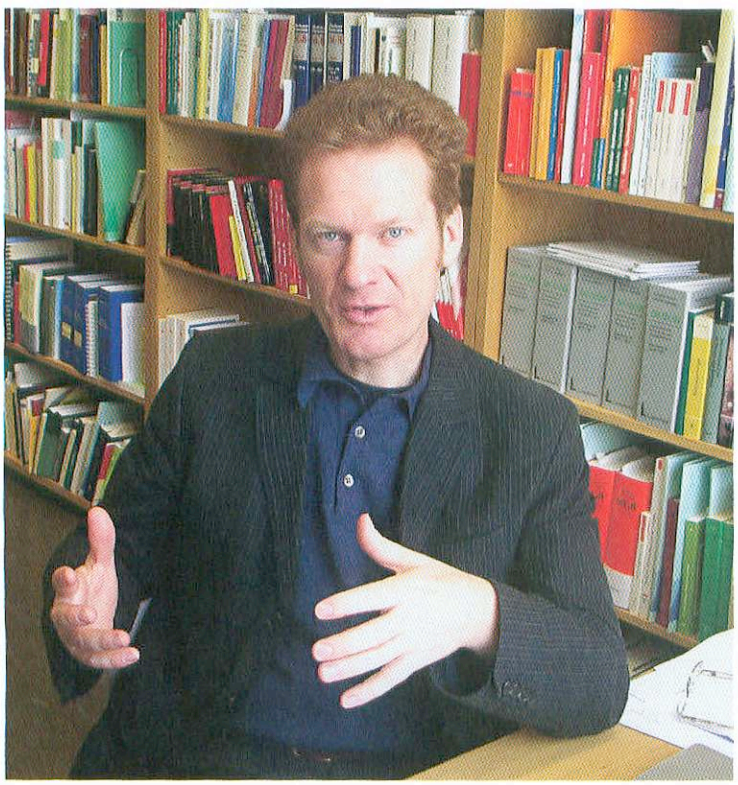
Prof. Dr. Christian Schwarzengger: Ermittler tappen bei «Cybercrimes» oft im Dunkeln

Fast täglich berichten die Medien über Aktionen gegen die verschiedensten Formen der «Cyber-Kriminalität». Besonders erschütternd sind dabei die weltweit grassierende Seuche der Kinderpornografie und der Missbrauch des Handys als Dokumentations- und Verbreitungsmittel von Gewalt und Vergewaltigung. Die Ermittlungsbehörden sind dauernd gefordert und müssen sich oft im Grenzbereich der Gesetzmässigkeit und ihrer technischen Möglichkeiten bewegen. Dr. Christian Schwarzenegger ist Assistenzprofessor für Strafrecht, Strafprozessrecht und Kriminologie an der Universität Zürich. Mit ihm unterhielt sich bulletin-Redaktor Guido Wemans über die Schwierigkeiten bei der Ermittlungsarbeit.

asut: Welches sind die Hauptprobleme bei der Ermittlung von Cyber-Kriminalität?

Prof. Schwarzenegger: Das Hauptproblem besteht darin, dass man zunächst den Tatort nicht kennt.



Denn: Um überhaupt sagen zu können, welche Strafverfolgungsbehörde zuständig ist, muss man herausfinden, wo der Täter die Strafhandlungen ausgeführt hat. Die Datenspuren liegen meistens auf irgendeinem Server im Netz oder auf einem PC eines Users. Daher kann es vorkommen, dass die falsche Behörde mit der Ermittlung beginnt, weil sich bei ihr das Opfer gemeldet hat. Erst im Verlauf der Ermittlungen stellt sich dann heraus, dass es sich um eine Tat im Ausland handelt, bei der die Schweiz gar nicht zuständig ist. Ebenso kann es möglich sein, dass in der Schweiz ein anderer Kanton die weitere Untersuchung übernehmen muss. Bei gewissen Deliktsarten wie beim Phishing kommt noch die Anknüpfung an den «Erfolgsort» in Frage, also dort, wo die Wirkung der Tat eingetreten ist. Aber grundsätzlich muss immer zuerst eine Lokalisierung vorgenommen werden, und diese ist bei der Cyber-Kriminalität am Anfang schwierig. Die zweite Schwierigkeit ist, dass man keine persönlichen Angaben zum Täter hat, kein Bild, keinen Namen, sondern lediglich eine IP-Adresse. Bestenfalls eine, welche zum Täter zurückführt; im schlechtesten Fall führt sie zu einem Internet-Café, zu einer Universität oder zu einem Wireless-Access-Point.

Wie kann man nun jemanden identifizieren?

Am Anfang hat diese Frage noch zu Diskussionen geführt, ob dies nach den strengen Vorgaben für die Überwachung des Fernmeldeverkehrs geschehen soll, die im BÜPF geregelt sind (Bundesgesetz betreffend der Überwachung des Post- und Fernmeldewesens). Schliesslich hat die REKO INUM (Rekurskommission des Eidgenössischen Departementes für Umwelt, Verkehr, Energie und Kommunikation) entschieden, dass die Provider, gestützt auf das BÜPF, die Pflicht haben, in einem vereinfachten Verfahren Auskunft über ihre Teilnehmeranschlüsse zu geben, also Name und Adresse des Teilnehmers mitzuteilen. Dies gilt für dynamische oder statische IP-Adressen gleichermassen.

Doch wegen der grenzüberschreitenden Dimension der Cyber-Kriminalität bedeutete dies bereits oft

das Ende einer Untersuchung. Die internationale Rechtshilfe in Strafsachen ist häufig zu langsam und kompliziert, um zeitgerecht an die Täter heranzukommen. Darum hat man seit einiger Zeit darüber diskutiert, ob solche Untersuchungen nicht zentralisiert werden sollten. Ob nicht eine Bundesstelle für den ersten Zugriff zuständig sein sollte. Mit der Gründung der KOBIK (Koordinationsstelle zur Bekämpfung der Internetkriminalität) wurde eine entsprechende Stelle geschaffen, obwohl dafür keine passende gesetzliche Grundlage bestand. Die KOBIK ist zuständig für den ersten Zugriff. Sie unterhält auch ein Internetportal (www.cybercrime.admin.ch), über welches Opfer und Dritte im Verdachtsfall Meldung erstatten können. Zeigen die ersten Vorermittlungen, dass die Tat einen Konnex zur Schweiz hat, wird das Dossier den zuständigen kantonalen Behörden übergeben; in schwerwiegenden Fällen auch an ausländische Stellen.

«Die internationale Rechtshilfe in Strafsachen ist häufig zu langsam und kompliziert, um zeitgerecht an die Täter heranzukommen.»

So ist die Zusammenarbeit innerhalb der Schweiz etabliert. Wie steht es mit der internationalen Zusammenarbeit?

Die Schweiz hat sich durch die Unterzeichnung der «Cybercrime Convention» verpflichtet, die internationale Zusammenarbeit zu verbessern. Allerdings ist dieses Abkommen noch nicht ratifiziert worden. Dies, weil einzelne Punkte der Konvention erst noch in das schweizerische Recht umgesetzt werden müssen. Eine wichtige Forderung der Konvention ist die Schaffung eines 24-stündigen Kontaktpunkts, über den ausländische Verfolgungsbehörden jederzeit Recherchen anstellen können. Der schnelle Informationsaustausch ist besonders wichtig, weil Datenspuren im Internet sehr kurzlebig sind.

Bezüglich der Kompetenzen des Bundes bei der Verfolgung strafbarer Handlungen mittels elektronischer Kommunikationsnetze liegt ein Vorentwurf einer Arbeitsgruppe vor. Nach diesem Vorentwurf könnten die Bundesanwaltschaft und die Bundeskriminalpolizei in Fällen, in denen eine der kantonalen Gerichtsbarkeit unterstehende strafbare Handlung mittels elektronischer Kommunikationsnetze begangen wurde und der zuständige Kanton noch nicht bekannt ist, erste, dringend notwendige Ermittlungen durchführen. Durch diese Ermittlungskompetenzen der Bundesanwaltschaft und der Bundeskriminalpolizei in der ersten Phase des Verfahrens würde keine Bundesgerichtsbarkeit begründet, doch könnte die Bundeskriminalpolizei durch Weisungen die Durchführung der Ermittlungen koordinieren. Das Geschäft ist aber noch nicht zu einer Botschaft an das Parlament ausgearbeitet worden. Man hat in der Zwischenzeit jedoch so etwas wie einen modus operandi gefunden, das heisst, KOBIK ist in der Vorfeldermittlung tätig. Sobald ein hinreichender Anfangsverdacht vorliegt, muss sie den Fall an die zuständige kantonale Strafverfolgungsbehörde weiterleiten. Damit soll ein unkoordiniertes Vorgehen, wie es in der Operation Genesis gegen Kinderpornografie vom Sommer 2002 in mehreren Kantonen auftrat, verhindert werden. Damals kam es zu Pannen, weil einzelne Kantone die Medien informierten, als andere Kantone mit den Hausdurchsuchungen noch gar nicht begonnen hatten.

Das sieht aber trotz allem noch ein wenig nach einer Baustelle aus. Und es entsteht der Eindruck, dass der Rechtsrahmen für derartige Aktionen doch noch gewisse Lücken aufweist. Bewegen sich da die Strafverfolgungsbehörden zum Teil noch in einem rechtlichen Grenz- oder Graubereich?

Wie es gegenwärtig durchgeführt wird, ist es schon rechtmässig. Man darf aber nicht vergessen: Die Strafverfolgung ist in erster Linie eine kantonale Angelegenheit. Die Kommission Netzwerkkriminalität, der ich angehörte, hat zwar 2003 eine Bundeskompetenz für komplexe, grenzüberschreitende Internet-Fälle vorgeschlagen. Die Diskussion dieses Vorschlages fiel aber in eine Zeit, wo man bereits schlechte Erfahrung beim Ausbau der Bundesstaatsanwaltschaft und Bundeskriminalpolizei im Bereich der organisierten Kriminalität und der Wirtschaftskriminalität gemacht hatte. Dies hatte viel gekostet und nicht das gebracht, was man erhofft hatte. Darum hat der Bund auch eine Abwehrhaltung eingenommen gegenüber Absichten, noch mehr Strafverfolgungen auf die Bundesebene zu hieven. Auch die Kantone haben ihre Bedenken. Dies

hat eine gewisse Berechtigung, denn bei «einfachen» Pornografie-Fällen, Datendiebstählen oder Fällen von Hacking sind die kantonalen Behörden schneller vor Ort und können die Untersuchung auch ohne weiteres selber erledigen.

Beim bisher geschilderten Vorgehen handelt es sich, einfach ausgedrückt, um «reaktive» Aktionen, die durchaus verständlich und auch notwendig sind. Ein gewisses Unbehagen lösen aber in jüngster Zeit auch gewisse «proaktive» Aktionen aus, wie etwa die Zusammenarbeit mit Kreditkarten-Unternehmen, um herauszufinden, wer gewisse Internetangebote mittels Kreditkarte bezahlt hat oder gar die bewusste Platzierung von «Trojanischen Pferden» in den PCs von Internet-Benutzern.

Diese Geschichte in Deutschland mit den Kreditkarten ist in der Tat äusserst heikel. Zur Erinnerung: Man hat einerseits herausgefunden, dass eine amerikanische Website Bilder mit kinderpornografischem Inhalt gegen die Bezahlung von $ 79.99 auf ein bestimmtes Konto anbot. Es bestand andererseits der Verdacht, dass Internetbenutzer aus Deutschland diese Website besuchten. Für einen Staatsanwalt aus Halle war dies bereits ausreichend, um daraus zu schliessen, dass es in Deutschland Konsumenten von Kinderpornografie geben musste. Darauf gestützt hat er eine Art von Informationsherausgabepflicht der Kreditkartenunternehmen angenommen, ist an diese gelangt und hat die Herausgabe von Daten über Zahlungen auf das betreffende Konto über den genannten Betrag verlangt. Die Kreditkartenunternehmen haben daraufhin die Kundendaten jener Personen herausgegeben, die eine entsprechende Zahlung vorgenommen hatten. Hier besteht einerseits die heikle Frage, ob zu Beginn überhaupt ein hinreichender Anfangsverdacht vorhanden war. Zwangsmassnahmen, wie sie das Strafprozessrecht vorsieht, können nur vorgenommen werden, wenn ein solcher Anfangsverdacht besteht. Ist der hinreichende Anfangsverdacht gegeben, kann die zuständige Staatsanwaltschaft per Editionsverfügung auch von Dritten Auskünfte verlangen. Eine Einzahlung von $ 79.99 ist aber nicht strafbar, und wenn über die Website auch legale Downloads möglich waren, würde das für einen hinreichenden Tatversacht nicht ausreichen. Ausserdem muss der Eingriff auch verhältnismässig sein. Ist es verhältnismässig, das Bankgeheimnis gegenüber von 22 Mio. Personen gestützt auf ein vage Vermutung aufzuheben? Nach dem Strafprozessrecht sind sogenannte «pishing expeditionen» verboten. Eine phishing expedition wäre zum Beispiel eine Überprüfung sämtlicher Konten einer Bank auf den blossen Verdacht hin, bei dieser Bank würde Geld gewaschen. Hier wäre ein Anfangsverdacht nicht gegeben. Nach meinen Informationen hat man sich in der Schweiz überlegt, ob man dem deutschen Beispiel folgen soll.

«Diese Geschichte in Deutschland mit den Kreditkarten ist in der Tat äusserst heikel.»

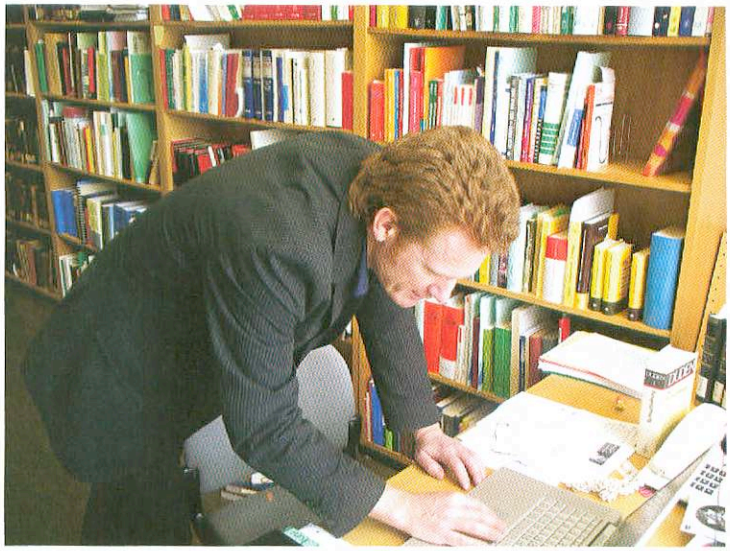
Kommen wir nun zur neusten Aktion deutscher Ermittler, zur erwähnten Platzierung von Trojanischen Pferden in den PCs von Verdächtigen. Man spricht in diesem Zusammenhang auch von Kontakten der Ermittler zu Virenschutz-Software-Herstellern, um diese zu bewegen, in den Virenschutz-Programmen «Hintertüren» offenzulassen, durch welche die «behördlichen» Trojaner eindringen könnten. Ich stelle mir vor, dieses Vorgehen steht hierzulande ausser Diskussion. Die Debatte über solche Methoden fand bereits vor zwei Jahren statt. Ein Polizeibeamter hatte an einer Fachtagung in Interlaken präsentiert, was für Software dazu verwendet werden könnte. Angefangen damit hat das amerikanische FBI mit einer eigens entwickelten Software namens Carnivore, welche mittels Trojanern einen PC ausspionieren konnte. Unter anderem konnte das Programm auch Tastatur-Eingaben aufzeichnen und damit Passwörter registrieren. Ein so präparierter PC wurde «gläsern» und konnte jederzeit online durchforscht werden. Und nun zur Rechtsgrundlage für ein solches Vorgehen in der Schweiz. Meines Erachtens besteht in den Schweizer Strafprozessordnungen keine Rechtsgrundlage für ein solches Vorgehen. Eine Ausspionierung eines PCs ist so etwas zwischen Überwachung und Hausdurchsuchung. Man könnte es auch virtuelle Hausdurchsuchung bezeichnen. Eine Hausdurchsuchung ist statthaft und wird auch eingesetzt; allerdings müssen bestimme Bedingungen erfüllt sein. Dazu gehört ein hinreichender Tatverdacht, dass auf einem sich im Haus befindlichen Computer relevantes Material gespeichert ist. Ferner muss ein Verbrechen oder eine Vergehen passiert sein, also nicht eine einfache Übertretung. Die Aktion muss mit an-

deren Worten verhältnismässig sein. Der Vorteil einer Hausdurchsuchung für den Betroffenen besteht darin, dass dieser sofort Bescheid weiss und bei Bedarf rechtliche Vorkehrungen verlangen kann, wie zum Beispiel die Versiegelung bestimmter Dokumente. In der Folge findet dann eine eigentliche Triage statt, bei welcher nichtbeweisrelevante Dokumente resp. Daten ausgeschieden werden. Ferner kann ein Betroffener sich sofort gegen die Handlung des Staatsanwalts wehren, zum Beispiel mittels eines Rekurses. Diese Möglichkeiten fehlen bei einer heimlichen Aktion. Solche verdeckten Untersuchungsmethoden greifen intensiver in die Freiheitsrechte der Bürger ein. Darum gilt der Grundsatz, dass man solche Aktionen nur bei schwerwiegenden Delikten und in engen Grenzen durchführen darf. Damit sind wir im Bereich der Telefon- und E-Mail-Überwachung, welcher im BÜPF geregelt ist. Die Platzierung von Trojanern ist im BÜPF nicht vorgesehen, denn sie stellt ja auch keine Überwachung dar, sondern ist, wie erwähnt, eine «virtuelle» Hausdurchsuchung, bei welcher Dateien geöffnet werden und deren Inhalt überprüft wird. Somit ist die Platzierung eines Trojaners in einem PC eine strafbare Handlung der Untersuchungsbehörde, denn das Ausspionieren von Daten stellt einen Strafbestand dar. Die Überwachung wäre eigentlich auch strafbar, wäre da nicht die gesetzliche Grundlage des BÜPF.

Wurden in der Schweiz auch schon «behördliche» Trojaner eingesetzt?

Darüber ist mir nichts bekannt. Wie erwähnt hat an einer kriminologischen Tagung ein Fachmann über das Thema referiert. Aber ob ein Einsatz stattgefunden hat oder geplant wurde, blieb damals offen. In unserem nördlichen Nachbarland hat er offensichtlich stattgefunden, wenn auch inzwischen vom Bundesgerichtshof als rechtswidrig bezeichnet. Der deutsche Innenminister Schäuble hat den Einsatz verteidigt und als moderne Antwort auf die Cyber-Kriminalität bezeichnet. Die Polizei und Staatsanwaltschaft müssten mit der Zeit gehen können. Bei der Verfolgung von Verbrechern müssten heute auch modernste Transportmittel wie Helikopter eingesetzt werden, was in Zeiten der Pferdekutsche nicht notwendig war.

Die Strafverfolgungsbehörde muss auch bei uns in die Lage versetzt werden, um effektiv arbeiten zu können. Aber man darf nie vergessen, dass diese heimlichen Zwangsmassnahmen intensive Eingriffe in die Privat- und Intimsphäre darstellen. Die Lösung kann nur in einer gesetzlichen Regelung bestehen, die dem Einsatz dieser Mittel enge Grenzen setzt.



Verschiedentlich haben Sie den Ausdruck «schwerwiegend» gebraucht. In was für eine Kategorie fällt denn die Kinderpornografie?

Immer wenn es um solche «Deliktskataloge» geht, entbrennt ein grosser Streit im Parlament darüber, was aufgenommen werden sollte und was nicht. Die Kinderpornografie ist zwar in der öffentlichen Debatte sehr stark im Vordergrund und wird als ganz schlimmes Delikt betrachtet. In der juristischen Klassifikation, im Gesetz, ist es ein «mittelschweres» Delikt, welches als Vergehen und nicht als Verbrechen bezeichnet wird. Die relevante Strafdrohung ist eine Freiheitsstrafe bis zu drei Jahren. Es ist auch interessant, dass bei der «weichen» Pornografie, welche von Erwachsenen konsumiert werden darf, die Strafdrohung die gleiche ist wie bei der harten Pornografie. Das Erwerben, elektronische Beschaffen oder Besitzen von «harter» Pornografie wird geringer bestraft: maximal ein Jahr Freiheitsstrafe. Man darf nicht vergessen, dass die schwerwiegendere Tat, die sexuelle Handlung mit einem Kind, durch eine separate Strafnorm verboten wird. Hier ist die Strafdrohung Freiheitsstrafe bis zu fünf Jahren. Wird ein Kind misshandelt, wird also härter bestraft. Beim Verbot der Pornografie geht es dagegen um Schriften, Ton- oder Bildaufnahmen, Abbildungen, andere Gegenstände solcher Art oder pornografische Vorführungen.

Lassen Sie uns noch auf eine andere Form von missbräuchlichem Einsatz von modernen Medien zu sprechen kommen. Auf die vor allem unter Jugendlichen beliebte Dokumentation von Gewalttaten und deren Weiterverbreitung via Handy-Kamera und MMS. Neben dem «happy slapping» – dem Prügeln von Altersgenossen – sind auch Vergewaltigungen, wie beispielsweise in Zürich Seebach, mittels Handys festgehalten worden. In der Folge davon griffen Schul- und polizeiliche Behörden zum Mittel der Beschlagnahme der Handys. Besteht dafür eine rechtliche Grundlage?

Ja, die rechtliche Grundlage besteht. Im Strafgesetzbuch gibt es Artikel 58, der den Einzug von Instrumenten, die zu einem Verbrechen oder einem Vergehen gedient haben oder als Produkt eines Verbrechens entstanden sind, regelt. Diese darf der Staat, vertreten durch die Strafverfolgungsbehörden, beschlagnahmen. Die Einziehung erfolgt danach durch ein Urteil des Gerichts. Dabei gibt es allerdings Differenzierungen. Man darf beispielweise von einem Provider nicht einen ganzen Server einziehen, weil darauf eine Datei mit kriminellem Inhalt gespeichert ist. Da spielt wiederum das Verhältnismässigkeitsprinzip eine Rolle. In diesem Fall muss eine Datei so gelöscht werden, dass sie nicht mehr rekonstruiert werden kann. Ob die Löschung vor Ort vorgenommen werden kann oder ob der Computer oder die Festplatte anschliessend wieder ausgehändigt werden soll, ist momentan Gegenstand von Diskussionen. Die Praxis hat gegenwärtig die Stossrichtung, dass Gegenstände eingezogen und dann unschädlich gemacht werden. Vom Verhältnismässigkeitsprinzip ausgehend, müsste man beim Handy die rechtswidrigen Daten löschen und dann das Handy wieder herausgeben. Man könnte aber auch den Memorystick, auf welchem die Datei gespeichert ist, zerstören und dann das Handy zurückgeben. Falls der SIM-Karten-Speicher die Daten enthält, müsste man die SIM-Karte einziehen und das Handy wieder aushändigen.

Jetzt noch eine Frage, die nicht unbedingt mit Ihrer Disiplin zu tun hat. Glauben Sie, dass die Repression, die sch als roter Faden durch unser Gespräch gezogen hat, ds Allerheilmittel darstellt oder müsste nicht vielmehr die Prävention unter Einbezug der Schulen, der Eltern und der Provider in den Vordergrund gestellt werden?

Bei dieser Frage müsste man vom Einzelfall ausgehen. Ich habe letzthin ein Beispiel mit Journalisten diskutiert: die Computer-Spiele, das „Gamen". Da regelt das Gesetz zwar gewisse Bereiche wie Gewaltdarstellungen oder Pornografie. Aber zu meinen, mit den im Gesetz vorgesehenen repressiven Massnahmen das Problem zu lösen, ist illusorisch. Es gibt zahlreiche Hinweise darauf, dass vor allem sozial entfremdete und zum Teil unter psychischen Störungen leidende Menschen gerne mit solchen Spielen gamen und dabei den Agressionsstau irgendwie ausleben. Sich dabei aber auch inspirieren lassen, wie jener, welcher vor kurzem mit dem Sturmgewehr einfach aus dem Fenster geballert hatte. Auch er ist offenbar nicht mit dem Leben zurecht gekommen und sich entschlossen, nun einfach einmal real auf Menschen zu schiessen. Was nötig wäre, ist eine mehrspurige Strategie. Dazu gehört beispielsweise bei den Herstellern von solchen Computerspielen darauf hinzuwirken, dass sie, wie das in Deutschland der Fall ist, ihre Spiele klar deklarieren. Also zum Beispiel, dass ein gewisses Spiel erst ab 18 Jahren gespielt werden darf. Dabei muss diese Deklaration auch beim Point-of-Sales klar beachtet werden, indem das Verkaufspersonal ein solches Spiel nicht an Jugendliche unter 18 Jahren verkauft. Das ist eigentlich eine Selbstregulierung der Industrie.

«Aber zu meinen, mit den im Gesetz vorgesehenen repressiven Massnahmen sei das Problem zu lösen, ist illusorisch.»

Eine weitere Massnahme ist die Erziehung der Beteiligten. Die Eltern oder Erziehungsberechtigten sind ebenfalls in die Pflicht zu nehmen. Wie bei der Drogenprävention gilt es, Verständnis zu schaffen. Eine Möglichkeit dazu wäre, dass so etwas wie «Packungsbeilagen» mit Erläuterungen zum Inhalt abgegeben würden, welche die Eltern darüber informierten, mit was für Spielen ihre Kinder gamen. Nehmen Sie zum Beispiel das sehr realistische, brutale Spiel «GodFather» (Der Pate): Darin kann man unter anderem Menschen mit dem Messer umbringen oder in den Kopf schiessen. Solche Präventivmassnahmen sollten auch auf das Handy ausgedehnt werden. Es gibt sicher Erwachsene, die nicht wissen, dass man mit dem Handy auch

Pornografie oder Gewaltdarstellungen herunterladen kann.

Ich sehe da verschiedene Präventionsstrategien: Erstens die Ausbildung in der Schule durch eine offene Thematisierung, eine eigentliche Medienerziehung durch Eltern und Schule; zweitens die Selbstregulierung und klare Kundeninformationen seitens der Industrie und drittens für die Extrembereiche die Repression. Es ist klar, dass das Ganze nur funktioniert, wenn alle Seiten mithelfen. Wenn man das Strafrecht alleine lässt und hofft es werde es schon richten, ist es bereits zu spät und funktioniert nicht mehr.

Bestünde nicht auch eine Möglichkeit, beispielsweise nur Handys ohne Kameras an Jugendliche abzugeben?
Ich glaube nicht, dass dies eine realistische Strategie darstellt. Das wäre, wie wenn man wegen den «Rasern» nur noch Autos mit Holzrädern auf den Markt bringen würde, damit nicht mehr schnell gefahren werden kann. Dazu kommt, dass Geräte, mit welchen verschiedene Tätigkeiten ausgeführt werden können, vom Markt nicht nur akzeptiert, sondern sogar in steigendem Mass gewünscht werden. Sie haben auch einen hohen gesellschaftlichen Nutzen, denn sie machen unsere Leben in verschiedenen Bereichen leichter. Nicht zuletzt besteht eine verfassungsrechtlich geschützte Wirtschaftsfreiheit. Ich möchte noch ein weiteres Beispiel erwähnen, und zwar aus dem Gebiet des Urheberstrafrechts, in welchem ich ebenfalls tätig bin. Es gibt zahlreiche «Peer-to-PeerA-Netzwerke, über welche urheberrechtlich geschützte Musik-, Film- oder Gamedateien angeboten und kopiert werden. Soll man jetzt die P2P-Software wie etwa «eDonkey» oder «BitTorrent» verbieten? Im Gegensatz zu den Kameras in den Handys werden diese Programme hauptsächlich für den illegalen Up- und Download verwendet. Aber auch diese Programme sind «dual-use»-Instrumente, die man sehr wohl auch für innovative Dienstleistungen benützen kann. Nach meiner Meinung sollte man bei «dual-use»-Geräten mit absoluten Verboten sehr zurückhaltend sein. Im Urheberstrafrecht geht man deshalb einen anderen Weg, um die Urheberrechte, die massenhaft verletzt werden, besser zu schützen: Man konzentriert sich auf eine Vorstufe, indem man technische Schutzvorkehrungen gegen das illegale Kopieren rechtlich absichert. Man muss aber bei allen Massnahmen bedenken, dass einseitige Verbote in der Schweiz überhaupt nichts bewirken würden. Notwendig ist vielmehr ein international harmonisierter Rechtsrahmen. Erst wenn in den USA, Russland und in der Schweiz die gleichen Verbote gelten, kann man sie effektiv durchsetzen.

Vielen Dank für das Gespräch. □

Fotos Wemans

Wer ist Prof. Dr. Christian Schwarzenegger?

Geboren am 11. November 1959 in Zürich

Ausbildung

1979–1984	Studium der Rechte und Politologie (Ergänzungsfach) an der Universität Zürich, anschliessend Sprachstudium in Perugia (I);
1985 –1992	wissenschaftlicher Assistent am Kriminologischen Institut der Universität Zürich (Prof. Dr. Dr. h.c. mult. Günther Kaiser);
1992	Promotion zum Dr. iur. an der Universität Zürich;
1992–1993	Akzessist und Gerichtsschreiber am Kantonsgericht Schaffhausen, Anwaltspatent (Schaffhausen);
1994–1996	Assistenzprofessor für die Fächer Europäisches Recht, Rechtsvergleichung, Strafrecht und Kriminologie an der Universität Niigata (Japan), Rechtswissenschaftliche Fakultät;
1997–999	Assistenzprofessor für die gleichen Fächer an der Universität Aichi (Japan);
seit 1.10.99	Assistenzprofessor für Strafrecht, Strafprozessrecht und Kriminologie in Zürich.
Details	http://www.rwi.unizh.ch/schwarzenegger/

asut bulletin

Prof. Dr. Christian Schwarzenegger:
Ermittler tappen bei «Cybercrimes» oft im Dunkeln

Prof Dr Christian Schwarzenegger:
Dans la lutte contre la «cybercriminalité», les enquêteurs avancent souvent à l'aveuglette

Swisscom investiert weiter in den Netzausbau und lanciert neue Angebote

Jahresbericht der ComCom 2006

Mobile Tagging – Schlüsseltechnologie für das mobile Internet

Web 2.0 – mehr als nur ein Buzzword

Schwerpunkt
Missbrauch von Handy und Internet: Repression oder Prävention?