Cyberfahnder-Newsletter 8 vom 10.10.2011

IuK-Strafrecht

Die Bestandsaufnahme von 4 ½ Jahren Cyberfahnder ist abgeschlossen. Im Mai 2010 erschien das Arbeitspapier ▸ Cybercrime, im Februar 2011 das über die ▸ Eskalationen und im April 2011 die letzte Aktualisierung wegen des ▸ Skimmings. Die ▸ Entwicklungsgeschichte der Arbeitspapiere im Cyberfahnder ist jetzt abgeschlossen. Ende Juli 2011 erschien das Arbeitspapier über die ▸ verdeckten Ermittlungen im Internet jetzt das über das ▸ IuK-Strafrecht als solches.

Fast zwei Monate lang hat sich auf der Webseite des Cyberfahnders nichts getan, weil ich das Projekt unterschätzt hatte. Ich wollte nur ein paar Erscheinungsformen und Aspekte der aktuellen Cyberkriminalität darstellen und die Lösungen beschreiben, die die Rechtsprechung dazu entwickelt hat. Nichts Großes also. Daraus geworden ist Anfang Oktober 2011 das Arbeitspapier:

▸ Dieter **Kochheim**, IuK-Strafrecht, 08.10.2011

Das Werk hat knapp 120 Seiten, rund 1,9 MB Größe, diversen Grafiken und nur einige wenige große Selbstzitate.

IuK-Strafrecht

Unter formellen Gesichtspunkten lässt sich das Cybercrime-Strafrecht ganz einfach auf kleine vernetzte Systeme herunter brechen und nach dem IuK-Strafrecht im engeren und weiteren Sinne unterscheiden. Das eine betrifft die IuK-Technik als solche und das andere den ganzen Missbrauch, den man mit ihr bei der Begehung gewohnter Straftaten anstellen kann.

Das engere IuK-Strafrecht ist das Terrain der Hacker und Schmarotzer, an denen der Gesetzgeber sich orientiert hat, als er es schuf.

Die wesentlichen Erscheinungsformen der heutigen Cybercrime sind aber auf Beute in klingender Münze aus. Ihre wichtigsten Erscheinungsformen sind autonome Homebanking-Trojaner, Botnetze und Boards, in denen Straftaten vorbereitet und abgesprochen und schließlich die Beutesicherung organisiert werden. Den Rahmen dafür liefern die Board-Betreiber und die Schurkenprovider, die die nötige Anonymität herstellen.

Meine Studien haben mir gezeigt, dass ich zunächst die Erscheinungsformen in ihrem Gesamtplan, ihrem Vorgehen und ihrer Technik begreifen muss – jedenfalls in ihren wesentlichen Grundzügen, um sie dann materiell-strafrechtlich bewerten zu können. Das Arbeitspapier kann angesichts der vielen Varianten nur einen Überblick und einen groben Rahmen bilden. Dennoch ist es mir gelungen, die meisten Ausformungen zu beschreiben und so zu bewerten, dass in vielen Fällen schon in einem ganz frühen Stadium eine Strafbarkeit begründet werden kann (und muss), die sich aus dem finalen Ziel der Täter ableitet und bereits im Vorbereitungsstadium greift.

Ich erwarte Wiederworte und kritische Diskussionen und behaupte nicht, dass ich die endgültige Wahrheit gepachtet habe. Etwas Anstrengung erwarte ich schon, weil meine Argumentation einigen Aufwand abverlangt hat, und ein wenig Anerkennung, weil ich diverse Neuländer betreten habe.

Neuland habe ich auch mit dem Arbeitspapier über die verdeckten Ermittlungen im Internet betreten. Es wurde inzwischen rund 1.500 Mal abgerufen und nur wenige Interessenten haben sich bei mir mit kritischen Anmerkungen gemeldet. Eine davon schlummert noch im Gästebuch und verdient meiner Beachtung. Dazu bin ich noch nicht gekommen. Sorry!

Ende des Cyberfahnders?

Man soll aufhören, wenn es am Schönsten ist.

Dazu wäre jetzt der richtige Zeitpunkt, weil ich den Eindruck habe, dass ich alle wesentlichen Aspekte der Cybercrime beschrieben und bewertet habe.

Darauf könnten andere aufbauen. Ich sehe aber kaum andere, die das könnten und noch weniger, die das wollten. Einer davon ist gerade gestorben, was mich tief getroffen hat.

Ich weiß also selber nicht, wie es mit dem Cyberfahnder weiter gehen wird.

Ihr Dieter Kochheim, der Cyberfahnder.