

1. Review complex types of internet-dependent crimes.

Complex internet-dependent crime is increasing every year, costing businesses and individuals in the UK billions of pounds per year. Although the National Crime Agency have a National Cybercrime Unit which deal with incidents in the UK, police forces and officers are required to deal with incidents initially where evidence is fresh and need to be preserved.

I will begin by reviewing the different types of internet-dependant crime, their impact and different types of offenders and their motivations for committing cyber related offences. I will then discuss the different legislations that such offences may fall into. Finally, I will look at the police response to such suspected offences, procedures and points of contact that should be followed on discovering evidence related to cybercrime.

Internet-dependant or cyber-dependent crime is defined as,

'Crimes that can be committed only through the use of Information and Communications Technology ('ICT') devices, where the devices are both the tool for committing the crime, and the target of the crime (eg. Developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity).' (CPS, 2021)

Cyber-dependant crimes fall into two main categories;

- Illicit intrusions into computer networks, such as hacking; and
- The disruption or downgrading of computer functionality and network space. (CPS, 2021)

Cybercrime costs UK businesses billions of pounds each year and this figure grows year on year. There were over 300,000 reports of fraud and cybercrime in the UK in 2020, reportedly costing individuals and businesses £1.9 billion. The exact cost to businesses and individuals is unknown due to the scale of the crimes and under-reporting of cybercrime. (Comparitech, 2021)

The CyberEdge 2020 Cyberthreat Defense Report (CDR) reported that 82.3% of UK businesses had experienced a cyberattack the previous year (Resource Library, 2021). Although this number is huge, there are many countries with higher figures reported which shows how big the problem is worldwide.

Cybercrime is difficult to police and bring offenders to justice due to it being so widespread and attackers could be operating from anywhere in the world bringing in complications of cross border jurisdiction even if they were to be identified.

There are many different types of cyber criminals which have different motives for committing cybercrimes.

Hackers are skilled individuals or groups who use these skills to access computer systems to commit crimes.

There are different types of hackers with different motives.

Identity thieves, attempt to gain personal information about individuals by different means, to use this information for financial gain.

Internet Stalkers, maliciously monitor online activity of their victims. Motives of this type of offender may vary but they can use the information acquired for bribery, blackmail and slander.

Phishing scammers, obtain personal information of victims for identity fraud scams and financial gain.

Cyber terrorists are highly skilled attackers that usually target businesses and corporate or government systems. These offenders could be financially or politically motivated.

As well as different types of offenders, there are different types of cyber-dependent crimes which I will discuss.

Hacking is an attempt to exploit a computer system or private network. Hackers are intelligent and very skilled individuals with a vast knowledge of computer systems and how to exploit weaknesses in security of networks to enable them to gain entry to the system. Once access is gained hackers can commit several offences depending on their motivations. They could hijack usernames and passwords, steal money, ruin credit, sell information obtained and release malware into the system or network.

Hacking or accessing a computer without permission is an offence under section 1 of the 'Misuse of Computer Act 1990' (Gov.UK, 2021). Other offences under this act or other act may then be committed depending on what the hacker does next.

Malware is software designed to damage computer systems. There are several different types of malwares that do different things. The best-known type of malware is the 'virus'. A virus attacks software, causing harm to it. Viruses are designed to spread easily through internet connections or storage devices.

Another type of malware is the 'worm'. A worm runs in the background of a system, making copies of themselves and damaging the system. Worms can also be spread easily through connections.

Trojans are now more commonly used by hackers as opposed to worms. Trojans can pop up in a screensaver such as a virus scan saying your computer is infected and to 'click here' to clean. Once the user clicks on the link, the trojan takes effect and the offender can take control of the system.

Ransomware is also malware which encrypts the data and prevents the user from accessing the system. This is a way to extort money from businesses and individuals. A financial 'ransom' is then demanded to release the data once paid.

One of the most famous UK and worldwide ransomware attacks was 'wannacry' in 2017 (Fruhlinger, 2021).

Over 200,000 computers in 150 countries had been affected by the ransomware within a day. One of the worse effected organisations was the NHS in the UK. This caused chaos to the NHS systems, affecting hospitals, GPs and pharmacies, leading to delays, cancellations, medical equipment malfunctioning and staff having to revert to pen and paper. The estimated cost of this attack to the UK is reported to be £92 million. (Acronis, 2021).

Phishing is an attack usually disguised as an email from a bank or company the user might be familiar with. The user trusts the email and clicks on a link within the email which may take them to a cloned webpage which again they recognise and trust. The user will then input their details and personal information which can then be captured by the offender.

Denial of service attacks or DOS the offender accesses the computer network, flooding the system with requests and traffic to overload the system. When this is achieved the server may shut down or in the case of popular websites or businesses, prevents visitors from accessing the website or services.

(Mirai botnet 2016)

There are different legislations that different types of cyber-dependant crimes can fall into. Looking into the cyber-dependent crimes I have already mentioned, when carrying out these cyber offences, offenders could be committing offences depending on their intentions and motivations. These are;

Fraud Act 2006

Theft Act 1968 and 1978

Criminal Law Act 1977

Computer Misuse Act 1990

Forgery and Counterfeiting Act 1981

Proceeds of Crime Act 2002

'The Computer Misuse Act' (Gov.UK, 2021) legislation was drafted in 1990 after acceptance by the government regarding the growing threat of cybercrime and the need for computer systems and data contained on them needed to be protected by law.

There are 3 main sections to the act;

Section 1 refers to unauthorised access to computer material. This would cover hacking as the offender is entering the system without permission.

Section 2 covers unauthorised access to computer materials with intent to commit a further crime. This would cover any attempts to steal data or cause damage to a system such as planting a virus.

Section 3 covers 'unauthorised modification of computer material. This section would cover offences where data is deleted or modified, or malware is released into systems which is capable of changing data such as the TalkTalk attack 2015.

The TalkTalk hack is one of the most famous in the UK. In 2015 hackers were able to compromise TalkTalk system and use a SQL injection to access thousands of user's sensitive data. As a result of this TalkTalk were fined £400,000 by the ICO for the breach and in turn lost thousands of customers due to concerns regarding their security. Five people were charged with offences under the CMA, 1990 in relation to the breach (The OU, 2021).

All 3 of these offences require the prosecution to prove the person accused of breaking the CMA INTENDED to access the computer while knowing they did not have permission to do so. The legal concept of intent consists of 2 conditions.

1. The desire to perform a crime
2. The action of attempting to perform that crime.

When faced with potential cyber-dependent crimes which involve devices, as with all crime scenes it is important that officers follow correct procedures to obtain evidence relating to potential offences and preserve this evidence.

The Association of Chief Police Officers (ACPO) provided a good practice guide and set of principles which all officers or anyone investigating digital evidence must adhere to (ACPO, 2012).

Principle 1: No action taken by law enforcement agencies, persons employed within those agencies, or their agents should change data which may subsequently be relied upon in court.

Principle 2: In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

Principle 3: An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Principle 4: The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

There are several different sources of evidence that an investigator may need to seize in relation to offences. These could be laptops, games consoles, storage devices, phones, cameras, sat nav systems and network devices such as hubs, routers and switches.

Aligned with the ACPO principles there are five principles outlined in 'The Electronic Evidence Guide' (Enisa, 2021) that investigators should always follow.

1. Data integrity - Officers must maintain the integrity of evidence at all stages. This would tie in with ACPO principle 1. Any examination processes should be documented in pocket notebook so that these could be replicated if necessary. Evidence needs to be documented, protected, preserved and examined. Volatile data needs to be preserved as much as possible. Turning a device off may lose critical evidence but there is also potential that leaving the device on could lead to evidence being deleted remotely.

Some important steps to take to ensure integrity of evidence.

- All devices should be photographed in the state they are discovered.
- Computers that are turned off should never be turned on.
- Printers should be left to finish printing
- Remove the main power supply from computers if turned off to ensure they are not accessed remotely
- If systems are turned on, document any running processes and photograph, then seek expert advice
- If no expert advice is available the power supply should be removed from the computer without shutting down the computer first.

2. Audit trail – Evidence should be seized in line with force policy regarding property. Evidence should be recorded and placed in evidence bags and sealed then inputted into the property system and placed in a secure location with individual exhibit labels.

Any actions taken with devices by any investigators should be recorded so it can be shown who has handled each device and what exactly they have done to it.

3. Specialist support – Officers need to request this as soon as potential cyber-dependant crime is suspected. Front line officers do not deal with these offences often and may not be aware of correct procedure. There are implications when dealing with complex equipment where evidence needs to be preserved and could easily be lost if correct procedures are not followed.

Gwent police have a SPOC (single point of contact) who can be contacted for expertise and liaison with external units such as NCA, public authorities, communication service providers. The SPOC can provide quality control within an investigation.

Also available within forces for expert advice are the high-tech crime unit which consist of digital forensics, digital media investigators and the cybercrime unit. A point of contact should be established as soon as cyber offences are suspected, for expert advice and guidance on how to manage the investigation.

These units may also need to be involved in the examination of devices further into the investigation.

4. Appropriate training – Training should be given to new officers regarding what to do when responding to cybercrime incidents.

5. Legality – this corresponds with ACPO principle 4 that the 'person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to'.

In conclusion the UK is fighting an ongoing battle against cyber-dependant crime. Criminals and systems are getting smarter increasing the risk and cost to businesses and individuals effected by these crimes. Front line officers do not deal with these offences on a day-to-day or even month-to-month basis. Officers dealing with such suspected offences need to know how to deal with equipment to preserve evidence and who to contact for expert advice and knowledge on the area of cybercrime.

(Word Count, 2128)

2. Evaluate the disruption options available to target criminal activity on the road network.

Criminals are using the national road networks in the UK daily, some are committing offences while driving, others require road access to carry out offences. Road's policing is an effective way of disrupting offences alongside keeping UK roads safe for users and bringing down the number of road related deaths and serious accidents each year. Disruption tactics by the police are needed to deter and identify offenders carrying out these offences.

Policing the roads effectively, is a large part collecting intelligence and using disruption tactics in a bid to disrupt criminality. Criminals rely on the road network as a way of facilitating their 'businesses'.

There are crimes that benefit from the road network more than others. Drug smuggling, human trafficking, child exploitation, moving counterfeit goods, organised crime groups, all rely on using the road network (Roach, 2017). If there was no road network these groups would not be able to operate and move their 'goods' around the country.

In October 2019, the bodies of 39 illegal immigrants were found in a refrigerated lorry in Essex. These people are believed to have been smuggled into the UK from Vietnam by an organised crime group. It is believed that there were previous successful attempts by the OCG to traffic people prior to this tragic incident. These crimes were only discovered due to the driver of the lorry discovering the dead bodies in the back and alerting the emergency services. (BBC News, 2020). This sort of offence is occurring every day on our road network and much of the time is going unnoticed.

The Essex lorry people trafficking incident indicates that it is not just cars and vans that are committing offences on UK roads but also large commercial vehicles.

It is the commercial vehicle driver's responsibility to ensure the vehicle is roadworthy. Police officers and Driving and Vehicle Standards Agency (DVSA) Officers both have powers to stop vehicles and issue prohibitions. To ensure the safety of other road users due to how big and heavy these vehicles can be, it is vital that commercial vehicles comply with regulations that apply to them. If these regulations are not

adhered, due to the size and weight of these vehicles, they could cause serious injuries and even deaths on the roads.

During stops of commercial vehicles, officers can check load weights and type, vehicle conditions, road worthiness, tachograph records to ensure drivers are complying with the rules of regular breaks and rest periods and occupational drivers' licence. Depending on the seriousness of any offences in these areas, officers have powers to issue prohibition notices which could result in immediate immobilising or seizing of the vehicle.

There have been links identified between offending on the roads and other more serious offences. There have been many studies over the years which have validated this link.

In a recent study it was found that 79% of disqualified drivers and 50% of dangerous drivers had other previous convictions. (Rose, 2000).

A study by Junger, West and Timman, (2001) identified links between 'risky' traffic behaviour and violent crime. In a 2018 study it was found that 82% of drug drivers had previous convictions (Nunn, 2018).

This research indicates that policing the roads effectively is an important part of policing and can be beneficial in gaining intelligence and disrupting criminality.

The National Police Chief's Council (NPCC) put together a 3-year strategy for policing the roads, which covers 2018-2021. The objectives listed in this strategy are;

- Safe roads, free from harm.
- Secure roads free from the threat of serious crime and terrorism.
- Efficient roads that promote public confidence and satisfaction.

(NPCC, 2021)

The NCPP's strategy for policing the roads prioritises the 'fatal 4' offences of drink and drug driving, seat belt offences, excess speed and driving whilst distracted (using devices).

The NCPP also highlight the importance of intelligence and information sharing with partner organisations in a bid to reduce the ability of criminals to use the road networks when committing crimes.

Forces in the UK have a dedicated traffic unit which are specifically trained in disruption tactics, advanced driving, and deal with mainly traffic related incidents.

While it is important for response units to know and utilise powers relating to roads policing, traffic units are more highly trained and skilled to deal with issues that response officers might not be trained or authorised to do.

Despite of forces using traffic units, figures show that due to budget cuts and officers leaving, traffic officer numbers are in decline and have decreased by over 30% in the last decade. (Evo, 2017)

Road safety charity 'Brake' has reported that as these number have fallen, so has traffic offences detected.

Brake also state in their findings that 'there is clear evidence that an increase in enforcement will lead to a reduction in both fatal and serious injury collisions. Brake have listed several recommendations to the home office, notably that Roads policing should be prioritised within Police and Crime Plans, the number of traffic officers should be increased and that the NPCC roads policing strategy should be revised. (Roads Policing and Roads Safety, 2021)

There are specific powers relating to road policing and vehicles which officers can implement. Section 163 of the Road Traffic Act, 1988, states that 'a person driving a mechanically propelled vehicle on a road must stop the vehicle on being required to do so by a constable in uniform or a traffic officer'. Section 163 is a very useful power for officers and allows officers the power to stop vehicles randomly, without any cause or suspicion.

There are other powers relevant to stops which allow officers to request information and documents, seize vehicles if necessary and search persons and vehicles. Regular patrols of roads and use of these powers alongside intelligence can help identify criminals and crimes and create further intelligence for future use.

Technology is a very effective tool in policing the roads and attempting to disrupt criminality on the road network. Automatic number plate recognition (ANPR) technology is a very useful tool in roads policing and the fight against crime. ANPR cameras have fixed and mobile locations on roads and can also be found in traffic officer's vehicles. The location of these cameras are not advertised as this could potentially assist criminals who would benefit in knowing their location in order to avoid the cameras.

There are around 13000 ANPR cameras nationally which submit 55 million reads daily (NPCC, 2021). ANPR data is subject to laws which regulate data and stipulate the rules for its usage, 'National ANPR Standards for Policing and Law Enforcement' (NASPLE) and 'National Compliance and Audit Standards for Law Enforcement ANPR' (gov.uk, 2021). These standards were set out by the Home Office to control the use of ANPR intelligence and to protect data of people not committing offences.

ANPR cameras can take information from vehicle number plates and instantly check the index against a database of stored records. Markers can be put on certain vehicles that the police want to locate. If a vehicle of interest triggers one of these cameras an alert is sent to police and police would be able to locate the vehicle and check for any criminality in progress. If a traffic vehicle has ANPR on board and the alert is triggered on their system this can be very effective as they are able to use police powers to immediately signal the vehicle to stop and complete relevant checks. ANPR systems system can flag up stolen vehicles, vehicles used in crime and vehicle used by persons who are wanted or disqualified from driving.

ANPR systems also store records of all vehicles passing a camera. This data is retained for 2 years and can assist officers with ongoing investigations.

ANPR led to the recapture of former royal aid and murder, Jane Andrews after she absconded from prison in 2018. (BBC, 2021).

ANPR has already been responsible for thousands of arrests across the country and has been welcomed by forces in the fight against criminals using the road network. A police spokesperson from North Yorkshire reported that 'during 2018, ANPR directly led to the arrest of 727 suspects and helped safeguard 36 vulnerable people.' (The Northern Echo, 2021).

There are other forms of technology that may also play an important role in roads policing such as CCTV, vehicle tracking which may identify stolen vehicles and average speed safety cameras to regulate speed on the roads and keep the roads safe.

Some forces are using roadside fingerprinting technology as a method of identifying offenders on the spot. This would prevent offenders giving incorrect details to officers and would be correctly identified instantly and check criminal history or if the person is wanted by police.

Traffic Units use pre-planned operations in areas that there is a high volume of traffic. A safe place is identified for the operation and other partnership agencies such as the driver and vehicle standards agency (DVSA) and local council join the force on the day to help improve road safety. Vehicles are pulled over by officers and directed to the operation site where checks are carried out on both driver and vehicles. These operations are very well organised and are effective in increasing road safety by identifying and enforcement of offences.

There are occasions where drivers do not comply with officers' requests for vehicles to stop. The college of policing define a pursuit as being 'when a driver indicates by their actions or continuance of their manner or driving that;

- They have no intention of stopping for the police, and
- the police driver believes that the driver of the subject vehicle is aware of the requirement to stop and decides to continue behind the subject vehicle with a view to either reporting its progress or stopping it.

(College of Police, 2021)

Only officers trained in advance driving may commence pursuit of a vehicle. Traffic officers, trained in advance driving, with suitable vehicles that are fitted with audio and visual warning systems, are authorised to do this but must maintain communication with force control regarding the ongoing situation. Considering health and safety to all persons involved and the public, where possible a pursuit should be avoided. Officers involved in a pursuit should consider the National Decision Model (College of Police, 2020), the pursuit should be proportionate and be able to justify their actions.

To conclude, alongside keeping the roads safe and preventing road related deaths and accidents, roads policing is a valuable tool in the fight against crime.

Criminals rely on the UK road network to facilitate their crimes and this will not stop. The reward for the offenders outweighs the risk of getting caught and they will continue to find a way and take chances to avoid detection by police and authorities. Road policing, information and intelligence and use of technology is imperative for the disruption of criminal activity and serious organised crime.

As there is concerning evidence to suggest depleted numbers of traffic units have influenced the reduction of offences detected and this needs to be addressed as a priority by the home office and UK forces.

Offenders using the roads will never be stopped completely but the more police are using disruption tactics, they will be at an advantage in this area.

(Word count, 1911)

References

- Acronis.com. 2021. The NHS cyber attack: how and why it happened, and who did it. [online] Available at: <<https://www.acronis.com/en-gb/articles/nhs-cyber-attack/>> [Accessed 9 October 2021].
- App.college.police.uk. 2021. Police pursuits. [online] Available at: <<https://www.app.college.police.uk/app-content/road-policing-2/police-pursuits/>> [Accessed 18 October 2021].
- BBC News. 2021. Essex lorry deaths: Two found guilty of killing 39 migrants. [online] Available at: <<https://www.bbc.co.uk/news/uk-england-55399004>> [Accessed 14 July 2021].
- Brake. 2021. Roads policing and road safety. [online] Available at: <<https://www.brake.org.uk/how-we-help/raising-awareness/our-current-projects/news-and-blogs/roads-policing-and-road-safety>> [Accessed 18 October 2021].
- College.police.uk. (2020). National Decision Model. [online] Available at: <https://www.app.college.police.uk/app-content/national-decision-model/the-national-decision-model> [Accessed 19 August 2020].
- Comparitech, 2021. UK Cyber Security and Cyber Crime Statistics in 2021. Comparitech. Available at: <https://www.comparitech.com/blog/information-security/uk-cyber-security-statistics/> [Accessed 2021].
- CPS, 2021. Cybercrime - prosecution guidance | The Crown Prosecution Service. Cps.gov.uk. Available at: <https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance> [Accessed 2021].
- Digital-detective.net. 2021. [online] Available at: <https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf> [Accessed 9 October 2021].
- Enisa.europa.eu. 2021. [online] Available at: <<https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders>> [Accessed 9 October 2021].
- Evo.co.uk. 2021. [online] Available at: <<https://www.evo.co.uk/news/19768/british-road-traffic-police-numbers-on-the-decline>> [Accessed 18 October 2021].
- Fruhlinger, J., 2021. What is WannaCry ransomware, how does it infect, and who was responsible?. [online] CSO Online. Available at: <<https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html>> [Accessed 9 October 2021].
- Imperva, 2020 Cyberthreat Defense Report | Resource Library. Resource Library. Available at: <https://www.imperva.com/resources/resource-library/reports/2020-cyberthreat-defense-report/> [Accessed 2021].
- JUNGER, M., WEST, R. and TIMMAN, R., 2001. Crime and Risky Behavior in Traffic: An Example of Cross-Situational Consistency. Journal of Research in Crime and Delinquency, [online] 38(4).
- Legislation.gov.uk. 2021. Road Traffic Act 1988. [online] Available at: <<https://www.legislation.gov.uk/ukpga/1988/52/section/163>> [Accessed 14 July 2021].

Legislation.gov.uk, 2021. Computer Misuse Act 1990. Legislation.gov.uk. Available at:
<<https://www.legislation.gov.uk/ukpga/1990/18/contents> [Accessed 2021].

News.bbc.co.uk. 2021. BBC - Automatic Number Plate Recognition catches criminals. [online] Available at:
<http://news.bbc.co.uk/local/kent/hi/people_and_places/newsid_8977000/8977235.stm> [Accessed 14 July 2021].

Npcc.police.uk. 2021. [online] Available at:
<<https://www.npcc.police.uk/documents/FoI%20publication/Disclosure%20Logs/Uniformed%20Operations%20FOI/2012/041%2012%20Att%202%20of%202%20Publications%20of%20Fatal%20Accidents.pdf>> [Accessed 14 July 2021].

Nunn, J., 2018. The Criminal Histories of Drug-Drive Offenders. Policing: A Journal of Policy and Practice, [online] 14(2). Available at:
<<https://academic.oup.com/policing/article-abstract/14/2/456/4967630?redirectedFrom=fulltext>> [Accessed 14 July 2021].

Roach, J., 2017. Self-selection Policing and the Disqualified Driver. Policing: A Journal of Policy and Practice, [online] 13(3). Available at:
<<https://academic.oup.com/policing/article-abstract/13/3/300/2951290?redirectedFrom=fulltext>> [Accessed 14 July 2021].

Rose, G., 2000. The criminal histories of serious traffic offenders. London: Policing and Reducing Crime Unit, Home Office, Research, Development and Statistics Directorate.

The Open University. 2021. case study 2: the Talktalk Hack. [online] Available at:
<<https://learn2.open.ac.uk/mod/oucontent/view.php?id=1432225§ion=4.4>> [Accessed 9 October 2021].