social research

Scottish Government
Riaghaltas na h-Alba
gov.scot

CRIME AND JUSTICE

Research Findings
65/2018

Cyber-crime in Scotland: A Review of the Evidence

This desk-based review has found that cyber-technology can impact on any type of crime. Therefore, it is helpful to conceptualise cyber-crime in terms of the method or locus of a crime, rather than it being a distinct type or group of crime. This is in line with the definition adopted by Police Scotland and also the way in which cyber-crime is defined in the Scottish Institute for Policing Research (SIPR) international review.

The review looked systematically at the crime groupings used to categorise police recorded crime statistics. While we have found some evidence gaps and our knowledge is not complete, we have been able to identify four ways in which cyber-technology has impacted on crime in Scotland:

1. Cyber-crime is forming a large proportion of certain crime types.
2. The internet and cyber technologies are changing the volume of certain crime types.
3. The internet and cyber technologies are changing the nature and victimisation of certain crimes.
4. Cyber-technologies have given rise to the introduction of an entirely new and high volume category of crime – computer misuse (incorporates activities involving unauthorised access to and attacks on computer systems, networks and data e.g. hacking and computer viruses and Ransomware).

Applying this to the crime groupings allows us to begin to understand these different types of impact that cyber-technology has on different types of crime, and also where the impact of cyber-technology has been limited:

- Group 1 (Non-sexual crimes of violence): The available evidence suggests cyber technology appears to be having no significant influence on the scale or nature of **non-sexual crimes of violence**.
- Group 2 (Sexual crimes): Cyber-technology has had an impact on both the scale and the nature of some types of **sexual crimes** in Scotland.

- Group 3 (Crimes of dishonesty): **Fraud** is one of the most frequently experienced crimes and a large proportion, although by no means all, is cyber-crime. There is also evidence of underreporting, which is likely linked to incidents generally being viewed as low impact and low harm.
- Group 4 (Fire raising, vandalism etc.): **Computer misuse** is a new category of crime which is almost entirely driven by the growth of the internet and cyber technology (e.g. computer viruses, hacking, Ransomware etc.). However, it is underreported to the police and in most cases impacts and harm are not severe.
- Group 5 (Other Crimes): Cyber technology has not had much of an impact here. There are concerns around the potential impact of cyber on two areas within this grouping which do not appear to have been borne out: (i) **sourcing drugs** (the majority of this is still via traditional means rather than online) and (ii) **contempt of court** issues (there is no evidence from police data that that increases in the amount and accessibility of information online have increased the likelihood of these types of issues).
- Group 6 (Misc. Offences): The impact of cyber technology has been limited. While the internet features in cases of **stalking and harassment**, being pestered, intimidated or insulted in person is much more prevalent than experiences carried out via electronic means.
- For **businesses' experience of cyber-crime**, the available UK evidence is complex. Many organisations collect data on the impact of cyber-crime on businesses, however as there is not consistency in how these data are collected across these organisations, it is not possible to present a robust overview of the impact of cyber-crime on business. Nevertheless, it is clear from the available evidence that cyber-crime is an issue for businesses. For example, whilst not including all sectors, the UK Cyber Breaches Survey estimates that 46% of UK businesses (covered by the survey) experienced at least one cyber breach or attack between 2016 and 2017.
- This review has also identified gaps in our knowledge. We still need to know more about cyber-crime in Scotland, such as the prevalence of different types of cyber-crime, the extent of underreporting, the cost and the harm of cyber-crime.

Cyber influence on crime: Summary of overall findings

Cyber-technology can impact on any type of crime. We conceptualise cyber-crime in terms of the method or locus of a crime, rather than it being a distinct type or group of crime.

From the available evidence, we know that:
Cyber-technology has had an **impact** on

The scale and nature of some types of **sexual crimes** in Scotland

The proportion of **fraud** conducted online. However still a lot of fraud is offline. As a whole, fraud is under-reported and mostly low impact

Computer misuse – now a commonly experienced crime. But it is under-reported and mostly low impact.

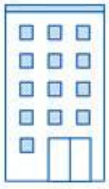
There has been **less influence** of cyber-technology on the following:

Cyber appears to have no real influence on the scale and nature of **violent crime**

Drugs are still mainly sourced via traditional means rather than online.

The internet features in cases of **stalking and harassment** but this is still more prevalent in-person than online.

Information of **businesses'** experiences of cyber-crime is limited and fragmented, however most sources indicate that cyber-crime is an issue for them.



For example, the UK Cyber Breaches Survey, whilst not covering all sectors, estimates that between 2016 and 2017, **46%** of responding business sectors experienced at least one cyber breach or attack.
(Cyber Breaches Survey, 2017.)

Justice Analytical Services

Purpose

This desk-based review aims to contribute to the evidence base and aid understanding of how cyber-technology is impacting on crime in Scotland.

The review is set against the backdrop of a number of recently published strategies which emphasise the challenges and risks of cyber-crime. These include the Scottish Government's Justice Vision and Priorities, Cyber Resilience Strategy and Policing 2026.

To inform this on-going strategic work, a number of analytical workstreams are being undertaken across a range of organisations and this evidence review marks the Scottish Government's contribution to the initial phase of developing an evidence base.

Structured according to recorded crime groups, the review summarises key evidence from a number of existing Scottish and UK sources. It focuses on how cyber-crime is measured, the nature and extent of cyber-crime, apparent evidence gaps and potential evidence sources going forward. The review firstly considers crimes impacting individuals before turning attention to businesses.

What is cyber-crime?

Defining cyber-crime is complex and contentious and there is not an agreed upon definition[1].The main debate centres around the extent to which the internet and cyber technologies need to be involved in order for the crime to be termed 'cyber-crime'. Views on this range from those who argue that cyber-crime is only the distinct set of activities which are committed by using a computer, computer networks or other forms of ICT (e.g. spread of viruses, hacking etc.), to others who view cyber-crime as including even the most minor involvement in more traditional crime types (e.g. using the internet to research how to commit or cover up a violent crime).

Given the remit of this review and the broader cyber-crime analytical work, it makes most sense to adopt a definition that considers criminal activity as cyber-crime if cyber-technology was in any way involved, regardless of the extent of involvement. This approach does not necessarily consider cyber-crime as a separate category of crime, instead it is defined by the method or locus of the crime. This is in line with the way in which Police Scotland conceptualise cyber-crime.

Context - Internet use in Scotland

In order to set the subsequent findings in context, it is important to consider the broader picture in terms of levels of and trends in internet use across Scotland. Whilst the growth of the internet has created many positive opportunities, these are accompanied by inherent risks and the potential to be exploited by criminals.

[1] Wall, D.S., (2017). Crime, Security, and Information Communication Technologies: The Changing Cybersecurity Threat Landscape and its Implications for Regulation and Policing.

- The vast majority of adults in Scotland (84%) reported using the internet for personal or work use in 2016, this figure has remained stable of late but has significantly increased since the 2007 baseline year of 63%[2].
- There is a clear relationship between internet use and age, with use increasing as age decreases. Usage also tends to increase in line with household income.
- There are indications that the public are aware of the potential risks of using the internet, with the majority taking precautions to protect themselves. In 2016 only 7% of internet users noted that they adopt no security measures[3].
- The 2017 Cyber Security Breaches Survey found that 74% of UK businesses[4] consider cyber security to be a high priority for senior management[5] and fewer firms now say it is a very low priority compared to 2016.
- The same survey revealed that the vast majority of UK businesses have cyber security measures in place including applying software updates (92%), malware protection (90%) and firewalls (89%).

Key findings- Crimes affecting individuals

The following provides an overview of the key findings to emerge from the review. Please see the glossary in the main review for definitions of the terms used.

Non-sexual crimes of violence

- The available evidence suggests cyber technology appears to be having no significant influence on the scale or nature of non-sexual crimes of violence.
- There is insufficient evidence to assess the role of cyber technologies in cases of threats and extortion in Scotland.

Sexual crimes

- Cyber technology has had an impact on both the scale and nature of sexual crime in Scotland.
- Estimated that the internet was used as a means to commit at least 20% of all sexual crimes recorded by the police in Scotland in 2016/17.
- Online sexual crimes tend to be concentrated around non-contact offending but the internet may be a precursor in contact sexual crimes e.g. rape, sexual assault.

[2] Scottish Household Survey, 2016

[3] Of those asked about in the Scottish Household Survey

[4] Representative of businesses in scope of the survey, excludes some sectors and businesses with no IT capacity.

[5] 31% very high, 43% fairly high

- Both the number and proportion of police recorded 'other sexual crimes'[6] which were cyber-enabled (internet used as a means to commit the crime) has increased. In 2016/17, 51% of other sexual crimes were cyber-enabled, up from 38% in 2013/14[7].[8]
- This increase has contributed to the growth in police recorded 'other sexual crimes', and sexual crimes as whole between 2013/14 and 2016/17.
- When the specific 'other sexual crimes' of 'communicating indecently' and 'cause to view sexual activity or images' are cyber-enabled:
- Victims and offenders tend to be younger (compared to non-cyber cases), with the majority of victims aged under 16.
- Victims and offenders are more likely to know of one another.

Fraud

- Evidence suggests that fraud is one of the most numerous crime types, but this is not entirely driven by the internet.
- Evidence from the Scottish Crime and Justice Survey (SCJS) shows in 2014/15, 5% of adults reported that they were victims of bank and credit account fraud. This has increased in recent years but the data is subject to caveats.
- Crime Survey for England and Wales (CSEW) data shows 3.2 million incidents of fraud were experienced by 5.9% of adults in the year ending Sept. 2017.
- For the year ending Sept. 2017, the CSEW estimates 56% of fraud incidents were coded as cyber (internet or any type of online activity related to any aspect of the offence), amounting to an estimated 1.8 million incidents.
- As yet no victimisation survey has published data looking specifically at the victims, impacts and reporting of fraud committed via the internet. This could reflect methodological challenges.
- Incidents of fraud (on and offline) are underreported to Action Fraud and the police. This is possibly linked to incidents generally being viewed as having no emotional or physical impact or as an inconvenience (rather than anything more harmful), in addition to the relatively high rates of financial reimbursement.
- There is insufficient CSEW time series data in order to establish any trends in the incidence and nature of fraud including the role of cyber technology.

[6] This is one of four categories Police Scotland use to record sexual crimes - the other three being 'Rape and attempted rape', 'Sexual Assault' and 'Crimes associated with prostitution'. 'Other sexual crimes' are made up of a wide range of sexual crimes, with the three most common being 'Communicating indecently', 'Cause to view sexual activity or images' and 'Indecent photos of children'.

[7] Based on a sample of crimes recorded by the police.

[8] Recorded Crime in Scotland: Other Sexual Crimes, 2013-14 and 2016-17.

Computer misuse

- The term 'computer misuse' is used to capture a number of crimes generally covered by the Computer Misuse Act 1990. Activities grouped under this label mainly centre around unauthorised access to and (sometimes subsequent) attacks on computer systems, networks and data e.g. hacking, computer viruses and Distributed Denial of Service (DDOS) attacks.
- Whilst evidence shows computer misuse to be numerous and fundamentally driven by the growth of cyber technology and the internet, in most cases there is either no resulting impact or such impacts tend to be of low severity.
- The most robust and comprehensive evidence on computer misuse is data gathered via the CSEW, which incorporates incidents of unauthorised access to personal information (including hacking) and computer viruses.
- CSEW evidence shows 1.5 million incidents of computer misuse were experienced by 2.6% of adults in the year ending Sept. 2017.
- Almost all (97%) incidents were coded as cyber (internet or any type of online activity related to any aspect of the offence) for the year ending Sept. 2017, amounting to an estimated 1.46 million incidents.
- Victimisation of computer misuse is generally spread across society but some groups are more at risk including higher income households.
- CSEW evidence shows that in 49% of computer misuse incidents victims identified no resulting emotional or physical impacts and by far the most common impact was a 'loss of time/inconvenience', experienced in 31% of incidents (year ending March 2017)[9].
- Police recorded crime data for Scotland suggests that incidents of computer misuse are underreported. In 2016/17 only 30 incidents were recorded under the Computer Misuse Act 1990.

Other crimes

- Available evidence suggests the vast majority of illicit drug users are still sourcing drugs via traditional means, with a very small proportion obtaining drugs online.
- Concerns that increases in the amount and accessibility of information online would increase the likelihood of contempt of court issues (e.g. jurors finding out information about a case), have yet to be borne out in police data.

Miscellaneous Offences

- Evidence suggests that the internet may commonly feature in cases of stalking and harassment, yet being pestered, intimidated or insulted in-person is much more prevalent than experiences carried out via electronic means.

[9] Emotional and physical impact on victims of incidents of computer misuse, Year ending March 2017, CSEW

- SCJS evidence indicates that of the 9% of adults 'insulted, pestered or intimidated' in Scotland in 2014/15, the vast majority (82%) experienced this in-person.
- SCJS evidence shows that in 2014/15, the most common type of stalking and harassment (arguably more serious than the above) was threatening/obscene texts or emails, experienced by 45% of adults who had encountered at least one form of stalking/harassment in the 12 months prior to interview (6.4%).
- Evidence suggests incidents of harassment and threatening/abusive behaviour are underreported to the police, with many viewing it as 'too trivial'.

Key findings- crimes affecting businesses

- Many organisations collect data on the impact of cyber-crime on businesses, however as there is not consistency in how these data are collected across these organisations, it is not possible to present a robust overview of the impact of cyber-crime on business. Nevertheless, it is clear from the available evidence that cyber-crime is an issue for businesses.

Fraud

- In spite of the challenges highlighted above, it is clear from the available evidence that fraudulent acts are frequently experienced by businesses.
- The 2017 Cyber Breaches Survey found that staff receiving fraudulent emails or being redirected to fraudulent websites was the most common type of cyber breach experienced by UK businesses covered by the survey.
- The 2016 Retail Crime Survey revealed fraud to be the second most commonly experienced crime amongst respondents, accounting for 18% of incidents.
- Evidence suggests the costs of online fraudulent activities are smaller than costs associated with traditional crimes and amount to a minority of total online transactional values.
- The 2016 Retail Crime Survey estimated that 53% of the total cost of fraud was cyber-enabled, representing a total direct cost to the retail industry of around £100 million. This translates to approx. 15% of the total direct cost of crime against retailers.
- UK evidence from Financial Fraud Action hows in 2016, fraud losses as a proportion spent on UK issued cards stood at 8.3 pence per £100.
- For 2016 Financial Fraud Action estimated value of transactions carried out online using fraudulently obtained cards accounted for 9.5 pence in every £100 spent with UK merchants.

Computer misuse

- 'Computer misuse' is used to capture a number of crimes generally covered by the Computer Misuse Act 1990 and incorporates activities such as unauthorised access (e.g. hacking) and attacks (computer viruses).

- The UK-level 2017 Cyber Breaches Survey estimates that 46% of businesses identified at least one cyber breach or attack between 2016 and 2017, but this data is subject to caveats.
- Incidence of such breaches increases with businesses size (number of employees) and turnover, in addition to varying by sector.
- The attractiveness of personal customer data to criminals could be increasing the risks for companies holding such information. The 2017 Cyber Breaches Survey found that 51% of UK businesses holding personal customer data experienced a breach, compared to 37% who didn't hold this information.
- Evidence from the UK 2017 Cyber Breaches Survey shows where businesses experience a breach, incidents of computer viruses, spyware and malware (33%) in addition to Ransomware (17%) are amongst the most common.
- Evidence suggests that staff are viewed as pivotal in the prevention of cyber attacks but are also potentially a weak link in businesses' defences.
- Very few businesses have systems in place to calculate the costs of cyber attacks and there is a lack of consistency in previous research which attempts to estimate costs.
- The majority of businesses identifying a breach do not report them to external bodies and even less report them beyond their cyber security provider. The main reason is that incidents or the impact were thought to not be significant enough.

Conclusions

This review has drawn attention to the increase in the number of people in Scotland using the internet and the potential for criminals to exploit this growth, under the banner of cyber-crime. There is a lack of clarity and consistency in the terminology used around cyber-crime, and moving forward it may be helpful to start to shift the focus towards cyber-crime being seen as the method or locus of a crime, rather than a distinct type or group.

Whilst this review has found that incidents of cyber-crime tend be concentrated around sexual crimes, fraud and computer misuse, a number of different types of crime can and likely do involve the use of the internet and cyber technologies, either as a precursor to a crime or in the committing of a crime itself.

The review has highlighted four key ways in which cyber technology is influencing crime:

1. **Cyber-crime is forming a large proportion of certain crime types.** For example evidence from the CSEW for the year ending Sept. 2017 estimates that over half (56%) of fraud incidents (which is one of the most numerous crimes) were cyber-crimes. This amounts to 1.8 million incidents during this time period.

2. **The internet and cyber technologies are changing the volume of certain crime types.** This is perhaps most evident amongst sexual crimes. Detailed evidence shows that both the number and proportion of police recorded 'other sexual crimes' in Scotland which were cyber-enabled increased. Consequently such incidents contributed to the growth in all 'other sexual crimes' and sexual crimes as a whole.

3. **The internet and cyber technologies are changing the nature and victimisation of certain crimes.** The police recorded 'other sexual crimes' research found that when the specific crimes of 'communicating indecently' and 'cause to view sexual activity or images' were cyber-enabled, both victims and offenders tended to be younger compared to non-cyber incidents. With cyber-enabled incidents, victims and offenders were also more likely to know of one another.

4. **Cyber-technologies have given rise to the introduction of an entirely new and high volume category of crime – computer misuse.** Without the internet, these crimes (including computer viruses, hacking etc.) would not be possible. Evidence from the CSEW for the year ending Sept. 2017 shows there were 1.5 million incidents of computer misuse, making it one of the numerous crimes.

However, we are operating in a complex landscape. The review has drawn attention to the challenges faced by authorities to investigate and take action against online risks. These include inconsistent terminology and the spectrum of possible internet involvement in crimes. Such situations also challenge the capability of research and statistics to accurately capture the scale, nature and impact of cyber-crime.

This review has also identified gaps in our knowledge. We still need to know more about cyber-crime in Scotland, such as the prevalence of different types of cyber-crime, the extent of underreporting, the cost and the harm of cyber-crime. Furthermore little evidence is available which allows for the comparison between cyber and non-cyber incidents of the same crime. This review has also drawn attention to gaps around cyber-crime offenders, in particular the extent to which different kinds of individuals and groups account for cyber-crime offences in Scotland.

Throughout, this review has found evidence that cyber-crime is underreported to the police and other authorities. Figures from the victimisation surveys are consistently higher than in police data, most notably for instances of fraud, computer misuse, abusive/threatening behaviour and stalking and harassment. Suggesting these occurrences are often not being reported to the police. Where apparent, the review has highlighted the possible links between underreporting and the perceived low severity of impacts resulting from many incidents, especially in relation to fraud and computer misuse. Underreporting may be inhibiting the ability of the police to take action and to assign resources accordingly.

Next steps

In addition to this review, a number of analytical workstreams are being taken forward across numerous organisations, including:

- Police Scotland Cyber Capability Review;
- Scottish Institute of Policing Research (SIPR) qualitative research which looks at policing practices from six different countries around the world; and
- HMICS Thematic Inspection of Police Scotland response to Cyber-crime.

Furthermore, there are some encouraging signs by way of emerging evidence sources in Scotland. Principal developments include:

- Police Scotland introduced a cyber-marker to their crime recording systems in April 2016. Police Scotland are currently considering how to enhance how crimes with a cyber-element are marked. Identifying a solution requires challenging the definitions and perceptions of "cyber-crime" and acknowledging the limitation of current legacy systems. Therefore improvement will be incremental as definitions and systems develop.
- The SCJS has the potential to capture crimes that are not reported to or recorded by the police. Whilst the SCJS does currently include a limited number of questions which provide insight on the extent to which the internet and cyber technology was involved in certain incidents, a more comprehensive module on cyber-crime/online behaviour questions will be included in the SCJS questionnaire from 2018/19. This represents an important step in developing SCJS evidence is this area[10]. More information is available in the SCJS 2018/19 Questionnaire Review Paper and the full 2018/19 questionnaire will be published in due course.
- It is likely that private companies and businesses including banks, hold useful information on cyber security and incidents where they have been the victim of a crime which occurred online or via cyber technology. The Scottish Government's Justice Analytical Services division is looking to explore this further.

Going forward it is intended that these developments combined with the above analytical work and existing sources, will contribute to a more complete picture about the influences cyber-technology is having on crime in Scotland.

[10] Will provide indicative findings. Data will not be included in the main SCJS incident or prevalence estimates.

The views expressed in this report are those of the researcher and do not necessarily represent those of the Scottish Government or Scottish Ministers.

This report is available on the Scottish Government Publications Website (http://www.gov.scot/Publications/Recent)

The Scottish Government
St Andrew's House
Edinburgh
EH1 3DG

ISBN: 978-1-78851-710-2 (web only)
Published by the Scottish Government, March 2018

Produced for the Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS382486 (03/18)