Twilight Zones in Cyberspace: Crimes, Risk, Surveillance and User-Driven Dynamics

Prof. Dr. Jo Groebel

Dr. Verena Metze-Mangold

Jowon van der Peet

Dr. David Ward

ACKNOWLEDGEMENTS

The authors would like to express their gratitude and thanks to Carlos Arnaldo (UNESCO, Paris), Uwe Kranz (O.C. Intell. & Spec. Knowledge, Europol, The Hague), Jens Walterman (Bertelsmann Stiftung), Marcel Machill (Bertelsmann Stiftung), Omar Leihitu, Marjolein Elshove and Sofia Johansson for their assistance.

ISBN 3–89892–013–5

Herausgeber: Stabsabteilung der Friedrich-Ebert-Stiftung
Redaktion: Klaus Reiff

Friedrich-Ebert-Stiftung, Godesberger Allee 149, D-53175 Bonn

Umschlag: Pellens Kommunikationsdesign GmbH, Bonn
Layout: PAPYRUS – Schreib- und Büroservice, Bonn
Druck: satz + druck GmbH, Düsseldorf
Printed in Germany 2001

Vorwort

Angriffe auf die modernen Informationstechnologien sind weltweit zu einem wirtschaft- und sicherheitspolitischen Problem geworden. Die Internet-Kriminalität entwickelt sich mehr und mehr zu einer potenziellen Bedrohung der öffentlichen Sicherheit wie auch der Informationsgesellschaft insgesamt. Gesellschaft und Politik sind angesichts dieser Entwicklung und dem hohen Abhängigkeitsgrad zentraler Lebensabläufe von digitalen Technologien zutiefst beunruhigt.

Der Präsident des Bundesnachrichtendienstes berichtete jüngst über Erkenntnisse, wonach fundamentalistische Gruppierungen, Anarchisten und Nachrichtendienste ein zunehmendes Interesse an Informationstechniken zeigen. So würden in einigen Ländern Soldaten systematisch als Computer-Hacker ausgebildet. Schon nahezu regelmäßig wird die Öffentlichkeit aufgeschreckt durch Warnungen vor Computerviren, die Millionenschäden verursachen.

Die länderübergreifende aktuelle Diskussion und die Bemühungen um mehr Sicherheit für die Informationstechnologien haben die Friedrich-Ebert-Stiftung veranlasst, ein Gutachten zur IT-Kriminalität in Auftrag zu geben, das die unterschiedlichen Formen des „Cybercrime“ analysiert und zugleich Empfehlungen für Schutzmaßnahmen gegen diese neuartige Form der Kriminalität ausspricht. Dabei wird auch zur „Convention on Cybercrime“ des Europarates Stellung genommen.

Die Friedrich-Ebert-Stiftung dankt den Autoren Prof. Dr. Jo Groebel, Dr. Verena Metze-Mangold, Jowon van der Peet und Dr. David Ward, die dieses Gutachten erstellt haben. Das Original dieses Gutachtens ist in englischer Sprache abgefasst, um es angesichts der Bedeutung des Themas auch international verbreiten zu können. In deutscher Sprache ist eine Zusammenfassung der zentralen Aussagen dieses Gutachtens vorangestellt.

Dr. Jürgen Burckhardt
Geschäftsführendes Vorstandsmitglied
der Friedrich-Ebert-Stiftung

Contents

CYBERCRIME-REPORT – ZUSAMMENFASSUNG 7

EXECUTIVE SUMMARY 13

INTRODUCTION..... 15

CHAPTER I.
THE PROBLEM 17
What is Cybercrime? 17
Lack of Authoritative Quantitative Data 20

CHAPTER II.
INCREASINGLY COMPLEX AND PROFOUND TRANSFORMATIONS OF CYBERSPACE 23
Potential Cyber Criminals 23
The Internet is Vulnerable 24
Convergence of the Internet and TV: Towards Digital Television..... 27
Strategies Towards DTV: Multi-Channel Formats and Cross Promotion..... 29

CHAPTER III.
SURVEILLANCE..... 31
Privacy: Convergence of Public and Private Space..... 31
Risks Inherent in the Use of the Internet: Monitoring and Tracking Capabilities..... 32
Cyber Marketing and Data Mining 34
Cyber Marketing Violence: The Risks to Children 39
Interactive Advertisements and Product Placement..... 39
Collection of Personal Information and Targeted Advertisements..... 40
Interception Capabilities and the State 41
Conclusions..... 42

CHAPTER IV.
NOVEL CRIMES IN CYBERSPACE 43
Hacking and Attacking..... 43
Financial Gain..... 45
Vandalism 46
From Traditional to New Forms of Organized Crime and New Terrorism 48
Cyber War and Net War 48

Net War Actors and Organisation Types…… 51
The World Wants to be Loved: Viruses, Worms and Trojan Horses …… 52
Computer Related Forgery and Fraud: Money Talks…… 57
Computer Related Fraud …… 57
Money Laundering …… 57
Fraud on the Web…… 60
Infringements of Copyright and Related Rights: The Rise and Fall of Napster ……. 61
Conclusions…… 64

CHAPTER V.
CHILD PORNOGRAPHY AND HATE SPEECH…… 65
Child Pornography…… 65
Hate Speech …… 71

CHAPTER VI.
CYBERCRIME AND ITS CONSEQUENCES: LEGAL AND REGULATORY CONSIDERATIONS…… 73
Financial Losses and Economic Impact…… 73
Legal and Regulatory Considerations …… 75
Countering Hacks and Attacks …… 75
Protection of Minors…… 77
Protected and Unprotected Speech…… 79
Security, Conflict and Terrorism…… 79
Privacy and Surveillance…… 80

CHAPTER VII.
A NEW REGULATORY PARADIGM?…… 83
Industry Regulation…… 84
State Regulation…… 84
The Council of Europe Draft Convention on Cybercrime …… 85
Conclusion…… 89

CHAPTER VIII.
CONCLUSIONS: BETWEEN SECURITY AND INDIVIDUAL FREEDOM .. 91

GLOSSARY OF TERMS…… 97

REFERENCES …… 101

APPENDIX…… 111

INTERNET SOURCES …… 133

ÜBER DIE AUTOREN…… 135

Cybercrime-Report Zusammenfassung

Prof. Dr. Jo Groebel, Europäisches Medieninstitut, Düsseldorf/Paris
Dr. Verena Metze-Mangold, UNESCO, Deutschland
Jowon van der Peet, Amsterdam
Dr. David Ward, Westminister University, London

Die Kontaktaufnahme zwischen Mörder und Opfer im Chatroom, der Einbruch in das Computer-System des Pentagon, Kinderpornographie, die Rolle des Internet bei terroristischen Anschlägen, die Verbreitung von extrem schädlichen Computerviren, die Gefährdung großer Unternehmen durch Datenmanipulation: diese alle sind Phänomene der letzten Jahre, die Gesellschaft und Politik außerordentlich beunruhigt haben. Die sogenannte Informationsrevolution wurde zunächst als große Chance für die weitere Gesundung der Wirtschaft und für neue demokratische Möglichkeiten gesehen. Aber mit einer immer weiteren Durchdringung des Alltags durch den Computer und mit einer hohen Abhängigkeit zentraler Abläufe des Lebens von digitalen Technologien nahm auch die Besorgnis zu, dass unsere Gesellschaft hochgradig durch gewollte oder ungewollte Zusammenbrüche des Systems gefährdet sein könnte.

In den letzten Jahren hat sich in Politik, Wissenschaft und Wirtschaft entsprechend eine fortlaufende Debatte über das sogenannte Cybercrime entwickelt, also über strafrechtlich relevante Übergriffe, die Internet und Computer zum Ziel haben, die sich der Informationstechnologie zu bedienen oder die als strukturell neue Kriminalitätsformen überhaupt erst auf der Basis der Digitaltechnologie zustande kamen. Der vorliegende Report, der auf die internationale Diskussion abzielt, systematisiert und beschreibt den Stand der unterschiedlichen Formen von Cybercrime bis zum Jahre 2001 und diskutiert zugleich mögliche Formen des Umgangs damit.

Ein zentrales Problem des Cybercrime ist die Tatsache, das es per Definition länderübergreifend ist sowie die Eigenschaft der digitalen globalen Computernetze hat, anonym und überkomplex zu sein. Damit stößt die strafrechtliche Behandlung des Phänomens da an die Grenzen, wo bisherige Kriminalitätsformen vor allem national behandelt wurden. Eine weitere Herausforderung ist die Tatsache, dass gerade durch die sich weiter entwickelnde Technologie noch keine auch nur annähernd endgültige Lösungsmöglichkeit gefunden wurde. Schließlich steht die Politik vor einer besonders großen Herausforderung, weil die Computerkriminalität die besonders in Europa ausgeprägten Ängste vor einer ungewissen Zukunft und vor Horrorszenarien gut bedient. Zwar wächst

mit der jüngeren Generation eine Gruppe heran, die Cybercrime als das nimmt, was es vermutlich ist, nämlich einen natürlichen Risikofaktor, der mit jeder neuen Technologie – auch in der Vergangenheit – verbunden war und ist, dennoch muss man das Thema auch im Sinne der weiteren gesellschaftlichen Perspektiven politisch ernst nehmen. Keine Entwicklung ist linear, keine Lösung ergibt sich von selbst, und die Annahme, die Informationstechnologie würde automatisch zu einer aufgeklärteren und demokratischeren Gesellschaft beitragen, ist nicht gerechtfertigt. Auch die digitale Gesellschaft der Zukunft muss in jedem Moment aktiv gestaltet werden.

Der Report behandelt unter anderem die Frage, wie Regulierungen, die für nationale Kommunikationsinfrastrukturen und national definiertes Strafrecht gelten, effektiv auf die globale Ebene gebracht werden können. Unter anderem wird die „Convention on Cybercrime“ des Europarats beleuchtet.

Die verschiedenen kriminellen Aktivitäten in der digitalen Welt lassen sich im einzelnen folgendermaßen kategorisieren:

Datensicherheit

Der Schutz der Privatsphäre ist nicht nur im Zusammenhang mit dem Internet zu einem zentralen Thema der Gesellschaft zu Beginn des 21. Jahrhunderts geworden. Während noch vor wenigen Jahren schon die Erfassung einiger weniger Daten durch den Staat politisch fast nicht durchsetzbar war, scheint es heute international fast selbstverständlich geworden zu sein, auch den Zugriff zu intimsten Informationen über andere Menschen haben zu können. Dabei sind die Übergänge zum Missbrauch von Daten fließend. Wenn in Großbritannien hunderttausende von Videokameras nahezu alle öffentlichen Plätze rund um die Uhr überwachen und mit digitalen Gesichtserkennungssystemen zunehmend auch jede einzelne Person jederzeit lokalisierbar ist, so mag das zwar einen hohen Vorbeugungseffekt hinsichtlich herkömmlicher Verbrechen haben, die Gesellschaft kauft sich damit aber eventuell eine Einschränkung aller Bürger mit ein. Noch sind in vielen Ländern der Welt diese Formen der Überwachung gesetzlich verboten, aber es gibt genauso häufig die Diskussion darüber, immer verfeinertere Methoden der Beobachtung einzusetzen. Steht der Begriff Big Brother für eine der harmlosen Fernsehshows, so droht die Gefahr, dass wir dem „echten“ im Sinne Huxleys bereits die Tür geöffnet haben. Neben staatlichen Behörden gibt es ein mindestens so großes Interesse an genauesten Datenprofilen der einzelnen Bürger von Seiten der Industrie. In den letzten Jahren wurden immer wieder neue Softwaremöglichkeiten debattiert, die ganz einfach deshalb nicht verboten waren, weil ihre bloße Existenz noch nicht bekannt war, so z.B. die Platzierung von Cookies auf der Festplatte von PC-Nutzern, die sie als Besucher bestimmter Websites jederzeit wieder identifizierbar machen. Technisch ist bislang jede E-mail-Bewegung lokalisierbar und zurückverfolgbar. Eine Zeitlang schien das sogenannte Data-Mining, das Sammeln von Daten über einzelne Konsumenten und deren Profilerstellung eine der größten Geschäftschancen der neuen Ökonomie. Dabei wurden Aspekte des Datenschutzes oft als eher geschäftsschädigend und hinderlich definiert.

Natürlich ist nicht das Problem, dass ein Kunde gerne und *freiwillig* Informationen über sich preisgibt, aber ein Großteil der Data-Mining Ansätze vernachlässigte unter Missachtung vieler nationaler Gesetze diesen Aspekt der „informationalen Selbstbestimmung". Inzwischen nehmen sich allerdings immer mehr globale Organisationen, so auch die UNESCO, des Themas an und versuchen, praktikable Vereinbarungen zu finden.

Cyberspezifische Kriminalitätsformen

Die meisten verbinden wohl mit Cybercrime Angriffe auf geschlossene und offene Computersysteme, die entweder der willkürlichen Zerstörung und Sabotage gelten oder dem Versuch, auch finanzielle und andere Vorteile durch Datenmanipulation zu erreichen. Die folgenden Zahlen sprechen für sich. In einer Erhebung aus dem Jahre 2000 berichteten 85% der Befragten, dass sie schon einmal Opfer eines Computervirus geworden seien, 71% gaben an, dass jemand unautorisiert Zugriff auf ihre internen Computersysteme genommen hätte. Bedenklich ist dabei, dass sehr viele Unternehmen diesen Einbruch nicht anzeigen, verständlich zugleich, da Kunden eine Gefährdung ihrer wirtschaftlichen oder persönlichen Sicherheit befürchten würden und das Unternehmen für nicht zuverlässig hielten. Die Motive der Angreifer variieren, die Tatsache, alleine und ohne soziale Kontrolle vom „Wohnzimmer" aus erheblichen Schaden anrichten zu können, dient Allmachtsgelüsten genauso wie Frustrationsventilen. Rache, z.B. entlassener Arbeitnehmer, spielt bei vielen digitalen Sabotageakten eine wichtige Rolle. Schließlich kann durch elektronische manipulierte Geldtransfers auch ein erheblicher finanzieller Gewinn erreicht werden. Eine weitere aktuelle Debatte bezieht sich neben der Möglichkeit des globalen Betrugs, z.B. durch falsche Angaben bei Internet-Auktionen oder Ausbeutung von Kindern, auf die Verletzung der Urheberrechte. Im Jahre 2001 gibt es noch nicht das effiziente Geschäftsmodell, gleichzeitig Inhalte online zu verbreiten und die Copyrights sicher zu stellen.

Eine ebenfalls neue Qualität ist die Möglichkeit der digitalen Konspiration. Ein zentrales Problem organisierter Kriminalität und von Terroristen war immer das Entdecktwerden bei persönlichen Treffen und das Einschleusen von V-Leuten. Die globale und anonyme Digitalkommunikation ohne direkten persönlichen Kontakt macht es zunächst erheblich einfacher, kriminelle Akte zu planen. Allerdings gilt hier auch im präventiven Sinne, dass Datenverkehr letztlich immer auch lokalisierbar ist. Es hilft dann jedoch nichts, wenn die Möglichkeit zur globalen Verfolgung fehlt.

In den Bereich der internationalen Sicherheitspolitik reicht die Möglichkeit hinein, sogenannte Cyberkriege zu führen. Blockade und Sabotage von Sicherheitssystemen sind dabei wiederum nur der Ausgangspunkt, das Pentagon wurde bereits mehrfach Objekt digitaler Angriffe. Im Extremfall würden ganze nationale Sicherheits- und Wirtschaftssysteme und die damit zusammenhängende gesellschaftliche Infrastruktur lahm gelegt werden können.

Ein genereller Schwachpunkt der digitalen Welt ist grundsätzlichen Ursprungs: Je komplexer ein System wird, das heißt je mehr gegenseitige Abhängigkeiten und schließlich

Undurchschaubarkeiten entstehen, desto schwieriger wird es, auch größere oder gar Gesamtausfälle dieses Systems noch einschätzen zu können. Das Millennium-Problem hat es gezeigt: Es ist zwar weitgehend gelöst worden, doch dürfte es sehr schwer sein, diese Lösung ausschließlich auf die Milliardendollar-Bemühungen zurückzuführen oder alternativ auf die generelle Überschätzung der Ausgangslage. Vielleicht ist sogar der Vergleich mit der Nukleartechnik zulässig. Wir können es eben nicht wirklich kalkulieren.

Kinderpornographie und Gewalt

Es kursieren international hunderttausende kinderpornographischer Abbildungen im Internet, viele davon allerdings schon Jahrzehnte alt. Das Internet hat diese Form der Kriminalität nicht erst geschaffen, aber es hat durch seine internationalen und vor allem anonymen Verbreitungsmöglichkeiten dem Phänomen eine neue Dimension gegeben. Inzwischen entspricht die Kinderpornographie nicht mehr nur dem Klischee der frustrierten alten Männer, die zu Hause am Computer ihr Privatvergnügen suchen. Es handelt sich vielmehr um einen kriminellen Wirtschaftszweig mit einem hoch entwickelten internationalen Organisationsgrad. Wie etliche Erfolge der Polizei aus den letzten Jahren zeigen, macht das Internet zwar auch die Verfolgung bei guter Koordination leicht, aber eine endgültige Lösung des Problems ist nicht in Sicht. Eine besondere Gefahrenquelle stellen mittlerweile Chatrooms dar, in denen sich Erwachsene und Kinder oder Heranwachsende zunächst virtuell treffen, Vertrauen zueinander aufbauen und schließlich den persönlichen Kontakt suchen. Erste spektakuläre Fälle, (siehe z.B. den Fall Laureen Leistner), wurden inzwischen im Zusammenhang mit Mordanklagen bekannt. Das, was für Kinderpornographie gilt, trifft auch für andere Formen extremer Abbildungen zu. Folterszenen, sadistische Tötungen, besonders brutale Vergewaltigungen von Frauen und jede vorstellbare Art von Sadismus findet sich in den Bildern des Internet wieder. Zwar gibt es inzwischen Filtersysteme (siehe die Ansätze der Internet Rating Association (ICRA), die zumal Kindern dazu den Zugang erschweren, doch ist ein Handicap dieser Systeme, dass sie zunächst des freiwilligen und gekonnten Eingriffs der Eltern bedürfen. Viele Eltern wissen gar nicht um den Computerkonsum ihrer Kinder oder haben gar kein Interesse an den Inhalten. Und so muss man schließlich auch die große Verbreitung rassistischer Angebote über das Internet nennen, die zwar in Deutschland strafrechtlich verfolgt werden, aber in vielen anderen Ländern ohne Sanktionen bleiben. Auch hier stellt sich wieder das Dilemma, Persönlichkeit und Menschenwürde zu schützen, zugleich aber die Freiheit der Meinungsäußerung strukturell nicht einzuschränken.

Insgesamt lassen sich folgende Schlussfolgerungen ziehen:

- Die Informationstechnologie ist bislang erheblich anfällig für Attacken. Die Sicherheit des Internet und anderer digitaler Infrastrukturen ist unzureichend und kann sehr leicht mit vergleichsweise einfachen Mitteln und Basiskenntnissen durchbrochen werden. Neben dem psychologischen und sozialen Schaden hat dies allein in den bekannt gewordenen Fällen Milliarden Dollar Schäden zur Folge gehabt.
- Cybercrime deckt ein breites Spektrum herkömmlicher wie traditioneller Verbrechen ab. Dabei wird die Digitaltechnologie in unterschiedlicher Art und Weise genutzt und

eingesetzt. Schon immer bestehende Kriminalität wie Terrorismus und Kinderpornographie fällt genauso darunter wie Virenverbreitung, Sabotage oder Datenmanipulation. Bislang gibt es allerdings keine allgemein gültige Definition für Cybercrime.

- Hat schon jetzt das Internet in Teilen der Welt eine große Verbreitung, so wird sich mit der Ausdehnung dieser Informationstechnik in den Bereich des Fernsehens und der Telekommunikation hinein eine weitere Vervielfachung der Nutzer ergeben, damit zugleich eine Erhöhung des Risikos, dass immer mehr Menschen potentiell vom Cybercrime berührt werden.
- Die exponentielle Zunahme des Internet ging nicht gleichermaßen einher mit effektiven Präventions- oder Bekämpfungsformen von Seiten der Nationalstaaten. Zwar besitzen auch viele herkömmliche Verbrechen eine internationale Komponente, doch ermöglicht es erst das Internet, konsequent vom Wohnzimmer aus in einem Teil der Welt ein Verbrechen zu begehen, das sich in einem ganz anderen Teil auswirkt. Die Schwelle ist dabei für den Einzelnen oder eine Gruppe erheblich niedriger geworden.
- Cybercrime nimmt weiter zu und es steht zu befürchten, dass viele neue Formen oder neue Auswüchse zunächst gar nicht entdeckt werden oder nur sehr allmählich zu effektiven Sanktionen führen.
- Da, wo die Struktur des Internet und der digitalen Technologie immerhin auch eine digitale Verfolgung ermöglicht, stellt sich zugleich die Frage, inwieweit die Lokalisierbarkeit und Aufspürbarkeit einzelner ihrerseits wieder zu neuem Missbrauch führen können. Sowohl viele Staaten als auch etliche Unternehmensbereiche mögen sich versucht fühlen, immer perfektere Datentransparenz auch gegen den Willen einzelner Bürger zu erzeugen.
- Der globale Aspekt des Cyberspace erfordert internationale Kooperation auf der Regulierungsebene. Ein Ausgangspunkt ist die Selbstregulierung durch die Industrie, zugleich müssen aber auch staatliche und internationale Institutionen eine Kontrolle von deren Wirksamkeit sicherstellen. Selbst wenn Großunternehmen hier schon vorbildliches geleistet haben, muss man immer noch mit berücksichtigen, dass kleine Anbieter notfalls problematische Nischen suchen oder sich Eltern gar nicht erst um den Konsum ihrer Kinder kümmern.
- Meinungsumfragen bestätigen, dass die Öffentlichkeit sich große Sorgen über die Sicherheit der Online-Dienste macht. Diese Sorge gehört zu den Hauptgründen neben Computerangst und wirtschaftlicher Krise, warum sich E-Commerce und Online-Handel bislang weniger schnell als möglich entwickelt haben.
- Eine weitere Sorge der Öffentlichkeit richtet sich auf den Datenschutz. Viele Bürger fürchten nicht zu Unrecht, dass sie durch Internet-Handeln zum gläsernen Menschen werden.

Neben gesetzgeberischen Maßnahmen und internationalen Vereinbarungen erfordert die technologische Entwicklung mehr und einfachere, vor allem eine sachliche Aufklärung

der Bürger. Jede neue Technologie ist mit Risiken verbunden, deren Ausprägung und Auswirkungen zunächst nicht endgültig einzuschätzen sind. Auch beim Cybercrime dürften diese Risiken letztlich beherrschbar werden. Allerdings erfordert dies eine noch bessere internationale Koordination und ein effektiveres Zusammenwirken von Politik, Unternehmen, Bürgern und gesellschaftspolitischen Institutionen. Der Ruf nach höherer Informations- und Medienkompetenz gehört natürlich auch hierhin, doch es kann nicht alleine dem Einzelnen überlassen werden, vorbeugend mit den digitalen Systemen umzugehen. So, wie es neue Formen von Verbrechen gibt, müssen auch neue Formen der Prävention und der Aufklärung entwickelt werden. Hierbei gilt das gleiche, was sich für die „Next-Economy“ herauskristallisiert, eine wirksame Verbindung traditioneller und neuer Maßnahmen. Konkret: Herkömmliche Institutionen wie Staat und Gesellschaft brauchen eine noch höhere Digitalkompetenz, neue Akteure sollten immer noch die positiven Errungenschaften der aufgeklärten und demokratischen Gesellschaft beherzigen lernen.

Executive Summary

The issue of cybercrime has become a pressing concern for nation states in recent years, as more cases of crime committed in cyberspace have reached the attention of the public. The report explores the areas where cybercrime has become a growth industry that exploits the borderless nature of the Internet in order to circumvent national legal agencies. It examines the economic, social and political consequences of this trend in terms of the current regulatory framework. It takes as a reference point the Council of Europe's Convention on Cybercrime and subsequently the report evaluates the need and potential effectiveness of such an internationally binding instrument.

Cybercrime is a growing problem for all States and it can be expected to increase in the near and long term future. It is a criminal activity that encompasses a whole range of criminal activities, some of which have a long history in the offline world and others that are unique to the online world. The international character of computer networks such as the Internet make the criminal activities executed online an international concern – paradigms of regulation developed for national communications infrastructures and nationally based criminal activities that involve electronic media need to be extended into the international domain in order to effectively regulate cyberspace.

The report's main findings are:

- There are serious vulnerabilities in the design of ICT communications that make them prone to intruders. Security on the Internet is therefore insufficient and can be easily overcome with a limited amount of resources and some basic knowledge. This has resulted in serious economic losses that are estimated to run into billions of U.S. dollars.
- Cyber criminal activities cover a wide range of both traditional and novel crimes that utilise new technologies in a number of different ways. The activities, which come under the umbrella term cybercrime, can consist of conventional crimes such as terrorism and child pornography as well as novel crimes such as hacking and computer sabotage. The term covers a number of different activities all associated in some way with exploiting new technologies to aid or commit a criminal offence. There is presently no universal agreement on what actually constitutes a cybercrime.
- With the current developments in television technology the vulnerabilities identified in the Internet, will affect far more people as television moves from analogue to digital delivery capacity, allowing transactional activity.
- The exponential growth of the Internet has left the nation state ill equipped to effectively combat an activity that is potentially global in breadth. Although many tradi-

tional crimes have an international component, the Internet enables individuals or groups to act in one part of the world in order to commit a crime in a country thousands of miles away with minimal resources and in some cases take advantage of the lack of international agreements to escape prosecution.

- Cybercrime is a growing trend and without significant international action to combat criminals who utilise ICT to execute criminal activity, it will continue to evolve into new novel areas.
- The capacity to use new technologies to track and monitor consumers or individuals is significant and poses a threat to individual liberty. Both the State and the commercial sector are potential threats in this area.
- Cyberspace is a globally accessible sphere that requires international cooperation in the regulatory sphere. This includes both self regulation by industry actors, and State regulation that must be developed internationally if it is to have any impact on the current growth of cybercrime.
- Public opinion surveys suggest the public hold a very negative perception of security of online services. This is likely to have a serious impact on the development of e-commerce and transactional activity both online and in new television T-commerce services.
- Furthermore the capacity of online services to collect information on users has supported public suspicion of e-commerce. This is largely due to privacy and safety concerns that could have a very negative impact on the development of economic strategies based on e-commerce.

The findings of the report suggest that it is essential for nation states to collectively develop regulatory instruments, in order that they are suitably equipped to satisfactorily ensure that the security of citizens is guaranteed online, as it is in democratic States in the offline world.

Moreover, distinctions between what is public and private are blurring in cyberspace and as more interactive and transactional services become available through television this historical division could blur even further. As many people are not yet fully aware of the capabilities of new technologies to infringe on their privacy, it is very likely that they are unaware of the risks to which their privacy and personal data are exposed. In this context the State must develop instruments that work to maintain a secure environment in which people can communicate and conduct transactions online. Whilst at the same time respecting, and ensuring, that both the State and commercial actors respect the right of the individual to privacy.

Introduction

Developments in information and communication technology (ICT) are having an increasingly important impact on certain areas of life, in many societies of the world. New technologies in the home and in the workplace have become, for many people an efficient and useful supplement to traditional communication media. The use of computers and computer technology has proliferated in all kinds of spheres of life and today it plays a central role in such diverse activities as banking, transport systems, the financial markets, hospitals and telecommunications. In this respect technology affects all of us, everyday, and in many ways that we do not necessarily take into account. In short information infrastructures have become an integral part of the way society organises a whole range of activities.

Depending on a variety of factors such as the quality of the available telecommunications infrastructure, affordability and reliability of access to ICT networks and the level of information security, society can potentially socially and economically benefit from future developments in the ICT sector. Whilst it is important not to see ICT as a panacea to a whole range of economic and social problems, it is also crucial to recognise the opportunities as well as the threats created by the development of new systems of communication that do not always follow the same spatial rules as other media.

ICT has become a source for generating revenues, job creation, and has to some extent transformed some traditional companies and employment trends. More generally, information and communication technology has also influenced a wide range of other spheres of life ranging from international relations to healthcare and education. In the past decade personal computers, workstations, databases, and mainframes have become increasingly interconnected with distribution information networks. This interconnectivity is increasing and today military networks are connected with financial networks, government networks are interconnected with commercial networks, and a whole set of interconnected systems are linked together through the Internet.

The exponential growth of the Internet on an international level also makes ICT a global issue. The Council of Europe estimates that today there are over 306 million PC users with access to the Internet or similar networks. This is supported with the continued growth of computer sales (over 60 million were sold around the world in 2000) and a proliferation of websites, of which there is estimated to be 28 million (Council of Europe Press Release July 2001). Although user estimates are notoriously difficult to precisely calculate the speed and increase of user take up, is unarguably unprecedented in modern communications. However, even in the developed countries in the Western

world the amount of users of the Internet varies widely. In the U.S. over 50 per cent of the population use the Internet (similar rates are evident in the Nordic countries). In Germany the figure is estimated to be around 30 per cent, the UK 40 per cent and in France and Spain approximately 20 per cent of the population use the Internet (Connectis 2001: 6–7).

As interconnectivity of computer-based (critical) infrastructures increases, the risk of problems affecting one system will also involve other interconnected systems. The issue of information security is therefore likely to become even more important in the near future. As systems become linked to one another, the potential for serious breaches of security will increasingly impact on a wider network of organisations simultaneously.

The objective of this report is to independently examine and assess several risks and different forms of crime in cyberspace, and to raise some points for consideration. As cybercrime concerns a complex and broad set of international issues, it is not possible, given the focus of this report, to give equal weight to all aspects of cybercrime and risk in cyberspace. The report will focus on central areas where activities, which utilise ICT, are seen to pose serious risk to the larger community. These areas are: privacy and surveillance, fraud, theft and security breaches, property infringements and the production and dissemination of harmful content. The categories are by no means exhaustive, but they have been selected as primary areas where ICT has been used to undertake illegal activities and are therefore immediate concerns for regulatory and legal agencies to address.

The current and future available capabilities of ICT, with a key role for the Internet, carry serious risks and also facilitate different forms of cybercrime, covering both public and private life. As broadband networks and developments in the digitalisation of television progress and make possible a greater amount of transactional activity in traditional media forms, the threats identified in this report can be seen to have far more applicability to a wider public. As a consequence, cybercrime and illegal activity that has largely been associated with new media can be expected to increasingly pervade other mediums and spheres of communication. Subsequently the vulnerability of the Internet identified in this report, will become an even more pressing issue.

This report takes the public version of the Draft Convention on Cybercrime, June 2001, and the Draft Explanatory Memorandum to the Draft Convention of the Council of Europe as a frame of reference. The members of the European Committee on Crime Problems agreed to the text on June 22nd 2001 and a preliminarily discussion of the text is expected to be taken up at the Committee of Ministers in September 2001.

Chapter I.
The Problem

The description of cybercrime is problematic in itself in two ways. The first difficulty is to provide a definition of cybercrime, as there is at this point in time no uniform or universally accepted definition. This is unsurprising given the different legal traditions around the world and the fact that cybercrime is used as an umbrella term to refer, partially at least, to a very recent set of activities that have yet to be incorporated fully into national legal traditions around the world.

As developments in communication technologies continues, cyberspace will evolve, at times at a rapid pace of change. In this respect the problem for legislators is that they have to carefully balance technologically dependent legislation with practical concerns, in order to prevent the legal and regulatory systems from running behind developments in a rapidly changing sector. In addition to the difficulties associated with rapid innovation, there is also the problem that cyberspace does not respect geographical boundaries in the traditional sense. As a consequence legislators have to consider which activities are classified as illegal offences within their jurisdiction and will need to develop novel methods to enable them to pursue cyber criminals, who may be active in another part of the world, but nevertheless commit a crime within the boundaries of a sovereign nation state.

The problem of criminal activities that utilise ICT is further amplified by the lack of shared available data on cybercrime, making it difficult, if not impossible at the current time, to assess, in quantitative terms the extent of criminal activities on line. Our lack of detailed knowledge and the absence of reliable data in the area of cybercrime are understandable given the underground nature of many of the criminal activities that are conducted in what this report refers to as twilight zones.

What is Cybercrime?

Given both the novel nature of the Internet and the subsequent growth of traditional crimes that exploit ICT as well new crimes, which have grown in parallel to technological developments in the communications sector, it is unsurprising that a standard, universal definition of cybercrime has not as yet evolved. The disparate range of criminal activities that are committed through ICT have largely been seen as separate criminal activities in the offline world.

The UN Manual on the prevention and control of computer-related crime (hereafter referred to as the UN Manual), provides the following definition of cybercrime: „Com-

puter crime can involve activities that are traditional in nature, such as theft, fraud, forgery and mischief, all of which are generally subject everywhere to criminal sanctions. The computer has also created a host of potentially new misuses or abuses that may, or should be criminal as well" (UN 1994, par. 22).[1]

In July 1996, the UK National Criminal Intelligence Service launched a study of computer crime called Project Trawler. In the study the terms computer crime, information technology crime and cybercrime are interchangeable. Project Trawler defines computer crime as follows: „An offence in which a computer network is directly and significantly instrumental in the commission of the crime. Computer interconnectivity is the essential characteristic" (UKNCIS).[2]

The COMCRIME study, a report analysing the legal issues of computer related crime, submitted to the European Commission (DG for Information Society), follows the definition provided by a group of experts of the OECD, who in 1983 defined the term computer crime as, „Any illegal, unethical or unauthorised behaviour involving automatic data-processing and/or transmission of data" (OECD, cited in Sieber 1998: 19).

Generally cybercrime refers either directly or indirectly to the environment of information systems and cyberspace. The OECD provides a definition of information systems in the Guidelines for the Security of Information Systems. The definition gives an outline of what information systems include:

> „Computer hardware, interconnected peripheral equipment; software, firmware and other means of expressing computer programs; algorithms and other specifications either embedded within or accessed by such computer programs; manuals and documentation on paper, magnetic optical and other media; communication facilities, such as terminal/customer premises equipment and multiplexes, on the information system side of the network termination point of public telecommunication transport networks as well as equipment for private telecommunication networks not offered to the public generally; security control parameters; storage, processing, retrieval, transmission and communication data, such as check digits and packet switching codes, and procedures; data and information about parties accessing information systems; and user identification and verification measures (whether knowledge-based, token-based, biometric, behavioural or other). This definition may include elements that are proprietary or non-proprietary, and private or public. This definition applies to elements whether or not they interact with the data being transmitted by the system or necessary for the operation, use and the maintenance of the other components of the system" (OECD 1992).[3]

The COE (COE 2001b) defines cyber space offences as „either committed against the integrity, availability and confidentiality of computer systems and telecommunications networks or they consist of the use of such networks of their services to commit traditional offences" (COE, Explanatory Memorandum 2001b: 2). The draft Convention defines nine offences in four different categories. These include offences against the confidentiality, integrity, and availability of computer data and systems. The definition of the Council of Europe therefore covers not only computers or computer networks, but also computer data and content issues.

1 http://www.uncjin.org:80/Documents/irpc4344.pdf [as of September 6, 1999]

2 http://www.ncis.co.uk/newpage1.htm [as of 1999, September 29] For the debate on the definition see also: Deutscher Bundestag. Sicherheit und Schutz im Netz. a.a.O., p. 111

3 http://www.oecd.org/dsti/sti/it/secur/prod/e_secur.htm [as of 1999, October 22]

Even taking the few attempts at definition above it is demonstrably clear that not one single definition is agreed upon. All appear to have a number of components in common, but by the same token there are nuances in their interpretations. Subsequently different sets of criteria are established in order to classify exactly what constitutes a cybercrime, with conflicting results. The divergence in definitions however, may not be entirely unhelpful as Sieber (1998: 20) points out; technical (the computer as a tool or an object of crime) and sociological classifications (insider and outsider offences) are of limited value for legal analysis. The benefit of a generic definition is that it leaves the possibility of including new forms of criminal action and behaviour, which might not be illegal at any one point of time.

Any satisfactory concept of cybercrime therefore needs to account for both a set of activities that are already classified as criminal offences, as well as the novel nature i.e. networks and computer systems, of how or where crimes are executed and committed. The central problem is therefore reconciling the location of where the actual crime has been committed with the fact that the victim may be based in another legal territory. It is therefore necessary to develop a definition of cybercrime that allows legal authorities to promulgate legal instruments, in order to be able to apply offline normative legal principles to the online world. This must necessarily include a definition that encompasses the non-tangible nature of cybercrime, the different activities that constitute a cybercrime, and the location (either storage or active communication in real time) of the execution of the crime and the location of the victim.

The term cyberspace is often used interchangeably with the Internet. Although the Internet has grown in prominence, particularly in the public eye, cyberspace comprises more than the Internet alone. According to Hamelink, ICT creates a new reality that consists, paradoxically, of a virtual world, which is commonly referred to as cyberspace. Cyberspace is therefore understood as a worldwide,[4] non-physical space; in which, (regardless of time, distance and location), interactions and transactions between people, between computers and people, and between computers takes place. An important feature of cyberspace is that it is difficult to locate exactly where and at what time a specific transaction is executed. In addition, Hamelink (1999: 23) identifies six spheres where elements of cyberspace can be detected:

- Digital computers (from laptops to expert systems).
- Communication networks that interconnect telephone, fax and computer, with the help of digital electronics.
- Digital electronics controlled transport systems such as cars, trains, airplanes, and elevators.
- Digital electronics controlled monitoring systems, applied in for example chemical processes, the medical sector and electricity providers.

4 As far as ICT and its necessary infrastructure are available and interconnected.

- Digital electronics controlled user tools such as watches, microwave ovens and video recorders.
- Digital electronics controlled robots (independent operating automatic systems).

(Hamelink 1999: 23).

The six elements all involve data processing and take place in the interconnected ICT infrastructure of cyberspace. With the availability, in the near future, of personal digital assistant (PDA) and wireless interconnections of ICT systems, a greater volume of transactions and a wider amount of functions and areas will probably be conducted in cyberspace.

Lack of Authoritative Quantitative Data

Reliable quantitative data that provides a full overview of cybercrime is unavailable. According to the UN Manual, law enforcement officials indicate that recorded computer crime statistics are not an accurate reflection of the actual number of crimes committed using ICT. Two reasons are given for the absence of sufficient data on cybercrime.

The first reason is technological and is based on the enormous storage capacity and the speed of computers, which make it very difficult to detect computer crime- some victims are not aware they have been a victim of a cybercrime, until the moment they have been informed. A second reason is that investigating officials often lack sufficient knowledge and training in the field of electronic data processing and its complex environment.

However, some quantitative data gives an impression of the problem. As of 1996, the Computer Security Institute (CSI) and the San Francisco Federal Bureau of Investigation (FBI) has conducted the CSI/FBI Computer Crime and Security Survey (hereafter referred to as the 2000 CSI/FBI survey). The objective of the survey is to raise the level of security awareness about computer related crime and to evaluate the extent and impact of computer crime in the U.S. In its fifth year, 643 security practitioners working for U.S. corporations, government agencies, financial institutions and universities responded to the survey.

In 1996, 42% of the respondents experienced unauthorised access to computer systems within the previous twelve months. In the 2000 CSI/FBI survey 70% recorded security breaches. Of those who reported their Internet connection as an object of attack, 37% reported intrusions in 1996 compared with 59% in 2000 (Power 2000: 4). For the last four years CSI/FBI have asked respondents to indicate which categories of electronic misuse or attack organisations they have detected in the past 12 months. Some of the results from the 2000 survey include:

- 85% of the respondents detected viruses.
- The number of respondents who reported unauthorised access by insiders rose from 40% in 1997 to 71% in 2000.

- 27% reported distributed denial of service (DDOS) attacks.
- After the percentage of computer system penetration by outsiders increased for three years in a row, from 20% in 1997 to 30% in 1999, it decreased to 25% in 2000.
- 20% of the respondents reported theft of proprietary information.
- 17% of the respondents reported sabotage of data and/or networks.
- 11% reported financial fraud.

(Power 2000: 5).

Some of the results outlined above concur with the findings of the 1999 Information Week Global Security Survey (hereafter referred to as the Global Security Survey). Whereas the CSI/FBI survey only involves respondents from the U.S., the Global Security survey includes other countries, thus providing an international perspective. According to the Global Security Survey, viruses appear to be the most frequently detected security breach and 64% (an increase of 11% from 53% in 1998) of the respondents reported them. This percentage is about four times higher than the next highest category of security breaches and unauthorised access.

When asked who the respondents thought would be the likely source of the breaches, 48% of responses in the 1999 survey, indicated that they suspected computer hackers or terrorists as the leading source of intrusion. This represents an increase of 34% on the previous year. In this context the ‘outsiders’ exchanged places with ‘insiders’ who, in the 1998 report, were perceived to represent the most likely source of intrusions. This is in contrast to the 1999 and 2000 CSI/FBI results where the U.S. respondents still believed employees were the most likely source of attack.

Whereas 32% of the respondents in the 1999 CSI/FBI survey reported computer security breaches to law enforcement agencies, only 25% in the 2000 survey reported intrusions. A fairly substantial decline over a period of only one year, but still a greater percentage than the 17% who reported intrusions three years previously, for the year ending 1997. This still leaves a large population of 44% (compared with 48% in 1999), who do not report intrusions and although there is a decrease in the number of respondents, who don’t know whether unauthorised use of computer systems took place (21% in 1999 and 12% in 2000), there are a significant amount of breaches that remain either undetected or unrecorded (Power 2000: 13).

The reasons organisations did not report intrusions to law enforcement agencies also changed significantly between the publication of the 1999 and 2000 CSI/FBI surveys:

- In the 1999 survey 84% of the respondents indicated negative publicity as the reason for not reporting, 52% of the survey suggested that this was a reason for not reporting offences in the 2000 survey.
- In 1999, 79% of participants did not report breaches because of the likelihood of conferring advantages on competitors. This contrasts with 39% in the 2000 report.

- 13% of respondents were unaware that they could report intrusions. Although this has continuously decreased since the 1997 report, it nevertheless remains significant.

(Power 2000: 13).

In respect of the available quantitative data, it should be noted that it is essential to remain cautious when using statistics on such a dynamic sector. The statistics outlined above provide data largely on trends in the U.S. and some indication of the international situation. To understand cybercrime and the risks posed by illegal activities in cyberspace, it is also necessary to go beyond quantitative data and analyse the various dimensions and dynamics of cybercrime, and engage with how these activities affect economic, political and social structures.

Chapter II.
Increasingly Complex and Profound Transformations of Cyberspace

According to Sieber (1998) the discussion about computer misuse has its roots in the 1960s, where the dangers posed to privacy by the development of computer storage and distribution capacity, and the risk of privacy infringements were raised. The initial interest was followed by a scientific focus on computer specific economic crimes in the 1970s. The second wave of research concentrated on economic offences, especially those involving computer manipulation, computer sabotage, computer espionage, and software privacy. Since the 1980s, with the growth of Internet connections, interest in illegal and harmful content (i.e. child pornography, and hate speech) and other offences related to content distributed on computer networks has increased.

Currently, the issue concerning risks to privacy has resurfaced. In the previous discussions in the 1960s, concerns existed about the protection of citizens' privacy rights against State violations. However, today the debate has shifted to include the commercial world and company and client privacy. Threats to individual liberty today encompass wider legal notions, which recognise corporations and organisations as having certain rights as legally established undertakings.

Potential Cyber Criminals

The UN Manual suggests that computer related criminal behaviour can originate from a broad range of groups in society. The age of offenders differs widely and their skill level varies from novice to professional. It states that any person with a limited skill base, motivated by the technical challenge, by the potential for gain, notoriety or revenge, or by the promotion of ideological beliefs, is a potential computer criminal (UN 1994: Par. 3.1).

The category of cyber criminal includes a number of identifiable groups, which can be understood in terms of the activities that they undertake. These include hackers (a category consisting of phreakers and crackers), child pornographers, criminal organisations, terrorists and individuals operating alone.

Furthermore, many cases of Internet terrorism, espionage and sabotage almost all involve aggressive actions by individuals or small groups. By the same token National Security Agencies are responsible for a growing percentage of these sorts of acts, especially in cases of information warfare. Whereas the public is rarely informed about the actions of

the latter group of offenders, other kinds of threats carried out by organised criminal groups, have become a prominent subject of concern for prosecutors and public debate.

In addition, cyber criminals can include employees. In the beginning of the 1980s, it was already evident that employees could play an important role in computer crime (Hearnden 1991: 419). Various studies have investigated the potential risks of employees exploiting internal access to computer resources and utilising them to commit a criminal action. In the 1999 CSI/FBI survey respondents were asked to rate the likely sources of computer related attacks. Dishonest and discontented employees were reported as a likely source by 80% of the respondents. Unauthorised access from inside was reported by 55% of the respondents, an increase for the third consecutive year running.

In the final analysis potential offenders can include any person with a degree of skill, motivation and the necessary resources. Potential offender groups could include religious sects, groups of political terrorists, employees, computer youth cultures, traditional and new groups of organised crime and State organisations, as well as just about anyone else that has access to a computer and some knowledge of networks.

The Internet is Vulnerable

The Internet offers many opportunities in varying spheres of public and private life. Unfortunately, the risks and vulnerability of the security of the Internet is under publicised and there is very little public information available on this area. A vulnerability is defined by Longstaff et al (1997) as „a weakness that a person can exploit to accomplish something that is not authorised or intended as legitimate use of a network or system" (Longstaff et al 1997).

The Internet has several characteristics that leave it prone or vulnerable to exploitation from a number of sources. Its apparently rapid developmental rates, coupled with its close relationship with technological innovation, its openness, and the original design of the protocols (which have not been designed to account for security) leave the Internet particularly vulnerable to exploitation and criminal activity.

Albert, Jeong and Barabási (2000) identify two kinds of networks; homogenous exponential networks[5], and the more naturally occurring, inhomogeneous scale-free networks,[6] such as the World Wide Web and the Internet. The researchers found that the inhomogeneous connectivity of scale-free networks helps make them robust and tolerant of random failures and malfunctions. With scale-free networks they conclude that, „despite frequent router problems, we rarely experience global network outages or, despite the temporary unavailability of many web pages, our ability to surf and locate information on the web is unaffected." However, the error tolerance of scale-free networks has a serious disadvantage when it comes to attack survivability as „the diameter of these networks increases rapidly and they break into many isolated fragments when the most

5 These are composed of various nodes (or points) that have roughly the same number of links.

6 These have complex structures in which most nodes have just one or two links.

connected nodes are targeted" (Albert, Jeong and Barabási, 2000). The structural weaknesses of the web and Internet, rooted in their inhomogeneous connectivity distribution, therefore seriously reduce their attack survivability. An individual wishing to exploit these weaknesses by seriously damaging important nodes, such as key Internet routers or websites and pages, could cause significant disruption or damage.

The Internet also allows attacks to take place in quick, easy and inexpensive ways, and subsequently attacks are difficult to detect or trace. The physical location of an attacker could be anywhere in the world and can easily be disguised. Moreover, due to third generation (3G) telecommunication infrastructures such as GPRS and UMTS and web enabling devices, e.g. WAP-phone, I-mode, handheld, personal digital assistant (PDA) the Internet is (partly) becoming wireless available, making the location of an attacker even more difficult to identify and locate.

It is not only the evolving and changing nature of technology that makes security measures difficult, but also attackers are continuously developing new attacking tools and techniques, rendering security solutions temporary. In August 1999, an eighteen year old Israeli consultant released a report, entitled 'The Internet Auditing Project' which to date is one of the largest surveys of Internet security. Nearly 36 million Internet hosts worldwide were probed with the help of homemade scanning software, over a period of eight months. With the help of the Bulk Auditing Security Scanner (BASS), UNIX systems were specifically searched for 18 widely known security vulnerabilities for which vendors already provided patches and other solutions. About 450,000 servers showed vulnerabilities, among them banks, e-commerce websites, nuclear weapons research centres, and even computer security companies. Although this involves less than 2 percent of the total number of servers, the report states that:[7]

- Even though 2 percent is a small amount, it is still enough to create significant disruption.
- An organised and well-funded group could develop software that could potentially take control of an impressive arsenal of computers connected to the Internet.

Since its release The Internet Auditing Project report has generated considerable interest from information security professionals. But some experts say that despite its significance, it is unlikely to get companies to take defensive action. At the end of January 2001, PGP Security, a unit of Network Associates, detected high-risk vulnerabilities. The flaws concerned versions (4 and 8) of Berkeley Internet Name Domain (BIND) software, the most commonly used implementation of Domain Name Servers (DNS) software. Organisations connected to the Internet depend on DNS systems to allow Internet users to make use of domain names such as – www.eim.org –, to translate those host names into numeric IP addresses, and to enable computers to communicate. The CERT[8]

7 http://www.internetnews.com/intl-news/article/0,1087,6_184381,00.html [as of 1999, October 4]

8 Formerly know as Computer Emergency Response Team at the Carnegie Mellon University's Software Engineering Institute (CMU/SEI).

Coordination Centre estimated that more than 80% of the domain name servers on the Internet were vulnerable to attack. Attackers could have gained control and executed change in the mapping of domain names by changing and rerouting numeric addresses. CERT claimed that as a result, Internet traffic such as web access, email, and file transfers could be redirected to arbitrary sites chosen by an attacker, and access could be disabled to or from targeted Internet users. The CERT/CC report recommended system and network administrators to upgrade their BIND versions immediately.[9] However, recent history suggests such advice is not automatically followed. Since 1997, CERT has described flaws in BIND and supplemented this with information and advice on upgrading and preventing exploitation of the vulnerabilities. Despite the recommendations many system and network administrators still have not upgraded their versions.[10] Whereas prior flaws in BIND have been exploited, the media attention of the recent findings were used to entice visitors of a popular security discussion board, Bugtraq,[11] to download a posted script, which promised it would compromise a recently discovered hole in BIND (Delio 2001). The offer actually materialised to be a hoax, as when people attempted to download and run the computer code, it launched a Denial of Service (DDOS) attack against Network Associates (the company who discovered the BIND vulnerability), in the hope of flooding its servers with large amounts of useless data and thereby disabling it.

Longstaff et al (1997) also note that a significant amount of Internet traffic is not encrypted, thus, can infringe the four basic aspects of security: authentication, confidentiality, integrity, and non repudiatability. As a result security of websites may be affected by another site over which it has no control over, for example, by a packet sniffer that is installed at one site but enables the intruder to collect information about other domains.

As hosts and sites often lack full security measures before going online, this naturally makes them vulnerable to attacks. The rapid growth and use of the Internet is accompanied by rapid deployment of network services. Often, these services involve complex applications, which are not designed, configured, or maintained securely. In the rush to get new products and services to the Internet market, developers do not adequately ensure that previous mistakes will not be repeated, or the new products will not create new vulnerabilities.

Finally, there is a gap between the demand and supply of well-trained and experienced network/computer security professionals who develop defensive software. This ultimately means that inexperienced or less qualified people are employed developing security measures, leaving opportunities for attackers and possible intruders with greater expertise in this area (Longstaff et al 1997).

9 http://www.nytimes.com/reuters/technology/tech-security-so.html [as of 2001, January 30]

10 http://www.cert.org/advisories/CA–2001–02.html [as of 2001, February 14]

11 http://www.bugtraq.com

Convergence of the Internet and TV: Towards Digital Television

The construction of broadband delivery pipes and the development of cable, terrestrial digital television (DTT), Digital Satellite broadcasting (DSB) and video streaming via the telephone line with the help of the IP-protocol (XDSL), ADSL, all enable greater interactivity between the producer and consumer of content-based commodities. In addition, with digitalisation, the same vulnerabilities identified above, in reference to the Internet, will become more applicable to digital TV (DTV) sets or set-top boxes. With interactive television (ITV) or Digital television (DTV) broadcasters will have the technological ability to:

- Broadcast in high definition television (HDTV)
- Data cast large amounts of information
- Offer a broader range of enhanced interactive programming
- Facilitate transactions between retailers and consumers

In the long term there might be a possibility that prime time will cease to exist with the deployment of DTV devices such as interactive digital cable boxes and digital video recorders (DVR) or personal video recorders (PVR) like TiVo[12] and ReplayTV.[13] TiVo, for instance is a technology that allows viewers to pause live television, easily record their favourite television programme by name, subject area or programme genre. Through a set-top box that can record up to 30 hours of programming, or more in some cases, the viewer is given far greater flexibility in when they choose to watch a television programme. Generally, a DVR service like TiVo, allows users to time-shift TV programmes to create their own schedule. This kind of technology allows far greater consumer flexibility and although it may only supplement generalist television channels in the near future, in the longer term it may play an increasingly central role in the way people package and consume audiovisual material.

At the present time the TiVo box costs several hundred dollars to purchase. In addition there are a number of charging options, which a consumer can select from, consisting of a monthly subscription fee of US$ 9.95, an annual charge of US$ 99.95, or a lifetime subscription fee of US$ 199. TiVo Inc. has alliances with major media and technology companies, including its equipment vendors, Philips and Sony, General Electric/NBC, DirecTV, and a US$ 200 million investment from AOL Time Warner. In January 2001, Microsoft announced the launch of its UltimateTV[14] service, which integrates DirecTV programming, digital video recording, live TV controls, interactive television and Internet access. In February 2001, Sonicblue[15] acquired ReplayTV, a primary competitor to TiVo (Martin, 2001). Other kinds of developments include InterVideo Inc. who have established a cooperative venture with Intel, to enable interactive HDTV viewing on per-

12 http://www.tivo.com

13 http://www.replaytv.com

14 http://www.ultimatetv.com/home_hybrid.html

15 http://www.sonicblue.com

sonal computers. The company is developing technology that enables high quality digital recording of TV broadcasts to hard drives or other storage devices. InterVideo will help integrate Intel's standard-based interactive TV technology with its own HDTV playback software, WinDTV. Allowing broadcasters to add interactive content and data to a broadcast video stream.[16]

Developments as stated above indicate that plain metrics of audience size and television schedules, as we currently know them, will to some degree change and a new business model for television may emerge for DTV. But it should be stressed it is difficult to predict the actual diffusion or impact of new technologies. In the UK for example the highly ambitious OPEN service developed by BSkyB, BT and others, has demonstrated that consumer demand for these services may not match over confident forecasts for the technology. Many forecasts are precarious, given the rapid climate of change that the ICT sector exists in. One vision of the near future is described by Forrester research, who predict that in the next five years DTV devices and new content packages will dramatically transform how viewers consume television programmes. In five years they forecast that in the U.S. alone, smarter devices will create US$ 25 billion in new revenues from DTV audiences interacting with their TV services. This forecast must be taken with caution and although new revenues will become available, the extent that they will transform television consumption is probably a long, rather than short term question, that will not only be determined by the capacity of technology to provide new services.

Another possibility for interactive TV is to bring streaming images and sound to the computer via the web user. This audio-video technology has been developed by hello-Network.com, and it allows users to stream high-quality images and sound over the Internet without downloading, installing or upgrading special software. As video files are so large they cannot be downloaded as complete files without broadband delivery systems; a way to circumvent this problem has been developed where the files arrive over the Internet in fragments and are collected, put together and shown on a web user's computer player. This results in a relatively steady movement of data and images, as fragments of the files reach the computer and are processed.

According to Strategy Analytics an estimated 38 million homes worldwide will have access to interactive digital television services by the end of 2001, a large increase on the 20 million homes that have access to interactive television today. Western Europe accounts for 62% of the viewers in 2001, North America 18%, Asia-Pacific 10% and Latin America 1%. With regard to the distribution of channels, 74% of the audience use a satellite-based service, 21% cable and 5% terrestrial. By the end of 2001, the top leading European markets include the UK where 40% of homes will have interactive digital television, followed by Denmark (25%), Spain (23%) and Sweden (22%). Strategy Analytics predicts that by 2005, 625 million people will have access to DTV services.[17] This adoption of DTV will be equally gradual and complex and it will take many years to reach

16 http://www.itvreport.com/news/1100/111300intel.htm [as of 2001, February 19]

17 http://www.strategyanalytics.com/press/index.html [as of 2001, February 27]

anything like full penetration even in the developed world. It is predicted that it will be at least 2008 before the majority of homes in the U.S. are equipped with DTV devices. In the early days of the transition from analogue to digital, most consumers will opt for the less expensive set-top box, in combination with existing analogue receivers, rather than expensive digital TV sets which will slow down diffusion.

Strategies Towards DTV: Multi-Channel Formats and Cross Promotion

At the present time the telecommunications infrastructure is not fully digitised and the penetration of digital receivers in the mass market has not been achieved to the degree of over optimistic forecasts, there is, however, already a trend towards multi-channel formats, cross-promotion and multi-channel marketing.

The format of the real life soap 'Big Brother' is one example of this. The really novel component of Big Brother consists of the multimedia platform that is exploited by the programme. The TV programme was, (and still is in the second run of the programme in some countries) supported by Big Brother's website[18] offering an online platform to the audience as a complement to the television programme. During the series viewers are able to watch the participants of the TV programme in their Big Brother house 24 hours a day online. A number of other features are also available, allowing viewers to interact by nominating the least popular members of the house, as well as to communicate with other Big Brother fans.

Game shows could also be used for the cross-promotion of certain programmes, channels or formats. The launch of the interactive version of the television game show Who Wants to be a Millionaire, the internationally popular quiz first broadcast by the UK broadcaster ITV in 1998, has been announced in 2001 and will be available online. ITV2, ITV's sister digital channel, will launch a new service allowing digital TV viewers to simultaneously play along with the programme as they watch. The online games will be available on ITV2's website.[19] ITV's main owners, Granada and Carlton Television, have a stated aim of cross-promoting the ITV brand across different platforms.[20] It is also very likely that other broadcasters will follow this strategy to promote programmes across channels and mediums.

The music channel MTV's project MTV360 integrates its two cable channels with its website in order to create 'a multimedia version of the MTV brand.' MTV aims to persuade cable operators to expand the distribution of a second MTV channel, MTV2. Music videos will continue to appear on MTV, but the entire programming format for MTV2 will be videos. The music channel intends to schedule programming across its cable channels and its website, directing viewers from one platform to another, and selling all three platforms to the same advertisers. An example of cross-promotion involves the

18 http://www.big-brother.nl/

19 http://www.itv.co.uk/

20 http://www.wired.com/news/business/0,1367,42651,00.html?tw=wn20010327 [as of 2001, March 27]

Dave Matthews Band on MTV's daily music show, 'Total Request Live.' During the show, viewers were directed to MTV2, which was playing the complete collection of music videos the band had produced to date, whilst also offering links to MTV.com, where the audience could access a free download consisting of a cut from the group's new album.

Chapter III.
Surveillance

Privacy: Convergence of Public and Private Space

In the real world, physical cues such as closed doors, locked properties, and sealed envelopes remind us to respect privacy and help us to clearly distinguish between public and private spaces. In cyberspace, the physical sign posts do not always apply. The Lack of clear cues between privacy and publicness suggests the distinctions between what is public and private are blurring and for most people it is unclear what risks their privacy and personal data are exposed to, in the online world.

Koekoek et al (1999) conducted a comparative study[21] on information and privacy in the context of constitutional law. According to Koekoek et al, privacy has four dimensions 1) physical privacy 2) spatial privacy 3) data privacy 4) relational privacy. With the increasing capabilities of ICT there are increased possibilities of infringements on the private lives of citizens. Koekoek et al outline some developments that could constitute risks to privacy, in four central areas:

- Physical privacy:
  In fighting crime and diseases there are more possibilities to exploit ICT and they are being utilised in a number of areas, for example DNA data collection. The U.S. and Great Britain are setting up DNA data bases.
- Spatial privacy:
  Due to miniature eavesdropping and other equipment, it is becoming easier to listen into or spy on someone's home.
- Data privacy:
  Developments in database technology; knowledge discovery in databases (KDD) and linking of databases are relevant for this dimension. The latter involves relating databases that contain personal data in order to make electronic exchange possible.
- Relational privacy:
  Concerns the protection of correspondence. This dimension of privacy is being threatened because citizens are being restricted in their choice of which person they want to communicate with.

(Koekoek et al 1999: 45–46).

21 Conducted for the Dutch Commission Constitution in the digital era. The sample of the research included constitutional states (emphasis on the role of the legislator) such as France, Germany, Sweden and the Netherlands, and 'rule of (common) law' countries (emphasis on the role of the judge) such as Canada, Britain, South Africa and the United States.

The Privacy Information Centre in Washington warns about the increasing commercial interest in the potential of ICT and they subsequently take the view that in the current situation, technology offers the possibility to undermine privacy rights. Databases can be commercially exploited as more personal ways of communication and monitoring systems become more extensive. Infringements can take place in three ways: violation by political and commercial powers, by individuals who are not aware of their rights and by contracts between partners with unequal status of power (Agre & Rotenberg 1997).

Risks Inherent in the Use of the Internet: Monitoring and Tracking Capabilities

The open environment of the Internet therefore creates significant security risks, which also involves risks related to online privacy of Internet users. The Data Protection Working Party, an independent EU advisory body on data protection and privacy, have produced a comprehensive document[22] (hereafter referred to as the DPWP Document) on risks of online privacy. The report offers a novel approach to online privacy risks and identifies a number of areas where privacy may be infringed inter alia 1) technical aspects of the Internet 2) email 3) surfing and searching 4) cyber marketing.

The technical ability of ICT to monitor consumer behaviour is great. Invisible hyperlinks remain hidden from the eyes of Internet users. A website can include an invisible hyperlink to an image located on the website of an Internet advertising or cyber marketing company. In this way a cyber marketing company will have detailed knowledge of the relevant page before sending a banner.

Cookies can also provide a detailed record of user movements around the web and can give an insight into a user's interests, consumer behaviour and movements online. Cookies are also useful in order to make use of certain Internet services or to facilitate surfing. For example, if a user places an order (e.g., books, music CD) on a page, this user information can be accessed when the user arrives at the transaction page. In this way, websites recognise a particular user on any subsequent visits to the site. Each time the visitor returns, the site can retrieve any information it wishes from the user, including preferred language, password information, or the user's interests and preferences, as indicated by the electronic trail which was left by accessing items or documents on previous visits. Usually website operators can only access their own cookies, which gives them a fairly limited picture of how a user acts online. However, in 2000 the largest Internet advertising company DoubleClick's attempt to acquire Abacus Direct, a marketing company with a data base on users' personal details and consumer profiles of approximately 90% of US households- allowing DoubleClick to cross reference the cookies with a user's real identity which represents a far more sophisticated method for data collection on consumers.

22 http://www.europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp37en.pdf [as of 2000, December 4]

Email data is valuable information that includes personal data on the Internet user. Email addresses can be obtained in several ways, inter alia:

1. The provider of the email client software, which is bought or obtained for free, could ask the user for registration.
2. From the client's software in which a code is built which will transmit an email address to the software provider without consent and knowledge.
3. From some browsers which can be configured to send the email address as an anonymous password when opening FTP (File Transfer Protocol) connections.
4. Web sites can directly request the email address from visitors, for example, in the case of a purchase order.
5. From interception during the transmission of a message.
6. From some browsers. There have been reports of security flaws that allow a site to know the email addresses of visitors. This can be made possible via, for example, JavaScript.

(DPWP Document 2000: 32).

When the Internet user is surfing the web data is generated and stored in different parts of that process. In November 1999, it came to light that the world's most popular (with 12 million registered users) software for listening to digital music through the Internet, 'RealJukebox', secretly transmitted information to the company's headquarters in Seattle. The data included details of what music each consumer listened to, how many songs were copied, and a globally unique identifying number (also called GUID) that could be used to identify a customer.

At the end of 1998, the world's largest manufacturer of microprocessor chips, Intel, started building Processor Serial Numbers (PSN) into its new Pentium III chips. The only computers that do not have PSN are Apple and machines built before the end of 1998. PSNs are a unique, unchangeable number built into the computer, which can be used to build up personal databases (i.e. what is purchased online, what programs are used by the system) and can be scanned whenever the computer is connected to the Internet. This allows marketing bureaus that are active in cyberspace to have electronic robots (applets) operating within web pages. When a web page is visited, the electronic robots can access systems and start running on the computer, in order to collect data. According to Intel, it has introduced a tool that allows users to switch off the PSN, but in reality the switch does not really work. In February 1999, a group of German computer experts managed to show that the serial number could be switched back on without the user's knowledge (Campbell 1999).

Table 1: Most relevant data generated and stored when online.

	Data generated and/or stored	Remarks
1. Telecom provider	Traffic data of connection to ISP	May be the same party as ISP
2. ISP: Network Access Server	CLI IP-address Session data	
3. ISP: Proxy	Web pages visited by IP-address at a certain time	
4. Routers	IP-address	
5. Websites	IP-address Previous page URL Session data (time, type of transaction) Name and sizes of files transferred Cookies	Assembled in the 'Extended Common Log File'
6. Portals	Collective information about visits to the websites it refers to cookies	Possibility of creating full profiles of users (communication and behavioural data of the user available to the ISP)
7. Service providers	Collects log analysis from websites Data/profiles from websites accumulated via cookies Search engines: keywords entered by the Internet user	NedStat DoubleClick

Source: EU Data Protection Working Party (2000).

Surfing computer networks like, for example, the World Wide Web on the Internet, generates enough information in itself. Whenever a web page is visited, certain header information is made available which can include the client's (the user's computer) IP address, from which the domain name and the name and location of the organisation who registered a specific domain name can be determined, through the Domain Name System (DNS) as well as other details of the user.

Furthermore, whenever a user browses through a site, click stream data such as the web pages visited, the time spent on each page and information sent and received can be recorded. Many commercial websites request users' personal data (i.e. name, address, telephone number at home or work and email address), through registration or subscription forms. Sometimes data such as age, sex, marital status, occupation, income and personal interests are collected on entry to websites. In addition, when a consumer would like to purchase a service or product, the person is required to disclose credit card details such as card type, number and expiry date.

Cyber Marketing and Data Mining

In the private sector it is easy to merge data from various commercial databanks, and user profiles can be made from Internet browser records. It becomes easy for marketers

and advertisers to target groups with spamming or other cyber marketing activities such as personalised DTV advertisements. The data is of increasing value to companies and can give a detailed profile of a user, and companies and advertisers can use this in a number of different ways.

DTV broadcasters have the increasing possibility to use techniques to collect a user's personal data and viewing behaviour via a connection to a website, an online service, or other IP based interactive platforms, and to use relevant information for data mining. Future strategies could include:

> „Targeted networks like Discovery will embed commerce in programming while real-time information providers like CNN will embed codes in their content so that smart devices can reassemble and manipulate the data. Broadcast networks will pursue product placement and divide programming into two categories – mass audience with dramas like ER and interactive-friendly programming, such as game shows and sport. Advertisers will target individuals based on the viewing data collected by smarter TV devices, raising privacy far beyond today's Internet data collection debates"
> (Forrester Research, Press Release 2000).[23]

In addition to Forrester Research's example, interactive commercials distributed in New York City collected personal information from viewers buying a DVD promoted in a Disney commercial. Assigning unique identifying numbers to DTV set-top boxes could also make possible the creation of a valuable customer profile. Enabling a broadcaster, or third party, to monitor viewing behaviour, in order to obtain data on how long a viewer watches a particular television programme, whether they link from the television programme to a website, and what is clicked on at the site. This information can be used to target commercials to the viewing audience.

The Privacy Foundation[24] and the University of Denver Privacy Centre examined TiVo, one of the digital video recorders available.[25] TiVo collects both a subscription fee and information about the programmes that home viewers record and watch. In August 2000, Nielsen Media Research and TiVo announced a strategic agreement to enable opt-in audience measurement through the TiVo service. According to the findings of the privacy foundation and the University of Denver Privacy Centre, TiVo is able to carry out a number of functions that include tracking consumer behaviour and identifying viewing habits.

23 http://www.forrester.com/ER/Press/Release/0,1769,366,FF.html [as of 2001, February 19]

24 http://www.privacyfoundation.org

25 Recommendations to TiVo Inc. are available at: http://www.privacyfoundation.org/privacywatch/reports

BOX – 1
Digital viewing: Who is watching who and what?

During a period of four months, researchers of the University of Denver Privacy Centre and the Privacy Foundation conducted an independent investigation of the TiVo device, a digital video recorder (DVR). The researchers reported the following findings.

Information gathering by the TiVo-DVR

During TiVo installation, the installer connects the TiVo unit to a cable TV feed or other video source, a television, and the home phone line. The home user then controls the television exclusively through the TiVo remote control.

During an automatic daily phone call, the TiVo device receives an updated copy of the most recent TV schedule from computers at TiVo headquarters. But during the same phone call, the TiVo device also transmits information to TiVo headquarters. At least two different types of information are transmitted: a *diagnostic log file* and a *viewing information file*.

The Diagnostic Log File

The diagnostic log file (a 'syslog') contains various debugging and system status reports, such as memory consumption, user interface response time, modem communication records, enclosure temperature, and enclosure fan speed. Here are some sample lines from the diagnostic log:

```
Jan 13 06:29:44 (none) fancontrol[54]: The current board temperature is 41
Jan 13 06:29:44 (none) fancontrol[54]: Setting the fan speed to 9
Jan 13 06:39:44 (none) fancontrol[54]: The current board temperature is 37
Jan 13 06:39:44 (none) fancontrol[54]: Setting the fan speed to 0
Jan 13 17:42:10 (none) LogTime[94]: WatchTV: change the channel: 0.015 sec
Jan 13 17:42:55 (none) LogTime[94]: Lineup: update the OSD: 0.949 sec
Jan 13 17:42:56 (none) LogTime[94]: Lineup: arrow up/down: 0.011 sec
Jan 13 17:42:57 (none) LogTime[94]: Lineup: arrow up/down: 0.009 sec
```

Even though the diagnostic log does not indicate which shows are being watched by the home viewer, entries like the last lines above do indicate that someone was manipulating the TiVo remote control at 5:42 P.M. on January 13.

The diagnostic log contains an enormous amount of information about the TiVo device's internal processes. On one day, for instance, we observed almost 100 pages of information being deposited in the diagnostic log. The researchers *are not aware of any other consumer device that routinely transmits so much operational information to corporate headquarters*.

Viewing Information File

The viewing information records transmitted to TiVo headquarters look like this in their raw form:

```
980389559|WatchTV|recorded|KDVR|3134603|980127000
```

The two numbers beginning with 980 are timestamps that count the number of seconds that have elapsed since midnight on January 1, 1970, and the number 3134603 identifies a specific television program. This record can be interpreted as:

„On Wednesday, January 24 2001 at 7:26 pm, the home viewer began watching an episode of *King of the Hill* that was originally recorded on Sunday, January 21 2001 at 6:30 pm on the KDVR station."

Also TiVo the following transmitting viewing records were observed:

```
980389520|WatchTV|live|IFC|27666|980384400
980389546|MWEvent|tyTivo
980389550|MWEvent|tySurfDown
980389565|MWEvent|tyVolumeUp
```

The first line above reveals the home user tuning in the movie *My Own Private Idaho* on the *Independent Film Channel (IFC)*, and the three lines below it correspond directly to pushing buttons on the TiVo remote control.

Viewing Information: Anonymous or Not?

TiVo describes this practice as a 'very sophisticated mechanism' to ensure that the subscriber information cannot be linked with the „anonymous" viewing information. However, the viewing information file is nonetheless transmitted during a session identified by the home viewer's TiVo serial number. In fact, this serial number is transmitted multiple times during the single phone call. TiVo receives all of the information necessary to attribute the viewing information to a particular subscriber during this phone call but gives no indication of this fact in any of its documentation. Therefore, the home viewing information can only be truly anonymous when TiVo headquarters intentionally treats it as such. TiVo's current 'anonymization' procedure does not change that fact.

Transferring the Information

During the daily phone call, TiVo headquarters chooses a name for the receiver's viewing information file and a name for the diagnostic log and transmits both to the TiVo unit. If one of these file names includes the word 'RANDOMIZE', then the TiVo unit replaces that word with a large randomly chosen number. This allows TiVo headquarters to decide whether a file's name will include identifying information or not. The TiVo unit then begins transferring the two data files to the TiVo headquarters computer, saving them under the chosen names.

Under normal operation, TiVo headquarters includes the word 'RANDOMIZE' in the viewing information file name and the TiVo unit serial number in the diagnostic log file name. This means that the viewing information file name will not immediately identify a subscriber, but the diagnostic log file name will.

For example, it was first observed that TiVo headquarters selected to transmit the names

```
/TivoData/bprv/20010124/000000.RANDOMIZE.80208.bz2
/TivoData/bpub/20010124/184023.00840336485942.log.bz2
```

and then the researchers' TiVo unit depositing files onto the TiVo server computer with the names

```
/TivoData/bprv/20010124/000000.C41CF33D1DC7F401.80208.gz
/TivoData/bpub/20010124/184023.00840336485942.log.gz
```

The first file, which contains the viewing information, is sent to the 'private' (bprv) directory and stored under a name that only identifies the subscriber's zip code. But the diagnostic log file goes to the 'public' (bpub) directory, and is stored under a name that contains a TiVo unit's serial number – in this case 00840336485942. Both files clearly show the date of the transfer, 2001 01/24.

Since both files are transferred to the same computer during the same phone call, this computer can easily reattach the subscriber ID to the viewing information file. In addition, it is standard computer security practice to keep a record of every FTP file that is transferred. These FTP records normally indicate both the name of the file transferred and the IP address of the computer (or

TiVo unit) that initiated the transfer. Just by consulting this log file – even months or years after the fact – TiVo could easily reconstruct the subscriber ID that deposited a viewing information file. (The researchers have no direct way to tell if FTP logging is on or off, but TiVo representatives indicated that FTP logging is disabled.)

Recommendations to TiVo Subscribers

TiVo permits its subscribers to disable the collection of viewing information and diagnostic logs by calling TiVo toll-free at 1–877–367–8486 (1–877-FOR-TIVO).

Listening to TiVo Transmissions

The researchers of this TiVo examination simply monitored calls made on their own phone lines and never even opened the TiVo case.

The researchers constructed a modem sniffing station consisting of two phone jacks connected to modems on a standard laptop computer. Then the TiVo device's telephone jack was connected to the station's incoming telephone jack, and the station's outgoing jack was connected to the real phone system. When the TiVo device made a telephone call, the sniffing system passed through the contents of the phone call undisturbed while saving a copy of everything transmitted over the line. Then the captured data were analysed, which led to the findings and an advisory to TiVo Inc.

The Privacy Foundation provided a draft version of this privacy advisory to TiVo on March 14, 2001. Senior officers of the company responded in a phone call on March 19, 2001 with the following points:

- TiVo turns off all logging at the incoming FTP servers to prevent the correlation of the anonymous viewing files with the diagnostic files that contain customer ID numbers. TiVo takes a number of other steps to prevent anonymous viewing files from being traced back to TiVo subscribers.
- TiVo claims that it is only interested in compiling customer data to assess aggregate viewing behaviour, and has no plans to identify the viewing habits of individuals, nor to use such data for direct marketing purposes.
- The server-side practices of TiVo are beyond the scope of the advisory. TiVo also notes that data about customers is kept in secure servers that can only be accessed by authorized TiVo employees.
- Version 2.0 of the TiVo software will encrypt files that contain personal information, as described in the latest Privacy Promise.
- The latest version of the TiVo Privacy Promise[26], dated September 2000, addresses many of the issues, which the Privacy Foundation advisory brings up.
- TiVo acknowledges that its privacy practices and disclosures may not be up-to-date in manuals sold with TiVo units, but the company notes that it attempts to alert all customers about the availability of the new Privacy Promise via email and messages on the TiVo service.

Source: Privacy Foundation (2001)

26 Available online at http://www.tivo.com/support/service_privacy_pvr.asp

The issue of consumer privacy is therefore a crucial one, as monitoring technologies developed by Internet companies become more suitable for television consumption. Historically television consumption habits have been mapped out with surveys, but new television technology potentially alters this relationship, as tracking and surveillance software is easily employed to record the exact nature of consumer behaviour. The new technology, which is being developed in this area, also allows some basic transactional activities and therefore can be expected to store and collect secure personal data such as credit card details. This suggests the vulnerability of the Internet will be extended into the world of television consumption.

Cyber Marketing Violence: The Risks to Children

Children represent a percentage of the population that are becoming increasingly targeted by cyber marketers. According to the Centre for Media Education (CME 2000: 24) this is due to the enormous amount of influence children under 12 have on spending patterns in certain markets. CME note that this is not merely coincidental and point to the trend that increasingly, companies are employing specialists such as child psychologists and researchers, in order to encourage children to buy products or to apply pressure on their parents to buy them. According to some sources the figure for spending in child related markets could be as high as US$ 500 billion (CME 2000: 24). At the same time, convergence of certain capabilities and cross utilisation of the Internet with television, offer cyber marketing and the advertising industry many opportunities which have never previously been available.

Interactive Advertisements and Product Placement

Some sections of the marketing industry are beginning to experiment with interactive DTV commercials for products targeted at children. For example, an interactive advertisement for ‘Lego Mindstorms’ allows children watching the advertisement (which shows an ‘I’ to indicate the advertisement is interactive), to click on the advertisement, through to a fully interactive platform. Once the user clicks through the child or adult is immediately taken to Lego’s online store. Another example concerns an interactive Coca-Cola commercial featuring the ‘Polar Bear Twins’ that enables the viewer to click on the advertisement in order to obtain a free toy animal. More sophisticated interactive commercials are to be expected. One strategy developed to capture the attention of children is to invite them to play games involving the products. CME provides an example of Mattel’s most popular doll „a Barbie commercial could invite a child to click on the ad to customise her own Barbie doll. The site could than give [the girl] the opportunity to design [her] own personalised Barbie, choosing from an inventory of physical features, clothing styles, and personality traits” (CME 2000: 25–26).[27]

Interactive advertisements have the potential for more overt product placement and this is becoming increasingly common practice in some television markets. Product place-

27 http://www.barbie.com [as of 2001, February 19]

ment is another central component of the digital cyber marketing paradigm. In the U.S. there are cases of TV programmes beginning to incorporate websites into their advertising models. For example, AsSeenIn.com[28] have a deal with Viacom, which enables Beverly Hills 902010 fans to purchase items on the AsSeenIn.com site such as furniture and set material. A further advancement could be that DTV is exploited to allow the audience to directly buy products embedded in the programme itself.

Disney's television company ABC is in talks with online auction site eBay, to develop a branded TV show that would provide viewers a 'buying opportunity' allowing viewers to purchase Disney products through eBay.com. Such a T-commerce application (the ability to purchase products instantaneously through television) could be embedded into programming aimed at children. The promotion of certain products such as pizza and video games can potentially exploit the impulsiveness of children. With DTV, marketing and advertising companies could allow children to click on the boots that their football hero is wearing while he is playing during a World Cup final and subsequently purchase them from the connected, branded website or online service.

Collection of Personal Information and Targeted Advertisements

Data collection websites can use games, prizes, surveys, and popular characters to obtain information from children. CME suggest that these kinds of practices would be even more harmful in combination with the persuasive power of television. The tracking and assembling capabilities of DTV can of course be used to exploit children. If a broadcaster or advertiser knows that a child in the household likes to watch Pokémon, one could target advertisements for the latest Pokémon game directly to that household. CME point out that children might be particularly vulnerable in this respect as, „this could take advantage of a child's trusting nature because a child does not understand that these uniquely targeted messages are coming from a market and not from a 'friend.' In addition, interactive advertisements, based on knowledge of a child's likes and dislikes, may raise to the level of unfairness, because children do not understand the persuasive intent of such messages" (CME 2000: 40).

The ability for companies to use technology for the surveillance and monitoring of consumer behaviour is enormous. Children could supply the consumption behaviour of their parents and large cross-promotional campaigns could be exploited in order to entice children into windows that sell products associated with specific television programmes. These strategies are only beginning to develop as marketing companies realise the potential of new technologies and they should be expected to become subtler and more sophisticated. The potential for gathering data appears to be almost endless and therefore has been raised as a serious threat to privacy by liberty groups.

28 http://www.asseenin.com/asihome/ [as of 2001, February 19]

Interception Capabilities and the State

The monitoring of traffic that flows over a wide range of channels has long been a practice that States have undertaken in order to protect national security. Communications intelligence systems like ECHELON (used by U.S., British, Canadian and Australian security agencies) and ENFOPOL (European counterparts) are the latest in a long history of the State utilising technology for monitoring communications flowing through a number of different mediums and delivery networks.

Campbell (1999) states that targets that are tracked and intercepted for communications intelligence purposes include a wide range of communications that are perceived to consist of content that might be illegal (drug trafficking, money laundering), a threat to State security (terrorist activities, military messages), or increasingly for purposes of conferring economic advantage and corporate promotion to national companies.

Some of the key characteristics of the capacity to use communications intelligence for the collection and interception of information include comprehensive systems that allow access, interception and processing of every important modern form of communications (cable, high frequency radio, submarine cable, satellites etc.) with few exceptions. Systems are also capable of a number of identifying capacities from speaker recognition (voiceprints) that recognise the speech of targeted individuals making international phone calls, trawling and topic spotting. All these methods allow fairly precise interception and record data on a huge scale, with seemingly few obstacles (Campbell 1999).

In the United States, as well as other countries, the development of tracking and interception devices has been a controversial issue. The Carnivore system came to light through a U.S. court case, as a result of a lawsuit between a U.S. based Internet Service Provider and Federal Marshals, who had demanded the ISP wire the Carnivore device into its network.

Carnivore is part of the U.S. tapping system and essentially consists of a computer and interface card. It runs a packet sniffer programme, to select specific data from inside an ISP network. Carnivore sees all the traffic flowing through a network where it is installed and is able to identify the origin and destination of an Internet packet- if an address corresponds to a particular address that has been authorised for tapping by a court order, then the device allows interception and retrieval of information. Because all Internet traffic consists of packets, which contain details of the sender and destination, the capacity to monitor identified user traffic allows law enforcement agencies to easily monitor specific users.

The U.S. is not the only State with such capacities. In the Netherlands, the Dutch security service BVD announced in 1999 that it had been collecting emails being sent overseas by companies and the Australian government has passed laws allowing law enforcement agencies to attack computers to obtain information about the content. The British government have established the Government Technical Assistance Centre; according to the Home Office's Encryption Coordination Unit the centre will have „the capability

to produce plain text, images, audio from lawfully intercepted communications and lawfully seized computer media which are encrypted" (Campbell 2000: 2).

Conclusions

The examples discussed above demonstrate a number of areas where ICT acts as a powerful means of surveillance. Although there is an obvious need for States to monitor certain kinds of communication in terms of national security, there is also a grey area where surveillance goes beyond what is necessary to defend the State. Individuals are caught within the wide catchment network of the communication intelligence facilities, and this information could and should be perceived as an infringement on the right of privacy.

The State however, is not the only institution that conducts sophisticated surveillance operations. With the diffusion of new technologies and the development of digitalisation, there is an increasing possibility that these devices will be exploited for commercial purposes to monitor consumer behaviour. The increasing possibilities of T-Commerce, offers commercial companies a huge opening to tailor advertising campaigns to individual consumers and exploit the promotional opportunity to associate popular programming with commercial products. Although the technology is still in a nascent stage of development and in the U.S., the 1984 Cable Act prevents any one company sharing personal information with other companies (though satellite and telephone companies are excluded from the rules of the Act), there is still concerns from privacy advocates.

As technological innovation extends the possibilities for transactional activities the vulnerabilities identified in the context of the Internet will therefore become far more integral to the television environment. Privacy is therefore a central concern for individuals as these advances in delivery capability are exploited by companies, in order to enter the home in a far more potent way than perhaps ever before.

Chapter IV.
Novel Crimes in Cyberspace

Hacking and Attacking

Hacking together with piracy is the most commonly known illegal activity associated with new computer technology. The hacking community have been the subject of films, books and numerous newspaper reports and the public image of the dangers posed by hacking into computer systems would be an interesting study in itself.

To the people of the computer underground, hacking still refers primarily to the imaginative and the unorthodox use of any artefact. In current use, the term usually refers to the unauthorised access to and subsequent use of other people's computer systems, and especially within the computer security industry, it is likely the term will be associated with electronic vandals (Taylor 1999: xii). Sieber (1998: 41) claims that the term computer hacking is traditionally a description of the penetration of computer systems, which is not performed with the purpose of manipulation, espionage, sabotage or theft, but for the gratification of overcoming security measures and showing vulnerabilities in computer network systems.

The computer security industry emphasises and makes use of a 'breaking and entering' analogy. The computer underground labels this analogy as dramatic and prefers to draw attention to the intellectual and pioneering contributions of hackers. The choice of this terminology needs critical interpretation. In order to stress hypothetical malicious intentions on behalf of the hacker, the security industry often focuses on fear and a sense of violation that accompany breaking into and entering property. In contradistinction the computer underground compare computer intrusion to a temptation to walk into somebody's home when the door has been left open. The hackers argue that if it involves such negligence and no damage is done the actions do not constitute illegal activity (Taylor 1999: 147).

In an interview with the BBC's Panorama programme, the hacker investigator Vranesevich, who claims to currently have access to files that contain details of around 7,000 individual hackers worldwide, provides some insights into the hacker community. He claims that the number of hackers in the U.S. is proportional to the number of people online. On a global level however, he suspects the number is far greater and is difficult to assess because of the difficulty in identifying the size of the hacker communities in societies, such as China and Indonesian, where due to the severity of punishments for

computer related crime and the oppressiveness of the regimes, the hackers go to far more effort to disguise their activities and identities.[29]

The motivations indicated by the computer security industry seem to emphasise vandalism and pathological aspects of hacking. Hackers themselves provide a classificatory approach to their motivations behind hacking, which are all in some ways related to psychological gratification. These include:

- Feelings of addiction
- Curiosity
- Boredom with educational system
- Enjoyment of feelings of power
- Peer recognition
- Political activism

(Taylor 1999: 45–46):

Allen et al (2000: 93) identify some possible objectives of an attacker (see table 2 below), providing an approximate correlation between the types of attack and the motives of an attacker. These consist of a range of motives for an attack and include the consequences as they are related to the motive of the attack.

Table 2: Attacker motives.

Objective	Denial of Service (Loss of availability)	Information retrieval (Loss of confidentiality)	Information modification or corruption (Loss of integrity)
Curiosity		X	
Vandalism	X		X
Revenge	X		X
Financial gain			X
Competitive advantage	X	X	X
Intelligence gathering		X	
Military gain	X	X	X

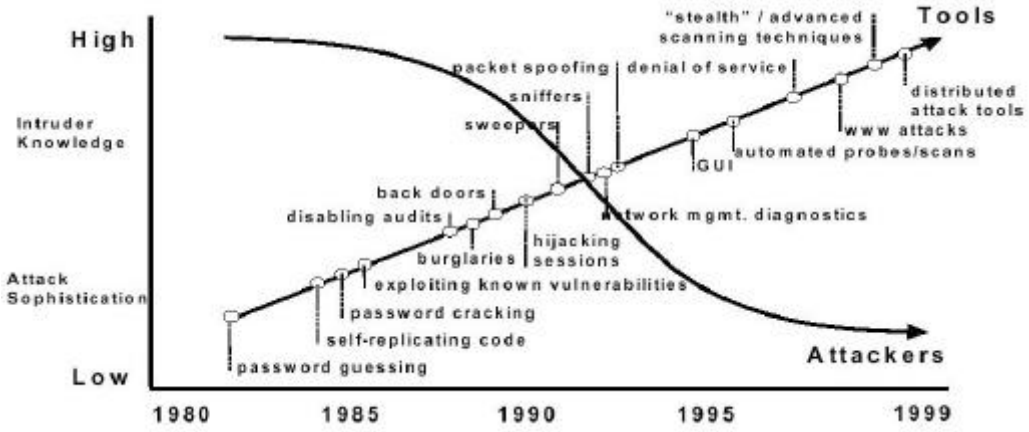
Source: CMU/SEI (2000).

Contrary to common belief the application of one hack to other systems is far greater than is usually perceived. According to Taylor the generic nature of computer systems means that a hack into one computer system can subsequently be applied to a whole class of systems. This ultimately means that once one system has been accessed, the same principles can be used to breach a whole range of other systems around the world.

29 http://news6.thdo.bbc.co.uk/hi/english/static/audio%5Fvideo/programmes/panorama/transcripts/

In this manner computer systems are far more vulnerable than is usually perceived, as the information enabling a hack on one system, can be exploited in order to attack a whole range of systems that share the make up of the one hacked into. This could lead to a number of systems' security being breached, with the possibility of significant damage or theft being committed.

Figure 1: Attack Sophistication vs. Intruder Technical Knowledge.



Source: CMU/SEI, 2000.

Financial Gain

Despite the claims made by the large percentage of the hacker community that hacking is not essentially about financial gain, there are several examples of attacks or hacks in which financial gain has acted as the central motive. China experienced its first cyber bank robbery which was committed by two brothers, who have been sentenced to death for hacking into a bank's computer system and stealing 720,000 Yuan (US$ 86,700). In Japan, hackers managed to break into a Japanese bank's computer system and, according to reports, stole information on up to 10,000 customers (CSI/FBI Survey 1999: 12). Citibank revealed in 1994 that a hacker had breached its security system and stole US$ 10 million. The bank recovered almost the total amount of the cyber theft except US$ 400,000. The primary hacker responsible was convicted for the offence.[30]

From a public relations perspective it is highly likely that some companies such as banks withhold information about security breaches due to the effects of adverse publicity. Revealing serious intrusions could result in damage to corporate image or even result in a loss of customers.

Malicious hackers may exploit this fear for purposes of extortion. In January 2000, the FBI started an investigation into a blackmailing case in which an unidentified hacker claimed to have stolen 300,000 customer credit card numbers from CD Universe.[31] The

30 http://www.businessweek.com/bwdaily/dnflash/aug2000/nf20000822_308.htm [as of 2000, August 22]

31 http://www.cduniverse.com/

company received a fax demanding US$ 100,000 in return for the destruction of the data. After CD Universe refused to pay, data was published on a website, with available links to credit card numbers and the associated names and addresses of their holders. The blackmailer sent email messages to The New York Times, stating that he used the numbers to obtain money for himself. The hacker supported his claim by sending emails containing actual credit card numbers in order to demonstrate that the claim should be taken seriously. The hacker indicated he had hacked into a database at CD Universe's website, by exploiting the weaknesses in vulnerable software used by the company. The chairman of the parent company of the online CD store confirmed that the hacker 'definitely has CD Universe data', but was not sure whether the site had been hacked or the data had been obtained in another way.[32]

The FBI investigation into the CD Universe case involved a wide study of online forums where trading in stolen credit cards was known to take place. The investigators participated in transactions between the groups and built up a bond with the community in order to contact the hacker responsible for the theft that they knew worked under the label Maxim. In this way the FBI succeeded in obtaining Maxus' bank account information, including the name Maxim Ivankauf who was based in Latvia. According to the hacker investigator, Maxim Ivankauf is safe and probably rather wealthy, living on the proceeds of his illegal activities, because the United States lacks an effective legal international instrument with Latvia to successfully prosecute the hacker and apply for extradition.[33]

Vandalism

In February 2000, the websites of Yahoo!, CNN, Amazon, eBay, and Dell were among the victims of distribution of denial of service (DDOS) attacks (DDOS attacks consist of hackers swamping servers with requests for information, so that other users are excluded from accessing the site). Although no confidential or personal data was stolen during the attack, millions of users were denied access to the popular sites, incurring financial losses for the websites rated at millions of US$. The US Minister of Justice, Janet Reno, made the case a top priority and the responsible DDOS attacker(s) became the most wanted cyber criminal(s) on the FBI listings. On 15 April 2000, the Royal Canadian Mounted Police (RCMP) arrested a 15 year-old boy, also known as 'Mafiaboy'. Both the FBI and the Canadian police alleged Mafiaboy of being involved in the attack. On 3 August 2000, the RCMP announced that the Provincial Crown Prosecutor authorised 64 additional charges against the minor. Of these charges, fifty-four of which relate to unauthorised access into websites, including several US universities.[34]

Attacks cannot only lead to revenue losses but also create serious threats to safety. The BBC's Panorama programme also revealed that during a 1997 space shuttle mission as-

32 http://www.wired.com/news/print/0,1294,33539,00.html [as of 2000, June 26]

33 http://news6.thdo.bbc.co.uk/hi/english/static/audio%5Fvideo/programmes/panorama/transcripts/

34 http://www.nipc.gov/pressroom/pressrel/mafiaboy.htm

tronauts were put at risk by systems interference. Michael Foale, a British scientist, was on the Mir Space Station during a linkup with the American astronauts, when hackers broke into the computer system that constantly monitor the astronaut's heartbeat, pulse and medical condition. The attack on the NASA computer system was orchestrated by an Israeli based hacker who was distributing information to hackers all around the world on how to infiltrate NASA's security systems. The high degree of disruption caused by the attack has raised concerns that technological reliance of sophisticated operations represents a critical vulnerability open to hackers and other individuals, who may not always be fully aware of the consequences of their actions. Many attacks and intrusions may have serious risks (see for example box 2) and show that the consequences are here, now and for real.

Europol (1999) also identifies crimes relating to telecommunication techniques such as illegal use of files and supporting devices, illegal use of telephone bugging devices and cloning fraud. Moreover, new challenges concern the illegal use of digitally manipulated images and electronic anti-theft devices. Also criminal use of digital colour-copy or printing machines has to be taken into account. The most frequently counterfeited documents include international passports and visas, border passes, birth certificates and bank details.

BOX – 2
Juvenile Computer Hacker Cuts off FAA Tower at Regional Airport – First Federal Charges Brought Against a Juvenile for Computer Crime

This case concerns the first U.S. federal charges against a juvenile hacker for commission of a computer crime. The criminal charges claimed the hacker temporarily disabled *loop carrier systems* at Worcester airport and in the community of Rutland, Massachusetts.

The loop carrier systems of the Bell Atlantic Telephone Company were accessible from a personal computer's modem, in order to offer the telephone company technicians the possibility to change and repair the service provided to customers quickly and efficiently from remote computers.

The juvenile computer hacker managed to identify the phone numbers of the modems connected to the loop carrier systems operated by the telephone company providing service to the airport and the community of Rutland.

On 10 March 1997, at approximately 9:00 a.m., the hacker intentionally, and without authorization, first managed to access the loop carrier system providing service to the Worcester Airport. Secondly, he sent a series of computer commands to the system that changed and impaired the integrity of data, on which it relied, thereby disabling the system. As a consequence, with the potential threat for public health and safety, the outage resulted in the loss of the telephone service until approximately 3:30 p.m., to the Federal Aviation administration Tower at the airport, to the airport's fire department and to other related concerns such as airport security, the weather service and various private airfreight companies. Furthermore, the main radio transmitter, which is connected to the tower by the loop carrier system, and a circuit that enables aircraft to send an electric signal to activate the runway lights on approach, were not operational for the duration when the system was incapacitated.

Later on that day, at approximately 3:30 p.m., the juvenile computer hacker, in a similar way, managed to cause an outage by accessing the loop carrier system-servicing customers in and round Rutland. This time the outage disrupted telephone service throughout the Rutland area, which caused financial damage and a threat to public health and safety.

The U.S. Attorney involved in the case, stated that as a result of Bell Atlantic's quick reaction and invaluable assistance, the Secret Service was able to identify a vulnerability that affected not only the two telephone company computers hacked in this situation, but hundreds of identical computers used by Bell Atlantic around New England and thousands used by telephone companies around the U.S.

The juvenile was sentenced to two years probation, during which he was disallowed from possessing a modem or other means of remotely accessing a computer or computer network directly or indirectly. Furthermore, he was also made to pay restitution to the telephone company, complete 250 hours of community service and has been required to forfeit all of the computer equipment that was used for the criminal activities.

Source: U.S. Department of Justice[35]

From Traditional to New Forms of Organized Crime and New Terrorism

Hoffman (1998) suggests that the tools and methods of terrorism can easily be obtained at bookstores, mail-order publishers, on CD-ROM, and increasingly from the Internet. In this way, terrorism has become accessible to anyone with a grievance, an agenda, a purpose, or any combination of the above. Well publicised examples of amateur terrorism include the attacks on civilian populations by the followers of the Japanese religious sect Aum Shinrikyo, who were responsible for sarin nerve-gas attacks on the Tokyo subway system in March 1995. As a result of the Japanese nerve-gas attack a dozen people were killed and 3796 were injured (Hoffman, 1998: 18). The bombing of the Oklahoma City federal office building in 1995, which represents one of the rare terrorist attacks on North American soil of such brevity and destruction, should also be included in the category of new forms of terrorism. Although the Internet cannot be blamed for these activities (indeed it is likely that the Internet had nothing to do with these crimes), there are other areas where the Internet can be used to conduct information sabotage and disruption of systems capacity that might not have the same tragic consequences as the above cases, but are nevertheless likely to cause disruptions and create havoc.

Cyber War and Net War

The former Minister of Foreign Affairs of the Russian Federation, Ivanov, submitted a draft resolution to the 53rd Session of the General Assembly of the United Nations (Sept. 1998/ Item 64 of the agenda). Ivanov expressed his concern about the developments in ICT and the potential risks to national security measures:

> „We are talking about the possible invention of an information weapon and the danger of outbreak of information wars, which, as we understand it, will have the form of one country taking action aimed at

35 http://www.usdoj.gov/criminal/cyber-crime/juvenilepld.htm

> destroying the information resources and systems of another country and to protect at the same time its own infrastructure“ (Ivanov 1998, 53rd Session of General Assembly of the UN).

In most studies the term cyber war is commonly used to refer to some form of information related warfare. However Arquilla et al (1998) distinguish between two kinds of ways that ICT is exploited in aggressive situations, and in this context they coin the term net war to identify acts of terrorism through ICT.

On one hand net war is a type of activity that is increasingly prevalent at the societal end of the spectrum, where the language has normally been about low-intensity conflict, operations other than war, and non-military modes of conflict and crime. The term therefore provides an understanding of how terrorism and organised crime, in combination with traditional and new technology, have been utilised in order to create the possibility of social, economic and political threat. Net war concerns non-state, paramilitary, and irregular forces as in terrorism. It refers to:

> „An emerging mode of conflict and crime at societal level, involving measures short of traditional war, in which the protagonists use network forms of organisations and related doctrines, strategies, and technologies attuned to the information age. These protagonists are likely to consist of dispersed small groups who communicate, co-ordinate, and conduct their campaigns in an ‘inter netted’ manner, without a precise central command“ (Arquilla et al 1998: 47).

On the other hand cyber war is a concept that refers to information-oriented military warfare and is identified as an increasingly important consideration at the military end of the spectrum, where the language has normally been about high-intensity conflicts. It typically involves formal military forces as adversaries. Due to innovative technology, it was, for example, possible to alert anti-missile stations about the launching of Iraqi Scuds, through American satellites transferring signals in a fraction of a second, to a centre in Colorado Springs. This in turn warned the batteries (by phone) to launch Patriot missiles in order to intercept the missiles aimed at sites in Israel. In this respect cyber war has a closer relationship with conventional warfare between belligerents. ICT is seen to supplement military strategies and aid the logistic strategies of warfare.

Although little evidence is available about terrorist groups making use of hackers or hacking techniques the ‘Chameleon’ case reveals some of the darker side of the potential relationship between terrorist groups and hackers. The hacker investigator Vranesevich identified an American teenager, who turned transpired to be M. Mifrett. The hacker managed to successfully break into a server on the Defence Information Systems Agency (DISA), which is a division of the United States Department of Defense. The DISA provides two systems that the hacker gained access to, giving him network access to the entire US Military.

Shortly after the intrusion by Chameleon he was contacted by K. Ibrahim, an individual purporting to be a supporter of Osama bin Laden, the FBI’s most wanted man and suspected of being involved with the bombing of US embassies in East Africa. Ibrahim sent Chameleon an amount of US$ 1,000 in advance, in exchange for software. On receipt of the software the hacker had used to breach U.S. security, he was also promised another US$ 10,000 and additional work.

The FBI tracked down Chameleon to his home (where he was operating from a computer lab in the garage) in California, before he had the opportunity to deliver the software. After the investigation the individual who attempted to commission Chameleon's software began to make severe death threats against the hacker investigators, their families, and others who had been involved in the case.

BOX – 3
Special Report: Israeli-Palestinian Cyber Conflict

Overview

Despite 3 months of relentless cyber attacks by pro-Israeli and pro-Palestinian attackers, the cyber conflict shows no sign of abating. New targets, tools, tactics and actors continue to appear almost daily. This activity parallels the increase in tensions and violence on the ground.

Targets are not limited solely to websites. They also include real-time chat rooms and critical infrastructures such as domain name servers. In addition to the obvious risk to sites perceived to support or advocate one side of the conflict, high-profile websites may find themselves targeted simply because attackers find them an effective means to garner attention for their causes. Along these lines, there is a strong possibility that attackers will step-up attacks against US government and commercial sites. For instance, one pro-Palestinian hacker threatened distributed DDOS attacks against 'Zionist' sites similar tot he assaults in February 2000 that disrupted Yahoo.com, CNN.com and eBay.com.

Following recent trends, there is a strong possibility that support for the cyber campaign will continue to grow among other high-profile Muslim extremist groups, many of which have a strong presence on the Internet. Attacks used by one side against the other have been and will continue to be turned around in a matter of hours, depending upon the amount of customisation and set-up time required. In addition to this trend, there is the potential for increased sophistication in attack tactics and tools by both sides, as both have time to prepare and launch more intricate actions. In the event that either side deploy viruses or Trojan horses, infections in all likelihood will not be confined to their intended targets.

Information on Cyber Incidents to Date

- Number of Sites/Targets Attacked by pro-Palestinian Supporters: 166+
- Number of Sites/Targets Attacked by pro-Israeli Supporters: 34+
- Government Targets Attacked (Eight Governments): Iran, Israel, Lebanon, Malaysia, Palestine, Qatar, United Arab Emirates, US
- Geographical Ties (23 Countries): Belgium, Brazil, China, Egypt, Germany, India, Iran, Israel, Italy, Japan, Lebanon, Malaysia, Mexico, Netherlands, Pakistan, Palestine, Peru, Qatar, South Korea, Taiwan, United Arab Emirates, UK, U.S.
- Targets Include: Web sites, e-commerce servers, email servers, Internet relay chat (IRC) servers, domain name servers (DNS), Internet service provider infrastructure, file transfer protocol (FTP) sites
- Languages Used: English, Arabic, Hebrew, Portuguese
- Attack Tools Used: 16+

Source: iDefense (2001)

Vranesevich states that there is an increasing awareness in terrorist organisations of the potential to exploit ICT in order to access sensitive military operation and sabotage military information. The damage that hypothetically could be done could be enormous:

> „I think, at this point, terrorist groups are just now beginning to wake up to the type of power that this could provide them. Typical terrorist groups are small and maybe not well funded. So you're talking about things like pipe bombs that as their name implies, strikes terror but doesn't necessarily do widespread, across the board damage, to a national infrastructure. Here we see terrorist groups who were watching news reports every day, just like this one where they're hearing about young teenagers being able to gain access to these types of things, or being able to cause this type of damage and concern. I am sure they're beginning to wake up to the fact that they too could have this type of power and this type of influence, where before a small terrorist faction, maybe 20 individuals, could at best cause havoc to a small community, it can now potentially cause havoc to an entire nation" (Vranesevich: Interview with BBC Panorama 2001).

According to Arquilla et al the term net war is meant to call attention to the prospect that network-based conflict and crimes are already evolving and will become major trends in the next decades. They identify a number of actors that would be able to exploit ICT in this manner including Hamas and Asian Triad organisations (Arquilla et al 1998: 47).

Net War Actors and Organisation Types

In their discussion of net war Arquilla et al (1998) identify three basic organisational structures in relation to network organisations:

- The chain network: as in a smuggling chain where people, goods or information transfer from one contact to another, and end-to-end communication takes place through intermediate nodes.
- The star, hub or wheel network: as in a franchise or a cartel structure where a set of actors is linked with a central node or actor, and communicate and co-ordinate through that central node, such as in for example, terrorist and criminal syndicates.
- The all-channel network: as in a collaborative network of militant small groups where each group is connected to the other.

(Arquilla et al 1998: 49).

Each node may represent an individual, a group, part of a group or institution, or a State. Arquilla et al argue that a variety of configurations are possible, such as a net war actor with an all-channel council at its core, whilst using chains for tactical operations. Some actors may have a hierarchical organisation, but use networks for tactical operations, and other actors may have an all-channel structure, but use hierarchical teams for tactical operations. Of the three network types, the all-channel structure provides the network with the most potential for collaborative actions, and it is the structure that benefits the most from the information revolution (Arquilla et al 1998: 50–51).

Arquilla et al suggest that net war agents are already prepared to take advantage from future developments in ICT, such as, for example, increases in the speed of communica-

tion, reductions in the cost of communication and increases in bandwidth. Lesser (1998) supports this assumption when he suggests, anti-government 'without a leader' militia groups in the U.S. or the highly separated cells as of Hamas and other powerful terrorist groups in the Middle East, are well equipped with encrypted phone communications and the Internet.

The World Wants to be Loved: Viruses, Worms and Trojan Horses

The range and impact of different forms of computer sabotage demonstrate how much we depend on interconnected computers and computer networks, and in the ways these are embedded in our daily lives. Computer sabotage includes the construction of time bombs, viruses, worms and Trojan horses, all of which can attack, damage or disarm a computer system or network. The growth of these kinds of computer crimes has become far more visible over the past decade. The speed and impact of a virus or worm, which can involve the infection of millions of computers, at work and in the home, probably means that this form of computer crime affects more people than any other.

Table 3: The increasing impact of computer viruses

Virus	Year	Type	Time to reach #1 „most prevalent"	Damages
Jerusalem, Cascade, Form…	1990	Exe File, Boot Sector	3 Years	US$ 50 Million for all viruses over 5 years
Concept	1995	Word Macro	4 Months	US$ 50 Million
Melissa	1999	Email enabled, Word Macro	4 days	US$ 93 – US$ 385 Million
Love Bug	2000	Email + enabled, VBS	5 Hours	> US$ 700 Million

Source: ICSA.net 2000.

Rapid increases in connectivity and data sharing leave operating systems increasingly open to attack. Targets for cybercrime vary, but companies such as Microsoft have found themselves particularly prone to the attention of the communities that develop and execute viruses. The motivation behind attacks on Microsoft software are usually underpinned by a sense that Microsoft represents a Leviathan in the computer industry and its operating system Windows, has been a constant target.

A member of one of the most infamous hacker groups – The Cult of the Dead Cow[36] stated his reasons for focusing on Windows, „My main issue at the time was with Windows 95 which was essentially released without any security built into it. It had very, very minimal security. That was a marketing decision by Microsoft. They wanted to

36 http://www.cultdeadcow.com

have as many people be able to use it as possible."[37] The same member is also known as the author of a Trojan horse called 'Back Orifice' a remote management tool that can be installed in computers running Windows 95/98. Installation and execution of the self-contained file can take place when a targeted user of a Windows operating system, has been persuaded to open an email attachment enticed by such file titles such as 'nudepics.exe.' or 'Kournikova.'

A malicious program could also be hidden in games and other audiovisual products. As a result, the program can intrude into the targeted Windows 95/98 system-running computer, without the user's knowledge. According to the Cult of the Dead Cow, Back Orifice allows a remote attacker to gain control of almost all parts of the operating system, including the file system, registry, system passwords, and network processes. It allows an intruder to take screenshots of the targeted system and send them back to the location of the attacker. The remote management tool also enables a hacker to 'sniff' a keyboard, allowing the intruder to make a remote record of all keystrokes, recording details such as passwords, logins to secure systems or credit card numbers. The revised version, Back Orifice 2000, also promises to be a great deal more difficult to detect than its predecessors (McKay 1999).

The Cult of the Dead Cow does not feel it is a criminal offence to make publicly available the remote management tool, which can be downloaded from the Internet. They consider it a public service that makes the larger public aware of the security flaws in the systems. By the same token, the idea that the virus is exposing security flaws in the operating system is a contradiction in terms- because without the viruses the computer systems would not have security flaws.

A further security vulnerability was reported in the WebTV for Windows application for computers running Windows 98, by a bug reporting service (BugTraq) of Security Focus. On investigation the flaw also appears to be in computers running the latest Microsoft operating system, Windows ME. The bug allows an attacker to execute a DDOS attack, and depending on the size of data packet, it could cause the target computer's programs to freeze up, shut down the computer, or force it to reboot.

According to the CERT Coordination Centre (CERT/CC), a centre for Internet security, one of the most serious macro viruses to date was Melissa. Its success was based on the speed at which it was spread. The first confirmed reports of the virus started to circulate on Friday, March 26, 1999 and by Monday, March 29 it had penetrated more than 100,000 computers. To be affected by macro viruses such as Melissa, attachments had to be opened using the e-mail program Microsoft Outlook. Some websites had to take their mail systems off-line and one reported having received more than 32,0000 copies of email messages containing Melissa on its systems, within 45 minutes.

Although the Melissa virus caused a minimum of damage and it was easily detected, the CERT Centre states that variants could be more destructive and far more difficult to de-

37 http://news6.thdo.bbc.co.uk/hi/english/static/audio%5Fvideo/programmes/panorama/transcripts/transcript%5F03%5F07%5F00.txt

tect.[38] Preceding Melissa, Bubbleboy showed in contrast to other viruses, it is not necessary to open email attachments to be affected; previewing of infected email in Microsoft's email program Outlook was sufficient for the virus to penetrate the system.[39] The Microsoft Outlook virus did not cause significant damage, such as deleting files or stealing passwords, but because Bubbleboy has been posted on a Japanese website, it could be developed by a malicious virus writer, who could easily copy it and launch a more destructive variant.

The 'Love Letter' computer worm was launched on Thursday, 4 May 2000 and tells a similar story. Infection with the 'Love Letter' worm takes place in a number of ways, possibly via web pages, email, Windows file sharing, and USENET news. The CERT Coordination Centre provided an advisory, in response to the Love Bug (see box 4). The Love story created many spectacular headlines, reports, and statements. But less publicised was a statement informing people what to do to avoid the virus. By 9 a.m. Eastern time Thursday 4 May 2000, the virus had already infected more than one million computer terminals, causing in excess of US$ 100 million in damage. Making the Love Bug the most expensive, pervasive and damaging virus in the short history of computer sabotage (Tippett 2000).

As the virus attacks become more sophisticated they will inevitably be more difficult to combat and they will subsequently create more damage. An increasing number of people around the world are accessing computer systems, enabling them to use email and other Internet related services, at the same time this means viruses can spread to even more users.

BOX – 4
CERT® Advisory CA–2000–04 Love Letter Worm

Original release date: May 4, 2000
Last revised: May 9, 2000

Systems Affected

- Systems running Microsoft Windows with Windows Scripting Host enabled

Overview

The 'Love Letter' worm is a malicious VBScript program that spreads in a variety of ways. As of 5:00 pm EDT (GMT–4) May 8, 2000, the CERT Coordination Centre has received reports from more than 650 individual sites indicating more than 500,000 individual systems are affected. In addition, we have several reports of sites suffering considerable network degradation as a result of mail, file, and web traffic generated by the „Love Letter" worm.

I. Description

You can be infected with the 'Love Letter' worm in a variety of ways, including electronic mail, Windows file sharing, IRC, USENET news, and possibly via web pages. Once the worm has executed on your system, it will take the actions described in the Impact section.

38 http://www.cert.org/tech_tips/Melissa_FAQ.htm [as of 1999, October 22]

39 http://www.wired.com/news/technology/0,1282,32529,00.html?tw=wn19991115 [as of 1999, November 19]

Electronic Mail

When the worm executes, it attempts to send copies of itself using Microsoft Outlook to all the entries in all the address books it can access. The mail it sends has the following characteristics:

- An attachment named 'LOVE-LETTER-FOR-YOU.TXT.VBS'
- A subject of 'ILOVEYOU'
- The body of the message reads 'kindly check the attached LOVELETTER coming from me.'

People who receive copies of the worm via electronic mail will most likely recognise the sender. We encourage people to avoid executing codes, including VBScripts, received through electronic mail regardless of the sender without firsthand prior knowledge of the origin of the code.

Internet Relay Chat

When the worm executes, it will attempt to create a file named *script.ini* in any directory that contains certain files associated with the popular IRC client mIRC. The script file will attempt to send a copy of the worm via DCC to other people in any IRC channel joined by the victim. We encourage people to disable automatic reception of files via DCC in any IRC client.

Executing Files on Shared File Systems

When the worm executes, it will search for certain types of files and replace them with a copy of the worm (see the Impact section for more details). Executing (double clicking) files modified by other infected users will result in executing the worm. Files modified by the worm may also be started automatically, for example from a startup script.

Reading USENET News

There have been reports of the worm appearing in USENET newsgroups. The suggestions above should be applied to users reading messages in USENET newsgroups.

II. Impact

When the worm is executed, it takes the following steps:

Replaces Files with Copies of the Worm

When the worm executes, it will search for certain types of files and make changes to those files depending on the type of file. For files on fixed or network drives, it will take the following steps:

- For files whose extension is *vbs* or *vbe* it will replace those files with a copy of itself.
- For files whose extensions are *js*, *jse*, *css*, *wsh*, *sct*, or *hta*, it will replace those files with a copy of itself and change the extension to *vbs*. For example, a file named *x.css* will be replaced with a file named *x.vbs* containing a copy of the worm.
- For files whose extension is *jpg* or *jpeg*, it will replace those files with a copy of the worm and add a *vbs* extension. For example, a file named *x.jpg* will be replaced by a file called *x.jpg.vbs* containing a copy of the worm.
- For files whose extension is *mp3* or *mp2*, it will create a copy of itself in a file named with a *vbs* extension in the same manner as for a *jpg* file. The original file is preserved, but its attributes are changed to hidden.

Since the worm code rather than being deleted overwrites the modified files, file recovery is difficult and may be impossible. Users executing files that have been modified in this step will cause the worm to begin executing again. If these files are on a file system shared over a local area network, new users may be affected.

Creates an mIRC Script

While the worm is examining files as described in the previous section, it may take additional steps to create a mIRC script file. If the file name being examined is *mirc32.exe*, *mlink32.exe*, *mirc.ini*, *script.ini*, or *mirc.hlp*, the worm will create a file named *script.ini* in the same folder. The *script.ini* file will contain:

```
[script]
n0=on 1:JOIN:#:{
n1= /if ( $nick == $me ) { halt }
n2= /.dcc send $nick DIRSYSTEM\LOVE-LETTER-FOR-YOU.HTM
n3=}
```

Where DIRSYSTEM varies based on the platform where the worm is executed. If the file *script.ini* already exists, no changes occur. This code defines an mIRC script so that when a new user joins an IRC channel the infected user has previously joined, a copy of the worm will be sent to the new user via DCC. The *script.ini* file is created only once per folder processed by the worm.

Modifies the Internet Explorer Start Page

If the file *<DIRSYSTEM>\WinFAT32.exe* does not exist, the worm sets the Internet Explorer Start page to one of four randomly selected URLs. These URLs all refer to a file named *WIN-BUGSFIX.exe*, which presumably contains malicious code. The worm checks for this file in the Internet Explorer *downloads* directory, and if found, the file is added to the list of programs to run at reboot. The Internet Explorer Start page is then reset to 'about:blank'. Information about the impact of running *WIN-BUGSFIX.exe* will be added to this document as soon as it is available.

Sends Copies of Itself via Email

The worm attempts to use Microsoft Outlook to send copies of itself to all entries in all address books as described in the Description section.

Modifies Other Registry Keys

In addition to other changes, the worm updates the following registry keys:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\MSKernel32
HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Win32DLL
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WIN-BUGSFIX
HKCU\Software\Microsoft\Windows Scripting Host\Settings\Timeout
HKCU\Software\Microsoft\Internet Explorer\Main\Start Page
HKCU\Software\Microsoft\WAB\*
```

Note that when the worm is sending email, it updates the last entry each time it sends a message. If a large number of messages are sent, the size of the registry may grow significantly, possibly introducing additional problems.

Source: CERT/CC (2000)

Computer Related Forgery and Fraud: Money Talks

Crimes that are related to fraud and forgery that use ICT in order to aid or commit a crime cover a range of activities from credit card fraud to company dishonesty, the establishment of bogus companies and other related activities. The individuals involved in such activities, as in the case of hacking, can include a wide range of actors from employees, legally established companies, criminal organisations and individuals looking for personal economic gain.

Computer Related Fraud

Europol identifies offences such as the skimming off of credit cards and shoulder surfing at Automated Teller Machines (ATMs) as crimes that are increasingly prevalent. The technological tools for skimming (copying magnetic files) can be bought in any specialist shop. Cracker programs (for example wizard or credit master) are available to download from the Internet and offer the possibility of obtaining registration numbers of credit cards. In the case of shoulder surfing, one case recorded that a miniature camera was secretly installed at a fuel station, so that when customers were using the ATM machine, the miniature camera recorded their fingers, and as a result, their secret PIN numbers were obtained. Subsequently, the perpetrators made dummy cards that contained a copy of the machine-readable data.

A higher level of high-tech theft concerns the devices used by Russian criminals, who seem to have infiltrated the banking industry through employees. One case involved the maintenance engineers of ATMs, who installed devices the size of a cigarette box, through which the magnetic file of a PIN or credit card number could be read. The tapped electronic data was sent to accomplices abroad who, with the help of the data produced new magnetic cards. In this way, it was possible that the credit of an owner (living in Moscow) of a savings account at a bank in the Netherlands could be withdrawn at the UNI-bank in Denmark. Another case consisted of an American citizen living in Moscow, who had not been in New York for a year and a half. Two tickets from New York to Paris were purchased from his account without his knowledge and clearly without his consent. (Westerman 1999: 5).

Credit cards, which are protected from fraud by a number of safety measures in the offline world, have become the main source of payment online world. Criminals in the online world easily use the cards, as they only need the account number and the expiry date to enable them to use them. The copied cards are usually used to buy virtual goods like software.

Money Laundering

Digital cash systems are common in the banking industry. With smart cards and other innovations, costs can be reduced by decentralising transactions, enabling them to be executed at a fraction of normal costs. While it is understandable that banks attempt to

create efficiency gains through employing new technologies, there are also new security risks that arise with incorporating these methods within the sector. In this context information on how to break into smart cards is already circulating and available on the Internet. There is an added possibility of money laundering and cross border flows of illegal sums and this might increase when denomination limits for transfers increases. Europol reports that the Financial Action Task Force (FATF) has not yet identified cases of money laundering through cyberspace. This could either mean that there are no appropriate detection methods or cyber payment systems do not carry money-laundering risks (though the Italian police estimate that the Sicilian Mafia is laundering vast sums of money through the Internet and online banking and trading which runs into millions of dollars in fraud). Even if at the present time money laundering remains largely tied to the off line world, the capabilities of the Internet and other networks will mean that there will be great incentives for money launderers to exploit this avenue.

BOX – 5
Using Cyber payments to Launder Money: Some Hypothetical Examples

The Street Drug Market

In this example drugs would be sold to users in exchange for disposable smart cards denominated in amounts typically associated with street drug transactions – $20, $50, or even $100. These smart cards would be collected by the street drug dealer and taken to a retail store. The merchant would then upload the electronic value from the smart cards from his/her merchant terminal to a bank or funds-holding account at a financial institution.

The merchant would most likely receive a standard fee for the use of his/her valuable upload capabilities. Once the funds have entered the legitimate payment system, the funds could then be transferred to a domestic or offshore account in a process analogous to the *placement*, *layering*, and *integration* phases of traditional money laundering.

Two types of Cyber payment Value Transfer

In this example stored value derived from drug-trafficking activity could be transferred in at least two simple ways. Perhaps the most predictable manner of funds movement is through the physical transport of high-value, stored value smart cards containing the proceeds of drug trafficking. Because of their small size these cards could be easily concealed and eventually disposed of through redeposit of the funds in a foreign country.

A second way of transporting/transferring value beyond the reach of law enforcement authorities could be to transfer stored value over smart card enabled telephones. Both cellular and conventional analogue telephones are being designed to enable them to inter-operate with stored value smart cards. Such products could obviate the need to launder funds by offering criminals an impressively rapid and efficient means for transferring and consolidating a stream of illicit funds such as those derived from drug trafficking. Once funds enter the payment system they are indistinguishable from funds derived from legitimate sources.

Funds transfers through Network-based Systems

In this example low denomination stored value smart cards could transfer their value onto personal computers which would then transfer that value over the Internet, using increasingly available anonymous remailers to conceal the points of origin of illicit funds. Recipients could then consolidate funds and reintegrate them into the payment system.

Cyber payment Value and the Web

The last example of cyber payment system misuse involves a fraudulent charity that only accepts electronic value (cyber payment value) as donations. Funds collected for an apparently legitimate harity could instead represent the proceeds of drug trafficking. These funds could be uploaded from the electronic purses on PCs to a bank account, and then redistributed from one financial institution to another individual group or elsewhere in the world.

Source: RAND (1998)

Two variants of cyber payment systems, network-based and stored value-type smart cards, offer criminals the opportunity to conceal the transfer of black money. A few hypothetical examples (see box 5) offer a glance at potential ways money launders could use Cyber payment systems (Molander et al 1998: 18). The Rand report suggests law enforcement agencies should consider the following features of cyber payment transactions:

- Disintermediation: involves financial value transfers between entities without the intermediate involvement of an identifiable third party subject to governmental supervision. Should cyber payment systems include disintermediation in the case of, for example, value transfers in unlimited amounts, this could offer money launders the opportunity to avoid traditional money tracing methods by law enforcement.
- Bank or Non-bank Issuance: different rules may apply to bank and non-bank cyber payment issuers. Just an extension of the monitoring of traditional payment system to non-bank entities of cyber payment systems is not necessarily appropriate because new systems can be configured differently and are constantly changing.
- Peer-to-Peer Transfers: some cyber payment systems allow users to make peer-to-peer (thus disintermediated) value transfers via an electronic wallet, a phone or the Internet. Peer-to-peer transfers lack intelligence information or evidence from other sources. Whereas physical surveillance for example could trigger investigation of specific suspected activities involving stored value instrument, peer-to-peer value transfers are unlikely to be detected.
- Transaction Anonymity: in some cyber payment systems, the origins of funds are unintelligible and the identity of the responsible individual or entity difficult to determine. Payer anonymity (identity of the party initiating a value transfer) could be a central feature of cyber payment systems. Transaction anonymity is in combination with possible ways of cyber payment (the Internet, telephone system) a bottleneck for detection by law enforcement.

- Denomination Limits and Expiration Dates: the issuers of cyber payment products are likely to limit the maximum amounts that can be stored on smart cards or other devices. Additionally, cyber payment value could be programmed to expire after a certain number of transfers. Despite these kind of limits law enforcement and cyber payment issuers have to take into account that money launders are early technology adopters and are quick to exploit new technology.

(Molander et al 1998: 16–17).

Europol has also recommended certain restrictions to limit the vulnerabilities of smart cards with measures to limit the amount of any transaction, distribute cards by issuers connected to financial institutions, and restricting payments from credit cards so they can only to be used within national territories (Europol 1999: 15).

Fraud on the Web

New technology has also been used in novel and imaginative ways to commit crimes. The case of the United States vs. Peterson is an example of some of the imaginative ways that the hacker community have attempted to exploit their knowledge of networks for personal gain. Two hackers in LA ensured they would win two Porsche automobiles and US$ 30,000 in cash by manipulating the telephone network. A local radio station ran a promotional competition, which consisted of callers telephoning the station and a numerically specified caller winning the prizes. The hackers manipulated the local telephone switch to make sure that the winning call was theirs.[40]

The U.S. Federal Trade Commission has been recording all its actions against computer-based crime online. In 1994, the Commission was involved in its first Internet case, and in 1996, it had to deal with the first 'big' case, which concerned a pyramid investment scheme promoted on a website (see box 6). The FTC's file includes a myriad of cases, varying from modem hijacking, deceptive domain name registrar, action against an online auction site, Internet privacy, deceptive health claims, page jacking and mouse trapping.[41]

In a case of page jacking and mouse trapping the FTC alleged that the defendants captured and constructed millions of counterfeit web pages. A redirect command was inserted into the counterfeit pages and placed under the defendants' website. When consumers used a search engine, they sometimes received listings of defendants' page jacked and copied sites. These lists described pages concerning recipes, games, automobiles and other harmless topics, but once the consumer clicked on the list for a counterfeit website with the mouse; they were taken immediately to the defendants' sexually explicit adult sites. Once there, it was difficult to leave because the defendants disabled the user's normal browser functions and trying to escape was made impossible by the 'mousetrap.' Clicking the back or close commands on the browser resulted in more pages of graphic sexual content.

40 See United States vs. Peterson, 98 F.3d 502, 504 (9th Cir. 1996), http://www.usdoj.gov/criminal/cyber-crime/sentechtest.html [as of 1999, August 20]

41 http://www.ftc.gov [as of 1999, October 15]

BOX – 6
The Federal Trade Commission's First Big Internet Case

This case involved defendants who promoted a pyramid investment scheme through a website (called 'Fortuna) and by word-of-mouth. They promised consumers that for each US$ 250 invested the investors would receive an income of US$ 5,000 per month. Furthermore, investors were encouraged to set up their own websites in order to advertise the scheme, and the defendants provided advice and promotional materials to achieve this goal. The scheme was dressed up by a New Age formula, but according to the FTC it was nothing but a high-tech chain letter, with losses for the great majority of participants (at least 25,000 consumers paid money) and large profits for the defendants.

The FTC alleged the investment scheme took in more than US$ 11 million from consumers. The major parts of the profits were systematically transferred to bank accounts abroad. Most of the money went to an account at a bank located in Antigua.

On May 23, 1996, the FTC filed a complaint and charged the defendants with violations of its FTC Act. Immediately action was taken and the following day, the FTC obtained a Temporary Restraining Order (TRO) freezing the defendant's assets, appointing a receiver to manage the company, and requiring the company's assets to be returned from the company funds that were deposited in overseas bank accounts. In addition, promotional materials had to be removed from Fortuna's website and be replaced with a notice. This notice informed about the FTC action and contained a hypertext link to a page on the FTC website with additional information and documents about the lawsuit. The FTC requested the Department of Justice's Office of Foreign Litigation to bring an action for an injunction in the Antigua Courts. In this way, it was possible to freeze the defendant's funds in the bank, whilst awaiting the decision to the case.

On February 24, 1997, the district court's final judgement required the company to pay full refunds to all Fortuna members. Refunds were secured by a letter of credit for US$ 2.8 million, drawing on the money in the Antigua bank account and additional frozen funds in the U.S. Also an order was entered which directed defendants to return to investors approximately US$ 2 million, in the form of cheques that were not deposited.

On June 5, 1998, a final contempt order was entered by the district court. The order required defendants to stop their promoting and marketing program until the US$ 2.2 million deficit was paid. The FTC's redress administrator made partial payments to remaining consumers. In total, the amount of US $5.5 million was redressed to 15,622 consumers from the U.S. and 70 other countries.

Source: Federal Trade Commission (1999)

Infringements of Copyright and Related Rights: The Rise and Fall of Napster

Infringement of copyright is one of the most common crimes committed using ICT. Both the copying of copyrighted materials from disc to disc or cassette to cassette and the distribution of material online are major industries. New technology both makes traditional forms of piracy easier and new forms of distribution increasing easier and more difficult to police.

In January 1999, the Business Software Alliance (BSA) announced it had shut down the largest illegal software and Internet sales operation in the European Union.[42] The case involved a Danish based operation and the production of 125,000 illegal CD-ROM copies of several BSA-members software (including Adobe, AutoDesk, Corel, Microsoft and Symantec), with a value of US $237 million. In 1997, the BSA received reports to its hotline that illegal CD-ROMs were promoted through a website.

The BSA case is an example of traditional forms of piracy moving into the computer software industry, which has long plagued the music industry. In 2000 the record industry body the International Federation of the Phonographic Industry (IFPI), that represents 1,400 record companies in 70 countries, estimated that pirated CDs and cassette tapes represent a total loss of revenues of US$ 4.2 billion from illegal physical recordings, with the average global piracy rate for CDs and cassettes at 36%, which represents over one third of recordings sold globally. In the UK alone sales of pirated music are estimated to cost the industry around US$ 30 million annually in lost sales (Hopkins 2001).

It is technologically not very difficult to produce illegal copies of CDs or CD-ROMS and in the past the only serious obstacle to pirating software has been distribution, which it has been possible to police through national legal instruments, albeit unsuccessfully in some States. Digitalisation serves to improve recordings of contraband material, however, new technologies have added an extra dimension to piracy and has created what is perceived to be a serious threat to a number of industries, particularly the music sector, through novel methods of pirating, enabling distribution methods based on peer to peer file sharing.

Digitalisation and the distribution of enabling devices and/or programmes via the Internet offer new opportunities for individuals to acquire copies of music, allowing them to circumvent traditional copyright laws. The MP3 format used on the Internet enables the encoding of digital music, and allows it to be compressed in a form that is easily distributed across computer networks. It therefore allows high quality copies of music to be distributed quickly and recopied and distributed with ease. In 2000 an estimated 50 million people downloaded music from servers and from the Napster site alone, some 2.79 billion separate downloads were estimated in one month (Mathiason 2001: 7). The significant amount of Internet music piracy has created a reaction from the music that demonstrates the seriousness of the potential for piracy, and the threat of the Internet as a medium for distributing music recordings.

According to the IFPI the global music market was worth some US$ 36.9 billion in 2000, a decrease of 1.3% on the previous year (Teather 2001). The biggest drop in sales was recorded in the US market, where there is the greatest amount of online users. Although there has been a continuing decrease of sales in the U.S. of CD singles over the past three years, due to the fact that consumers have replaced their old stock of vinyl with CDs which added extra growth in the past; the drop in sales last year represented a

42 Press release: http://www.bsa.org/danmark/presse/200199eng.htm [as of 1999, October 18]

decrease of 39% in 2000. Although not as significant as the decrease in the U.S., international sales also declined by 14.3%. In Europe contradictory trends are evident as music sales actually increased in Sweden and the UK while in France, Germany and Italy there was a decrease, largely due to CD copying and piracy rather than online music exchanges (Teather 2001).

The song swapping websites also appear to be having an increasing impact on international music sales. There are signs that the industry is suffering some decrease in sales due to these sites, though the true extent of the impact is probably very small compared to offline pirating. Whilst offline sales and pirating sit side by side the Internet on the other hand is almost totally a medium that is used for purposes of piracy.

Napster is the highest profile pirate service and it is estimated that 70 million registered users have stored music files on their computers on the basis of peer to peer trading with MP3 files, allowing users to search each other's hard disks for MP3 files and to exchange them for free. In 2000 the ISP companies reported the term 'Napster' was the most popular search term entered into their search engines. The phenomenal success of Napster has not gone unnoticed by the major music corporations. A high profile U.S. court case ruling against Napster for infringements to artist copyright has forced Napster to remove all music protected by copyright from its server. Since it has started removing files, Napster has seen downloads dramatically fall from a peak in February 2001 of 2.8 billion to 400,000- a decline almost as astonishing as its growth. Although Napster has maintained that it has had to overcome technical problems in order to comply with the court's ruling, as of July 2001 it claims that it is able to filter out 99.4% of copyrighted works.

Over the past couple of years each of the music majors have also increasingly shown interest in the potential of the Internet to distribute and sell music files. All of the majors have signed deals with online companies to begin online services. Napster itself has a tie in with Bertelsmann, potentially giving Bertelsmann access to consumer information on all its users. Napster is also developing software in cooperation with the five Majors to track online music exchanges and charge users, therefore making the market for online music a source of sales for the record companies. Though it should be stated that with the current levels of access to broadband, forecasts for online music sales are inflated and it is unclear whether consumers will be willing to pay for music in this manner.

The demise of Napster does not necessarily eradicate the problems of Internet piracy. The technology that Napster employs can be reproduced, as in the case of Gnutella and Wrapster. These sites have proliferated on the net recently and they can be expected to grow. A UK based website called Espra promises to deliver what the other sites have been unable to do and provide user anonymity- whether this is the case remains to be seen, as there are developments in technology that may make the exchange systems more visible and therefore accountable. IBM has developed a 'system of locks', which allow users to exchange music, but at the same time only listen to the record once. In June

2001 the music companies announced they are developing software called songbird that is able to track copyrighted material over peer-to-peer services allowing publishers to remove the work of artists.

Conclusions

Cyberspace facilitates traditional (organised) crime and terrorism, which can turn into flexible and professionally organised criminal or terrorist networks. Although hacking in the first place, is not performed with the purpose of manipulation, espionage, sabotage, theft or blackmailing, but for the pleasure of overcoming security measures, the different cases in this chapter have shown that the risks range from harmless to life threatening, from large financial losses incurred through hacks or denial of services to security breaches of systems designed to defend national security.

The Internet offers possibilities for all kinds of new crime, ranging from specifically Internet based fraud to the dissemination of viruses. More than ever conflicts will have to deal with perception management and psychological disruptions. However, all forms of cybercrime remain in the first place a problem in the real world, and the same can be said of the possible solutions for the problem.

The range of crimes committed that are somehow related to ICT or the Internet is extremely broad and can potentially effect anybody who has made a transaction using a credit card (both online and offline), holds a bank account or withdraws cash from an ATM. There are also crimes where consumers are more indirectly affected which include money laundering and threats to State security. Taken together these activities are potentially very serious and could incur significant costs on companies and individuals.

Chapter V.
Child Pornography and Hate Speech

There is no doubt that there are many positive possibilities of cyberspace and the Internet. People who have access to the technology can search for a whole range of information efficiently and with the breadth that would take enormous resources in the offline world. It allows people separated by huge geographical distances to converse openly and flexibly and it enables a whole range of groups to share interests, express thoughts, ideas and opinions.

Whilst these positive aspects of the online world are worth noting and encouraging there is also a negative side to the world of cyberspace that acts as a platform for the negative side of freedom of expression, where radical and extreme views are aired that are usually deemed unacceptable in democracies in the offline world. Some areas of cyberspace pose significant risks, especially because of the risks to the protection of minors, human dignity and the right that individuals hold to live their lives unhindered by prejudice and bigotry. As cyberspace provides many channels for user-driven dynamics and has no geographical borders; as opposed to sovereign states and more traditional mass media, a definition or classification of what is considered to be bad or ugly on one side of the world, may be interpreted differently on the other side of the world. The ease with which the Internet crosses national boundaries creates problems for legal and regulatory authorities, as normative modes of behaviour enshrined in one legal system may not be universally shared throughout the world. Making enforcement difficult, or at this point of time perhaps impossible.

Child Pornography

Historical differences between cultural backgrounds, social norms and national legal systems are some of the reasons there is no legal consensus on the definition of child pornography. Although paedophilia does not technically have to concern child pornography, it is often confused with child pornography. However, serious risks remain when paedophiles exchange ideas and fantasies, and start looking for ways to achieve sexual gratification. Producers of child pornography have been caught with cutting edge digital CD production equipment such as film-free digital cameras and reproduction equipment.

The Internet provides low cost and easily accessible information, publication, streaming, and communication. These features make the Internet an ideal platform for the distribution of materials that are illegal. It simultaneously operates for paedophiles in at least three ways:

- It facilitates easy, anonymous fast dissemination of an immediate and constant supply of illegal child pornography images. For paedophiles, it allows the expression of their fantasies for the purposes of affirmation. Images can be posted in a sympathetic environment that is supportive of members.
- It enables the creation and maintenance of a sense of deviant behaviour. Mutual association is an indicator of organisational sophistication in deviant associations. The presence of complex social structures in the computer underground indicates that on a social level, paedophiles act as 'colleagues' in the online community they construct.
- It provides a facilitating and supportive environment. The easy accessibility and possible worldwide distribution of child pornography and rationalisations for child sex has broader implications in the context of sexualising children to an audience who may not have any primary interest in child sex per se.

O'Connell (1998) carried out two case studies exploring the social structures of paedophile groups operating on the Internet, particularly in Usenet newsgroups. First, subscription was made to all newsgroups in which pictures were posted. Second, those newsgroups with adult sexual interest in children (including references) were noted and accessed. The study showed that of the 40,000 newsgroups, 0.07% contains child pornography, child erotica and children in stages of undress (but not sexually explicit and therefore technically not illegal). A total of a quarter of 0.07% concerned child pornography directly (UNESCO 1999: 20, O'Connell 1998).

O'Connell (1998) identifies posters to paedophile newsgroups with a variety of roles, some of which might be ''promoting' and others 'detracting'. Promoting roles include:[43]

Infrastructure advice/coordinators: These people act as a protective buffer zone coordinating paedophile Usenet newsgroup activity and giving advice about the most appropriate way to respond to Flames, i.e., (anti paedophile reactionaries) in the following ways:

a) Writing Frequently Asked Questions (FAQ) texts to help child sex related newsgroup readers (especially new readers in the group), by pre-empting and answering any questions they might have about the group and how it operates.
b) Providing technical information about how to download and decode articles.
c) Giving advice about how to post anonymously by using anonymous re-mailers.
d) Making posts that are encouraging and supportive, and giving email addresses of the authors that afford new users the opportunity to comment directly to the authors via private correspondence, i.e. email.

Furthermore, infrastructure advice/coordinators also give advice on which newsgroups are the most suitable to post articles on – particularly those articles that contain images. O'Connell highlights that integration and acceptance into a virtual paedophile commu-

43 http://www.uclan.ac.uk/facs/science/psychol/rachel/crime1.htm

nity or network is not signposted in a traditional manner, although virtual rules and netiquette do very definitely exist. The infrastructure advice/coordinators would generally be the first contact for those who are new to the virtual paedophile world. They are the purveyors of the rules of conduct and adopt a hospitable role in outlining the various points of 'netiquette' that are imperatives to navigating successfully in the paedophile world. These people play a central role in the deviant process, although it may not always be clear whether they are committing an offence.

The community can also be broken down into roles undertaken by the members. This includes:

- Literature reviewers: these people provide detailed information regarding the content of paedophile related publications such as books and magazines, how to procure these items, and how to become a member of paedophile organisations such as NAMBLA and the address of the NAMBLA website.
- Story/fantasy generators: these posters directly engage in the production of fantasy material, by posting stories containing lurid accounts of sexual interactions between adults and children. It is impossible to know if these are real or fantasy accounts, although some are so bizarre as to strain anyone's credibility.
- Support people: the main role of these posters is to contribute to the non-threatening, facilitating and supportive context in which sexual interest in children can develop. Support people detail positive aspects of adult child sexual interaction, claim to disagree with coerced sex between adult and child and fully support consensual sex between adult and child. A particular feature of these postings is the support of the rights of 'boy' and 'girl' lovers, and drawing a distinction between paedophiles and child molesters.
- Posters and traders of child erotic and child pornographic pictures: those who actually engage in posting pictures are generally quite specific in what they do. Individual posters may fall into the following categories:
  A. Child erotica only
  B. Child pornographic only
  C. Hard core child pornography only
  D. Mixed child erotica and child pornography
  E. Multi-sex deviants

In addition, detracting roles include:

- Reactionaries: posters who aggressively react against the postings of paedophile newsgroup postings.
- Paedophile register propagators: people who post identification details of paedophiles.

According to Interpol the amount of child pornography available via the Internet has increased. There has been a steady increase in the size of seizures with each search, and

the numbers of seizures varied from 75,000 to 250,000 images depicting minors in sexual acts, and in some cases up to 500,000 images have been seized (UNESCO 1999: 12). Since 1992 the U.S. Customs Service have arrested more than 1,000 individuals for child pornography-related crimes and since January 2000, the Custom's Cyber Smuggling Centre has investigated more than 10,000 tip offs. In 1996, U.S. Customs' Operation Cheshire Cat started an investigation into a child pornography network known as the Orchid Club.

Evidence collected during the investigation in Operation Cheshire Cat led to the discovery of a much larger, more sophisticated child pornography trading ring known as the Wonderland Club, which as the investigation discovered had strong links to the United Kingdom (see box 7). The joint investigation between U.S. and British law enforcement agencies led to the arrest and successful prosecution of suspected ringleaders of the group.

BOX – 7
Alison and the Wonderland Club

The story of the *Wonderland Club*, the largest child pornography network on the Internet ever, started in **April 1996** in Greenfield, California.

Alison, ten years old, stayed the night with her school friend and a few days later her mother received a telephone call. This school friend's father, Ronald R., had been arrested for abusing a child. Mr. R. encouraged his daughter to have friends over to stay. One night in the Easter holidays, Alison's stay would become a horrible one. She was pulled out of a slumber party, taken into a computer room and was abused in front of a little camera (connected to a computer) while a dozen men were watching. Men from Australia, Canada, Finland and the U.S. typed in requests for R. to perform specific sexual acts with the child. Mr. R.'s molesting activities came to light because a local child had complained that Ronald had tried to abuse her. Ronald R. was sentenced to over a hundred years in prison in California and a dozen other men around the U.S. were sentenced to shorter jail sentences.

The electronic trail crossed U.S. borders and led to Hastings, Sussex. U.S. Customs had found an e-mail address of Ian B. on Ronald R.'s computer in California. In **October 1997**, Sussex police seized the computer of Ian B., a 28 year-old computer technician. A police computer forensics expert had examined the computer, in which more than 42,000 paedophile images had been stored, and through which 1642 images had been distributed to 17 other Internet users in the six days prior to Ian B.'s arrest. After Ian's computer had been examined for five months, evidence was discovered of an extensive and sophisticated club of paedophiles called Wonderland. The main purpose of the Wonderland Club was to exchange paedophile materials, pictures, movies, information, and very appallingly, sounds. The Club had its own committee, rules, and procedures. For example, in order to be admitted new members were requested to contribute 10,000 original images of child pornography. The Club operated very carefully out of a secure Internet Relay Chat (IRC) channel that could be accessed through a number of private servers. It often happened members vanished from one computer server, only to reappear on another server based somewhere else in the world. A „Traders Security Handbook" showed members how to use encryption to conceal images, confuse police, and what to do if arrested. Members who wanted to get in the private chat room had to pass seven security checks and were only known by pseudonyms such as „Satan", „Sheepy" and „Hopeful Spank Dad". The chat room was run

on a special software programme, known as „Sandra" or (how appropriate) „Alice" to its regulars, which acted as a gatekeeper denying access to anyone who was not a subscribed Wonderland Club member. Images were swapped through a direct File Transfer Protocol (FTP) connection to each connected computer.

In **April 1998** the National Crime Squad (NCS) set up Operation Cathedral to track down the British members of the Wonderland Club. Electronic trails had led to Stockport, Cheshire. In Stockport, Manchester police arrested Gary S., former RAF engineer, and found 20,000 images of child pornography in his computer. Gary's computer provided the police more up to date information on the Wonderland Club and improved the chance of online tracking. Gary S. turned out to be one of the key members. As he was actively abusing children and producing images for others, this enhanced Gary's status within the Club. Three members of the Club actually travelled to Stockport to Gary's home address and had pictures taken on his bed with the victims. Those pictures did not contain indecent poses but were apparently taken, as one of the members e-mailed them round the Net, as some remembrance of the visit to Gary's house. As one of the detectives of the Crime Squad stated: „…just so that they could get a buzz out of saying they'd met the stars of the movie." Gary S. has already been sentenced to 12 years in prison for the abuse of three children.

Police and computer specialists worked out a technique which enabled them to actually watch suspects on the Internet. Additionally, names and addresses of suspects' customer accounts were obtained from ISPs. As this was not enough, it had also to be proved that the suspects actually were downloading the child porn images, detectives of the NCS watched 13 addresses of Wonderland suspects.

Police tracked down „Hopeful Spank Dad" or „Spank daddy" the nickname of Gavin S., a 24 year-old computer technician from Dartford, Kent. Gavin S. had long online conversation with other Club members as for example with Ian B. who supported and encouraged Mr. S. in his paedophile activities. After the computer of Ian B. was seized, he had been allowed out on bail without conditions and police tracked him down to Charlbury, Oxfordshire where he was being watched at his home address. In **May 1998**, the NCS located Gavin S. in hut of the local Sea Cadets headquarters. Gavin S. was a volunteer youth leader, in contact with 25 boys and girls between the age of 10 and 18. The police had to continuously balance the need for evidence against the risk to children. Such as a undercover officer involved in the surveillance of Mr. S. stated: „When we took him to the Sea Scout hut, the heckles on the back of our neck all stood up on end and we were all concerned as to what our next cause of action should be, and we just ensured that whenever he was going to the Sea Scouts that we had the surveillance team with him to ensure that at no time when he departed did he take anyone with him. If at any stage he had the children with him on a one to one basis, or a two to one basis, then our instructions were to arrest him." By June, investigations of the NCS revealed 10 British suspects and up to 180 potential Wonderland Club members in 12 other countries.

In **July 1998**, the British police team briefed U.S. Customs on 90 suspected American Wonderland members and passed on lists of pseudonyms and e-mail addresses. U.S. Customs identified another key member, Scott A. in St. Charles Missouri. Also Scott A. appeared to be well respected within the network because he was actually abusing children and producing images on demand. According to a computer forensics expert of U.S. Customs „if you want a special request you would talk to him about certain things that you wanted to see him do the next time he's abusing a child he would do it for you." Among the members who traded child pornographic material Customs not only found stereotypical paedophiles, e.g. those who are exploring playgrounds, but also people one would never have suspected like those who were married and with children, a professor in the University of Connecticut, law students and medical students.

By now eight European countries were looking for Wonderland members. Also in Germany where the National Computer Crime Unit was haunting for a dozen suspected Club members. The Crime Unit examined computer logs, e-mails and images received from the UK National Crime Squad. German police tracked down „Ultima" to a government guesthouse near Bonn. Ultima, a civil servant in public, turned out to be a committee member of the Wonderland Club and the person to decide whether a candidate would be carefully examined for a new membership or would not be given access. Ultima had very close contacts to the leading persons, both to the UK and to the US.

By the end of August, thirteen countries were hunting for Wonderland suspects and although not all of them had been identified time was running out. Some members were becoming suspicious and started to secretly encode their images to hide evidence. Across the world police forces decided not to wait any longer and the Wonderland Club was about to be arrested. Getting in suspects' homes, securing evidence, and preserving evidence were some major concerns, moreover, police forces had also to prevent suspects from one country warning suspected members in other countries.

On **2 September 1998**, in 13 countries, more than a thousand police and child protection officers simultaneously raided 105 Wonderland members. Worldwide more than 100 computers were seized. The surveillance of and hunt for the Wonderland Club and its members, world's largest Internet child pornography network, resulted in the seizure of 750,000 paedophile and child porn images as well as around 1,800 computerized videos. According to detectives of the British National Crime Squad the images not just concern children running on the beach, but in some occasions the worst kind of abuse one could imagine, including people committing vaginal and anal rape on children as young as six and nine months of age. A chief inspector of the NCS comments: „Certainly one series that sticks in my mind is a series that was labelled 'Colby'. Colby would appear to be a child of no more than a year old and the initial images are of a young toddler, a very blond-haired lad, walking in a hallway in nappies. That image goes through some 20 or 30 slides and ends up with the most horrific abuse of the child and certainly, like the rest of the team, I guess that one image probably stays with you and that for me would be the most horrible that I saw."

Regretfully, the revelations about Wonderland are just part of the whole story. The identification of many victims remains a major problem. Three years ago, an 11 year-old Portuguese boy Rui Pedro M. had been kidnapped on his way to school and, since then, has never been found. Images of Rui Pedro M. were traded in the Wonderland network, for example, an image was found on the computer of one of the suspects, Gavin S.. Sadly, so far the Portuguese boy is the only child that has been positively identified.

On 13 February 2001, before Kingston Crown Court, seven Britons were sentenced for their participation in the Wonderland Club. Ian B. and David H. received 30 months, Gavin S. was jailed for 24 months, two other members were sentenced to 24 months, one member received 18 months, and the final individual was sentenced to 12 months. It is very likely that other child porn networks remain to exist on the Internet or new ones will emerge. This is what one of the Wonderland members, David H., had to say before he received his sentence: „They'll hide up and then they'll start their own channel and then they'll regroup, and the group will eventually be as big as it was with new members, with new pictures, and with all of the old pictures which are still floating out there."

Sources: BBC, Panorama (2001), U.S. Customs Service (2001) & ZDNet (2001)

Hate Speech

Hate speech remains a sensitive issue, though material, which attempts to incite racial hatred, is not universally considered to be illegal. In countries attaching a great value to freedom of expression and speech, any restrictive measures on these principles could be interpreted as a form of censorship.

The Simon Wiesenthal Centre for human rights in Los Angeles conducts research on hate sites annually and distributes the results in the interactive CD-ROM Digital Hate report.[44] According to the interactive Digital Hate 2001 report there are over 3,000 websites that can be understood as problematic (600 were recorded in 1997 and 73 in 1995),[45] as they are responsible for generating and distributing a wide range of potentially harmful material, from the promotion of terrorism, racial violence, anti-Semitism to hate music.[46]

Besides the overt issue of specific hate sites, there are also issues that concern the more publicly well known websites such as Amazon.com, Barnesandnoble.com, eBay, and Yahoo.com, where a difficult ethical conflict, between the right to publish and the right of individuals to be protected against literature that is seen to incite racial hatred arises. In November 1999 Amazon banned the sale of the English-language edition of 'Mein Kampf' on request of the German Minister of Justice Däubler-Gmelin (German law prohibits the sale of the German-language edition).

Without an international consensus on content-related issues and with the Internet crossing national borders and therefore circumventing national jurisdiction, it becomes almost impossible to enforce a total ban. Barnesandnoble was the other U.S. online bookstore that received a letter from the German Minister of Justice requesting them to withdraw the book from distribution. Contrary to Amazon's decision, Barnesandnoble.com decided not to withdraw the publication, unless it was left no other choice (Kettman 1999).

The same problem arises as far as the auction and sale of Nazi materials via websites such as Amazon, eBay and Yahoo. In France, Yahoo.fr, the French-language version of the English-language Yahoo.com, does not provide access to auctions of Nazi memorabilia, which would be illegal under French law. Despite this, the knowledgeable surfer knows that Yahoo.co.uk is a few clicks away. Therefore, the Paris judge's emergency ruling ordering the blocking of U.S. based websites, is not only almost impossible to implement, but utterly futile.

44 http://www.wiesenthal.com [as of 1999, September 20]

45 http://www.nua.ie/surveys/?f=VS&art_id=905354792&rel=true [as of 1999, November 12], and http://www.wiesenthal.com/feature/digitalhatecd.html [as of 1999, September 20]

46 http://www.wiesenthal.com/social/press/pr_print.cfm?ItemId=494

Chapter VI.
Cybercrime and its Consequences: Legal and Regulatory Considerations

As the individual cases discussed above demonstrate, there are many actors involved in the activities that fall under the umbrella term cybercrime and there are many ways in which a serious risk or threat can be posed to society, industry and the State. However, it is important not to overstate the risks and the extent of cybercrime. Relatively new media or new technologies always raise some concerns and almost always these concerns are exaggerated. It is very difficult to give definitive statistics on the amount of cybercrime that is actually committed for a number of reasons, which have been discussed above, but we can expect, given the potential of new technology to be exploited in order to commit a criminal offence; whether this be money laundering or cyber terrorism, that crime using ICT will increase, without sufficient legal and security structures to combat these acts.

Criminal organisations, ranging from transnational terrorists groups, transnational crime syndicates, fundamentalists, organised software and music pirating organisations to smugglers of black-market products, are all adapting or have adapted their structures and strategies in order to make use of the advantages that networked design offers. According to the United Nations Organisation (UNO), the new environment of the international financial network economy creates a breeding ground for the criminalisation of business and political life. Cybercrime may not have reached anything like the proportions of offline criminal activity in terms of economic loss or physical damage, but it is nevertheless, a significant problem and one that can be expected to increase in all of the areas that have been explored in this report, as well as in new novel areas. Indeed UK official crime figures suggest that crime on the Internet is the biggest growth area of criminal activity, in the year ending 2000, it reported that Internet forgery and fraud in England and Wales increased by 29% (70,000 offences were reported), making it the leader among other growth industries (Travis 2000: 4).

Financial Losses and Economic Impact

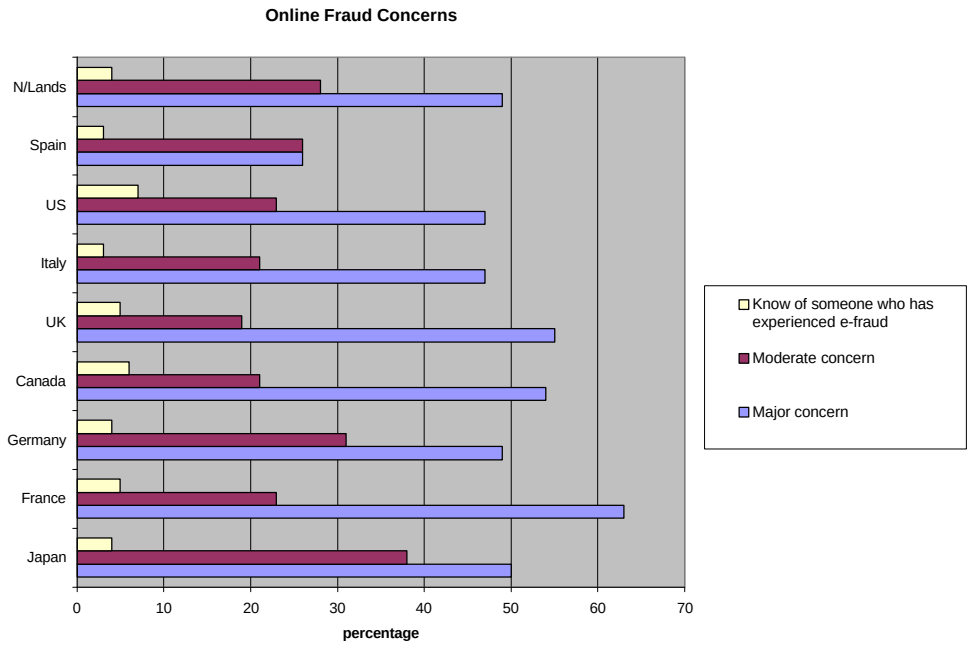
In the 2000 CSI/FBI survey of American companies, respondents reported a total of US$ 265,586,240 in losses due to cyber criminal activities; representing the fourth consecutive year that losses exceeded US$ 100,000,000. Between 1997 and 2000, the total reported losses amounts to US $626,055,495. According to 66 respondents an amount of US$ 66,708,000 of financial losses was the result of theft of proprietary information whilst 53

respondents reported losses of US $55,996,000 due to financial fraud. By far the greatest source of revenue loss was reported to be from viruses (US$ 29,171,700), sabotage (US$ 27,148,000), and unauthorised insider access (US$ 22,554,000) (Power 2000: 6–7).

The Centre for Strategic & International Studies (CSIS) states that almost all of the top Fortune 500 companies have experienced some form of intrusion by cyber criminals. The FBI estimates losses due to electronic crime, of around US$ 10 billion annually.[47] According to Computer Economics,[48] in 2000 the economic impact of virus attacks alone on information systems around the world amounted to US$ 17.1 billion a significant increase on the previous year when US$ 12.1 billion in losses were reported (Handelsblad 2000). The notorious ILOVEYOU virus and 40 related variants have caused an estimated US$ 8.7 billion in damage alone.

Quantification of cybercrime and financial losses incurred by companies, individuals, the public sector, as well as the State, need to be accounted for with far greater precision and clarity, in order to really understand the impact of cybercrime. A market research company, the Yankee Group, estimated that Mafia boy's DDOS attacks in February 2000 could result in US$ 1.2 billion in financial losses to business by adding loss of sales and advertising revenues, decrease in share prices due to security concerns, and the cost of upgrading the system against a repeat attack (Power 2000: 13). Until a more transparent and sophisticated system is developed to evaluate the costs of such events speculative figures will continue to cloud the whole area of the impact of cybercrime.

Figure 2.



Source: WWW. Marketer.com: Ipsos Reid 2001.

47 http://www.csis.org/pubs/cyberfor.html [as of 1999, October 12]

48 http://www.computereconomics.com/

Whatever the extent of the income losses are another problem arises concerning consumer confidence of online services. According to Forrester Research by 2000 only 4% of Internet users in France, Germany, Sweden, the Netherlands and Britain have purchased anything online – 40% of the sample also claimed that they have no intention of buying online in the following 6 months (McIntosh 2000). As figure 2 demonstrates the disparity between the level of computer crime and the public perception of the risks of cybercrime is great. The report surveyed 8,500 adults in 16 countries and finds that 46% of the adult population have a major concern about the potential for online credit card fraud- this was highest in France, but in all the samples the public perception of credit card fraud far surpasses the actual incidents that the respondents had heard about first hand.

The negative public perception of cybercrime is bound to slow down the growth of online activities, as consumers are suspicious of conducting transactions in the online world. Indeed Forrester research estimates that the lack of confidence in online security costs the e-commerce sector US$ 12.4 billion annually in lost sales. Moreover the Pew research centre recognises a trend where online consumers are increasingly wary of conducting transactions online because of infringements on their privacy (Despeignes 2001).

Legal and Regulatory Considerations

There are a number of legal and regulatory issues raised with the growth of a globally accessible medium like the Internet. The structure and capability of the Internet makes old regulatory paradigms, based on national borders acting in isolation of other nation states, ineffective. All the criminal activities discussed in this report have an international dimension – whether this involves the distribution and downloading of illegal content such as child pornography or credit card fraud, the potential to exploit the network of the Internet to circumvent national borders appears to be endless. This does not represent the death of the nation state as the central organisation that regulates many different spheres of public life. But, it does suggest that with mediums that are transnational and global in nature that enable crimes to be executed in one part of the world, which have consequences in another part of the world, international legal agreements and cooperation are essential for any effective measure to combat this problem.

Countering Hacks and Attacks

In their response to security breaches and hacking, Sieber (1998) suggests many States have developed new statutes or concepts that protect a formal sphere of privacy for computer data, by criminalizing the illegal access to, or use of, a third person’s computer or computer data. In this way the concept of the protection of a private sphere is not necessarily antagonistic with the concept of freedom of information. Subsequently, legislation covering wiretapping and unauthorised access to data processing and communication systems has been enacted in different countries (Sieber 1998: 69–70).

Table 4: Updated Legal Instruments.

Countries with Updated Laws										
Country	Data Crimes			Network Crimes		Access Crimes		Computer-related Crimes		
	Inter-ception	Modifi-cation	Theft	Inter-ference	Sabo-tage	Access	Virus	Aiding and Abetting	Forgery	Fraud
Australia	✓	✓	✓	✓		✓			✓	✓
Brazil		✓			✓	✓		✓		
Canada		✓		✓	✓	✓				
Chile	✓	✓	✓	✓	✓					
China		✓		✓			✓			
Czech Re-public		✓	✓		✓	✓				✓
Denmark		✓		✓						✓
Estonia		✓	✓	✓	✓	✓	✓	✓		✓
India		✓	✓	✓	✓	✓	✓	✓		✓
Japan	✓	✓	✓	✓	✓	✓		✓	✓	✓
Malaysia		✓				✓		✓		✓
Mauritius	✓	✓		✓	✓	✓	✓	✓	✓	
Peru	✓	✓	✓	✓	✓	✓				✓
Philippines	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Poland		✓	✓	✓				✓		
Spain	✓	✓	✓					✓		✓
Turkey		✓	✓	✓	✓		✓	✓	✓	✓
UK		✓		✓	✓	✓		✓		
US	✓	✓	✓	✓	✓	✓	✓	✓		✓

Source: McConnell International (2000).

The range of laws enacted by national legislators demonstrates a number of disparate approaches, with punitive measures applied to different levels of access intrusion. Sieber identifies these levels as:

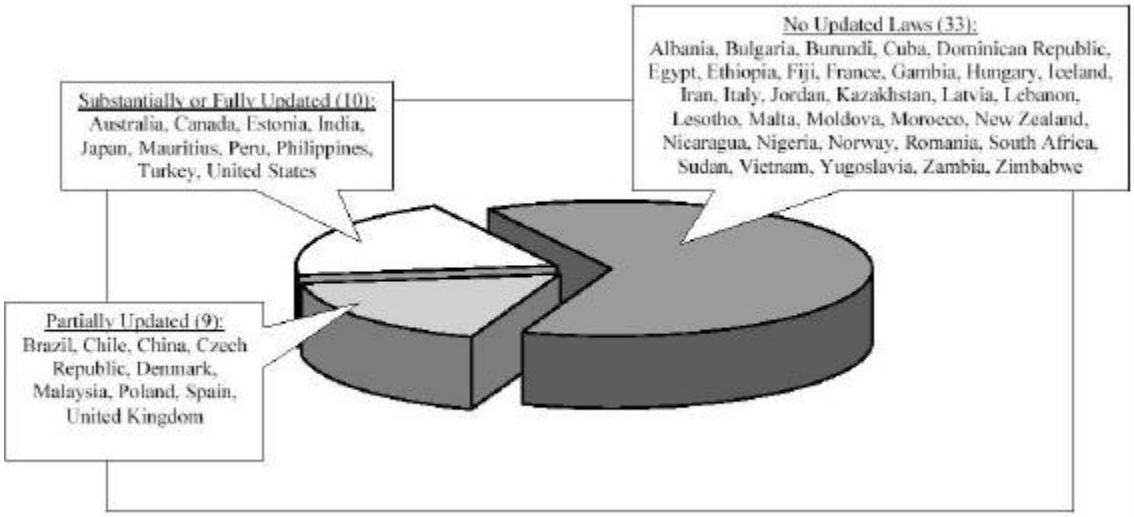
- Criminalizing unauthorised access to data processing systems (Australia, Denmark, England, Greece and the majority of states in the USA).
- Punishing access only if the accessed data are protected by security measures (Germany, the Netherlands, Norway).
- Punishing where the perpetrator has harmful intentions (Canada, France, Israel, New Zealand, Scotland).

- Punishing where information is obtained, altered or damaged (some states of the USA).
- Punishing where a minimum damage is caused (Spain).
- A combination of the approaches above (e.g., Finland, the Netherlands, the UK) with a 'basic' hacking offence and the creation of qualified forms of access (in a more serious ulterior offence) carrying more severe sanctions.

(Sieber 1998: 71).

The legal threshold when a hack or security breach actually becomes a crime in national law is therefore different- even amongst the Member States of the European Union. A far more liberal paradigm has been adopted in Germany and Norway, where only an intrusion on a network with security measures is seen as an offence, where simple access is deemed illegal in Australia and the UK. In Spain damage must be shown to have been caused for the security breach to be defined as illegal activity and in Canada, France and Scotland intent, rather than actual harm is enough to cross the threshold between legal and illegal activity.

Figure 3.



Source: McConnell International (2000).

Protection of Minors

As far as illegal and harmful content is concerned, balancing the moral spectrum of freedom of expression from the one side and the protection of the public interest on the other is central. At the international level, the UN Covenant and Article 19 of the Universal Declaration of Human Rights enshrines the principle of freedom of expression. The European Convention on Human Rights (ECHR) Art 10 is also applicable to the protection of minors and human dignity, as is the UN Convention on the Rights of the Child[49]

49 http://www.crin.org/crc/conv.htm [as of 1999, September 4]

(Articles 17, 31, 34). The protection of minors from harmful images has been an important issue on the European political agenda for several years. The protection of minors from certain kinds of content is enshrined in the Television Without Frontiers Directive,[50] the Green Paper on the Protection of Minors and Human Dignity in Audio-visual and Information Services[51] and more recently in the Action Plan on Promoting Safer use of the Internet.[52]

Categorising certain content as illegal might seem to be straightforward when it concerns, for example, child pornography or the distribution of material that is perceived to incite racial hatred. However, because of historical differences between national legal systems, there is no legal consensus on the definition of an offence such as child pornography. Sieber describes four different concepts of legal interests protected by the national legal systems:

- Protection of actors: protection of children and other persons requiring similar protection against exploitation of actors in pornographic scenes.
- Protection of mental and moral development of minors: protection of children from being handed over, or getting access to, pornographic images.
- Protection of human dignity: protection of general public from incidentally being exposed to pornography.
- Protection of public moral standards: protection of general morals in society.

(Sieber 1998: 88–89).

Combinations of the four concepts are reflected in different national legal systems. Thus, material which a particular individual country or region interprets as offending, could be interpreted differently in another cultural and legal context. The absence of a standard definition and lack of harmonisation has also been recognised at UNESCO's Experts Meeting on the Sexual Abuse of Children, Child Pornography and Paedophilia, in January 1999.

The above categories tend to concentrate on dissemination and reception processes rather than on the production of pornographic images involving minors. It is in this latter sphere (A) where real harm and the real victims of the operations of child pornographers can be identified, where children are sexually abused and exploited. Some of the cases discussed in this report demonstrate that the flexibility that ICT production affords to individuals makes it a particularly easy medium to utilise for people wishing to exploit children in this manner. A small digital camera, a computer with the necessary software, a small private space, access to an Internet connection and a victim, are the only requirements that enable people with intent to produce and disseminate child pornography online.

50 Directive 97/36/EC, available at http://www.europa.eu.int/comm/dg10/avpolicy/twf/newtwf-e.html [as of 1999, October 22]

51 COM (96) 483, final, available at http://www2.echo.lu/legal/en/internet/gpen-ann.htm [as of 1999, October 18]

52 Decision no 276/1999/EC, available at http://www.echo.lu/iap/decision [as of 1999, September 27]

The suppliers of child pornography are not the only problem for regulators to confront. Where there is supply there is usually demand for a specific commodity form and even where an offensive on supply side factors is successful, the architectonic of paedophile groups identified by a number of reports, would suggest the twilight zone in which these groups interact would continue to resurface in novel ways that are even more difficult to trace.

Protected and Unprotected Speech

Due to potentially harmful and illegal content on the Internet, an understanding of the question of balancing free speech, freedom of expression, the public interest and (inter) national security is vital. In order to determine when government regulation of an act of communication, whether peer to peer or one to many, is legitimate Pool (1983) refers to four strategies used by the U.S. Supreme Court which establishes four tests which have application to the examples and cases discussed in this report:

- Clear and present danger
- Balancing public interests
- Protected and unprotected speech
- Speech that merges into action

(Pool 1983: 59–73).

The application of the test, balancing public interest to the virtual environment, does not result in a clear distinction between what content is deemed to be in the realm of legitimate regulation by the State or not, as the boundaries between the two categories consist of grey areas where it is difficult to classify some areas in any one of the two groups (Pool 1983: 61–66). The question of how the public interest is served with the availability of bomb-making manuals is debatable, but one cannot assume that a causal relation exists between bombings and the commercially available bombing manuals available from a number of sources, including the Internet.

In terms of hate speech and literature that may incite racial hatred and offend certain groups in society national rules are extremely disparate. In America the privileging of a formal notion of free speech and the importance stressed on the principles of the First Amendment to the Constitution allow individuals to propagate views that are unacceptable in other countries. The fact that any individual in the world with access to the Internet can download these files may be anathema to other individuals in that community, but there appears to be little that a government can do if some responsibility for material understood as offensive is not placed on a legal undertaking, within its administrative borders.

Security, Conflict and Terrorism

The threat of cyber terrorism in combination with the threats posed by hacking have an increasing impact on policy decisions concerning national security as well as at the in-

ternational level (Denning, 2000). U.S. government officials are increasingly concerned about attacks from individuals and groups with malicious intentions, such as terrorists and rogue nations.

According to Vranesevich the military nomenclature of *physical risk assessment* may not always apply to *digital risk assessment.* Vranesevich questions the U.S. government's assumption that in many cases intrusions consist of what appears to be large scale organised attacks, perpetrated by organisations with extensive resources (i.e. foreign governments or terrorist organisations). Contrary to the idea that large organised actors can potentially launch full scale attacks on systems; he claims that the key to understanding and detecting aggressive attacks on computer networks lies in low density, low key intrusion that can lie outside detection because it does not stand out from other minor hacking attempts. Full-scale intrusion can be detected easily because it breaks with normal occurrences of intrusion, and would therefore draw attention to itself and trigger an investigation.

Hoffman (1998: 20–21) warns that commercially obtainable bomb-making manuals and operational guidebooks empower the amateur terrorist to be just as deadly, destructive, and even more difficult to track and anticipate than the professional terrorist. On the low end of the technological spectrum fertiliser bombs, as used in the Oklahoma bombing, and by Islamic radicals in the World Trade Centre bombing in New York in 1993, or by the IRA at St. Mary Axe and Bishop's gate in 1991 and 1992, are not only efficient devices but they also the most cost-effective weapon. The Bishop's Gate explosion is estimated to have caused US$ 1.5 billion in damage. The World Trade Centre bomb cost only US$ 400 to construct, but resulted in US$ 550 million in damages and lost business revenues (Hoffman 1998: 29).

Information networks and systems clearly have an important role to play in military strategies and logistics today. Recent examples of international warfare have been characterised by high tech and low risk strategies that can and should be expected to increase as a dominant template for international conflicts involving the developed countries, where casualties are unpopular with the public. However, low risk and high tech strategies have a price in that the systems used to deploy missiles and organise military structures and logistics are vulnerable to attack and intrusion from the hacker community. There are some signs, and expert opinion would suggest that these are increasing, that terrorist groups and other subversive organisations are beginning to understand the potential for exploiting vulnerabilities in ICT network technology. Hacker knowledge of security breaches could also easily be adapted to pursue more sinister and destructive objectives.

Privacy and Surveillance

Whilst it is important to recognise that the State does have a significant role to play in ICT development it should also be pointed out that there should be limits to how far the State should be allowed to exploit new technology to monitor and intercept communica-

tion. Intelligence is an important part of the role of the State in securing a safe environment for its citizens to live in, but there is a threshold that the State should not cross, where individual liberty is threatened. The sophisticated tracking and interception devices that the State has developed could potentially act as a real threat to the liberty of individuals, if these capabilities were abused by the State and exploited in order to collect information about the private lives of people, in areas where the State has no right to intrude.

Likewise the monitoring capacity of ICT is also being enthusiastically embraced by corporations and marketing companies, albeit for different purposes than the State. The possibility to closely record the consumer behaviour of computer users through devices like cookies can represent a serious infringement on the right of individuals to privacy. If cookies become collated with other details of an individual user, a data and consumer profile could be built up to a level of sophistication that is unsurpassed. In the near future television viewers may also be exposed to similar surveillance tools and the marketing industry may justify this on grounds of consumer service, but it is unlikely, given the responses to a variety of studies and reports that consumers will find such strategies acceptable.

The UCLA Internet Report states that privacy has emerged as the greatest concern about the Internet among users and non-users. The evidence produced above would suggest that although the exploitation of technology has been used to monitor and intercept information by States for a number of years, and continues to be used this way, there is a growing possibility that un-elected and unaccountable actors such as corporations may have access to similar surveillance technologies. At the current time tracking technology is largely restricted to the Internet through cookies. As television technology develops it should be expected that consumer monitoring will be attempted, in order for companies to map out a whole range of consumer data about what people watch, when and what transactions they conduct through electronic media. The importance consumers place on privacy could act as a powerful deterrent to developing new markets in this area.

As online transactions increase, so will the processing of personal data and the possibilities granted to marketing companies to collect data on users. Data mining in cyberspace is perhaps the most effective and powerful tool ever developed to track consumer behaviour, and does, in the final analysis, raise significant questions about the right of individuals to privacy.

Chapter VII.
A New Regulatory Paradigm?

Historically mass communication media and telecommunications have been regulated by nation states. A wide range of requirements have been placed on the communication sector institutions from universal service to positive and negative content requirements – what content producers should or should not do in the public interest. The State, or regional authorities in some countries, has been responsible for issuing licenses to broadcasters and the national legal apparatus has acted to protect various areas of private and public life, even where the State has traditionally taken on a minimal role i.e. the market model of the press sector. The balance between guaranteeing communication media and individuals the right to access and express their views, within certain parameters of acceptability; and the need to ensure security is integral to any system of regulation, and it subsequently provides the legitimacy of regulation in this sphere in the eyes of the citizens. This has historically encompassed a view that some media should be free of the State as well as the market, in order that communication should take place in a sphere where distorting influences can be minimised.

However, the Internet does not share the same characteristics as traditional media and its distribution capacity to a degree undermine previous instruments developed by nation states, who find themselves ill equipped to deal with something that possesses the ability to be utilised, distributed and disseminated from a globally dispersed system of computer terminals. Many transactions and digital flows of information simply overcome most of the traditional regulatory instruments that have been used to enforce social norms and legal codes. Doyle and Morris (1999) identify four regulatory models that could be utilised to regulate the Internet:

- National: existing nationally based instruments and rules could be adapted to account for the global distribution capacity of the Internet. The instruments will be enforceable in a specific State, but have no application in external territories.
- Regional and International: ‘clusters’ of nations could homogenise legal instruments and combine resources through multilateral agreements in order to develop a coherent regional strategy.
- Global: a universal set of codes and instruments that all States would share and enforce.
- Laissez Faire: self regulation by the market would act as the mechanism of regulation based on the classic liberal paradigm. The State, or States collectively would have a

> minimal role that would be restricted to intervention only when self regulation clearly breaks down.
>
> (Adapted from Doyle and Morris 1999: 9).

Any effective regulatory solution would realistically have to include all of these regulatory paradigms, to some degree and at different levels. What is essential is that any regulatory instrument must have the scope and scale to be legally enforceable and effective. In this context some pooling of sovereignty is inevitable- no nation state is capable of regulating the Internet in isolation, and there appears to be recognition of this in recent developments.

Industry Regulation

There are a number of effective methods that can be used in order to prevent unacceptable material being consumed by minors, including sophisticated filtering devices that allow a number of subject related topics and keywords to be blocked at receiver level. Internet client and server based filtering systems include: allow or white lists, deny or black lists, keyword matching, over blocking, keyboard monitoring, self-rating (ICRA), and third party rating. The second solution is what is commonly referred to as the notice and take down approach which involves making the host service provider responsible for being fully aware of illegal content, and subsequently placing on them the obligation to delete and control or block the offensive data.

There is also the option of a code of conduct that is usually set up by self regulatory organisations or by national associations of ISPs. Such codes of conduct make it obligatory for Internet providers to adhere to certain rules and in some cases to cooperate with criminal law enforcement authorities. Codes of conduct of international on-line providers have the potential, in the form of a ‘softlaw’ to become forerunners for a more satisfactory international agreement.

The responsibility of ISPs for regulating illegal content goes beyond the need for self regulation and in this sense Sieber (1999) identifies self regulation as part of six other regulatory approaches that can overlap or combine:

1) General criminal law principles
2) Special press regulations and cascade liability
3) Independent responsibility
4) Procedural model
5) Specific obligations on the ISPs
6) Self regulation

State Regulation

The State alone clearly does not have the necessary legal instruments, international scope or manpower to deal with criminal activities that are either conducted in cyber-

space or use ICT to aid or commit some form of crime. The Internet and other networks do not abide by old regulatory models of nation states, based on national boundaries. However, this is not to suggest the State does not have a role in regulating ICT. Its future role is integral to the development of regulation in the area of computer related criminal activities, but it would be absurd for nation states to act in isolation of each other. For effective regulation at the State level the crime must be planned, executed and affect a victim (whether defined as an individual or a legally established undertaking) within those specific territorial borders. Whether one uses the case of the production or possession of child pornography, credit card fraud or hacking, the spheres of the crime are increasingly geographically dislocated and therefore international cooperation between States to combat and investigate cases of cybercrime is essential.

There are significant functions within the State that governments can promote such as best practice and information campaigns, notifying individuals and companies about the risks in transactions online and how people should use the Internet safely. Hotlines to allow people to report all sorts of computer related offences would encourage individual responsibility and promote common sense solutions to things like parents worried about their children downloading pornography. As Naughton (2000) suggests the easiest solution to such a problem is to take computers out of private spaces and place them in living rooms where parents are able to keep an eye on the minor's Internet activity.

These are common sense solutions that begin at the grass roots level. In terms of other forms of cybercrime the problem requires a legal and political solution, which is effective on an international level. In this respect the Council of Europe's Draft Convention on Cybercrime that was agreed upon by the European Committee on Crime Problems at its 50th plenary session, June 2001, is a significant attempt at developing an international agreement to deal with the problems that crime in cyberspace creates for national legal systems. The Convention is the result of 4 years cooperation by a number of countries in the field of ICT related criminal activities, with input from experts representing the governments of the members of the Council of Europe, Canada, Japan and the U.S. amongst others.

The Council of Europe Draft Convention on Cybercrime

If the Council of Europe's Committee of Ministers adopts the Convention (it is expected to take up the matter in mid September 2001), then it will be opened up to both member and non-member state Parties to sign and then it will proceed to be ratified by national parliaments. The instrument will represent the first international treaty that attempts to combat criminal offences that utilise computer networks in order to commit a whole range of criminal activities. The offences covered by the Convention range from child pornography, fraud to copyright infringements and piracy. Its central aim, as stated in the preamble to the text consists of creating a „common criminal policy aimed at the protection of society against cybercrime… in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effec-

tive and to enable the collection of electronic evidence of a criminal offence" (COE 2001b: 3–4). The Convention's purpose is therefore not to replace international instruments (whether bilateral or multilateral), but to supplement existing instruments with a set of shared legal foundations, in order that nation states are better equipped to deal with the international scope of cyber criminal activities. The principal objectives are therefore:

- The harmonisation of domestic criminal law in areas where cybercrime is evident.
- Develop and incorporate into national law investigative and procedural powers in order for enforcement authorities to have the necessary national legal tools to pursue investigations into criminal activities that exploit or in some way utilise ICT.
- Establish a set of rules for international cooperation in the field of cybercrime.

(Adapted from COE Explanatory Memorandum 2001b: 4).

The Convention basically consists of three parts that 1) identifies areas that can be understood as cyber criminal activities 2) grants legal rights to legal and enforcement agencies, and 3) lays the basic foundations for international cooperation and jurisdiction in the field of cybercrime, defined widely in a number of areas.

The range of offences identified by the Convention cover activities related to computer crime i.e. child pornography as well as crime committed by means of a computer system. The act of committing a criminal offence is based on two premises- 'intentionality' and 'without right,' and in some areas the case of intentionality must be supported with harmful intent. These two conditions of criminal activity are built into the text to enable activities to be pursued that are seen to be necessary in order to undertake and update security measures and to account for other areas such tracking devices which are placed on user hard drives like cookies. Intentionality and without right therefore refer to unauthorised access where permission to enter or manipulate any aspect of a computer system has not been granted. In the former area there is an attempt to develop instruments to allow law enforcement to better deal with crimes that deal in non-tangible objects i.e. computer stored or transmitted data rather than tangible items that are associated with traditional crimes.

The first section of the Convention is dedicated to listing the offences, which it defines within the scope of cyber criminal activities. The range of offences include ones that have a long history in the offline world where criminals have evolved new techniques to utilise the advantages of new technology, as well as novel crimes that may have equivalents in the offline world, but are nevertheless more or less exclusive to the online world (i.e. DDOS attacks and hacking).

Articles 2–11 define the range of activities that the Convention attempts to combat they include:

Table 5: The Offences Identified as Criminal Offences by COE Convention on Cybercrime 2001.

COE Convention Articles	Activity Covered
Art 2 Illegal Access	Infringement of security measures
Art 3 Illegal Interception	Intercepting non-public transmissions
Art 4 Data Interference	Damaging, manipulating or deleting information
Art 5 System Interference	Hindering (DDOS) or damaging data on a system
Art 6 Misuse of Devices	Supply or exchanging tools to commit an offence
Art 7 Computer Forgery	Relating to inauthentic data used for illegal activity
Art 8 Causing of Loss	Causing loss of property for economic gain
Art 9 Child Pornography	Number of offences relating to all spheres of pornography
Art 10 Copyright	Piracy and distribution
Art 11 Aiding and Abetting	Assisting the planning or execution of a cybercrime

Source Council of Europe 2001b.

Article 9 covers a number of activities related to child pornography, covering areas of production, dissemination, reception and storage. Drawing on the principles of the Council of Europe's Convention for Human Rights and Fundamental Freedoms, the Convention reiterates the protection, under the rule of law that children are granted against a number of exploitative practices including pornography. The Convention defines a number of illegal activities related to child pornography including producing, acquiring, offering, distributing and possessing pornography defined as in Art 9, section 2, paragraphs A to C:

A. A minor engaged in sexually explicit conduct.

B. Person appearing to be a minor engaged in sexually explicit conduct.

C. Realistic images representing a minor engaged in sexually explicit conduct.

(Art 9, Section 2, COE 2001b).

The term minor is established to be any person under the age of eighteen, though the Parties, in line with domestic law have the right to lower the age limit to sixteen where domestic law stipulates a lower age than eighteen.

The Convention therefore covers a wide range of illegal activities related to attempts to breach security measures of computer systems, interception of data to protect the privacy, fraud and forgery, child pornography and DDOS attacks, and is fairly comprehensive in identifying the criminal activities which utilise ICT in some way to either enter a system, disrupt or manipulate a system or distribute harmful images or data (defined either as an infringement of artist copyright or causing harm to minors). Whilst the need to police these areas is largely uncontroversial, the powers that would be granted to au-

thorities in order that they could pursue investigations into cyber criminal activities on ratification of the Convention into national law are more controversial.

Procedural law and common provisions applied to computer related crimes pursuant of Arts 2–11 establish the scope of the procedural provisions enabling criminal investigation under the protection of domestic judicial or independent supervision. The articles grant national authorities powers of data retrieval and confiscation, search and seizure of a computer system, access to traffic information about individual users and the right to intercept 'real time communications.'

Art 21 empowers authorities to collect information and data through technical means (or oblige a service provider to collect on behalf of the authorities) enabling law enforcement agencies to collect certain content of 'specified communications.' This enables relevant authorities to monitor the *content* of communications either directly from accessing a computer system or using tapping devices and surveillance tools. Because of the perceived difficulty in confronting criminal activity in cyber space the need to identify and locate communication flows is seen to be essential to allow effective legal enforcement to be executed.

The Convention defines two forms of communication data that law enforcement agencies will have the power to intercept or retrieve- information traffic, which is data relating to information such as identification tags, origin, destination, time, date and size (Art 1 Paragraph d) and content data. The collection of traffic data can either be executed through the State or the State could oblige the ISP companies to assist the legal authorities in collecting certain information about communications, if the Convention comes into force. This is also restricted by the Convention in order not to endorse 'fishing' for data and random monitoring and data collection and the Convention states that access to information about traffic data must be related to a specific instance where a criminal activity is being directly investigated.

The provisions on the interception of content data would allow the relevant authorities to use similar techniques such as traditional telephone tapping. Because of the potentially ephemeral nature of computer data and the non tangible nature of the crimes, the Convention understands content monitoring of real time communications, defined as 'the meaning or purport of the communication,' as essential to the pursuit of an individual or individuals involved in a criminal offence using ICT. The monitoring of real time communication is understood by the Convention in far more serious terms than traffic data monitoring due to the possibility of serious infringements on civil liberties. The use of the latter power is therefore restricted by the Convention to an interception relating only to 'a range of serious offences to be determined by domestic law' (COE Explanatory Memorandum 2001d: 23). What offences therefore can be defined as serious enough to invoke a category of serious offence is therefore left to the Parties to decide within the field of domestic law and is understood by the Convention as already determined by the very fact that such laws are already listed in national laws.

Conclusion

The Convention's attempt to harmonise some aspects of national law in order that the increasing problem of cybercrime can be confronted with a set of more coherent international instruments, allowing a greater degree of cooperation in criminal investigations and prosecutions across borders, is a necessary move by nation states. As the cases in this report demonstrate cybercrime is a global problem, both in terms of its execution and consequences.

The key to the success of the Convention however, is how it is implemented and the balance between individual liberty and security. The criticism from freedom of speech groups is that the Convention focuses on, and privileges law enforcement, and grants the legal authorities a wide range of powers to seize, search and monitor an individual's on-line activity without due attention to the question of an individual's rights to privacy. In a fully developed democracy with a fully developed legal system that can be used to protect these freedoms the problem may not be critical. However, in States where the rights of the individual are not as respected by the State, this may cause a far greater problem. Human Rights groups cite a number of nations where the State could use the powers granted by the Convention negatively in order to oppress and monitor individuals who carry out perfectly legitimate activities (Waldmeir 2000: 17).

The Convention also does not approach the question of commercial monitoring and surveillance of users. Indeed it accepts that companies have a certain right to utilise certain tracking strategies such as cookies as well as continue sending unsolicited emails (spamming). Such practices, the Committee claim 'should only be criminalized where the communication is intentionally and seriously hindered' (COE Explanatory Memorandum 2001b: 13). The criminalisation of DDOS attacks which are seen to hinder and in many cases cripple websites is therefore understood as an illegal activity, whilst at the same time high frequency and high volume spamming is seen not to cause hindrances. However, the Convention does state that a Party may introduce measures in order to combat privacy intrusion of commercial actors who employ strategies such as spamming. This should be seen as an important absence from the instrument, especially as a number of reports suggest that consumer surveillance is highly unpopular with the public and perceived to be a serious intrusions on an individual's right to privacy. There is enough scope within the text for Parties to pursue such initiatives within national borders, as regulation of company behaviour can be implemented in a number of spheres including market location and the States should clearly take action to regulate such activities in the consumer and individuals' interest.

Although the Convention has predictably remained flexible, to take into account the different legal traditions in the participating countries, there are some very constructive and necessary moves in the Convention to produce a better and more efficient system to combat cybercrime. The challenge is to enact the Convention into national laws whilst guaranteeing its spirit is implemented, in order to ensure that States do not use the sig-

nificant powers granted to authorities to police the Internet by the Convention, to abuse the rights of the individual.

Chapter VIII.
Conclusions: Between Security and Individual Freedom

The report has discussed a number of different types of cybercrime that in their own way pose different challenges to legal enforcement agencies and governments. The broad array of crimes that utilise ICT in order to commit a crime against an individual or community, minimally present challenges that require action to be taken in the offline world. These range from serious crimes committed against the State such as terrorism, fraud and deception to the production and distribution of child pornography.

Cyberspace, like any other social space where individuals interact represents a space that cannot be separated from the physical world, where modes of behaviour have developed within certain relationships that have evolved, for the past two hundred years in a world system of nation states. The Internet challenges the perception of sealed national borders that can be policed and regulated by nation states. Indeed the capacity of computer communications to bypass legal and State authorities on the scale of the Internet is probably unprecedented in the history of communications. Again, mirroring the physical world there is the good and there is bad and in this sense the good must be encouraged and the bad discouraged, and where it cannot be halted the law enforced, through legally endorsed instruments which enable legitimate authorities to take action against offenders.

As the above cases of cybercrime suggest there is the potential to commit a wide range of crimes using new technologies and the Internet. The breadth of the crimes range from traditional cases of fraud to the growth of twilight zones where illegal activities can be nurtured, within a supportive community that relies on a global network of individuals. Race hate websites containing information that many societies would deem illegal allow individuals access to prohibited views and information; bypassing ordinary nation state instruments that act to regulate the kind of information that reaches the public domain through traditional mass media.

There is almost universal agreement about the need for some form of regulation in order to control cybercrime in its various forms. The big difference between the actors in the debate about regulatory structures is who should regulate, and once this has been decided what should be regulated and how. This is the key issue.

Industry actors argue that self regulation is the most suitable framework to ensure the Internet is used in a manner that respects individual privacy. They argue for a legal framework that tackles issues such as serious crime, whilst at the same time leaving the

larger issue of privacy to the industry. State regulation is seen to potentially hinder the development of ICT and e-commerce at a time when the dot.com companies have suffered a huge blow from their decreasing values on NASDAQ.

In this context the development of self regulatory devices in order to regulate certain aspects of cybercrime such as music piracy are in progress. In July 2001 the technology company Macrovision released the first 'anti piracy' CD which has undergone tests in California. The SafeAudio system both stops high quality CDs being reproduced from copy to copy as well as stopping the exchange of files over the Internet. Any copy of a CD would be characterised by a decrease in sound quality by distorting the content of the original CD, by contaminating the original content with 'grossly erroneous values' which adds a hissing noise to the content Fox 2001: 22).

Self regulation certainly has a part to play in the promotion of a safe environment for users to participate in a wide range of activities on the Internet, from participating in chat room discussions to online transactions. Current initiatives to encourage self regulation include the establishment of a Pan European association (Euro-ISPA) representing Internet provider associations of the European Union countries, Internet Content Rating for Europe (INCORE), Internet Hotline Providers in Europe (INHOPE), and an international effort to manage and develop an acceptable voluntary self-rating system through the Internet Content Ratings Alliance (ICRA)53 (Price and Verhulst 1999). But even these have faced obstacles related to different national laws and standards. There are however, far deeper conflicts of interest with the idea of a self regulatory paradigm. On one hand Internet companies and ISP's insist on universal service to increase their profits and extend their market, and wish to target their consumers in personalised way. On the other hand, protection of personal privacy and access to information are relevant rights for citizens. The rights of the latter actors have to be balanced against market interest and intrusion through information retrieval and storage.

The State has a responsibility to protect individuals from intrusion by corporations that new technologies make possible. Commercial monitoring is not discussed in any detail in the Convention and this certainly needs further discussion and public debate. The significant surveillance tools developed by the advertising and marketing industries may not be a crime in the same league as say credit card fraud or terrorism, but it does nevertheless pose a serious ethical question as to the extent that communications mediums be allowed to track and monitor the behaviour of their users. In this respect the self regulatory paradigm promoted by industry actors is insufficient- it has a part to play, but this must be supplemented with State regulation in both positive and negative spheres. Indeed it must be ancillary to the legal and social norms that already exist in the offline world

53 Established by among others AOL, Bell Canada, Bertelsmann Foundation, British Telecom (BT), Cable & Wireless, Demon Internet, IBM, Electronic Network Consortium (Japan), EuroISPA, Internet Watch Foundation (IWF), Microsoft, T-Online and Uunet. ICRA's mission is to develop, implement and manage internationally acceptable voluntary self-rating system which provides Internet users worldwide with the choice to limit access to content they consider harmful. ICRA has received the RSAC assets including the RSACi system that provides consumers with information about the level of nudity, sex, language, and violence on web sites.

and a democratic States should create a framework where industry actors are obliged to act in a certain manner to ensure that the Internet is a safe place to communicate.

Privacy and security are both essential to the freedom of the citizen. Without both of these inviolable rights citizenship would be impoverished, indeed the ideal of a democratic system of government is that it defends and upholds both of these rights in order that individuals can live private and public lives, without undue interference or threat. The problem is however, the balance between these two central objectives and how regulation and the relationship between the institutions of the State, the market and individuals is maintained. Any regulatory response to the Internet will have to necessarily address the problem of balancing the safety of citizens with the right of individuals to participate in communication without coercion, and with the knowledge that they will not be persecuted for writing or speaking in the public domain. Despite claims to the contrary many nation states already have such tools and normative constraints that define the relationship between negative interference from the State and positive interception of activities that are perceived to endanger or threaten the security of people that share a legal community. At the same time the failure of the Convention on Cybercrime to incorporate an article outlawing material online understood as racial propaganda or likely to incite racial hatred is a reflection of some of the difficulties in agreeing, on an international stage, as to what should or should not be classified as illegal material.

Although tracking and monitoring capabilities developed by the State lead to a number of reservations about the right of individuals to live private lives without surveillance, it is important that legal enforcement agencies have the necessary tools; in order that they can satisfactorily pursue individuals who commit cybercrime. These activities may be conducted without infringing on citizens' rights. There are by the same token, limits to how far the State should be permitted to intrude into the private lives of individuals and these parameters between public and private space that have been established in healthy democracies in the offline world need to be applied in the context of the online world.

The State's role in regulating the Internet cannot only be seen to lie in the negative sphere. Government has an important part to play in areas that go beyond law enforcement and detection. Legal criminal policy needs to be supplemented with wider public involvement in order that the public not only plays a part in taking advantage of the opportunities of ICT, but also promotes safe use of the Internet. Public information campaigns cannot only be educational and informative, but also a valuable source of information. With clear lines of communication such as hotlines they could help law enforcement agencies pursue cyber criminals. In this respect the European Union's decision to adopt a Community Action Plan on Promoting Safer Use of the Internet is a constructive move forward.

Whilst many of these initiatives can be undertaken within the confines of the nation state, the larger issue of how to regulate the Internet cannot be effectively dealt with within the paradigm of national regulation. Global communication facilitates international criminal activities and although much serious crime entails an international di-

mension the ease that ICT enables international crime to be committed makes it a very difficult area to enforce with fragmented and disparate legal instruments, which can be easily circumvented and can, as a number of cases have illustrated, lead to offenders being identified, but escaping prosecution.

International treaties and agreements alone are not a solution to the problem of illegal activities that exploit new technologies. The crime might be executed in cyberspace, but they are actually conducted in the offline world as any other criminal offence. Law enforcement agencies with a knowledge of online crime is crucial, but probably as vital is the availability of structures of law enforcement in the offline world that can trace and prosecute offenders. Legal instruments will count for nothing without the manpower to trace and solve Internet based criminal activities. In this context there is a clear need for training and development of legal enforcement officers supported with more sophisticated security measures such as fire walls. This could be achieved with the pooling of both resources and knowledge.

Although legal instruments are beginning to be introduced to combat cybercrime there is still the problem of pursuing and actually identifying individuals who are responsible for committing any of the above listed infringements. Hackers break into networks using scripts that allow identification and therefore software has been developed that recognises hacker scripts and known hackers. The software used to undertake this task is regularly updated in order to monitor any new scripts that have been developed, to ensure that the defensive systems are continuously able to identify intrusions in network systems. However, according to the Canadian based hacker group K2 a piece of software known as chameleon can camouflage scripts and make them look like they are different, every time they are used to enter a network. The script remains the same, but escapes identification by intruder detectors. In this respect legal instruments may help legally established agencies to combat cybercrime in its various forms, but it cannot be expected to act alone. A whole system of protective measures would need to be developed; to make cyberspace a secure place that people can conduct transactions and search for information, without the dangers posed by criminals who appear to easily circumvent the existing arrangements.

In sum, although the Convention on Cybercrime is a first tentative step and presently there is no agreed global regulatory norm for regulating the Internet to account for cybercrime. More countries all over the world are taking cybercrime far more seriously today and there are positive moves to create a more coherent framework to combat cybercrime; in order to protect users of network services. Due to the dynamic nature of ICT this will need to be continually updated and reassessed with the support of both States as well as industry actors.

Ultimately an effective instrument will need to be international and it will have to be implemented by nation states in the spirit of democratic freedom. Whether the balance between individual privacy and the need for the State to apply legally endorsed codes to the online world in a fair and just manner, will be achieved in many parts of the world,

is a significant problem given the human rights records of a number of countries that may be Parties to the Convention. In this sense the Convention is open to being exploited by regimes that could interpret it widely, rather than in the spirit that which it has been developed. Nevertheless a legal instrument in itself is insufficient and a whole set of resources will need to be deployed in the offline world in order to bring the issue of cybercrime into the public eye and where a balance that respects human rights with privacy and safety can be achieved through regulatory standards which have historically defined the parameters between the State, the individual and the market.

Glossary of Terms

Allow List Filtering: Users can only access the list of sites supplied with, and supported by, the system. Access to all other sites is denied.

Browser: Client software that allows a system to read information on the World Wide Web.

BBS (Bulletin Board system): Areas within the Internet where messages and announcements can be posted.

Client: Any program that uses the service of another program. On the web, a web client is a program, such as a browser, editor, or search robot that reads or writes information on the web.

Cookies: Small data packets created by a website server and stored on the Internet user's hardware, while a copy may be kept by the website. They are a standard part of HTTP traffic, and can as such be transported unobstructed with the IP-traffic. A cookie can contain a unique number which allows better personalisation than dynamic IP-addresses. It provides a way for the website to keep track of a user's patterns and preferences. It is possible for the Internet user to have the browser disable cookies or warn before cookies are accepted.

Cryptography: A discipline that embodies principles, means and methods for the transformation of data in order to hide information content, establish its authenticity, prevent its undetected modification, prevent its repudiation and/or prevent its unauthorised use.

DDOS (Distributed Denial of Service): An attack with the goal of preventing legitimate users of a service from using it. A distributed denial of service attack can come in many forms. Attackers may flood a network with large volumes of data or deliberately consume a scarce or limited resource, such as process control blocks or pending network connections. They may also disrupt physical components of the network or manipulate data in transit, including encrypted data.

DSL (Digital Subscriber Line): A technology that dramatically increases the digital capacity of ordinary telephone lines (the local loops) into the home or office.

Exponential Networks: Networks composed of various nodes (or points) that have roughly the same number of links. It can be compared to highway networks, in which the nodes are the cities and the links are the highways.

FTP (File Transfer Protocol): A protocol used to transfer files over a TCP/IP network (Internet, UNIX, etc.). Allows a user on one host to access, and transfer files to and from another host over a network.

Hacking: Refers in the first place to the imaginative and the unorthodox use of any artefact. Currently, the term refers to the unauthorized access to and subsequent use of other people's computer systems.

HTML (Hypertext Markup Language): A computer language for representing the contents of a page of hypertext; the language that most web pages are currently written in.

HTTP (Hypertext Transfer Protocol): A computer protocol for transferring information across the Internet in such a way as to meet the demand of a global hypertext system.

IP (Internet Protocol): The protocol that governs how computers send packets across the Internet.

Keyboard Monitoring: Check for inappropriate input on the keyboard against a preset list. This technique is best for outgoing information such as credit card numbers and personal information in chat rooms or emails.

Keyword Matching: A flexible filter technique that analyses downloaded material and blocks any site containing previously determined unacceptable words or phrases. If the filter finds any unacceptable matches, it will either completely block access to the site or the offending words will be stripped from the page when it is displayed.

LAN (Local Area Network): A network of all the computers linked at a single location.

Modem: A device that adapts a terminal or computer to an analogue telephone line by converting digital pulses to audio frequencies and vice versa. The term usually refers to 56 Kbps modems (V.90), the current top speed, or to older 28.8 Kbps modems (V.34). The term may also refer to higher-speed cable or DSL modems or to ISDN terminal adapters, which are all digital and technically not modems.

Packet Sniffer: A packet sniffer is a program that captures data from information packets as they travel over the network. That data may include user names, passwords, and proprietary information that travels over the network in clear text. With perhaps hundreds or thousands of passwords captured by the sniffer, intruders can launch widespread attacks on systems. Installing a packet sniffer does not necessarily require privileged access.

Probe: A probe is characterised by any unusual attempt to gain access to a system or to discover information about the system. Probing is the electronic equivalent of testing doorknobs to find an unlocked door for easy entry. Probes are sometimes followed by a more serious security event, but they are often the result of curiosity or confusion.

Protocol: A language and a set of rules that allow computers to interact. Examples of which include FTP, HTTP, and NNTP.

Scan: A scan is a large number of probes with an automated tool. Scans can sometimes be the result of a misconfiguration or other error, but they are often a prelude to direct attack on a system that the intruder has found to be vulnerable.

Server: A program that provides a service (typically information) to another program, called the client. A web server holds web pages and allows client programs to read and write them.

Server-based Filtering Systems: Filters are installed either at a central location maintained by a network administrator at the institution or remotely where an Internet Service Provider (ISP) administers them. In the second instance, filtering is one of the services available to subscribers to the ISP.

Smart Card: a plastic card the size of a credit card that contains an integrated circuit (IC) chip that makes it 'smart'. This microprocessor allows an immense amount of information to be stored, accessed and processed either online or offline. Smart cards can store several hundred times more information than conventional cards with a magnetic stripe.

TCP/IP (Transmission Control Protocol/Internet Protocol): A computer protocol that allows one computer to send the other a continuous stream of information by braking it into packets and reassembling it at the other end, resending any packets that get lost in the Internet. TCP uses IP to send the packets, and the two together are referred to as TCP/IP.

Traffic Data: Are the data needed by the protocols to execute the proper transmission from the sender to a recipient. Traffic data consists partly of information of the sender and partly of technical information generated automatically during the process of sending an email (i.e. date, time sent, and type and version of email client).

Trojan Horse: Is a malicious code usually hidden in legitimate programs or files that attackers have altered in order to disrupt systems.

Viruses: Are also self-replicating programs, but usually require some action on the part of the user to spread inadvertently to other programs or systems. These sorts of programs can lead to serious data loss, downtime, denial of service, and other types of security incidents.

WAN (Wide Area Network): Any Internet or Network that covers an area larger than a single building.

Worms: Are self-replicating programs that spread with no human intervention after they are started.

References

Agre, P.E. & Rotenberg, M. (1997) Technology and Privacy: The New Landscape. Cambridge Massachusetts: The MIT Press

Albert, R. Jeong, H. & Barabási, A. (2000) Error and attack tolerance of complex networks. Nature, 406, 378–382. (WWW-document). URL: http://www.nature.com/cgitaf/DynaPage.taf?file=/nature/journal/v406/n6794/full/406378a0_fs.html (as of 2001, March 30)

Allen, J. Christie, A. Fithen, W. McHugh, J. Pickel, J. & Stoner, E. (2000) State of the Practice of Intrusion Detection Technologies. (WWW-document). Pittsburgh: Carnegie Mellon University, Software Engineering Institute. URL: http://www.sei.cmu.edu/pub/documents/99.reports/pdf/99tr028.pdf (as of 2000, June 26)

Arlen, G. (2000) Getting Serious About Set-Top VOD. Broadband Week. URL: http://www.broadbandweek.com/news/0010/print/0010_opinion_arlen.htm (as of 2001, February 28)

Arquilla, J. Hoffman, B. Lesser, I. O. Ronfeldt D. and Zanini, M. (1998). Countering the New Terrorism. (WWW-document). URL: http://www.rand.org/publications/MR/MR989.pdf (as of 1999, September 27)

Arquilla, J. & Ronfeldt, D. (1998a) The Zapatista Social Netwar in Mexico. (WWW-document). URL: http://www.rand.org/publications/MR/MR994/MR994.pdf/ (as of 2000, September 7)

Barua, A. Pinnel, J. Shutter, J. & Winston, A.B. (1999) Measuring the Internet Economy: An Exploratory Study. (WWW-document). The University of Texas at Austin, Centre for research in Electronic Commerce. URL: http://cism.bus.utexas.edu/works/articles/internet_economy.pdf (as of 1999, October 4)

Barry, R. (2001) Seven Britons Guilty over Child Porn Ring. ZDNet. URL: http://www.zdnet.co.uk/news/2001/1/ns–20151.html (as of 2001, February 21)

Batista, E. (2000) Wireless Phone Hack Attack? Wired News. URL: http://www.wired.com/news/print/0,1294,38557,00.html (as of 2000, August 31)

Berners-Lee, T. (1999) Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by its Inventor. New York: HarperCollins Publishers

Bertelsmann Foundation (1999) Memorandum on Self-regulation of Internet Content. (WWW-document). Gütersloh (Germany): Bertelsmann Publication. URL: http://www.stiftung.bertelsmann.de/internetcontent/english/frameset_nojs.html (as of 1999, September 16)

Blankesteijn, H. (2001) Virussen Maken voor Beginners. NRC Handelsblad, February 26. 2001, Page 22

Brown, D. (2000) Notre Dame physicists discover weakness in Web and Internet. URL: http://www.nd.edu/cgi-bin/news.cgi?article=200007261109 (as of 2001, March 30)

Brown, K. (2001) Financial Times. June 21, 2001, Page 1

Campbell, D. (1999) How your privacy is caught in the Net. The Age. URL: http://www.theage.comau.daily/990808/news/specials/news1.htm (as of 1999, September 27)

Campbell, D. (1999) Interception Capabilities 2000. Luxembourg: European Parliament. (WWW-document). URL: http://www.iptvreports.mcmail.com/ic2kreport.htm (as of 1999, November 19)

Campbell, D. (2000) The Spy in your Server: There is no Hiding Place on the Net as Governments Around the World Chase Data. The Guardian Online Supplement, August 10. 2000, Page 2

Carnivore Can Read Everything (2000) Wired News. URL: http://www.wired.com/news/print/0,1294,40256,00.html (as of 2000, November 20)

Carter, B. (2001) MTV to Mesh Its 2 Channels With Web Site. The New York Times. URL: http://www.nytimes.com/2001/03/26/technology/26MTV.html (as of 2001, March 26)

Centre for Media Education (1996) Web of Deception: Threats to Children from Online Marketing. (WWW-document). Washington, D.C.: CME. URL: http://www.cme.org/children/marketing/deception.pdf (as of 2001, February 12)

Centre for Media Education (1998) Changing Channels: How Digital Television will Affect the Public Health. (WWW-document). http://www.cme.org/children/digital_tv/dtvph.html (as of 2001, February 12)

Centre for Media Education (2000) Comments from CME, et al: In the Matter of Children's Television Obligations of Digital Television Broadcasters. MM Docket No. 00–167. (WWW-document). Washington, D.C.: Georgetown University Law Centre. URL: http://www.cme.org/press/DTV_NPRM_comments.pdf (as of 2001, February 12)

Centre for Media Education (2000b) Comments from CME and Coalition Call for Strong FCC Rules on Educational Obligations, Advertising Safeguards in Digital Television. Press release. URL: http://www.cme.org/press/001219pr.html (as of 2001, February 12)

Chinese Website Creator Goes on Trial (2001) URL: http://news.bbc.co.uk/hi/english/world/asia-pacific/newsid_1167000/1167050.stm (as of 2001, February 15)

Civil Liberty Groups Slam European Treaty (2000) Cluebot.com. URL: http://216.110.36.217/article.pl?sid=00/10/17/1622228&mode=nested (as of 2000, November 14)

Choi, S. Y. & Winston, A. B. (1998) Smart Cards Enabling Smart Commerce in the Digital Age. White Paper (Draft). (WWW-document). The University of Texas at Austin, Center for Research in Electronic Commerce. URL: http://cism.bus.utexas.edu/works/articles/smartcardswp.html (as of 1999, October 4)

Comments from CME and Coalition Call for Strong FCC Rules on Educational Obligations, Advertising Safeguards in Digital Television (2000) Centre for Media Education. URL: http://www.cme.org/press/001219pr.html (as of 2001, February 12)

Computer Economics (2000) Malicious Virus Attacks Cost Organizations More Than $12 Billion in 1999. URL: http://www.computereconomics.com (as of 2000, January 17)

Computer Economics (2001) Virus Attacks Cost Organizations $17.1 Billion in 2000. URL: http://www.computereconomics.com (as of 2001, January 12)

Connectis (2001) E-Index. Financial Times Supplement July 2001, Issue 13

Consumers International (2001) Privacy@net: An International Comparative Study of Consumer Privacy on the Internet. London: Consumers International, Office for Developed and Transition Economies (ODTE). (WWW-document). URL: http://www.consumersinternational.org (as of 2001, February 3)

Cooper, M. (1999) A Consumer Perspective on Economic, Social and Public Policy Issues in the Transition to Digital Television. (WWW-document). Consumer Federation of America. URL: http://www.bettertv.org/digtvf41.pdf (as of 2000, February 28)

Council of Europe (2000) Draft Convention on Cyber-Crime. PC-CY Draft N° 25 REV.5, Declassified, Public version. (WWW-document). URL: http://conventions.coe.int/treaty/EN/cadreprojets.htm (as of 2001, January 15)

Council of Europe (2001a) Riding the Web- Over 350 Million Surfers. Press Release. http://press.coe.int/press2/press.asp?B=54,0,0,107,0&M. July 2001

Council of Europe (2001b) Draft Convention on Cyber-crime and Explanatory Memorandum. http://www.conventions.coe.int

Council of Europe (2001c) Draft Explanatory Memorandum to the Draft Convention on Cybercrime. EXPC-CY (2001) 1. (WWW-document). URL: http://conventions.coe.int/treaty/EN/cadreprojets.htm

Crackers Attack Pro-Israeli Site (2000) Wired News. URL: http://www.wired.com/news/politics/0,1283,39950,00.html (as of 2001, February 21)

Critical Internet Software Found Vulnerable (2001) The New York Times. URL: http;//www.nytimes.com/reuters/technology/tech-intersecurity-so.html (as of 2001, January 30)

Delio, M. & King, B. (2000) MP3.Com Must Pay the Piper. Wired News. URL: http://www.wired.com/news/business/0,1367,38613,00.html (as of 2000, September 6)

Delio, M. (2001) Security Mavens Invaded by Trojan. Wired News. (WWW-document). URL: http://www.wired.com/news/print/0,1294,41563,00.html (as of 2001, February 2)

Delio, M. (2001) Davos Attendees' Info Stolen. Wired News. URL: http://www.wired.com/news/print/0,1294,41603,00.html (as of 2001, February 6)

Delio, M. (2001) Call Them Kiddies? Watch Out. Wired News. URL: http://www.wired.com/news/culture/0,1284,41866,00.html?tw=wn20010216 (as of 2001, February 19)

Denning, D.E. (2000) Activism, Hacktivism and Cyber Terrorism: The Internet as a Tool for Influencing Foreign Policy. Georgetown University. (WWW-document). URL: http://www.nautilus.org/info%2Dpolicy/workshop/papers/denning.html (as of 2000, December 18)

Despeignes, P. (2001) Exorcising the Ghost in the Internet Machine: Online Security. Financial Times, February 28. 2001, Page 14

DoubleClick Privacy Lawsuit Dismissed (2001) The New York Times. URL: http://www.nytimes.com/2001/03/31/technology/31CLIC.html (as of 2001, March 31)

Doyle, C. and Morris, H. (1999) The Net Effect: Rethinking the Regulatory Role of the Nation State in the Global Electronic Economy. Fabian Society Report 47, 1999

Eijsvoogel, J. (1999) Menseneitjes te koop op Internet. NRC Handelsblad, October 25. 1999, Page 4

Eijsvoogel, J. (1999) Amerikaanse Zedendelinquenten staan voor de Hele Wereld te Kijk. NRC Handelsblad, October 23. 1999, Page 35

EU Data Protection Working Party (2000) Privacy on the Internet: An integrated EU Approach to On-line Data Protection. 5063/00/EN/FINAL – WP 37. (WWW-document). URL: http://www.europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp37en.pdf (as of 2000, December 4)

European Commission (1996) Green Paper on the Protection of Minors and Human Dignity. COM (96) 483, final. (WWW-document). URL: http://www2.echo.lu/legal/en/internet/gpen-ann.html (as of 1999, October 4)

European Commission (1997a) Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions Ensuring Security and Trust in Electronic Communication: Towards A European Framework for Digital Signatures and Encryption. COM (97) 503. (WWW-document). URL: http://www.ispo.cec.be/eif/policy/97503toc.html (as of 2000, August 31)

European Commission (1997b) Green Paper on the Convergence of the Telecommunications, Media and Information Technology Sectors, and the Implications for Regulation: Towards an Information Society Approach. COM (97) 623. (WWW-document). URL: http://www.ispo.cec.be/convergencegp/97623.html#Heading59 (as of 1999, September 27)

European Commission (1998) Proposal for a European Parliament and Council Directive on a Common framework for Electronic Signatures. (COM(1998) 297 final). (WWW-document). URL: http://www.ispo.cec.be/eif/policy/com98297.html (as of 1999, October 11)

European Commission (1999) Decision of the European Parliament and of the Council on Adopting a Multi Annual Community Action Plan on Promoting Safer use of the Internet by Combating Illegal and Harmful Content on Global Networks. No 276/1999/EC. (WWW-document). URL: http://www.echo.lu/iap/decision (as of 1999, September 27)

European Commission (2001) Communication from the Commission to the Council, the European Parliament, the European Central Bank, the Economic and Social Committee and Europol: Preventing Fraud and Counterfeiting of Non-cash Means of Payment. COM (2001) 11 final. (WWW-doucment). URL: http://europa.eu.int/comm/internal_market/en/finances/payment/fraud/com11en.pdf (as of 2001, February 19)

Europe Slaving Over Cybercrime (2001) Wired News. URL: http://www.wired.com/news/politics/0,1283,42228,00.html?tw=wn20010307 (as of 2001, March 6)

Europol (1999) Situation Report on High Technology Linked with Organised Crime. The Hague: Europol Organised Crime Department

Finley, M. (2000) Now That Was a Nasty Worm. Wired News. URL: http://www.wired.com/news/technology/0,1282,36119,00.html (as of 2000, May 4)

Fox, B. (2001) Trial or Error. New Scientist, 14th July 2001, Page 22

Free Gift Could Entice Children Into Revealing Personal Family Information Online (2000) The Annenberg Public Policy Center of the University of Pennsylvania. URL: http://www.appcpenn.org/final_release_fam.pdf (as of 2001, April 2)

FTC Halts Internet Highjacking Scam. Millions of Legitimate Web Pages Cloned by Highjackers; Innocent Surfers Barraged with Smut (1999) Federal Trade Commission. URL: http://www.ftc.gov/opa/1999/9909/atariz.htm (as of 1999, October 15)

Gallagher, D.F. (2001) Movie Industry Frowns on Professor's Software Gallery. The New York Times. URL: http://www.nytimes.com/2001/03/30/technology/30CYBERLAW.html (as of 2001, March 30)

GAO (1998) Information Security Management: Learning From Leading Organizations. GAO/AIMD–98–68. Washington, D.C.: United States General Accounting Office

GAO (1999) Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences. GAO/AIMD–00–1. Washington, D.C.: United States General Accounting Office. (WWW-document). URL: http://www.gao.gov/new.items/ai00001.pdf (as of 1999, October 11)

GAO (1999) Financial Management Service: Significant Weaknesses in Computer Controls. GAO/AIMD–00–4. Washington, D.C.: United States General Accounting Office. (WWW-document). URL: http://www.gao.gov/new.items/ai00004.pdf (as of 1999, October 11)

GAO (1999) Information Security: The Proposed Computer Security Enhancement Act of 1999. GAO/T-AIMD–99–302. Washington, D.C.: United States General Accounting Office. (WWW-document). URL: http://www.gao.gov/new.items/ai99302t.pdf (as of 1999, October 11)

GAO (1999) Securities Fraud, The Internet Poses Challenges to Regulators and Investors. GAO/T-GGD–99–34. Washington, D.C.: United States General Accounting Office. (WWW-document). URL: http://www.gao.gov (as of 1999, October 10)

Gauthronet, S. & Drouard, E. (2001) Unsolicited Commercial Communications and Data Protection. Summary of study conducted for the European Commission. (WWW-document). URL: http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/spamsum.pdf (as of 2001, February 19)

Gentile, C.J. (2000) Hacker War Rages in Holy Land. Wired News. URL: http://www.wired.com/news/print/0,1294,40030,00.html (as of 2000, November 8)

Gentile, C.J. (2000) Israeli Hackers Vow to Defend. Wired News. URL: http://www.wired.com/news/print/0,1294,40187,00.html (as of 2000, November 15)

Glave, J. (1998) Back Orifice a Pain in the…? Wired News. URL: http://www.wired.com/news/technology/0,1282,14092,00.html (as of 2000, January 27)

Graham-Rowe, D. (2001) Masters of Disguise. New Scientist, 14th July 2001, Page 7

Griggs, K. (2001) How Kiwi Girl Becomes U.S. Hero. Wired News. URL: http://www.wired.com/news/business/0,1367,42716,00.html?tw=wn20010329 (as of 2001, March 29)

Groebel, J. (1998) The UNESCO Global Study on Media Violence. Paris: UNESCO

Groebel, J. & Smit, L. (1997) Gewalt im Internet. Report for the German Parliament. Bonn: Deutscher Bundestag

Groebel, J. & Smit, L. (1996) Media en Geweld. Rapport in opdracht van het Ministerie van Onderwijs, Cultuur en Wetenschappen, OCenW. Utrecht: Universiteit Utrecht, Vakgroep Massacommunicatie

Guisnel, J. (1995) Guerres dans le Cyberspace: Services Secrets et Internet. Paris: Editions La Découverte

Guernsey, L. (2001) Yahoo to Try Harder to Rid Postings of Hateful Material. The New York Times. URL: http://www.nytimes.com/2001/01/03/technology/03YAHO.html (as of 2001, January 3)

Hacker in Japan 'Corrigeert' (2000) NRC Handelsblad, January 27). 2000, Page 5

Hacker Posts Credit Card Info (2000) Wired News. URL: http://www.wired.com/news/technology/0,1282,33539,00.html (as of 2000, June 26)

Hackers Say Attack was Easy (2001) The New York Times. URL: http://www.nytimes.com/aponline/business/AP-World-Forum-Hackers.html (as of 2001, February 11)

Hamelink, C. (1997) New information and Communication Technologies, Social Development and Cultural Change. Discussion paper No. DP 86. Geneva: United Nations Research Institute for Social Development (UNRISD)

Hamelink, C. J. (1999) Digitaal Fatsoen: Mensenrechten in Cyberspace. Amsterdam: Uitgeverij Boom

Hearnden, K. (1991) Computer Criminals are Human, Too. In T. Forester (Ed.), Computers in the human context. Pages 415–426. Cambridge, Massachusetts: The MIT Press

Hershman, T. (2001) Israel's 'First Internet Murder'. Wired News. URL: http://www.wired.com/news/print/0,1294,41300,00.html (as of 2001, January 21)

Hopkins, N. (2001) Success of CD Piracy Hits Music Industry. The Guardian, June 13. 2001, Page 10

How to Halt Nazi Sales in France? (2000) Wired News. (WWW-document). URL: http://www.wired.com/news/print/0,1294,38183,00.html (as of 2000, September 1)

iDEFENSE (2000) Muslim Hackers Launch Phase 3 of 'E-Jihad': Cyber War Could Spill-Over to Other Regions of the World. URL: http://www.idefence.com/pages/flashreports?MidEast_110100.htm (as of 2000, November 8)

iDEFENSE (2001) Israeli-Palestinian Cyber Conflict. Version 2.0PR Public Release. (WWW-document). URL: http://www.idefense.com/pages/ialertexcl/ipccv2–0PR.pdf (as of 2001, February 19)

Interactive Digital TV to Reach 625 Million Viewers (2001) Strategy Analytics. URL: http://www.strategyanalytics.com/press/index.html (as of 2001, February 27)

Janofsky, M. (1999) Hackers Interrupt 2 Federal Web Sites. The New York Times. URL: http://www.nytimes.com (as of 1999, August 6)

Information Technology Annual Report (1999) (WWW-document). Business Week Online. URL: http://www.businessweek.com/technology/index.html (as of 1999, September 27)

Judge, P. C. (1998) How Safe is the Net? Business Week Online. URL: http://www.businessweek.com/1998/25/b3583019.html. (as of 1999, September 27)

Kaplan, C.S. (2001) Legal Expert Sees Light Focused on Napster Users. The New York Times. URL: http://www.nytimes.com/2001/02/16/technology/16CYBERLAW.html (as of 2001, February 16)

Kaplan, C.S. (2001) Legal Expert Sees Napster Competitors Thriving. The New York Times. URL: http://www.nytimes.com/2001/02/23/technology/23CYBERLAW.html (as of 2001, February 23)

Kelley, J. (2001) Terror Groups Hide Behind Web Encryption. USA Today. URL: http://www.usatoday.com/life/cyber/tech/2001–02–05-binladen.htm (as of 2001, February 8)

Kelley, J. (2001) Terrorist Instructions Hidden Online. USA Today. URL: http://www.usatoday.com/life/cyber/tech/2001–02–05-binladen-side.htm (as of 2001, February 8)

Kerr, D. (2000) Self-labelling and Filtering. (WWW-document). URL: http://europa.eu.int/ISPO/iap/INCOREreport.doc (as of 2000, November 20)

Kettmann, S. (1999) He Won't Join Amazon's 'Kampf'. Wired News. URL: http://www.wired.com/news/business/0,1367,32835,00.html (as of 2000, September 1)

Kettmann, S. (2000) German Hate Law: No Denying It. Wired News. URL: http://www.wired.com/print/0,1294,40669,00 (As of 2000, December 16)

Kettmann, S. (2001) German Threat Raises Infowar Fear. Wired News. URL: http://www.wired.com/news/politics/0,1283,42921,00.html?tw=wn20010409 (as of 2001, April 9)

King, B. (2001) TV Towers Power Netcasts. Wired News. URL: http://www.wired.com/news/business/0,1367,41353,00.html (as of 2001, February 19)

Knight, W. (2001) Yahoo! to block adult rooms from UK chat client. Yahoo! News. URL: http://uk.news.yahoo.com/010212/152/b12mg.html (as of 2001, February 12)

Koekoek, A., Vlemminx, F. Leenknegt, G.J. Nouwt, S. & Matthijssen, L. (1999) Vergelijking van grondrechten inzake informatie en privacy, een oriënterend onderzoek. (WWW-document). In opdracht van het Wetenschappelijk Onderzoek – en Documentatiecentrum van het Ministerie van Justitie ten behoeve van de Commissie Grondrechten in het digitale tijdperk. Tilburg (The Netherlands): Katholieke Universiteit Brabant. URL: http://www.minbz.nl/gdt (as of 1999, October 22)

Kraaijeveld, K. (1999) Investeerders Maken Elkaar gek op Internet. NRC Handelsblad

Larson, A.M. (1999) Global Security Survey: Virus Attack. InformationWeek. (WWW-document). URL: http://www.informationweek.com/743/security.htm. 1999, July 12

Legal, Regulatory, Policy and Organizational Considerations for Assurance (1996) 2nd edition. (WWW-document). URL: http://www.infowar.com…int3whitppr.doc

Lohr, S. (1997) Go Ahead, Be Paranoid: Hackers Are Out to Get You. The New York Times. URL: http://searchnytimes.com/search/daily/b…oc+site+site+17575+24+wAAA+Cyber%7ECrime.html (as of 1999, August 6)

Longstaff, T.A., Ellis J.T. Hernan, S.V. Lipson H.F. McMillan, R.D. Pesante, L.H. & Simmel, D. (1997) Security of the Internet. The Froehlich/Kent Encyclopedia of Telecommunications Vol. 15, Pages 231–255. New York: Marcel Dekker. (WWW-document). URL: http://www.cert.org/encyc_article/tocencyc.html

Manjoo, F. (2000) Broadband Could be Hackland. Wired News. URL: http://www.wired.com/news/print/0,1294,39235,00.html (as of 2000, October 23)

Manjoo, F. (2001) The Tech Take on TV's Future. Wired News. URL: http://www.wired.com/news/technology/0,1282,42211,00.html?tw=wn20010306 (as of 2001, March 6)

Marien, M. (1991) IT: You Ain't Seen Nothing Yet. In T. Forester (Ed.), Computers in the Human Context. Pages 41–47. Cambridge, Massachusetts: The MIT Press

Marketing to Children Harmful: Experts Urge Candidates to Lead Nation in Setting Limits (2000) Centre for Media Education. URL: http://www.cme.org/press/001219pr.html (as of 2001, February 12)

Marriott, M. (2001) Tiny TV Station Turns to the Web. The New York Times. URL: http://www.nytimes.com/2001/03/01/technology/01TVEE.html (as of 2001, March 1)

Martin, D. (2001) TiVo's Data Collection and Privacy Practices. (WWW-document). Privacy Foundation. URL: http://www.privacyfoundation.org/privacywatch/report.asp?id=62&action=0 (as of 2001, March 26)

Mathiason, N. (2001) The Day the Music Died for Online Rebel Napster. The Observer Business, June 24. 2001, Page 7

McAuliffe, W. (2000) 2000 Roundup: The dangers of chatrooms exposed. ZDNet. URL: http://www.zdnet.co.uk/news/2000/52/ns–19870.html (as of 2001, February 21)

McAuliffe, W. (2001) Wonderland paedophiles are sentenced. ZDNet. URL: http://www.zdnet.co.uk/news/2001/6/ns–20942.html (as of 2001, February 21)

McAuliffe, W. (2001) Police lack resources for paedophile hunts. Yahoo! News. URL: http://uk.news.yahoo.com/010215/152/nlomu.html (as of 2001, February 21)

McConnell International (2000) Risk E-Business: Seizing the Opportunity of Global E-Readiness. (WWW-document). URL: http://www.mcconnellinternational.com

McConnell International (2000) Cyber Crime … and Punishment? Archaic Laws Threaten Global Information. (WWW-document). URL: http://www.mcconnellinternational.com

McCullagh, D. (1999) Looking for Something to Blame. Wired News. URL: http://www.wired.com/news/print/0,1294,19291,00.html (as of 1999, April 23)

McCullagh, D. & Morehead, N. (2000) Privacy a Likely Loser in Treaty. Wired News. URL: http://wwwwired.com/news/politics/0,1283,40576,00.html?tw=wn20001208 (as of 2000, December 12)

McCullagh, D. (2001) Safe Harbour is a Lonely Harbour. (WWW-document). Wired News. URL: http://www.wired.com/news/print/0,1294,41004,00.html (as of 2001, January 6)

McCullagh, D. (2001) Bin Laden: Steganography Master? Wired News. (WWW-document). URL: http://www.wired.com/news/politics/0,1283,41658,00.html?tw=wn20010207 (as of 2001, February 8)

McCullagh, D. (2001) Feds Say Fidel is Hacker Threat. Wired News. URL: http://www.wired.com/news/politics/0,1283,41700,00.html?tw=wn20010209 (as of 2001, February 9)

McIntosh, N. (2000) Cyber crime: Consumers Fear of Fraud Deters Most Europeans from Buying Online. The Guardian, February 10. 2000, Page 17

McKay, N. (1999) Coming Soon: Back Orifice 2000. Wired News. URL: http://www.wired.com/news/technology/0,1282,20493,00.html (as of 2000, January 27)

McWilliams, B. (1999) Israeli Teen Finds Web Full of Security Holes. URL: http://www.internetnews.com/intl-news/article/0,1087,6_184381,00.html (as of 1999, October 4)

Metze-Mangold, V. (2000) Weltweiter Wertekodex. Auf dem Weg zu einer digitalen Civil Society. In Kubischek, H. u.a. (Ed.): Jahrbuch Telekommunikation und Gesellschaft

Metze-Mangold, V. (1998) INFOethics '98. Die UNESCO sucht ihre Rolle im internationalen System. In: UNESCO Heute, Volume 4/98, Pages 93ff.

Miljardenschade door computervirussen (2000) NRC Handelsblad, January 27. 2000, Page 15

Molander, R.C. Mussington, D. & Wilson, P. (1998) Cyber payments and Money Laundering: Problems and Promise. (WWW-document). URL: http://www.rand.org/publications/MR/MR965/MR965.pdf/

Napster Said to Hurt CD Sales (2001) The New York Times. URL: http://www.nytimes.com/aponline/business/AP-Napster-CD-Sales.html (as of 2001, February 25)

NASA Denies Hacker Endangered Astronauts (2000) USA Today. URL: http://www.usatoday.com/life/cyber/tech/cti189.htm. 2000, July 5

Negroponte, N. (1995) Being Digital. London: Hodder & Stoughton. A Coronet Paperback edition

Neumann, L.A. (2001) The Great Firewall. (WWW-document). New York: CPJ. URL: http://www.cpj.org/Briefings/2001/China_jan01.html (as of 2001, February 15)

Nieuwstadt, M. van (1999) De Kracht van oude Paradigma's, Denken over de 21ste eeuw: Hal Varian. NRC Handelsblad, October 6. 1999, Page 16

Oakes, C. (2000) Web Enters Privacy 'Safe Harbour'. Wired News. URL: http://www.wired.com/news/print/0,1294,39909,00.html (as of 2000, November 2)

O'Connell, R. (1998) The Structure and Social Organisation of Paedophile Activity in Cyberspace: Implications for Investigative Strategies. (WWW-document). URL: http://www.uclan.ac.uk/facs/science/psychol/rachel/crime1.htm (as of 2001, February 21)

O'Connor, A. (2001) Online Piracy Plagues Music Industry. Financial Times June 13. 2001, Page 12

OECD (1998) Implementing the OECD 'Privacy Guidelines' in the Electronic Environment: Focus on the Internet. DSTI/ICCP(97)6/Final. (WWW-document). URL: http://www.oecd.org//dsti/sti/it/secur/prod/reg97–6e.pdf (as of 1999, October 11)

OECD (1999a) Inventory of Instruments and Mechanisms Contributing to the Implementation and Enforcement of the OECD Privacy Guidelines on Global Networks. DSTI/ICCP/REG(98)12/Final. (WWW-document). URL: http://www.oecd.org/dsti/sti/it/ec/act/paris_ec/pdf/inv-mech_e.pdf (as of 1999, September 27)

OECD (1999b) Inventory of Approaches to Authentication and Certification in a Global Networked Society. DSTI/ICCP/REG(99)13/Final. (WWW-document). URL: http://www.oecd.org/dsti/sti/it/ec/act/paris_ec/pdf/inv-auth_e.pdf (as of 1999, October 4)

OECD (1999c) Progress Report on the OECD Action Plan for Electronic Commerce. SG/EC(99)4. (WWW-document). URL: http://www.oecd.org/dsti/sti/it/ec/act/paris_ec/pdf/progrep_e.pdf (as of 1999, September 20)

Patrizio, A. (1999) DVD Piracy: It Can Be Done. Wired News. URL: http://www.wired.com/news/print/0,1294.32249,00.html (as of 1999, November 1). 1999, November 1

Peet, J. van der & Groebel, J. (1998) Parental Control of Broadcasting, Film, Audiovisual and On-line Services in the European Union: Country Report for the Netherlands. Contribution to the Final Report of Oxford University: Parental Control of Television Broadcasting. Utrecht: Utrecht University

Philipkoski, K. (2000) How The Slimy Worm Works. Wired News. URL: http://www.wired.com/news/technology/0,1282,36129,00.html. 2000, May 4

Pool, I. de Sola (1983) Technologies of Freedom. Cambridge: The Belknap Press of Harvard University Press

Power, R. (1999) 1999 CSI/FBI Computer Crime and Security Survey. Computer Security, Issues & Trends, 5(1), 1–16

Power, R. (2000) 2000 CSI/FBI Computer Crime and Security Survey (2000). Computer Security, Issues & Trends, 6(1), 1–15

Price, M.E. & Verhulst, S.G. (1999) The Concept of Self Regulation and the Internet. Draft Version. In J. Waltermann & M. Machill (Eds.), Protecting our Children on the Internet. Towards a new Culture of Responsibility. (WWW-document). URL: http://www.stiftung.bertelsmann.de/internetcontent/english/frameset_nojs.html (as of 1999, September 6)

RNC Site Shut Down by Hackers (2000) Wired News. URL: http://www.wired.com/news/politics/0,1283,40016,00.html. 2000, November 7

Repke, I. Wensierski, P. & Zimmermann, F. (2001). Let it be. Der Spiegel, 9, 78–80

Richtel, M. (2001) Napster Suffers Setback in Appeals Court Ruling. The New York Times. URL: http://www.nytimes.com/2001/02/13/technology/13NAPS.html (as of 2001, February 13)

Salkever, A. (2000) Cyber-Extortion: When Data Is Held Hostage. BusinessWeek Online. URL: http://www.businessweek.com/bwdaily/dnflash/aug2000/nf20000822_308.htm

Scheeres, J. (2001) Will the Hatemongers Survive? Wired News. URL: http://www.wired.com/news/culture/0,1284,41460,00.html (as of 2001, January 30)

Scheeres, J. (2001) Bomber's Death May Be Online. Wired News. URL: http://www.wired.com/news/business/0,1367,42752,00.html?tw=wn20010331, 2001, March 30

Schwartz, J. (2001) In Tapping Net, F.B.I. Insists Privacy Is Not a Victim. The New York Times. URL: http://www.nytimes.com/2001/02/08/technology/08CARN.html, 2001, February 8

Shaki Trimble, P. (2000) NASA: Hack didn't Endanger Astronauts. Federal Computer Week. URL: (2000, July 7). http://www.fcw.com/fcw/articles/2000/0703/web-nasa–07–07–00.asp

Sieber, U. (1998) Legal Aspects of Computer Related Crime in the Information Society, COMCRIME-Study. Würzburg: University of Würzburg. (WWW-document). URL: http://www2.echo.lu/legal/en/crime/crime.html (as of 1999, September 27)

Sieber, U. (1999) Responsibility and Control for Illegal and Harmful Contents in the Internet. Draft Version. In J. Waltermann & M. Machill (Eds.), Protecting our Children on the Internet. Towards a new Culture of Responsibility. (WWW-document). URL: http://www.stiftung.bertelsmann.de/internetcontent/english/frameset_nojs.html (as of 1999, September 6)

Spiegel, P. (2000) US Cybercops Face Global Challenge as World Gets Wired Up. Financial Times, October 25. 2000, Page 16

Stefik, M. (1999) The Internet Edge. Social, Technical, and Legal Challenges for a Networked World. Cambridge, Massachusetts: The MIT Press

Taylor, P. A. (1999) Hackers: Crime in the digital sublime. London: Routledge

Teather, D. (2001) Music Pirates Sink Industry: Global Record Sales Drop for the First Time. The Guardian, April 20. 2001, Page 23

Tippett, P.S. (2000) Malicious Code and Internet Security. Congressional Testimony. U.S. House of Representatives Committee on Science, Subcommittee on Technology. (WWW-document). URL: http://i2k.icsa.net/html/communities/loveletter/testimony.shtml#observations

Tomkins, R. (2000) Cookies Leave a Nasty Taste: Marketing Internet Privacy. Financial Times, March 3. 2000, Page 16

Travis, A. (2000) Net Fuels Huge Growth in Fraud Alarm Bells. The Guardian, January 19th. 2000, Page 4

Turow, J. (2001) Privacy Policies on Children's Websites: Do They Play By the Rules? (WWW-document). The Annenberg Public Policy Center of the University of Pennsylvania. URL: http://www.asc.upenn.edu/usr/jturow/PrivacyReport.pdf (as of 2001, April 2)

UCLA (2000) The UCLA Internet Report: Surveying the Digital Future. Los Angeles: UCLA Centre for Communication Policy. (WWW-document). URL: http://www.ccp.ucla.edu (as of 2000, November 20)

UNESCO (1999) Sexual abuse of children, child pornography and paedophilia on the Internet: an international challenge. Final Report, Declaration and Action Plan. Paris: UNESCO

UN Manual on the Prevention and Control of Computer-related Crime (1994). International Review of Criminal Policy. No. 43 & 44. (WWW-document). URL: http://www.uncjin.org: 80/Documents/irpc4344.pdf (as of 1999, September 6)

U.K. Millionaire Goes Interactive (2001, March 27). Wired News. URL: http://www.wired.com/news/business/0,1367,42651,00.html?tw=wn20010327 (as of 2001, March 27)

U.S. Customs Service, Russian Police Take Down Global Child Pornography Web Site (2001) U.S. Customs Service. URL: http://www.customs.gov/hot-new/pressrel/2001/0326–00.htm (as of 2001, March 26)

Velden, B. Van der (2001) Met medeweten van topambtenaar: VS controleren codesysteem EU. NRC Handelsblad, March 2. 2001, Page 1

Velden, B. Van der (2001) Zwijgzame Perkins gaat onverwachts praten. NRC Handelsblad, March 2. 2001, Page 5

Velden, B. van der (2001) Excuus van Commissie: Ambtenaar EU-geheimen vergiste zich. NRC Handelsblad, March 7. 2001, Page 5

Velden, B. Van der (2001) Rapporteur EU over Afluisteren: Mogelijkheden van Echelon Overschat. NRC Handelsblad, March 8. 2001, Page 1

Waldmeir, P. (2001) Dark Side of Cyber crime Fight: An International Treaty on Law Enforcement for the Web Poses Unsettling Questions about Civil Liberties. Financial Times, May 10. 2001, Page 17

Weston, R. (1999) Security Survey Methodology. InformationWeek. (WWW-document). URL: http://www.informationweek.com/743/securit2.htm. July 12, 1999

WIPO (1979) Berne Convention for the Protection of Literary and Artistic Works. Paris Act of July 24, 1971, as amended on September 28, 1979. No. 287(E). (WWW-document). URL: http://www.wipo.int/eng/iplex/wo_ber0_.htm

WIPO (1996) WIPO Copyright Treaty. Adopted by the Diplomatic Conference on December 20, 1996. CRNR/DC/94. (WWW-document). URL: http://www.wipo.int/eng/diplconf/distrib/94dc.htm

WIPO (1996) WIPO Performances and Phonograms Treaty. Adopted by the Diplomatic Conference on December 20, 1996. CRNR/DC/95. (WWW-document). URL: ttp://www.wipo.int/eng/diplconf/distrib/95dc.htm

Webster, F. (1995) Theories of the Information Society. London: Routledge

Westerman, F. (1999) Pinnen in Moskou is Riskant. NRC Handelsblad, October 6. 1999, Page 5

Whiteside, T. (1978) Computer Capers: Tales of Electronic Thievery, Embezzlement and Fraud. New York: Crowell Publishers

Zernike, K. (2001) From Classrooms to Chatrooms, All Threats Turn Serious. The New York Times. URL: http://www.nytimes.com/2001/03/24/nyregion/24THRE.html (as of 2001, March 24)

Zimbardo, P.H. & Leipe, M.R. (1991) The Psychology of Attitude Change and Social Influence. New York: McGraw-Hill. ANNEX

Appendix I.

Council of Europe: European Committee on Crime Problems (CDPC), Committee of Experts on Crime in Cyber-Space (PC-CY)

DRAFT CONVENTION ON CYBER-CRIME, JUNE 2001.

Chapter I – Use of terms

Article 1 – Definitions

For the purposes of this Convention:

a. „computer system" means any device or a group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b. „computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c. „service provider" means:

   (i) any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

   (ii) any other entity that processes or stores computer data on behalf of such communication service or users of such service.

d. „traffic data" means any computer data relating to a communication by means of a computer system, generated by the computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration or type of underlying service.

Chapter II – Measures to be taken at the national Level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without

right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

(a) the production, sale, procurement for use, import, distribution or otherwise making available of:

1. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2 – 5;

2. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offences established in Articles 2 – 5; and

(b) the possession of an item referred to in paragraphs (a)(1) or (2) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 – 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this Article is not for the purpose of committing an offence established in accordance with articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3. Each Party may reserve the right not to apply paragraph 1 of this Article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 (a) (2).

Title 2 – Computer-related offences

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally and without right the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent

that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another by:

(a) any input, alteration, deletion or suppression of computer data

(b) Any interference with the functioning of a computer or system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another.

Title 3 – Content-related offences

Article 9 – Offences related to child pornography

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

(a) producing child pornography for the purpose of its distribution through a computer system;

(b) offering or making available child pornography through a computer system;

(c) distributing or transmitting child pornography through a computer system;

(d) procuring child pornography through a computer system for oneself or for another;

(e) possessing child pornography in a computer system or on a computer-data storage medium.

2. For the purpose of paragraph 1 above „child pornography" shall include pornographic material that visually depicts:

(a) a minor engaged in sexually explicit conduct;

(b) a person appearing to be a minor engaged in sexually explicit conduct;

(c) realistic images representing a minor engaged in sexually explicit conduct.

3. For the purpose of paragraph 2 above, the term 'minor' shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4. Each Party may reserve the right not to apply, in whole or in part, paragraph 1(d) and 1(e), and 2(b) and 2(c).

Title 4 – Offences related to infringements of copyright and related rights

Article 10 – Offences related to infringements of copyright and related rights

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 of the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such Conventions, where such acts are committed wilfully, [at least] on a commercial scale and by means of a computer system.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the

law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations done in Rome (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such Conventions, where such acts are committed wilfully, [at least] on a commercial scale and by means of a computer system.

3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5 – Ancillary liability and sanctions

Article 11 – Attempt and aiding or abetting

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 – 10 of the present Convention with intent that such offence be committed.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, 9 (1) a and 9 (1) c of this Convention.

3. Each State may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12 – Corporate liability

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that a legal person can be held liable for a criminal offence established in accordance with this Convention, committed for its benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on:

(a) a power of representation of the legal person;

(b) an authority to take decisions on behalf of the legal person;

(c) an authority to exercise control within the legal person.

2. Apart from the cases already provided for in paragraph 1, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 – Sanctions and measures

1. Each Party shall take the necessary measures to ensure that the criminal offences established in accordance with Articles 2 – 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2. Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Section 2 – Procedural law

Title 1 – Common provisions

Article 14 – Scope of procedural provisions

1. Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this Section for the purpose of specific criminal investigations or proceedings.

2. Except as specifically otherwise provided in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 to:

(a) the criminal offences established in accordance with articles 2–11 of this Convention;

(b) other criminal offences committed by means of a computer system; and

(c) the collection of evidence in electronic form of a criminal offence.

3. Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation so as to enable the broadest application of the measure referred to in Article 20.

Article 15 – Conditions and safeguards

1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2. Such conditions and safeguards shall, as appropriate in view of the nature of the power or procedure concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation on the scope and the duration of such power or procedure.

3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, a Party shall consider the impact of the powers and procedures in this Section upon the rights, responsibilities and legitimate interests of third parties.

Title 2 – Expedited preservation of stored computer data

Article 16 – Expedited preservation of stored computer data

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such leg-

islative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of 90 days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3. Each Party shall adopt such legislative or other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17 – Expedited preservation and partial disclosure of traffic data

1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

(a) ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

(b) ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 3 – Production order

Article 18 – Production order

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

(a) a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

(b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control;

2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3. For the purpose of this article, 'subscriber information' means any information, contained in the form of computer data or any other form, that is held by a service provider, relating to subscribers of its service, other than traffic or content data, by which can be established:

(a) the type of the communication service used, the technical provisions taken thereto and the period of service;

(b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

(c) any other information on the site of the installation of communication equipment available on the basis of the service agreement or arrangement.

Title 4 – Search and seizure of stored computer data

Article 19 – Search and seizure of stored computer data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

(a) a computer system or part of it and computer data stored therein; and

(b) computer-data storage medium in which computer data may be stored, in its territory.

2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1 (a), and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, such authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

(a) seize or similarly secure a computer system or part of it or a computer-data storage medium;

(b) make and retain a copy of those computer data;

(c) maintain the integrity of the relevant stored computer data; and

(d) render inaccessible or remove those computer data in the accessed computer system.

4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 – Real-time collection of computer data

Article 20 – Real-time Collection of Traffic Data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

(a) collect or record through application of technical means on the territory of that Party, and

(b) compel a service provider, within its existing technical capability, to:

i. collect or record through application of technical means on the territory of that Party, or

ii. co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1 (a), it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications in its territory through application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of and any information about the execution of any power provided for in this Article.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – Interception of content data

1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

(a) collect or record through application of technical means on the territory of that Party, and

(b) compel a service provider, within its existing technical capability, to:

i. collect or record through application of technical means on the territory of that Party, or

ii. co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1 (a), it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data of specified communications in its territory through application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of and any information about the execution of any power provided for in this Article.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3 – Jurisdiction

Article 22 – Jurisdiction

1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 – 11 of this Convention, when the offence is committed:

(a) in its territory; or

(b) on board a ship flying the flag; or

(c) on board an aircraft registered under the laws of that Party; or

(d) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2. Each State may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs (1) b – (1) d of this article or any part thereof.

3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph (1) of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him/her to another Party, solely on the basis of his/her nationality, after a request for extradition.

4. This Convention does not exclude any criminal jurisdiction exercised in accordance with domestic law.

5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Chapter III – International co-operation

Section 1 – General principles

Title 1 – General principles relating to international co-operation

Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 2 – Principles relating to extradition

Article 24 – Extradition

1. (a) This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 – 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.
2. (b) Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2. The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3. If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this Article.

4. Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this Article as extraditable offences between themselves.

5. Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6. If extradition for a criminal offence referred to in paragraph 1 of this Article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as in the case of any other offence of a comparable nature under the law of that Party.

7. (a) Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of

Europe the name and addresses of each authority responsible for the making to or receipt of a request for extradition or provisional arrest in the absence of a treaty.

(b) The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Title 3 – General principles relating to mutual assistance

Article 25 – General principles relating to mutual assistance

1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2. Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 – 35.

3. Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communications, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4. Except as otherwise specifically provided in Articles in this Chapter mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance solely on the ground that the request concerns an offence which it considers a fiscal offence.

5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominates the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26 – Spontaneous information

1. A Party may, within the limits of its domestic law, without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2. Prior to providing such information, the providing Party may request that it be kept confidential or used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1. Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 10 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation is available, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2.

(a) Each Party shall designate a central authority or authorities that shall be responsible for sending and answering requests for mutual assistance, the execution of such requests, or the transmission of them to the authorities competent for their execution.

(b) The central authorities shall communicate directly with each other.

(a) Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph.

(b) The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3. Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party except where incompatible with the law of the requested Party.

4. The requested Party may, in addition to grounds for refusal available under Article 26, paragraph (4), refuse assistance if:

(a) The request concerns an offences which the requested Party considers a political offence or an offence connected with a political offence; or

(b) It considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

5. The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6. Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7. The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. If the request is refused or postponed, reasons shall be given for the refusal or postponement. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8. The requesting Party may request that the requested Party keep confidential the fact and substance of any request made under this Chapter except to the extent necessary to execute the request. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9.

(a) In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

(b) Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

(c) Where a request is made pursuant to subparagraph (a) and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

(d) Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

(e) Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28 – Confidentiality and limitation on use

1. When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation, is available unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2. The requested Party may make the furnishing of information or material in response to a request dependent on the condition that it is:

(a) kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

(b) not used for investigations or proceedings other than those stated in the request.

3. If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information is nevertheless provided. When the requesting Party accepts the condition, it shall be bound by it.

4. Any Party that furnishes information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

Article 29 – Expedited preservation of stored computer data

1. A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, which is located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2. A request for preservation made under paragraph 1 shall specify:

(a) the authority that is seeking the preservation;

(b) the offence that is the subject of a criminal investigation or proceeding and a brief summary of related facts;

(c) the stored computer data to be preserved and its relationship to the offence;

(d) any available information to identify the custodian of the stored computer data or the location of the computer system;

(e) the necessity of the preservation; and

(f) that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3. Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4. A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data may, in respect of offences other than those established in accordance with Articles 2 – 11 of this Convention, reserve the right to refuse the request for preservation under this Article in cases where it has reason to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5. In addition, a request for preservation may only be refused if:

(a) the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

(b) the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

6. Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of, or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7. Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than 60 days in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such request, the data shall continue to be preserved pending a decision on that request.

Article 30 – Expedited disclosure of preserved traffic data

1. Where, in the course of the execution of a request made under Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data in order to identify that service provider and the path through which the communication was transmitted.

2. Disclosure of traffic data under paragraph 1 may only be withheld if:

(a) the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

(b) the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

Title 2 – Mutual assistance regarding investigative powers

Article 31 – Mutual assistance regarding accessing of stored computer data

1. A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2. The requested Party shall respond to the request through application of international instruments, arrangements and laws referred to in article 23, and in accordance with other relevant provisions of this Chapter.

3. The request shall be responded to on an expedited basis where:

(a) there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

(b) the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without obtaining the authorisation of another Party:

(a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

(b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33 – Mutual assistance regarding the real-time collection of traffic data

1. The Parties shall provide mutual assistance to each other with respect to the real-time collection of traffic data associated with specified communications in its territory transmitted by means of a computer system. Subject to paragraph 2, assistance shall be governed by the conditions and procedures provided for under domestic law.

2. Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34 – Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other with respect to the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted by their applicable treaties and domestic laws.

Title 3 – 24/7 Network

Article 35 – 24/7 Network

1. Each Party shall designate a point of contact available on a 24 hour, 7 day per week basis in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of

evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out:

(a) provision of technical advice;

(b) preservation of data pursuant to Articles 29 and 30; and

(c) collection of evidence, giving of legal information, and locating of suspects.

2.

(a) A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

(b) If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3. Each Party shall ensure that trained and equipped personnel are available in order to facilitate the operation of the network.

Chapter IV – Final provisions

Article 36 – Signature and entry into force

1. This Convention shall be open for signature by the member States of the Council of Europe and by non-member States, which have participated in its elaboration.

2. This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3. This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4. In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37 – Accession to the convention

1. After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20 (d) of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2. In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 38 – Territorial application

1. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2. Any Party may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3. Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39 – Effects of the Convention

1. The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:

– The European Convention on Extradition opened for signature in Strasbourg on 13 December 1957 (ETS No. 24);

– The European Convention on Mutual Assistance in Criminal Matters opened for signature in Strasbourg on 20 April 1959 (ETS No. 30);

– The Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters opened for signature in Strasbourg on 17 March 1978 (ETS No. 99).

2. If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or otherwise have established their relations in this matter, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with on the present convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3. Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40 – Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Article 2, Article 3, Article 6, paragraph 1 (b) Article 7, Article 9, paragraph 3 and Article 27, paragraph 9 (e).

[Article 41 – Federal clause

A federal State may notify the Secretary General that it shall assume obligations under this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities. When making a declaration, a federal State shall provide a statement regarding the nature of its federal system, and of the effect of its federal character on the implementation of the Convention.]

Article 42 – Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, ap-

proval or accession, declare that it avails itself of the reservation(s) provided for in Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 2, Article 23, paragraph 2, Article 29, paragraph 4. No other reservation may be made.

Article 43 – Status and withdrawal of reservations

1. A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2. A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3. The Secretary General may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44 – Amendments

1. Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2. Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3. The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the European Committee on Crime Problems (CDPC) and, following consultation with the non-member State Parties to this Convention, may adopt the amendment.

4. The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5. Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45 – Settlement of disputes

1. The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2. In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the European Committee on Crime Problems (CDPC), to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46 – Consultations of the Parties

1. The Parties shall, as appropriate, consult periodically with a view to facilitating:

(a) the effective use and implementation of this Convention;

(b) the exchange of information on significant legal, policy or technological developments pertaining to cyber-crime and the collection of evidence in electronic form;

(c) consideration of possible supplementation or amendment of the Convention.

2. The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3. The European Committee on Crime Problems (CDPC) shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4. Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5. The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this Article.

Article 47 – Denunciation

1. Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2. Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 48 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

(a) any signature;

(b) the deposit of any instrument of ratification, acceptance, approval or accession;

(c) any date of entry into force of this Convention in accordance with Articles 36 and 37;

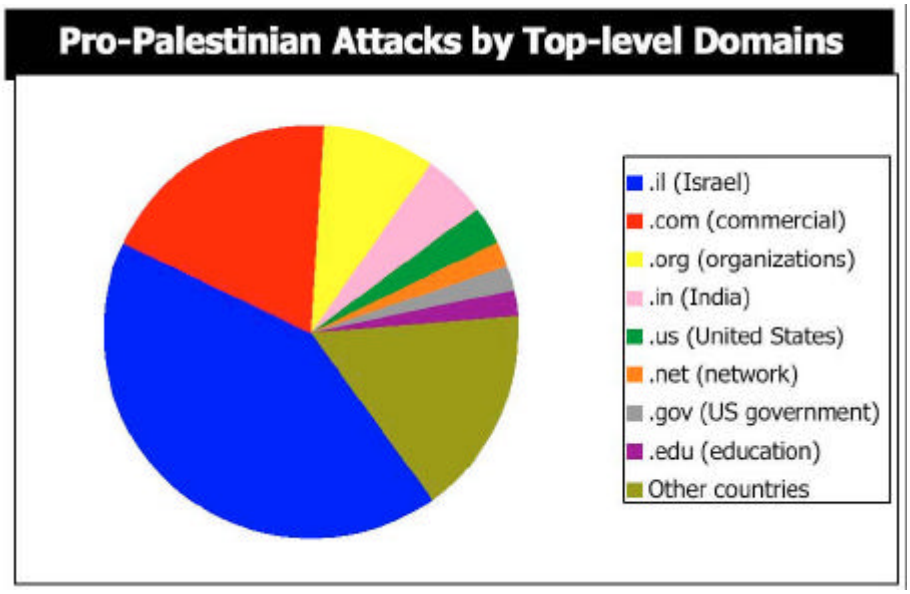
(d) any declaration made under Article[s] 40 [and 41] or reservation made in accordance with Article 42;

(e) any other act, notification or communication relating to this Convention.

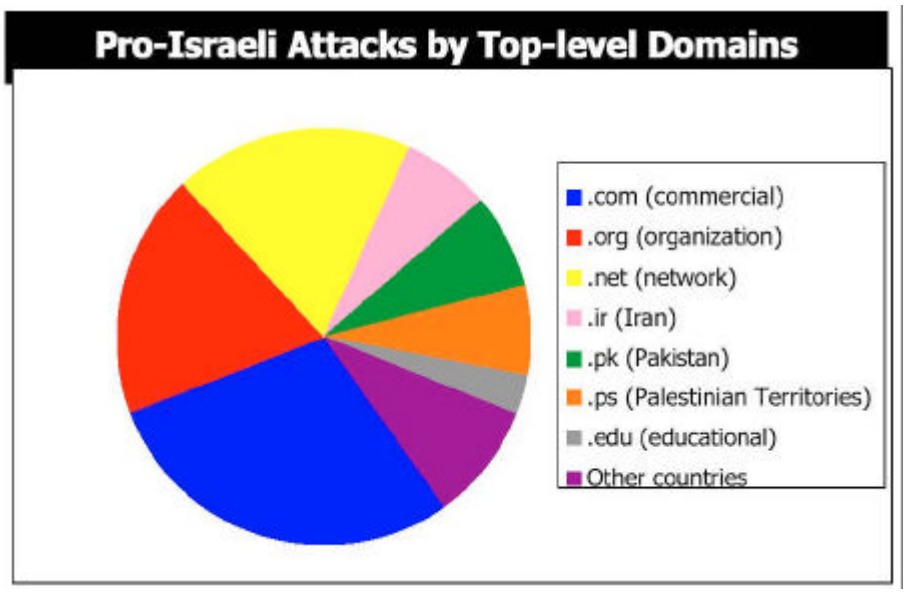
In witness whereof the undersigned, being duly authorised thereto, have signed this Convention. Done at Strasbourg, on …. 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each Member State of the Council of Europe, to the non-member States, which have participated in the elaboration of this Convention, and to any State invited to accede to it.

ANNEX II.

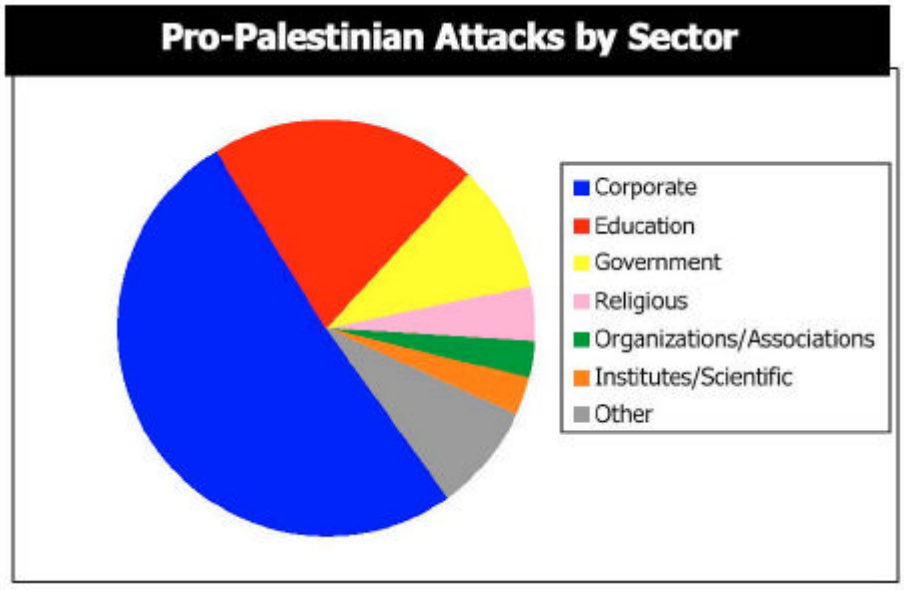
Israeli-Palestinian Caber Conflict



Pro-Palestinian Attackers – Percent of Targeted Sites within a Top-level Domain (TLD)
(does not include every attack or take into consideration repeat attacks)
.il (Israel): 42%
.co.il (59%), .ac.il (21%), .gov.il (13%), .org.il (4%), .k12.il (2%), .idf.il (1%)
.com (commercial): 19%
.org (organizations): 9%
.in (India): 5%
.us (United States) and .sk (Slovak Republic): 3% each
.edu (education), .net (network), .gov (US government) and .my (Malaysia): 2% each
.eg (Egypt) and .cn (China): 1%
.br (Brazil), .it (Italy), .de (Germany), .jp (Japan), .qa (Qatar), .tw (Taiwan), .cz (Czech Republic), .si (Slovenia), .pe (Peru), .be (Belgium), .nl (Netherlands) and .mx (Mexico): 0.7% each

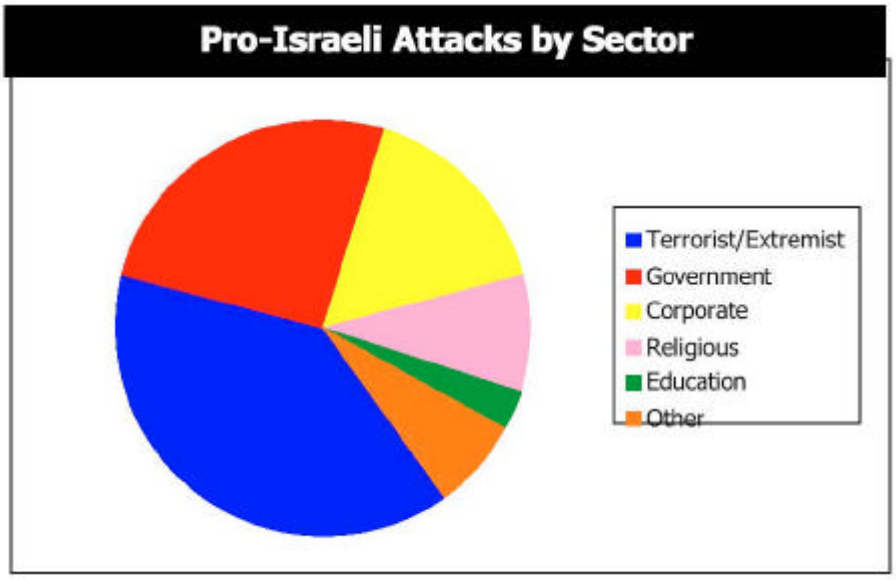


Pro-Israeli Attackers – Percent of Targeted Sites within a TLD
(does not include every attack or take into consideration repeat attacks)
.com (commercial): 29%
.org (organization) and .net (network): 19% each
.ir (Iran), .pk (Pakistan) and .ps (Palestinian Territories): 7% each
.lb (Lebanon), .qa (Qatar), .edu (US education) and .ae (United Arab Emirates): 3% each



Pro-Palestinian Attackers – Targets by Sector
(does not include every attack or take into consideration repeat attacks)
Corporate: 51%
Technology (49%),

Telecommunications (23%),
Media (3%),
Financial, Entertainment, Health (2% each),
Fashion (1%),
Other (6%)
Educational: 21%
Government: 10%
Other: 7%
Religious: 4%
Organizations/Associations, Institutes/Scientific: 3% each
Political: 1%



Pro-Israeli Attackers – Targets by Sector
(does not include every attack or take into consideration repeat attacks)
Terrorist/Extremist: 39%
Government: 26%
Corporate: 16%
Religious: 9%
Educational: 3%
Other: 7%

Internet Sources

http://ash.xanthia.com
http://cism.bus.utexas.edu
http://conventions.coe.int
http://go.to/forum3222
http://ir.jmm.com
http://mitglied.tripod.de
http://news.bbc.co.uk
http://news6.thdo.bbc.co.uk
http://slashdot.org
http://www.adl.org
http://www.antionline.com
http://www.asc.upenn.edu
http://www.asseenin.com
http://www.appcpenn.org
http://www.barbie.com
http://www.big-brother.nl
http://www.bsa.org
http://www.businessweek.com
http://www.cerias.purdue.edu
http://www.cert.org
http://www.childhub.ch
http://www.cme.org
http://www.cnn.com
http://www.computereconomics.com
http://www.crin.org
http://www.cs.cmu.edu
http://www.csis.org
http://www.customs.gov
http://www.cwi.nl
http://www.cyber-snoop.com
http://www.cultdeadcow.com
http://www2.echo.lu
http://www.echo.lu
http://www.ecpat.net
http://www.eff.org
http://www.entertainmentnetwork.com
http://www.europa.eu.int
http://www.fcw.com
http://www.forrester.com
http://www.ftc.gov
http://www.gao.gov
http://www.gocsi.com
http://www.guns.com
http://www.idefense.com
http://www.infowar.com
http://www.internetnews.com
http://www.iptvreports.mcmail.com
http://www.ispcan.org
http://www.ispo.cec.be
http://www.itv.co.uk
http://www.itvreport.com
http://www.i2kcc.org
http://www.keentv.com
http://www.lasvegassun.com
http://www.mcs.dundee.ac.uk
http://www.minbz.nl
http://www.nada.kth.se
http://www.napster.com
http://www.nature.com
http://www.natvan.com
http://www.ncis.co.uk
http://www.nd.edu
http://www.netnanny.com
http://www.nua.com
http://www.oecd.org
http://www.privacyfoundation.org
http://www.rand.org
http://www.rcmp-grc.gc.ca
http://www.replaytv.com
http://www.resist.com
http://www.reuters.com
http://www.ronsangels.com

http://www.rotten.com
http://www.rsac.org
http://www.selbstmordforum.de
http://www.sims.berkeley.edu
http://www1.surfwatch.com
http://www.solidoak.com
http://www.spiegel.de
http://www.splcenter.org
http://www.stiftung.bertelsmann.de
http://www.strategyanalytics.com
http://www.techweb.com
http://www.tivo.com
http://www.un.org
http://www.uncjin.org
http://www.unesco.org
http://www.ucla.edu
http://www.usatoday.com
http://www.usdoj.gov
http://www.vsp.state.va.us
http://www.w3.org
http://www.wiesenthal.com
http://www.whiteracist.com
http://www.wired.com
http://www.zdnet.com

Über die Autoren

Prof. Dr. Jo Groebel

Prof. Dr. Jo Groebel, born 11–11–1950 in Jülich, Germany, is Director-General of the European Institute for the Media, Düsseldorf/Paris, holds the chair for media psychology at the University of Utrecht and is a visiting professor at the University of California in Los Angeles (UCLA) and the University St. Gallen. He was President of the Dutch Association for Communication Sciences (1994–1999). Jo Groebel was/ is advisor to the Dutch government, the President of Germany, the United Nations and UNESCO and several FORTUNE 500-companies. He was head of the media monitoring missions for the European Commission during the 1999 DUMA and the presidential elections 2000 in Russia and the general elections in Serbia, 2000. He has co-operated in his research with, a.o Harvard Law School, Yale and Cambridge Universities. He is author/editor of 20 books and app. 200 articles, published in Europe and the United States. His paper presentations included keynote speeches at the National Academy of Sciences in Washington, D.C., the World Congress of Psychology in Sydney, the World Congress of Mental Health in Auckland, N.Z. and the French Senate. Jo Groebel was co-promoter of the honorary doctorate for British film director Peter Greenaway. He has worked on numerous TV- and radio productions internationally and is an author for press publications including Frankfurter Allgemeine Zeitung, Die Zeit and De Volkskrant. In 1990, he received the ´Outstanding Contributions Award` of the International Council of Psychologists in Tokyo. In June 2000, Jo Groebel presented his vision on the Future Digital Society during the Government conference in Berlin, with 14 Heads of State, where he met personally with, a.o., Clinton, Jospin, Schröder and Mbeki. He also presented his perspective on the future information society to the German chancellor, Gerhard Schröder and part of his cabinet.

Status as at January 2001

Dr. Verena Metze-Mangold

Dr. Verena Metze-Mangold, born 07/10/1946 in Kassel, Germany, is head of the Department of hr-coordination in the General Directorate Hessischer Rundfunk, Frankfurt. She is member of the German Commission for UNESCO, chaired the Board of Experts for Communication, Information and Informatics, is member of the Executive Council and, since 1997, Vice President of the German Commission for UNESCO. Verena Metze-Mangold studied Political Science, Sociology and History at the University of Marburg und finished with honours. She worked in broadcasting stations, the editing-room of a

Berlin based newspaper and on several TV- and radio-productions. She was head of the Protestant Medienakademie, Frankfurt, (1976 – 1987) and head of the communication department of the public broadcasting station, Frankfurt.

She was representative of the German Government at the advisory conference on the Southafrican constitution, where she presented models of freedom of information acts and broadcasting Law. In May 2001 she was German representative at the Stability Pact Conference on media development in East- and Southeast-Europe.

Verena Metze-Mangold lectured at the University of Frankfurt and the University of Marburg and is author and editor of several books and numerous articles on international media development.

Dr. David Ward

David Ward is head of Communication Policy at the European Institute for the Media. Prior to joining the EIM he was a visiting lecturer at the University of Westminster, where he taught on a wide range of media related courses. He is currently a Senior Research Fellow at the Centre for Communication and Information Studies. He has cooperated on a number of research projects that have covered various aspects of the mass media and has published a number of articles on European audiovisual policy.