Die rechtlichen Rahmenbedingungen von Hackback

Dr. Alexander Koch
Institut für das Recht der Netzwirtschaften,
Informations- und Kommunikationstechnologie

Gang des Vortrages

- Schnellkurs Jura.
- Vorstellung der einschlägigen Straftatbestände.
- Straf- und zivilrechtliche Rechtfertigung von Verteidigungsmaßnahmen.
- Verteidigungsmaßnahmen durch staatliche Stellen.
- Irrtumsproblematik.
- Kriegsvölkerrecht.

IRNIK
Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie

Schnellkurs Jura

IRNIK
Institut für das Recht der Netzwirtschaften,
Informations- und Kommunikationstechnologie

Warnungen!

- Es gibt keine juristischen Wahrheiten.
  - „Zwei Juristen, drei Meinungen.“
- Gerichte entscheiden anders als man denkt.
  - „Auf hoher See und vor Gericht ist man in Gottes Hand allein.“
- Juristen legen sich nicht fest.
  - Standardantwort: „Es kommt darauf an.“

Tatbestand / Rechtswidrigkeit / Schuld

- Ein Verhalten erfüllt den Tatbestand, wenn es den im Gesetz beschriebenen Voraussetzungen genügt.
- Eine Tat ist gerechtfertigt, wenn ein Rechtfertigungsgrund eingreift.
- Eine Tat ist schuldhaft begangen, wenn dem Täter ein Vorwurf gemacht werden kann.
- Strafbarkeit setzt Tatbestand, Rechtswidrigkeit und Schuld voraus.

- „Wer einen Menschen tötet, wird bestraft."
- „Wenn Du angegriffen wirst, darfst Du zur Verteidigung diesen Menschen töten."
- „Du wirst nicht bestraft, wenn Du Dich aus Furcht heftiger verteidigst, als Du eigentlich dürftest, und dabei einen Menschen tötest."

Tatbestand / Rechtswidrigkeit / Schuld

- § 212 StGB, Totschlag
  (1) Wer einen Menschen tötet, ohne Mörder zu sein, wird als Totschläger mit Freiheitsstrafe nicht unter fünf Jahren bestraft.
  ...

- § 32 StGB, Notwehr
  (1) Wer eine Tat begeht, die durch Notwehr geboten ist, handelt nicht rechtswidrig.
  ...

- § 33 StGB, Überschreitung der Notwehr
  Überschreitet der Täter die Grenzen der Notwehr aus Verwirrung, Furcht oder Schrecken, so wird er nicht bestraft.

Vorsatz und Fahrlässigkeit

- Grundsätzlich ist nur vorsätzliches Verhalten strafbar.
- Vorsatz bedeutet, dass der Täter weiß, was er tut und dennoch willentlich handelt.
- Bsp.: Bewusstes Hacken eines fremden Rechners.

- Fahrlässigkeit ist nur strafbar, wenn es im Gesetz ausdrücklich angeordnet wird.
- Fahrlässig verhält sich, wer nicht sorgfältig ist und hierdurch einen anderen schädigt.
- Bsp.: Fehlerhafte Administration eines Rechners, die zu einem Wurmbefall führt, durch die ein Dritter geschädigt wird.

Vollendung und Versuch

- Viele Delikte sind nur strafbar, wenn sie erfolgreich begangen wurden.
- Der Versuch ist nur in Ausnahmefällen strafbar.
- Vorbereitungshandlungen sind grundsätzlich (d.h. nicht immer!) straffrei.
  - Eine wichtige Ausnahme ist § 202c StGB!

Strafbares und verbotenes Verhalten

- Strafrecht ist ultima ratio.
- Viele Verhaltensweisen sind zwar verboten (z.B. Vertragsbruch), aber nicht strafbar.
- Aus einer fehlenden Strafbarkeit kann also nicht auf ein Erlaubtsein geschlossen werden.
- Bsp.: Bestimmte Formen von DoS-Angriffen sind zwar nicht strafbar, aber dennoch rechtswidrig.

Strafrecht und Polizeirecht

Strafrecht und Polizeirecht haben unterschiedliche Funktionen:

Strafrecht

- Nachträgliche Sanktionierung eines Verhaltens.
- Konsequenz: Es muss eine Tat vorliegen, bevor bestraft werden kann.
- Bsp.: Keine Strafbarkeit des Einbrechers, der auf dem Weg zum Tatort ist.

Polizeirecht

- Präventives Verhindern von Rechtsgut-verletzungen.
- Konsequenz: Polizei kann im Vorfeld von Straftaten einschreiten.
- Bsp.: Einbrecher festnehmen, der auf dem Weg zum Tatort ist.

IRNIK
Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie

IT-Strafrecht

IRNIK
Institut für das Recht der Netzwirtschaften,
Informations- und Kommunikationstechnologie

IT-Strafrecht

- § 202a Ausspähen von Daten
  - „Virtueller Hausfriedensbruch“.
  - Zugangskontrollsystem muss überwunden werden.
- § 202b Abfangen von Daten
  - Sniffing, Van-Eck-Phreaking (diskrete Abstrahlung).
  - Der nicht gerechtfertigte (Einwilligung!) Einsatz von IDS-Systemen kann erfasst sein.

IT-Strafrecht

- § 202c Vorbereiten des Ausspähens und Abfangens von Daten „Hacker-Paragraph
  - Programmieren und Verbreiten von „Hackerwerkzeugen“.
  - Gesetzgeberische Intention: Vertrieb von Viren, Würmern & Trojanern sowie Angriffssoftware sollte unterbunden werden.
  - Problem: Dual-use-Software: Schwachstellenscanner kann eingesetzt werden, um in ein fremdes System einzubrechen oder um das eigene System zu prüfen.
  - Grenzen noch völlig offen.
    - StA Bonn hat aber kein Verfahren gegen BSI-Verantwortliche eingeleitet.

IT-Strafrecht

- § 206 Verletzung des Post- oder Fernmeldegeheimnisses
  - Täter können nur Inhaber oder Beschäftigte von geschäftsmäßigen TK-Dienstleistern sein.
  - Abs. 1 erfasst nur das Mitteilungmachen.
  - Abs. 2 erfasst auch das „Unterdrücken“ von Sendungen - Vorsicht bei SPAM-Bekämpfung ohne Einwilligung.

IT-Strafrecht

- § 263a Computerbetrug
  - Auch Computer können durch Täuschung zu einem „Irrtum“ verleitet werden.
  - Verwendung von Kontodaten beim Phishing.
- § 265a Erschleichen von Leistungen
  - Geschützt werden nur „öffentliche Telefonnetze“, nicht erfasst ist also die Verwendung eines fremden (eroberten) Rechners.

IT-Strafrecht

- § 268 Fälschung technischer Aufzeichnungen
  - Zugeschnitten auf mechanische Aufzeichnungen.
  - Eine „abtrennbare“ Aufzeichnung wird verlangt – Logfiles werden also nicht erfasst (andere Sichtweise aber durchaus möglich!).

IT-Strafrecht

- § 269 Fälschung beweiserheblicher Daten
  - Fälschung „hypothetischer“ elektronischer Urkunden. Geschützt werden nur menschliche Gedankenerklärungen – etwa elektronisch gespeicherte Verträge, aber auch E-Mails.
  - Bislang keine besondere praktische Bedeutung.
  - Aber: Spam und Phishing mit gefälschten Absenderkennungen lassen sich erfassen.

IT-Strafrecht

- § 303a Datenveränderung („virtuelle“ Sachbeschädigung)
  - Der „echten“ Sachbeschädigung nachgebildet.
  - Erfasst wird „Vandalismus“ auf gehackten Systemen;
  - aber auch Veränderungen / Manipulationen durch Viren, Würmer & Trojaner.

IT-Strafrecht

- § 303b Computersabotage
  - „Besonders schlimme“ Datenveränderung.
  - Erfasst werden die meisten Formen von (D)DOS-Angriffen.
- § 89 i.V.m. § 148 TKG (Abhörverbot)
  - Erfasst möglicherweise auch die Nutzung offener WLAN.

Verteidigung

IRNIK

Institut für das Recht der Netzwirtschaften,
Informations- und Kommunikationstechnologie

Verteidigung

- Der Verteidiger nutzt die gleichen Techniken wie ein Angreifer.
- Verteidigung erfüllt die gleichen Tatbestände wie Angriffe.
- Verteidigung unterscheidet sich juristisch nur auf der Rechtfertigungsebene von Angriffen.

Notwehr und Notstand

§ 32 StGB, Notwehr

(1) Wer eine Tat begeht, die durch Notwehr geboten ist, handelt nicht rechtswidrig.

(2) Notwehr ist die Verteidigung, die **erforderlich** ist, um einen **gegenwärtigen** rechtswidrigen **Angriff** von sich oder einem anderen abzuwenden.

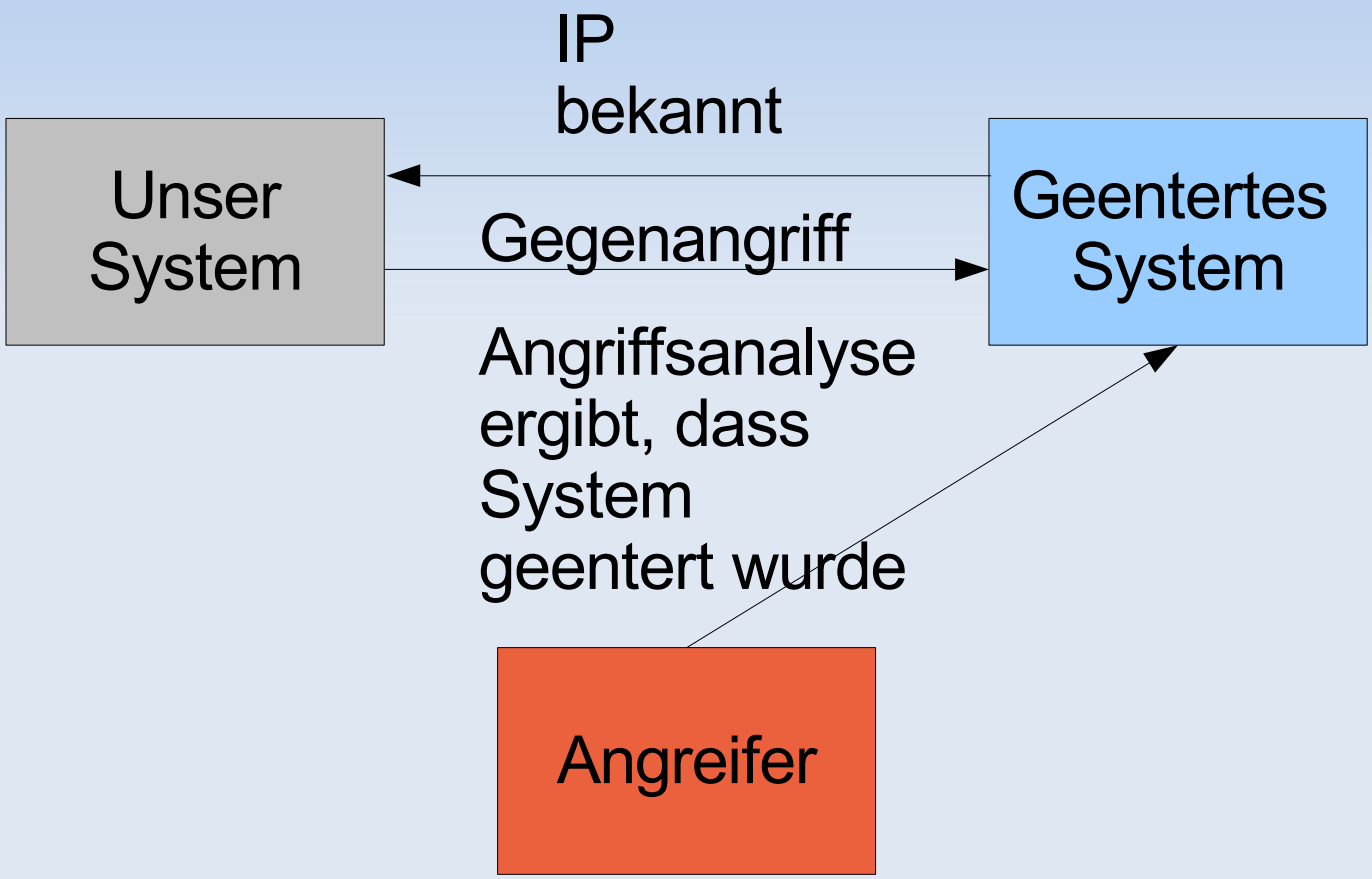
§ 34 StGB, Notstand

Wer in einer **gegenwärtigen**, nicht anders abwendbaren **Gefahr** für Leben, Leib, Freiheit, Ehre, Eigentum oder ein anderes Rechtsgut eine Tat begeht, um die Gefahr von sich oder einem anderen abzuwenden, handelt nicht rechtswidrig, wenn bei **Abwägung der widerstreitenden Interessen**, namentlich der betroffenen Rechtsgüter und des Grades der ihnen drohenden Gefahren, das geschützte Interesse das beeinträchtigte wesentlich überwiegt. Dies gilt jedoch nur, soweit die Tat ein angemessenes Mittel ist, die Gefahr abzuwenden.

Notwehr und Notstand

	Notwehr	Notstand
Voraussetzung	Gegenwärtiger rechtswidriger Angriff.	Gegenwärtige Gefahr.
zeitliche Dimension	Angriff muss stattfinden.	Gefahr muss drohen, Abwehrmaßnahmen also schon im Vorfeld eines Angriffs / Verhinderung künftiger Angriffe.
Verteidigung	Jedes erforderliche Verteidigungsmittel ist erlaubt, zunächst keine Rücksicht auf den Angreifer.	Zulässige Verteidigung ist einer umfassenden Güterabwägung unterworfen.
Gegner	Nur gegen Angreifer und seine Rechtsgüter.	Gegen Beteiligte und Unbeteiligte.

Beispiel: Verteidigung gegen ein geentertes System



IRNIK
Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie

Notwehr und Notstand im Beispiel

	Notwehr	Notstand
Voraussetzung	Gegenwärtiger rechtswidriger Angriff.	Gegenwärtige Gefahr.
zeitliche Dimension	Angriff muss stattfinden.	Gefahr muss drohen, Abwehrmaßnahmen also schon im Vorfeld eines Angriffs / Verhinderung künftiger Angriffe.
Gegner	Nur gegen Angreifer und seine Rechtsgüter.	Gegen Beteiligte und Unbeteiligte.

Hier: Verteidigung nach Notstandsrecht.

IRNIK
Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie

Notwehr und Notstand

- Häufig scheitert Notwehr, weil der Angriff nicht mehr (oder noch nicht) gegenwärtig ist.
- Häufig scheitert Notwehr, weil eine fremde Sache für den Angriff verwendet wird (geenterter Rechner).
- In diesen Fällen ist häufig eine ***Notstand***slage gegeben.

IRNIK
Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie

Nothilfe

- Notwehr- und Notstandshilfe ist auch zugunsten von Dritten möglich.
- Vorsicht: Ob Nothilfe erlaubt ist, richtet sich allein nach dem Willen des Opfers:
  - Es kann durchaus sinnvoll sein, einen Angriff auszusitzen.
  - Auch irrationale Entscheidungen sind zu respektieren.
- Keine aufgedrängte Nothilfe!

Notwehr- / Notstandsfähige Rechtsgüter

- ***Jedes*** rechtlich geschützte Interesse des Verteidigers oder bei Nothilfe des Opfers.
  - Also auch: „virtuelles Hausrecht“.
- Problem: Staatliche Güter.
  - Fiskus (z.B. staatliches Netzwerk). (+)
  - Überindividuelle Rechtsgüter (z.B. Angriff auf Seite mit pornographischem Inhalt). (-)
  - Notwehr und Notstand ermächtigen nicht dazu, Hilfspolizei zu spielen!

Zeitliche Dimension

Portscann

System-anayse

Einbruch über Schwachstelle

Angreifer verlässt System

Gegenangriff auf vermittelndes System

Verfolgung um neuen Angriff zu verhindern

Notstand?

Notstand

Notwehr

Notstand, weil gegen Dritten

Notstand

Notstand?

IRNIK

Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie

Verteidigungshandlung

Notwehr

- Geeignetheit
- Erforderlichkeit
- (Gebotenheit)

Notstand

- Geeignetheit
- Erforderlichkeit
- Güterabwägung
- (Angemessenheit)

IRNIK
Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie

Geeignetheit

- Grundsätzlich keine hohen Anforderungen.
- Verteidigung darf sich bei mehreren Angreifern auch gegen einzelne Täter richten.

Erforderlichkeit

- Es muss das mildeste zur Verfügung stehende Abwehrmittel gewählt werden.
- Soweit möglich, muss ein „Warnschuss“ abgegeben werden.

Einzelprobleme

- Vorweggenommene Verteidigung („Selbstschussanlagen“)?
  - Irrtumsrisiko!
- Ermittlung der Täteridentität?
  - Regelmäßig nicht geeignet, um den Angriff zu beenden.
- Ausweichen?
  - Notwehr: Ausweichen ist keine Verteidigung.
  - Notstand: Ausweichen kann mildestes Abwehrmittel sein.

Einzelprobleme

- Löschen von Daten?
  - Immer beachten, ob hierdurch tatsächlich der Angriff beendet werden kann.
  - Keine Rache!
- Einrichten eines eigenen Zugangs?
  - Notwehr: Nie geeignet, den Angriff zu beenden.
  - Notstand: Es kommt darauf an.

Güterabwägung

- Rangfolge der Rechtsgüter.
- Ausmaß der Schädigung.
- Schadenswahrscheinlichkeit.
- Ursprung der Gefahr.

Praxistipp Notwehr und Notstand

- Immer das mildeste Mittel wählen.
- Immer nach Notstandsregel verteidigen: Also immer Güterabwägung durchführen.
- Lieber ausweichen als angreifen.

IRNIK
Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie

Staatliche Verteidigung (unterhalb des Völkerrechts!)

IRNIK
Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie

Kann sich der Staat auf die straf- und zivilrechtlichen Rechtfertigungsgründe berufen?

- Gesetzesvorbehalt
  - Jedes belastende staatliche Verhalten bedarf einer ausdrücklichen Ermächtigungsgrundlage.
- Bestimmtheitsgebot
  - Gesetze müssen so bestimmt sein, dass der Bürger klar erkennen kann, was ihn erwartet.
- Verhältnismäßigkeitsgrundsatz
  - Jedes staatliche Handeln muss verhältnismäßig sein.
- Systematische Überlegungen
  - Weite Teile des Polizei- und Ordnungsrechts wären überflüssig.

→ Der Staat kann sich **nicht** auf die allgemeinen Rechtfertigungsgründe berufen.

Ermächtigungsgrundlagen für Verteidigung

- Unterscheidung zwischen Aufgabenzuweisung und Befugnis
  - Aufgabenzuweisung: Kompetenzbereich der Behörde; hieraus folgt noch nicht:
  - Befugnis: Bei Grundrechtseingriffen muss ausdrücklich geregelt sein, welche Befugnisse die Behörde haben soll.

Bundespolizeigesetz

Aufgabenzuweisung
§ 4 Luftsicherheit
Der Bundespolizei obliegt der **Schutz vor Angriffen** auf die Sicherheit des Luftverkehrs ...

Befugnis
§ 22 Befragung und Auskunftspflicht
(1) Die Bundespolizei kann eine Person **befragen** ... Zum Zwecke der Befragung kann die Person **angehalten** werden. Auf Verlangen hat die Person mitgeführte Ausweispapiere zur Prüfung **auszuhändigen**.

Für Verteidigung ermächtigte Behörde

- Bundespolizei (-)
- Bundeskriminalamt (-)
- Bundesamt für Verfassungsschutz (-)
- Bundesnachrichtendienst (-)
- Bundesamt für Sicherheit in der Informationstechnik (-)
- Bundeswehr (-)

→ Es fehlt jeweils an einer Aufgabenzuweisung oder einer Ermächtigungsgrundlage.

Für Verteidigung ermächtigte Behörde

Allgemeine Polizei- und Ordnungsbehörden

- Aufgabenzuweisung: Gefahrenabwehr
- Befugnis:
  - Keine spezielle Befugnis (sog. Standardmaßnahme).
  - Aber: Generalklausel: „Erforderliche Maßnahmen“.

§ 1 Abs. 1 Hessisches Gesetz über die öffentliche Sicherheit und Ordnung

Die Gefahrenabwehrbehörden [...] und die Polizeibehörden haben die gemeinsame **Aufgabe der Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung** [...]

§ 11 HSOG (Generalklausel)

Die Gefahrenabwehr- und die Polizeibehörden **können die erforderlichen Maßnahmen treffen**, um eine im einzelnen Falle bestehende Gefahr für die öffentliche Sicherheit oder Ordnung (Gefahr) abzuwehren, soweit nicht die folgenden Vorschriften die Befugnisse der Gefahrenabwehr- und der Polizeibehörden besonders regeln.

IRNIK
Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie

Folgen „illegaler“ Verteidigung

- Staatshaftungsrecht.
  - Schadensersatzpflicht.
- Strafrechtliche Folgen für den Beamten.
- Disziplinarrechtliche Folgen für den Beamten.

Strafrechtliche Folgen „illegaler“ Verteidigung

Gelten die strafrechtlichen Rechtfertigungs-normen auch für Beamte persönlich?

Nein

- Umgehung der öffentlich-rechtlichen Regelungen.
- Überlagerung durch spezialgesetzliche Regelungen.

Ja

- Wortlaut von §§ 32, 34 StGB.
- Landesgesetzgeber kann Bundesrecht nicht modifizieren.

Trotzdem: VORSICHT!
(2 Juristen, 3 Meinungen...)

IRNIK
Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie

Disziplinarrechtliche Folgen „illegaler“ Verteidigung

- Disziplinarrechtlicher Überhang.
- Normalerweise laufen Straf- und Disziplinarrecht parallel.
- Hier: Öffentliches Recht verbietet ein strafrechtlich erlaubtes Verhalten.

§ 14 Abs. 2 Bundesdisziplinargesetz
Ist der Beamte im Straf- oder Bußgeldverfahren rechtskräftig freigesprochen worden, darf wegen des Sachverhalts, der Gegenstand der gerichtlichen Entscheidung gewesen ist, eine **Disziplinar-maßnahme nur** ausgesprochen werden, wenn dieser Sachverhalt **ein Dienstvergehen darstellt, ohne den Tatbestand einer Straf- oder Bußgeldvorschrift zu erfüllen.**

Das heißt im ungünstigsten Fall: Freispruch und trotzdem Job und Pension los!

IRNIK
Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie

Irrtumsproblematik

IRNIK

Institut für das Recht der Netzwirtschaften,
Informations- und Kommunikationstechnologie

Problem der maßgeblichen Perspektive

- Strafrecht:
  - Notwehr: Perspektive eines allwissenden Beobachters.
  - Notstand:
    - Gefahrrelevante Umstände: objektiv.
    - Prognose: subjektiv.
- Zivilrecht:
  - Grundsätzlich: Perspektive eines allwissenden Beobachters.

Irrtum

- Erlaubnistatbestandsirrtum:
  - Irrtum über die sachlichen Voraussetzungen eines Rechtfertigungsgrundes.
  - Bsp.: Verteidigung richtet sich gegen ein falsches System.
  - Rechtsfolge: Keine Strafbarkeit wegen eines Vorsatzdelikts.
- Erlaubnisirrtum:
  - Täter verkennt die rechtlichen Grenzen eines Rechtfertigungsgrundes oder glaubt an einen der Rechtsordnung unbekannten Rechtfertigungsgrund.
  - Bsp.: Täter meint auch im Notstand sei jedes Verteidigungsmittel erlaubt.
  - Bsp.: Täter wägt falsch ab.
  - Rechtsfolge: Strafmilderung.

Folgen eines Irrtums

- Strafrecht:
  - Erlaubnistatbestandsirrtum: Praktisch folgenlos.
  - Erlaubnisirrtum: Regelmäßig vermeidbar, nur Strafmilderung.
  - Salopp: Geld- oder Bewährungsstrafe ist wegzustecken.
- Zivilrecht
  - **Grundsätzlich volle Schadensersatzpflicht!**
  - Salopp: Der Schadensersatz frisst das Haus und die Pension!

Exkurs: Staatenübergreifende Angriffe oder Verteidigungen

IRNIK
Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie

Exkurs: Staatenübergreifende Angriffe oder Verteidigungen

Deutsche Rechtslage:

- Handlungs- / Unterlassensort.
- Erfolgsort.
- Erfasst werden:
  - Angriffe aus Deutschland.
  - Angriffe auf Rechner in Deutschland.

§ 9 StGB Ort der Tat

(1) Eine Tat ist an jedem Ort begangen, an dem der Täter **gehandelt** hat oder im Falle des Unterlassens **hätte handeln müssen** oder an dem der zum Tatbestand gehörende **Erfolg** eingetreten ist oder nach der Vorstellung des Täters eintreten sollte.

(2) ...

In anderen Ländern vergleichbare Regelungen!

Fallstricke im internationalen Recht

§ 32 StGB-D, Notwehr

(1) Wer eine Tat begeht, die durch Notwehr geboten ist, handelt nicht rechtswidrig.

(2) Notwehr ist die Verteidigung, die erforderlich ist, um einen gegenwärtigen rechtswidrigen Angriff von sich oder einem anderen abzuwenden.

Art. 33 StGB-CH, Notwehr

Wird jemand ohne Recht angegriffen oder unmittelbar mit einem Angriffe bedroht, so ist der Angegriffene und jeder andere berechtigt, den Angriff in einer den Umständen **angemessenen Weise** abzuwehren.

...

Schneidige Notwehrverteidigung ist in Deutschland erlaubt und kann in der Schweiz (als nicht gerechtfertigte Tat) strafbar sein.

IRNIK
Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie

Exkurs: Staatenübergreifende Angriffe oder Verteidigungen

- Im Ausland mögen andere Vorstellungen über die Voraussetzungen der Rechtfertigung existieren.
- Das Strafmaß kann extrem unterschiedlich sein.
- Schadensersatzforderungen können die deutschen „Sätze“ weit übersteigen.

Finger weg!

IRNIK
Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie

Kriegsvölkerrecht

IRNIK

Institut für das Recht der Netzwirtschaften,
Informations- und Kommunikationstechnologie

Ius ad bellum

IRNIK
Institut für das Recht der Netzwirtschaften,
Informations- und Kommunikationstechnologie

Gewaltverbot und Recht zum Krieg

- Anders als in früheren Zeiten gilt heute im Völkerrecht ein Gewaltverbot.
  - Art. 2 Nr. 4 UN-Charta: „Alle Mitglieder unterlassen ... [die] Androhung oder Anwendung von ***Gewalt***."
- Gewalt darf nur aufgrund eines UNO-Mandats angewendet werden.
- Ausnahme: Art. 51 UN-Charta.
  - „Diese Charta beeinträchtigt im Falle eines ***bewaffneten Angriffs*** ... keineswegs das naturgegebene Recht zur individuellen oder kollektiven Selbstverteidigung, ..."

IRNIK
Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie

Ius ad bellum

- „Gewalt“ in Art. 2 Nr. 4 UN-Charta meint „Waffengewalt“ oder „militärische Gewalt“.
- Es gibt im Völkerrecht keine verbindliche Definition des „bewaffneten Angriffs“.
- Resolution 3314 (XXIX) versucht, „Aggression“ zu definieren.
  - Z.B. Invasion, Bombardierung, Seeblockaden.
  - Aufzählung ist nicht abschließend.

Angriff mit Computerwaffen als Aggression

- Wortlautgrenzen:
  - Kann ein Programm eine „Waffe“ sein?
- Historischer Hintergrund:
  - Normen sind zugeschnitten auf herkömmliche Art der Kriegsführung durch unmittelbare physische Einwirkung.
- Telos:
  - Es macht keinen Unterschied, ob Kraftwerke bombardiert werden oder ein Virus das Stromnetz eines Landes ausschaltet.

Zurechenbarkeit von Computerangriffen

- Staatlicher Angriff ./. Störfall.
  - Stromausfälle an der Ostküste der USA im Jahr 2003 .
- Staatlicher Angriff ./. private Hacker.
  - „Russland“ ./. Estland im Frühjahr 2007.
  - Staaten sind nur ausnahmsweise für Handlungen Privater verantwortlich.
    - Aber: Krieg gegen die Taliban und Al-Qaida in Afghanistan.

lus in bello

IRNIK

Institut für das Recht der Netzwirtschaften,
Informations- und Kommunikationstechnologie

Militärische Notwendigkeit ./. zivile Ziele

- Grundsätzlich dürfen nur militärische Ziele angegriffen werden ...
- ... aber viele potentielle Ziele werden militärisch und zivil genutzt.
  - Amerikanisches Militär nutzt für 95% seiner Kommunikation private Netze.
- TK-Einrichtungen stellen – vermutlich – ein legitimes Ziel dar.

Nichtdiskriminierende Waffen

- Das Kriegsvölkerrecht verbietet nichtdiskriminierende Waffen:
  - Waffen, die keinen Unterschied zwischen militärischen und zivilen Zielen machen können.
- Fallen Viren, Würmer und Trojaner unter dieses Verbot?

Umgang mit Kombattanten

- Kombattanten müssen erkennbar sein.
- Sie genießen dafür aber einen besonderen Schutz.
  - Keine persönliche Verantwortung für militärisches Verhalten.
- Wer ist Kombattant bei einem Computerangriff?

Verbot der Heimtücke

- Das Kriegsvölkerrecht verbietet bestimmte Formen der Heimtücke.
  - Missbrauch der Zeichen des Gegners oder von Schutzzeichen.
- Fallen bestimmte Formen des Spoofings unter das Heimtückeverbot?

Neutralität

- Angriffe über Computernetzwerke können die Netze neutraler Staaten betreffen.
- Müssen neutrale Staaten eine solche Nutzung verhindern?
  - Völkerrecht fordert nicht die Sperrung von Kommunikationswegen für die Kriegsparteien.
  - Ist das zeitgemäß?
    - Nutzung von Netzwerken für Angriffe ist vergleichbar mit dem Durchmarsch einer Armee.
    - Wie soll die militärische Nutzung verhindert werden? - Nationale Firewalls?

IRNIK
Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie

Vielen Dank für die Aufmerksamkeit!

Für weitere Informationen:

IRNIK
Dr. Alexander Koch
Postfach 15 01 61
53040 Bonn
Tel.: 02 28 / 8 50 86 63
Fax: 02 28 / 8 50 86 62
ak@irnik.de
http://www.irnik.de

IRNIK

Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie