angewiesen.
- Erscheinungsformen der Kriminalität ändern sich.
- Herausforderung:
  - Können alte Strafvorschriften auf neue Kriminalitätsformen übertragen werden?
  - Müssen neue Strafvorschriften geschaffen werden?

Beispiel: Sachbeschädigung

- „Wer eine Sache beschädigt, wird bestraft.“
- Sachen sind körperlich.
- Nicht erfasst werden also Daten.
- Neue Vorschrift erforderlich.
- Aber: Die Probleme bleiben gleich.
- Wir brauchen keine neue Dogmatik, sondern können auf die Erkenntnisse zur Sachbeschädigung zurückgreifen.

Problem: Wir müssen die Technik verstehen!

- Einbruch in ein Netzwerk.
- Wie hat es der Täter geschafft, die Zugangskontrolle zu überwinden?
  - Wie funktioniert die Zugangskontrolle?
  - Identifikation z. B. über IP-Adresse.
    - Was ist eine IP-Adresse?
- Täter kann beispielsweise seine IP-Adresse manipuliert haben.
- Vergleichbar mit Fälschen eines Ausweises.
- Probleme der Urkundendelikte!

Cybercrime Convention

- Übereinkommen über Computerkriminalität des Europarates (Cybercrime Convention – CCC).
- Mitgliedstaaten des Europarats plus Japan, USA, Kanada und weitere Staaten.
- Am 23.11.2001 unterzeichnet,
- am 1.7.2004 in Kraft getreten,
- am 1.7.2009 in Deutschland in Kraft getreten,
  - Umsetzung in nationales Recht jedenfalls im Kernstrafrecht abgeschlossen.
- Türkei hat die CCC *nicht* unterzeichnet.

Aktuelle Problemstellungen

Pornographie

- Kein spezifisches Computerdelikt, aber Verbreitung und Zugang hat sich vereinfacht.
- Früher: pornographische Schriften.
- Gesetzgeber: Gleichstellung von Datenträgern mit Schriften!

Kinderpornographie

- CCC hat Schutzalter gesenkt.
  - Deutschland bislang 14 Jahre.
  - Jetzt Differenzierung zwischen Kinder- und Jugendpornographie.
- Problem: Besitz-, aber keine Konsumverbote.
  - Nachweisprobleme!
    - Reicht „Besitz“ im Cache?
  - Streaming-Angebote werden derzeit nicht erfasst.

Identitätstäuschungen im E-Commerce

- Urkundenproblematik!
- Situation in Deutschland:
  - Rechtsprechung und Wissenschaft haben ausdifferenzierte Dogmatik der Urkunde entwickelt.
    - Unmittelbare Wahrnehmbarkeit erforderlich (streitig!).
  - Lösung: neuer Tatbestand: Fälschung beweiserheblicher Daten (1986) – hypothetischer Urkundentest.

Identitätstäuschungen im E-Commerce

- Probleme der Praxis: Welche Anforderungen sind an hypothetische Urkunden zu stellen?
  - Ist die leichte Fälschbarkeit ein Problem?
  - Welche Anforderungen sind an die Erkennbarkeit des Ausstellers zu stellen?
    - „Digitale Signatur“ erforderlich?
  - Strikte Übertragung der herkömmlichen Urkundendogmatik vermeidet Scheinprobleme!
- CCC: Strafbarkeit „Computerbezogene Fälschung“.

Phishing

- Vorbereitung: Fälschen von E-Mails und Nachbauen von WWW-Seiten.
  - Urkundendelikte!
- Eigentliche Tathandlung 1: Erschleichen von Zugangsdaten zu Bankkonten.
  - Betrug?
    - Rechtsprechung und Lehre in Deutschland haben Problem.
    - Muss der Schaden unmittelbar der Vermögensverfügung folgen?
    - Liegt schon ein Schaden vor, wenn Zugangsdaten nur „gestohlen“ wurden?

Phishing

- Eigentliche Tathandlung 2: Abheben von Geld.
  - Computerbetrug bei der unbefugten Verwendung von Daten.
    - Der Bankcomputer „irrt“ über die Verfügungsberechtigung.
    - Erfasst werden – wohl – auch hochkomplexe Man-in-the-Middle-Angriffe.
- Nachtat: Verschleiern des Geldflusses über „Finanzagenten“.
  - Geldwäsche – typisches Delikt der organisierten Kriminalität.
- CCC:
  - Computerbezogene Fälschung und computerbezogener Betrug als Zentralnormen.

Botnetze

- Mariposa-Netz soll über ca. 13.000.000 Bots verfügen.
- Srizbi-Netz soll über 60.000.000.000 Spam-Mails am Tag verschicken.
- Organisierte Kriminalität.
- Botnetze werden vermietet.
  - Einschließlich einfach zu bedienender Frontends ...

Botnetze

- Eindringen in fremde Systeme.
  - Deutschland:
    - Ausspähen von *Daten.*
    - Überwinden einer Zugangssicherung erforderlich.
    - Lücke: Wenn kein Zugang zu Daten erstrebt!
      - Historisch: Früher nur Verschaffen von Daten strafbar.
  - CCC:
    - Rechtswidriger Zugang zu einem *Computersystem.*
    - Optional unter Verletzung eines Sicherheitssystems.

Botnetze

- Missbrauch fremder Systeme.
  - Erschleichen von Leistungen?
    - Norm, um Anzapfen von öffentlichen Telefonnetzen zu sanktionieren.
    - Erfasst keine privaten Systeme (hat aber etwa Phreaking erfasst)!
- Angriffe auf andere Systeme.
  - Computersabotage.
  - Unbrauchbarmachen einer Datenverarbeitungsanlage – etwa durch DDoS-Angriff?
  - Probleme der Sachbeschädigung!
    - Ist ein Auto beschädigt, wenn die Reifen abmontiert werden?

Botnetze

- Vorfeld: Vorbereitung durch Herstellen oder Verschaffen von „Angriffssoftware“.
  - Deutschland und CCC: Herstellen, Verschaffen von Programmen zur Begehung bestimmter Straftaten ist strafbar.
  - Probleme:
    - Was ist Angriffssoftware?
      - Programm zum Aufspüren von Systemlücken?
      - Programme zum Erstellen von Computerviren?
    - Massive Verunsicherung in der Computersicherheitsszene.

Botnetze

- Probleme jenseits des Strafrechts:
  - Botnetze setzen ungesicherte Systeme voraus – wie kann man die Benutzer für die Problematik sensibilisieren?
  - Welche Möglichkeiten hat der Staat / haben die Internetprovider, um Botnetze aufzuspüren?
  - Täter sind hochmobil – Probleme der internationalen Zusammenarbeit.
  - Wie können wir unsere kritischen Infrastrukturen vor Angriffen schützen?
    - Entkoppeln vom Internet ...

Angriffe auf kritische Infrastrukturen

- Strafrecht:
  - Datenveränderung, Computersabotage.
  - Spionage, Sachbeschädigung, Körperverletzung, Mord ...
- Rahmenbeschluss der EU über Angriffe auf Informationssysteme.
  - Erfasst alle Formen des klassischen Hackens.
  - Erfasst aber auch moderne Erscheinungen wie DDoS-Angriffe.

Angriffe auf kritische Infrastrukturen

- Kriegsvölkerrecht:
  - Wann liegt ein bewaffneter Angriff nach Art. 51 UN-Charta vor?
  - Wie erkennt man, wer überhaupt der Angreifer ist?
  - Wann sind Angriffe von Privaten einem Staat zuzurechnen?

Fazit

- Das aktuelle europäische und deutsche Computerstrafrecht erfassen (fast) alle aktuellen Formen von Computerstraftaten.
- These: Neue Erscheinungsformen erfordern nicht unbedingt ein Umdenken in der Rechtswissenschaft – wohl aber ein Verständnis der Technik.

Vielen Dank für die Aufmerksamkeit!

Für weitere Informationen:

IRNIK
Dr. jur. Alexander Koch
Postfach 15 01 61
53040 Bonn
DEUTSCHLAND
Tel.: +49-2 28-8 50 86 63
Fax: +49-2 28-8 50 86 62
ak@irnik.de
http://www.irnik.de

IRNIK

Institut für das Recht der Netzwirtschaften,
Informations- und Kommunikationstechnologie