THE INTERNATIONAL LIBRARY OF CRIMINOLOGY, CRIMINAL JUSTICE & PENOLOGY

SECOND SERIES

COMPUTER CRIME

Indira Carr

Computer Crime

Edited by

Indira Carr

University of Surrey, UK

ASHGATE

Published by
Ashgate Publishing Limited
Wey Court East
Union Road
Farnham
Surerey GU9 7PT
England

Ashgate Publishing Company
Suite 420
101 Cherry Street
Burlington, VT 05401-4405
USA

Ashgate website: http://www.ashgate.com

British Library Cataloguing in Publication Data
Computer crime. – (International library of criminology,
criminal justice and penology. Second series)
1. Computer crimes 2. Compter crimes – Prevention
I. Carr, Indira
364.1'68

Library of Congress Cataloging-in-Publication Data
Computer crime / edited by Indira Carr.
p. cm. – (International library of criminology, criminal justice & penology. Second series)
Includes index.
1. Computer crimes – United States. 2. Computer networks–Law and legislation–United States–Criminal provisions. 3. Data protection–Law and legislation–United States. 4. Computer crimes–Europe. 5. Computer networks–Law and legislation–Europe–Criminal provisions. 6. Data protection–Law and legislation–Europe. I. Carr, Indira.
KF9350.C645 2009
345.73'0268–dc22

2008030280

ISBN: 978-0-7546-2835-4

Printed and bound in Great Britain by
TJ International Ltd, Padstow, Cornwall

Acknowledgements

The editor and publishers wish to thank the following for permission to use copyright material.

Copyright Clearance Center for the essay: Richard W. Downing (2005), 'Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cyber Crime', *Columbia Journal of Transnational Law*, **43**, pp. 707–62. Copyright © 2005 Columbia Journal of Transnational Law.

Emory International Law Review for the essay: Lauren L. Sullins (2006), '"Phishing" for a Solution: Domestic and International Approaches to Decreasing Online Identity Theft', *Emory International Law Review*, **20**, pp. 397–433.

Fordham Intellectual Property, Media and Entertainment Law Journal for the essay: Jessica Habib (2004), 'Cyber Crime and Punishment: Filtering Out Internet Felons', *Fordham Intellectual Property, Media and Entertainment Law Journal*, **14**, pp. 1051–92. Copyright © 2004 Fordham Intellectual Property, Media and Entertainment Law Journal and Jessica Habib.

George Mason School of Law for the essays: Christopher J. Coyne and Peter T. Leeson (2005), 'Who's to Protect Cyberspace?', *Journal of Law, Economics and Policy*, **1**, pp. 473–95; Bruce P. Smith (2005), 'Hacking, Poaching, and Counterattacking: Digital Counterstrikes and the Contours of Self-Help', *Journal of Law, Economics and Policy*, **1**, pp. 171–95; Orin S. Kerr (2005), 'Virtual Crime, Virtual Deterrence: A Skeptical View of Self-Help, Architecture, and Civil Liability', *Journal of Law, Economics and Policy*, **1**, pp. 197–214.

John Marshall Journal of Computer and Information Law for the essay: Miriam F. Miquelon-Weismann (2005), 'The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?', *John Marshall Journal of Computer and Information* Law, **23**, pp. 329–61. Copyright © 2005 John Marshall Journal of Computer and Information Law.

John Marshall Law School for the essay: Adrienne N. Kitchen (2002), 'Go to Jail – Do Not Pass Go, Do Not Pay Civil Damages: The United States' Hesitation Towards the International Convention on Cybercrime's Copyright Provisions', *John Marshall Review of Intellectual Property Law*, **1**, pp. 364–82. Copyright © 2002 John Marshall Law School.

Mary Ann Liebert, Inc. for the essay: John McMullan and Aunshul Rege (2007), 'Cyberextortion at Online Gambling Sites: Criminal Organization and Legal Challenges', *Gaming Law Review*, **11**, pp. 648–65. Copyright © 2007 Mary Ann Liebert, Inc.

Michael A. Sussman (1999), 'The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium', *Duke Journal of Comparative and International Law*, **9**, pp. 451–89. Copyright © 1999 Michael A. Sussman.

Temple International and Comparative Law Journal for the essay: Dina I. Oddis (2002), 'Combating Child Pornography on the Internet: The Council of Europe's Convention on Cybercrime', *Temple International and `Comparative Law Journal*, **16**, pp. 477–518.

Walters Kluwer for the essay: Brian M. Hoffstadt (2007), 'The Voyeuristic Hacker', *Journal of Internet Law*, **2**, pp. 12–23. Copyright © 2007 Walters Kluwer.

Washington and Lee Law Review for the essay: Christopher D. Van Blarcum (2005), 'Internet Hate Speech: The European Framework and the Emerging American Haven', *Washington and Lee Law Review*, **62**, pp. 781–830.

Wiley-Blackwell for the essay: Ray August (2002), 'International Cyber-Jurisdiction: A Comparative Analysis', *American Business Law Journal*, **39**, pp. 531–73.

Every effort has been made to trace all the copyright holders, but if any have been inadvertently overlooked the publishers will be pleased to make the necessary arrangement at the first opportunity.

Preface to the Second Series

The first series of the International Library of Criminology, Criminal Justice and Penology has established itself as a major research resource by bringing together the most significant journal essays in contemporary criminology, criminal justice and penology. The series made available to researchers, teachers and students an extensive range of essays which are indispensable for obtaining an overview of the latest theories and findings in this fast-changing subject. Indeed the rapid growth of interesting scholarly work in the field has created a demand for a second series which, like the first, consists of volumes dealing with criminological schools and theories as well as with approaches to particular areas of crime criminal justice and penology. Each volume is edited by a recognized authority who has selected twenty or so of the best journal essays in the field of their special competence and provided an informative introduction giving a summary of the field and the relevance of the essays chosen. The original pagination is retained for ease of reference.

The difficulties of keeping on top of the steadily growing literature in criminology are complicated by the many disciplines from which its theories and findings are drawn (sociology, law, sociology of law, psychology, psychiatry, philosophy and economics are the most obvious). The development of new specialisms with their own journals (policing, victimology, mediation) as well as the debates between rival schools of thought (feminist criminology, left realism, critical criminology, abolitionism etc.) make it necessary to provide overviews that offer syntheses of the state of the art.

GERALD MARS
Honorary Professor of Anthropology, University College, London, UK

DAVID NELKEN
Distinguished Professor of Sociology, University of Macerata, Italy
Distinguished Research Professor of Law, University of Cardiff, Wales
Honorary Visiting Professor of Law, LSE, London, UK

Introduction

The information technology (IT) revolution in the form of the Internet,[1] a communication medium enabling rapid dissemination of and access to information stored on servers using a computer, a modem, an Internet service provider (ISP) and the World Wide Web, needs no special introduction. It has now become a vital tool for conducting everyday human affairs in many countries, developing and developed. However, major technological innovations always raise important issues: among them the economic, moral and social impact of the technology and the legal framework to establish the rights and liabilities of the various actors involved in the use of that technology. The extent to which a state should intervene in the affairs of those affected by the technology is dependent on a number of factors: the level of the perceived risk, both in the short and in the long term, to a given society by the various actors, including the criminal elements, interests and individuals within that society; the flexibility of the existing legal framework to cope with legal issues that arise in the context of the new technology and its use; the abilities of those within a given society to regulate their affairs in a manner that ensures that legal rights of individuals (or, for that matter, the moral fabric of that society) are not undermined; and the nature of the actors involved in the use of the technology. Policy-makers, legislators and other stakeholders such as non-governmental entities face tough choices. Among the questions they need to address are the following:

- Does the Internet pose problems that are unique to that medium?
- Does it pose special security risks?
- To what extent should the authorities regulate this medium? What form should this regulation take?[2]
- To what extent should dissemination of information using the Internet be monitored?
- Would self-regulation be an adequate means of protecting the vulnerable against exploitation?

On the plus side, the Internet provides a global reach such that people regardless of their geographical location can acquire as well as distribute information as long as they have the necessary tools. It has the advantage of being cheap. Its global reach means new opportunities for growth for the commercial sector. Sellers can advertise their wares and services globally,

---

[1] The Internet is a vast collection of interconnected computer networks that use a protocol known as TCP/IP. The Internet evolved from ARPANET (Advanced Research Projects Network) established by the US Department of Defense. It is a wide area networking system that will survive nuclear attacks. See http://1001.resources.com for further definitions. The World Wide Web is not the same as the Internet. Using a language called HTTP protocol it is a means of disseminating information over the Internet. The Web is also used for various purposes such as e-mail and instant messaging. For further on this, see http://www.webopedia.com.

[2] See Geist (2003) for a review of the different approaches to regulating the Internet, including through code proposed by Lawrence Lessig and Joel Reidenberg.

and buyers, businesses and consumers alike have access to products at competitive prices. Sellers can provide product information, prices and delivery terms, and interested parties can negotiate terms and conclude contracts electronically. Direct access to a potentially large customer base means that sellers do not have to opt for the traditional methods for selling their products – for example, the use of agents to market their products in distant lands. Equally, buyers do not have to go through agents to find suitable manufacturers of the products they require. The IT revolution has created a new means of conducting business electronically, namely e-commerce. The financial and entertainment sectors have also realized the potential of the Internet to provide services such as online banking and online gambling that are instant and uncurtailed by geographical location or time (see, for example, Field, 1997).

On the minus side the Internet is an open network lacking security and so it is open to a variety of abuses. In the 1990s unauthorized access of computers, and the non-availability of computer systems through the introduction of viruses, worms and denial of service attacks[3] were seen to undermine computer security, thus raising the need for criminal law to make the network a safe place to conduct everyday human affairs. Since the 1990s computer crimes have become more sophisticated partly as a result of the realization of the potential of the Internet by criminals for conducting activities ranging from fraud, extortion and blackmail to dissemination of offensive and illegal information. In recent years, we have witnessed, for instance, the growth of identity theft through 'phishing' attacks where users are tricked into divulging details of bank accounts and other personal information for the purposes of fraud; extortion via threats to bring down websites through distributed denial of service attacks; software piracy; and terrorists exploiting the opportunities that the Internet creates for funding their activities (see, for example, Hinnen, 2004).

Securing computer networks from the threat of criminal activity became one of the top priorities of governments in the mid-1990s and remains so to this day. The literature on national laws on computer crime and emerging trends of criminal activity on the Internet has grown steadily over the last twenty years. There are well over three thousand articles on the subject written in the English language and published in national and international academic journals. The task of adhering to the page limit imposed by the publishers made the choice of essays for inclusion in this volume an extremely difficult task and necessitated a selective choice. The selection is intended to give the reader an appreciation of the legal framework for countering cyber crime,[4] the move towards harmonization of the laws on computer crime through an international legal instrument, the issues in respect of investigation and jurisdiction of computer crimes that transcend borders, and non-legal means of countering cyber crime. Since it was not possible to include in this volume all the essays chosen in the initial shortlist, this Introduction concludes with a list of references and further reading for the interested reader to follow up. The extensive references of the essays selected for the volume will also prove a rich source for delving further into the subject matter.

The book is organized into four parts: Part I focuses on the definition of computer crime and emerging criminal activities on the Internet; Part II examines the only international convention aiming to harmonize the laws on computer crime, the Council of Europe Convention on

[3] See Kroczynski (2008) for definition of terms such as viruses and worms.

[4] 'Computer crime' and 'cyber crime' are used interchangeably here.

Cybercrime; Part III highlights issues surrounding investigation, jurisdiction and sentencing; and Part IV looks at ways in which cyber security could be improved.

The Parameters of Computer Crime

Computer crime (also known as cyber crime or net crime) has been variously defined but as yet there is no consensus on its definition. The interpretation of computer crime extends from situations where the computer is the target of the crime (such as in hacking and the spreading of the viruses) to situations where the computer is used as a tool to commit other offences found in traditional criminal law (such as blackmail, fraud and extortion), computer-related economic crime (such as software piracy) and computer-related infringements of privacy (see Sieber, 1998). While it would have been desirable to include essays on all types of computer crime the limited choice in this section was driven by page length.[5]

Richard Downing's essay (Chapter 1) provides a comprehensive legal framework to address computer crime and in this process deals with the issue of definition of terms such as computer crime and network crime. Downing's essay includes substantive and procedural laws in building the framework and also draws the attention of the reader to the Council of Europe Convention on Cybercrime. Chapters 2–4 deal with hacking, phishing and extortion.[6]

In Chapter 2 Brian Hoffstadt, who bases his analysis on US law, is of the view that the law is haphazard when it comes to dealing with the hacker who, for instance, obtains information on a real-time basis through wireless access points.[7] He proposes that a response to protecting against the threats posed by what he terms the 'voyeuristic hacker' needs to be informed by two questions, namely 'what information is worthy of criminal protection and what conduct should be made criminal' (p. 69). Lauren Sullins, in Chapter 3, focuses on the ever-increasing threat of identity theft using phishing attacks and puts forward suggestions that would bring both the private sector and consumers within the fold in the fight against identity theft. She sees co-operation between the private sector and the enforcement authorities, and consumer awareness as vital tools in combating phishing (see also Lynch, 2005). John McMullan and Aunshul Rege's essay (Chapter 4) highlights the challenges and possible solutions for the governance of the online gambling sector by focusing on an emerging threat on the Internet – cyberextortion of online gambling sites where cyber intrusion, destruction and modification of data, and fear are used for the purposes of financial gain.

Harmonization of Computer Crime Laws – The Council of Europe Convention on Cybercrime and the Additional Protocol to the Council of Europe Convention

Many jurisdictions since the 1990s have passed legislation to address computer crime. The problem, however, is that there is no uniformity in the legislation adopted across jurisdictions

---

[5] For an interesting essay on virtual crimes in virtual worlds, see Lastowka and Hunter (2004–2005).

[6] Some of the traditional forms of criminal activities now found on the Internet such as child pornography and hate speech are dealt with in Part II on the Council of Europe Convention on Cybercrime.

[7] For more on wi-fi and wireless hackers (whackers), see Kern (2004).

and this can pose problems when it comes to prosecution because of the borderless character of computer crime. For instance, State X could have made unauthorized access of computers an offence while State Y may not have. An individual located in State Y could access a computer located in State X without authorization. While this access under State X's law is a criminal offence, prosecuting the individual is likely to be difficult since he is located in State Y. It is possible for a state to include an extraterritorial component in its computer crime legislation, as has been done by a number of states such as Singapore and the US (see, for example, Geist 2003). This, however, does not provide a satisfactory solution since cross-border investigation and extradition may be problematic. Against this context it makes sense to harmonize the substantive law across jurisdictions through an international convention which also provides for cross-border investigation and co-operation and extradition.

The Council of Europe responded to this need with its Convention on Cybercrime (COE Convention). The work commenced in 1997 and the final draft was adopted on 23 November 2001. It is the only international treaty on the subject of computer crime and came into force on 1 July 2004.[8] From the beginning, observer nations such as Canada, Japan, South Africa and most importantly the US have participated fully in the negotiations and this inevitably has had marked effects on the shape of the final document. It is also seen as an instrument for global adoption.

As for the historical background, the Council of Europe started work on computer-related crime in the late 1980s and in 1989 published its Recommendation R89(9) on Computer-Related Crime (R89(9)).[9] R89(9) suggested that eight specific types of conduct should be incorporated into the criminal laws of member states: computer-related fraud, computer forgery, damage to computer data or programs, computer sabotage, unauthorized access, unauthorized interception of data transmissions, unauthorized reproduction of a protected computer program, and unauthorized reproduction of a topography. It also suggested four other activities that should be discouraged: alteration of computer data or computer programs, computer espionage, unauthorized use of a computer and unauthorized use of a protected computer program. Since investigation of crime involving information technology poses special problems for enforcement authorities, the Council of Europe started work on this aspect in the early 1990s culminating in Recommendation 95(13) on the Harmonisation of Criminal Procedural Laws Relating to Information Technology (R95(13)).[10] This recommendation includes provisions not only on search, seizure, surveillance and cryptography but also on other aspects such as collection of statistics, training of personnel and co-operation between enforcement authorities.

Casting its net wide, the COE Convention requires signatory states to criminalize a host of activities that, in one way or another, are connected to a computer, computer material, computer operation or a computer system. Offences are categorized into four groups:

---

[8] CETS No. 185. Text of the convention is available at http://www.coe.int. Ratifications have been received from Albania, Armenia, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Latvia, Lithuania, Netherlands, Norway, Romania, Serbia, Slovakia, Slovenia, the former Yugoslav Republic of Macedonia, Ukraine and the United States of America.

[9] 1989, Strasbourg, Council of Europe.

[10] 1995, Strasbourg: Council of Europe. The text of this document is also available at http://www.coe.int.

Group 1: Offences against confidentiality, integrity and availability of computer systems (to include unauthorized illegal access to a computer system, illegal interception encompassing eavesdropping, blocking or interfering with the use of a system, import, sale or distribution of devices capable of commission of the offences against the confidentiality or integrity of a computer system or data)

Group 2: Computer-related offences (computer forgery and computer fraud)

Group 3: Content-related offences (offences related to child pornography through the medium of a computer)

Group 4: Copyright-related offences (infringement of copyright as defined in the Berne Convention for the Protection of Literary and Artistic Works 1886, the WIPO Copyright Treaty 1996 and the 1993 TRIPS Agreement involving a computer system).

Offences listed in Groups 1, 2 and 4 are to be found in Recommendation R89(9) on Computer-Related Crime. Group 3 is an important development in the light of the use of the Internet for distribution of offensive material and aims to uphold human dignity by focusing on child pornography. Equally the drafters of the COE Convention seem to have taken R95(13) fully on board, while expecting parties to ensure that in the implementation and application of the COE Convention there will be safeguards in place for the adequate protection of human rights and liberties (Art 15). The COE Convention imparts enforcement authorities to search computer systems and seize information (Art 19); to order service providers (within its jurisdiction) to provide information in respect of the subscriber, such as identity, postal address, billing and payment information (Art 18); to collect traffic data in real time and ask others such as service providers to assist in its collection (Art 20); and to intercept content data (Art 21).

An area that was the subject of much discussion during the drafting of the COE Convention was the provision on criminalizing hate speech on the Internet. Largely due to resistance from the US which does not have laws criminalizing or prohibiting hate speech the relevant provisions were omitted in the adopted text. The Council of Europe drafted the Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems, which was adopted on 28 January 2003 and came into force on 1 March 2006.[11]

Part II begins with Mike Keyser's essay (Chapter 5) which provides an article by article analysis of the COE Convention. It also highlights some of the deficiencies of the procedural provisions – for instance, the extensive powers imparted to the investigating authorities that call into question the protection of human rights and the right to privacy. Carr and Williams (1998, pp. 475–79) in an essay on R95(13) raise their concerns about both the wide powers conferred on investigating authorities requiring the co-operation of those investigated and possible breaches of human rights – for instance, under Arts 6(1) and (2) of the European Convention of Human Rights. Since many of the recommendations made in R95(13) have been adopted by the COE Convention the issues raised in relation to R95(13) resurface. In Chapter 6

[11] CETS No. 189. Text of the protocol is available at http://www.coe.int. Ratifications were received from Albania, Armenia, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, France, Latvia, Lithuania, Norway, Serbia, Slovenia, the former Yugoslav Republic of Macedonia and Ukraine.

Miriam Miquelon-Weismann considers the procedural provisions of the COE Convention and examines the model for due process in that Convention. She finds the model wanting since no minimal standard for due process is provided and the excuse of 'cultural differences' given by the Council of Europe in its Explanatory Memorandum to the Convention for the absence of providing such a standard unjustifiable. In Chapter 7 D.C. Kennedy, after examining the increased police powers imparted by the COE Convention and the privacy issues, argues that the increase in police powers necessitates an offsetting in privacy protection for individuals and that suitable provision for this should have been made in the Convention.

On the substantive side, the two most important departures in the COE Convention from the list of offences found in most national computer crime legislation are offences in respect of copyright and child pornography. The inclusion of the copyright offence within the COE Convention has come under constant criticism since the purpose of copyright protection is largely seen as protecting creativity, and infringements are normally addressed using civil law. In a thoughtful essay Adrienne Kitchen (Chapter 8) raises the issue of whether the creation of the criminal offence in respect of copyright infringement involving a computer system will make serious inroads into deterring such activities since it does not address issues of enforcement. She suggests that the inclusion of issues and consequences of copyright infringement which are largely economic would have more impact if included in the context of a free trade agreement since it would provide a 'practical forum through which laws may be created and effectively enforced in the marketplace' (p. 281). The US-Jordan Free Trade Agreement is provided as a model of how intellectual property rights could be protected. An alternative suggestion put forward is for the drafting of an international convention for copyright infringement in the digital environment.

Chapter 9, by Dina Oddis, examines the COE Convention's provisions on computerized child pornography, the procedural law and the safeguards to protect individual human rights. In a tightly argued section Oddis concludes that, despite criticisms that the COE Convention has not 'adequately attended' to the protection of human rights, the Convention is firmly embedded in the fundamental freedoms and human rights enshrined in the European Convention on Human Rights.

Chapter 10 focuses on the important issue of hate speech. While providing an analysis of the hate speech provisions in the COE Cybercrime Protocol Christopher van Blarcum considers the impact of the Protocol on the US and whether it will have the effect of making the US a safe haven for Internet hate speech. In examining ways to mitigate the US as a safe haven, he suggests, among other solutions, that 'if hate speech becomes a debilitating social problem in the US, a "Constitutional moment" could occur' (p. 374) that may result in a reassessment of the First Amendment which protects free speech.

Investigation, Jurisdiction and Sentencing Issues

Since the Internet is borderless, the enforcement of computer crime laws poses special problems. Investigation across borders is a major issue and so also is the issue of jurisdiction. And where these difficulties have been surmounted and the offender has been apprehended and successfully prosecuted, questions arise in respect of sentencing.

In Chapter 11 Michael Sussman highlights the challenges that computer crimes pose to enforcement authorities – from sufficient laws to punish computer crimes, personnel and

resources, locating and identifying criminals, preservation of data and means of obtaining evidence from other jurisdictions,[12] to preservation of evidence and extradition. He also considers the various international organizations working towards finding solutions to these issues. Reference is also made to the COE Convention on Cybercrime, which has extensive provisions on questions such as preservation of data and trans-border searches.

In Chapter 12 the issue of international criminal and civil jurisdiction in cyberspace is explored by Ray August, using examples. He concludes that in respect of international criminal jurisdiction the nexuses of territoriality, nationality, protection and universality used traditionally by courts will apply equally in cyberspace. Since there is a high risk of multiple and conflicting jurisdictional claims in applying the nexuses his view is that there is a strong need to harmonize international criminal jurisdiction in cyberspace through an international convention. Jessica Habib's essay (Chapter 13) focuses on the issue of sentencing computer criminals. Some jurisdictions have indeed taken a tough stance[13] while others have given rather light sentences in the form of community services orders.[14] Habib raises the interesting question of denying computer criminals access to the Internet. Using developments in respect of such bans in the US courts she argues that given the central role of the Internet as a communication medium in modern society the courts need to balance the question of banning Internet use against how the Internet use related to the criminal act committed by the offender.

Cyber Security

Given the threats to the computer environment the question of how this space should be protected remains. Christopher Coyner and Peter Leeson's thoughtful essay (Chapter 14) strongly suggests that an analysis of cyber security requires the inclusion of economic considerations. They make a number of interesting suggestions for increasing cyber security through, for instance, cyber insurance and extending liability to software authors and system operators.

Much has been written about the ineffectiveness of criminal legislation to control criminal activity on the Internet. Besides problems such as low reporting of breaches of computer security by corporations and cross-border issues in respect of investigation, there is also a lack of adequate enforcement personnel. In these circumstances, use of technological means to protect computer systems seems attractive. Firewalls and anti-virus programs are the widely used means for protecting computers and computer networks. However, in March 2004 Symbiot Inc. announced the development of a product that that could not only repel hostile attacks but counter-attack the originators of the hostile attack. In Chapter 15 Bruce Smith examines both the physical and the legal pitfalls of the counterstrike technologies, especially whether such technologies would violate laws on computer crime. Relying on an analogy of the use of spring guns to combat illegal poaching in nineteenth-century England for his analysis, he concludes that unlike the spring guns that proved to be "'remorseless engines,

---

[12] On trans-border searches see Seitz (2004–2005).

[13] For instance, Singapore (see Carr and Williams, 2000).

[14] See, for instance, the following cases in England: *R* v. *Mark Hopkins*, Westminster Magistrates Court (9/8/2007); *R* v. *Joseph McElroy*, Southwark Crown Court (3/2/2005).

[that] sacrificed every thing within their range," twenty-first century digital counterstrike technologies at least hold out the prospect of counterattacks that are clear-sighted, calculating, discriminating, and – if not remorseful – at least compensable' (p. 555). Finally, Orin Kerr's essay (Chapter 16), which questions securing the Internet through self-help, redesigning the architecture of cyberspace and civil liability, provides much food for thought.

Conclusions

There is no doubt that computer crime, be it defined narrowly or broadly, causes both untold human misery and economic harm to organizations. For organizations it can cause reputational loss alongside the financial cost of putting things right when computer systems have been subject to computer attacks. In the event of identity theft it causes individual loss and misery. And through dissemination of illicit images it greatly undermines human dignity and decency and questions basic human values. Computer attacks have the potential to lower the security of a state thus putting lives at danger. In these circumstances it is clear that the question of who is to ensure that the Internet is a safe environment in which to carry on legitimate activities is an important one.

Should it be left to criminal law and governments to bear the burden of making the Internet a safe place? Criminalization of itself is insufficient to increase the safety of the Internet since it is dependent on detection, investigation and successful prosecution. There is only a certain amount a government can do in enforcing its laws due to its myriad of national commitments ranging from education, health and safety to infrastructural support. Other means of protecting this space, ranging from self-help, setting minimum levels of security against cyber attacks for software and hardware manufacturers to setting minimum standards of security to be met by the users, are equally important. As for the dissemination of illegal materials through the Internet, more could be required of the ISP on whose servers racist and child pornography websites are located. It may also be worth thinking further about setting up an international organization to regulate Internet content, a solution put forward by Paul Przybylski (2000). Inevitably all this will raise the cost of using the Internet. Ultimately it is a policy decision, a matter of balancing safety against cost.

References and Further Reading

Barnes, Douglas A. (2004), 'Deworming the Internet', *Texas Law Review*, **83**, pp. 279–329.

Baron, Ryan M.F. (2002), 'A Critique of the International Cybercrime Treaty', *CommLaw Conspectus*, **10**, pp. 263–78.

Bellia, Paula M. (2004), 'Defending Cyber Property', *New York University Law Review*, **79**, pp. 2164–273.

Benoliel, Daniel (2005), 'Law, Geography and Cyberspace: The Case of On-Line Territorial Privacy', *Cardozo Arts and Entertainment Law Journal*, **23**, pp. 125–96.

Brenner, Susan W. (2003), 'Complicit Publication: When Should the Dissemination of Ideas and Data be Criminalized?', *Albany Journal of Science and Technology*, **13**, pp. 273–429.

Brenner, Susan W. (2007), '"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare', *Journal of Criminal Law and Criminology*, **97**, pp. 379–476.

Brenner, Susan W., Carrier, Brian and Henninger, Jef (2004), 'The Trojan Horse Defense in Cybercrime Cases', *Santa Clara Computer and High Technology Law Journal*, **21**, pp. 1–54.

Brenner, Susan W. and Scherwa IV, Joseph J. (2002), 'Transnational Evidence Gathering and Local Prosecution of International Cybercrime', *John Marshall Journal of Computer and Information Law*, **20**, pp. 347–96.

Carr, I. and Williams, K.S. (1998), 'Council of Europe on the Harmonisation of Criminal Procedural Laws Relating to Information Technology (Recommendation No. R 95(13)) – Some Comments', *Journal of Business Law*, pp. 468–84.

Carr, I.M. and Williams, K.S. (2000), 'A Step too Far in Controlling Computers? The Singapore Computer Misuse (Amendment) Act 1998', *International Journal of Law and Information Technology*, **8**, pp. 48–64.

Corbett, Patrick E. (2004), 'Anatomy of a Computer Crime: Awareness of the Problem may Provide a Remedy', *Thomas M. Cooley Journal of Clinical and Practical Law*, **7**, pp. 149–73.

Field, Richard L. (1997), '1996: Survey of the Year's Developments in Electronic Cash Law and the Laws Affecting Electronic Banking in the United States', *American University Law Review*, **46**, pp. 967–1025.

Geist, Michael (2003), 'Cyber Law 2.0', *Boston College Law Review*, **44**, pp. 323–58.

Goodno, Naomi Harlin (2007), 'Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws', *Missouri Law Review*, **72**, pp. 125–97.

Heller, Ian (2007), 'How the Internet has Expanded the Threat of Financial Identity Theft, and What Congress can do to Fix the Problem', *Kansas Journal of Law and Public Policy*, **17**, pp. 83–107.

Hinnen, Todd M. (2004), 'The Cyber-front in the War on Terrorism: Curbing Terrorist Use of the Internet', *Columbia Science & Technology Law Review*, **5**, available at: http://www.stlr.org/cite.cgi?volume=5&article=5.

Howell, Beryl A. (2004–2005), 'Real World Problems of Virtual Crime', *Yale Journal of Law and Technology*, **7**, pp. 103–22.

Katyal, Neal Kumar (2001), 'Criminal Law in Cyberspace', *University of Pennsylvania Law Review*, **149**, pp. 1003–114.

Katyal, Neal Kumar (2005), 'Community Self-Help', *Journal of Law, Economics and Policy*, **1**, pp. 33–67.

Kenneally, Erin E. (2005), 'Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection', *UCLA Journal of Law and Technology*, **1**, pp. 5–40.

Kern, Benjamin D. (2004), 'Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law', *Santa Clara Computer and High Technology Law Journal*, **21**, pp. 101–63.

Kroczynski, Robert J. (2008), 'Are the Current Computer Crime Laws Sufficient or Should the Writing of the Virus Code be Prohibited?', *Fordham Intellectual Property, Media and Entertainment Law Journal*, **18**, pp. 817–65.

Lastowka, F. Gregory and Hunter, Dan (2004–2005), 'Virtual Crimes', *New York Law School Review*, **49**, pp. 293–316.

Leeson, Peter T. and Coyne, Christopher J. (2005), 'The Economics of Computer Hacking', *Journal of Law, Economics and Policy*, **1**, pp. 511–32.

Lynch, Jennifer (2005), 'Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks', *Berkeley Technology Law Journal*, **20**, pp. 259–300.

Marler, Sara L. (2002), 'The Convention on Cyber-Crime: Should the United States Ratify?', *New England Law Review*, **37**, pp. 183–219.

Preston, Cheryl B. (2007), 'WIFI in Utah: Legal and Social Issues', *Utah Law Journal*, **20**, pp. 29–37.

Przybylski, Paul (2000), 'A Common Tool for Individual Solutions: Why Countries Should Establish an International Organization to Regulate Internet Content', *Vanderbilt Journal of Entertainment and Technology Law*, **9**, pp. 927–56.

Roche, Edward M. (2007), 'Internet and Computer Related Crime: Economic and Other Harms to Organizational Entities', *Mississippi Law Journal*, **76**, pp. 639–64.

Seitz, Nicolai (2004–2005), 'Transborder Search: A New Perspective in Law Enforcement?', *Yale Journal of Law and Technology*, **7**, pp. 23–50.

Sieber, U. (1998), *Legal Aspects of Computer-related Crime in the Information Society – COMCRIME-Study*, Prepared for the European Commission (Legal Advisory Board). Available at: www.archividelnovecento.it.

Williams, Katherine S. and Carr, Indira (2002), 'Crime, Risk and Computers', *Electronic Communication Law Review*, **9**, pp. 23–53.

Yang, Debra Wong and Hoffstadt, Brian (2006), 'Countering the Cyber Crime Threat', *American Criminal Law Review*, **43**, pp. 201–16.

Xiaomin Huang, Radkowski III, Peter and Roman, Peter (2007), 'Computer Crimes', *American Criminal Law Review*, **44**, pp. 285–335.

Contents