Bundesamt für Polizei
Office fédéral de la Police
Ufficio federale di polizia
Federal Office for Police

"Cyberkriminalität"

Die dunkle Seite der Informationsrevolution

Strategischer Analysebericht
Oktober 2001

Bundesamt für Polizei / Dienst für Analyse und Prävention / www.bap.admin.ch

Problemstellung und Abgrenzung

Der vorliegende Bericht stellt das polizeilich relevante Gefährdungspotenzial durch die Cyberkriminalität dar und gibt einen Überblick über die wichtigsten elektronischen Bedrohungen für die nationalen Infrastrukturen. Auf Grund dieser Darstellung wird ein Fazit gezogen und es werden Empfehlungen abgegeben, wie künftig in der Schweiz und im internationalen Kontext gegen Cyberkriminalität vorgegangen werden kann.

Ausgeklammert wird zum einen das Problem, dass es sich bei der heutigen Informationstechnologie angesichts ihrer Komplexität um eine per se nicht absolut zuverlässige Technologie handelt. Gemeint sind beispielsweise Pannen, Ausfälle und Schäden wegen Zufällen, fehlerhafter Software, Programmierfehlern (Bugs) oder unzureichender Ausbildung der für die Informatiksicherheit Zuständigen. Zum andern ist der so genannte Informatikkrieg (Information Warfare), bei dem sich ein Staat die Möglichkeiten der Informatik zum elektronischen Angriff gegen einen anderen Staat zu Nutze macht, nicht Gegenstand dieses Berichts. Information Warfare fällt primär in den militärischen Verantwortungsbereich.

Es ist vorgesehen, diesen Analysebericht regelmässig zu aktualisieren und ihn insbesondere verstärkt mit Bezügen zur konkreten Situation in der Schweiz anzureichern.

Zusammenfassung und Haupterkenntnisse

1. Informationen sind heutzutage ohne grossen Aufwand schnell und kostengünstig nahezu jederzeit und überall fast jedem zugänglich. Die Computertechnologie entwickelt sich in Riesenschritten, das Internet erlebt ein exponenzielles Wachstum. Mit dieser Informationsrevolution nicht Schritt gehalten haben die Massnahmen zum Schutz von Informations- und Kommunikationstechnologien. Dies trotz des sehr hohen Risikopotenzials für Pannen, Ausfälle und elektronische Angriffe im Bereich dieser Technologien.
2. Zur Cyberkriminalität zählen zum einen bekannte Kriminalitätsformen, die mit den modernen Mitteln der Technologie begangen werden: Verbreitung von rassendiskriminierendem oder extremistischem Gedankengut, Aufruf zu Gewalttaten, In-Umlaufbringen von kinderpornografischem Material, Abwicklung von Betrugsgeschäften oder Geldwäscherei auf elektronischem Weg. Zum andern umfasst Cyberkriminalität spezifisch neue Deliktsformen: Unbefugte Datenbeschaffung, unbefugtes Eindringen in ein Datenverarbeitungssystem, Datenbeschädigung und betrügerischen Missbrauch einer Datenverarbeitungsanlage. Das Schadenspotenzial im Bereich der Cyberkriminalität ist als hoch einzustufen. Viele Angriffe auf Informationsinfrastrukturen bleiben verborgen, weil sie nicht erkannt oder den zuständigen Stellen nicht gemeldet werden.
3. Für die strafrechtliche Verfolgung von Cyberkriminalität ergeben sich wegen des Aufbaus, der Struktur und der Möglichkeiten des für die Tatbegehung oft zentralen Internets besondere Schwierigkeiten. Die rechtlichen Grundlagen zur Verfolgung von Cyberkriminalität liegen in der Schweiz im Wesentlichen vor. Das Strafgesetzbuch (StGB) deckt die relevanten Straftatbestände ab (Artikel 143, 143bis, 144bis, 147, 150, 150bis StGB). Zudem nimmt der Bund aktiv teil an der Ende 1999 von Firmen unter anderem aus den Bereichen Telekommunikation, Informatik, Banken, Treuhand und Industrie gegründeten Stiftung InfoSurance. Im Finanzdepartement werden ein Koordinationsorgan und ein Krisenstab im Bereich Information Assurance aufgebaut. Noch ungeklärt ist die strafrechtliche Verantwortung von Internet-Providern bei Cyberkriminalität im gewaltextremistischen und rassistischen Spektrum. Das Bundesamt für Justiz (BJ) hat den Auftrag, die rechtliche Situation zu klären. Stärker in die Pflicht genommen werden die Provider auch durch die kurz vor der Verabschiedung stehende Konvention des Europarats zur Cyberkriminalität. Zur besseren Koordination der Strafverfolgung in diesem Bereich hat eine Arbeitsgruppe von Bund und Kantonen zur Bekämpfung des Missbrauchs der Informations- und Kommunikationstechnik (AG BEMIK) im Januar 2001 dem Bundesrat beantragt, zum einen im Bundesamt für Polizei (BAP) beim Dienst für Analyse und Prävention (DAP) eine so genannte Monitoring-Stelle, die im Internet systematisch nach strafbaren Inhalten recherchiert zu schaffen. Zum andern beantragt die Arbeitsgruppe, bei der Bundeskriminalpolizei (BKP) eine Clearing-Stelle zur Anzeige- und Verfahrenskoordination im Bereich Cyberkriminalität einzurichten. Ausserdem sollen entsprechende Analysekapazitäten aufgebaut werden.

Inhaltsverzeichnis

1. Die bedrohte Gesellschaft

Seit der Einführung des Personal-Computers vor rund zwanzig Jahren und der weltweiten Vernetzung von Computern durch das Internet im vergangenen Jahrzehnt hat sich der Umgang der Gesellschaft mit Information grundlegend verändert: Informationen sind ohne grossen Aufwand schnell und kostengünstig nahezu jederzeit und überall fast jedem zugänglich. Die Computertechnologie entwickelte sich in Riesenschritten, das Internet erlebte ein exponenzielles Wachstum. Diese Informationsrevolution ist weiterhin voll im Gang.

Die moderne Gesellschaft ist in hohem Mass von so genannten **kritischen Informationsinfrastrukturen** abhängig. Information und Kommunikation, Banken und Finanzwesen, die Versorgung mit den Energien Wasser, Strom, Öl und Gas, die Transport- und Logistikstrukturen sowie Gesundheits- und Rettungswesen[1] basieren alle zum überwiegenden Teil auf Informatik- und Telekommunikationslösungen und sind nicht zuletzt wegen ihres stetig steigenden Komplexitätsgrads immer stärker verletzbar.

Mit dieser Entwicklung nicht Schritt gehalten haben die Massnahmen zum Schutz dieser Informations- und Kommunikationstechnologien. Dies trotz des sehr hohen Risikopotenzials für Pannen, Ausfälle und elektronische Angriffe im Bereich dieser Technologien. Wegen der elektronischen Steuerung fast aller für die Gesellschaft lebenswichtigen Bereiche sowie wegen der starken nationalen und globalen Vernetzung der Informationsinfrastrukturen ist das Schadenspotenzial ausgesprochen hoch. Als hoch einzuschätzen ist auch die Wahrscheinlichkeit von Störungen der Systeme durch technische Mängel oder willentliche elektronische Angriffe. Die Zahl der weltweit im Einsatz stehenden Computer steigt weiter, die Entwicklung im Hardware- und Softwarebereich verläuft rasch und die Bedeutung offener Netzwerke wie das Internet nimmt rasant zu. Weder die Rechtsprechung noch die Methoden zur Bekämpfung mutwilliger Angriffe auf die Informationsinfrastrukturen konnten mit dieser Entwicklung vollumfänglich Schritt halten.

Unter dem Begriff **Information Assurance** werden Schutzmassnahmen gegen Störungen im Bereich der lebenswichtigen kritischen Infrastrukturen etwa im Energie-, Transport- und Logistikbereich, in der Wasserversorgung oder im Gesundheits- und Rettungswesen ebenso zusammengefasst wie elektronischer Diebstahl oder die unerlaubte Veränderung von Daten beispielsweise einer Bank, Versicherung oder staatlichen Institution.

Die Bekämpfung der **Cyberkriminalität** im Kontext der Information Assurance umfasst das weite Feld krimineller Aktivitäten im Bereich der Informationsinfrastrukturen. Zur Cyberkriminalität zählen zum einen bekannte Kriminalitätsformen, die neu mit den Mitteln der Informationstechnologie begangen werden: Beispielsweise die Verbreitung von rassendiskriminierendem oder rechtsextremem Gedankengut, der Aufruf zu Gewalttaten, das In-Umlaufbringen von kinderpornografischem Material, die Abwicklung von Betrugsgeschäften oder Geldwäscherei auf elektronischem Weg. Zum andern umfasst Cyberkriminalität spezifisch neue Deliktsformen: Die unbefugte Datenbeschaffung, das unbefugte Eindringen in ein Datenverarbeitungssystem, die Datenbeschädigung und den betrügerischen Missbrauch einer Datenverarbeitungsanlage.[2] Bei der Tatbegehung im Bereich der

[1] Aufzählung laut Schlussbericht der am 15. Juli mittels Executive Order 13010 von US-Präsident Bill Clinton einberufenen President's Commission on Critical Infrastructre Protection (PCCIP) vom Oktober 1997.
[2] Schweizerisches Strafgesetzbuch (StGB) Artikel 143, 143bis, 144bis und 147.

Cyberkriminalität findet vor allem das globale Computernetzwerk Internet als zentrales Übertragungs- und Zugangsmedium Verwendung.

2. Das bedrohte Netz

Das Internet umfasst eine Vielzahl von Netzwerken, in denen Computer (Hosts) durch ein gemeinsames Übertragungsprotokoll, das so genannte Transmission Control Protocol/Internet Protocol (TCP/IP) miteinander verbunden sind und so Daten austauschen können. Die beiden bekanntesten Möglichkeiten der Internet-Nutzung sind das World Wide Web (WWW) sowie das Versenden und Empfangen von elektronischer Post (E-Mails). Daneben bietet das Internet weitere Funktionalitäten wie den Dateiversand mittels File Transfer Protocol (FTP), die Nutzung eines örtlich entfernten Grossrechners über eine Datenleitung via Terminalemulation (Telnet), die Übertragung von Telefonie-, Radio- und Fernsehdaten sowie die Teilnahme an elektronischen Diskussionsgruppen. Für den einzelnen Benützer schaffen Internet Service Provider (ISP) als Zugangsprovider (Accessprovider) oder Dienstleistungsprovider (Hostprovider) die technischen Voraussetzungen für den Zugang zum Internet.

Der Ausbau des in seinen Grundlagen Ende der 60er-Jahre des 20. Jahrhunderts entwikkelten Internets beschleunigte sich ab Anfang der 90er-Jahre rapid. Die Entwicklung des WWW und Preissenkungen für die Datenübertragung zwischen dem europäischen und dem amerikanischen Kontinent führten ab 1994 zu einem rasanten Ausbau des Angebots und einer immensen Zunahme der dem Internet angeschlossenen Hosts. In den letzten Jahren fand etwa im Rhythmus von neun Monaten eine Verdoppelung der Anzahl der angeschlossenen Computer statt.[3] So stieg die Zahl der registrierten Hosts weltweit von gut 4,8 Millionen im Januar 1995 innert sechs Jahren auf fast 109,6 Millionen im Januar 2001. Ähnlich verlief die Entwicklung in Europa: War Ende 1994 noch rund 1 Million Hosts im Netz, wurden Ende 1999 schon über 10 Millionen gezählt. Im Mai 2001 waren in Europa knapp 14,3 Millionen Hosts registriert. Im Jahr 2000 nutzten gemäss einer repräsentativen Studie rund 45 Prozent der Deutschschweizer im Alter zwischen 14 und 69 Jahren das Internet beruflich oder privat.[4] Im Mai 2001 waren rund 262'600 Hosts mit Schweizer Domain (.ch) registriert.[5] Die Zahl der Internet-Benützerinnen und Benützer dürfte gemäss Schätzungen bis ins Jahr 2002 auf weltweit rund 320 Millionen steigen.

Mit Blick auf die Cyberkriminalität ergeben sich für die Strafverfolgung einige Schwierigkeiten, die nicht zuletzt darin begründet sind, dass das Internet trotz seines gewaltigen Wachstums und damit mittlerweile globalen Charakters nach wie vor Grundzüge aufweist, wie sie für die ursprünglich als Benutzer anvisierte ausgesuchte Gruppe von Personen aus Wissenschaft und Militär ausreichten:

- Das Internet ist als offenes, kooperatives Forschungsnetzwerk konzipiert, in dem jeder Benützer selbst entscheidet, welche Informationen er zur Verfügung stellen und welche Informationen er beziehen will.

[3] Peter Wiedemann: Tatwerkzeug Internet. Ein Überblick über das System und seine kriminelle Nutzung. Kriminalistik Heft 4/2000, Seite 229-239.
[4] Neue Zürcher Zeitung: Zwei Stunden täglich im Cyberspace. Neue Internet-Zahlen der AG für Werbemedienforschung. 25.8.2000.
[5] www.switch.ch/domain/hostcount.html.

- Im Vergleich zu anderen Kommunikationsmitteln haben Benützerinnen und Benützer des Internets verhältnismässig grössere Möglichkeiten, ihre Kommunikation direkt zu beeinflussen.
- Die offene Struktur des Internet stellt es jedem Benützer frei, für die Einspeisung seiner Daten ins Netz die Umgebung zu wählen, die ihm für seine Bedürfnisse die am besten geeigneten rechtlichen Rahmenbedingungen bietet. Ist beispielsweise eine Aktivität in einem bestimmten Staat strafbar, kann der Benützer ohne grossen Aufwand von einem anderen Standort aus operieren.
- Das Sicherheitsniveau der Informationstechnologie im Allgemeinen hat mit der weltweiten Vernetzung nicht Schritt gehalten und ist nicht zuletzt wegen mangelnder Ausbildung der Benützerinnen und Benützer weiterhin tief.

3. Formen der Bedrohung und Akteure

Informationsinfrastrukturen können Ziele unterschiedlichster Formen von Angriffen werden. Nebst konventionellen physischen Akten (Sabotage durch den Unterbruch von Verbindungen, Durchtrennen von Kabeln, Sprengung von Einrichtungen usw.) und psychologischen Aktionsformen (Desinformation, politischer Druck, Untergrabung des Vertrauens in die Zuverlässigkeit eines Systems) stehen im Bereich des Internets vor allem elektronische Angriffe im Vordergrund (jeweils mit einem aktuellen Beispiel):

- **Computerviren** sind kleine Programme, die heute meist als Anhang (Attachment) zu einem E-Mail verbreitet werden. Werden die Programme gestartet, replizieren sie sich selbst und richten unter Umständen enorme Schäden auf dem Computer des Empfängers an (beispielsweise indem die Festplatte neu formatiert wird, was einen totalen Datenverlust zur Folge hat).

  Im Juni 2001 versuchten Unbekannte mit einer Virus-Attacke, die Daten der Walliser Gemeinde Leukerbad zu zerstören. Die Täter verwendeten als Absender den Namen des wegen finanzieller Schwierigkeiten der Gemeinde eingesetzten Beirats. Der Gemeindeschreiber kannte allerdings die korrekte E-Mail-Adresse des Beirats und schöpfte Verdacht. Der Virus wurde als Anhang zum E-Mail verschickt und hätte nach dem Öffnen die Daten der Gemeinde gelöscht.[6]

- **Trojanische Pferde (Trojaner)** sind Programmsegmente, die entweder schon bei der ursprünglichen Programmierung oder durch späteren illegalen Zugriff beispielsweise in Form eines Virus unbemerkt in ein Programm eingebaut werden. Sind sie einmal aktiviert, ermöglichen Trojaner Drittpersonen Zugriffe auf den betroffenen Computer, senden automatisch Informationen aus den Betriebsprozessen an Drittpersonen oder setzen ein Programm auf Befehl oder zu einer bestimmten Zeit ausser Betrieb (beispielsweise ein Textverarbeitungsprogramm nach einer gewissen Anzahl Betriebsstunden).

  Anfang Mai 2000 führte ein Virus namens "I Love You" zu einer weltweiten Krise in den Informatiknetzwerken. Ein 23-jähriger Informatikstudent aus den Philippinen, der Computerviren erforschte, löste den Vorfall aus, weil ihm der Virus angeblich aus Versehen entwischte. "I Love You" konnte innert 36 Stunden weltweit nachgewiesen werden. Als Kombination von Virus und trojanischem Pferd nützte er eine Schwäche des weit verbreiteten E-Mail-Programms Outlook aus. Ohne Zutun des Benützers fragte der Virus die Adressenliste des betroffenen Computers ab

[6] Newsletter der Stiftung InfoSurance, Nr. 4/5 - Juni/Juli 2001, Seite 4. Und: Sonntagszeitung vom 8.6.2001 (www.sonntagszeitung.ch/sz/szFeinRubrik.html?ArtId=100277&ausgabeid=1476&rubrikid=188).

und versandte sich selbstständig im Schneeballsystem weiter. Wurden die E-Mails geöffnet, löschte ein im Anhang des E-Mails versteckter Trojaner Bilddaten auf dem Computer und versuchte Passwörter zu lesen, um diese an eine vordefinierte Adresse weiterzuverschicken.

- Beim **Hacking** wird versucht, bestehende Sicherheitsvorkehrungen zu umgehen und so in ein geschütztes und/oder geschlossenes System einzudringen. Einmal im attakkierten System, kann der Hacker möglicherweise verheerende Manipulationen vornehmen (beispielsweise Daten verändern, löschen oder stehlen). Handelt der Hacker böswillig, wird seine Tat oft auch als *Cracking* bezeichnet.

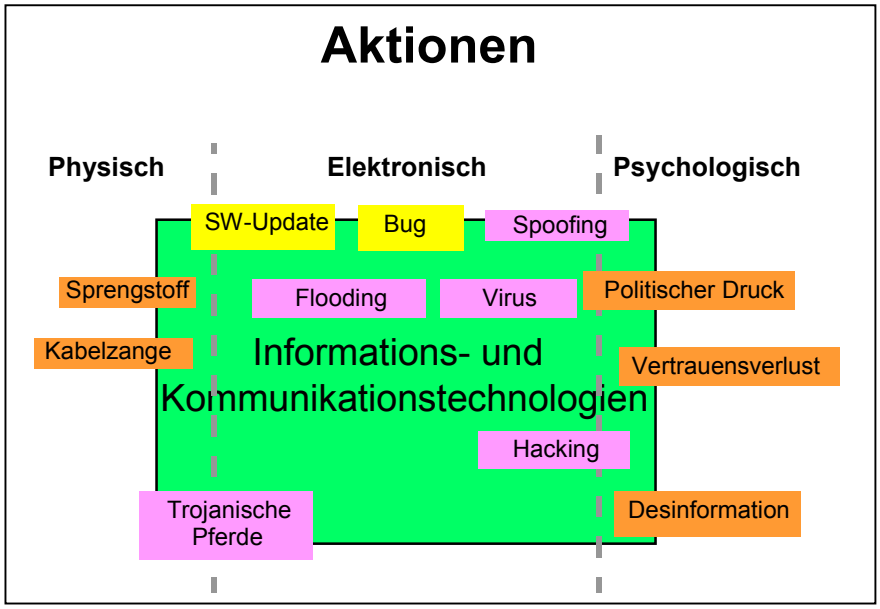
  Im Umfeld des World Economic Forum (WEF) 2001 in Davos drang eine Gruppe von Hacker in das System des WEF ein und erlangte so Zugriff auf vertrauliche Daten von WEF-Teilnehmern. Unter den Daten befanden sich unter anderem Telefonnummern, Privatadressen, E-Mail-Adressen und Passwörter für den gesicherten Bereich des WEF-Internetangebots. Das Hacking war verhältnismässig einfach zu bewerkstelligen, da die gängigen Sicherheitsvorkehrungen nicht umfassend umgesetzt wurden.

- **Flooding** bedeutet, einen Computer durch Überlastung lahm zu legen. Dazu werden massenweise E-Mails an eine bestimmte E-Mail-Adresse geschickt oder möglichst viele gleichzeitige Zugriffe auf eine Websites ausgelöst. Macht sich der Angreifer dabei nicht genutzte Rechnerkapazitäten anderer ungeschützter Computer im Netz zu Nutze, wird von einem Distributed Denial of Service (DDoS)-Angriff gesprochen.

  Anfang Februar 2000 legte ein DDoS-Angriff die Websites führender amerikanischer E-Commerce-Anbieter sowie verschiedene Newssites über Stunden lahm. Ein 16-jähriger Kanadier war unter dem Pseudonym "Mafiaboy" in Dutzende von schlecht gesicherten Computern vor allem an Hochschulen eingedrungen und hatte von dort aus ferngesteuert jeweils Tausende von Abfragen auf die anvisierten Webserver der Firmen lanciert. Die Server brachen unter der Last der Anfragen zusammen und konnten von legitimen Kunden nicht mehr erreicht werden. Grosse Einnahmeausfälle waren die Folge.

- Eine **Mailbombe** überflutet die Mailbox eines Benützers mit unnützen Informationen und verunmöglicht ihm praktisch die Benützung seines Mailkontos. Handelt es sich bei den Informationen in den Mails um Werbung, wird von **Spamming** gesprochen. Beim **Spoofing** gibt der Täter falsche Identitäten als Absender der versendeten Mails an (beispielsweise Adressen einer Universität).

  Anfangs 2001 versandte ein Spammer in den USA Millionen von Werbe-E-Mails, deren Absender fiktive Adressen einer schweizerischen Hochschule waren. Weil die Adressen der Empfänger zu einem Grossteil ungültig oder falsch waren, wurden die nicht zustellbaren Mails an die angebliche Absenderadresse zurückgesandt. Die schweizerische Hochschule wurde daraufhin täglich mit bis zu einer Viertelmillion zurückgewiesener E-Mails überflutet. Dies führte nicht nur zu Zusammenbrüchen des Servers, sondern auch zu Produktionsausfällen und dazu, dass gewisse Provider in den USA echte E-Mails der Hochschule nicht mehr weiterleiteten, weil diese wegen der vom Spammer verwendeten falschen Adressen als nicht mehr vertrauenswürdig angesehen wurde.



Grafik: Angriffsmittel gegen Informationsinfrastrukturen.

Die Täter, die Informationsinfrastrukturen angreifen, lassen sich im Überblick in drei Kategorien einordnen[7]:

- In der Kategorie **Cyberkriminalität** sind häufig Einzeltäter aktiv. Allerdings sind auch Aktivitäten organisierter krimineller Gruppen beispielsweise im Bereich des Betrugs oder der Geldwäscherei künftig wahrscheinlicher. Bereicherungsabsichten und Sabotage sind häufige Motive für die kriminellen Taten.
- In der Kategorie **Cyberterrorismus** sind in erster Linie ideologisch-politisch motivierte Gruppierungen aktiv. Bei extremistisch beziehungsweise terroristisch motivierten Angriffen steht vielfach politische Erpressung im Vordergrund. Häufig sind Netzwerke von Regierungen oder anders gesinnten Gruppierungen Ziel der Attacken. Zwar sind in dieser Kategorie erst Einzelfälle bekannt, die Wahrscheinlichkeit ist aber hoch, dass die Zahl der Vorfälle künftig zunimmt.
- In der Kategorie **Information Warfare** führen Staaten elektronische Angriffe gegen andere Länder. Bis anhin sind allerdings noch keine solchen Fälle bekannt. Information Warfare wurde aber bereits in mit konventionellen Mitteln geführten Konflikten unterstützend eingesetzt. Zu dieser Kategorie gehört auch die unter dem Stichwort Echelon bekannte Abhörung politisch und wirtschaftlich relevanter Informationen im Ausland, die anschliessend den politischen Institutionen und der Industrie des eigenen Landes zur Verfügung gestellt werden.[8] Denkbar sind zudem im Rahmen staatsterroristischer Aktivitäten auch Szenarien, bei denen Staaten ihnen genehmen Gruppen Hacker (Information Warriors) oder die Geldmittel zur Anheuerung von Hackern zur Verfügung stellen, um bei einer Rückverfolgung nach Angriffen nicht selbst impliziert zu werden.

[7] Genau genommen ist eine Einteilung in vier Kategorien möglich. Wie bereits oben erwähnt, wird aber auf die vierte Kategorie, die Pannen und systembedingte Ausfälle umfasst, nicht eingegangen.

[8] Dazu auch: Nichtständiger Ausschuss der EU über das Abhörsystem Echelon: Vorläufiger Entwurf eines Berichts über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON), Berichterstatter Gerhard Schmid. 18. Mai 2001 (www.europarl.eu.int/tempcom/echelon/pdf/prechelon_de.pdf).

Während in den Kategorien Cyberterrorismus und Information Warfare nur vereinzelte Fälle bekannt sind, nehmen die Vorfälle in der Kategorie Cyberkriminalität im Zuge der Informationsrevolution rasant zu.

4. Cyberkriminalität konkret

Cyberkriminalität beinhaltet oft keine neuen Kriminalitätsformen, die spezifisch auf die modernen Informatiktechnologien zugeschnitten sind. Vielmehr werden lediglich bekannte Delikte statt mit konventionellen Hilfsmitteln mit Hilfe der Informatik begangen. Im Vordergrund stehen zum einen die Bereitstellung und Verbreitung von kinderpornografischem Material, Betrugsdelikte, elektronischer Diebstahl und Geldwäschereidelikte. Wichtig sind zum andern die innere Sicherheit eines Staates tangierende Aktivitäten, wie Gewaltaufrufe ideologisch-politisch motivierter Gruppen aus dem links- und aus dem rechtsextremen Spektrum, die Verbreitung von gewaltextremistischem und rassendiskriminierendem Gedankengut sowie die Spionage durch Einzelpersonen oder Gruppen. Ein europäischer Polizeidienst schätzt, dass zirka ein Drittel der Hinweise auf mit Hilfe des Internets begangenen Straftaten auf Kinderpornografie hindeutet. Ebenfalls rund ein Drittel der Hinweise auf Straftaten entfällt auf betrügerische Aktivitäten. Das verbleibende Drittel sind Hinweise auf Verletzungen des geistigen Eigentums, die Verbreitung von Viren und extremistische Gewaltaufrufe. Wegen fehlender Statistiken handelt es sich bei diesen Zahlen allerdings um grobe Schätzungen.

Kinderpornografisches Material wird in Form von Fotografien, Filmen und Texten hergestellt und verbreitet. Die Skala reicht von bildlichen Darstellungen sexueller Handlungen von Erwachsenen mit Kindern bis zu Mordszenarien. Bei der Sammlung solchen Materials wie auch bei dessen Verbreitung gewinnt das Internet an Bedeutung. Kinderpornografisches Material wird sowohl im WWW wie auch über einschlägige Diskussionsforen (Newsgroups, Chatrooms) verbreitet. Die grossen Internet-Provider in der Schweiz sperren solche Diskussionsforen mit kinderpornografischen Inhalten aktiv. Kinderpornografie wird in der Schweiz durch Artikel 197 des Strafgesetzbuchs (StGB) verfolgt.[9] Insgesamt stieg die Zahl der Anzeigen wegen Verstössen gegen Artikel 197 StGB seit 1997 nicht, allerdings nahm der Anteil der Anzeigen mit Bezügen zum Internet deutlich zu. 1997 wurden gemäss Erhebungen des Bundesamts für Polizei (BAP) bei den Kantonen 6 Fälle von Kinderpornografie mit Bezügen zum Internet angezeigt. Die Zahl stieg kontinuierlich bis auf 75 Anzeigen im Jahr 2000. Hier ist allerdings mit einer hohen Dunkelziffer zu rechnen, da momentan nur wenige spezialisierte Polizeieinheiten Pädophilie auf dem Internet verfolgen.

[9] Artikel 197 StGB: Pornographie 1. Wer pornographische Schriften, Ton- oder Bildaufnahmen, Abbildungen, andere Gegenstände solcher Art oder pornographische Vorführungen einer Person unter 16 Jahren anbietet, zeigt, überlässt, zugänglich macht oder durch Radio oder Fernsehen verbreitet, wird mit Gefängnis oder mit Busse bestraft. 2. Wer Gegenstände oder Vorführungen im Sinne von Ziffer 1 öffentlich ausstellt oder zeigt oder sie sonst jemanden unaufgefordert anbietet, wird mit Busse bestraft. Wer die Besucher von Ausstellungen oder Vorführungen in geschlossenen Räumen im voraus auf deren pornographischen Charakter hinweist, bleibt straflos. 3. Wer Gegenstände oder Vorführungen im Sinne von Ziffer 1, die sexuelle Handlungen mit Kindern oder mit Tieren, menschlichen Ausscheidungen oder Gewalttätigkeiten zum Inhalt haben, herstellt, einführt, lagert, in Verkehr bringt, anpreist, ausstellt, anbietet, zeigt, überlässt oder zugänglich macht, wird mit Gefängnis oder mit Busse bestraft. Die Gegenstände werden eingezogen. 4. Handelt der Täter aus Gewinnsucht, so ist die Strafe Gefängnis und Busse. 5. Gegenstände oder Vorführungen im Sinne der Ziffern 1–3 sind nicht pornographisch, wenn sie einen schutzwürdigen kulturellen oder wissenschaftlichen Wert haben.

Im Januar 1998 entdeckte eine auf Cyberkriminalität spezialisierte Polizeieinheit (Cybercops) in Grossbritannien in 23 Newsgroups rund 6'000 kinderpornografische Bilder. Sechs Monate später fanden dieselben Cybercops gut 7'300 Darstellungen von Kinderpornografie in 16 Newsgroups. Angebote mit kinderpornografischem Material werden nur ausgesprochen selten von der Schweiz aus ins Internet eingespiesen. 50% bis 80% der einschlägigen Websites befinden sich auf Servern in den USA.

Fast alle gängigen **Betrugsdelikte** werden heute auch mit Hilfe des Internets begangen. Beim Handel übers Internet (E-Commerce) kommt es am weitaus häufigsten bei Internet-Auktionen (Internet Auction Fraud) zu betrügerischen Aktivitäten. Gemäss der aktuellen Erhebung des der amerikanischen Bundespolizei angegliederten Internet Fraud Complaint Centers (IFCC)[10] wurden 65 Prozent der im Jahr 2000 gemeldeten Betrugsfälle bei Internet-Auktionen begangen. Bei den Auktionen ging es um den Verkauf von kleinen Plüschtieren (Beanies), Videogeräten und -filmen, Spielen, Musikkassetten, Computern, Fotokameras und Schmuckstücken. Typischerweise gibt der Betrüger als Kontaktmöglichkeit meist nur eine Mail-Adresse bei einem Anbieter von Gratismailkonten an. Die Zahlungen sollen in bar oder mit Scheck erfolgen. Andere übers Internet abgewickelte Betrugsgeschäfte beispielsweise bei Verkaufsangeboten ohne Auktionscharakter, bei Angeboten für Heimarbeit, im Kreditgeschäft und bei Pyramidenspielen/Kettenbriefen sind noch vergleichsweise selten, zeigen aber steigende Tendenz.

Betrügerbanden aus Nigeria machten bisher vor allem mit Briefen und Faxen auf sich aufmerksam. In den letzten Monaten ist eine deutliche Zunahme von E-Mails zu verzeichnen, in denen betrügerische Angebote unterbreitet werden. Die Betrüger fordern den Mail-Empfänger auf, in seinem Namen ein Bankkonto zu eröffnen, auf dem vorübergehend riesige Geldsummen von bis zu 90 Millionen US-Dollar deponiert werden sollen. Als Entschädigung für diese Dienstleistung soll das potenzielle Opfer 15% bis 35% der Anlagesumme erhalten. Wird auf diese Mails reagiert, fordern die Betrüger die Überweisung grösserer Geldbeträge, mit denen der reibungslose Ablauf des vermeintlichen Geschäfts finanziert werden soll. Leistet das Opfer solche Zahlungen, ist das Geld verloren.[11]

Die gängigste Vorgehensweise beim **elektronischen Diebstahl** ist, durch gezielte Fehltransfers Geld auf falsche Konten zu überweisen. Dabei wurde in den wenigen bisher bekannten Fällen die Website des anvisierten Unternehmens gefälscht, wozu meist die Hilfe eines Mitarbeitenden dieses Unternehmens nötig war. Einbezahlte Geldbeträge flossen damit beim Gelingen des elektronischen Diebstahls nicht auf das korrekte Zielkonto, sondern auf Konten der Täter. In einer anderen Spielart wird versucht, an sämtliche Identifikationsmerkmale von echten Bankkunden zu gelangen und dann deren Konten zu plündern.

Im Oktober 2000 meldete die Staatsanwaltschaft im italienischen Bologna, sie habe einen versuchten elektronischen Bankraub grösseren Ausmasses verhindert. Organisiert durch eine sizilianische Mafia-Gruppe hätten insgesamt über 1,5 Milliarden Franken durch einen gezielten elektronischen Fehltransfer gestohlen werden sollen. Der Gruppierung war es gelungen, mit Hilfe von Angestellten der betroffenen Bankfiliale und von Telecom-Mitarbeitern das elektronische Portal der Bank zu fälschen.[12]
Im Sommer 2000 brachten Hacker bei Kunden einer schweizerischen Grossbank einen Virus in Umlauf, der den befallenen Computer nach Telebanking-Daten durch

[10] www.ifccfbi.gov.
[11] Pressemitteilung des Bundesamt für Polizei (BAP) vom 24.7.2001 (www.admin.ch/bap - Rubrik Aktuell, Kategorie Pressemitteilungen).
[12] Der Spiegel "Raub am Geisterschalter. Computerhackern der Mafia wäre es beinahe gelungen, der Bank von Sizilien zwei Milliarden Mark zu entwenden." Der Spiegel, 23.1.2000.

suchte und gefundene Dateien als Kopien an verschiedene Mail-Adressen verschickte. Ebenso protokollierte der Virus die Tastatureingaben und sandte auch diese Informationen an die Mail-Adressen der Hacker. Mittels dieser Daten war es den Dieben möglich, sich mit der Identität des betroffenen Kunden beim Rechner der Bank auszuweisen und Vergütungsaufträge zu Lasten der Geschädigten aufzugeben.[13]

Wer in der Schweiz bei einer Bank ein Konto eröffnet, muss bei der Aufnahme oder im Verlauf der Geschäftsbeziehungen nach dem Grundsatz "know your customer" seine Identität zweifelsfrei nachweisen.[14] Im Bereich des elektronischen Bankgeschäft (E-Banking) fehlen solche Regelungen zum Grundsatz der Identitätsabklärung bislang in vielen Staaten noch. Die Identitätsabklärung ist jedoch ein zentrales Element im Kampf gegen die **Geldwäscherei** und es besteht die Gefahr, dass Geldwäscherei auf elektronischem Weg konventionelle Methoden mindestens teilweise ablöst.

Weltweit werden jährlich je nach Schätzung zwischen zwei und fünf Billionen US-Dollar gewaschen. Der Anteil der Geldwäscherei im Internet wird auf rund 50 Milliarden US-Dollar geschätzt.[15] *In der Schweiz verfügen derzeit sechs reine Internet-Banken über eine Bewilligung. Im Frühjahr 2001 hat die Eidgenössische Bankenkommission (EBK) strengere Vorschriften bei der Identifikation und Überwachung der Kunden von reinen Internet-Banken erlassen. Unter anderem müssen Kunden, die mehr als 500'000 Franken deponieren wollen, zwecks Identifikation persönlich vorsprechen.*[16]

Auf einschlägigen Websites veröffentlichen ideologisch-politisch motivierte Gruppierungen des links- und rechtsextremen Spektrum **Gewaltaufrufe** sowie **rassendiskriminierendes Material**. Die Sperrung von Websites mit gewaltextremistischen und rassistischen Inhalten gestaltet sich schwierig. Dies zum einen wegen der nach wie vor unklaren Rechtslage[17] und zum andern, weil Sperren relativ einfach umgangen werden können, indem das Angebot auf einer anderen Website publiziert wird oder der Zugriff über so genannte Anonymisierungsserver erfolgt.

Ab Dezember 2000 wurde auf verschiedenen einschlägigen Websites zur Teilnahme an nicht bewilligten Demonstrationen gegen das World Economic Forum (WEF), das Ende Januar 2001 in Davos stattfand, aufgerufen. Nebst Informationen zur Demonstration wurden auch Tipps abgegeben, wie Davos trotz der polizeilichen Sperren erreicht werden könne.

Seit vier Jahren beobachtet die private Initiative "Aktion Kinder des Holocaust" (AkdH) das Netz betreffend rechtsradikaler Seiten. Ziel dieser Initiative ist nicht nur das Sperren der Seiten, sondern auch das Identifizieren der Täter und deren Strafverfolgung. Allein im Jahr 2000 wurden gegen 100 meist erfolgreiche Strafanzeigen eingereicht.[18]

Auch im Bereich der **Spionage** durch Einzelpersonen oder Gruppierungen kommt das Internet zu Anwendung. Mittels Viren oder durch Hacking gelangen die Täter in den Besitz

[13] Der Bund "Hacker plünderten Konto von Bankkunden", Der Bund 28.2.2001.
[14] Vereinbarung über die Standesregeln zur Sorgfaltspflicht der Banken (VSB) vom 28.1.1998.
[15] Der Bund "'Mickey Mouse' als Kontoinhaber", Der Bund 27.12.2000.
[16] "Schweiz verschärft Vorschriften für Internet-Banken", AP 27.4.2001. "Kontoeröffnung über das Internet - Unveränderte Praxis zur Identifikation durch die EBK", Neue Zürcher Zeitung, 8.1.2001. " Bittere Pillen für die Bankenkommission - Verbesserte Bankenrevision und E-Finance im Visier", Neue Zürcher Zeitung 27.4.2001.
[17] Siehe Abschnitt Rechtslage in der Schweiz.
[18] Aktion Kinder des Holocaust (AkdH). www.adkh.ch.

vertraulicher Daten. Diese werden dann entweder verkauft oder direkt zur Erpressung der Opfer oder für andere kriminelle Aktivitäten verwendet. Die Spionage wird häufig von Mitarbeitenden der betroffenen Firma oder Institution begangen.

5. Riesiges Schadenspotenzial, grosse Dunkelziffer

Das Schadenspotenzial im Bereich der Cyberkriminalität ist als sehr hoch einzustufen. Dies dokumentieren folgende Zahlen:

- Das Computer Security Institute (CSI) kam in seiner zusammen mit dem FBI durchgeführten neuesten Umfrage bei Unternehmen und Institutionen der Wirtschaft und Verwaltung zum Ergebnis, dass sich die Schäden durch elektronische Angriffe im Jahr 2000 allein in den USA auf über 151 Millionen US-Dollar beliefen.[19]
- Die französischen Behörden bezifferten die Zahl der in Frankreich mit dem Internet in Verbindung stehenden Delikte im Jahr 1999 auf gut 2'400.[20]
- Der "I Love You"-Virus befiel laut Schätzungen von Lloyd's in London rund 50 Millionen Computer und verursachte weltweit Schäden von 15 Milliarden US-Dollar.

Gemäss einer Erhebung von Experten für Wirtschaftskriminalität der Internationalen Handelskammer (ICC) standen 67 Prozent der im Jahr 2000 gemeldeten Fälle von Cyberkriminalität in Zusammenhang mit kriminellen Aktivitäten beziehungsweise absichtlicher Täuschung durch Handel im Internet.[21] Dabei stellten nach wie vor elektronische Angriffe von Einzeltätern die bei weitem grösste Gefahr für Informationsinfrastrukturen dar. Eine grosse Zahl der Angriffe kam von Angestellten der betroffenen Unternehmen und Institutionen.[22] Gemäss einer aktuellen Studie zur Wirtschaftskriminalität sehen 60 Prozent der befragten Unternehmen in der Schweiz und 43 Prozent in Europa Cyberkriminalität als das grösste Risiko der nächsten fünf Jahre.[23]

Viele Angriffe auf Informationsinfrastrukturen bleiben verborgen, weil sie den zuständigen staatlichen und privaten Instituten nicht gemeldet werden. Nebst der Tatsache, dass längst nicht alle elektronischen Angriffe überhaupt entdeckt werden, dürfte vor allem die Furcht vor einem möglichen Image- und Vertrauensverlust der Grund dafür sein, dass Unternehmen Angriffe auf ihre Informationsinfrastruktur nicht publik machen. Zudem dürfte es auch Zweifel an der effizienten strafrechtlichen Verfolgung der Täter geben. Und nicht zuletzt erachten wohl die geschädigten Unternehmen die Aussicht auf die Rückführung des verlorenen Vermögens als gering.[24]

[19] CSI/FBI: 2001 Computer Crime and Security Survey (www.gocsi.gov)
[20] "Faut-il avoir peur du Web?", www.linteraute.com/0redac_dossiers/0008-aout/cybercrim/cybercrimrapport.sthml und Direction centrale de la police judiciaire, Ministère de l'Interieur.
[21] "Internet-Betrugsfälle dramatisch angestiegen", AP 15.1.2001
[22] CSI/FBI: 2001 Computer Crime and Security Survey (www.gocsi.gov)
[23] Wirtschaftskriminalität in Europa. Die Resultate der Schweiz. PricewaterhouseCoopers Juni 2001. www.pwc.com.
[24] Wirtschaftskriminalität in Europa. Die Resultate der Schweiz. PricewaterhouseCoopers Juni 2001. www.pwc.com

6. Schwierige Strafverfolgung, rechtliche Probleme

Insgesamt gestaltet sich die Verfolgung von Straftaten im Bereich der Informationsinfrastrukturen verhältnismässig schwierig. Dies hat verschiedene Gründe:

Technologie
- Das Internet als offenes und auf Kooperation basierendes Netzwerk bietet verhältnismässig viele Angriffspunkte.
- Örtliche und zeitliche Gebundenheit besteht nur in sehr begrenztem Mass. So kann etwa ein Angebot eines Schweizers auf einem Server in Russland ausschliesslich in arabischer Sprache platziert sein.
- Die Anonymität im Internet ist relativ hoch. So existieren beispielsweise Angebote (Anonymizer), bei denen Benützerinnen und Benützer ihre Identität verschleiern können. Auch E-Mails können dank so genannter Freemail-Angebote ohne Schwierigkeiten unter falscher Identität versandt werden.
- Längst nicht alle elektronischen Angriffe auf die Informationsinfrastruktur werden publik.
- Im oberen Management von privatwirtschaftlichen Unternehmen, aber teilweise auch in den Führungsebenen der Verwaltung, ist die Sensibilität für die Bedrohungen der Informationsinfrastruktur noch gering.

Strafverfolgung
- Die finanziellen und personellen Ressourcen zum Aufbau und zur Umsetzung von Schutzmassnahmen für die Informationsstruktur wie auch für die Strafverfolgung sind im Vergleich zu anderen Kriminalitätsformen noch immer bescheiden.
- Die Frage nach der Verantwortung der Internet Provider ist nicht abschliessend geklärt.[25] Deshalb sind längst nicht alle Provider gewillt, illegale Inhalte auf ihren Servern zu sperren.
- Sperren von illegalen Angeboten lassen sich dank der globalen Struktur des Internets relativ leicht umgehen.
- Die Rechtslage ist in vielen Staaten unterschiedlich. Was im einen Staat als illegaler Inhalt gilt, ist anderswo nicht strafbar. Die internationale Abgleichung der rechtlichen Grundlagen ist noch im Gange.
- Die internationale und rasche unbürokratische Zusammenarbeit zwischen den Strafverfolgungsbehörden ist noch nicht ausreichend.
- Rechtshilfeverfahren dauern oft länger als die Beweise bei den Providern im Zielland elektronisch gespeichert bleiben.

6.1. Strafverfolgung und Rechtslage in der Schweiz

In der Bekämpfung und strafrechtlichen Verfolgung von Cyberkriminalität ist zwischen den zwei Bereichen Strafverfolgung und Rechtssetzung zu unterscheiden. Die mit Hilfe des Internets begangene Netzwerkkriminalität stellt vor allem die Strafverfolgung vor neue Herausforderungen. Die spezifisch neuen Formen der Cyberkriminalität stellen zusätzlich ein Problem für die Rechtssetzung dar. In der Schweiz liegen diese rechtlichen Grundla

[25] Vgl. dazu das Positionspapier der Bundespolizei, das Gutachten des Bundesamts für Justiz und das Gutachten im Auftrag des Verbands Inside Telecom (im Literaturverzeichnis).

gen zur Verfolgung von Cyberkriminalität - auch spezifisch neuer Formen - im Wesentlichen vor.

Das Schweizerische Strafgesetzbuch (StGB) deckt folgende Straftatbestände ab:

- Unbefugte Datenbeschaffung (Artikel 143 StGB)[26]
- Unbefugtes Eindringen in ein Datenverarbeitungssystem (Artikel 143bis StGB)[27]
- Beschädigung von Daten (Artikel 144bis StGB)[28]
- Betrügerischer Missbrauch einer Datenverarbeitungsanlage (Artikel 147 StGB)[29]
- Erschleichen einer Leistung (Artikel 150 StGB)[30]
- Herstellen und Inverkehrbringen von Materialien zur unbefugten Entschlüsselung codierter Angebote (Artikel 150bis StGB)[31]

In der Schweiz existiert bislang keine umfassende Statistik über die bei den Strafverfolgungsbehörden eingegangenen Anzeigen. Die Polizeiliche Kriminalstatistik (PKS) erfasst als Teilstatistik lediglich ausgewählte Delikte. Die Informatikkriminalität gehört nicht dazu. Für einen gesamtschweizerischen Überblick über die Fälle im Bereich Cyberkriminalität kann daher einzig die vom Bundesamt für Statistik (BFS) geführte schweizerische Urteilsstatistik (SUS) herangezogen werden.

[26] Artikel 143 StGB: Wer in der Absicht, sich oder einen andern unrechtmässig zu bereichern, sich oder einem andern elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten beschafft, die nicht für ihn bestimmt und gegen seinen unbefugten Zugriff besonders gesichert sind, wird mit Zuchthaus bis zu fünf Jahren oder mit Gefängnis bestraft.

[27] Artikel 143bis StGB:
Wer ohne Bereicherungsabsicht auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt, wird, auf Antrag, mit Gefängnis oder mit Busse bestraft.

[28] Artikel 144bis StGB: 1. Wer unbefugt elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten verändert, löscht oder unbrauchbar macht, wird, auf Antrag, mit Gefängnis oder mit Busse bestraft. Hat der Täter einen grossen Schaden verursacht, so kann auf Zuchthaus bis zu fünf Jahren erkannt werden. Die Tat wird von Amtes wegen verfolgt. 2. Wer Programme, von denen er weiss oder annehmen muss, dass sie zu den in Ziffer 1 genannten Zwecken verwendet werden sollen, herstellt, einführt, in Verkehr bringt, anpreist, anbietet oder sonstwie zugänglich macht oder zu ihrer Herstellung Anleitung gibt, wird mit Gefängnis oder mit Busse bestraft. Handelt der Täter gewerbsmässig, so kann auf Zuchthaus bis zu fünf Jahren erkannt werden.

[29] Artikel 147 StGB: 1. Wer in der Absicht, sich oder einen andern unrechtmässig zu bereichern, durch unrichtige, unvollständige oder unbefugte Verwendung von Daten oder in vergleichbarer Weise auf einen elektronischen oder vergleichbaren Datenverarbeitungs- oder Datenübermittlungsvorgang einwirkt und dadurch eine Vermögensverschiebung zum Schaden eines andern herbeiführt oder eine Vermögensverschiebung unmittelbar darnach verdeckt, wird mit Zuchthaus bis zu fünf Jahren oder mit Gefängnis bestraft. 2. Handelt der Täter gewerbsmässig, so wird er mit Zuchthaus bis zu zehn Jahren oder mit Gefängnis nicht unter drei Monaten bestraft. 3. Der betrügerische Missbrauch einer Datenverarbeitungsanlage zum Nachteil eines Angehörigen oder Familiengenossen wird nur auf Antrag verfolgt.

[30] Artikel 150 StGB: Wer, ohne zu zahlen, eine Leistung erschleicht, von der er weiss, dass sie nur gegen Entgelt erbracht wird, namentlich indem er ein öffentliches Verkehrsmittel benützt, eine Aufführung, Ausstellung oder ähnliche Veranstaltung besucht, eine Leistung, die eine Datenverarbeitungsanlage erbringt oder die ein Automat vermittelt, beansprucht, wird, auf Antrag, mit Gefängnis oder mit Busse bestraft.

[31] Artikel 150bis StGB: 1. Wer Geräte, deren Bestandteile oder Datenverarbeitungsprogramme, die zur unbefugten Entschlüsselung codierter Rundfunkprogramme oder Fernmeldedienste bestimmt und geeignet sind, herstellt, einführt, ausführt, durchführt, in Verkehr bringt oder installiert, wird, auf Antrag, mit Haft oder Busse bestraft. 2. Versuch und Gehilfenschaft sind strafbar.

Zu Artikel 150bis StGB liegen in der SUS noch keine Urteile vor. Für die anderen Artikel werden die folgenden Zahlen ausgewiesen:

	Art. 143	Art. 143bis	Art. 144bis	Art. 147	Art. 150
1994	0	1	2	0	0
1995	1	0	14	52	59
1996	2	1	18	225	84
1997	2	0	131	370	116
1998	2	1	21	378	131

Die Aufstellung zeigt, dass für die relevanten Artikel des StGB zwar bisher erst relativ wenige Urteile gesprochen wurden, die Zahlen aber insbesondere bei den Artikeln 147 StGB und Artikel 150 StGB steigende Tendenz aufweisen.

Nebst dem StGB kommen im Zusammenhang mit Angriffen gegen die Informationsinfrastruktur auch die Regelungen des Bundesgesetzes über das Urheberrecht und verwandte Schutzrechte (URG)[32] sowie des Bundesgesetzes gegen den unlauteren Wettbewerb (UWG)[33] zum Tragen. Diese Urteile werden hier nicht aufgeführt, weil sie häufig nicht als Cyberkriminalität im engeren Sinn anzusehen sind. Was die Ausübung klassischer Delikte mit Hilfe des Internets betrifft, liegen keinerlei Zahlen vor.

Die Kriminalstatistik des Kantons Zürich (KRISTA), die im Gegensatz zur PKS Informatikdelikte enthält, weist für die letzten fünf Jahre folgende Zahlen aus:

	Computerdelikte (Art. 143, 143bis, 144bis, 147)	Davon Art. 147
1996	794	786
1997	1'200	1'162
1998	1'623	1'612
1999	1'692	1'673
2000	2'140	2'100

Erfahrungsgemäss wird im Kanton Zürich etwa ein Viertel aller in der Schweiz erfassten Straftaten begangen. Es ist zudem davon auszugehen, dass es sich bei den meisten Straftaten nach Artikel 147 StGB um nicht mit dem Internet in Beziehung stehende Delikte handelt (Geldautomatenbetrug etc.). Für das Jahr 2000 ist damit im Kanton Zürich von etwa 40 und für die Schweiz von zirka 160 angezeigten Fällen von Cyberkriminalität auszugehen. Wie schon angeführt muss allerdings eine sehr hohe Dunkelziffer angenommen werden.

Während die rechtlichen Instrumente zur Verfolgung von Cyberkriminalität also vorhanden sind, stellt die mit dem Internet begangene Netzwerkkriminalität die Strafverfolgungsbehörden vor grosse neue Herausforderungen. Diese sind weder in der Schweiz noch international gelöst.

[32] Systematische Sammlung des Bundesrechts SR 231.1.
[33] Systematische Sammlung des Bundesrechts SR 241.

6.2. Strafverfolgung und Rechtslage im internationalen Umfeld

Die meisten Staaten verfügen heute über rechtliche Grundlagen zur Strafverfolgung von Cyberkriminalität. Die Straftaten werden entweder im Rahmen bestehender Gesetze oder gestützt auf eigens für diesen Bereich geschaffenen Rechtsgrundlagen verfolgt. Die internationale Staatengemeinschaft ist zudem bestrebt, künftig stärker gemeinsam gegen die Bedrohungen durch die Cyberkriminalität vorzugehen. So befassen sich die Vereinten Nationen sich im Rahmen der Kriminalitätsprävention mit diesem Problemkreis.[34]

Der Europarat, dem auch die Schweiz angehört, hat am 16. Mai 2001 eine neue Konvention gegen die Cyberkriminalität vorgestellt.[35] Die Konvention hat eine verbesserte Verfolgung und Ahndung der Cyberkriminalität zum Ziel. Im Vordergrund steht die Internet-Kriminalität im engeren Sinn, also die Tatbestände des illegalen Zugriffs auf Daten oder Computersysteme, illegales Abhören, Verändern von Daten, Störung von Systemen und illegale Mittel (Hackertools). Überall strafbar sollen zudem Betrug durch Manipulation oder Fälschung von Daten, die Herstellung und Verbreitung sowie der Besitz von kinderpornografischem Material sowie Verletzungen des Urheberrechts sein.[36] Die Provider werden zur Datensicherung und zur aktiven Zusammenarbeit mit den Strafverfolgungsbehörden verpflichtet. Die Unterzeichnerstaaten ihrerseits haben für eine effiziente Verfolgung der Cyberkriminalität zu sorgen, in dem sie die nationalen Gesetzgebungen harmonisieren, die Vorgehensweise für die Strafermittlung und -verfolgung definieren sowie ein schnelles und effektives System der internationalen Kooperation etablieren. Die Konvention listet in vier Kategorien die verfolgten Straftaten auf, stellt konkrete Regeln etwa zur Sicherstellung von Computerdaten sowie zur Sperrung von illegalen Inhalten auf und bildet die Grundlage für den Aufbau eines rund um die Uhr funktionierenden internationalen Kontaktnetzwerks zwischen den Strafverfolgungsbehörden. Die Konvention soll voraussichtlich im November 2001 zur Unterschrift durch die Mitgliedstaaten des Europarats aufgelegt werden. Sie wird auch von der Europäischen Union (EU), den USA, Japan und anderen Staaten unterstützt.

7. Sicherung der Information Assurance und Bekämpfung der Cyberkriminalität in der Schweiz

Die Schweiz hatte im Vergleich zu anderen Staaten mit gut ausgebauter Informationsinfrastruktur[37] einen verhältnismässig späten Start in der Sensibilisierung gegenüber elektronischen Risiken für die Informationsinfrastruktur und der Bedrohungen durch Cyberkriminalität. Im umfassenden Sinn wurde das Thema Information Assurance durch die Strategische Führungsübung (SFU) 1997 lanciert. Auf Grund der Vorschläge der SFU und der Arbeiten weiterer Gremien wurden im Jahr 2000 verschiedene konkrete Schritte gemacht. Im Bereich der Information Assurance sind folgende Initiativen im Gang:

- Der Bund nimmt aktiv teil an der Ende 1999 von Firmen unter anderem aus den Bereichen Telekommunikation, Informatik, Banken, Treuhand und Industrie gegründeten

[34] Vgl. Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders: Background paper for the workshop on crimes related to the computer network. Vienna 2000. (www.uncjin.org/Documents/congr10/10e.pdf)
[35] Council of Europe: Draft Convention on Cyber-crime. Final version. Strassburg, 2001.
[36] Delikte gegen die Geheimhaltung, Integrität und Verfügbarkeit von Computerdaten und Systemen (unerlaubter Zugriff, unerlaubtes Abhören, Datenstörung, Systemstörung, Missbrauch von Geräten); computerbezogene Delikte (Fälschung, Betrug); inhaltsbezogene Delikte (Herstellung, Vertrieb und Besitz von kinderpornografischem Material); Delikte gegen das Urheberrecht (Verbreitung geschützter Werke, Software-Piraterie)
[37] Beispielsweise die USA und Deutschland.

Stiftung InfoSurance[38]. Der Bund beteiligt sich mit einer Viertelmillion Franken pro Jahr für vorläufig drei Jahre an der Stiftung. Zudem ist er durch Vertreter verschiedener Bundesstellen, darunter auch vom BAP, in der Stiftung vertreten.

- Im Sommer 2000 hat der Bundesrat das Finanzdepartement beauftragt, ein Koordinationsorgan und einen Krisenstab im Bereich Information Assurance aufzubauen. Dieser Krisenstab soll die Sicherheit der Informationsinfrastrukturen bei Bundesstellen verbessern und bei elektronischen Krisenfällen sofort einsatzbereit sein. Beide Organe arbeiten eng mit vergleichbaren Institutionen aus der Privatwirtschaft zusammen.
- Im Bundesamt für wirtschaftliche Landesversorgung des eidgenössischen Volkswirtschaftsdepartements ist ein neues Milizamt für Informations- und Kommunikationsinfrastruktur geschaffen worden. Dieses kann bei grösseren Schadenfällen aktiv werden.

Im Bereich der Cyberkriminalität im engeren Sinn wurden folgende Schritte unternommen:

- Die ehemalige Bundespolizei (heute der Dienst für Analyse und Prävention im BAP) setzte sich seit 1998 mit Fragen der Cyberkriminalität auseinander. Im Rahmen von Interventionen zur Verhinderung des Zugriffs auf rassistische und gewaltextremistische Seiten wurden 1999 und 2000 sowohl von Bundes- als auch Providerseite mehrere Gutachten zur Strafbarkeit der Internet-Accessprovider verfasst.[39] Während sich der Bund auf den Standpunkt stellt, dass diese Strafbarkeit unter bestimmten Umständen gegeben ist und darauf auch seine Sperrempfehlungen abstützt, weist ein Gutachten der Provider vor allem auf die unsichere Rechtslage hin und sieht einen dringenden gesetzgeberischen Handlungsbedarf.[40]
- In einigen wenigen Kantonen bestehen bereits Polizeieinheiten, die spezialisiert in der Bekämpfung von Cyberkriminalität tätig sind.[41]
- Die Motion von Ständerat Thomas Pfisterer "Netzwerkkriminalität. Änderung der rechtlichen Bestimmungen" vom 14. Dezember 2000 fordert den Bundesrat auf, so rasch wie möglich eine international kompatible Regelung im Strafrecht einzuführen.[42] Der Bundesrat ist gemäss seiner Antwort vom 28. Februar 2001 zwar bereit, eine Ergänzung des Strafgesetzbuches zu erarbeiten, will aber dabei die im Fluss befindliche rechtliche[43] und technische Entwicklung des Internets berücksichtigen. Die Motion ist am 6. März 2001 vom Ständerat und am 20. September 2001 vom Nationalrat überwiesen worden.
- Im Zusammenhang mit den Aktivitäten von Interpol gegen die Cyberkriminalität diente 1998/1999 eine Internet-Monitoring-Stelle (Cybercops) im BAP als direkter Kontaktpunkt in der internationalen Polizeizusammenarbeit. Sie musste allerdings Ende 1999 aus Gründen der Personalknappheit wieder geschlossen werden.
- Die im Juni 2000 im Auftrag der Konferenz der Kantonalen Polizeikommandanten der Schweiz (KKPKS) konstituierte interkantonale Arbeitsgruppe zur Bekämpfung des Missbrauchs der Informations- und Kommunikationstechnik (AG BEMIK) hat im Januar 2001 ihre Empfehlungen dem Auftraggeber unterbreitet. Die AG BEMIK beantragt unter anderem, im Bundesamt für Polizei (BAP) beim Dienst für Analyse und Prävention

[38] www.infosurance.ch.
[39] Siehe auch Staatsschutzbericht 1999 sowie Gutachten des Bundesamts für Justiz vom Dezember 1999 und Positionspapier der Bundespolizei "Die strafrechtliche Verantwortung von Internet Service Providern" vom April 2000. www.admin.ch/bap.
[40] Position der Provider inklusive Gutachten unter www.vit.ch.
[41] Beispielsweise in Genf und Zürich.
[42] Motion Thomas Pfisterer: Netzwerkkriminalität. Änderung der rechtlichen Bestimmungen. Vorstoss Nummer 00.3714 (www.pd.admin.ch/afs/toc/d/gesch/d_mainFrameSet.htm).
[43] Etwa im Blick auf Europaratskonvention gegen Cyberkriminalität (www.conventions.coe.int/treaty/en/projets/FinalCybercrime.html).

(DAP) eine so genannte Monitoring-Stelle, die im Internet systematisch nach strafbaren Inhalten recherchiert, und bei der Bundeskriminalpolizei (BKP) eine Clearing-Stelle zur Anzeige- und Verfahrenskoordination im Bereich Cyberkriminalität einzurichten. Ausserdem sollen entsprechende Analysekapazitäten aufgebaut werden. Momentan werden zwischen Bund und Kantonen die Finanzierungsmodalitäten diskutiert. Eine Einführung der beiden Stellen auf Frühjahr 2002 scheint möglich.

8. Fazit und mögliche Massnahmen

Die moderne Gesellschaft sieht sich durch die Informationsrevolution vor schwierige neue Herausforderungen gestellt. Das Schadenspotenzial, das elektronische Angriffe auf Informationsinfrastrukturen haben, ist immens. Die stetig zunehmende Zahl von Informatiksystemen und die immer engere Vernetzung dieser Systeme untereinander führen zu einer als hoch anzusetzenden Eintretenswahrscheinlichkeit von Zwischenfällen und Angriffen. Daraus ergibt sich, dass die Bedrohung der Gesellschaft im Bereich der Informationsinfrastrukturen als hoch einzustufen ist. Die Zahl der Computer hat im letzten Jahrzehnt stark zugenommen, die Zahl der Hosts im Internet wächst exponenziell und auch die Zahl der Delikte sowie Urteile steigt kontinuierlich. In diesem Kontext ist davon auszugehen, dass auch die Kriminalität im Bereich der Informationsinfrastrukturen und besonders die Cyberkriminalität im engeren Sinn in den kommenden Jahren weiter zunehmen werden.

Zur nachhaltigen Verbesserung der Strafverfolgung von Cyberkriminalität und zur Sicherung der kritischen Informationsinfrastrukturen werden folgende Massnahmen vorgeschlagen:

Internationale Zusammenarbeit, nationale Koordination

1. Bedrohungen für die Informationsinfrastrukturen sind genuin international. Konsequenterweise muss auch die Bekämpfung international koordiniert erfolgen. Dazu sind international harmonisierte Rechtsgrundlagen und eine effiziente sowie rasche Zusammenarbeit von Justiz- und Polizeibehörden über nationale Grenzen hinweg notwendig. Die Teilnahme an internationalen Initiativen ist unabdingbar.
2. Die globale Bedrohung bedingt eine gesamtschweizerische Koordination der weiterhin in die Zuständigkeit der Kantone fallenden polizeilichen Erkennung und Bekämpfung von Cyberkriminalität.
3. Zur Koordination der polizeilichen Arbeit ist die rasche und konsequente Umsetzung der Antrage der AG BEMIK (Monitoring, Analyse, Clearing) zentral.

Qualität der Strafverfolgung

4. Traditionelle Untersuchungs- und Ermittlungsmethoden müssen hinterfragt werden. Ergäben sich daraus neue Ansätze für die Ermittlung und Bekämpfung, bräuchte es die Bereitschaft der Strafverfolgungsbehörden, die neue Methoden zu akzeptieren, damit sie umgesetzt werden können. Dazu sind allenfalls Rechtsgrundlagen zu schaffen, die solche neuen Methoden überhaupt ermöglichen.
5. In der Strafverfolgung sollten vermehrt spezialisierte Einheiten, die flexibel und interdisziplinär arbeiten, eingesetzt werden.
6. Ein gesamtschweizerisch gültiger Standard für die Durchführung von Untersuchungen und Ermittlungen sowie für die Sicherung von bei Straftaten relevanten Daten sollte eingeführt werden. Dies würde zu einer Vereinfachung und Vereinheitlichung der Strafverfolgung führen.

7. Eine stärkere Zusammenarbeit zwischen privatem Sektor und Verwaltung ist anzustreben. Diese würde zu einem Wissenstransfer beitragen, von dem angesichts des hohen technischen Wissensstands, den Ermittlungen gegen Cyberkriminalität voraussetzen, insbesondere die Strafverfolgung profitieren würde.
8. Nebst dem Einsatz der nötigen personellen Ressourcen ist die Anpassung der Infrastrukturen an den heutigen Stand der Technik unabdingbar.
9. Angesichts der rasanten Entwicklung im Informatikbereich sollte den spezialisierten Einheiten in der Strafverfolgung ermöglicht werden, sich mit einem breiten Ausbildungsangebot auf dem aktuellen Wissensstand zu halten.

Prävention und Zusammenarbeit

10. Nur regelmässige Präventionsmassnahmen können das Bewusstsein für Sicherheitsaspekte der Informationsinfrastrukturen bei Führungskräften sowie Angestellen in Unternehmen der Privatwirtschaft und in der Verwaltung stärken. Die vom Bund unterstützte Stiftung InfoSurance erfüllt bereits heute einen Teil dieser notwendigen Aufgaben. Verstärkte Präventionsmassnahmen sind zu prüfen.
11. Die Kooperation zwischen Strafverfolgungsbehörden und Internet Providern ist weiter voranzutreiben. Dabei drängt sich die Beantwortung der Frage nach der Verantwortung der Internet Provider im Zusammenhang mit dem Zugriff auf illegale Inhalte auf.
12. Sicherheitsmassnahmen im Bereich der verwendeten Programme und seitens der Computerbenützerinnen und -benützer beispielsweise bei der Vergabe von Passwörtern sind konsequenter umzusetzen. Dies würde bereits entscheidende Verbesserungen mit sich bringen.
13. Die Einführung von Sicherheitszertifikaten für Programme und Software, die beim Betrieb von kritischen Infrastrukturen zum Einsatz kommt, ist zu prüfen.

Information Assurance

14. Für den Schutz der kritischen Infrastrukturen ist ein Frühwarnsystem einzurichten. Dabei müssten Nachrichtenquellen sowohl beim Bund wie auch in der Privatwirtschaft involviert und ein vertraulicher, rascher Informationsaustausch gewährleistet werden.

9. Quellen / Literatur / Web-Links

Arbeitsgruppe zur Bekämpfung des Missbrauchs der Informations- und Kommunikationstechnik (BEMIK): Massnahmen zur effizienten Bekämpfung des Missbrauchs der Informations- und Kommunikationstechnik. Empfehlungen der Arbeitsgruppe BEMIK. Januar 2001

Atomic Tangerine (weltweit im Bereich Informatiksicherheit und Cyberkriminalität tätige Firma)
www.atomictangerine.com

Associated Press: Internet-Betrugsfälle dramatisch angestiegen. AP 15.1.2001
www.root.admin.ch/root_cgi-bin/agen_aggroup.pl/agen.apd.wirtschaft/20122

Daniel Bircher: Information Assurance für das System Schweiz. Ein Szenario und erfolgversprechende Lösungsansätze. CCG Seminar FA 1.20 2000/2001

Der Bund: Schweizer Internet ohne Aufsicht. Der Bund 23.5.2001
www.derbund.ch

Bundesamt für Justiz: Gutachten zur Frage der strafrechtlichen Verantwortlichkeit von Internet Access Providern gemäss Artikel 27 und 322bis Strafgesetzbuch vom Dezember 1999
www.vpb.admin.ch/deutsch/doc/64/64.75.html

Bundesamt für Polizei: Schlussbericht zum Pilotbetrieb Internet-Monitoring und Konzept zum Aufbau einer Fachgruppe zur Bekämpfung des Missbrauchs der Informations- und Kommunikationstechnik. Dezember 1998

Bundesamt für Polizei: Positionspapier der Bundespolizei zur strafrechtlichen Verantwortung von Internet Service Providern vom April 2000
www.admin.ch/bap/d/archiv/berichte/weitere/2000-05-15-d-internet-isp.pdf

Bundesrat: Schweizerisches Konzept Information Assurance. 22.6.2000

Center for Strategic and International Studies (CSIS): Cybercrime... Cyberterrorism... Cyberwarfare. 2000
www.csis.org/pubs/cyberfor.html und www.csis.org/pubs/cybersum.html

CSIS: Cyber Threats and Information Security. Meeting the 21st Century Challenge. By Arnaud de Borchgrave, Frank J. Cilluffo, Sharon L. Cardash, Michèle M. Ledgerwood. December 2000

Computer Security Institute (CSI): Computer Crime and Security Survey 2001.
www.gocsi.com

Eidgenössisches Justiz- und Polizeidepartement: Staatsschutzberichte 1998/1999/2000

Europarat: Draft Convention on Cyber-crime. Final version, 16 May 2001
www.coe.fr und www.conventions.coe.int/treaty/en/projets/FinalCybercrime.html

Jane Fulford/Mark Furner: Computer Crime. The Risks and simple Rules. In: Der Schweizer Treuhänder. Monatsschrift für Wirtschaftsprüfung, Rechnungswesen, Unternehmens- und Steuerberatung. Spezialnummer Wirtschaftskriminalität. 5/2001, Zürich 2001, Seite 487 - 492

Steve Gibson: The Strange Tale of the Denial of Service Attacks Against grc.com. Last modified 2 June 2001
grc.com/dos/grcdos.htm

Marc Goodman: Why the Police Should Care About Cybercrime. In: Harvard Law School Journal of Law & Technology, Summer 1997

Internet Fraud Complaint Center (IFCC): Internet Auction Fraud. May 2001

www. ifccfbi.gov

Internet Fraud Complaint Center (IFCC): Six-Month Data Trends Report. May - November 2000

Interpol: Interpol Computer Crime Manual. 2000
www.interpol.int

MSNBC: A Brief History of Hacking. MSNBC Research May 2001
www.msnbc.com/news/568036.asp

National Institute of Justice: Electronic Crime Needs Assessment for State and Local Law Enforcement. Research Report. March 2001 (NCJ 186276)
www.ojp.usdoj.gov/nij

Neue Luzerner Zeitung: Neue Piraten entern das Netz. Neue Luzerner Zeitung 6.3.2001

Neue Zürcher Zeitung: Wer kann oder muss Strafbares im Internet verhindern? Gesetzgeberischer Klärungsbedarf bei der Bekämpfung illegaler Inhalte (mit Beiträgen von Hans-Ulrich Bühler/Philipp Kronig, Marcel Niggli und Ulrich Sieber). Neue Zürcher Zeitung 29.5.2001
www.nzz.ch

Marcel Niggli/Franz Riklin/Günther Stratenwerth: Gutachten zur strafrechtlichen Verantwortung von Internet Providern im Auftrag des Verbands Inside Telecom vom November 2000
www.vit.ch/gutachten_isp.pdf

Andreas Ochsenbein/Peter Heinzmann: Strafrechtliche Aspekte des Internet. Kriminalistik 8/9, August/September 1998

Stephen Philippsohn: An Overview of Electronic Crime in the 21st Century. Intersec 10/4, April 2000.

PricewaterhouseCoopers: Wirtschaftskriminalität in Europa. Die Resultate der Schweiz. Juni 2001
www.pwc.com

RAND: The Security Dimension of the Information Revolution. RAND-Conference Belgium, May 2001 (in print).

SearchSecurity: Link-Sammlung zum Thema Information Security/Information Assurance
searchsecurity.techtarget.com/bestWebLinks/0,,sid14,00.html

Sonntagszeitung: WEF war offen für Hacker. Sonntagszeitung 4.3.2001
www.sonntagszeitung.ch

Sonntagszeitung: "Totale Abschreckung auch im virtuellen Raum". Sonntagszeitung 11.3.2001

Sonntagszeitung: Den Nazis das Netz sperren. Sonntagszeitung 15.7.2001

Sonntagszeitung: Cyber-Kriminalität: Bundesamt für Polizei wieder mit Web-Monitoring. Sonntagszeitung 11.3.2001

Der Spiegel: Raub am Geisterschalter. Computerhackern der Mafia wäre es beinahe gelungen, der Bank von Sizilien zwei Milliarden Mark zu entwenden. Der Spiegel 23.10.2000

Stiftung InfoSurance
www.infosurance.ch

Switch
www.switch.ch

Trojaner-Info
www.trojaner-info.de

United Nations: Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders: Background paper for the workshop on crimes related to the computer network. Vienna 2000 www.uncjin.org/Documents/congr10/10e.pdf

Peter Wiedemann: Tatwerkzeug Internet. Ein Überblick über das System und seine kriminelle Nutzung. Kriminalistik 4, April 2000