

References

- Archick, K. (2006), *Cybercrime: The Council of Europe Convention*, Washington, DC: The Library of Congress.
- ASRS (2006), 'The ASRS celebrates its 30th anniversary', *Callback From NASA's Aviation Safety Reporting System*, retrieved 19 February, 2010, from http://asrs.arc.nasa.gov/publications/callback/cb_317.htm
- ASRS (2008), ASRS Program Briefing, retrieved 19 February, 2010, from <http://asrs.arc.nasa.gov/overview/summary.html>
- Auerbach, C. F. and L. B. Silverstein (2007), *Qualitative Data: An Introduction to Coding and Analysis*, New York: New York University Press.
- Ayres, I. and J. Braithwaite (1992), *Responsive Regulation: Transcending the Deregulation Debate*, Oxford: Oxford University Press.
- Ayto, J. (2007), *A Century of New Words*, Oxford: Oxford University Press.
- Barlow, J. P. (1996), *A Declaration of Independence for Cyberspace*, retrieved 28 September, 2007, from <http://homes.eff.org/~barlow/Declaration-Final.html>
- BBC (2007a, 4 September), 'China denies Pentagon cyber-raid', *BBC News Online*, retrieved 26 September 2007, from <http://news.bbc.co.uk/2/hi/americas/6977533.stm>
- BBC (2007b, 17 May), 'Estonia hit by "Moscow cyber war"', *BBC News Online*, retrieved 31 October 2008, from <http://news.bbc.co.uk/2/hi/europe/6665145.stm>
- BBC (2008, 25 January), 'Estonia fines man for "cyber war"', *BBC News Online*, retrieved 25 March 2010, from <http://news.bbc.co.uk/2/hi/technology/7208511.stm>
- BBC (2009, 20 September), 'Taiwan city to screen Kadeer film', *BBC News Online*, retrieved 18 September 2010, from <http://news.bbc.co.uk/2/hi/8265259.stm>
- BBC (2010, 15 January), 'Microsoft admits Explorer used in Google China hack', *BBC News Online*, retrieved 18 January 2010, from <http://news.bbc.co.uk/2/hi/technology/8460819.stm>
- Beccaria, C. (1819), *An Essay on Crimes and Punishments*, Philadelphia: Philip H. Nicklin.
- Benyon, J. (1996), 'The politics of police co-operation in the European Union', *Journal of the Sociology of Law*, **24**, 353–379.
- Black, D. (1976), *The Behavior of Law*, New York: Academic Press.

- Bort, J. (2007, 6 July), 'Attack of the killer bots', *Network World*, retrieved 21 March 2010, from <http://www.networkworld.com/research/2007/070607-botnets.html>
- Braithwaite, J. (2002), 'Reward and regulation', *Journal of Law and Society*, **29**(1), 12–26.
- Braithwaite, J., T. Makkai and V. Braithwaite (2007), *Regulating Aged Care: Ritualism and the New Pyramid*, Northampton, MA: Edward Elgar.
- Braithwaite, V. (2007), 'Responsive regulation and taxation: Introduction', *Law and Policy*, **29**(1), 3–10.
- Brenner, S. (2004), 'Distributed security: A new model of law enforcement', *Journal of International Law*, **8**(5), 7–25.
- Brenner, S. (2006), 'Cybercrime jurisdiction', *Crime, Law and Social Change*, **46**, 189–206.
- Brenner, S. (2009), *Cyberthreats: The Emerging Fault Lines of the National State*, Oxford: Oxford University Press.
- Brenner, S. (2010), *Cybercrime: Criminal Threats from Cyberspace*, Santa Barbara, CA: Praeger.
- Butterfield, F. (1982), *China: Alive in the Bitter Sea*, New York: Times Books.
- Cairncross, F. (1997), *The Death of Distance: How the Communications Revolution Will Change Our Lives*, Boston, MA: Harvard Business School Press.
- Cameron, S. (2009), *Reporting HIV in Australia: Information for Journalists*, Canberra: Australian Federation of AIDS Organisations.
- Capeller, W. (2001), 'Not such neat net: some comments on virtual criminality', *Social and Legal Studies*, **10**, 229–242.
- Central Intelligence Agency. (2010), *The World Factbook*, retrieved 19 March, 2010, from <https://www.cia.gov/library/publications/the-world-factbook/index.html>
- Chabinsky, S. R. (2010), *The cyber threat: Who's doing what to whom?*, Paper presented at the FOSE 2010: Technology Solutions for the Business of Government, retrieved 20 March 2010, from <http://fose.com/events/fose-2010/sessions/wednesday/chabinsky.aspx>
- Chandler, A. (1996), 'The changing definition and image of hacker in popular disclosure', *International Journal of the Sociology of Law*, **24**, 229–251.
- Chang, G. L. (2010), 'Mutual assistance between Taiwan and China: It is still difficult to repatriate criminals', *Chinatimes*, retrieved 3 January, 2010, from <http://news.chinatimes.com/CMoney/News/News-Page-content/0,4993,11050701+122010010300163,00.html>

- Chang, K. F. (2006, 29 December), '32 companies signed the self-regulation against malicious software', *CBINews*, retrieved 28 February 2010, from <http://www.cbinews.com/inc/showcontent.jsp?articleid=48377>
- Chang, S. Y. and G. M. Zhao (2006, 25 August), 'Anti-Chen Shiu-bing: Chinese hackers hack into Taiwanese systems', *Chinatimes*, retrieved 15 March 2010, from <http://forum.icst.org.tw/phpbb/viewtopic.php?t=10765>
- Chang, Y. C. (2009a, 5 August), 'The support from China and the legislative Yuan is important in combating telecommunication fraud', *UDN*, retrieved 21 January 2010, from <http://www.coolloud.org.tw/node/44183>
- Chang, Y. C. (2009b), 'Wiki' crime prevention – What Routine Activity Theory teaches us about cybercrime prevention, *Journal of Criminology*, **12**(2), 87–116.
- Chang, Y. C. (2011), 'Cyber-conflict between Taiwan and China', *Strategic Insight*, **10**(1), 26–35, available at http://www.nps.edu/Academics/Centers/CCC/Research-Publications/StrategicInsights/2011/Apr/SI-v10-i1-_Chang.pdf
- Chang, Y. C. (2012a), 'Combating cybercrime across the Taiwan Strait: Investigation and prosecution issues', *Australian Journal of Forensic Sciences*, **44**(1), 5–14.
- Chang, L. Y. C. (2012b), 'Responsive regulation and the reporting of information security incidents', *Issues & Studies*, **48**(1), 93–127.
- Chang, Y. C. and S. Jou (2007), 'A comparative research on cybercrime laws: The experience of International Organizations and Taiwan', *Essays on Criminal Justice Policy and Research*, **10**, 139–158.
- Chang, Y. C. and J. Wu (2008), 'Study on information security incidents reporting and information sharing mechanism in Taiwan – From the viewpoints of the U.S. experience', *Science and Technology Law Review*, **20**(8), 39–61.
- Chao, Y. (2010, 16 January), 'Google attacks used addresses based in Taiwan', *Taipei Times*, retrieved 15 March 2010, from <http://www.taipetimes.com/News/front/archives/2010/01/16/2003463643>
- Chen, A. (2005), 'Secret society and organized crime in contemporary China', *Modern Asian Studies*, **39**(1), 77–107.
- Chen, L. Q. (2008, 22 March), 'War on 322 – Chinese hackers shut down the website of DPP's presidential candidate', *NowNews*, retrieved 22 April 2009, from <http://www.nownews.com/2008/03/22/11480-2249184.htm>
- Chen, R. and J. S. Wang (2009), 'From the "Kinmen Agreement" to the "Agreement on Cross-Strait Mutual Assistance in Crime Matters"', *Fu-Jen Law Journal*, **99**, 51–55.

- Chen, T. Z. (2002, 13 June), 'Taiwan Tea Party website attacked by DDoS', *PCzone*, from <http://www.pczone.com.tw/vbb3/archive/t-47652.html>
- ChinaByte. (2004, 23 September), 'Credit card websites are suffering DDoS attack', *ChinaByte Online*, retrieved 20 September 2008, from <http://www.yesky.com/busnews/216485043416072192/20040923/1857545.shtml>
- Choo, K.-K. R., R. G. Smith and R. McCusker (2007), *Future Directions in Technology-Enabled Crime: 2007–2009*, Canberra: Australian Institute of Criminology.
- Cisco (2009), *Infiltrating a Botnet*, San Jose, CA: Cisco Systems Inc.
- Clarke, R. and M. Felson (eds) (1993), *Routine Activity and Rational Choice*, New Brunswick: Transaction.
- Clarke, R. V. (1999a), *Hot Products: Understanding, Anticipating and Reducing Demand for Stolen Goods*, London: Home Office.
- Clarke, R. V. (1999b), *Opportunity Makes the Thief: Practical Theory for Crime Prevention*, London: Home Office.
- Clinton, H. R. (2010), *Remarks on Internet Freedom*, retrieved 21 January, 2010, from <http://www.state.gov/secretary/rm/2010/01/135519.htm>
- CNCERT/CC (2008), *CECERT/CC Annual Report 2007*, Beijing: CNCERT/CC.
- CNCERT/CC (2009), *Internet Security Working Report – The First Half of 2008*, Beijing: CNCERT/CC.
- Cohen, L. and M. Felson (1979), 'Social change and crime rate trends: A routine activity approach', *American Sociological Review*, **44**, 588–607.
- Collins, R. (1979), *The Credential Society*, New York: Academic Press.
- Council of Europe (2001a), *Convention on Cybercrime*, retrieved 17 November 2009, from <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.
- Council of Europe (2001b), *Convention on Cybercrime: Explanatory Report*, retrieved 10 November 2009, from <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>
- Council of Europe (2009, 11 November), *Convention on Cybercrime*, retrieved 11 November, 2009, from <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>
- Crow, I. and N. Semmens (2008), *Researching Criminology*, Maidenhead: Open University Press.
- Cui, Y. and Y. Chen (eds) (2008), *Jisuanji Wanlufanzui ji Anlifenshi [Information Security and Cybercrime Prevention]*, Beijing: Chinese People's Public Security University.
- DFAT (2010a), *People's Republic of China country brief*, retrieved 10 October, 2010, from http://www.dfat.gov.au/geo/china/china_brief.html
- DFAT (2010b), *Taiwan brief*, retrieved 10 October, 2010, from http://www.dfat.gov.au/geo/taiwan/taiwan_brief.html

- DiMaggio, P. J. and W. W. Powell (1983), 'The iron cage revisited: institutional isomorphism and collective rationality in organizational fields', *American Sociological Review*, **48**, 147–160.
- Dirro, T. (2009, 24 July), 'Counting badness', *McAfee Avert Labs Blog*, retrieved 30 August 2009, from <http://www.avertlabs.com/research/blog/index.php/2009/07/24/counting-badness>
- Doyle, T. J. M. K. Glynn and S. L. Groseclose (2002), 'Completeness of notifiable infectious disease reporting in the United States: An analytical literature review', *American Journal of Epidemiology*, **155**(9), 866–874.
- Duff, L. and S. Gardiner (1996), 'Computer crime in the global village: Strategies for control and regulation', *International Journal of the Sociology of Law*, **24**, 211–228.
- Dunn, J. E. (2009, 22 September), 'Botnet PCs stay infected for year: Trend Micro analysis finds "hidden continent" of zombies', *Network World*, retrieved 21 March 2010, from <http://www.networkworld.com/news/2009/092209-botnet-pcs-stay-infected-for.html>
- Dvorsky, G. (2007, 24 September), 'Storm botnet storms the Net', *IEET Newsletter*, retrieved 15 August 2009 from <http://ieet.org/index.php/IEET/more/dvorsky20070927/>
- ENISA (2009), *ENISA Inventory of CERT activities in Europe*, Heraklion, Greece: European Network and Information Security Agency
- Ericson, R. V. (2007), *Crime in an Insecure World*, Cambridge: Polity Press.
- ERIUM (2007), *Cyber-crime reporting and intelligence: How do we know what is happening?*, Paper presented at the Tackling Crime and Achieving Confidence in the On-Line World Parliament and the Internet Conference. Retrieved 27 January 2010, from http://www.eurim.org.uk/activities/ecrime/PIC07_techapp_reporting.pdf
- Evans, M. (2007), 'China "tops list" of cyber-hackers seeking UK government secrets', retrieved 26, Sept, 2007, from <http://www.timesonline.co.uk/tol/news/world/asia/article2393979.ece>
- F-Secure (2002), 'F-Secure Virus Descriptions: CIH', retrieved 10 March, 2010, from <http://www.f-secure.com/v-descs/cih.shtml>
- FAA (1997), *Aviation Safety reporting Program*, retrieved 19 February 2010, from [http://rgl.faa.gov/REGULATORY_AND_GUIDANCE_LIBRARY/RGADVISORYCIRCULAR.NSF/0/64358057433fe192862569e7006da716/\\$FILE/AC00-46D.pdf](http://rgl.faa.gov/REGULATORY_AND_GUIDANCE_LIBRARY/RGADVISORYCIRCULAR.NSF/0/64358057433fe192862569e7006da716/$FILE/AC00-46D.pdf)
- Fafinski, S. (2009), *Computer Misuse: Response, Regulation and the Law*, Cullompton, Devon: Willan Publishing.
- Feeley, M. M. and J. Simon (1992), The new penology: Notes on the emerging strategy of corrections and its implications, *Criminology*, **30**(4), 449–474.

- Feeley, M. M. and J. Simon (1994), 'Actuarial justice: The emerging new criminal law' in D. Nelkin (ed.), *The Future of Criminology*, Thousand Oaks, CA: Sage, pp. 173–201.
- Fei, H. T. (1947/2002), *From the Soil: The Foundation of Chinese Society* (G. Hamilton and W. Zheng, trans.), Berkeley, CA: University of California Press.
- Fei, H. T. (1980 [1939]), *Peasant Life in China*, London: Routledge & Kegan Paul.
- Felson, M. (1994), *Crime and Everyday Life*, Thousand Oaks, CA: Sage.
- Felson, M. (2000), 'The routine activity approach: A very versatile theory of crime', in R. Paternoster and R. Bachman (eds), *Explaining Criminals and Crime*, Thousand Oaks, CA: Sage, pp. 43–46.
- Find (2006), *2006 Report on the Use of Information Application in Industries*, Taipei: Institute for Information Industry.
- Fisher, L. (2003), 'The rise of the risk commonwealth and the challenge for administrative law', *Public Law*, Autumn, 455–478.
- Flight Safety Information (2003), 'Aviation safety action program', *Flight Safety Information*, Q3, 5–6.
- Fong, J. (2009, 24 August), 'Crash of the transportation monitoring system lasts 1.5 hours – Suspiciously caused by cyber attack', *UDN*, retrieved 24 August 2009, from <http://udn.com/NEWS/NATIONAL/BREAKING/NEWS1/5096528.shtml>
- Fong, J. G. (2003), 'Cybercrime and Convention on Cybercrime (I)', *Taiwan Jurist*, 4, 124–136.
- Fontana, A. and J. H. Frey (2000), 'The interview: From structured questions to negotiated text' in N. K. Denzin and Y. S. Lincoln (eds), *Handbook of Qualitative Research*, Thousand Oaks, CA: Sage, pp. 645–672.
- Fukuyama, F. (1999), *Social capital and civil society*, Paper presented at the IMF Conference on Second Generation Reforms, retrieved 3 March 2010, from <http://www.imf.org/external/pubs/ft/seminar/1999/reforms/fukuyama.htm#1>
- GAO (2004a), *Critical Infrastructure Protection: Establishing Effective Information Sharing with Infrastructure*, Washington, DC: U.S. Government Accountability Office.
- GAO (2004b), *Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors*, Washington, DC: U.S. Government Accountability Office.
- GAO (2006), *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*, Washington, DC: U.S. Government Accountability Office.

- GAO (2009), *Information Security: Further Actions Needed to Address Risks to Bank Secrecy Act Data*, Washington, DC: U.S. Government Accountability Office.
- GAO (2010), *Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative*, Washington, DC: U.S. Government Accountability Office.
- Garland, D. (1997), 'The punitive society: Penology, criminology and the history of the present', *The Edinburgh Law Review*, **1**, 180–199.
- Gerspacher, N. (2008), 'The history of international police cooperation: a 150-year evolution in trends and approaches', *Global Crime*, **9**(1), 169–184.
- Gibson, W. (1982), *Burning Chrome*, retrieved 15 March, 2010, from http://project.cyberpunk.ru/lib/burning_chrome/
- Gibson, W. (1984), *Neuromancer*, London: Harper Collins.
- Gladwell, M. (2000), *The Tipping Point: How Little Things Can Make a Big Difference*, London: Little Brown.
- Gold, T., D. Guthrie and D. Wank (2002), 'An introduction to the study of guanxi', in T. Gold, D. Guthrie and D. Wank (eds), *Social Connections in China: Institutions, Culture, and the Changing Nature of Guanxi*, Cambridge: Cambridge University Press, pp. 1–13.
- Goldsmith, J. T. and T. Wu (2006), *Who Controls the Internet? Illusion of a Borderless World*, Oxford: Oxford University Press.
- Gordon, S. and R. Ford (2006), 'On the definition and classification of cybercrime', *Journal in Computer Virology*, **2**(1), 13–20.
- Government Information Office (2009), *The Republic of China Year Book 2009*, Taipei: Government Information Office.
- Grabosky, P. (1995), 'Regulation by reward: On the use of incentives as regulatory instruments', *Law and Policy*, **17**(3), 257–282.
- Grabosky, P. (2007), *Electronic Crime*, Upper Saddle River, NJ: Pearson.
- Grabosky, P., R. Smith and G. Dempsey (2001), *Electronic Theft: Unlawful Acquisition in Cyberspace*, Cambridge: Cambridge University Press.
- Greene, T. (2010, 18 January), 'FAQ: The Kneber botnet revealed', *Networkworld*, retrieved 21 January 2010, from <http://www.networkworld.com/news/2010/021810-kneber-botnet-faq.html>
- Gunningham, N. and P. Grabosky (1998), *Smart Regulation: Designing Environmental Policy*, Oxford: Oxford University Press.
- Hannan, M. T. and J. Freeman (1977), 'The population ecology of organizations', *The American Journal of Sociology*, **82**(5), 929–964.
- Hayes, P. (2005, 11 May), 'No "sorry" from Love Bug author', *The Register*, retrieved 8 February 2010, from http://www.theregister.co.uk/2005/05/11/love_bug_author/
- Henderson, S. (2008) 'Beijing's rising hacker stars ... How does mother China react?', *IO Sphere*, Fall, 25–30.

- Higgins, K. J. (2009a, 20 August), 'Botmaster: It's all about infecting, selling big batches of bots', *InformationWeek*, retrieved 24 August 2009, from <http://www.darkreading.com/security/client/showArticle.jhtml?articleID=219400902&cid=RSSfeed>
- Higgins, K. J. (2009b, 14 January), 'Storm botnet makes a comeback: Researchers confirm "Waledac" is the work of new and improved Storm', *InformationWeek*, retrieved 24 Aug 2009, from <http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=212900543>
- Hirsch, P. (1997), 'Sociology without social structure: Neoinstitutional theory meets brave new world', *American Journal of Sociology*, **102**, 1702–1723.
- Hoffman, A. J. (1999), 'Institutional evolution and change: Environmentalism and the U.S Chemical Industry', *The Academy of Management Journal*, **42**(4), 351–371.
- Hsieh, L. K. (2003), *Money-Laundry in Taiwan and China – Legal Responses and Mutual Assistance*, Tao-Yuan: Central Police University Press.
- Huang, D. S. (2007, 25 August 2007), 'An engineer sells hacking program', *Libertytimes*, retrieved 18 September 2010, from <http://www.libertytimes.com.tw/2007/new/aug/25/today-life6.htm>
- Huang, J. L. (2007, 11 January), 'False reports hurt farmers', *Liberty Times*, retrieved 2 January 2009, from <http://www.libertytimes.com.tw/2007/new/jan/11/today-life12.htm>
- Huang, K. (1987), 'Face and favor: The Chinese power game', *American Journal of Sociology*, **92**(4), 944–974.
- Huaxia (2007, 23 August), 'The Kinmen Agreement is becoming an important foundation for sending back the stowaway', *Huaxia*, retrieved 15 January 2010, from <http://hk.huaxia.com/thpl/wzzdlj/2007/08/34796.html>
- IBM (2009), *IBM Internet Security Systems X- Force 2009 Mid-Year Trend and Risk Report*, Somers, NY: IBM Corporate.
- Ilett, D. (2004, 27 October), 'Betting websites blackmailed with child pornography', *Silicon.com*, retrieved 13 July 2009, from <http://software.silicon.com/malware/0,3800003100,39125346,00.htm>
- Information Warfare Monitor (2009), *Tracking GhostNet: Investigating a Cyber Espionage Network*, Canada: Information Warfare Monitor.
- ITU (2009), *ITU Toolkit for Cybercrime Legislation*, Geneva: International Telecommunication Union.
- Jacobs, J. B. (1979), 'A preliminary model of particularistic tie in Chinese political alliance: Kan-ch'ing and kuan-hsi in a rural Taiwanese township', *The China Quarterly*, **78**, 237–273.

- Jayaraman, G. C., J. K. Preiksaitis and B. Larke (2003), 'Mandatory reporting of HIV infection and opt-out prenatal screening for HIV infection: effect on testing rates', *Canadian Medical Association Journal*, **168**(6), 679–682.
- Jeffery, C. R. (1993), 'Obstacles to the development of research in crime and delinquency', *Journal of Research in Crime and Delinquency*, **30**(4), 491–497.
- Jen, M. H. (2009, 26 April), 'Mutual assistance between Taiwan and China. C.I.B.: Institutionalised the collaboration of combating crime', *Central News Agency*, retrieved 18 January 2010, from http://www.rti.com.tw/big5/topic/2009/0426/news_090426-07.aspx
- Jewkes, Y. (2003), *Dot.cons: Crime, Deviance and Identity on the Internet*. Cullompton, Devon: Willan Publishing.
- Jiang, J. Y. (2009, 31 March), 'Issues of Hacking and Extradition will all be included in the Jiang-Chen Meeting', *Haixiainfo*, retrieved 17 January 2010, from <http://www.haixiainfo.com.tw/44565.html>
- Jou, S. (2008), 'Book Review: Richard Ericson's Crime in an Insecure World', *Taiwanese Journal of Sociology*, **40**, 141–149.
- Kaplan, J. A. (2010, 18 January), 'Google hack leaked to Internet; security experts urge vigilance', *FOXNews*, retrieved 18 January 2010, from <http://www.foxnews.com/scitech/2010/01/18/google-exploit-leaked-internet-security-experts-urge-vigilance/>
- Katyal, N. K. (2003), 'Digital architecture as crime control', *Yale Law Journal*, **112**(8), 2261–2289.
- Ke, Y. C. (2008), *Suggestions on the Amendments of Criminal Law Relating to Combating Cybercrime*, Taipei: Ministry of Justice.
- King, A. Y.-C. (1991), 'Kuan-hsi and network building: A sociological interpretation', *Daedalus*, **120**(2), 63–84.
- Klayman, A. (2009, 31 March), 'China denies any role in "GhostNet" computer hacking', *VOANews.com*, retrieved 20 August 2009, from <http://www1.voanews.com/english/news/a-13-2009-03-31-voa12-68812997.html>
- Konowitz, P. M., G. A. Petrossian and D. N. Rose (1984), 'The under-reporting of disease and physicians' knowledge of reporting requirements', *Public Health Report*, **99**, 91–35.
- Koppell, J. G. S. (2000), 'No "There" there: Why cyberspace isn't', *The Atlantic Monthly*, **286**, 16–18.
- Krebs, B. (2006, 21 March), 'Bringing botnets out of the shadows: Online volunteers monitor illegal computer networks', *The Washington Post*, retrieved 22 August 2009, from <http://www.washingtonpost.com/wp-dyn/content/article/2006/03/21/AR2006032100279.html>

- Krekel, B. (2009), *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, McLean, VA: Northrop Grumman Corporation.
- Lan, S. L. (2006, 13 April), 'New attacking methods – DNS recursive', *lslnet.com*, retrieved 10 May 2009, from <http://www.lslnet.com/linux/ff/docs/linux-4795.htm>
- Landler, M. and J. Markoff (2007, 29 May), 'Digital fears emerge after data siege in Estonia', *New York Times*, retrieved 15 February 2008, from <http://www.nytimes.com/2007/05/29/technology/29estonia.html>
- Larson, M. S. (1977), *The Rise of Professionalism: A Sociological Analysis*, Berkeley, CA: University of California Press.
- Lee, H. F. and J. H. Wu (2009, 29 December), 'Judicial mutual assistance safeguards the rights and interests of citizens in both sides', *Xinhuanet*, retrieved 22 January 2010, from http://news.xinhuanet.com/tw/2009-12/30/content_12728447.htm
- Lee, J. (2009, 22 May), 'China is suffering serious cyber attack', *Xinhuanet*, retrieved 10 June 2009, from http://news.xinhuanet.com/zgjx/2009-05/22/content_11416880.htm
- Lee, M. S. and L. J. Feng (2007, 13 December), 'Hackers attack KMT's websites', *UDN*, retrieved 23 April 2008, from <http://www.itis.tw/node/1323>
- Lee, P. I. and T. R. Weitzel (2005), 'Air carrier safety and culture: An investigation of Taiwan's adaption to western incident reporting programs', *Journal of Air Transportation*, **10**(1), 20–37.
- Legislative Yuan (1997), 'Partial amendment on the Criminal Law', *Gazette of the Legislative Yuan*, **86**(31), 298–305.
- Legislative Yuan (1999), 'Partial amendment of the Criminal Law', *Gazette of the Legislative Yuan*, **88**(13), 77–219.
- Legislative Yuan (2003), 'Offences relating to the abuse of computers', *Gazette of the Legislative Yuan*, **92**(29), 137–152.
- Lemos, R. (2000, 5 May), 'In less than six hours Thursday, Love spread worldwide', *ZDNet*, retrieved 8 February 2010, from http://news.zdnet.com/2100-9595_22-107344.html
- Lessig, L. (1999), *Code and Other Laws of Cyberspace*, New York: Basic Books.
- Liang, B. and H. Lu, H. (2006), 'Conducting fieldwork in China: observations on collecting primary data regarding crime, law, and criminal justice system', *Journal of Contemporary Criminal Justice*, **22**(2), 157–172.
- Liao, Y. (2001), 'Analysis of computer crime characteristics', *Journal of Information, Technology and Society*, **1**, 119–133.
- Liao, Y. and C. Tsai (2006), 'Analysis of computer crime characteristics in Taiwan', in H. Chen, F.-Y. Wang, C. C. Yang, D. Zeng, M. Chau and K.

- Chang (eds), *Intelligence and Security Informatics: International Workshop, WISI 2006, Singapore, April 9, 2006*. Proceedings, Heidelberg: Springer, pp. 49–57.
- Libbenga, J. (2008, 1 September), 'Neo-Nazi forum hacked', *The Register*, retrieved 10 April 2010, from http://www.theregister.co.uk/2008/09/01/neo_nazi_forum_hacked/
- Liu, P.W., J. C. Wu and P. C. Liu (2008), *TWNCERT Social Engineering Drill: The Best Practice to Protect against Social Engineering Attacks in E-mail Form*, Taipei: TWNCERT.
- Liu, S. F., C. Fang, H. J. Yeh, S. S. Fang, C. Wang, L. H. Shen et al. (2006). *Study on the Cyber Criminal Law under the Technology*, Beijing: Beijing University Press.
- Lombardi, C. (2006, 9 June), 'Spam: made in Taiwan?', *CNET*, retrieved 31 August 2009, from http://news.cnet.com/2100-7349_3-6082377.html
- Lucas, J. R. (1973), *A Treatise on Time and Space*, London: Methuen.
- Lui, J. P. (2006, 12 June), 'Money or hacking', *Xinhuanews*, retrieved 10 May 2008, from http://big5.xinhuanet.com/gate/big5/news.xinhuanet.com/politics/2006-06/12/content_4685002.htm
- Makkai, T. and J. Braithwaite (1983), 'Praise, pride and corporate compliance', *International Journal of the Sociology of Law*, **21**, 73–91.
- Markoff, J. (2010, 18 February), 'Malicious software infects computers', *New York Times*, retrieved 19 February 2010, from <http://www.nytimes.com/2010/02/19/technology/19cyber.html?emc=eta1>
- Martin, K. (2006, 24 June), 'Viruses, phishing, and Trojans for profit', *SecurityFocus*, retrieved 10 July 2009, from <http://www.securityfocus.com/columnists/419>
- Mason, J. (2002), *Qualitative Researching* (2nd edn), Thousand Oaks, CA: Sage.
- Masters, G. (2010, 23 April), 'Global cybercrime treaty rejected', *SC Magazine*, retrieved 21 September 2010, from <http://www.scmagazine.com/global-cybercrime-treaty-rejected-at-un/article/168630/>
- Mazanec, B. M. (2009), 'The art of (cyber) war', retrieved 18 September, 2010, from <http://www.securityaffairs.org/issues/2009/16/index16.php>
- McGuire, M. (2007), *Hypercrime: the New Geometry of Harm*, Abingdon, Oxon: Routledge-Cavendish.
- Meier, R. F. and T. D. Miethe (1993), 'Understanding theories of criminal victimization', *Crime and Justice*, **17**, 459–499.
- MessageLabs (2008), *MessageLabs Intelligence: Q1/March 2008*, NY: MessageLabs.
- Ministry of Justice (2000), *Ministry of Justice Bulletin*, retrieved 12 December, 2009, from <http://gaz.ncl.edu.tw/detail.jsp?sysid=E0006245>

- Morse, J. M. (1995), 'The significance of saturation', *Qualitative Health Research*, **5**, 147–149.
- Myers, S. L. (2007, 19 May), 'Estonia computers blitzed, possibly by the Russians', *New York Times*, retrieved 15 February 2008, from <http://www.nytimes.com/2007/05/19/world/europe/19russia.html>
- National Infrastructure Advisory Council (2003), *The National Strategy to Secure Cyberspace*, Washington, DC: White House.
- National Transportation Safety Board (1974), *Aircraft Incident Report*, Washington, DC: National Transportation Safety Board.
- Newman, G. R. and R. V. Clarke (2003), *Superhighway Robbery: Preventing E-commerce Crime*, Portland, Oregon: Willan Publishing.
- O'Brien, D. (2006), *The World's Worst Internet Laws Sneaking Through the Senate*, retrieved 6 July, 2009, from <http://www.eff.org/deeplinks/2006/08/worlds-worst-internet-laws-sneaking-through-senate>
- O'Malley, P. (1992), 'Risk, power and crime prevention', *Economy and Society*, **21**(3), 252–275.
- O'Malley, P. and S. Hutchinson (2007), 'Reinventing prevention: why did "crime prevention" develop so late?', *British Journal of Criminology*, **47**, 373–389.
- Odendahl, T. and A. Shaw (2001), 'Interview elites', in J. Gubrium and J. Holstein (eds), *Handbook of Interview Research: Context and Method*, London: Sage, pp. 299–310.
- OECD (1986), *Computer-related Crime: Analysis of Legal Policy*, Paris: OECD.
- Olesen, A. (2007, 14 October), 'China tightens Internet controls: Content under scrutiny in run-up to sensitive Communist Party Congress', *Associated Press*, retrieved 23 March 2009, from <http://www.msnbc.msn.com/id/21268635>
- Osen, M. (2009, 14 August), 'IH 2009: Malware threat grows ever larger', *TrendLabs Malware Blog*, retrieved 31 August 2009, from <http://blog.trendmicro.com/wp-content/uploads/2009/08/2009-08-07-blog1.jpg>
- Pan, W. T., Y. Y. Chen, C. S. Yeh, S. C. Fa and Y. A. Hsu (2008), *An Analysis on the Collection and Preservation Procedure of Digital Evidence*, Taipei: Ministry of Justice.
- Parker, C. (2002), *The Open Corporation: Effective Self-Regulation and Democracy*, Cambridge: Cambridge University Press.
- Pi, Y. (2005), 'On the measures of ordering to offer electronic evidence in criminal investigation', *Journal of Shangdong Police College*, **80**, 53–58.
- Pi, Y. (2008), *Research on Cyber-Security law*, Beijing: Chinese People's Public Security University.
- Pi, Y. (2009a), *Comparative Research on Convention on Cybercrime and Chinese Relevant Legislation*, Paris: Council of Europe.

- Pi, Y. (2009b), 'On Cybercrime legislation in China – And on Cybercrime legislation in amendment 7th of China Penal Code', *Hebei Law Science*, **27**(6), 49–57.
- Pi, Y. (2009c), 'On the legislation of Cybercrime in amendment VII to the Criminal Law of the People's Republic of China', *Journal of Shangdong Police College*, **104**, 15–20.
- Rajab, M. A., J. Zarfoss, F. Monrose and A. Terzis (2007), *My botnet is bigger than yours (maybe, better than yours)*, Paper presented at the HotBots 2007, retrieved 24 August 2009, from https://www.usenix.org/events/leet08/tech/full_papers/zhuang/zhuang.pdf
- Raywood, D. (2009), 'North Korea blamed for DDoS attacks on United States and South Korea', retrieved 18 September, 2010, from <http://www.scmagazineuk.com/north-korea-blamed-for-ddos-attacks-on-united-states-and-south-korea/article/139764/>
- Rees, J. V. (1988), *Reforming the Workplace: A Study of Self-regulation in Occupational Health and Safety*, Philadelphia: University of Pennsylvania Press.
- Register, T. (2007), 'France blames China for hack attacks', retrieved 26, Sept, 2007, from http://www.theregister.co.uk/2007/09/12/french_cyberattacks/
- Reidenberg, J. R. (2004), 'State and Internet enforcement', *University of Ottawa Law and Technology Journal*, **1**, 213–230.
- Richardson, M. (2010), *Taiwan-based Aurora cyber attack part of larger hack than previously reported*, retrieved 20 September, 2010, from <http://www.examiner.com/taiwan-policy-in-national/taiwan-based-aurora-cyber-attack-part-of-larger-hack-than-previously-reported>
- Rigakos, G. (1999), 'Risk society and actuarial criminology: Perspective for a critical disclosure', *Canadian Journal of Criminology*, **41**(2), 137–150.
- Robel, D. (2006), *International Cybercrime Treaty: Looking Beyond Ratification*, Maryland: The SANS Institute.
- Rothenberg, R., D. C. Bross and T. M. Vernon (1980), 'Reporting of gonorrhoea by private physicians: A behaviour study' *American Journal of Public Health*, **70**, 983–986.
- RTI (2010, 18 January), 'New computer virus will create a backdoor', *SinaNews*, retrieved 8 February 2010, from <http://news.sina.com.tw/article/20100118/2696582.html>
- Rubin, H. J. and I. S. Rubin (2005), *Qualitative Interviewing: The Art of Hearing Data* (2nd edn), Thousand Oaks, CA: Sage.
- Sandoval, G. (2001, 31 May), 'Virus poses as nude Jennifer Lopez photos', *CNET*, retrieved 10 March 2010, from <http://news.cnet.com/2100-1001-267644.html>

- Schjolberg, S. and S. Ghernaoui-Helie (2011), *A Global Treaty on Cyber-security and Cybercrime* (Second edition), available from http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime_Second_edition_2011.pdf
- Schneier, B. (2008), *The Truth About Chinese Hackers*, retrieved 18 September, 2010, from <http://dsc.discovery.com/technology/my-take/computer-hackers-china.html>
- Schramm, M., R. L. Vogt and M. Mamolen (1991), 'The surveillance of communicable disease in Vermont: who reports?', *Public Health Report*, **106**, 95–97.
- Scott, W. R. (2008), *Institutions and Organizations: Ideas and Interests* (3rd edn), London: Sage.
- Shau, J. M., B. H. Yu, R. Huang, L. J. Wong, H. J. Jheng, S. P. Jou et al. (2005), *The Evolution of Crime*, Beijing: Peking University Press.
- Shi, W.B. (2009, 20 April), 'Taipei becomes the headquarters of bots in the Asia and Pacific Region', *IThome Online*, retrieved 25 August 2009, from <http://www.ithome.com.tw/itadm/article.php?c=54571>
- Shih, H. (2007), *GIO prohibits work from home after hacker attack*, retrieved 23 Sept, 2007, from <http://www.taipeitimes.com/News/taiwan/archives/2007/05/26/2003362509>
- SinaNews (2009, 10 February), '38,936 persons have been repatriated under the Kinmen Agreement', *SinaNews*, retrieved 18 January 2010, from <http://news.sina.com/c/2009-02-11/111617192947.shtml>
- Sklar, L. (1977), *Space, Time, and Spacetime*, Berkeley, CA: University of California Press.
- Smart, A. (1993), 'Gift, bribes, and guanxi: A reconsideration of Bourdieu's social capital', *Cultural Anthropology*, **8**(3), 388–408.
- Smith, R., P. Grabosky and G. Urbas (2004), *Cyber Criminals on Trial*, Cambridge: Cambridge University Press.
- Steele, J. (2004), *Risks and Legal Theory*, Oxford: Hart Publishing.
- Sterling, B. (1994), *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, London: Penguin.
- Stone-Gross, B., C. Marco, L. Cavallaro, B. Gilbert, M. Szydlowski, R. Kemmerer, C. Kruegel et al. (2009), *Your botnet is my botnet: Analysis of a botnet takeover*, Paper presented at the 16th ACM Conference on Computer and Communications Security, retrieved 30 August 2009, from <http://www.cs.ucsb.edu/~seclab/projects/torpig/torpig.pdf>
- Storey, R. O. (2009, 23 September), 'Asia enterprises more vulnerable to cybercrime', *Network World*, retrieved 24 September 2009, from <http://www.networkworld.com/news/2009/092309-asia-enterprises-more-vulnerable-to.html>

- Su, J. Y. (2008, 9 December), 'Golden Shield Project – Everyone in China is under the surveillance', *Liberty Times*, retrieved 15 March 2009, from <http://www.libertytimes.com.tw/2008/new/dec/9/today-fo5.htm>
- Sun, C. Y. and S. S. Jia (eds) (2007), *Jiasuanji Yu Wangluo Fanzui Zhuanti Zhengli [Topics on Information Security and Cybercrime]*, Beijing: Chinese People's Public Security University.
- Symantec (2006), *Symantec Internet Security Threat Report X: Trend for January–June 2006*, Cupertino, CA: Symantec Corporation.
- Symantec (2007a), *Symantec APJ Internet Security Threat Report XI: Trend for July–December 2006*, Cupertino, CA: Symantec Corporation.
- Symantec (2007b), *Symantec APJ Internet Security Threat Report XII: Trend for January–June 2007*, Cupertino, CA: Symantec Corporation.
- Symantec (2007c), *Symantec Internet Security Threat Report XI: Trend for July–December 2006*, Cupertino, CA: Symantec Corporation.
- Symantec (2007d), *Symantec Internet Security Threat Report XII: Trend for January–June 2007*, Cupertino, CA: Symantec Corporation.
- Symantec (2008a), *Symantec APJ Internet Security Threat Report XIII: Trend for July–December 2007*, Cupertino, CA: Symantec Corporation.
- Symantec (2008b), *Symantec Internet Security Threat Report XIII: Trend for July–December 2007*, Cupertino, CA: Symantec Corporation.
- Symantec (2009a), *State of Phishing – A monthly report #22 (Aug 2009)*, Cupertino, CA: Symantec Corporate.
- Symantec (2009b), *Symantec APJ Internet Security Threat Report XIII: Trend for 2008*, Cupertino, CA: Symantec Corporation.
- Tapscott, D. and A. D. Williams (2007), *Wikinomics: How Mass Collaboration Changes Everything*, London: Atlantic Books.
- Taylor, G. (2001), *The Council of Europe Cybercrime Convention: A Civil Liberties Perspective*, Adelaide: Electronic Frontiers Australia.
- Taylor, P. A. (2005), 'From hackers to hacktivists: Speed bumps on the global superhighway', *New Media Society*, 7(5), 625–646.
- Thibodeau, P. (2010, 24 March), 'Cyberattacks are "existential threat" to U.S., FBI says', *Computerworld*, retrieved 25 March 2010 from http://www.networkworld.com/news/2010/032410-cyberattacks-are-existential-threat-to.html?source=NWWNLE_nlt_compliance_2010-03-26
- Thomas, V. and N. Jyoti (2007), 'Bot Countermeasures', *Journal in Computer Virology*, 3(1), 103–111.
- Thornburgh, N. (2005), 'The invasion of the Chinese cyberspies', retrieved 15 March, 2010, from <http://www.time.com/time/magazine/article/0,9171,1098961,00.html>
- Tong, W. S. (2009, 3 May), 'An analysis on the judicial agreement between Taiwan and China', *EpochTimes*, retrieved 21 January 2010, from <http://www.dajiyuan.com/b5/9/5/3/n2514809.htm>

- Toth, B. (2007), *Estonia under Cyber Attack*, Budapest: Hun-CERT.
- Toy, M.-A. (2009, 26 July 2009), 'Chinese hack into film festival site', *The Age*, retrieved 18 September 2010, from <http://www.theage.com.au/national/chinese-hack-into-film-festival-site-20090725-dwvx.html>
- Traynor, I. (2007, 17 May), 'Russia accused of unleashing cyberwar to disable Estonia', *Guardian*, retrieved 23 September 2009, from <http://www.guardian.co.uk/russia/article/0,,2081438,00.html>
- Trend Micro (2009), *Trend Micro 2008 Annual Threat Roundup and 2009 Forecast*, Cupertino, CA: Trend Micro Inc.
- Trepka, M. J., G. Zhang and F. Leguen (2009), 'An intervention to improve notifiable disease reporting using ambulatory clinics', *Epidemiology and Infection*, **137**, 22–29.
- United Nations (1990a), *Resolution Adopted by the General Assembly on the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (A/RES/45/121)*, retrieved 25 September 2009, from <http://www.un.org/documents/ga/res/45/a45r121.htm>.
- United Nations (1990b), *Resolution Adopted by the General Assembly on the Model Treaty on Mutual Assistance in Criminal Matters (A/RES/45/117)*, retrieved 25 September 2009. from <http://www.un.org/documents/ga/res/45/a45r117.htm>.
- United Nations (2001), *Resolution Adopted by the General Assembly on Combating the Criminal Misuse of Information Technologies (A/RES/55/63)*, retrieved 23 September 2007, from http://www.unodc.org/pdf/crime/a_res_56/121e.pdf.
- United Nations (2002), *Resolution Adopted by the General Assembly on Combating the Criminal Misuse of Information Technologies (A/RES/56/121)*, retrieved 25 September 2009 from <http://daccessdds.un.org/doc/UNDOC/GEN/N01/482/04/PDF/N0148204.pdf?OpenElement>.
- United Nations (2003), *Resolution Adopted by the General Assembly on Creation of a Global Culture of Cybersecurity (A/RES/57/239)*, retrieved 25 September 2009 from http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_57_239.pdf.
- United Nations (2004a), *Resolution Adopted by the General Assembly on Creation of a global culture of cybersecurity and the protection of critical information infrastructure (A/RES/58/199)*, retrieved 25 September 2009 from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf
- United Nations (2004b), *United Nations Convention against Transnational Organised Crime and the Protocols Thereto*, New York: United Nations.
- Wakefield, J. (2005), 'Online service foils ransom plot', *BBC News Online*, retrieved 6 April 2009, from <http://news.bbc.co.uk/1/hi/technology/4579623.stm>

- Walder, A. G. (1983), 'Organized dependency and cultures of authority in Chinese industry', *Journal of Asian Studies*, **63**(1), 51–75.
- Walkley, S. (2005), *Regulating Cyberspace: An Approach to Studying Criminal Behaviour on the Internet*, Unpublished PhD thesis, The Australian National University, Canberra.
- Wall, D. S. (2005), 'The Internet as a conduit for criminal activity' in A. Pattavian (ed.), *Information Technology and the Criminal Justice System*, Thousand Oaks, CA: Sage, pp. 77–98.
- Wall, D. S. (2007), *Cybercrime*, Cambridge: Polity Press.
- Wall, D. S. (2008), 'Cybercrime, Media and Insecurity: the shaping of public perceptions of cybercrime', *International Review of Law, Computers and Technology*, **22**, 45–63.
- Wall, D. S. (2008/2010), 'Cybercrime and the culture of fear: Social science fiction(s) and the production of knowledge about Cybercrime' (revised May 2010), *Information, Communication & Society*, **11**(6), 861–884.
- Wang, P., S. Sparks and C. C. Zou (2007), *An advanced hybrid peer-to-peer botnet*, Paper presented at the First Workshop on Hot Topics in Understanding Botnets, retrieved 20 July 2009, from http://www.usenix.org/event/hotbots07/tech/full_papers/wang/wang.pdf
- Wang, P. L. (2007, 12 December), 'PayEasy were hacked with a leaking of 5,400 personal information', *Liberty Times*, retrieved 3 March 2010, from <http://www.itis.tw/node/1313>
- Wang, S. R. (2007, 14 February), 'The Panda with burning incense: profit-oriented virus', *China's First Financial Daily*, retrieved 20 March 2009, from http://hacker.cn/News/aqwh/2007-2/14/0721409031215205_2.shtml
- Westervelt, R. (2009), *DDoS attacks hit U.S., South Korean government websites*, retrieved 18 September, 2010, from http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1361258,00.html
- Wilson, C. (2008), *Botnet, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, Washington, DC: The Federation of American Scientists.
- Wilson, J. Q. and G. L. Kelling (1982), 'Broken Windows', *The Atlantic Monthly*, **249**, 29–38.
- Wines, M. (2011, 10 June), 'Nearly 600 arrested in Asian Swindling Ring', *New York Times*, retrieved 26 September 2011, from <http://www.nytimes.com/2011/06/11/world/asia/11taiwan.html>
- Wolfgang, M. E. (1975), *Patterns in Criminal Homicide*, Montclair, NJ: Patterson Smith.
- World Health Organization (2005), *Avian influenza frequently asked questions*, retrieved 4 February, 2010, from http://www.who.int/csr/disease/avian_influenza/avian_faqs/en/

- Xinhua (2009, 26 April), 'Mainland's Taiwan affairs chief says economic co-op priority for cross-straits relations', *Xinhuanews*, retrieved 19 January 2010, from http://www.gwytb.gov.cn:8088/detail.asp?table=headlines&title=Headlines&offset=75&m_id=1001
- Xu, S. C. (2009, 24 March), 'Over 3,100 cyber attacks towards Taiwanese Government System were originated by Chinese cyber army', *Liberty Times*, retrieved 21 September 2010, from <http://www.libertytimes.com.tw/2009/new/mar/24/today-fo2.htm>
- Yang, M. M. (1988), 'The modernity of power in the Chinese socialist order', *Cultural Anthropology*, 3(4), 408–427.
- Yang, Y. Z. (2008, 30 April), 'Online gaming companies suffer DDoS attacks from Chinese hackers', *UDN*, retrieved 25 August 2009, from http://mag.udn.com/mag/digital/storypage.jsp?f_MAIN_ID=319&f_SUB_ID=2941&f_ART_ID=123192
- Yar, M. (2005), 'The novelty of "Cybercrime": An assessment in light of routine activity theory', *European Journal of Criminology*, 2(4), 407–427.
- Yau, Y. S. (2006, 5 September), 'Specific modelling model found which is targeting Taiwan only', *IThome Online*, retrieved 27 August 2009, from <http://www.ithome.com.tw/itadm/article.php?c=39235>
- Zetter, K. (2010, 14 January), 'Google hack attack was ultra sophisticated, new details show', *Wired News*, retrieved 18 January 2010, from <http://www.wired.com/threatlevel/2010/01/operation-aurora>
- Zhang, H. Y. (2007, 1 November), 'Taiwanese net-armies are targeting China', *People*, from <http://tw.people.com.cn/BIG5/88649/6468348.html>
- Zucker, L. G. (1983), 'Organisation as institutions', in S. B. Bacharach (ed.), *Research in the Sociology of Organizations* (Vol. 2), Greenwich, CT: JAI Press.

