heitsrisiko einzustufen ist: In den fünf Versuchen am Rechner der University of Southern California infizierte das Virus jeweils alle im Rechner belassenen Programme in weniger als einer Stunde, und bei Experimenten am Computer einer Privatfirma betrug die „Infektionszeit“ etwa 20 Sekunden.

Bei den Versuchen wurde das eingeschleuste Virus vorher elektronisch markiert. Auf diese Weise ließen sich Infektionswege und infizierte Programme leicht ausfindig machen. Der Rechner konnte anschließend wieder „desinfiziert“ werden. Doch jeder geschickte Programmierer, der ein Computersystem sabotieren will, kann das Virus so unscheinbar gestalten, daß es im Computer „nur wenige Spuren, wenn überhaupt welche“ hinterläßt. Solche Viren können über Daten-Ferntaster „komplette Rechnernetze epidemisch befallen“.[7]

Inzwischen sind die zu den „Versuchen“ verwandten Grundmuster weiterentwickelt und verfeinert worden. Und wer will da bei nahezu 99 Prozent Dunkelziffer schon sagen, in welchem Ausmaß kriminelle Hardware- und Softwaremodifikation ganze Informationssysteme anders als beabsichtigt arbeiten läßt? H. Gliss bemerkt dazu: „Durch die Manipulation von Anspruchsdaten können finanzielle Transaktionen ausgelöst werden, die völlig korrekt wären, wenn die Anspruchsdaten der Wirklichkeit entsprächen. Von der beim Arbeitsamt gespeicherten Zahl der anspruchsberechtigten Kinder hängt das Kindergeld ab, von den Verdienstangaben, die die Gemeinde erhebt, das Wohngeld, von Eintrittsdaten, Urlaubsanspruchsdaten und Angaben über An- und Abwesenheit hängen Entgeltbestandteile ab etc. Diese und ähnliche Anspruchsdaten sind in der Vergangenheit immer wieder manipuliert worden. “

Und weiter: „Daten, die einen hohen Informationswert haben, können Gegenstand deliktischer Handlungen sein. Kundendateien, Angaben über Konditionen, Lieferantenverzeichnisse, Aufzeichnungen über Herstellungsverfahren, Archivinhalte (man denke an Patente, Lizenzen und Verfahrensbeschreibungen), ja sogar Computersoftware, die entwickelt wurde, um bestimmte Verwaltungs- oder Produktionsabläufe optimal zu gestalten, können für die Konkurrenz von außerordentlicher Bedeutung sein. Entwicklungskosten können gespart, Angebotsstrategien durchkreuzt, Lieferanten beeinflußt und Ausschreibungen unterboten werden, wenn die Konditionen rechtzeitig bekannt sind. “[8 9]

Man wird des weiteren den — wenn auch nicht sehr zahlreichen — Verlautbarungen unterschiedlichster Herkunft schon glauben können, daß sich auf dem Gebiet der Software-Piraterie gegenwärtig in den kapitalistischen Ländern ein ganz neues Phänomen entwickelt, das die Industrie und auch die Polizei vor gänzlich neue Probleme stellt: Denn an „Einbußen“ sind gegenwärtig schon Milliardenbeträge im Spiele und das Verhältnis zwischen verkauften Originalen und dem Hand-zu-Hand-Geschäft mit Raubkopien hat sich schwindelerregend auseinander entwickelt[8]. Auf eine Originaldiskette sollen jetzt schon zwischen fünf und fünfzig Raubkopien entfallen.

1985 wurde über erste Strafrechtsentscheidungen zur Software-Piraterie berichtet und in diesem Zusammenhang darauf verwiesen, daß die große Zahl der 1984 aufgetauchten Raubkopien zu einer explosionsartigen Zunahme der Strafanzeigen wegen Software-Piraterie führten. „Ende 1984 war eine deutliche Abnahme der Verletzungsfälle durch sogenannte .Computer-Freaks' feststellbar. Demgegenüber nahm die Zahl der Computer-Läden, die u. a. auch Raubkopien verbreiteten, Ende 1984 und Anfang 1985 deutlich zu. Von den Computer-Läden wurden häufig nicht nur Computer-Spiele, sondern auch teure Anwendungsprogramme als Raubkopien angeboten. Soweit bisher Strafentscheidungen bekannt sind, betrafen sie mit einer Ausnahme jedoch nur Verletzungsfälle durch die sogenannten .Computer-Freaks', da die Ermittlungsverfahren gegen die Computer-Läden naturgemäß aufwendiger und umfangreicher sind.“[10 11]

H. Gliss schätzt ein, daß sich ein deutlicher Schwerpunkt im Bereich der Raubkopien herausbildet und der Aufwärtstrend ungebrochen ist. Computersoftware, die auf Magnetdatenträger leicht vervielfältigt und vertrieben werden kann, ist damit auch leicht dem Mißbrauch ausgeliefert. Angesichts der Preise, die für Software gezahlt werden, und im Hinblick auf eigene Entwicklungskosten ist die Versuchung, billiger an fremde Software heranzukommen, für viele Anwender sehr groß. Natürlich hat sich ebenfalls ein schwarzer Markt für Raubkopien etabliert.[1]* Das Geschäft mit Raubkopien erreicht, wie auch der Landespolizeipräsident von Baden-Württemberg, A. Stümper, unterbreitet hat, Schadenswerte in dreistelliger Millionenzahl; in einem einzigen Tatkomplex einer vierzigköpfigen internationalen Fälscherbande wurde allein ein Schaden von etwa 80 Millionen DM verursacht. Die Schäden aus dem Bereich der Wirtschaftsspionage, speziell des Know-how-Diebstahls, wurden z. B. bereits 1972 in der BRD auf drei bis vier Milliarden DM jährlich errechnet.[12]

Als einen weiteren Block von Varianten kriminellen Agierens mit dem Computer nennt R.A.H. von Zur Mühlen unter dem Aspekt der Betriebskriminalität Computermanipulationen im Personalbereich, Zeitdiebstähle im Rahmen der Computerkriminalität sowie Organisationssabotage mit Hilfe des Computers. Auch andere Varianten der Organisationssabotage werden zu einem ernsthaften Problem, so z. B. das Verändern von Programmen, um Unordnung zu schaffen. Über einfache, durch Ändern einiger weniger Parameter leicht modifizierte Sortierprogramme werden u. a. in Produktestammdatensätze die Warengruppenschlüssel anders gestaltet oder die Lagersorte im Hochregallager umbenannt. Das Ergebnis wird als chaotisch gewertet.[13 14]

Die sogenannte Computersabotage schließlich, die mitunter als vereinzelte Erscheinungsform von Maschinenstürmerei oder psychiatrischer Fälle in Medien apostrophiert wird — was jedoch mitnichten der Fall ist —, spielt eine nicht zu unterschätzende Rolle. J. Soyka verdeutlicht, was angefangen von primitiven Formen schießwütiger Computerstürmer bis hin zu gezielten Attacken der Konkurrenz gegen die Hardware-Einrichtungen des Gegners alles auf diesem Felde des Konkurrenzkampfes praktiziert wird.[1]* „Die Verläßlichkeit des Computers hängt also, wie man sieht, buchstäblich nur an einem Faden“ — hatte schon 1975 G. Elgozy gemahnt und wohl nicht zu Unrecht geschlußfolgert: „Wahrhaftig beklemmend zu denken, daß in unserer Gesellschaft sämtliche Vorgänge so perfekt arrangiert sind, daß ein Sandkorn, ein Fetzen Papier oder ein falsch übertragenes Wort alles blockieren oder ins Rollen bringen kann.“[15 16]

Der Münchner Rechtsanwalt P. Kragler spricht von zunehmender Radikalisierungswirkung der privaten Wirtschaftsspionage, die mit Hilfe des Computers von den Vorstandsetagen aus betrieben wird. „Betriebsspionage beginnt in aller Regel an der Front: Im Außendienst, im Vertrieb, in der Produktion, auf Messen, in der Poststelle, in der Kalkulation, in der Datenzentrale. Die Sensibilisierung aller Mitarbeiter bietet die größte Gewähr dafür, jeden Versuch einer Betriebsspionage bereits im Anfangsstadium zu registrieren. Hierfür ist die seismographische Wahrnehmung aller betrieblichen Auffälligkeiten, die Aktivierung aller Mitarbeiter und die Einrichtung vertraulicher Informationsstellen unerläßlich.“[15]

Es ist also durchaus zutreffend, hier bereits vom Vokabular her mit Begriffen wie Radikalität, Front und wirtschaftlicher Spionage zu sprechen — denn die Methoden sind so und die Täter wissen um Preis und Gewinn, der aus derlei Tätigkeit im Nadelstreifenbereich zu Buche schlägt.

Straf V erfo Igungspraxis

Der Bundesjustizrrfinister der BRD, Hans A. Engelhardt, hoffte mindestens seit 1985, daß die Strafbarkeitslücken durch ein neues Gesetz geschlossen werden könnten. Mit dem dann am 15. Mai 1986 vom Bundestag verabschiedeten Zweiten Gesetz zur Bekämpfung der Wirtschaftskriminalität[17] wurde allenthalben proklamiert, daß es nun den Computertätern an den Kragen gehen werde. Eine solche Wende wird allerdings kaum praktisch werden, wenn man die vielen Wenn und Aber schon bei der Aufdeckung und erst recht bei der Verfolgung und Bestrafung dieser Art von^Delikten in den Chefetagen bedenkt. Hinzu kommt das Computerspezifische. Während es früher für einen Unternehmer und seinen engsten Kreis nahezu unmöglich war, innerhalb der kurzen Zeit bis zu der auf Weisung der Staatsanwaltschaft eintreffenden Kriminalpolizei alle belastenden Unterlagen und Akten zu beseitigen, hat heute der Bankrotteur dergleichen auf einer

7 So der Bericht in: Der Spiegel vom 19. November 1984, S. 262 ff.
8 H. Gliss, a. a. O., S. 33 f.
9 J. Soyka, Computer-Kriminalität, a. a. O., S. 109.
10 G. Frhr. von Gravenreuth. „Erste Strafentscheidungen zur Software-Piraterie“, Gewerblicher Rechtsschutz und Urheberrecht (Weinheim) 1985, Nr. 6, S. 416 ff. (Zitat S. 417).
11 H. Gliss, a. a. O., S. 40 f.
12 A. Stümper, „Fällt Deutschland unter die Räuber?“, Die Welt (Bonn) vom 10. April 1986.
13 R.A.H. von Zur Mühlen, „Ausgewählte Probleme der Betriebskriminalität“, Betriebswirtschaftliche Forschung und Praxis 1985, Heft 1, S. 50 f.
14 J. Soyka, Computer-Kriminalität, a. a. O.
15 G. Elgozy, Der Computer-Wahn, Frankfurt am Main 1985, S. 142f.
16 P. Kragler, „Rechtliche und betriebliche Aspekte zur Problematik der provanten Wirtschaftsspionage“, Betriebswirtschaftliche Forschung und Praxis 1985, Heft 1, S. 19 ff.
17 Bundesgesetzblatt Teil I Nr. 21 S. 721.