CYBER-CRIME

Neue Bedrohungs-Szenarien in der Kriminalpolitik

Werner Rüther

An das Internet knüpfen sich mannigfaltige Erwartungen. Die einen sehen darin ein interaktives Massenmedium, das die (welt-)gesellschaftlichen Kommunikationsstrukturen revolutioniert und das nicht nur ein besonderes ökonomisches, sondern auch ein enormes demokratisches und freiheitliches Potenzial besitzt, wozu wie selbstverständlich auch neuartige Risiken und Gefährdungen krimineller Art gehören, für die sich auf der internationalen Bühne immer mehr der Begriff der ›cyber-crimes‹[1] durchzusetzen beginnt. Daraus ergeben sich Anforderungen an (welt-)gesellschaftliche Kontrollstrategien, Herausforderungen für neue und globale kriminologische und kriminalpolitische Denk- und Vorgehensweisen. Dabei kann zum Teil auf bekannte Erkenntnisse aus nationalen Kontroll-Diskursen zurückgegriffen werden.

Am 22.5.2001 fand im ›Internationalen Kongress-Zentrum Bundeshaus Bonn‹ (im ehemaligen Plenarsaal des Deutschen Bundestages) der 4. Europäische Polizeikongress zum Thema ›Elektronische Kriminalität‹ (oder neudeutsch abgekürzt ›e-crime‹) unter der Schirmherrschaft von Europol statt.

Nachdem der Innenminister von NRW Fritz Behrens in seinem Einführungsvortrag[2] die Veranstalter noch dazu beglückwünschen konnte, dass sie mit dem Thema ›e-crime‹ oder auch ›cyber-crime‹ ein gutes Gespür für aktuelle Entwicklungen bewiesen hätten und sozusagen voll im Trend zukünftiger behördlicher und auch politischer Thematisierungen lägen, blieb er in seinen inhaltlichen Ausführungen zu dem sich neu abzeichnenden kriminalpolitischen Thema relativ zurückhaltend und alles in allem (auch wenn für ihn als Innenminister die staatlichen Kontroll- und Sicherheitsaspekte im Vordergrund standen) nicht auffallend dramatisierend.

Neuartige Kriminalitätsformen und bekannte Bedrohungs-Szenarien

Diesen Part übernahm ganz offensichtlich und mit überwiegend fesselnder Rhetorik und deutlicher Vehemenz der nachfolgende Redner, der Europol-Chef Jürgen Storbeck.[3] Er zeichnete in seinem Vortrag ein wahres Horror-Szenario von in letzter Zeit eingetretenen Störfällen, die im weltweiten Kommunikationsnetz des Internet durch aktives Handeln aufgetreten seien und die sofortiges Reagieren staatlicher Instanzen erforderlich machten, wenn man nicht schon in naher Zukunft eine Art elektronisches ›Pearl Harbor‹ erleben wolle. Hier eine kleine Auswahl:

- Hacker seien auf dem Weltwirtschaftsgipfel in Davos in das dortige Computersystem eingedrungen und es sei für sie ein Leichtes gewesen, sämtliche Daten der 3200 Gipfelgäste inklusive 1400 Kreditkartennummern zu stehlen.
- ›Viren-Anschläge‹, die an anderer Stelle[4] auch schon begrifflich mit ›Terror-Anschlägen‹ gefasst und verglichen werden, verursachten Milliarden-Schäden bei Millionen ›Netz-Teilnehmern‹ und seien daher als besonders gefährlich einzustufen.
- Auch wirkliche Terroristen hätten inzwischen das Internet zum Kriegsschauplatz erklärt. Vor allem im Nahost-Konflikt zwischen den Palästinensern und Israelis griffen beide Seiten vermehrt zu virtuellen Waffen.
- Illegale Geldtransfers der sizilianischen Mafia von mehreren hundert Millionen Dollar seien durch die Polizei aufgedeckt worden; das organisierte Verbrechen nutze zunehmend auch die Möglichkeiten des Internet.
- Zwischen China und den USA seien im Anschluß an die Flugzeugaffäre Anzeichen eines regelrechten ›cyber-war‹ erkennbar gewesen.

Nach den dramatisch anmutenden Schilderungen dieser ›Cyber-Phänomene‹, die zwar einen gewissen Realitätshintergrund haben, die jedoch vor allem begrifflich aufgeladen und hinsichtlich des Bedeutungsgehaltes und ihrer Auswahl stark konstruiert und dramatisiert erscheinen, erlebt das Bedrohungs-Szenario eine Steigerung, indem nun mögliche zukünftige elektronische Super-GAUs an die Wand gemalt werden, die so noch nicht passiert sind, die aber bald schon passieren könnten:

- So sei es durchaus möglich, dass Hacker in die EDV-Systeme von Flughäfen, Wirtschaftskonzernen und Regierungszentralen eindringen und finanzielle oder politische Forderungen stellen.
- Im Ernstfalle würden beim Gros der Firmen die Lichter ausgehen; doch nur ein Bruchteil der potenziell Gefährdeten sei nach Untersuchungen von Fachleuten gewappnet.

Die Quintessenz, die der Europol-Chef aus diesem eindrücklichen Horror-Szenario ableitete, bestand im wesentlichen darin, dass die vorhandenen Kapazitäten der nationalen und vor allem auch der supranationalen Strafverfolgungsbehörden absolut nicht ausreichen, um auf diese neue Gefahrenlage angemessen und effektiv reagieren zu können. Nach Meinung Storbecks müsse hier schleunigst etwas geschehen, um ein Desaster bzw. Inferno (à la ›Pearl Harbor‹) zu verhindern.

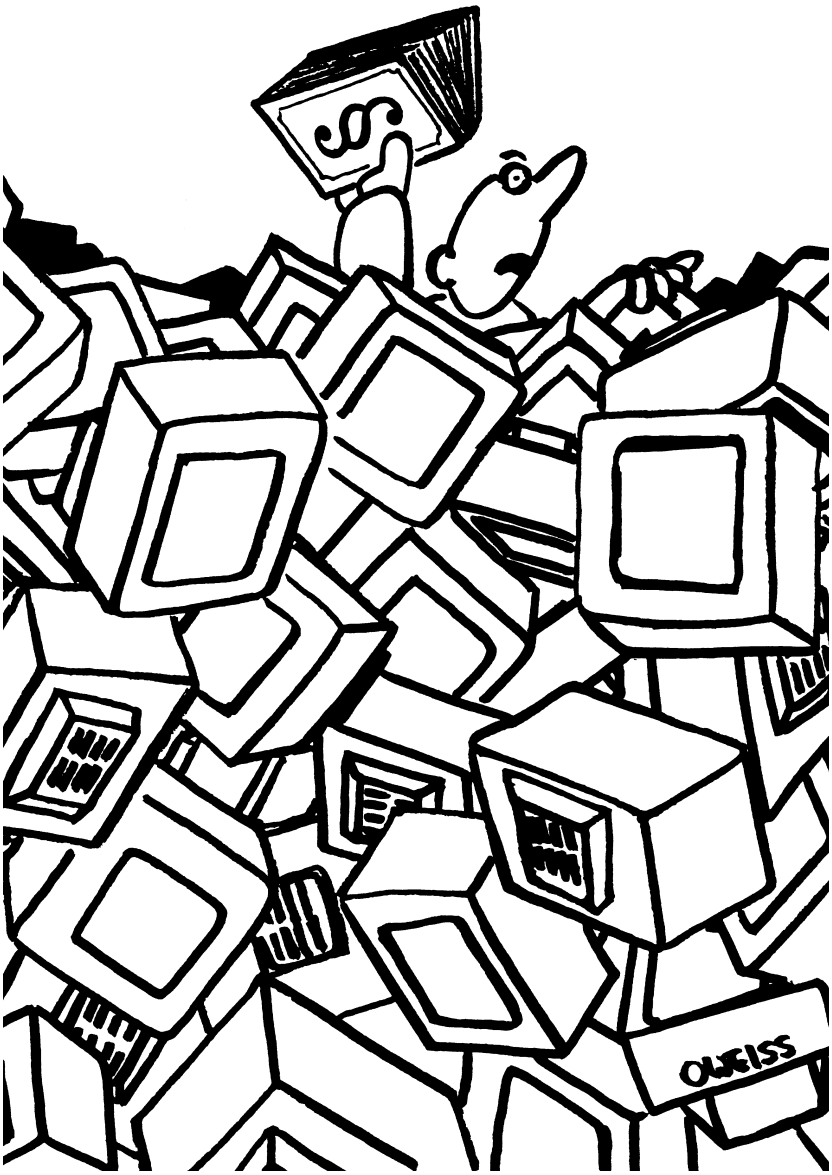
Europol und die Interessen eines supranationalen Sicherheits-Anbieters

Als einen möglichen Retter aus der gezeichneten Misere bot er dezent, aber unmissverständlich seine eigene Behörde an, für die er in seinen Ausführungen durchaus differenziert und reflektierend, in der Themenformulierung seines Vortrags[5] aber unübersehbar plakativ, direkt und offen um mehr Kompetenzzuweisung warb. Die derzeitige Diskussion um Europols Mandatserweiterung[6] auch hinsichtlich ›cyber-crime‹ werde in naher Zukunft, so hofft er, »*zu einer konsequenteren europäischen Zusammenarbeit bei der Fahndung und Ermittlung von Internetkriminellen und Internetkriminalität führen*«. Meines Erachtens spricht einiges dafür, dass die neu und aus gutem Grund gebildete Europäische Polizeiorganisation Europol einerseits noch keine ausreichende rechtsstaatlich abgesicherte Legitimation für strafrechtliche Ermittlungstätigkeiten hat, dass sie dies andererseits und aus den eigenen Interessen heraus als veränderungsbedürftig ansieht und somit über das Vehikel ›cyber-crime‹ versucht, die ihr bisher nicht zustehenden Fahndungs- und Ermittlungskompetenzen zu begründen und möglichst rasch zu erreichen. Vor diesem Hintergrund erfährt das von Storbeck gezeichnete Szenario eine gewisse Plausibilität und innere Logik.

Der kriminologischen Forschung sind derartige Inszenierungen und Dramatisierungen aus anderen Kriminalitätsbereichen durchaus bekannt. Man bezeichnet sie in Anlehnung an den US-Kriminologen Howard S. Becker auch als ›moralische Unternehmen‹ oder auch ›moralische Kreuzzüge‹. Dabei wird, durch die Motivationslage einzelner Akteure und Interessengruppen getrieben, ein gesellschaftlicher Thematisierungsprozess in Gang gesetzt, der über die Zeichnung von besonderen Gefährdungslagen ganz bestimmte staatliche Aktionen und Reaktionen als unverzichtbar darzustellen versucht. Dies geschieht auch und gerade im Bewusstsein einer äußerst mangelhaften objektiven Datengrundlage.

Neue globale Herausforderungen für die Kriminalpolitik und für die kriminologische Forschung

Im aktuellen Falle der ›Cyber-Crime-Thematisierung‹ erleben wir ein derartiges Vorgehen hinsichtlich der Dramatisierung eines neuartigen, supranationalen Phänomens, welches in erster Linie auch supra-



national zu regeln ist. Für den kriminologischen Beobachter geht es sozusagen um die Beobachtung und Analyse eines globalen Normgeneseprozesses. Die bekannten Strukturen und Interesseneinflüsse aus nationalen Normgenese- und Kriminalisierungsprozessen einerseits und die vollkommen neuartigen Zusammenhänge und Mechanismen in einem alle Grenzen sprengenden globalen System andererseits machen diesen sich hier anbahnenden Prozess zu einer hochinteressanten und intellektuellen Herausforderung gerade auch für die empirische kriminologische Forschung.

Bei der bekannten, weitgehend dezentralen und anarchischen Struktur des Internet bleibt es eine spannende Frage, inwieweit ein derartiges System durch die nationalstaatlich orientierten und begrenzten Regelungsformen des klassischen Strafrechts überhaupt erreicht werden kann und inwieweit dieses Regelungssystem sich mehr oder weniger globalisieren kann, ohne fundamentale rechtsstaatliche Standards, die in einzelnen demokratischen Ländern erreicht worden sind (Freiheits- und Menschenrechte, informationelle Selbstbestimmungs- und Datenschutzrechte, strafprozessuale Rechte etc.) in Gefahr bringen zu müssen.

Die aus nationalen kriminalpolitischen Diskursen bekannten Konfliktlagen und Abwägungen zwischen Sicherheits- und Freiheitsinteressen können aus einer global und fundamental rechtsstaatlich orientierten Perspektive auch auf der supranationalen Ebene nicht einseitig und zugunsten eines überzeichneten Sicherheitsinteresses entschieden werden. Es geht dabei im Kern um die Verhinderung einer unverhältnismäßigen Kriminalisierung und übermäßigen Kontrolle der Internet-Kommunikation. Auch die neuartigen Massendelikte, welche sich aufgrund der technologischen Entwicklungen aus dem klassischen Eigentumsbereich (wie z.B. Ladendiebstahl) sozusagen in den geistigen und elektronischen Eigentumsbereich (wie z.B. Software-Piraterie) verflüchtigen,[7] zeigen die Grenzen strafrechtlicher Regelungskompetenzen für den Bagatellbereich noch deutlicher auf als bisher schon.

Was aus kriminologischer Sicht zunächst einmal ansteht, ist eine gründliche und differenzierte Bestandsaufnahme der neuartigen Abweichungs-Phänomene, die mit dem Internet zusammenhängen. So gibt es derzeit neben den sehr subjektiv gezeichneten Lagebildern einzelner Interessenvertreter (aus den Bereichen Wirtschaft, Medien und Strafverfolgung) keinerlei umfassende und möglichst unabhängige und objektive Zustandsbeschreibungen; diese sind jedoch Voraussetzung auch für eine möglichst rationale supranationale Kriminalpolitik, um die es hier letztendlich geht. Eine derartige globale Kriminalpolitik braucht auch eine global und supranational ausgerichtete kritisch-rationale Kriminologie.

Die kriminologische Forschung, die durch das weltweite Kommunikationssystem des Internet nicht nur neue inhaltliche Fragestellungen geliefert bekommt, sondern auch ganz neuartige methodische Zugangswege und elektronische Techniken nutzen kann, ist hierdurch im doppelten Sinne herausgefordert.[8] Es bleibt eine spannende Frage, inwieweit sie in nächster Zukunft für diese Herausforderung die notwendige Kraft und Unterstützung erhält.

Dr. Werner Rüther ist als wissenschaftlicher Mitarbeiter am Kriminologischen Seminar der Universität Bonn beschäftigt. Schwerpunkte u.a.: Normgenese, Umwelt-Kriminalität, Internet-Kriminalität, (kommunale) Kriminalitätsanalysen

Anmerkungen

1 Siehe hierzu die vom ›Committee of Experts on Crime in Cyber-Space‹ für den Europarat erarbeitete ›Draft Convention on Cyber-Crime‹, No. 27 Rev. v. 25.5.2001 (http://conventions.coe.int/treaty/EN/cadreprojets.htm).

2 Siehe: Behrens, Fritz, Elektronische Kriminalität – eine besondere Herausforderung an die Sicherheit. Bonn 2001.

3 Dass er mit seinen Ausführungen vor allem auch in Richtung Medien anschlussfähig wird, zeigt die breite Resonanz, die er dort gefunden hat. Erwähnt sei hier stellvertretend für viele andere der Beitrag vom 23.5.2001 im Kölner Stadtanzeiger: Spilcker, Axel, Europäischer Polizeikongress, »Aktenzeichen Computerkriminalität« ungelöst …, S. 3.

4 Seit dem 19.2.2001 ist in Großbritannien der ›Terrorism Act 2000‹ in Kraft. Dieses Gesetz erweitert die Definition eines terroristischen Tatbestands beträchtlich; danach können künftig auch Angriffe gegen elektronische Systeme als Terrorakt geahndet werden, wenn die Regierung oder die Öffentlichkeit davon betroffen sind.

5 Storbeck, Jürgen, E-Crime – Europäisierung von Fahndung und Ermittlung. Vortrag auf dem 4. Europäischen Polizeikongress in Bonn, Bonn 2001.

6 Diese trifft wegen der derzeit (noch) mangelnden parlamentarischen und demokratischen Legitimation und der defizitären rechtsstaatlichen und strafprozessualen Absicherung auf relativ große Kritik vor allem aus der Bundesrepublik Deutschland.

7 Siehe hierzu meine ›elektronische Verflüchtigungsthese‹, die davon ausgeht, dass der kontinuierliche Rückgang der PKS-Zahlen beim ›einfachen Diebstahl‹ und damit auch der leichte Rückgang der PKS-Zahlen insgesamt seit 1997 u.a. darauf zurückzuführen ist, dass diese Delikte sich vermehrt in das Internet bzw. die ›Cyber-Society‹ verlagern und verflüchtigen, wo sie der polizeilichen Registrierung weitgehend entzogen sind.

8 Nähere Ausführungen hierzu finden sich in meinem Vortrag, den ich auf dem 4. Europäischen Polizeikongress in Bonn gehalten habe: Rüther, Werner, Internet und ›Cyber-Kriminalität‹ – eine Herausforderung auch für die Kriminologie. Bonn 2001.