Cyber Crime, Insecurity and the Dark Web

CRIM6002 (MSc. Criminology)

CRIM6008 (MSc. Cyber Security)

Semester 2 2017

Co-ordinator Dr Craig Webber



Cyber Crime, Insecurity and the Dark Web Semester 2, 2017

***Unit Handbook: A guide to course organization, readings, seminars and lecture programme***

**Credit points**:

CRIM6002 (CRIMINOLOGY) = CATS 20

CRIM6008 (CYBER SECURITY) = CATS 15

**Student class time**: 90 minutes a week

***This*** **UNIT** **HANDBOOK** ***is a basic reference source for all aspects of this unit, so please have it with you for all lectures and classes. Details of essay titles are included and please pay special attention to the details of the seminar programme.***

Welcome to Cyber Crime.

This module is designed to introduce you to the human dimension of cybercrime and cyber security. It is not coming from a technical perspective, but instead a critical criminological approach is applied to the topic. This means that we will be questioning theory, policy and practice, and discuss the way that this area might develop in the future. This module is a ‘transdisciplinary’ approach to a very contemporary human development. As such, we are all still pioneers making our way through the subject. We will traverse a wide range of literature, ideas and research drawn from a dizzying array of subject areas, and their interactions. A bold claim might be that we are at the end of subject insularity and only a transdisciplinary approach provides the robust analytical tools that we need to understand issues like the Web and Cybercrime.

**PLEASE NOTE: THERE ARE TWO CODES FOR THIS MODULE AND THE TWO CODES DENOTE SLIGHTLY DIFFERENT CREDIT POINTS. THIS DIFFERENCE IS DUE TO THE MODULE BEING TAUGHT ACROSS TWO DEGREES HOSTED IN TWO FACULTIES. IT IS IMPORTANT FOR THE PURPOSES OF THE ASSESSMENT ONLY. PLEASE MAKE SURE YOU FOLLOW THE WORD COUNT FOR YOUR MODULE CODE.**

**Laptops and Tablets**

We strongly advise you to bring a Laptop or Tablet that has network access, to workshops. We will sometimes ask you to conduct web searches or visit web sites in the workshop.

**Contact details**

The teaching team are free to see students during our ‘office and feedback hours’ (notification of times outside our offices) and outside of these hours by prior appointment. Contact information:

Craig Webber Room 58/4065; email: [c.webber@soton.ac.uk](mailto:c.webber@soton.ac.uk)

Anita Lavorgna Room 58/4067; email: [a.lavorgna@soton.ac.uk](mailto:a.lavorgna@soton.ac.uk)

We hope you enjoy the module and profit from it and we look forward to getting to know you this semester.

***Dr Craig Webber, Module Coordinator***

**Aims and learning outcomes**

**The following are, as ever, important. These aims and objectives form the basis of our assessment of your progress.**

Aims

* To critically evaluate cutting edge research in the area of Cyber Crime and Cyber Security
* To introduce the history of research into Cyber Crime
* To understand the organisations and key stake holders in the business of preventing, controlling and policing Cyber Crime.
* To critically evaluate the theoretical foundation of research into Cyber Crime
* To develop an approach to Cyber Crime and Cyber Security that recognises the interdisciplinary nature of the area

Continuing Academic Support  
  
If you find yourself experiencing any study skills difficulties with your work please consult the following resources and then contact your personal academic tutor to discuss any issues:  
  
For face to face help you should contact the Academic Skills Hub, level 2 in the Hartley Library, just past the IT Help desk: Monday - Friday: 10am - 12 noon, 2pm - 4pm, Lunchtime drop-in and signup sessions as advertised.  
[http://library.soton.ac.uk/sash](https://www.outlook.soton.ac.uk/owa/redir.aspx?C=UVywRh_KegBI6ZknE3kq4ikezWJRuzniQVmgGqZXVvP7EBVp9uLTCA..&URL=http%3a%2f%2flibrary.soton.ac.uk%2fsash)

[http://www.southampton.ac.uk/edusupport/study\_support/index.page?](https://www.outlook.soton.ac.uk/owa/redir.aspx?C=M05ViCORfxXS7Wue9SJ9KP11AlGdXvN-DNPqXhOrM4eEHWo09eLTCA..&URL=http%3a%2f%2fwww.southampton.ac.uk%2fedusupport%2fstudy_support%2findex.page%3f)  
  
If you experience any more specific difficulties with the content of the module, please contact your module convenor or seminar tutor.

**Programme Outline:**

**Week**

|  |  |  |
| --- | --- | --- |
| **Week/Week Beginning** | **Lecture** | **Assessment** |
| **1**  **30/01/17** | **Cyber: A History of a Prefix (CW)** |  |
| **2**  **06/02/17** | **Bitcoins and the political economy of crime (CW)** |  |
| **3**  **13/02/17** | **Surveillance and the Web: Research and Investigation online (AL)** |  |
| **4**  **20/02/17** | **Hacking, Spoofing and Cracking (AL)** |  |
| **5**  **27/02/17** | **Cyber Piracy (AL)** |  |
| **6**  **06/03/17** | **Cyber Crime grows up: Carding, Escrow and the Dark Markets (AL)** |  |
| **7**  **13/03/17** | **Everyday Cybercrimes: from trolling and hate crime, violent pornography, online grooming, to the purchasing of pharmaceuticals (AL)** | **Group Presentation on Current Concerns and Future Risks from Cyber Crime** |
| **8**  **20/03/17** | **From Cyber Crime to Cyborg: The Bio-Intuitive Web (CW)** | **Essay Due: Elaboration of the Presentation**  **Thursday 16th March** |
| **9**  **27/03/17** | **Hacktivism: Political Protests on the web or Threat to National Security (CW)**  **Guest Lecture from Neil MacEwan** |  |
|  | **Easter Break** |  |
| **10**  **24/04/17** | **Policing and punishing cybercrime (CW)** |  |
| **11**  **01/05/17** | **No workshops. You are expected to work on your essay** |  |
| **12**  **08/05/17** | **No workshops** |  |
|  |  | **Essay Due: WEDNESDAY 17th May: Testing the fears: How likely are the future shock scenarios and what methods will be needed to overcome them?** |

**BLACKBOARD**

**Extensive use is made of this resource. Wherever possible some or all of the material for a specific lecture topic will be on Blackboard prior to the lecture. An effective way of working is to print this up for yourself, bring it to the lecture and add notes. THE BLACKBOARD RESOURCE IS NOT A SUBSTITUTE FOR READING AND NEITHER IS IT A SUBSTITUTE FOR NOTE TAKING IN LECTURES.**

**The Blackboard material for this module consists primarily of ‘Power Point’ presentations and these often include more material than is actually covered in the lecture. As we encourage some discussion in the lecture which will use up time anything not covered in the lecture itself will be on Blackboard. Hence the importance of checking this source regularly. Blackboard material on this unit covers more ground than in the lectures and as part of the lecture you will frequently be asked to explore parts of this in detail including key concluding points and critical commentaries. So Blackboard builds upon and extends the lecture, it is NOT simply a repeat of the lecture. It is *better to understand this key point from the start.***

**Readings:**

The Cybercrime reading list operates as follows:

‘***Essential*** ***readings’*** are to be completed ***PRIOR*** to attending the seminar. It’s a good idea to take notes on these essential readings and, importantly, to identify areas you find difficult. Note these and raise them in seminars.

While we expect each student to have completed the essential readings before the seminar, at this level we also expect students to explore some of the sources listed under ***‘further readings’***. This will certainly be the case when preparing for seminars and researching the essays. At this level we expect students to use journals and you should browse all criminology and sociology journals (set up alerts so that you can track the latest editions). Here is a link to the British Journal of Criminology, there is an Alerting service, you need to sign up for an account and then they will email you when new editions appear. This is essential if you want to raise your marks: <http://bjc.oxfordjournals.org/>

Of course, there are many other journals. We recommend that you spend some time browsing and setting up alerts both within Criminology, and more widely.

**Text Book?**

There are no set texts for this module, but those of you new to criminology or those who would like an overview, you might consider purchasing one, or both, of the following:

Yar, M., 2013. Cybercrime and Society. 2nd Edition. London: Sage.

Wall, D.S., 2007. Cybercrime: The Transformation of Crime in the Information Age. Malden: Polity Press.

**A good general criminology textbook**

Newburn, T. (2012), *Criminology,* London: Routledge

Newburn, T. (2009), *Key Reading in Criminology,* London: Routledge

**Key Readings**

The majority of the readings below are in the library or can be found online. However, in the interests of exposing you to the widest possible literature on this subject, you may find some of the sources are not available without purchasing them or getting an interlibrary loan.

**Week 1: Cyber: A History of a Prefix**

Because this subject is ‘transdisciplinary’, this opening lecture and workshop aims to introduce you to the main issues in the study of cybercrime that later sessions will expand upon. We will introduce you to transdisciplinary working, a practice encouraged and supported by the research councils, such as the ESRC and EPSRC. The research councils financially support University research. Recently, funding has been focused on this form of cooperative research and learning. Web Science and Cyber Security at Southampton are two recent examples of this. We want to expose you to this type of learning as it will increasingly spread from Universities and into the wider workplace. Criminology at Southampton is a key partner in these transdisciplinary endeavours.

Useful Link: Hacker slang

<http://www.outpost9.com/reference/jargon/jargon_toc.html>

Essential Reading

Curran, J. (2010), ‘Reinterpreting Internet History’, in Y. Jewkes and M. Yar (eds.) *Handbook of Internet Crime,* Cullompton, Devon: Willan publishing.

Wall, D. S. (2010), ‘Criminalising cyberspace: the rise of the Internet as a ‘crime problem’, in Y. Jewkes and M. Yar (eds.) *Handbook of Internet Crime,* Cullompton, Devon: Willan publishing.

Further Reading

Ablon, L., Libicki, M.C., and Golay, A.A., (2014). Markets for Cybercrime Tools and Stolen Data: Hacker’s Bazaar [online]. Available from: <http://www.rand.org/pubs/research_reports/RR610.html>.

Berners-Lee, T.J., (1992). The world-wide web. *Computer Networks and ISDN Systems*, 25 (4-5), 454–459.

Gibson, W. (1984), *Neuromancer*

Maguire, M. (2007) *Hypercrime: The New Geometry of Harm* Abingdon, Oxon: Routledge Cavendish

Paget, F., 2010. Cybercrime and Hacktivism [online]. Available from: <http://www.arifyildirim.com/ilt510/francois.paget.pdf>

Poulsen, K., (2011). *Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground*. New York: Crown Publishing.

Sandywell, B., (2010). On the Globalisation of Crime: the Internet and New Criminality. In: Y. Jewkes and M. Yar, eds. *Handbook of Internet Crime*. Devon: Willan Publishing, 38–66.

Taylor, P.A., (1998). Hackers: Cyberpunks or microserfs? *Information, Communication & Society*, 1 (4), 401–419.

Taylor, P.A., (1999). *Hackers*. London: Routledge.

Taylor, P.A., (2001). ‘Hacktivism: in search of lost ethics’. In: D.S. Wall, ed. *Crime and the Internet*. London: Routledge.

Taylor, P.A., (2005). From hackers to hacktivists: speed bumps on the global superhighway? *New Media & Society* , 7 (5 ), 625–646.

Wall, D.S., (2008). Cybercrime and the Culture of Fear: Social science fiction(s) and the production of knowledge about cybercrime. *Information*, *Communication & Society*, 11 (6), 861–884.

Webber, C. & Vass, J., (2010). Crime, film and the cybernetic imagination. In Y. Jewkes & M. Yar, (eds). *Handbook of Internet Crime*. Cullompton: Willan.

Yar, M., (2005). The Novelty of “Cybercrime”: An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, 2 (4), 407–427.

Yar, M., (2013). *Cybercrime and Society*. 2nd Edition. London: Sage.

**Week 2: Bitcoins, cryptocurrencies and the political economy of crime**

Cryptocurrencies use decentralised technology in order to adopt a different approach towards creation, management and implementation of cash systems. Released during the Great Recession, riding on a wave of discontent for existing monetary systems, Bitcoin has introduced a host of unknowns with regards to regulating the movement of money across the world. This week’s session will explore some of the issues presented by cryptocurrency technologies to crime and policing issues on the Web and examine some of the initial ideas and approaches to dealing with decentralised currencies in a world used to centralised financial technologies.

Essential Reading

Ali, R., Barrdear, J., Clews, R., & Southgate, J. (2014). The economics of digital currencies. *Bank of England Quarterly Bulletin*, Q3.

<http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q302.pdf>

Jeong, S. (2011). The Bitcoin Protocol as Law, and the Politics of a Stateless Currency. *NEW YORKER*, *62*, 70.

<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2294124>

EBA Opinion on Virtual Currencies

<http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf>

Further Reading

Christin, N. (2013, May). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. In *Proceedings of the 22nd international conference on World Wide Web* (pp. 213-224). International World Wide Web Conferences Steering Committee.

<http://arxiv.org/abs/1207.7139>

European Central Bank. (2012). *Virtual Currency Schemes*. Frankfurt. Retrieved from http://www.ecb.int/pub/pdf/other/virtualcurrencyschemes201210en.pdf

Filippi, P. De. (2014). Bitcoin: a regulatory nightmare to a libertarian dream. *Internet Policy Review*, *3*(2), 1–11. doi:10.14763/2014.2.286

**Week 3: Surveillance and the Web: Research and Investigation Online**

In contemporary Western societies, most citizens have come to expect that many aspects of their public lives are observed, monitored, classified and controlled to a certain degree. The Web adds yet another dimension to the wealth of surveillance technologies that govern our modern world, further diminishing the boundaries between the public and the private. With investigations conducted by security agencies encroaching on the lives of all citizens, the Web is both the problem and the solution where *cybersurveillance* is concerned. This lecture and workshop will explore how and why surveillance techniques have dramatically expanded over the last two decades, the role that the Web plays in this ‘*Brave New World*,’ as well as the opportunities and challenges afforded to research and investigation online.

Essential Reading

Chapter 8 ‘*Crime and the Surveillance Culture’* in Jewkes, Y. (2011) *Media and Crime.* London: SAGE Publications

Chapter 10 *‘Cybercrimes and Cyberliberties: Surveillance, Privacy and Crime Control*,’ in Yar, M. (2006) *Cybercrime and Society.* London: SAGE

Further Reading

Ball, K. & Webster, F. (2003) ‘*The intensification of surveillance’* in Ball, K. & Webster, F. (eds.) *The intensification of surveillance: crime, terrorism, and warfare in the information age*. Sterling, VA : Pluto Press.

Bauman, Z. & Lyon, D. (2013) Liquid surveillance. A conversation. Polity Press.

Chapter 1 ‘*Surveillance, Crime and Controversy’* in Coleman, R. & McCahill, M. (2010) *Surveillance and Crime.* London: SAGE Publications.

Chapter 5 *‘Globalisation, Surveillance, and the ‘War’ on Terror’* in Coleman, R. & McCahill, M. (2010) *Surveillance and Crime.* London: SAGE Publications.

Chapter 1 *‘Internet and Surveillance’*  in Fuchs, C., Boersma, K., Albrechtslund, A., & Sandoval, M. (Eds.). (2013). *Internet and surveillance: The challenges of Web 2.0 and social media* (Vol. 16). Routledge.

Chapters 6 ‘*Global Data Flows’*, 7 ‘*New Directions in Theory’, 8 ‘The politics of surveillance’, & 9 ‘The future of surveillance’* in Lyon, D. (2001) *Surveillance Society: Monitoring Everyday Life*.

Decary-Hetu, D. & Aldridge, J. (2015) Sifting through the net: monitoring of online offenders by researchers. The European Review of Organised Crime, 2(2), 122-141.

Haggerty, K. D., & Ericson, R. V. (2000). The Surveillant Assemblage. *The British Journal of Sociology*, *51*(4), 605-622.

Haggerty, K. D., Wilson, D. and Smith, G. J. D. (2011), ‘Theorizing surveillance in crime control’, *Theoretical Criminology*, 15 (3), 231-237.

Lyon, D. (1994) The Electronic Eye: The Rise of Surveillance Society. Minneapolis, MN: University of Minnesota Press.

Lyon, D. (2001) Surveillance Society: Monitoring Everyday Life. London: Open University Press (especially chapters 8, 9, & 10).

Lyon, D. (2006) Theorizing Surveillance: The Panopticon and Beyond. Cullompton: Willan.

Miller, V. in Jewkes, Y., & Yar, M. (Eds.). (2013). *Handbook of Internet crime*. Routledge.

Chapter 4 *‘The Internet and Everyday Life’*

Maguire, M. (2010), ‘Online surveillance and personal liberty’, in Y. Jewkes and M. Yar (eds.) *Handbook of Internet Crime,* Cullompton, Devon: Willan publishing.

Sugiura, L., Pope, C., Weal, M. J., & Webber, C. (2012). Observing deviancy online. Available at Eprints: <http://eprints.soton.ac.uk/>

**Week 4: Hacking, Cracking and Social Engineering**

Online offending concerning attacks against the integrity of computer systems involve actions such as hacking, spoofing and cracking. These crimes assault the security of network access mechanisms and may enable more serious types of offending. A great deal of academic research has focused on these cybercrimes, and the media has helped to evoke a cultural perception of the ‘hacker’ that enhances public expectations of fear towards the Web. However, amongst the criminals out to rob and defraud, we have the modern day vigilante in groups such as Anonymous who conduct their own form of justice online. This lecture and workshop will investigate and differentiate between types of hacking, hackers and their motives.

Essential Reading

Chapter 4 *‘Computer Integrity Crime: Hacking, Cracking and Denial of Service’* in Wall, D. (2007). *Cybercrime: The transformation of crime in the information age* (Vol. 4). Polity.

Furnell,S. in Jewkes, Y., & Yar, M. (Eds.). (2013). *Handbook of Internet crime*. Routledge

* Chapter 9 *‘Hackers, Viruses and Malicious Software*,’

Webber, C. (2014). ‘Hackers and Cybercrime’. *Shades of Deviance: A Primer on Crime, Deviance and Social Harm*, 95.

*’*

Further Reading

Holt, T.J. and Bossler, A.M. (2013) ‘Examining the relationship between routine activities and malaware infection indicators’*. Journal of Contemporary Criminal Justice* 20(10), 1-17.

Marcum, C.D., Higgins, G.E., Ricketts, M.L., & Wolfe, S.E. (2014) ‘Hacking in high school: cybercrime perpetration by juveniles’. Deviant Behaviour 35(7), 581-591.

Mitnick, K. D., & Simon, W. L. (2001). *The art of deception: Controlling the human element of security*. John Wiley & Sons.

Wall, D.S. (2008) “Cybercrime and the Culture of Fear: Social Science fiction and the production of knowledge about cybercrime,” Information Communications and Society, vol. 11, no. 6, pp 861-884

Yar, M. (2005). Computer hacking: Just another case of juvenile delinquency? *The Howard Journal of Criminal Justice*, *44*(4), 387-399.

Yar, M. (2006) *Cybercrime and Society.* London: SAGE, Chapter 2 *‘Hackers, Cracker and Viral Coders’.*

**Week 5: Cyber Piracy**

“You wouldn’t steal a car” is the often mocked slogan from an anti-piracy campaign, which attempts to compare online media downloading with scenarios of theft offline. Although attitudes toward cyberpiracy may be indifferent and there are perceptions that large corporations are so wealthy that copying their intellectual property will not affect them, such activity is stealing, it is a crime to use the Web to copy digital documents without authorization. Examples of cyberpiracy include: copying and distributing music or video without the copyright holder’s permission, using cloned credit card information to steal from an online store, or copying software onto a CD without paying for it. If these activities become widespread, the effects are like those of shoplifting, where producers are compelled to stop issuing their product or increase prices to compensate for losses. As such, governments have created copyright laws to protect companies and artists. This lecture and workshop will investigate the role and actions of ‘pirates.’ In many discussions of cybercrime the actions and behaviours of cyber criminals can seem technically complicated and skilful. The level of sophistication, assumed or implied, is not always justified. Internet piracy in particular represents one such case, where the actions of cyber criminals are often much simpler than technical accounts might imply. This presentation will seek to explain some of the methods used by modern internet pirates. In doing so, it is hoped that this will not only explain some of technical mechanisms at play, but also highlight the social understanding that cybercriminals do not need to be ‘super hackers’, separate in skill and understanding from the rest of society.

Essential Reading

Chapter 13 *‘Intellectual Property Crime and the Internet: Cyber-piracy and ‘stealing’ information tangibles,’* Wall, D.S. & Yar, M. in Jewkes, Y., & Yar, M. (Eds.) (2013) *Handbook of Internet crime*. Routledge.

Chapter 4 *‘Virtual ‘Pirates’: Intellectual Property Theft Online’* inYar, M. (2006) *Cybercrime and Society.* London: SAGE

Further Reading

Cvetkovski, T. (2014) ‘The farcical side to the war on the media piracy: a popular case of Divine Comedy?’*Media, Culture & Society*, *36*(2), 246-257.

Farrand, B., & Carrapico, H. (2012) ‘Copyright law as a matter of (inter)national security? The attempt to securitise commercial infringement and its spillover onto individual liberty’. *Crime Law and Social Change* 57, 373-401.

Gray, K. (2012), ‘Stealing From The Rich To Entertain The Poor? A Survey Of Literature On The Ethics Of Digital Piracy.’ *The Serials Librarian* 63.3-4: 288-295.

Hinduja, S. (2007). ‘Neutralization theory and online software piracy: An empirical analysis’. *Ethics and Information Technology*, *9*(3), 187-204.

Moore, R., & McMullan, E. C. (2009). ‘Neutralizations and rationalizations of digital piracy: a qualitative analysis of university student’s. *International Journal of Cyber Criminology*, *3*(1), 441-451.Yar, M. (2005) ‘The global ‘epidemic’ of movie ‘piracy’: crime-wave or social construction?’ *Media, Culture & Society*, 27(5), 677-696.

**Week 6: Cyber Crime grows up: Carding, Escrow and the Dark Markets**

This lecture and workshop will consider how particular types of hacking such as carding have developed into more sophisticated forms of online crime. It will discuss a particular method of how trust became established within criminal networks in the form of Escrow. The ‘dark’ web and ‘dark’ markets will also be considered to highlight the expanding online underground economy. Regardless of agency intervention, such as the closure of Silk Road, these dark market outlets continue to thrive regardless.

Essential Reading

Martin, J. (2013). Lost on the Silk Road: Online drug distribution and the “cryptomarket.” Criminology and Criminal Justice, 14(3), 351–367.

Further Reading

Brenner, S., 2002. ‘Organized Cybercrime ? How Cyberspace May Affect the Structure of Criminal Relationships’. *North Carolina Journal of Law & Technology*, 41 (1984), 1–50.

Federal Bureau of Investigation. (2014). Dark Markets Seizure Forfeiture Complaint <http://www.scribd.com/doc/246024090/Dark-Markets-Seizure-Forfeiture-Complaint>

Federal Bureau of Investigation. (2014). Criminal Complaint: Blake Benthall a/k/a Defcon. Available at < <http://www.scribd.com/doc/245744857/Blake-Benthall-Criminal-Complaint>>

Holt, T.J., 2007. ‘Subcultural evolution? examining the influence of on- and off-line experiences on deviant subcultures’. Deviant Behavior, 28 (2), 171–198.

Holt, T.J., 2010. Examining the Role of Technology in the Formation of Deviant Subcultures. Social Science Computer Review, 28 (4), 466–481.

Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets online: products and market forces. *Criminal Justice Studies*, *23*(1), 33-50.

Holt, T.J., Burruss, G.W., and Bossler, A.M., 2010. Social Learning and Cyber-Deviance: Examining the Importance of a Full Social Learning Model In the Virtual World. Journal of Crime and Justice, 33 (2), 31–61.

Holt, T.J. and Lampke, E., 2010. Exploring stolen data markets online: products and market forces. Criminal Justice Studies, 23 (1), 33–50.

Lavorgna, A. (2015) ‘Organised crime goes online: realities and challenges’. *Journal of Money Laundering and Control*, 18(2), 153-168.

Van Hout, M. C., & Bingham, T. (2013). Silk Road’, the virtual drug marketplace: a single case study of user experiences. *International Journal of Drug Policy*, *24*(5), 385-391.

Webber, C., & Yip, M. (2012). ‘Drifting on and off-line: humanising the cyber criminal’, in S. Winlow and R. Atkinson (eds) *New Directions in Crime and Deviancy*, London: Routledge.

Yip, M., Shadbolt, N., Tiropanis, T., & Webber, C. (2012). The digital underground economy: a social network approach to understanding cybercrime. Available at Eprints

**Week 7: Everyday Cybercrimes: from trolling and hate crime, violent pornography, online grooming, to the purchasing of pharmaceuticals**

So far we have considered crimes against and using the computer, but what about other online illicit actions, conducted by ‘ordinary’ people? Digital technologies have revolutionized the ways we interact and communicate with each other, and transformed our leisure activities. This lecture and workshop will look at how the Web is used by people to engage in deviant and criminal behaviours, from the extreme to the banal.

Essential Reading

Adler, P. A., & Adler, P. (2006). The deviance society. *Deviant Behavior*, *27*(2), 129-148.

Jewkes, Y. (2011) *Media and Crime.* London: SAGE Publications. Chapter 9 *‘The role of the Internet in Crime and Deviance’*

Further Reading

Bryce, J. Jewkes, Y., & Yar, M. (Eds.). (2013). *Handbook of Internet crime*. Routledge. Chapter 16 *‘Online Sexual Exploitation of Children and Young People*

Denegri‐Knott, J. (2006). Consumers behaving badly: deviation or innovation? Power struggles on the web. *Journal of Consumer Behaviour*, *5*(1), 82-94.Jewkes, Y. (Ed.). (2002). *Dot. cons: Crime, deviance and identity on the Internet*. Routledge.

Lavorgna, A. (2015) ‘The social organisation of pet trafficking in cyberspace’. *European Journal of Criminal Policy and Research*, 21(3), 353-370.

Lavorgna, A. (2014) ‘The online trade in counterfeit pharmaceuticals: new criminal opportunities, trends, and challenges’. *The European Journal of Criminology,* 12(2), 226-241.

Lavorgna, A. (2014) ‘Internet-facilitated drug trafficking: towards a better understanding of new criminal dynamics’. *Trends in Organized Crime* 17(4), 250-270.

Lusthaus, J. (2013). ‘How organised is organised cybercrime?’ Global Crime, 14(1), 52-60.

McCusker, R. (2006). ‘Transnational organized cybercrime: Distinguishing threat from reality’. Crime, Law and Social Change, 46(4), 257-273.

Rege, A. (2009) ‘What’s love got to do with it? Exploring online dating scams and identity fraud’. *International Journal of Cyber Criminology*, 3(2), 494-512.

Sanders, T. in Jewkes, Y., & Yar, M. (Eds.). (2013). *Handbook of Internet crime*. Routledge. Chapter 15 *‘The Sex Industry, Regulation and the Internet’*

Treadwell, J. (2012). ‘From the Car boot to booting it up? eBay, online counterfeit crime and the transformation of the criminal marketplace’. Criminology and Criminal Justice, 12(2), 175-191.

Yar, M. (2006) *Cybercrime and Society.* London: SAGE

Chapter 5 ‘Cyber frauds, scams, and cons’

Chapter 6 *‘Illegal, Harmful and Offensive Content Online: From Hate Speech to the ‘Dangers’ of Pornography’*

Chapter 7 *‘Child pornography and Child Sex Abuse imagery’*

Chapter 8 *‘The Victimization of Individualisms Online: Cyberstalking and Paedophilia*’

**Week 8: From Cybercrime to Cyborg: The Bio-Intuitive Web**

Are passwords outdated? Have we come to the stage where the human brain cannot cope with any more passwords? What effect does forgetting passwords have on the Web? What might we replace passwords with? Can we trust biometrics? This workshop takes these questions as its starting point and asks what the future might hold for cybersecurity. But, crucially, with the rise of biometric registers and advanced AI, what does this trend mean for human identity? When computer-mediated devices know more about our lives than we do, are we becoming cyborgs? This workshop also explores the science of biometrics and traces the discussion back to equivalent controversies around fingerprints and DNA profiling.

Essential Reading

Cole, S.A. (2012) “Forensic Culture as Epistemic Culture: The sociology of forensic science” Studies in History and Philosophy of Biological and Biomedical Sciences Vol. 44 pp. 4-15

Eng, A. and Wahsheh, L.A. (2013), ‘Look into my Eyes: A Survey of Biometric Security’, in *Information Technology: New Generations*

<http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6614344&tag=1>

Further Reading

A.M. Bojamma, B. Nithya, Prasad .C.N., M.N.Nachappa (2013), ‘Biometric Security Systems’, in *International Journal of Inventive Engineering and Sciences* (IJIES), Volume-1, Issue-3, February 2013

<http://www.ijies.org/attachments/File/v1i3/D0158031413.pdf>

Cole, S.A. (1999) “What Counts for Identity? The historical origins of the methodology of latent fingerprint identification” *Science in Context* Vol. 12 pp. 139-72

Cole, S.A. (2002) *Suspect Identities: A history of fingerprinting and criminal identification* (Cambridge, Mass.: Harvard University Press)

Haraway, D. (1991), ‘A Cyborg Manifesto’, extract from ‘Science, Technology, and Socialist-Feminism in the Late Twentieth Century’, in *Simians, Cyborgsand Women: The Reinvention of Nature* , New York; Routledge, pp.149-181.

<http://people.oregonstate.edu/~vanlondp/wgss320/articles/haraway-cyborg-manifesto.pdf>

Duster, T. (2004) "Selective Arrests, an Ever-Expanding DNA Forensic Database, and the Specter of an Early Twenty-First Century Equivalent of Phrenology," in Lazer, D. (ed.) *DNA and the Criminal Justice System: The Technology of Justice* (Cambridge, MA: MIT Press) available at http://sociology.fas.nyu.edu/object/troyduster

Edmond, G. & Mercer, D. (1998) “Trashing Junk Science” *Stanford Technology Law Review* available at *http://stlr.stanford.edu/STLR/Articles/98\_STLR\_3*

Hamlin, C. (2012) “Forensic Cultures in Historical Perspective: Technologies of witness, testimony, judgement (and justice?) *Studies in History and Philosophy of Biological and Biomedical Sciences* Vol. 44 pp.

Heinemann, T., Lemke, T. & Prainsack, B. (2012) “Risky Profiles: Societal dimensions of forensic uses of DNA profiling technologies” *New Genetics and Society* Vol. 31 pp. 249-58

Lynch, M., Cole, S.A., McNally, R. & Jordan, K. (2008) “Fingerprinting: An inversion of credibility” in *Truth Machine: The contentious history of DNA fingerprinting* (Chicago: University of Chicago Press)

**Week 9: Hactivism: Political Protests on the Web or Threat to National Security?**

Hacktivism is a new phenomenon in which hacking converges with political activism (Denning 2001: 263). It has become especially newsworthy since a loose knit group of politically motivated hackers called “Anonymous” launched a series of high profile cyber-attacks against companies who had cut off services to Wikileaks due to the intense pressure from the US government. This caught the attention of the media who followed the event with increasing interest and hyperbole. The term hacktivism has been widely credited to Jason Sack in an article written about the artist Shu Lea Cheang in InfoNation in 1995. Hacktivism takes political demonstration onto the Internet and it often emulates activities seen in the real world. However, increasingly it is able to extend the kinds of demonstration typical of traditional attacks. This workshop looks at the future of democracy in a world where hacktivism allows almost anyone to demonstrate against anything, anytime and anywhere.

Essential Reading

Taylor, P. A. (2005) ‘From Hackers to Hacktivists: speed bumps on the global superhighway?’ *New Media and Society,* Vol. 7, No.5, 625-646

Yip, M. and Webber, C. (2011) ‘[Hacktivism: a Theoretical and Empirical Exploration of China’s Cyber Warriors.](http://eprints.soton.ac.uk/272350/)’ In, *ACM WebSci '11,Koblenz, Germany, 14 - 17 Jun 2011.*

Further Reading

Denning, D.E., (2001) ‘Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing’ In J. Arquilla & D. Ronfeldt, (eds.) Networks and Netwars: The Future of Terror, Crime, and Militancy. Santa Monica: RAND Corporation, pp. 239-288.

Doyle, A. (2011), ‘Revisiting the synopticon: Reconsidering Mathiesen’s ‘The Viewer Society’ in the age of Web 2.0’, Theoretical Criminology, 15 (3), 283-299.

Jordan, T. (2002), *Activism! Direct Action, Hacktivism and the Future of Society,* London: Reaktion Books

Jordan, T. and Taylor, P. (2004) *Hacktivism and Cyberwars: Rebels with a cause?* London: Routledge.

Jewkes, Y. (ed.) (2002), *Dot.cons: Crime, deviance and identity on the Internet,* Cullompton, Devon: Willan.

Manion, M. And Goodrum, A. (2000) ‘Terrorism or Civil Disobedience: Towards a Hacktivist Ethic’ *Computers and Society,* 30 (2), 14-19.

Shalhoub-Kevorkian, N., (2012) ‘E-Resistance and Technological In/Security in Everyday Life’ *The British Journal of Criminology*. 52 (1), 55-72

Taylor, P. A. (2001) ‘Hacktivism: in search of lost ethics?’ in D. S. Wall (ed.), *Crime and the Internet,* London: Routledge, pp. 59-73

**Week 10: Policing and Punishing Cybercrime**

Traditional crime, such as armed robbery, took the form of one big heist netting a lot of money (if the criminal was lucky). This is still true of some forms of cybercrime. For example, the more successful carders can steal large sums of money from credit cards. But, perhaps uniquely, cybercrime can also be the large accumulation of small amounts of money. £1 stolen from a million people can bring wealth to the criminal, but be hardly noticed by the victim. This makes detection and punishment of the criminal especially tricky. This final workshop explores these issues and brings the module to a close.

Essential Reading

Wall, D.S. (2013), ‘Policing identity crimes’, *Policing and Society, 23:4*.

Wall, D.S. and Williams, M. (2013), ‘[Policing cybercrime: networked and social media technologies and the challenges for policing’,](http://www.tandfonline.com/doi/full/10.1080/10439463.2013.780222) *[Policing and Society,](http://www.tandfonline.com/doi/full/10.1080/10439463.2013.780222)* [23:4.](http://www.tandfonline.com/doi/full/10.1080/10439463.2013.780222)

Further Reading

Algarni, A.F. (2013), ‘Policing Internet fraud in Saudi Arabia: expressive gestures or adaptive strategies?’, *Policing and Society*, 23:4.

Chan, J., Goggin, G. and Bruce, J. (2010), ‘Internet technologies and criminal justice’, in Y. Jewkes and M. Yar (eds.) *Handbook of Internet Crime,* Cullompton, Devon: Willan publishing.

Jewkes, Y. (2010), ‘Public policing and Internet crime’, in Y. Jewkes and M. Yar (eds.) *Handbook of Internet Crime,* Cullompton, Devon: Willan publishing.

Maguire, M. (2010), ‘Online surveillance and personal liberty’, in Y. Jewkes and M. Yar (eds.) *Handbook of Internet Crime,* Cullompton, Devon: Willan publishing.

[[Procter](http://www.tandfonline.com/doi/full/10.1080/10439463.2013.780223)](http://www.tandfonline.com/action/doSearch?Contrib=Procter%2C+R)[, R.,](http://www.tandfonline.com/doi/full/10.1080/10439463.2013.780223) [[Crump](http://www.tandfonline.com/doi/full/10.1080/10439463.2013.780223)](http://www.tandfonline.com/action/doSearch?Contrib=Crump%2C+J)[, J.,](http://www.tandfonline.com/doi/full/10.1080/10439463.2013.780223) [[Karstedt](http://www.tandfonline.com/doi/full/10.1080/10439463.2013.780223)](http://www.tandfonline.com/action/doSearch?Contrib=Karstedt%2C+S)[, S.,](http://www.tandfonline.com/doi/full/10.1080/10439463.2013.780223) [[Voss](http://www.tandfonline.com/doi/full/10.1080/10439463.2013.780223)](http://www.tandfonline.com/action/doSearch?Contrib=Voss%2C+A)[, A. &](http://www.tandfonline.com/doi/full/10.1080/10439463.2013.780223) [[Cantijoch](http://www.tandfonline.com/doi/full/10.1080/10439463.2013.780223)](http://www.tandfonline.com/action/doSearch?Contrib=Cantijoch%2C+M)[, M. (2013), ‘Reading the riots: what](http://www.tandfonline.com/doi/full/10.1080/10439463.2013.780223)*[were](http://www.tandfonline.com/doi/full/10.1080/10439463.2013.780223)*[the police doing on Twitter?’,](http://www.tandfonline.com/doi/full/10.1080/10439463.2013.780223) *[Policing and Society, 23:4](http://www.tandfonline.com/doi/full/10.1080/10439463.2013.780223)*[.](http://www.tandfonline.com/doi/full/10.1080/10439463.2013.780223)

Walden, I. (2010), ‘Computer forensics and the presentation of evidence in criminal cases’, in Y. Jewkes and M. Yar (eds.) *Handbook of Internet Crime,* Cullompton, Devon: Willan publishing.

Wall, D.S. and Williams, M., 2007. Policing Diversity in the Digital Age. Criminology and Criminal Justice, 7 (4), 391–415.

Williams, M. (2010), ‘The virtual neighbourhood watch: netizens in action’, in Y. Jewkes and M. Yar (eds.) *Handbook of Internet Crime,* Cullompton, Devon: Willan publishing.

Yar, M. (2010), ‘The private policing of Internet crime’, in Y. Jewkes and M. Yar (eds.) *Handbook of Internet Crime,* Cullompton, Devon: Willan publishing.

Yip, M., Webber, C., and Shadbolt, N., 2013a. Trust among Cybercriminals? Carding Forums, Uncertainty and Implications for Policing. Journal of Policing and Society.

**Even Further Reading**

*The following references can be followed up by anyone wishing to explore this area further.*

Birk, D., Gajek, S., Grobert, F., and Sadeghi, A.-R., 2007. Phishing Phishers - Observing and Tracing Organized Cybercrime. Second International Conference on Internet Monitoring and Protection (ICIMP 2007), (Icimp), 3–3.

Cárdenas, A., Radosavac, S., Grossklags, J., Chuang, J., and Hoofnagle, C., 2010. An Economic Map of Cybercrime. In: The 37th Research Conference on Communication, Information and Internet Policy (TPRC).

Carley, K., 2006. Destabilization of Covert Networks. Computational & Mathematical Organization Theory, 12 (1), 51–66.

Chattoe, E. and Hamill, H., 2005. It’s Not Who You Know--It's What You Know About People You Don't Know That Counts: Extending the Analysis of Crime Groups as Social Networks. British Journal of Criminology, 45 (6), 860–876.

Choo, K.-K.R., 2008. Organised crime groups in cyberspace: a typology. Trends in Organized Crime, 11 (3), 270–295.

Choo, K.-K.R. and Smith, R.G., 2007. Criminal Exploitation of Online Systems by Organised Crime Groups. Asian Journal of Criminology, 3 (1), 37–59.

Cohen, S., 2002. Folk Devils and Moral Panics. London: McGibbon and Kee.

Coles, N., 2001. It’s Not What You Know--It's Who You Know That Counts. Analysing Serious Crime Groups as Social Networks. British Journal of Criminology, 41 (4), 580–594.

Dhamija, R., Tygar, J.D., and Hearst, M., 2006. Why phishing works. Proceedings of the SIGCHI conference on Human Factors in computing systems - CHI ’06, (November 2005), 581.

Europol, 2011. Threat Assessment: Internet Facilitated Organised Crime. Threat Assessment (Abridged).

Finckenauer, J., 2005. Problems of definition: what is organized crime? Trends in organized crime, 8, 63–83.

Florêncio, D. and Herley, C., 2010. Phishing and money mules. Information Forensics and Security (WIFS), 2010 IEEE International Workshop on.

Franklin, J., Paxson, V., Perrig, A., and Savage, S., 2007. An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants. In: Proceedings of the 14th ACM conference on Computer and communications security. New York, NY, USA: ACM, 375–388.

Glenny, M., 2011. Darkmarket: Cyberthieves, Cybercops and You, London: The Bodley Head.

Gordon, S. and Ford, R., 2006. On the definition and classification of cybercrime. Journal in Computer Virology, 2 (1), 13–20.

Grabosky, P., 2007. The Internet, Technology, and Organized Crime. Asian Journal of Criminology, 2 (2), 145–161

Herley, C. and Florêncio, D., 2008. A profitless endeavor: phishing as tragedy of the commons. In: Proceedings of the 2008 workshop on New security paradigms. New York, NY, USA: ACM, 59–70.

Herley, C. and Florêncio, D., 2010. Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy. In: T. Moore, D. Pym, and C. Ioannidis, eds. Economics of Information Security and Privacy. Springer US, 33–53.

Hewson, C., Yule, P., Laurent, D., and Vogel, C., 2003. Internet Research Methods. London: Sage.

Hinduja, S., 2007. Neutralization theory and online software piracy: An empirical analysis. Ethics and Information Technology, 9, 187–204.

HM Government, 2010. The National Security Strategy [online]. Available from: http://www.direct.gov.uk/prod\_consum\_dg/groups/dg\_digitalassets/@dg/@en/documents/digitalasset/dg\_191639.pdf?CID=PDF&PLA=furl&CRE=nationalsecuritystrategy.

Holt, T.J., 2007. subcultural evolution? examining the influence of on- and off-line experiences on deviant subcultures. Deviant Behavior, 28 (2), 171–198.

Holt, T.J., 2010. Examining the Role of Technology in the Formation of Deviant Subcultures. Social Science Computer Review, 28 (4), 466–481.

Holt, T.J., Burruss, G.W., and Bossler, A.M., 2010. Social Learning and Cyber-Deviance: Examining the Importance of a Full Social Learning Model In the Virtual World. Journal of Crime and Justice, 33 (2), 31–61.

Holt, T.J. and Lampke, E., 2010. Exploring stolen data markets online: products and market forces. Criminal Justice Studies, 23 (1), 33–50.

Holz, T., Engelberth, M., and Freiling, F., 2009. Learning More about the Underground Economy: A Case-Study of Keyloggers and Dropzones. In: M. Backes and P. Ning, eds. Computer Security – ESORICS 2009. Springer Berlin / Heidelberg, 1–18.

Home Office, 2010. Cyber Crime Strategy. Surrey.

IC3, 2012. IC3 2011 Internet Crime Report [online]. Available from: http://www.ic3.gov/media/annualreport/2011\_IC3Report.pdf.

Johnson, M., 2011. A look inside the SpyEye Trojan admin console [online]. Available from: http://www.webroot.com/blog/2011/10/24/a-look-inside-the-spyeye-admin-console/ [Accessed 31 Dec 2014].

Krebs, V.E., 2001. Mapping Networks of Terrorist Cells. Connections, 24 (3), 43–52.

Kumar, R., Novak, J., and Tomkins, A., 2006. Structure and Evolution of Online Social Networks. In: Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining. New York, NY, USA: ACM, 611–617.

Levi, M., 2008. Organized Fraud and Organizing Frauds. Criminology and Criminal Justice, 8 (4), 389–419.

Levi, M., 2009. Suite Revenge?: The Shaping of Folk Devils and Moral Panics about White-Collar Crimes . British Journal of Criminology , 49 (1 ), 48–67.

Lu, Y., Luo, X., Polgar, M., and Cao, Y., 2010. Social Network Analysis of a Criminal Hacker Community. Journal of Computer Information Systems, 51 (2).

Lusthaus, J., 2012. Trust in the World of Cybercrime. Global Crime, 13 (2), 71–94.

Mann, D. and Sutton, M., 1998. >>NETCRIME: More Change in the Organization of Thieving. British Journal of Criminology, 38 (2), 201–229.

McAfee and CSIS, 2014. Net Losses: Estimating the Global Cost of Cybercrime [online]. Available from: http://csis.org/files/attachments/140609\_McAfee\_PDF.pdf [Accessed 31 Dec 2014].

McCusker, R., 2007. Transnational organised cyber crime: distinguishing threat from reality. Crime, Law and Social Change, 46 (4), 257–273.

McIllwain, J.S., 1999. Organized crime: A Social Network Approach. Crime, Law and Social Change, 32 (4), 301–323.

Memon, N. and Hicks, D.L., 2008. Detecting Key Players in 11-M Terrorist Network: A Case Study. In: Availability, Reliability and Security, 2008. ARES 08. Third International Conference on. 1254–1259.

Memon, N., Hicks, D., and Larsen, H., 2007. How Investigative Data Mining Can Help Intelligence Agencies to Discover Dependence of Nodes in Terrorist Networks. In: R. Alhajj, H. Gao, X. Li, J. Li, and O. Zaïane, eds. Springer Berlin / Heidelberg, 430–441.

Memon, N., Larsen, H., Hicks, D., and Harkiolakis, N., 2008. Detecting Hidden Hierarchy in Terrorist Networks: Some Case Studies. In: C. Yang, H. Chen, M. Chau, K. Chang, S.-D. Lang, P. Chen, R. Hsieh, D. Zeng, F.-Y. Wang, K. Carley, W. Mao, and J. Zhan, eds. Springer Berlin / Heidelberg, 477–489.

Moore, T., Clayton, R., and Anderson, R., 2009. The Economics of Online Crime. Journal of Economic Perspectives, 23 (3), 3–20.

Morselli, C., Giguère, C., and Petit, K., 2007. The Efficiency/Security Trade-off in Criminal Networks. Social Networks, 29 (1), 143–153.

Morselli, C. and Petit, K., 2007. Law-Enforcement Disruption of a Drug Importation Network. Global Crime, 8 (2), 109–130.

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., and Voelker, G.M., 2011. An Analysis of Underground Forums. In: Proceedings of the ACM Internet Measurement Conference (IMC). Berlin, Germany.

Panda Security, 2011. The Cyber Crime Black Market [online]. Available from: <http://press.pandasecurity.com/wp-content/uploads/2011/01/The-Cyber-Crime-Black-Market.pdf>.

Peretti, K.K., 2008. Data Breaches: What the Underground World of “Carding” Reveals. Santa Clara Computer and High Technology Journal, 25, 375–414.

Raab, J. and Milward, H., 2003. Dark Networks as Problems. Journal of Public Administration Research and Theory, 13 (4), 413–439.

Raban, J., 1974. Soft City. London: Hamilton.

Radianti, J., 2010. A Study of a Social Behavior inside the Online Black Markets. In: Emerging Security Information Systems and Technologies (SECURWARE), 2010 Fourth International Conference on. 189–194.

Ressler, S., 2006. Social Network Analysis as an Approach to Combat Terrorism : Past , Present , and Future Research. The Journal of Naval Postgraduate School Center for Homeland Defense and Security, 2 (2).

Robins, G., 2008. Understanding individual behaviors within covert networks: the interplay of individual qualities, psychological predispositions, and network effects. Trends in Organized Crime, 12 (2), 166–187.

Schwartz, D.M. and Rouselle, T., 2009. Using social network analysis to target criminal networks. Trends in Organized Crime, 12 (2), 188–207.

Skinner, W.F. and Fream, A.M., 1997. A Social Learning Theory Analysis of Computer Crime among College Students. Journal of Research in Crime and Delinquency, 34 (4), 495–518.

Smith, R., 2010. Identity theft and fraud. In: Y. Jewkes and M. Yar, eds. The Handbook of Internet Crime. Devon: Willan Publishing, 273–301.

Sparrow, M., 1991. The application of network analysis to criminal intelligence: An assessment of the prospects. Social Networks, 13 (3), 251–274.

Stone-Gross, B., Holz, T., Stringhini, G., and Vigna, G., 2011a. The underground economy of spam: a botmaster’s perspective of coordinating large-scale spam campaigns. In: Proceedings of the 4th USENIX conference on Large-scale exploits and emergent threats. Berkeley, CA, USA: USENIX Association, 4.

Stone-Gross, B., Abman, R., Kemmerer, R.A., Kruegel, C., Steigerwald, D.G., and Vigna, G., 2011b. The Underground Economy of Fake Antivirus Software. Proceedings of the Tenth Workshop on the Economics of Information Security WEIS, 1–14.

The Economist, 2010. Cyberwar: The Threat from the Internet [online]. The Economist. Available from: http://www.economist.com/node/16481504 [Accessed 31 Dec 2014].

Thomas, R. and Martin, J., 2006. the underground economy : priceless. The USENIX Magazine, 31 (6), 7–16.

Van Calster, P., 2006. Re-visiting Mr. Nice. On Organized Crime as Conversational Interaction. Crime, Law and Social Change, 45 (4), 337–359.

Verizon, 2014. 2014 Data Breach Investigation Report [online]. Available from: http://www.verizonbusiness.com/resources/reports/rp\_data-breach-investigations-report-2012\_en\_xg.pdf.

Von Lampe, K., 2003. Criminally Exploitable Ties: A Network Approach to Organized Crime. In: Transnational Organized Crime: Myth, Power, and Profit. North Carolina: Carolina Academic Press, 9–22.

Von Lampe, K. and Johansen, P., 2004. Organized Crime and Trust: On the Conceptualization and Empirical Relevance of Trust in the Context of Criminal Networks. Global Crime, 6 (2), 159–184.

Von Lampe, K., 2005. Making the second step before the first: Assessing organized crime. Crime, Law and Social Change, 42 (4), 227–259.

Weerman, F.M., 2003. Co-offending as Social Exchange. Explaining Characteristics of Co‐offending. British Journal of Criminology, 43 (2), 398–416.

Wehinger, F., 2011. The Dark Net: Self-Regulation Dynamics of Illegal Online Markets for identities and Related Services. In: European Intelligence and Security Informatics Conference (EISIC). 209–213.

Williams, M., 2007. Policing and Cybersociety: The Maturation of Regulation within an Online Community. Policing and Society, 17 (1), 59–82.

Williams, P., 1998. The Nature of Drug-Trafficking Networks. Current History, 97 (618), 154–159.

Xu, J. and Chen, H., 2003. Untangling Criminal Networks: A Case Study. In: H. Chen, R. Miranda, D. Zeng, C. Demchak, J. Schroeder, and T. Madhusudan, eds. ISI 2003. Springer Berlin / Heidelberg, 958.

Xu, J., Marshall, B., Kaza, S., and Chen, H., 2004. Analyzing and Visualizing Criminal Network Dynamics: A Case Study. In: H. Chen, R. Moore, D. Zeng, and J. Leavitt, eds. Intelligence and Security Informatics. Springer Berlin / Heidelberg, 359–377.

Xu, J., Chen, H., Zhou, Y., and Qin, J., 2006. On the Topology of the Dark Web of Terrorist Groups. In: Proceedings of the IEEE International Conference on Intelligence and Security Informatics (ISI). 367–376.

Xu, J. and Chen, H., 2008. The topology of dark networks. Communications of the ACM, 51 (10), 58–65.

Yip, M., 2011. An Investigation into Chinese Cybercrime and the Applicability of Social Network Analysis. In: ACM Web Science Conference 2011, Koblenz, 14-17 June.

Yip, M., Shadbolt, N., and Webber, C., 2013b. Why forums? An Empirical Analysis into the Facilitating Factors of Carding Forums. ACM Web Science 2013.

Zhuge, J., Holz, T., Song, C., Guo, J., Han, X., and Zou, W., 2009. Studying Malicious Websites and the Underground Economy on the Chinese Web. In: Managing Information Risk and the Economics of Security. Springer US,

**Assessment**

|  |  |  |  |
| --- | --- | --- | --- |
| **CRIM6002 (MSc CRIMINOLOGY) Assessment Method** | Number | % contribution to final mark | Final assessment (√) |
| Group Presentation on Current Concerns and Future Risks from Cyber Crime | 1 | 20 |  |
| Essay 1500 words: an individual elaboration of the presentation:  Criminology in the future: Horizon Scanning  What are the future problems for which criminology will need to find the answers? | 1 | 30 |  |
| Essay 3000 words: What does criminology know about Cybercrime and is it helping us to confront the problem? | 1 | 50 | √ |
|  | | | |
| **CRIM6008 (MSC CYBER SECURITY) Assessment Method** | Number | % contribution to final mark | Final assessment (√) |
| Group Presentation on Current Concerns and Future Risks from Cyber Crime | 1 | 20 |  |
| Essay 1500 words: an individual elaboration of the presentation:  Criminology in the future: Horizon Scanning (What are the future problems for which criminology will need to find the answers?) | 1 | 30 |  |
| Essay 2000 words: What does criminology know about Cybercrime and is it helping us to confront the problem? | 1 | 50 | √ |

**Essay 1 due Thursday 16th March**

**Essay 2 due Wednesday 17th May**

**General notes**

* **All course work is submitted via Turnitin through the module BlackBoard site.  Guidance on how to submit via BlackBoard and how to access your marks and feedback is loaded on the module site under 'assignments'.**
* Essay length does not include a. Bibliography

* All essays must be typed/word processed

Submitting your essay

* **All course work is submitted via Turnitin through the module BlackBoard site.  Guidance on how to submit via BlackBoard and how to access your marks and feedback is loaded on the module site under 'assignments'.**

Work submitted after the deadline without an agreed extension will be marked as usual. You will also receive feedback as you normally would for that module. However, a penalty is imposed, as described in the table below:

University working days Penalty mark

1 10% of final mark removed

2 20% of final mark removed

3 30% of final mark removed

4 40% of final mark removed

5 50% of final mark removed

More than 5 Zero awarded

The penalty system deducts points from the mark you would have received if the assignment had been submitted on time. For example, if your mark would have been 60, but the assignment is submitted one working day late, your assignment will be reduced by 10% of the final mark ie 6 marks, resulting in a 54.

Working days are Monday to Friday throughout the calendar year, including student vacation periods (but excluding University staff closure dates at Easter and Christmas).

Work submitted after the published deadline may be accompanied by a completed Special Considerations application form should a valid reason exist for the late submission, but submitting the form does not guarantee that a penalty will be taken off.

These penalties do not apply when within the period of a formally granted extension to the original submission deadline.

* Essays must have a bibliography which is set out following standard procedures

(see Student Handbook)

* Essays must be correctly referenced with all quotations acknowledged in the appropriate way. See Handbook for what constitutes **‘plagiarism’**, the penalties for it and how to avoid it. *(Note that if you copy sections from a source and* ***only*** *in brackets at the end of this add author and page number then this is still plagiarism as you are not acknowledging this as a quote using quotation marks and a correct reference))* If in doubt refer to *Cite it Right*. Do not lose marks unnecessarily for poor citations.
* **Essays which fail to follow the above will be penalized and may fail**
* **Re-assessment**: in the event of failure caused by poor performance in assessments, re-assessment is in the form of ***one essay*** (weighted at 100%) in the August Supplementary period. The word count will be the same as the failed or missed essay.
* Extensions: If you require an extension to an assignment, you must complete the Deadline Extension Request form, which you can download from the Form Store on the FSHMS Hub Blackboard site or via this link (<http://www.southampton.ac.uk/quality/assessment/special_considerations.page>? ) and submit this to the Student Office (SSPC.StudentOffice@soton.ac.uk ).  This will be considered by the appropriate Extensions Officer and you will receive a response via email.  Extensions can only be granted up to the date of submission, so we recommend that you submit the form as soon as you are aware of any concerns.
* Marking process: For an overview of our Marking and Moderation policy please go to the following link: <http://www.southampton.ac.uk/quality/assessment/framework/marking_and_feedback.page>?
* Date of returned work - university policy is that this should be four weeks after the deadline day, however, there are occasionally unforeseeable circumstances that might extend this period. We will keep you updated should we encounter any problems.

**Marking Criteria for Assessed Written Work**

The following table gives details of the scale which is used to award marks for coursework submitted in connection with the Diploma/MSc in Sociology, Diploma/MSc in Social Policy and the Diploma/MSc in Sociology and Social Policy. The table also provides an indication of the qualities which are normally found in work which is placed within each mark band.

|  |  |
| --- | --- |
| Distinction  70-79%  High Distinction 80-100% | Displays most of the following characteristics:   * Comprehensive systematic knowledge and understanding of the implications of the question and the subject area * Very high degree of analytical competence in evaluating different theoretical approaches, concepts, evidence and arguments and makes clear links with other areas of the subject * Very well structured and sustained argument * Clear evidence of Independence of thought * Evidence of extensive reading and study, well beyond immediate or key sources * Presentation is crisp, fluent, focused and in an appropriate format * Citation and referencing is accurate, consistent and in appropriate style (for essays only)   Displays all the above characteristics, and willingness to challenge received wisdom. Work may be of publishable quality. |
| Merit  60-69% | * Reasonably systematic knowledge and understanding of the implications of the question and the subject area with no major errors * Good analytical competence in evaluating different theoretical approaches, concepts, evidence and arguments and establishes links with other areas of the subject * Good structure and sustained argument * Some independence of thought * Wide reading and study beyond immediate or key sources * Presentation fluent and focused and in an appropriate format * Citation and referencing is accurate, consistent and in appropriate style (for essays only) |
| Pass  50-59% | * Competent knowledge and understanding of the implications of the question and the subject area with no major errors * Competent in evaluating different theoretical approaches, concepts, evidence and arguments and some recognition of links with other areas of the subject * Reasonable structure and sustained argument * Evidence of critical awareness, but limited originality * Some reading and study beyond immediate or key sources * Presentation reasonably focused and in an appropriate format * Citation and referencing is reasonably accurate, consistent and in appropriate style (for essays only) |
| Qualifying Mark  35-49% | * Mainly competent knowledge and understanding of the implications of the question and the subject area, but with some errors and omissions of key issues * Some recognition of different theoretical approaches, concepts, evidence and arguments, but fails to make links with other areas of the subject * Structure and focus of argument weak * Lacks originality * Limited reading and study beyond module materials * Presentation reasonably focused and in an appropriate format * Some mistakes in citations and referencing (for essays only) |
| Fail  25-34 | * Limited knowledge and understanding of the implications of the question and the subject area, marred by serious errors and omissions of key issues * Lack of recognition of different theoretical approaches, concepts, evidence and arguments * Poor structure and focus of argument * Lacks originality * Little attempt to identify relevant materials * Organisation and presentation poor * Mistakes in citations and referencing (for essays only) |
| Low fail  0-24% | * Little or no knowledge and understanding of the subject * No recognition of different theoretical approaches, concepts, evidence and arguments * Poor structure and focus of arguments * No evidence of serious study * Organisation and presentation poor * Significant mistakes in citations and referencing (for essays only) |

Essays must have a bibliography which is set out following standard procedures (see Student Handbook)

Essays must be correctly referenced with all quotations acknowledged in the appropriate way. See University Library website for what constitutes **‘plagiarism’**, the penalties for it and how to avoid it. *(Note that if you copy sections from a source and* ***only*** *in brackets at the end of this add author and page number then this is still plagiarism as you are not acknowledging this as a quote using quotation marks and a correct reference))*

Essay which fail to follow the above will be penalized and may fail

Below you will find an example of the marking form we use, you can use this as a way to understand how we mark your work.

|  |  |  |
| --- | --- | --- |
| **Department of Sociology, Social Policy and Criminology** | | |
| Essay Feedback Form 2016/17 | | |
| Module number: | | |
|  | | Candidate Number: |
| Assignment number: | | |
| Understanding of the question | Strengths  To get a better mark, you would need to: | |
| Knowledge of subject and its key concepts | Strengths  To get a better mark, you would need to: | |
| Evidence of ability to summarise and critically engage with relevant literature | Strengths  To get a better mark, you would need to: | |
| Clarity of structure and argument | Strengths  To get a better mark, you would need to: | |
| Use of evidence in support of argumentation | Strengths  To get a better mark, you would need to: | |
| Strength of conclusions reached | Strengths  To get a better mark, you would need to: | |
| Accuracy of bibliographical referencing | Strengths  To get a better mark, you would need to: | |
| Additional comments: | | |
| Recommended mark: | | Recommended grade: |
| Assessed by:  Date: | | Moderated by: |

**NB**

The feedback above is intended to provide a broad indication of the characteristics of a piece of assessed work. Assessed work might display these characteristics in varying degrees, and these variations may not correlate precisely with one another. Assessment, therefore, necessarily involves a judgement on the part of markers of the extent to which relative strengths and weaknesses balance against one another, but always includes a baseline assessment of the student's ability to answer the question that has been set.