Sociology Factsheet

www.curriculum-press.co.uk Number 180

Cybercrime

Introduction

Within the developed world, cybercrime is one of the fastest growing criminal activities. This is not at all surprising given the pace of technological developments and globalisation. In fact, it could be argued that cybercrime is primarily a consequence of globalisation, as well as new media – the two are inextricably linked.

The information in this Factsheet would be relevant to exam questions on the topics of:

Crime & Deviance: Globalisation and crime in contemporary society; the media and crime; green crime; human rights and state crimes**;** crime control, surveillance, prevention & punishment; victims and the role of the criminal justice system and other agencies.

Mass Media: The new media and their significance for an understanding of the role of the media in contemporary society; globalisation and popular culture.

Activity
What do you understand by the term cybercrime, and what crimes do you think would be included in this category?

What is Cybercrime?

It is difficult to define cybercrime, partly because of the scale of it and partly because of the globalised nature of it. However, it has been defined by different people and different organisations as follows:

Cybercrime covers a wide range of illegal and criminal activities and costs the UK Government around £27 billion every year according to Detica (2011), and includes for example:

- Computer hacking,
- Virus attacks,
- Child pornography and paedophilia,
- Terrorist websites,
- Financial online scams,
- Stalking by email,
- Identity theft,
- Websites that promote/incite racial and/or religious hatred,
- Fraud relating to tax, pensions and benefits, local and central governments and the NHS,
- Intellectual property theft (such as stealing copyright, ideas, designs and trade secrets).

All of these contribute to this huge amount of money.

Activity
Look up a definition of all of the crimes in this list.

Douglas Thomas & Brian Loader (2000) define cybercrime as computer-mediated activities that are either illegal or considered illicit by some, and that are conducted through global electronic networks.

Yvonne Dukes (2003) suggests that the internet creates opportunities to commit both conventional crimes e.g. fraud, and new crimes using new tools e.g. computer hacking.

According to Wall (2001) – four categories of cybercrime can be identified:

- **Cyber-trespass:** this is where boundaries are crossed into others cyber-property, this would include computer hacking or the spreading of viruses.
- **Cyber-deception and theft:** this would include identity theft, phishing (which means obtaining identity or bank account details by deception), and violation of intellectual property rights, e.g. software piracy, illegal downloading, and file-sharing.
- **Cyber-pornography:** this includes both porn involving minors and opportunities for children to access online porn.
- **Cyber-violence:** this is where psychological harm is done or inciting physical harm, this could include e.g. cyber-stalking and hate crimes against minority groups.

Activity
The above four categories have been put into the table below. For each category, do some research and find two examples that have been reported in the media.

	Cyber-trespass	Cyber-deception & theft	Cyber-pornography	Cyber-violence
Example one				
Example two				

Norton (the consumer security software company) – http://uk.norton.com ask on their website: **What is cybercrime?** They respond with: Cybercrime is a bigger risk now than ever before due to the sheer number of connected people and devices. But what is it exactly? In a nutshell, it is simply a crime that has some kind of computer or cyber aspect to it.
They continue with:

Cybercrime: The Facts

- Cybercrime has now surpassed illegal drug trafficking as a criminal moneymaker.
- Somebody's identity is stolen every 3 seconds as a result of cybercrime.
- Without a sophisticated security package, your unprotected PC can become infected within four minutes of connecting to the internet.

Activity
It is quite clear that cybercrime has become a big problem, both at home and globally. However, Norton clearly have a commercial reason for scaring us about computer security. What is your take on this? How much do you pay for protecting your PC? Have you or any of your family or friends been hacked?

Cybercrime and Consumers

The National Crime Agency (NCA) www.nationalcrimeagency.gov.uk states on its website 'Organised crime has been quick to take advantage of the opportunities offered by the internet, particularly the growth in e-commerce and on-line banking. Specialist criminal groups target individuals, small businesses, and large corporate networks to steal personal information in bulk in order to profit from the compromised data available to them. They suggest that common cyber-threats to consumers are:

1. Phishing: bogus emails asking for security information and personal details.
2. Webcam manager: where criminals take over your webcam.
3. File hijacker: where criminals hijack files and hold them to ransom.
4. Keylogging: where criminals record what you type on your keyboard.
5. Screenshot manager: allows criminals to take screenshots of your computer screen.
6. Ad clicker: allows a criminal to direct a victim's computer to click a specific link.

Cybercrime and Politics

An article in the i, dated 15th February 2017, by Kim Sengupta, entitled *Cyber-chief: parties at risk from hackers*, looks at how nervous political parties are about the potential of being hacked. British political parties have approached the security agencies following cyber-attacks during the 2015 British general election, and the hacking of the Democratic Party emails in the US as part of an alleged campaign by Russia to help Donald Trump win the presidential election. This followed an attack on France's TV5Monde by hackers believed to be linked to the Kremlin. The article reports on the fact that the head of the UK's new National Cyber Security Centre, Ciaran Martin, had been in informal talks with the political parties. He goes on to say that there is a need to protect Britain's political system from the danger of cyber-attacks – protecting the integrity of the electoral democratic system is a top priority. It continues to state that there had been persistent reports of the Kremlin's interference in the West's political system, using cyber-attacks – with claims that the forthcoming elections in Holland, France, and Germany (countries with right-wing populist parties, which have varying degrees of Russian support) may be vulnerable.

Activity
Do some research into the claims that Russia used cyber-attacks to interfere with the recent US presidential election.
Summarise what you find.
What are your views on this?

Exam Hint: *The Specifications for Sociology A-Level stress that you should be encouraged to use examples/illustrations drawn from your own experience of small-scale research. This is particularly relevant to crime and deviance/theory and methods. Think about what example you could use to support your answers on cybercrime*

Why Has There Been an Increase in Cybercrime?

- Globalisation - this has led to greater worldwide accessibility,
- Increased reliance on computers at home and at work,
- The spread of the internet,
- It is often difficult to detect and prosecute individuals responsible.

Activity
Can you think of any more reasons why cybercrime has increased? Add your reasons to this list and then discuss them with other students.

Cybercrime and the Media

It is certainly the case that crime and deviance make up a large proportion of news coverage, Williams & Dickinson (1993) found that up to 30% of British newspapers coverage is devoted to crime stories. It can be argued that while the media show interest in crime, they give a distorted representation of crime, criminals and policing – for example, the media over represent violent and sexual crime. Ditton & Duffy (1983) found that 46% of media reports were about violent or sexual crimes, however, these only made up 3% of all crimes recorded by the police.

Activity
Why do you think this is?
Do some content analysis of daily newspapers and see what you find. Do your results support the findings of Ditton & Duffy?

There has been quite a long history of debates as to whether the media causes crime and deviance generally, and cybercrime can now be included in that debate. Pearson (1983) calls this respectable fear – meaning the concerns or fears of respectable people. For example, it has long been argued that the media creates deviancy amplification – the media reports on a crime and this can help create an amplification. The seaside skirmishes of the Mods & Rockers in the 1960s are a good example of this. Drug use and gun and knife crimes are other examples. This links to moral panics – usually driven or inspired by the media where the reaction enlarges the problem out of all proportion, in relation to its seriousness. The media identify a group as a folk devil, which then poses a threat to societal values.

Activity
Research the work of Stanley Cohen: *Folk Devils & Moral Panics: The Creation of the Mods and Rockers*.
How could this study link to cybercrime?

Exam Hint: *You need to use evidence in your answers to support what you are writing. The work of Cohen is a useful and relevant study for several of the Sociology A level topics.*

Another debate has been whether the media passes on knowledge on how to commit a crime, or a criminal technique – computer games such as Grand Theft Auto would be a good example, with gamers acting out crimes.

Activity
How relevant do you think this is? Do you think computer games, etc. encourage crime in society?
How relevant do you think this is to cybercrime?

Crime & Deviance/Theory & Methods.
Think about what examples you could use to support your answers on cybercrime.

Research evidence supports the view that there is a link between media use and the fear of crime. Schlesinger and Tumber (1992) found a correlation between media consumption and the fear of crime, with tabloid readers and heavy users of television expressing greater fear of becoming a victim, especially of physical attack.

McRobbie & Thornton (1995) argue now that moral panics have become routine, and therefore have low impact. In late modern society, and from a postmodern perspective, there is little consensus about what is now, actually deviant.
The developments in new technology and arrival of new types of media can often be met with a moral panic, as is also the case with the internet. The speed and scale of the development of the internet has clearly created moral panics around cybercrime. Policing cybercrime is difficult because of the scale of the internet, the limited resources of the police, and the globalised nature of the internet causing problems of jurisdiction.

It could be argued that the media is responsible for passing on new means of committing crimes, with the internet providing new opportunities for committing cybercrimes. Quite clearly, the examples of cybercrimes looked at within this Factsheet can be linked to the internet, but how responsible the media are for this is also debatable. As with most arguments, there is no way of isolating the media from all other aspects of social life to determine how responsible it is.

Activity
Write a paragraph outlining how responsible you think the media is.

What Is Being Done in the UK to Protect the UK against Cyber-Attacks?

A BBC News article written by Gordon Corera on 14th February 2017 under the title *Cybersecurity: Queen to open centre to protect against attacks*, states: A new centre to protect the UK against cyber-attacks is to be officially opened by the Queen later. The National Cyber Security Centre (NCSC) in London is designed to improve Britain's resilience to attacks and act as an operational nerve centre. NCSC part of intelligence agency GCHQ says the UK is facing about 60 serious cyber-attacks a month. There were 188 attacks classed by the NCSC as Category Two or Three during the last three months although they had not experienced a Category One attack – the highest level. The UK is one of the most digitally dependent economies, with the digital sector estimated to be worth over £118bn per year – so the country has much to lose. The article concludes by saying a five-year National Cyber Security Strategy was announced in November 2016, with £1.9bn of investment.

Activity
The UK government are clearly now taking the issue of cybercrime much more seriously. Do some research to find out more about the initiatives the government has put in place to tackle cybercrime. How successful do you think these initiatives might be?

Exam Hints: *When answering a question such as -*
Outline and assess the role of the media in the amplification of crime and deviance:
You would need to consider the following:

- *Demonstrate accurate knowledge of 'crime', 'deviance' and 'media' – and 'amplification',*
- *Remember that in answering any essay question you should engage in theoretical debate whilst showing active involvement with the research process.*
- *Show knowledge and understanding of theoretical perspectives,*
- *Show knowledge and understanding of concepts such as 'moral panics', 'labelling' and 'self-fulfilling prophecy',*
- *You could include the concept of cybercrime – focusing on moral panics, plus examples to illustrate where cybercrime has been amplified by the media e.g. cyber-attacks on governments. Show your critical awareness of this concept,*
- *Always ensure that you include both analysis and evaluation.*

When answering a question such as –
Outline and assess the role of globalisation in the rise of cybercrime
You would need to consider the following:

- *Demonstrate accurate knowledge of 'globalisation' and 'cybercrime',*
- *Show knowledge and understanding of theoretical perspectives*
- *Show knowledge and understanding of categories of cybercrime, potential problems with tackling cybercrime, given its global nature and initiatives put forward to tackle cybercrime – nationally and globally,*
- *Always ensure that you include both analysis and evaluation.*

Acknowledgements: *This* ***Sociology Factsheet*** *was researched and written by* ***Tina Dixon*** *and published in April 2017 by* ***Curriculum Press****.* ***ISSN 1351-5136***