The Computer Misuse Act and Hackers: A review of those convicted under the Act

James Crawford

Technical Report

RHUL–ISG–2021–1

10 March 2021

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

Student Number: 100910920
James Crawford

The Computer Misuse Act and Hackers: A review of those convicted under the Act

Supervisor: Dr. Rikke Bjerg Jensen

Submitted as part of the requirements for the award of the
MSc in Information Security
at Royal Holloway, University of London.

I declare that this assignment is all my own work and that I have acknowledged all quotations from published or unpublished work of other people. I also declare that I have read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences, and in accordance with these regulations I submit this project report as my own work.

Signature: 

Date: 24 August 2020

Table of Contents:

Introduction

The Computer Misuse Act 1990 (hereafter referred to as the CMA) was introduced in order to close the 'loophole for hackers' [HC90 col.1135] that had become evident in the United Kingdom throughout the 1980s. Updated in 2006 and 2015, it remains the UK's primary 'hacking law' [ERY12 p.413]. The Parliamentary debates around the introduction of the CMA provided some initial views on who these hackers were thought to be. Emma Nicholson MP commented that hackers, or 'German hackers, at any rate, support a drug-based lifestyle on their activities' [HC90 col.1154]. Dr Moonie MP, a psychiatrist by profession, believed that 'a profound sexual inadequacy is often related to such behaviour' [HC90 col.1156]. Both the nature of these hackers and the Parliamentary view on them have moved on somewhat since 1990, with the threat (and the understanding of the threat) evolving over time:

> 'where a decade ago the public perception of the e-criminal was of a lonely hacker searching for attention, today's 'bad guys' belong to organised crime groups, are highly skilful, specialised, and focused on profit. They want to stay invisible, and so far they have largely succeeded' [HLP07 p.6].

Not all of these hackers, though, have managed to stay invisible: 384 individuals were proceeded against under the CMA between 2008-2018 alone, with 303 convicted [MTCE].

Whether these convicted hackers reflect the stereotypes put forward in Parliament, though, is up for debate. This project aims to go some way to answering the question of who these individuals are through an analysis of the cases of 132 people convicted under the CMA since 2008. An accurate understanding of who is being convicted has implications for both government policy and law enforcement attempts to deal with the threat, as well as serving as a reflection on the effectiveness of the CMA and efforts to enforce it. This is particularly pertinent as 'law enforcement agencies have shown a willingness to make inferences about real-life hackers and their activities from depictions of their fictional counterparts' [YS19 p.56]. A comprehensive review of convicted hackers will also allow for conclusions around the wider hacker population to be drawn.

The core research objectives of this project, then, are to:

- identify the initial aims that drove the introduction of the CMA, particularly focusing on the type of criminals the Act was aimed at;

- provide a definition of a criminal ‘hacker’ and explore the academic literature around them, identifying their key characteristics and traits;
- compare these characteristics and traits with those of the individuals convicted under the Computer Misuse Act; and
- determine whether the CMA can claim to have been a success in prosecuting the individuals envisaged as its primary targets.

Report structure

This project begins by placing the analysis in context, with Chapter 1 providing an overview of the CMA, its origins, and the initial intentions behind the Act: who it was aimed at and what Parliament hoped to achieve by bringing it in. Chapter 2 then provides a definition of hackers and places hacking activity in the context of wider cybercrime. This is necessary to provide a clear framework upon which to base the later analysis of hackers, as well as to provide an initial delineation between those convicted under the Act who can be considered hackers, and those who simply exceeded their authority. Chapter 3 then outlines the methodology used for the central analysis in chapters 4 to 8, including a discussion of its limitations. Chapters 4 to 8 look at key characteristics of the convicted hackers under review, and compare them to the existing academic literature, focusing on the following aspects: skill level; motivation; demographic factors; what relationships these hackers had to their victims and/or other hackers; and whether they fit into existing academic typologies. The conclusion then draws together the key findings from these chapters.

It is worth noting that this project is not intended as a legal overview of the CMA, or an analysis of the difficulties of policing or convicting criminals under the Act (except where these issues are likely to have an impact on the profiles of the individuals convicted). This is effectively covered by Walden [IW16], amongst others. Instead, the focus is on the individuals against whom the Act was aimed; and against whom it has come to have an impact.

Chapter 1 - The Computer Misuse Act 1990

This chapter outlines the genesis of the CMA, showcasing its intended role as both a practical measure and a public statement against the emerging hacking threat. It showcases its historical context and intent, drawing out relevant themes for an analysis of the CMA and those individuals prosecuted under it.

The CMA was given Royal Assent on the 29 June 1990, having started its journey in Parliament as a Private Members' Bill introduced by Michael Colvin MP [HC90]. The Bill was based on two studies produced by the Law Commission in 1988 and 1989 [LCW88, LCR89], as well as one by the Scottish Law Commission published in 1987 [SLR87]. Section 1 of the Act criminalises "unauthorised access to computer material" and section 3 "unauthorised modification of computer material" [CMA90]. The offence in section 2 is a more serious version of section 1 where there is an 'intent to commit or facilitate further offences' [AP04 p.3].

The CMA was updated in the Police and Justice Act 2006 (coming into force in late 2008), which: increased the maximum penalties under the Act; amended section 3 from prohibiting the unauthorised modification of computer material to one 'concerning unauthorised acts with intent to impair the operation of a computer' [SF08 p.54]; and finally, brought in a new Section 3A offence which criminalised making, supplying or obtaining articles for computer misuse purposes [CMA90]. Further amendments were made as part of the Serious Crime Act 2015, including significantly greater sentences where acts caused serious harm [IW16 p.186].

A necessary Act?

The immediate trigger for the CMA's introduction in 1990 was the case of *R vs. Schifreen and Gold* [RGS88]. Schifreen and Gold, a freelance journalist and an accountant, used weak passwords to obtain unauthorised access to BT's Prestel system in order simply to 'cause mischief' [MW12 p.399]. Initially convicted under the Forgery and Counterfeiting Act 1981, the House of Lords overturned the convictions in 1987, with Lord Lane CJ criticising them as a 'procrustean attempt to force the facts of the present case into the language of an Act not designed to fit them' [RGS88]. This judgement gave the case of legislating against computer misuse impetus as it had 'established that computer hacking, as such, was not an offence under the existing criminal law' [MW00 p.274]. Indeed the Law Commission had considered the judgement in *Schifreen and Gold* so important that they had paused the drafting of their working paper while the case was heard in the Lords, but 'once the

house had dismissed the appeal, the pressure was on to produce firm proposals to fill the gaps' [MW12 p.400].

While this judgement had clearly highlighted a gap [SF06 p.429], in that computer trespass was not in itself illegal, existing legislation had until then held up rather well in the face of the new forms of criminality posed by the computer. Working papers from both the Scottish and English Law Commissions had initially been sceptical of the need for additional legislation [LCWP 3.64; also, MW12 p.402], believing existing laws would cover any malicious activity. Others, such as the Data Protection Registrar, took the view in the late 1980s that mere access to a computer network causing no damage was not a criminal act in and of itself [DH01 p.113]. Even after the judgement on *Schifreen and Gold* in the Lords, doubters remained [see MW91 pp.74-75]. Some argued that hackers could, and should, have been found guilty of the theft of electricity [SF06 p.429]; and Harry Cohen MP, as the sole Parliamentary voice opposing the introduction of the CMA in the 1990 debates, gave voice to further concerns around the breadth and wording of the Bill [HC90 col.1163]. Nevertheless, the arguments for legislation carried the day, with Colvin's Bill receiving 'swift and favourable' passage through Parliament [MW p.403].

The debate around the necessity of the CMA is of continued relevance as it reflects the fact that hacking was often a precursor to other criminal activity (e.g. fraud, theft) and hence the criminal activities of individuals could be prosecuted under other legislation [DW07 p.54]. This clearly remains the case today; the vast variety of cases on the Cambridge Computer Crime database [CCCD] shows that hacking offences often form part of a wider suite of criminality activity; and that a large number of these individuals are not prosecuted under the CMA but rather under other legislation relevant to their further criminal acts [see also HO15]. A recent example of this was sentencing of five fraudsters on 28 February 2020 who used malware to steal the login credentials of email accounts in order to dupe their victims into misdirecting large transfers of money [case details on CCCD]. These five individuals were charged with conspiracy to commit fraud and conspiracy to convert criminal property. Not all hackers, then, are prosecuted under the CMA; and the individuals prosecuted for other offences will fall outside of this project. For a discussion of the relevant legislation and how it interacts with the CMA, see Walden [IW16 pp.120-158].

<u>Reasons for its introduction</u>

The Law Commission outlined, in their opinion, the key reasons as to why the CMA was required:

> "the most compelling arguments for the criminalisation of hacking are those stemming from, first, the actual losses and costs incurred by computer system owners whose security systems are (or might have been) breached; secondly, that unauthorised entry may be the preliminary to general criminal offences; and thirdly, that general willingness to invest in computer systems may be reduced, and effective use of such systems substantially impeded, by repeated attacks and the resulting feeling of insecurity on the part of computer operators." (LCR 2.14)

Similar points were put forward during debates in Parliament, with Colvin noting how closely he had relied on the Law Commission's work in his Bill [HC90 col.1136]. Colvin and others argued that: computer misuse cost UK PLC up to £2 Billion a year [HC90 col.1134]; hacking had a chilling effect on information sharing [HC90 col.1135]; and the UK was falling behind other jurisdictions [HC90 col.1155]. The latter has come to be seen to be particularly important: Walden has stated that 'the primary motivation for government support [for the Bill] was probably a belief that if the United Kingdom did not follow the example of many of its European partners then the UK's position in the European information market could suffer '[IW01 p.282]. These arguments were echoed in particular by industry [MPC16 p.1], members of which provided advice to the Law Commission.

The nature of this advice is instructive. After requesting that they be provided with 'chapter and verse' to enable them to assess the need for new legislation, the Law Commission lamented the lack of any specific evidence that had been forthcoming (generously attributing it to the security concerns of the respondents) [LCR89 1.9], despite the fact they had 'received a record number of submissions' [MW91 p.vii]. This demonstrates that the fear of hacking was, at this point, largely based on supposition rather than the actual experience of industry. This lack of clear knowledge of the problems was not quickly overcome: even in 2004, Derek Wyatt, the Chairman of UK All Party Internet Group (APIG), made the point that 'officially, the government is not aware of exactly how big a problem cybercrime is' [cited in DW07 p.17]. This lack of evidence comes in for criticism from MacEwan, who notes that the sharp about-turn between the Law Commission's working paper and its final report was largely based on 'confidential counsel from interested parties' [NM08 p.5]. These issues were reflected in debates in the House of Commons, where evidence was scant. Colvin's figure of £2 Billion, noted above, was £1.6 Billion above the Confederation of British Industry's own estimate; with the reason for the increase 'unclear' [SF09b p.31]. Indeed, the majority of the risks put forward in the debate 'could be argued to be somewhat sensationalist' [SF09b p.33]. Evidence from an M&S spokesman was cited in debates, despite the fact M&S had not at that point

suffered any form of cyber-attack [HC90 col.1143]. Nevertheless, 'industry and commerce lobbied very hard for the Act at the time' [MW00 p.272].

Coupled with this, the Bill was pushed through both Parliament and the Law Commission at quite some speed. Once the argument had been won, the 'widespread view [was] that the problems associated with computer misuse [were] sufficiently serious to justify the accelerated consideration of any possible legislation' [LCWP 1.13]. The Law Commission diverted additional resources to their working paper, but the hastened timetable meant they did not accompany the report with a draft bill [LCWP 1.13]. Cohen MP noted this as a flaw in the Bill, accusing Nicholson MP of having 'harassed' the Law Commission into rushing out the report [HC90 col.1163]. The frenzied birth of the Act, based on speculation and a lack of evidence, highlights the fact that the nature and shape of the threat Parliament was legislating against was largely unclear. While there was a general belief that this threat existed, it had not yet coalesced into any meaningful form. This implies, then, that the introduction of the Act at such speed was as much of a PR exercise intended to placate rising fears as it was intended to bring about prosecutions.

Managing public opinion

The hacker had also caught the imagination of the public. Indeed, Wasik, in a contemporaneous and comprehensive review of the debates and issues around the introduction of the CMA, identified the 'remarkable manner in which public and media attention [had] been gripped… by the phenomena of computer misuse' [MW91 p.3; also SF09b p.31], noting that these were 'fears which [were] often held largely in ignorance of the key facts of computer misuse' [MW91 p.4]. The debates took place during the rise of the 'early second-generation hacker films' (War Games, 1983, Electric Dreams 1984; Real Genius 1985; Weird Science 1985; Ferris Bueller's Day Off 1986, Sneakers 1992, Independence Day 1996 '[DW07 p.15]. These films 'typically identified the hacker as a young genius, usually a misunderstood male teenager, who used technology to put wrongs right and usually have some fun while doing so' [DW07 p.15]. This was an image, it is clear, that the Law Commission and Parliament wanted to combat: it was time to 'dispel any lingering belief that the computer hacker [was] some sort of Raffles of the microchip' [HC90 col.1142]. These Hollywood representations were seen as representative of genuine risks: War Games was presented to the US Congress as an example of the threats emanating from hackers [YS19 p.56].

Throughout this period, Wasik states that 'public attitudes… seem to [have been] varied and complex' [MW91 p.18-19]. Parliamentarians were fighting against the 'barely concealed public admira-

tion ʼfor the hackers and their crimes [MW91 p.19], and they lamented that amongst the general public it was clear that hacking was ʻoften thought of as being entirely innocent and, in some cases, just good clean fun ʼ[HC90 col.1147]. Nevertheless, there was a growing public awareness of the threat [LCR89 1.3], where 'horror stories abounded concerning vast commercial frauds being perpetrated, allegedly by the application of electronic wizardry; and fears were raised that outsiders, known as hackers, could with relative ease break into computer networks and cause untold loss and damage' [SLC87 1.1]. A hacker, Matthew Bevan, was described in the course of a US Congress hearing in 1996 as 'possibly the single biggest threat to world peace since Adolf Hitler' [DW07 p.24]. Bevan, commenting later, stated that he believed his 'case was not about hacking, but an exercise in propaganda' [cited in DW07 p.24]. Fears were exacerbated by a scare-mongering press [MW p.496], and it was this perceived threat that gave strength to the 'ideology of regulation' [DW07 p.16] that formed the basis for legislative action [SF09a p.3; IW16 p.178]. This has been argued as a clear case of hacking being, as Yar and Steinmetz term it, 'actively constructed' [YS19 p.54] by HMG, industry, and the media [see also KS16 p.178ff; MR11 p.232].

Banks goes further, with his article (he claims) 'demonstrating how state-corporate powers ideologically manipulate technocrime and technocriminals to service the needs of informational capitalist economies' [JB18 p.112]. Banks' article provides little evidence and is largely limited towards expressing the unfounded allegations of the conspiracy theorist, crediting establishment parties with an agency, consciousness and coordination that is unlikely. However, it is clear that around the introduction of the CMA there were a number of parties with vested interests taking active steps to elide the hacking community with criminality in the public consciousness. This was not a battle easily won: the conviction of Mafiaboy, in Canada in 2001, showed the general public still held a sneaking admiration for the hacker, while the ambivalence of the jury in *R v. Bedworth* is seen as demonstrative of the continuing attitude of the British public [DH01 p.115; see similar in MY06 p.26]. The legislature and executive were still trying to demonstrate that hackers 'are not so-called computer buffs or nerds, they happen to be criminals' [judgement in *R v. Vallor*, cited in BN03 p.402]. Indeed, the CMA emerges as much as a way point in a cultural battle against the hacker as a piece of criminal legislation intended solely to enable prosecutions. This is a view backed up by Taylor, who argues that ʻthe Billʼs introduction had more to do with a desire to be seen to be doing something about the problem ʼand that parts of the parliamentary debate amounted to little more than a degradation ritual [PT p.130 ff].

<u>Prosecutions</u>

While the CMA was, at least in part, a statement of intent from the UK Parliament and a public relations exercise to combat the ambiguous public profile of hacking, it was nevertheless also intended to achieve law enforcement outcomes and bring criminals to justice; and there is little doubt about who the legislation was aimed at. As outlined in the introduction, the 'hacker' was the threat at hand and the debates in Parliament were entirely around 'hacking' (*a la* the popular definition) and the great fear of it [e.g. HC90 col.1136]. The Law Commission made clear their work was intended to address the 'activity colloquially referred to as computer 'hacking'', which was essentially the 'obtaining of unauthorised access to a computer' (LWP 1.10, similar definition in PST90 p.1]. The hacker in the consciousness of the Commons was a clear threat that needed to be robustly mitigated, with international hacking conspiracies dredged up in order to illustrate the point [HC90 col.1152-3]. While some stakeholders, such as the Data Protection Registrar, expressed concerns that juvenile offenders would be disproportionately caught by the Act [DH01 p.113], and others worried that the Act was too broad [HC90 col.1163-68], the vast majority of Parliamentarians agreed on the need to bring offenders to justice. While external hackers were not the only ones caught under the CMA- the legislation was also 'apt to cover the employee or insider as well '- the 'thrust of the basic hacking offence [was] aimed at the remote hacker'[LCR89 3.35; also HC90 col.1138]. The focus on the outsider was intellectually justified by the nature of insider crime; any crimes committed by insiders for e.g. financial gain or revenge were argued to be covered by pre-existing legislation [HC90 col.1161].

The best evidence for the relevance of the CMA for bringing about prosecutions, however, is the fact that it is still in use today and has been sporadically updated in order to ensure its continued relevance. The lack of a clear framework from the Law Commission and fact it was a Backbenchers Bill, means that it would have been no surprise should the Act have been deemed unsuitable and replaced in fairly short order. However, despite initial concerns that the CMA would need to be the start of a 'package of Computer Misuse legislation' [HC90 col.1148], initially low numbers of prosecutions (around 100 in the first decade) [SF09b p.49-50], and later commentators stating that the Act has suffered egregiously at the hands of technical progress [SF06, MPC], it has only been updated twice. The first, as part of the Police and Justice Act 2006, made black and white the hither-to grey area of denial-of-service attacks, rendering them illegal; while also increasing potential sentences across the board [PJA06]. Alongside this, the new section 3A offence also sought to 'criminalise the creation, supply or application of 'hacker tools' for use in computer misuse offences' [SF08 p.60].

The relevant debates in Parliament ahead of updates to the Act in 2005 show a continued focus on a growing remote threat [HC05 col.1293-1295] and a desire to move the image of the hacker away from a bedroom-bound teenager [HC05b col.699]. The thrust of the debates remained the same as in 1990 [SF09b p.69], although with renewed vigour now that the threat seemed to have grown [APPG p.15]. The 2015 update, as part of the Serious Crime Act, introduced section 3ZA which covered acts that caused, or created a significant risk of, serious damage to human welfare, the environment, any economy or to the national security of any country [SCA15]. This was punishable by up to 14 years in prison. The Serious Crime Act also created an additional territorial dimension. These updates reflected the increased reach of networked systems into lives, economies and government machineries, and hence increased potential for damage. While the CMA has certainly been criticised throughout its 30 year existence [see NM08, SF06], it remains the 'leading statutory measure in the field' [IW16 p.19] and is the 'principle instrument for the conviction of those charged with computer-related offences' [MPC p.5]. Writing in 2000, Walden stated that the Act 'had been successfully applied against the range of offences for which it was envisaged' [IW00 p.290]. While hackers and computer criminals can and are prosecuted under other relevant legislation, the CMA clearly remains a valid tool in the prosecutors box. From inauspicious and fuzzy beginnings, it has aged well over the thirty years of its existence and, while there have been some updates of significance, the original force of the Act continues to be of relevance.

Conclusion

This chapter has drawn out four main conclusions:

- First, the CMA remains largely intact as a tool for prosecuting hacking activity, thirty years after its inception. While it has come in for criticism, and it has been updated to increase its effectiveness as new threats have emerged (e.g. DDOS; longer sentences as risks have increased in line with dependence on networks), it essentially remains the same Act as was introduced in 1990 and is still used as the basis for prosecutions.
- Second, the CMA was specifically brought to life in order to battle the remote threat. While the insider threat was acknowledged as included under the CMA, the thrust of the debates around the introduction of the Act clearly show that they were not the primary target. These first two conclusions provide a clear basis for the research objectives in this project: the CMA was intended as a tool for prosecuting remote hackers capable of significant disruption.
- Third, the CMA never was, and is not today, the only legislation under which hackers could be prosecuted. The debate around the necessity of the CMA reflects the fact that hacking is often a

precursor to other criminal activity (e.g. fraud, theft) and hence nefarious activity is often caught under other legislation. The implications this has for the representativeness of the criminals analysed as part of this project is discussed in the limitations section of the methodology.

- Fourth, the CMA was not just intended as a tool for prosecutions, but also as a clear societal statement that hacking activity was unacceptable and that hackers were criminals. As such, the effectiveness of the CMA should not be solely judged on how many people have been convicted under it, or who these individuals are.

Following this analysis of the origins and intentions of the CMA, this project will now examine the evolution of the term hacker and attempt to reach a definition, before moving on to the central analysis.

Chapter 2 – Hackers: An attempt at a definition

A suitable definition of a 'hacker' is needed to underpin this analysis. This is largely due to the need to differentiate between those who have conducted hacking activity, and those who have simply exceeded their authority (e.g. unauthorised use of authorised access). The terms 'hacker' and 'hacking' come, in 2020, loaded with negative and criminal connotations. This was not always the case: the term hacker started out 'first and foremost, as [describing] ardent (if quirky) programmers, capable of brilliant, unorthodox feats of machine manipulation '[HN04 p.190]. The 'hacker ethic 'was egalitarian, anti-authoritarian, emphasised free access to computing resources, and believed in the power of computers to transform lives and societies for the better [HN04 p.191; for further discussion of the hacker ethic, see KS16 p.25 ff.; SM06 p.233; AC96; PT01 p.60; PT99 p.24; TFL15 p.70]. Some hackers lamented those who used their skills for criminality, derogatorily naming them 'crackers '[YS19 p.54]. However, over time, the term was appropriated by the mainstream media to signify those involved in criminality [SH12 p.1470; for a history of hacking see KS16 p.7 ff.]; and the Jargon File lamented that 'unfortunately many journalists and writers have been fooled into using the word 'hacker' to describe crackers' [ERJF; further in PT99]. Decades later, the term has evolved to the point where it is, in common parlance, intrinsically linked to criminality; and it is with this modern connotation that this project uses the term. The evolution of the term is well-covered in the academic literature [HN04, AC96, DH97, TFL15, YS19]; and it should be noted that the hacking community itself remains defiant in drawing a distinction between hacking and criminal hacking [TFL p.75].

In terms of what constitutes hacking, Furnell has stated that 'at its core, hacking refers to activities involved in attempting or gaining unauthorised access to IT systems,' [SF12 p.173] while Wall states that 'hacking generally describes deliberate unauthorised access to spaces over which rights of ownership or access have already been established. The primary aim of hacking is to breach the security of a networked computer system by assaulting its integrity' [DW07 p.53; DW01 p.3]. Taylor uses a simple definition, citing hackers as those who 'illicitly access other peoples' computers' [PT00 p.36]; and the basic definition of hacking as 'computer break-in' is one that Yar and Steinmetz, writing in 2019, consider to be both clear-cut and widely accepted ('a fairly definite and unambiguous starting point'), although they acknowledge that its history is 'deeply contested' and that even to this day the term 'hacker' still has a multitude of definitions within the hacker community [YS19 p.53-54].

This project contests that a definition of hacking is not quite so easily arrived at. There is a difference between computer break-in [YS19] and obtaining unauthorised access to IT systems and spaces (DW07; SF12): an individual may have authorised access to a computer system/space, yet not be authorised to access all of the data held on the system unless for a specific purpose (such is the case with databases held on Law Enforcement systems, for example). An individual should only be considered a hacker where the criminal act included the circumvention of a security control, however limited. These definitions also do not take into account 'a number of important, illicit activities usually associated with hacking but which do not, in fact, require unauthorised access or a break-in to a computer system' [YS19 p.62]. These include, for instance, denial of service attacks and the distribution of malicious software. These activities are intimately linked with the activities of 'hackers' in the popular consciousness and, indeed, are criminalised by the CMA. As such, this project provides a separate definition of a hacker: as someone who subverts technical security controls in order to commit, help to commit, or attempt to commit, unauthorised and illegal acts which undermine the integrity and/or proper functioning of an information system (most prominent amongst which is gaining unauthorised access).

This quest for a definition is not just an academic exercise: it is highly relevant to this project due to the large number of individuals convicted under the CMA for using authorised access for unauthorised purposes. Of the 132 cases examined, 32 involved unauthorised access to, or use of, data without the circumvention of any security controls (this includes where this authorisation had been presumed to be removed). These individuals cannot be considered hackers in any sense of the word, and are predominantly law enforcement officials who misused police systems. They make up a substantial proportion of those convicted under the CMA (32 of 132), were clearly not the intended targets of the Act, but nevertheless have fallen foul of it. This boost in prosecutions has the impact of significantly inflating conviction rates under the CMA, leading to an inaccurate reflection of the CMA's effectiveness against the hacking threat. For the remainder of this project, the 32 individuals who cannot be considered hackers are largely removed from the analysis. Where individuals used the credentials of others to gain access, or they conducted activity beyond the scope of simply unauthorised access to data (e.g. modifying data), they are included as hackers under the definition above.

It is also important to note that the hacker is just one star in a galaxy of cyber-criminals. While 'cybercrime is most popularly associated with the acts of hacking and virus-writing' [IW16 p.39], the term encompasses a broader swathe of actors than that [for specific discussion on the term cybercrime, see GF06 and DOB19]. Cybercrime has been dismissed as 'at best… a general label for

many emerging and evolving types of IT crime' [SM06 p.17], Smith, Grabosky and Urbas [SGU04] provide a more structured definition. They define it as entailing conduct proscribed by legislation and/or common law as developed in the courts, that: involves the use of digital technologies in the commission of the offence; is directed at computing and communications technologies themselves; or is incidental to the commission of other crimes [SGU04 p.7]. This essentially covers computer content crimes, computer-assisted crimes, and computer-integrity crimes [DW09 p.xviii; also. JH11 p.167-168, PC06 p.483]; or, to put it more memorably, cyber-violence, cyber-obscenity, cyber-theft, and cyber-trespass [DW99]. Thomas and Loader focus on the individual, dividing cyber-criminals into three categories: these are 'hackers and phreaks; information merchants and mercenaries; and terrorists, extremists and deviants' [TL00 p.6-7].

These categories are clearly overlapping and cyber-criminals carry out different 'combinations of illicit actions in the course of committing abuse, attacks and/or crimes' [SM06 p.133; also YS19 p.60-62]. For instance, extremists may use hacking techniques in order to obtain information or disrupt services; or those committing content-related crimes may use hacking techniques to obfuscate their criminality. In reality, the overlapping nature of the activity of cyber-criminals makes it difficult to comfortably categorise them under neat headings; indeed, it is likely that the vast majority of those convicted under CMA committed hacking offences in order to further other criminal ends. In this context, it is open to debate whether an individual should be considered a hacker. However, harking back to the definition, for the purposes of this project an individual will be considered a hacker where they have subverted a technical control in order to further criminal ends (e.g. not including those who have used authorised access for unauthorised means).

These fuzzy boundaries are reflected in the academic literature, where it is often difficult to determine where the line is drawn between hackers and cyber-criminals, with the two regularly conflated in various studies of their characteristics and crimes. As such, due to the difficulties in separating both the crimes (e.g. hacking as a precursor crime for other types of criminality) and the literature (e.g. studies that provide an overview of cyber-criminals, including hackers), this section will tend towards inclusion over exclusion. Nevertheless, the terms 'hacker 'and 'cyber-criminal 'are used deliberately throughout the project, reflecting the scope of the texts referenced.

Conclusion

This chapter has highlighted three key facets, beyond the definition provided above, upon which the resulting analysis rests:

- those who have not subverted any technical controls are not considered hackers. For example, a member of a police force who uses their own account and access rights to accessed data outside of their legal or policy remit is not, for the sake of this project, considered a hacker.
- any individual, however, who subverts a technical control to commit a criminal act is considered a criminal hacker, no matter how mundane (e.g. using an account belonging to another user). This is a significant move away from the original definition of a hacker, discussed above; nevertheless, if an individual is guilty of criminal hacking as defined above, then they should be considered a hacker.
- where hacking forms only part of the criminality (e.g. as part of a conspiracy to commit fraud or theft), these individuals are considered hackers.

Following this discussion of definitions, the next chapter outlines the methodology employed to (1) collect the required data and (2) conduct the analysis.

Chapter 3 - Methodology

A review of the current academic literature around hackers (discussed below) draws out a number of key areas of debate or interest around the profiles of hackers. These are:

- the motivations behind the actions of hackers;
- the demographics of hackers;
- the skill level of hackers;
- whether hackers act alone or in groups;
- differences (motivation, skill, demographics) between convicted insider and outsiders; and,
- whether hackers can be seen to fit into the typologies previously developed by academics.

These aspects are subject to review below, with each chapter beginning with an overview of the academic literature relevant for the area under examination, outlining previous studies and their conclusions. The academic literature is then compared to this project's analysis of those convicted under CMA.

Methodology and Sources

The analysis in this project is based on a qualitative review of 132 cases that resulted in convictions under the CMA between 2008 to the present day (2020). With no central repository of cases held on any government or legal website, the starting point for identifying these cases was Michael Turner's website, www.computerevidence.co.uk [MTCE]. Turner is a long-standing expert witness around computer evidence, and his website provides the names of the individuals convicted under the CMA, summaries of the cases, and links to further information for a large number of cases during this period. All of the cases referenced on MTCE for this period (2008-2020) were included in this analysis, and these were augmented by a number of others identified via Alice Hutchings' work on compiling the CCCD (with the most recent convictions under the CMA chosen).

Once a sufficient number of individual cases of relevance had been identified, searching of the internet and legal databases (e.g. LexisNexis) was used to identify the available material pertaining to the case. The results of this largely consisted of the relevant media coverage, alongside a small smattering of court records and appeal documents (relevant sources can be found in Appendix A).

The amount of information on each case was found to vary considerably depending on the profile of the offender and offences. Once the maximum amount of information had been identified for each case (within the constraints of feasibility) the cases were examined individually. This involved reading and analysing all relevant documents in order to identify information around the following facets:

- the nature of the case;
- an approximation of the skill of the offender;
- the basic motivation of the offender;
- whether the offender was an insider or outsider;
- the age and gender of the offender;
- whether the offender operated alone or in a group;
- whether the offender had identifiable mental health issues;
- whether the offender fitted the various academic typologies put forward for hackers;
- and, finally, based on the above parameters, whether an individual should indeed be considered a hacker or not.

Once these aspects were drawn out of the relevant articles and documents, they were compiled into the table at Appendix A. These results were then analysed and grouped together in order to draw the wider conclusions in chapters 4-8. These results, and further specifics around the methodology for each section, are outlined below.

Limitations

There are numerous limitations associated with this methodology. Firstly, not all cases over this period have been examined, although this project covers a fair proportion of those convicted. More pertinent is that the number of individuals convicted under the CMA is extremely low compared to the number of crimes believed to have been committed over the period. Indeed, one source has estimated that less than five per cent of all computer offences are reported [DH p.101], let alone lead to a conviction. This is an issue across many studies that attempt to analyse data linked to cybercrime: as Wall states, 'the distributed environment in which cybercrime thrives undermines conventional methodologies for collecting data '[DW07 p.17] and there is largely a lack of any form of officially recorded statistics [DW01 p.7]. The sample size, then, is likely to be extremely small compared to the delinquent population. Coupled with this, Hutchings and Chua state that 'cases brought

before the courts are unlikely to be representative of the larger population of offenders who are not apprehended or prosecuted' [HC17 p.185]. Part of the reason for this may be, in line with the view amongst a Russian hacker community, that 'really competent hackers… would never be caught… the young men who are already exposed and convicted of cybercrime are scornfully called lamers, not hackers' [VBS00 p.77]. Highly skilled hackers are unlikely to leave evidential trails and are also likely to take advantage of the extra-territorial nature of hacking to commit crimes in jurisdictions where the odds of being apprehended are limited (e.g. Russian hackers targeting Western countries) [see discussion in NK06 p.36]. While this is offset slightly by the fact that police resources are likely to be directed against the most dangerous hackers, and hence some highly skilled hackers are likely to have been convicted, the corollary of all of this is that this project should in no way be seen as providing a conclusive or representative outline of the whole gamut of hackers; rather it provides a small snapshot of UK based hackers that is likely to be inherently skewed by the very fact of their conviction.

Another aspect that is likely to skew the data is the reliance on media reporting for information; as Wall states, media discourses are based in 'FUDmongering 'as much as in fact [DW07 p.24; SM05 p.436; DW01 p.10]. However, there is no central repository of documents relating to all cases convicted under CMA, and details around the cases are largely only practicably available through newspaper reports. The impact of this for each individual case has been mitigated by solely examining the facts underpinning the articles, but this does not escape the fact there is likely to be a bias in the data around the types of cases covered (e.g. those that newspapers deem to be worth covering). For instance, it seems logical that all of those who committed the highest profile and most destructive activity are captured in the data as their stories will have been deemed worth reporting, whereas the smaller fish may have escaped the net. As such, it is difficult to say whether these cases are themselves representative of the wider convictions under CMA. Some details of relevance may also be omitted from reports (e.g. around the mental health of the offender), and hence some of the data may be incomplete.

The qualitative methodology is also more suited to some aspects of the analysis than others. While some facets are straightforward (age, gender), others such as motivation and skill level are more complex questions. While, as Bloombecker points out, 'motivation can often be inferred from the outcome of the criminal activity' [JB90 p.39], the cognitive reality behind a single individual's actions could form the basis for a 20,000 word project in itself. Without a clear knowledge of the controls circumvented and the methods used, it is also difficult to understand exactly how skilled each

individual hacker is. Nevertheless, enough information around these aspects is discernible to make an examination worthwhile: a hack being conducted for payment on behalf of a third party is clearly indicative of at least some financial motivation, while an individual who uses openly available tools without obfuscating their home IP address is unlikely to be highly skilled.

Despite these limitations, the methodology proposed in this project still has merit. The individuals covered remain representative of sections of the hacking community, however vilified by others in their field. This is also an area of study in which a large degree of uncertainty exists, as outlined in the introduction. Moitra, writing in 2005, claimed that finding out who hackers are is 'the most intriguing question since we know very little about [them] and also because the prospect of knowing much about cybercriminals is particularly dim given the extraordinary anonymity on the internet ' [SM05 p.439].

All relevant references for the individual cases discussed below can be round in the table at Annex A.

Chapter 4 - Skill

Walden states that the ‘three widely-accepted variables said to drive criminal activity are motivation, opportunity and skill' [IW16 p.62]. This chapter focusses on the latter. As Moitra states, skill ‘is particularly important in cybercrime since a vulnerable, unguarded site may provide an opportunity, but unless the cybercriminal has the requisite skills, he or she will not be able to take advantage of that opportunity’ [SM05 p.449]. Nevertheless, set against the public perceptions of omnipotent hackers, as outlined earlier, is the reality that there has been a significant decline in the level of skill required to prosecute hacking acts [IW16 p.64; see also BAE12 p.5; HSSK p.893; UNC p.39]. The ubiquity and automation of software, either designed explicitly for malicious activity or for penetration testing, has meant that the barrier for entry has been significantly lowered in recent years.

A review of cases over a decade ago showed that 66.1% of hacking and illegal access cases ‘involved no complicated techniques or techniques that could be available to the most common computer or network user at the time of committing such offences’, while only 18.3% of such cases ‘might involve complicated techniques or techniques unavailable to common users at the time of committing such offences’ [XL08 p.35]. While the skill level required for ‘cases of viruses, worms, spyware and logic bombs’ was significantly higher, with 72.7% using the most complicated techniques [XL08 p.35], these statistics undermine the view of hackers as the embodiment of the ‘genius of youth’ [Wall p.54]. This has long been recognised by the academic and hacking community, with derogatory names such as script-kiddy and lamer levelled at the less-adept practitioner.

As a framework to understand the skill levels, Holt and Kilger [HK12] divide hackers into three groups: a very small number of high skill actors, ‘who have substantive abilities to identify new vulnerabilities, create exploits and implement new programs that can be used for various attacks’; a ‘large population of semi-skilled actors who can recognise and use various tools and exploits’ in a concerted fashion, though they cannot create their own; and the bottom of the pyramid houses the low or unskilled hackers who have ‘little understanding of the mechanics of an attack or compromise, and depend entirely upon the ingenuity of other hackers in order to engage in attacks’ [HK12 p.1-2].

Analysis

This framework is used as the basis for the analysis of the skill levels of offenders in this project. The skill levels of the individuals convicted under the CMA have been assessed based on the criminal act(s) that they are known to have carried out (not necessarily just the one that lead to the specific conviction under the CMA). Where it is unclear what techniques an individual used to execute their criminality, indicators such as the use of widely available malware, not obfuscating a home IP address or the nature of the crime (e.g. accessing old employers' or colleagues' systems through known passwords) are used in order to help determine the skill level. Once the skill levels were identified for each individual, they were classified as high, semi, low or unskilled in the appendix, with a short justification provided. The reality of this assessment is necessarily 'light-touch', largely based on media articles written at the time of conviction alongside a small number of identified court/appeal documents. As such, there may be inaccuracies where individuals may have 'got lucky' (and their skill level is over-estimated), or where individuals have used complex techniques in order to carry out relatively minor acts of criminality (and their skill level is underestimated): it has not proven possible to gain an accurate understanding of the exact steps/techniques employed by each individual.

Following this, 64 of those convicted under the CMA are assessed as either unskilled, or possessing low skill. There is a large degree of variation within this group. At the lower (unskilled) end sit individuals such as Mark Johnson, whose crime was to retweet a link in support of Anonymous' DDOSing of the UK Home Office's website, or Piotr Smirnow and Patrick Surmacki who subcontracted out their hacking to a Ukraine-based individual. A number of other individuals circumvented technical controls (e.g. logged onto accounts not their own - Astrid Curzon, Zoe Gregory, Scott Willey, Quadsys Five), but are unlikely to have used any technical means to do so. The complete absence of skill raises the question as to whether these individuals should be considered 'hackers' at all, despite their convictions under the CMA. Nevertheless, they committed crimes (or assisted in the prosecution of crimes) against information systems that involved the circumventing of controls, however nebulous this might be. Needless to say, none of the 32 individuals (the non-hackers) who did not subvert any controls showed any skill.

The low skill category is largely made up of ex-IT employees who used their knowledge of the systems that they used to operate in order to damage their previous employers (Samir Desai, Scott Burns, Vladimir Yanpolsky and others), and other individuals using open source software or rented botnets (usually coupled with a lack of obfuscation techniques) in order to conduct their activity. Of the latter, it is arguable whether their criminality 'involved no complicated techniques or techniques that could be available to the most common computer or network user at the time of committing

such offences'; however, the crimes committed are those that anybody armed with a reasonable level of computer literacy, criminal intent, and google would be able to carry out.

Twenty-eight individuals are classed as semi-skilled. These are individuals engaged in sophisticated and concerted activity, usually over a prolonged period of time, and fitting the usual perception of a hacker. Examples include: Elliott Gunton, who used a wide variety of hacking tools to victimise a variety of targets; Grant West, who stole data from the websites of around 100 different companies in order to sell it on; and Sean Caffrey, who gained access to the US Department of Defence satellite communications systems. While some of these individuals carried out similar activity to some of the 'low skill' hackers, this was done in a more prolonged and systematic fashion, indicating greater competence in the execution of the crimes. Similarly, there are those who carried out activity akin to those in the higher skilled category; the dividing line has been drawn where individuals have shown an ability to develop independent tools or capabilities, rather than rely at least in part on the work of others (semi-skilled).

Eight of the individuals convicted under the CMA are classed as high skilled actors. This includes those who wrote their own malware (such as Titanium Stresser, developed by Adam Mudd), controlled and rented out destructive botnets (such as Mirai#14, controlled by Daniel Kaye, or the vDOS service run by Jack Chappell), or were high-profile members of prominent groups (such as Ryan Ackroyd and Mustafa Al-Bassam of Lulzsec). These individuals uniformly carried out a wide array of criminal activity, both for their own ends and (more often) on behalf of others.

Table - Skill level of convicted hackers

Unskilled	Low Skill	Semi-skilled	High Skill
18	46	28	8

Conclusion

The analysis above fits well with Holt and Kilger's pyramid model of hackers' skill levels, with the majority of individuals in the low/unskilled sections, fewer semi-skilled actors and even fewer high-skilled actors. This is unsurprising, and fits with the general understanding of the skill distribution amongst active hackers. It should be noted, however, when drawing comparisons to the wider hacker population, that the data on skill level is likely to be skewed by two major factors. First, unskilled or low skilled individuals are likely to be overly represented amongst those convicted due to the

greater likelihood of them making errors that lead to their identification, prosecution and conviction. Second, and conversely, highly skilled individuals are likely to be overly represented in the media coverage of criminals prosecuted under the CMA, with their cases seen as exciting and newsworthy by the media; with the result that they are more likely to appear in this project (based on the fact that any prominent cases would have been picked up on MTCE).

Following this, this second factor implies that those 172 individuals prosecuted under the CMA between 2008-2020 that have not been analysed as part of this project (304 convictions in total, 132 analysed) are likely to be either low/unskilled actors, or insiders exceeding their authorisations. As such, it seems safe to conclude that the CMA has seen a total return of eight convictions for hackers who have shown a high level of skill (or at least not substantially more than eight). This is not a particularly impressive return from the CMA over 12 years, especially considering the prominence that has been given to cybercrime over the period (caveated by the fact that highly skilled hackers may have been convicted under separate legislation). As well as indicating the presence of difficulties in policing cybercrime, this lack of convictions of high skilled individuals also demonstrates that the way in which the CMA is currently used does not tie in neatly with its initial intent. The Act was meant for use in catching the highest profile remote hackers; but, with only 35 of the 132 individuals analysed demonstrating any level of developed skill, its primary use seems to be in convicting individuals that are a far-cry from the original hacker stereotype and ideology (clearly, there are complex reasons behind this that are beyond the scope of this project). Even with a broad definition of hackers, with no requirement for any skill to be shown, the fact that 32 of the 132 individuals analysed can not even be considered hackers shows the way in which the CMA's focus has shifted over time.

The preponderance of low/unskilled hackers in the data also indicates the ease with which malware can be utilised by individuals with no skill; the large number of individuals using widely available remote access trojans or DDOSing services is testament to this. It is also clear in a number of cases that individuals have used hacking simply as an efficient and effective means to commit criminality; criminal intent has preceded the development of hacking skill, rather than individuals with pre-existing skills later deciding to use them for nefarious purposes. This leads directly on to a discussion of the motivations of hackers.

Chapter 5 - Motivations

One of the key areas of investigation around hackers is why they conduct criminal hacking activities: their motivations. According to some commentators, there is nothing new under the sun: cyber-criminals (including hackers) are driven 'by time-honoured motives, most obvious of which are greed, lust, power, revenge, adventure, and the desire to taste 'forbidden fruit'' [GSD01 p.02; see also PG01]. Thomas and Loader reduce this down to three core motives: curiosity; financial reward; and illegal political or social activity [TL00 p.6-7]. This is reflected by an official Home Office study into cyber-dependent crimes, which paints a similarly blunt picture: 'motivations for cyber-dependent crimes focus largely around personal profit or financial gain (for example, the use of malware to gain access to bank account details) or can also be a form of protest and/or criminal damage (e.g. hacking and website defacement)' [HO13 p.6]. These approaches largely translate the motives for terrestrial criminality directly into cyber-space. However, in an extensive comparison between 'traditional criminals' and cyber-criminals, Weulen Kranenbarg argues that there are some key differences: 'extrinsic motivations were less important for cybercrime compared to traditional crime… [while] intrinsic motivations, like curiosity and learning from committing crimes, were most important for all cybercrime clusters' [WK18 p.205].

As such, it is necessary to delve deeper into the literature. Fortunately, others have taken a slightly more nuanced approach, taking into account the peculiar social dynamics of hacking and cyber-criminal communities. Taylor identified six motivations for individuals to start hacking: feelings of addiction; curiosity; boredom with the educational system; desire for power; peer recognition; and the desire for political expression or agency [PT99 p.46]. Wall cited similar motivations as fundamental to the committing of cybercrimes: 'self-satisfaction', to include the alleviation of curiosity, intellectual urges, or boredom; 'the need for peer respect; to 'impress potential employers'; 'criminal gain or commercial advantage'; 'revenge'; as well as political motivation [DW07 pp.62-64]. While the wider applicability of some of these motives can be called into question (e.g. boredom with the educational system is unlikely to motivate a 30-something hacker), they provide a more tailored approach to looking at the reasons behind individuals' desire to hack.

Kilger, Arking and Stutzman look at similar motivations but provide greater structure [KAS04]. They repurposed the FBI's counter-intelligence (CI) framework for understanding motivation in the CI sphere (MICE- Money, Ideology, Compromise and Ego) to create a hacking-specific acronym, MEECES (Money, Entertainment, Ego, Cause, Entrance to social group, and Status [KAS04 p.510]). The first of these, money, was initially likely to see a hacker shunned from the wider com-

munity, although now clearly plays a fundamental part in a large proportion of cybercrimes [KAS04 p.511; TLY18 p.583; and as discussed in MB12]. This is demonstrated by the sale of data acquired through hacks, as well as the sale and leasing of malware and botnet infrastructure [HK12 p.10]. Entertainment as a motivation, on the other hand, is seen as having remained a constant in the hacker community [HK12 p.8], with Lulzsec as a named example of this. It might consist of interested individuals hacking to satisfy an intellectual curiosity, or simply causing havoc on systems for the supposed joy of doing so.

The driving force of a cause, or hacktivism, is largely self-explanatory; and easy to determine due to the clear link between act and message (e.g. Anonymous). That of ego is rather more conceptually stimulating when it comes to hacking. Kilger et al suggest that this is a particularly powerful form of motivation; the desire for mastery even overwhelming any fear of repercussions [KAS04 p.514]. The persistent use of handles by hackers shows a clear desire for recognition, and individuals can obtain significant respect from their peers through the carrying out of a technically skilled act. A study of 462 website defacements by Woo et al. [WKD04] neatly draws these two facets (cause and ego) together. The study indicated that 70% of the defacements reviewed were done as pranks, with the underlying motivators being ego, personal accomplishment and peer recognition. However the other 30% of attacks were primarily motivated by political, nationalist or activist concerns against the target site. The vast majority of these attacks indicated that the perpetrators acted as part of extensive networks and actively identified with other members.

This last point dovetails neatly with the motivation of ‘entering the community’ of hackers, as laid out by Kilger et al. These networks and communities have their own cultural mores, and a substantial body of study has grown up specifically analysing the dynamics within hacker subcultures [e.g. JT98, PT99, TH07, GC11, HSSK12, HK12, MB12, BC12, TFL15]. Uniform across these are a meritocratic nature that demands that individuals demonstrate advanced technical skills. Those who do so, obtain ‘status’. This is seen by Kliger et al as the ‘most powerful social force’ within the hacking community and a key motivating factor behind individual hacks [KAS04 p.517; also see BC12]. Sharma backs this up, outlining that ‘penalties for computer crime may have minimal effect as hackers constitute a counterculture and operate in a world of anonymity where chances of being caught are minuscule… [and] penalties might serve more as a challenge to boast about eluding them’ [RS07 p.6].

Hackers have proven to be happy to give their own views of their motives: looming large amongst these are often curiosity, challenge, peer recognition, and a desire to undermine a grasping, vindic-

tive state (PT99 p.46 ff; KS16 p.105 ff]. The attitude espoused in *The Hacker Manifesto* is a clear example of this [TFL15 p.82], and some hackers even see their activities as 'prosocial', thinking their crime is a positive action (e.g. by educating others about security vulnerabilities) [TFL15 p.74]. Indeed, in a wide-ranging survey of 567 hackers, 14% of them claimed to hack for the good of the victim, with 30% claiming curiosity as the primary motivation [CDC09 p.77). In a study of Russian hackers, Voiskounsky et al. found that hackers insist that their actual motives 'include getting money, cognitive interests, and the prospect of becoming famous'; alongside the desire to be 'ranked at the top', active self-assertion (very likely compensating for inferiority complexes), the need for challenge, and a desire to belong to a reference group of top level experts (VBS p.79-80).

Similarly, Bachmann's findings (from a survey of 124 hackers at a professional conference at the US) provide the following breakdown of primary motivations for an initial interest in hacking: 59.7% for intellectual curiosity; 16.9% had experimentation, and 12.1% noted excitement; but only 3.2% noted a feeling of power, 0.8% had peer recognition down, and 0% claimed financial gain. These motivations shifted as hackers moved further into their careers, with Bachmann's respondents claiming the following primary motivations for continuing to hack: 29.8% for intellectual curiosity; 22.6% for financial gain; and 17.7% for experimentation [MB12 p.186]. In Turgeman-Goldschmidt's study of 54 Israeli hackers, the primary motivators were given as: fun, thrill and excitement; curiosity for its own sake; and computer virtuosity (TG12 p.1535]. She makes the point that hackers 'provide internal justifications… [they] accept responsibility, attribute it to themselves, and are interested in being given the credit' [TG12 p.1541]. How much these motivations are created as *post hoc* justifications, and with one eye on the agendas of those who oppose them is an open question [see discussion in PT99 p.46]. It should also be noted that those studies that rely on self-identified hackers to voluntarily participate are unlikely to be representative of active criminal hackers, who are likely to avoid participating in them.

Analysis

The analysis of the 100 convicted hackers examined will use the MEECES framework (chosen as the most comprehensive framework) in order to classify these motivations. Clearly, multiple motivations can be identified for a number of the individuals, and these have been attributed where relevant. Where clear and direct information has been given on the motivations of offenders (e.g. quotes from judges, court/appeals documentation), these are used. Where there is no explicit statement around the motivation of the offenders, the target and nature of the offence is used in order to deduce motivation (e.g. where an individual has obtained data in order to sell it, financial motiva-

tion is ascribed; where an individual has illegally obtained sexually explicit images of a victim, sexual motivation is attributed).

Money, or financial motivation, is the most prevalent motivation identified. Of all of the hackers examined, 44 of them had at least some financial motivation. These include: hacking databases in order to sell on identifiers and credentials (e.g. Elliott Gunton, Grant West, Nazariy Markuta); carrying out hacks, running botnets or providing further illegal services to further the interests of third parties in exchange for payment (e.g. Daniel Kaye, Adam Mudd, Goncalo Esteves, Alex Bessell, Jack Chappell, Seth McDonagh); using ransomware to extort money from others (e.g. Zain Qaiser); accessing others details/accounts in order to perpetrate fraud (e.g. Daniel Thompson & Idris Akinwunmi, Ernest Edjeren, Alexander Akinyele, Tyrone Ellis); to gain an unfair business advantage or save business costs (e.g. Mustafa Kasim, the 'Quadsys Five', Philip Tong & Adam Hinkley); or to enable a terrestrial crime (e.g. Adam Penny). These hackers ranged in skill, from highly skilled guns for hire, such as Daniel Kaye, to those using insider knowledge to commit criminality against former employers, such as Mustafa Kasim. There are likely to be complex reasons for the higher representation of financial motivation in this project compared to others. Among these are: the fact that crimes with a significant financial impact are more likely to be prosecuted to completion; that hackers are likely to under-play their own financial motivation when questioned; and that lower-skilled hackers, of which there are a preponderance in the data, are more likely to see hacking tools as a means to a criminal/financial end.

With limited information available on the majority of cases, it is difficult to separate out the interlinked motivations of entertainment, ego, entrance to the community and status. This is illustrated by the case of Gareth Crosskey, who used social engineering techniques to hack into the Facebook account of the celebrity Selena Gomez before boasting about his success on Twitter and Youtube. The author of a pre-sentence report referenced in his Appeal Summary had 'formed the view that the offences appeared to have been the product of youthful bravado and a desire to prove himself to his peers'. Crosskey has also made the claim 'that his invasion of the Facebook account was meant to be harmless fun'. As such, all four of these motivations can be seen to have been present. This is backed up by a number of other cases (e.g. James Jeffrey, Charlton Floate), where the perpetrators took to social media to boast about their exploits. While these posts no doubt served the purpose of taunting the relevant authorities/victims, they are likely to also have been driven by ego and a desire for peer recognition. For the purposes of this analysis, then, these four motivations will be grouped together (and, in the table below, sit under the banner 'ego-centric').

Of the 100 hackers in this project, 28 of them were at least partly motivated by entertainment, ego, entrance to the community or status. These were often aligned with other motivations (e.g. Lulzsec members Cleary, Davis, Akroyd and Al-Bassam can be seen to be motivated by a Cause as well), but equally were not. Following Sean Caffrey's conviction, Judge Patrick Thomas QC stated that 'this was a serious crime but your motives were not seriously criminal. You did what you did just to show that you could'. These individuals are far more likely to demonstrate a higher level of skill than the average (20 of the individuals are classed as either semi or highly skilled), a fact that links back to the playful nature of the original hacking ethos.

Under-pinning the motivations of ego, status and entry to groups can be seen to be Rousseau's theory of *amour-propre*, or self-love [JR54]. *Amour-propre* is defined as an unhealthy concern with how one compares to others; motivating individuals to seek significance in the eyes of other people and requiring validation from others in a search for personal happiness. This is usually contrasted with Rousseau's sibling concept of *amour de soi* (or love of self), which is an individualistic, animalistic concern for personal wellbeing. While the concept of *amour-propre* has been the subject of a fascinating study with regard to terrorism [AK13], there seems to be a paper waiting to be written *vis a vis* the hacking community; a desire for validation and personal significance can be seen to drive much of the behaviour of what is (considered as part of wider society) a niche, isolated community whose members often fail to achieve the real world outcomes they believe is their entitlement.

Of the 100 hackers in this project, 16 of them are linked to hacktivism or a cause. It should be noted that this does not include those whose victims happened to be establishment targets (e.g. Daniel Devereux - airport/hospitals; Caffrey- US DOD, Paul Dixon - various police forces, British Airways; Floate - FBI & UK government; Lewys Martin- Kent Police, Oxford and Cambridge Universities), but where there is no clear underlying ideological thread. The four individuals associated with Lulzec are, however, included: while the groups primary stated purpose was to have fun causing havoc, they also committed attacks clearly based on ideological motivations (e.g, Operation Antisec). Six further individuals are linked to the hacktivist group Anonymous. Of the other individuals, the causes vary broadly, including: animal rights (unnamed sixteen year old), terrorism (Junaid Hussain); personal grievances (Ian Sullivan); and even the desire to obtain previously unreleased Michael Jackson material (which can be seen as a protest in favour of creative freedom- James Marks & James McCormick). The majority of these individuals are, again, relatively skilled individuals whose pattern of hacking fits into a broader picture of computer use and skill rather than a

one off use of hacking tools. The one exception to this is Sullivan, who researched how to commit his DDOS attacks only after his six children were removed by social services.

Sixty eight of the 100 individuals identified as hackers were motivated by aspects that fall under the MEECES framework. Two aspects that are not covered by the MEECES framework, sexual motivation and revenge, also played a large part in motivating individuals (27 individuals). Nine of the 100 individuals identified as hackers were motivated to using hacking techniques in order to commit further sexual offences. These offences were all committed by men against women, and the majority involved gaining access to personal images or to cameras with the intent of capturing video footage of the victims. The one exception is Christopher Topliss, who used hacking techniques in order to facilitate the grooming of children. All of these individuals used openly available software and/or demonstrated little skill in carrying out their attacks; these are criminals who saw hacking as the most effective means to perpetrate their criminal ends, rather than hackers who used their skills for criminal purposes. One exception to this, it could be argued, is Elliott Gunton, a semi-skilled hacker who was also subjected to a Sexual Harm Prevention Order for having indecent images of children on his computer. He is not included in the numbers in this paragraph, however, due to a lack of evidence linking his hacking offences with these indecent images (he was charged under the CMA for other offences). In terms of non-hackers convicted under the CMA, an additional four individuals went beyond their access permissions in order to carry out crimes linked to a sexual motivation. Three of these latter individuals were police officers who accessed official databases in order to contact women, while one individual assumed the identity of a second man and sent sexually explicit images to his victims using the stolen identity.

Of those 18 individuals who can be seen as being motivated by revenge, nine were ‘insiders’: disgruntled employees or ex-employees who used their knowledge of the systems in order to cause disruption. All of these individuals were IT specialists (e.g. Oliver Baker, Alan Thorpe, Anthony Elliott), and while they represented a significant threat to their victims due to their insider knowledge, they all demonstrated a limited level of skill in perpetrating their attacks: they used known credentials and their knowledge of the systems in order to cause disruption (e.g. by deleting files). The further nine cases all took revenge for perceived slights or injustices: against institutions deemed to have harmed them (Sullivan, Kyoji Mochizuki, Liam Watts); unhappiness with their schools (Daniel Kelley, Matthew Higgins); or due to personal vendettas (Zoe Gregory, the Hutchesons). Again, of these individuals, eight of them are low or unskilled, indicating that hacking activity was seen as a viable means to a premeditated criminal end.

This is true of three others, who circumvented technical controls for personal reasons: Scott Willey downloaded a legal certificate off a colleague's computer in order to forge his credentials; Paul McLoughlin stole gaming facilities; and Astrid Curzon used a second user's credential to log on to a profile for curiosity's sake. Convicting judges concluded that they were unable to identify motivations for two remaining individuals, Imran Uddin and Samir Desai. One further individual, Jason Polyik, hacked into two major companies in a misguided attempt to get them to employ him to patch their vulnerabilities.

Five sets of offenders (eight offenders in total) claimed to be acting in a prosocial fashion towards their victims. Lulzsec, while clearly stating that their core motivation was hacking for the 'lulz', also historically claimed that their releasing of passwords provided those who had been hacked with a warning around the need to use different passwords for accounts. Glenn Mangham, who hacked into Facebook, claimed during his trial that he had done so in order to alert Facebook to vulnerabilities in its system; although this was rejected by the Judge. Jason Polyik hacked Sports Direct and one further company, leaving his contact details on their website in the hope they would offer him a job monitoring their systems. Instead, they reported him to the police. Devereux claimed in court that he was working to help improve and benefit the systems, while Hounsell committed his criminality as part of his job running a website providing details of Windows build strings.

Table - Motivations of convicted hackers

	Money	Ego-centric	Cause	Sexual	Revenge	Other	Pro-Social
Total (100)	44	28	16	9	18	6	8
High skill (8)	6	5	2	0	0	0	2
Semi-skilled (26)	15	14	6	0	1	1	4
Low skill (48)	11	8	6	8	16	3	1
Unskilled (18)	12	1	2	1	1	2	1

Conclusion

These motivations can only, however, be used to paint with the thickest of brushes. There is no doubt that 'the ability to isolate offender motivations' is problematic [DW07 p.21], and 'hacker motivations differ over a wide spectrum' [RS07 p.17; see also SF12 p.176; PT99 p.64-65] and often overlap (e.g. clearly ego and status often go hand-in-hand). Individuals are unendingly complex, an essential fact that can become lost when attempting to translate the real world onto the page: any one hacker no doubt reflects pieces from each of the MEECES. Indeed, there is also a need to differentiate between the motivation for learning to hack/becoming a hacker, and the motivation that may lie behind a single attack. For example, an individual may have: initially learnt how to hack for enjoyment and entertainment purposes; carved out a place within a hacking community and found that they are now primarily driven by their ego and achieving status within that community; but may also carry out individual attacks in order to obtain money so that they can maintain their lifestyle. Due to the nature of the research, this section has necessarily focussed on the motivation for an individual hack, rather than that of a hacker to e.g. develop their skills. While there is clearly some overlap (e.g. a White Hat hacker who learnt to hack for prosocial reasons is unlikely to have conducted criminal activity for financial gain), this is a significant caveat.

Nevertheless, some important conclusions can be drawn. The first and most obvious is that the MEECES framework is not sufficient for an analysis of criminal hackers. While revenge could be argued to be a form of cause, and criminal sexual motivation could be argued to be a form of perverse entertainment, that is stretching the intent of Kilger, Arking and Stutzman. The absence of these motivations may be explained by the fact that 26 of the 27 of the individuals who held these motivations are considered to be low or unskilled, and saw hacking as a viable way to achieve a preconceived objective (rather than hackers who learnt their skills first and later turned to crime); and hence might not be considered hackers in the purest sense. Nevertheless, they subverted technical controls to gain unauthorised access to data and hence must be considered hackers, no matter how limited the skill levels of a number of them. The second is that there are correlations between motivation and skill level; as shown in the table above. Those motivations that track most clearly onto terrestrial, or traditional, crime (e.g. revenge, sexual) are most often found in low or unskilled actors; and those motivations that are more commonly associated with the hacking community (ego, status, entertainment, entrance to the community) see higher representation in the semi and highly skilled categories. There are two exceptions to this: financial motivation is common across all skill levels; and there are a number of low skilled actors that fit squarely into the 'script-kiddy' category

- individuals using open source tools to cause criminal damage simply for personal enjoyment and to show off to their peers.

Chapter 6 - Demographics

One aspect of the popular image of hackers that is backed up by empirical studies is that it is a group dominated by males. While a clear handle on the exact demographics of hackers is difficult to obtain in the literature, where hackers tend to be lumped in with cyber-criminals [e.g. XL08, LCC06], it is possible to extrapolate from them. Li's study, drawn on above, used a sample of 115 typical cases of cybercrime prosecuted between 18 March 1998 and 12 May 2006, which were published on the official website of the United States Department of Justice. It found that 98% of offenders were male [XL08 p.132]. Geopolitically close but geographically distant, Turgeman-Goldschmidt's study of 54 self-defined Israeli hackers found that 51 were men and three were women. [TG p.35]. Bachmann, who conducted a survey of 124 self-identifying hackers at a US conference in 2008, reports that only 5.6% of his participants were female [MB12 p.180]. In an empirical study of cyber-criminals in Taiwan, based upon data taken from the Criminal Investigation Bureau of Taiwan's cybercrime database over the interval of 1999 through 2004, Lu et al. found that 81.1% of those studied were male [LCC06 p.13]; while in Chiesa et al., 6% of their respondents were female [CDC p.74].

The reasons behind this dominance is the subject of numerous studies. Taylor, in his 1999 book based on interviews with numerous individuals involved in the hacking community, enlarges on the three main factors that he perceives for the male's dominance of the hacking community: societal factors, such as sexual stereotyping early in age; the masculine environment, with the culture representing a 'locker room climate'; and the gender in the language of hacking (PT99 p.33 ff). The most comprehensive, recent exploration of gender in cybercrime was conducted by Hutchings and Chua [HC17], who conclude that cybercrime remains a male-dominated offence, although female representation is higher is in the committing of crimes that do not require a high level of technical skill [HC17 p.184].

Of the 100 hackers, three in the data are women. Two of these, Zoe Gregory and Astrid Curzon, used credentials for accounts that were not their own; although it is not clear how they obtained these credentials (e.g. whether through technical means or through having personal knowledge of them). One other, Shakira Ricardo, was involved in the Gh0stMarket forum; she was described by the Guardian as a junior member who was keen to learn the ropes of hacking, but also whose 'ability to control fraudulent activities from her iPhone was described as cutting-edge.' As such, it's clear that the vast majority of hackers in this project are men, and all of the semi-skilled or high

skilled individuals are male. As for those not considered to be hackers, eight of the 32 are women; a significant difference in proportion.

Coupled with this, these males are largely described as young and criminally naive. In Turgeman-Goldschmidt's study, only five of those hackers studied had computer related criminal records. Interviewees tended to be young, single, educated and earning an above average income' [TG11 p.35]. In a separate look at cyber-criminals by Graboksy et al. 'those convicted tend to be first offenders with the ability to adduce evidence of previous good character as a mitigating factor… many cyber criminals are also young' and tended to cooperate with the police investigation, and pleading guilty, often at the earliest opportunity [GSU p.138-9]. In Chiesa et als.' survey of 567 self-identified hackers; 61% of those who responded were under 25, with only 3% over 45 [CDC p.74]. Li's age range of 17-45 is unhelpfully broad, and captures 79.3% of offenders [XL08 p.133]; whereas Lu et al.'s study is more helpful, indicating that 44.8% of all cybercrime suspects were younger than 24 [LCC06 p.14]. Taylor wrote that interviewees even only in their mid-20s complained of being has-beens by the constantly replenishing stock of new younger hackers [PT99 p.32]. On the other hand, Bachmann provides a slightly higher average age of 30.6 for his hackers surveyed. While he explains this as a result of the survey having been conducted at a convention geared towards security experts and computer professionals, it clearly shows that hacking is 'not just a young man's game' [MB12 p.181-2]. This is backed up by Steinmetz's analysis of the pseudonymous Union Hack collective, where the average age was 34.71 [KS16 p.44]. However, how unique this makes hacking and cybercrime is open to debate: most criminals are young and male, so cybercrime is the norm rather than the exception.

The average age of those deemed to be hackers in this project is just over 29 years old at the point of conviction. The youngest hacker in the survey was 16 on conviction (14 at the time he committed the crimes). The oldest was 69. Focussing solely on those motivated by factors under the MEECES framework, the average age falls to under 27 years old, with the oldest being 51 (although this is Sullivan who learnt how to hack in response to around kids being taken away). Across the 100 hackers, the higher the skill level, the lower the average age (high skill - 23.37 years old; semi-skilled - 23.39 years old; low skill - 30.5 years old; unskilled - 35.4 years old). The average age of those not considered to be hackers is 38 years old.

Another area where hackers and cybercriminals vary from their terrestrial counterparts is likely to be in their levels of introversion and sociability. In those brought to trial, 'cyber criminals have, in a number of cases, raised health and particularly mental health problems in mitigation' [GSU p.140].

This resonates with the data compiled by Chiesa et al. Of 276 hackers surveyed, 34% said they were insomniacs, 27% suffered from anxiety, 20% are paranoiac, 13% have panic attacks and 6% hallucinate [CDC09 p.83]. Wall states that cyber-criminals 'are more likely to be introverted and more likely to share a much broader range of social characteristics' [DW p.21; echoed in Rogers 2000]. However, this is a narrative routinely propagated, and it is difficult to unearth the raw data underpinning these assumptions, as tempting as they might be. Bachmann refutes the claim of introversion, stating that 'the vast popularity of social hacking methods and their high success rates also indicated that the commonly presumed social incompetence of hackers is wrong and misleading' [MB12 p.190]. This chimes with Schell and Melnychuk's study of 136 attendees of a hacker conference (notable for its inclusion of 70 female respondents, unusually high for the field), which concludes that 'the bulk of the hacker respondents' thinking and behaving patterns are seemingly not very different from those choosing careers in computer science, mathematics, and the physical sciences', and that even those who conduct malicious activity in their youth have often reverted by the time they are 30 [SM12 p.1096]. Their study does, however, suggest a link between highly-functioning autism spectrum conditions and the skills required to be a successful hacker [SM12 p.1096]. Across the 100 hackers studied in this project, 17 are linked in media coverage to mental health or development disorders at the time of the attack, with 11 of these individuals stated as having autism or Aspergers syndrome (a significantly higher proportion than the wider population, which is around 1%). Of the 17 individuals, 16 of them are classed as having motivations included in the MEECES category, and 14 classed as either high or semi-skilled.

Other demographic facets have also been explored in the academic literature, although fall outside the scope of this project. Ethnicity is noted as a relevant factor in numerous studies, including in Bachmann's survey of 124 hackers in the US where over 93% of these individuals were caucasian [MB12 p.181]. Social class is also considered: Steinmetz, in his analysis of hacker groups, states that hacking is 'decidedly middle class' [KS16 p.36], and this conclusion is echoed in most other studies of hacker groups. Steinmetz also argues that 'unlike many populations characterised as criminal or deviant, the hackers in [his] study were relatively educated' [KS16 p.46]. These characteristics mean that the hacker stands slightly apart from their more physical brethren [for a comprehensive comparison, see MWK18].

Table outlining key demographic facets of convicted hackers

	Gender	Average Age	Identified mental health issue
High Skill	8 Male, 0 Female	23.375 years	1
Semi-skilled	28 Male, 0 Female	23.4 years	13
Low skill	45 Male, 1 Female	30.5 years	3
Unskilled	16 Male, 2 Female	35.4 years	0

Conclusion

The demographic data reflects that found elsewhere in the literature: hackers are young and male, with mental health and development disorders over-represented in their number. The greater the skill level, the more pronounced these demographic characteristics become. Indeed, this reflects a growing division in the data. Where the individuals have displayed a higher level of skill, they more closely reflect the traits and characteristics commonly associated with hackers in the academic literature (e.g. high/semi-skilled individuals are more likely to be younger, have a mental health issue, and be associated with ego-centric motivations) while lower skilled actors diverge from the normal hacker tropes (e.g. lower skilled actors include all of those motivated by revenge or with sexual motivations, and these individuals average over 34 years of age).

Chapter 7 - Insiders and Groups

As discussed above, hackers are often portrayed as lone wolves indiscriminately targeting their victims. This chapter explores this stereotype, through an analysis of two major themes around relationships in the academic literature: insiders and groups.

Insiders

A good, if long, definition of an insider is 'a malicious criminal (current or former employee, contractor, or business partner) who has had legitimate access to an organisation's computing environment (network, systems, or data), and has intentionally exceeded or intentionally used access in a manner that negatively affected the confidentiality, integrity, or availability of the organisation's information or information systems' [TFL15 p.74]. It should be specifically noted that for an individual to be considered an insider they do not have to have subverted any technical controls (and hence not all insiders are hackers).

When the CMA was introduced, it was the insider who was the real bogeyman in computer crime in terms of volume of criminality and damage caused. In a review of computer crimes during the period, Wong shows that 'the majority of computer-related frauds were committed by trusted employees, sometimes in collusion with outsiders who are either trading partners to the company or simply the general public' [KW90], and even then these were largely unskilled employees [KW86]. Indeed, throughout the period leading up to the introduction of the CMA, it was largely the 'unauthorised use of authorised access' that was recognised as the basis for most computer-based crime, rather than hacking [LCR 2.3; Sieber's International Handbook, cited in MW12 p.402; AC94]. While the case law around insider crimes was initially contested (see judgements in R. vs Bignell and R. vs Allison), it was clarified that they were caught under the legislation [VK16] even if, 'in most cases, misuse by employees is not viewed as criminal in nature but as an issue of employment law' [Walden p.19].

These individuals are often seen as distinct from external hackers in their skill levels (they typically exploit non-technical vulnerabilities [SB10 p.123]) and motivation (e.g. there is no desire to enter a wider hacker community) [see TFL15 p.76; IW16 p.64]. An early study by Shaw, Ruby and Post states that a combination of 'computer dependency, a history of personal and social frustrations (especially anger toward authority), ethical "flexibility," a mixed sense of loyalty, entitlement, and lack of empathy' are typical characteristics of the insider [SRP98 p.5]. Liang, Biros and Luse pro-

vide a more recent overview of the threat to organisations from malicious insiders [LBL15], covering characteristics and motivations of these individuals. There have been a number of empirical studies focussed solely on insiders. One example is a U.S. Secret Service study which concluded that, for the insider threat in banks and financial institutions, 'most attacks were committed out of a desire for financial gain' [USSS04] by unskilled employees. A similar study, this time focussed on the complex infrastructure sector, shows attacks predominantly carried out by technical employees (86%) who were motivated by revenge (84%) at least in part [USSS05]. The opportunities available to insiders, as well as the unique dynamics afforded by being a constituent part of the victim organisation [XL08 p.36], means they stand apart. These last two examples, drawn from the US Secret Service, also suggest that one could develop an independent typology solely for the insider threat based on a correlation between skill level and motivation (e.g. low-skilled, financially motivated; whereas those with higher levels of skill were motivated by revenge).

That insiders form a key threat is inarguable: the only thing up for debate is whether they pose a greater or lesser threat than the external hacker. Some argue that insiders 'present the highest risk for cybercrime and corporate and industrial espionage' [TFL15 p.75; also SB10 p.123]. This is backed up by early studies [e.g. KW86, KW90], and a host of others since [NTV05; see XL08 p.131 for overview]. However, other studies have put forward the opposite viewpoint: 'the 2006 CSI/FBI survey findings revealed that most IT respondents perceived that their organisation's major cyber losses resulted from system breaches by outsiders' [cited in SH12 p.1465]. With regard to insiders, it is likely easier to obtain evidence (due to audit functions) and hence prosecute; but companies may choose to treat this as an employment rather than criminal issue [for a discussion of these issues, see IW00 p.77; XL08 p.137]. Indeed, companies are highly likely not to report cybercrimes at all, with the reputational damage of having been breached outweighing the benefits of pursuing an unlikely conviction [DW07 p.26]. It is therefore difficult to reach a clear conclusion: as Li states 'there have been different findings as to whether insiders or outsiders constitute the greatest threat to computer system security' [XL08 p.130].

Analysis

Twenty-two of the individuals identified as hackers are classed as insiders (either insiders themselves or using an associated insider's access in order to conduct criminality), alongside 31 of the 32 non-hackers (the one exception was Graeme Brandon who downloaded publicly available photos of someone else to use in sexual harassing his victims). In total, then, 53 of the 132 individuals under review were insiders (over 40%); despite the CMA's emphasis on the external threat. All of

these 53 individuals are classed as either unskilled or having low skill. Their average age at conviction was 38.8. Fifteen of these individuals were motivated simply out of curiosity, 12 out of feelings of revenge against their employer, 11 motivated by financial gain (including by obtaining a competitive advantage over rivals); with the rest having a wide assortment of other motivations. The damage caused by the attacks varies wildly: a large proportion of offenders did no more than access and examine data, sometimes to advance other criminal purposes but often just out of curiosity. However, a number of the cases clearly demonstrate the damage a malevolent insider can cause: Andrew Skelton released the confidential personal details of 100,000 Morrisons employees into the wild, while Scott Burns took down Jet2's systems for 12 hours through the deletion of accounts. The overall pernicious effect of a significant number of officials associated with the police and law enforcement accessing data for unauthorised reasons should also not be understated.

Of the individuals who were motivated by revenge, the vast majority of these were employees in the victim companies' IT departments. While other employees would also be able to cause damage through insider acts, it is likely that IT employees' knowledge of the systems and the harm they could cause them, access to relevant credentials, and their living and working in a world where computer misuse was part of their framework of reference explains their overwhelming preponderance.

A large proportion of the hackers in this study (22 out of 100), then, had a professional relationship with their victims. Beyond insiders, a further eight individuals had some form of direct relationship with their victims; they either knew them personally (Christoper, Chris and Adam Hutcheson; Grant Morton), were students at the victim institution (Imran Uddin, David Buchanan), or felt they had been victims of a specific injustice perpetrated by their victim (Kyoji Mochizuki, Liam Watts). Others were also tasked against specific victims.

Groups

A further area of interest is whether hackers act alone, or as part of a group. Well known hacker collectives like Anonymous or Lulzsec attract column inches, while 'much of the current focus of UK policy and law enforcement on computer and cybercrime revolves around the use and abuse of ICT in organised crime' [IW16 p.64]. This is backed up by the 2010 Home Office Cyber Crime Strategy, that states 'the most significant cyber criminal activity is conducted within multi-skilled, virtual criminal networks [HO10 p.11]; and a BAE paper that states 80% of online crime is carried out by organised groups [BAE12 p.3]. Nevertheless, Lu's study highlights that 64% of cyber-criminals

surveyed acted alone (although this is heavily caveated by the fact individuals may have been wrongly identified as acting alone by law enforcement) [LCC06 p.13]. Despite the caveat, this propensity for individuals to act alone is reflected in Chiesa et al.'s hacker survey. 55% of this surveyed claimed to operate alone, 7% in a group and 38% alone or in a group [CDC p.85]. A study by Schell, Dodge and Moutsatos in *The hacking of America: Who's doing it, why, and how* found that of the 200 hackers (both white and black hat) they surveyed, 57% stated they liked to hack solo (cited in SH12 p.1473).

Analysis

Of the 100 hackers studied, 51 acted as part of a group (of two or more) or were associated with a group for at least some of their identified criminal activity (this does not include those who committed a crime such as data theft, prior to selling it on to others to commit further criminality); with a further six tasked by third parties. These numbers are broadly reflective of the wider literature: around half of the individuals acted alone, or half in groups (although there is likely to be a relatively large margin for error around these numbers, as an individual thought to be acting alone may have been acting in a group where the other perpetrators were not detected/prosecuted). Some of these individuals were convicted alongside their accomplices (e.g. The Quadsys Five, Lulzsec, Anonymous); some claimed to be part of a hacking group or collective, but did not necessarily commit the criminal act for which they were convicted alongside others (e.g. Nazariy Markuta, Kane Gamble); some were involved in international conspiracies but were convicted alone (e.g. Zain Qaiser); and still others acted as the hacker amongst a wider criminal conspiracy that included terrestrial crimes (e.g. Adam Penny, Matthew Beddoes). Of the non-hackers, 11 of 32 acted as part of a wider group, largely accessing information to be used for criminal ends by others. A further six individuals (not included in the 51) were tasked by third parties, carrying out criminality on behalf of others in exchange for payment.

There are two prominent types of group associated with cyber crime: hacker collectives, such as Anonymous or Lulzsec, who carry out their crimes for reasons beyond just the financial; and organised criminal gangs (OCG), who seek to exploit information systems largely for financial gain. While this latter is seen as a key threat, only 12 of the individuals convicted are known to have formed part of what can be considered criminal gangs (although a further four individuals operated as part of Gh0stMarket, a key enabler for organised criminal gangs). This is in comparison to 16 individuals who claimed association with, or carried out activity on behalf of, named hacker collectives. The remaining individuals who carried out activity alongside others did so with either friends

or colleagues, although these groups would struggle to fit under the banner of an OCG or hacking group. This, then, seems to belie the emphasis on hacking as forming a key part of organised criminal activity (although may be indicative of the greater skill exhibited by these individuals and hence lower numbers in prosecution; or the fact these individuals may be prosecuted under other legislation). However, when correlated with skill level, there is a clear preponderance for individuals to act in concert. All eight high skilled hackers were either tasked by third parties or acted as part of a group, along with 21 of the 28 semi-skilled actors. This is opposed to 28 of the 64 low or unskilled actors.

Conclusion

Of the 100 criminal hackers, then, over half acted with at least one accomplice and, clearly, others will have had relationships within various hacking communities but did not act with them directly. However the preponderance of hackers to act together becomes greater the higher their skill level, indicating there is merit in the claims that the most dangerous hackers act in collectives. This project has also demonstrated that around a third of the hackers convicted under the CMA were known in some way to their victims (either as employees or in some other capacity); leaving around two thirds who chose their victims based on something other than first-hand contact with them. However, again, when skill level is taken into account, there is a clear divide. Only one high or semi-skilled actor appeared to have had a direct relationship with their victim (and his school was only one of David Buchanan's many victims); and the proportion of individuals who knew or were associated with their victims (either as employees or otherwise) increases the lower the skill level. This is set out in the table below.

	Group	Lone operator	Tasked by third parties	Known to victim	Unknown to victim
High skill (8)	5	0	3	0	8
Semi-skilled (28)	18	7	3	1	27
Low skill (46)	16	30	0	17	29
Unskilled (18)	12	6	0	11	7

Chapter 8 - Typologies

Building on top of these variations in motivation, characteristics and skill level on the part of hackers, there have been a number of attempts at classifying hackers into basic typologies. An overview of early attempts is given by Rogers [MR00], Woo [HW03] and Meyers et al. [MPF05]. Landreth proposed five categories of hacker, divided largely by motivation: novices (petty mischief making), students (intellectual challenge), tourists (thrill), crashers (destructive), and thieves (profit) [B. Landreth (1985), *Out of the Inner Circle: a Hacker's Guide to Computer Security cited* in MPF05 p.5]. Hollinger divided hackers by skill, demarcating them into pirates (who committed mainly copyright infringements), browsers (who gained occasional unauthorised access to another user's account) and crackers (the most serious abusers, who copied, modified and sabotaged others' files and programs) [RH88]. Chantler, writing a few years later, gave a separate three categories based on skill and motivation: an elite group (high skill, high motivation, motivated by excitement and challenge); neophytes (mid-skill, still learning); and losers/lamers (no skill, motivated by profit, theft or vengeance) [N. Chantler (1996), *Profile of a Computer Hacker*, cited in MR00 p.4]. Other typologies were developed by Parker (seven profiles: pranksters; hacksters; malicious hackers; personal problem solvers; career criminals; extreme advocates; and malcontents, addicts, irrational and incompetent people) [D. Parker (1998), *Fighting Computer Crime: A new framework for protecting information*, cited in MR00 p.6] and Power (three categories: sport intruders, competitive intelligence, and foreign intelligence) [R. Power (1998), *Current and future danger*, cited in MR00 p.5].

Crossing the threshold into the new millennium, Taylor et al. divided the hacker universe into: script kiddies, who are 'primarily concerned with bragging and attacking each other or anyone else who draws their wrath… the term script kiddie comes from their use of remade tools or scripts'; white (ethical) hat, black (malicious) hat or grey (sometimes violates ethics) hat hackers, who were skilled practitioners with varying motivations; and hacktivists, who use 'hacker skills and attitudes to convey a political message' [TFL15 p.77-80]. The foundation for most recent hacker typologies, however, is that of Rogers [MR05]. He argues that there are at least eight primary types of hacker, based on a cross-section of skill and motivation. These are: Novices, Cyber-Punks, Internals, Petty Thieves, Virus Writers, Old Guard hackers, Professional Criminals, and Information Warriors (IW). Political Activists were also added as a possible ninth category.

Novices are new to hacking, rely on software written by others and are primarily motivated by thrill seeking and ego stroking [MR05 p.3], with the aforementioned Mafiaboy fitting into this category. Novices seek to develop their skills and gain acceptance into wider hacker communities. Cyber

punks have a mid level of skill, and intentionally engage in malicious acts motivated by a desire for media attention (e.g. by choosing high profile victims) and monetary gain [MR05 p.3]. On the other hand, Petty Thieves look to avoid any notoriety and are simply attracted to the internet and technology as an effective means to line their pockets [MR05 p.4]. The Old Guard is the group that most typifies the old-school hacker ethic, discussed previously, with deep technical skills and motivated by curiosity and intellectual challenge [MR05 p.4]. Professional Criminals are those with a high degree of technical acumen and are often employed by organised crime groups. They are not interested in fame, seeking financial reward instead. Information Warriors seek to conduct attacks designed to destabilise, disrupt or effect the integrity of information systems and are usually highly professional [MR05 p.5]. Information warriors are distinct from political activists who are, essentially, hacktivists; individuals who use online tools to further a political cause. The Virus Writers are, according to Rogers, ‘a bit of an anomaly’ and there is a wide spectrum of behaviour that sits under this category; later works add them as a subset of cyber-punks rather than anything more distinct [HP12 p.82; for further on Virus-Writers, see SG06]. And finally, the Internals group is made up of disgruntled employees or ex-employees who go beyond their authorisations to cause harm. Rogers sees these as most often IT professionals or administrators, with motivation centred on revenge.

Hald and Pedersen [HP12] specifically build on Rogers’ work, updating the categories. Novices become script kiddies, cyber-punks encompass both cyber-punks and virus writers. Internals become insiders, old guard become grey hats, and political activists are badged hacktivists. These latter are, by definition, ideologically motivated and have widely varied skill levels. Professional criminals and petty thieves remain the same, while the information warrior category is spread under the professional criminal banner, as well as a new one of 'nation states.’ The latter commit crimes for geopolitical reasons, and are hugely skilled and resourced [HP12 pp.84-85]. However, while Grabosky’s review of the development of cybercrime between 2006-2016 indicates that there has occurred ‘a narrowing distinction between cybercrime and cyberwarfare’ [PG17 p.30], nation states are likely to remain out of scope of this analysis.

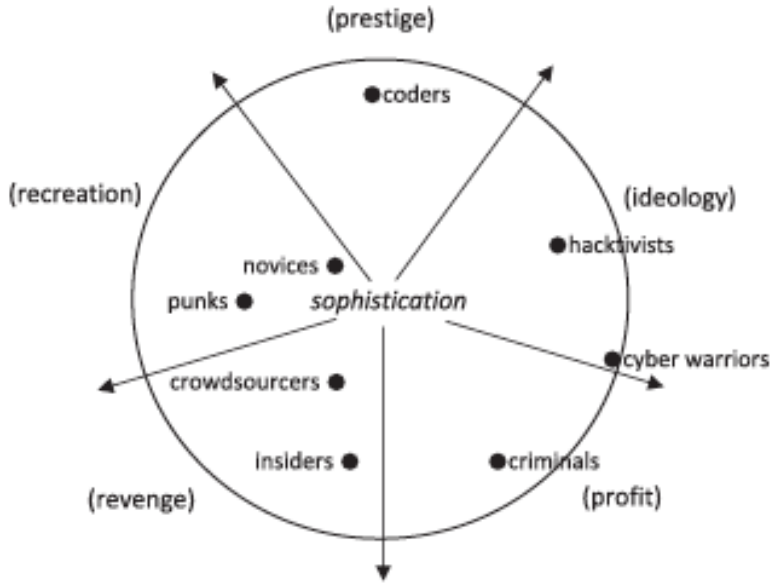
Two further typologies that provide a strong, explicit nod to Rogers are worth noting. Meyers et al. provide an updated typology based on skill level, maliciousness, motivation, and method [MPF05]. This is outlined in the table below.

Adversary Class	Skills	Maliciousness	Motivation	Method
script kiddies, newbies, novices	very low	low	boredom, thrill seeking	download and run already-written hacking scripts known as 'toolkits'
hacktivists, political activists	low	moderate	promotion of a political cause	engage in denial of service attacks or defacement of rival cause sites
cyber punks, crashers, thugs	low	moderate	prestige, personal gain, thrill seeking	write own scripts, engage in malicious acts, brag about exploits
insiders, user malcontents	moderate	high	disgruntlement, personal gain, revenge	uses insider privileges to attack current or former employers
coders, writers	high	moderate	power, prestige, revenge, respect	write scripts and automated tools used by newbies, serve as mentor
white hat hackers, old guard, sneakers	high	very low	intellectual gain, ethics, respect	non-malicious hacking to help others and test new programming
black hat hackers, professionals, elite	very high	very high	personal gain, greed, revenge	sophisticated attacks by criminals/thieves; may be 'guns for hire' or involved in organized crime
cyber terrorists	very high	very high	ideology, politics, espionage	state-sponsored, well-funded

Table 1. A Taxonomy of Cyber Adversaries [MPF05 p.8]

Seebruck builds on both Rogers and Meyers et al., with his most notable addition being a greater emphasis on ideology as a core motivation [RS15]. Seebruck sees hacktivism as an under appreciated element of both Meyers et al. and Rogers, and part of the hacker-sphere that has increased over time. He also argues that a category for 'crowdsourcers' (where crowdsourcing is a collective effort to solve a problem, e.g. via doxing a target individual) ending with the following types: novices,

crowdsourcers, punks, hacktivists, insiders, criminals, coders, and cyber warriors [RS15 p.39]. These are plotted on the circumflex below, based on motivation and skill level.



Notes: Nodes depict hacker types; nodes placed nearer to circle edges are more sophisticated; regular text indicates hacker groups; parenthesized text indicates motivations.

Fig 1. A circular order circumplex of hacker types [RS15 p.40]

Analysis and Conclusion

Following the analysis of the 100 hackers above, however, it is clear that these typologies can only act as a rough guide. Clearly, this analysis has focussed solely on hackers convicted of criminal acts, so a number of the 'types 'of hacker (e.g. white hat, old guard hackers, coders) are unlikely to feature. Coupled with this, individuals clearly display traits drawn from a number of the hacker types: an example being Elliott Gunton, who showed a relatively advanced level of sophistication (semi-skilled), while displaying a desire for both money (criminal) and self-aggrandisement (punk). While the typologies are only intended as rough guides, this makes it difficult to classify many of the individuals with any real confidence and undermines the utility of the typologies [see MR11 p.222].

Nevertheless, a number of the hacker types come across clearly in the data, particularly amongst those high or semi-skilled hackers. Professional and skilled criminals are evident (e.g. Daniel Kaye, Adam Mudd), as are punks and hacktivists (e.g. Lulzsec). A number of the low skill actors also fit neatly into some hacker stereotypes, with script kiddies/novices noticeably prevalent. These indi-

viduals are usually guilty of DDOSing prominent websites before boasting about their exploits (e.g. Paul Dixon; the 16 year old from Plymouth; Lewis Martin); and a number of professional and skilled criminals are also evident (e.g. Daniel Kaye, Adam Mudd).

However, a large number of the individuals covered in this project sit outside of the types identified in the typologies. These are individuals who seemingly (and misguidedly) identified hacking as an easy and supposedly secure way in which to commit their criminality. The cases clearly show that individuals who are obviously criminals (e.g. for profit) do not require high skill levels. Whether motivated by profit or a desire to commit further criminal acts (e.g. content crime), these individuals use the tools and techniques of novices, but with the intent of criminals. Criminal motivation is clearly, in these cases, a precursor to these individuals learning how to carry out basic hacking techniques in order to perpetrate the crime (motivation before skill). This is in contrast to those high or semi-skilled actors who, perhaps having developed their skills out of an interest in hacking itself rather than criminality, turn to these skills in order to carry out criminal behaviour for profit, ego or status (skill before motivation).

A further set of individuals can also be seen as opportunists who used limited skills for specific purposes: computers and information systems were the medium for their crimes, but hardly the focus of it. It is tempting to try and explain away these low skill individuals as outside the 'hacker' realm, so removed are they from the ethos, spirit and skills of the early hackers. However, this would be incorrect: they have all clearly committed acts of hacking. Just as with any other crime type, these acts can range hugely in sophistication and damage while the underlying nature of the crime remains consistent. Instead, what it clearly demonstrates is the democratisation of hacking through the spread of automated tools and software. With access to Google and Metasploit (or even just someone else's password or unlocked computer) any individual with basic computing skills can turn themselves into a criminal hacker (doing so securely and with criminal 'success' is perhaps another matter).

Chapter 9 - Conclusion

The number of convictions under the CMA is widely seen to be low. An early estimate by the Audit commission estimated only 20% of hackers detected were prosecuted [AC94], and instances of cybercrime have increased exponentially since then. As Wall states, 'fairly high levels of victimisation contrast sharply with the remarkably low prosecution figures and also the results of the surveys of individual victimisation' [DW07 p.54]. Nevertheless, there have been convictions under the Act, showing at least some success in using it as a tool for law enforcement.

As demonstrated above, though, the individuals convicted under the CMA do not make up a rogues' gallery of the most skilled and dangerous hackers; the initial vision of who would be prosecuted under the Act. With the number of highly skilled hackers being outnumbered four to one by individuals who simply exceeded their access rights, it is more likely that someone convicted under the CMA has demonstrated no hacking skill than shown any semblance of advanced knowledge. While there is a handful of highly skilled and prolific hackers in the roster, the stereotypical hacker prosecuted under the Act is an individual with no or low skill, carrying out an attack using widely available hacking tools, and who has made a basic error in the prosecution of their crime (e.g. logging into a network from their home IP address, boasting of their exploits on Twitter). It is clear that people can turn to hacking as just another tool for their criminality: no prior skill required. While some of the motivations displayed by the criminal hackers are reflective of those peculiar to the hacking community (e.g. status, entertainment, entrance to community), larger numbers are indicative of more common criminal concerns (e.g. preponderance of financial motivations, criminal sexual motivation, revenge). These hackers are not, by and large, aligned with OCGs or hacker collectives (although this does not mean that these hackers are less common- they are just less commonly apprehended). These aspects all undermine the common stereotype of the gifted hacker with the ability to cause major damage to public infrastructure.

That having been said, the criminal hackers studied do reflect a number of the common threads of hacker profiles highlighted in other academic studies (as well as the media stereotype). The vast majority of the hackers are male, and some developmental disabilities, such as autism, are overrepresented in the population. The higher the skill level of the hacker, the younger the average age. Script kiddies are easily identifiable in the data. A significant number of individuals commit their criminality motivated by the desire for status, for entertainment or to satisfy their own ego. The proportion of unskilled, semi-skilled and highly skilled actors reflects the proportions laid out by

Holt and Kilger. The insider threat is both real and prominent, both from hackers and individuals exceeding their authorisations. All of these find their echo in other studies.

Returning to the research objectives around the characteristics and nature of hackers laid out in the introduction, it is clear that the individuals analysed in this study can be seen to fall into three broad camps. A division in the data exists between:

- those individuals guilty of unauthorised use of authorised access. These individuals can in no way be considered hackers;
- those individuals who have turned to hacking as the most expedient way to commit further criminality. They do not use hacking tools and techniques out of any interest in the technology or any desire to impress a community of others (or themselves). They show low levels of skill, and they are significantly more likely to be motivated by money, revenge or criminal sexual motivations than by ego-centric motivations peculiar to hacking communities, such as entertainment or status. They are more likely to know their victims, and to act alone in committing their crime. They are older, and less likely to suffer from mental health issues. These individuals are the beneficiaries of the democratisation of hacking through the existence of widely available, easy to use malware and other tools; and
- those individuals who are clearly identifiable as hackers, reflecting the well-known traits and typologies discussed in the wider academic literature. They are young males, who tend to display a reasonable level of skill (or at least appear to have an affinity with the technology if they do not), and are often motivated, at least in part, by ego, status, entertainment or peer recognition (although money remains a key motivator). They do not know their victims, and act in concert with others (or are tasked by others). They are often identifiable as a hacker ‘type’, even if these labels are never a snug fit.

It is these latter hackers, a new type of criminal emerging in the 1980s, that the CMA was initially aimed at (as laid out in Chapter 1). Technological evolution and the proliferation of easily usable malware are responsible for the second group (criminals who have turned to hacking); while the high proportion of non-hackers prosecuted under the Act goes clearly against its initial intent - these individuals were not the threat at hand when it was passed into law, and not the intended convictions. While the CMA is criticised for the low number of prosecutions brought under it, even then the number of those prosecutions is bolstered by employees going beyond their remit and low skilled criminals turning to hacking out of expediency. The reasons for this lack of success are var-

ied, and largely out of scope of this project. The CMA is not the only tool for prosecuting hackers and, as Wall points out, it is 'very possible that since security breaches are usually precursors to further offences, some [offenders] might have been prosecuted under the more substantive offences' [DW07 p.54]. There are also wider issues with obtaining convictions under the Act that are out of scope of this analysis: around policing (e.g. the skills and resourcing required to successfully prosecute), obtaining evidence (e.g. due to the criminal use of encryption), a lack of understanding amongst authority figures [MR11 p.230-231] and jurisdictional authority (due to the globalised nature of hacking) amongst others [WLD12 p.12; also GSU p.26-27].

This is not, though, to paint the CMA as an abject failure. It was intended, alongside being a tool for prosecutions, as a statement against the hacking threat. As chapter 1 demonstrated, it was a marker in a cultural war against a new type of criminal. While its success in shifting public opinion has not been examined, the evolution of the term hacker is testament to a shift in the perception of these individuals, with the term now often used pejoratively to denote someone conducting criminal activity (far removed from its original emphasis). The fact that this project is even possible is, in itself, a statement of the longevity of the CMA: in a field which would be barely recognisable to Colvin MP when he introduced his bill before Parliament, it remains alive and at the forefront of UK legislation in battling the threat. Nevertheless, the CMA cannot claim to have been a huge success in securing the level of prosecutions (either in number or in 'calibre' of criminal hacker) that was initially envisaged, despite grand words and hopes in Parliament.

19,015 words

References

AP04 All Party Parliamentary Internet Group, *Report on Revision of the Computer Misuse Ac*t, June 2004; available at https://www.cl.cam.ac.uk/~rnc1/APIG-report-cma.pdf

AC94 Audit Commission, *Opportunity Makes a Thief: An Analysis of Computer Abuse* (HMSO, London; 1994)

MB12 Bachmann, M., 'Deciphering the Hacker Underground: First Quantitative Insights', in *Information Resources Management Association: Cyber-crime: Concepts, Methodologies, Tools and Applications, Volume 1,* (IGI Global; 2012), pp. 175-194

BAE1 BAE Systems Detica and London Metropolitan University, *Organised Crime in the Digital Age,* 2012. Accessed on 17 December 2019 at https://www.yumpu.com/en/document/read/2424098/organised-crime-in-the-digital-age-the-real-detica

JB18 Banks, J., 'The Techno-Security-Capitalist Complex' in Steinmetz, K., and Nobles, M. (eds), *Technocrime and Criminological Theory* (Routledge, New York; 2018), pp. 102-115

BN03 Barton, P., and Nissanka, V., 'Cyber-crime - a criminal offence or civil wrong?', in *Computer Law and Security Report,* vol. 19, no. 5, 2003, pp. 401-405

BC12 Benjamin, V., and Chen H., 'Securing Cyberspace: Identifying Key Actors in Hacker Communities', conference paper given at *IEEE International Conference on Intelligence and Security Informatics,* 2012. Accessed on 10 February 2020 at https://ieeexplore.ieee.org/document/6283296

JB90 Bloombecker, J., 'Computer crime and abuse', in *The EDP Auditor Journal* II, 1990, pp. 34-41

SB10 Brenner, S., *Cybercrime: Criminal Threats from Cyberspace* (Praeger, Oxford; 2010)

AC96 Chandler, A., 'The changing definition and image of hackers in popular discourse', in *International Journal of the Sociology of Law,* vol. 24, no. 2, 1996, pp. 229-51

CDC0 Chiesa, R., Ducci, S., and Ciappi, S., *Profiling Hackers: the Science of Criminal Profiling as Applied to the World of Hacking* (Taylor and Francis, Boca Raton; 2009)

GC11 Coleman, G., 'Hacker politics and publics', in *Public Culture,* vol. 23, no. 3, 2011, pp. 511–516

CMA9 Computer Misuse Act 1990; available at http://www.legislation.gov.uk/ukpga/1990/18/contents

CPS1 Crown Prosecution Service, *Cybercrime: Prosecution Guidance*; available at https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance

PC06 Csonka, P., 'The Council of Europe's Convention on Cyber-crime and other European initiatives', in *Revue internationale de droit pénal,* vol. 77, no. 3-4, 2006, pp. 473-501

DOB1 Donalds, C., and Osei-Bryson, K-M., 'Toward a Cybercrime Classification Ontology: A Knowledge-Based Approach', in *Computers in Human* Behavior, vol. 92, 2019, pp. 403-418

ERY1 Edwards, L., Rauhofer, J., and Yar, M., 'Recent Developments in UK Cybercrime Law', in Jewkes, Y., and Yar, M., (eds), *Handbook of Internet Crime* (Willan, New York; 2012), pp. 413-436

SF08 Fafinski, S., 'Computer Misuse: the implications of the Police and Justice Act 2006', in *The Journal of Criminal Law,* vol. 72, no.1, 2008 pp. 53-66

SF09 Fafinski, S., 'The UK legislative position on Cybercrime: A 20 year retrospective', in *The Journal of Internet Law,* vol. 134, no. 4, 2009, pp. 3-11

SF09 Fafinski, S., *Computer Misuse: Response, Regulation and the Law* (Willan, Cullompton; 2009)

SF12 Furnell, S., 'Hackers, Viruses and Malicious Software', in Jewkes, Y., and Yar, M., (eds), *Handbook of Internet Crime,* (Willan, New York; 2012), pp. 173-193

GF06 Gordon, S., and Ford, R., 'On the definition and classification of cybercrime', in *Journal of Computer Virology,* vol. 2, no. 1, 2006, pp. 13-20

PG01 Grabosky, P., 'Virtual Criminality: old wine in new bottles', in *Social and Legal Studies*, vol. 10, no.2, 2001, pp. 243-249

GSD0 Grabosky, P., Smith, R., Dempsey, G., *Electronic Theft: Unlawful Acquisition in Cyberspace* (Cambridge University Press, Cambridge; 2001)

PG17 Graboksy, P., 'The evolution of cybercrime' in Holt, T. J., Cybercrime through an interdisciplinary lens (Routledge, 2017; Abingdon), pp. 15-31

GF06 Gordon, S., and Ford R., 'On the definition and classification of cybercrime', in *Journal of Computer Virology*, vol. 2 , no.1, 2006, pp. 13-20

SG06 Gordon, S., 'Understanding the adversary: Virus Writers and Beyond', in *IEEE Security and Privacy*, vol. 4, no. 5, 2006, pp. 67-70

HP12 HaId, S., and Pedersen, J., 'An Updated Taxonomy for Characterizing Hackers According to Their Threat Properties' in *14th International Conference on Advanced Communication Technology (ICACT)*, 2012, pp. 81-86

DH01 Hancock, D., 'To What Extent Should Computer Related Crimes Be the Subject of Specific Legislative Attention,' in *Albany Law Journal of Science & Technology*, vol. 12, no. 1, 2001, pp. 97-124

HC90 Hansard, House of Commons, 09 February 1990, vol. 166, cols. 1134 ff; available at https://api.parliament.uk/historic-hansard/commons/1990/feb/09/computer-misuse-bill

HC05 Hansard, House of Commons, 05 April 2005, vol. 432 cols. 1293 ff; available at https://publications.parliament.uk/pa/cm200405/cmhansrd/vo050405/debtext/50405-15.htm

HC05 Hansard, House of Commons, 12 July 2005, vol. 448, cols. 699 ff; available at https://publications.parliament.uk/pa/cm200506/cmhansrd/vo050712/debtext/50712-05.htm

JH11 Herrera, J., 'International Aspects of Cybercrime' in Clifford, R. (ed.),*Cybercrime: The Investigation, Prosecution and Defence of a Computer-related Crime, 3rd edition* (Carolina Academic Press, North Carolina; 2011), pp. 165-190

RH88 Hollinger, R., 'Computer Hackers Follow A Guttman-Like Progression', *Phrack Magazin*e, vol. 22, 1988; available at http://phrack.org/issues/22/7.html

HK12 Holt, T., and Kilger, M., 'Know your enemy: the Social Dynamics of Hacking', in *The Honeynet Project*, 2012, pp. 1-17; available at https://stratcomcoe.org/thomas-j-holt-max-kilger-know-your-enemy-social-dynamics-hacking

HSSK Holt, T., Strumsky, D., Smirnova, O., and Kilger, M., 'Examining the Social Networks of Malware Writers and Hackers', in *International Journal of Cyber Criminology*, vol. 6, no. 1, 2012, pp. 891–903

HO10 Home Office, *2010 Cyber Crime Strategy;* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf

HO13 Home Office, *Research Report 75: Cyber-crime: A review of the evidence*, 2013; available at https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence

HO15 Home Office, *Research Report 82: The Nature of Online Offending: Explored from Crown Prosecution Service Case Files*, 2015; available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/468067/horr82.pdf

HLP0 House of Lords, Science and Technology Committee, *Personal Internet Security volume 1: House of Lords Paper 165*, 2007; available at https://publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf

HC17 Hutchings, A., and Chua, Y., 'Gendering Cybercrime' in Holt, T. (ed.), *Cybercrime through an Interdisciplinary Lens* (Routledge, Abingdon; 2017), pp. 167-188

CCCD Hutchings, A., Cambridge Computer Crime Database, https://www.cl.cam.ac.uk/~ah793/cccd.html

VK16 Karagiannopoulos, V., 'Insider unauthorised use of authorised access: What are the alternatives to the Computer Misuse Act 1990?', in *International Journal of Law, Crime and Justice*, vol. 47, 2016, pp. 85-96

KAS0 Kilger, M., Arking, O., and Stutzman, J., 'Profiling', in *Honeynet Project, Know Your Enemy: Learning about security threats, 2nd edition*, (Addison-Wesley, Boston; 2004), pp. 505-556

AK13 Kruglanski, A., Bélanger, J., Gelfand, M., Gunaratna, R., Hettiarachchi, M., Reinares, F., Orehek, E., Sasota, J., and Sharvit, K., 'A (Self) Love Story: Redirecting the Significance Quest Can End Violence' in *American Psychologist,* vol. 68, no. 7, 2013, pp. 559-575

NK06 Kshetri, N., 'The Simple Economics of Cybercrimes', in *IEEE Security and Privacy,* vol. 4, no. 1, 2006, pp. 33-39

LCW8 Law Commission, *Working Paper No. 110: Computer Misuse*, 1988; available at https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2016/08/No.110-Computer-Misuse.pdf

LCR8 Law Commission, *Report no. 186: Computer Misuse*, 1989; available at https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2015/06/lc186.pdf

XL08 Li, X., 'The Criminal Phenomenon on the Internet: Hallmarks of Criminals and Victims Revisited through Typical Cases Prosecuted', in *University of Ottawa Law & Technology Journal*, vol. 5, no. 1, 2008, pp. 125-140

LCC0 Lu, C., Jen, W., Chang, W., and Chou, S., 'Cybercrime & Cybercriminals', in *Journal of Computers*, vol. 1, no. 6, 2006, pp. 1-10

NM08 MacEwan, N., 'The CMA 1990: Lessons from the Past and Predictions for its Future', *University of Salford Research Paper*, 2008; available at http://usir.salford.ac.uk/15815/6

SM06 Mcquade, S., *Understanding and Managing Cybercrime* (Allyn and Bacon, Boston; 2006)

MPF0 Meyers, C., Powers, S., Faissol, D., 'Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches', *Lawrence Livermore National Laboratory Technical report LLNL-TR-419041*, 2009; available at https://www.hsdl.org/?abstract&did=5953

SM05 Moitra, S., 'Developing Policies for Cybercrime: Some Empirical Issues', in *European Journal of Crime, Criminal Law and Criminal Justice*, vol. 13, no. 3, 2005, pp. 435-64

MPC1 Montasari, R., Peltola, P., Carpenter, V., 'Gauging the Effectiveness of Computer Misuse Act in Dealing with Cybercrimes', in *International Conference On Cyber Security and Protection Of Digital Services*, 2016, pp. 1-5; available at https://ieeexplore.ieee.org/document/7502346/

NTV0 Nykodym, N., Taylor, R., and Vilela, J., 'Criminal profiling and insider cyber crime', in *Computer Law and Security Report*, vol. 21, no. 5, 2005, pp. 408-41

EO14 Onyilofor, E., 'The Effectiveness of the Computer Misuse Act 1990: Technological development and technological neutrality', 2014; available at https://ssrn.com/abstract=2760024

PST9 Parliamentary Office of Science and Technology, *Computer Misuse: Information for Members- Briefing Note*, 1990; available at https://researchbriefings.parliament.uk/ResearchBriefing/Summary/POST-PN-9

PJA0 Police and Justice Act 2006; available at http://www.legislation.gov.uk/ukpga/2006/48/contents

RGS8 *R. v. Gold and Schifreen*, AC 1063, Crim LR 437 (HL), 1988

ERJF Raymond, E., *The Jargon File;* available at https://people.redhat.com/zaitcev/notes/hacker-howto.html

MR00 Rogers, M., 'A New Hacker Taxonomy', University of Manitoba, 2000; available at http://homes.cerias.purdue.edu/~mkr/hacker.doc

MR05 Rogers, M., 'The Development of a Meaningful Hacker Taxonomy: A Two Dimensional Approach', Purdue University, 2005; available at https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2005-43.pdf

MR06 Rogers, M., ‘A Two-dimensional Circumplex Approach to the Development of a Hacker Taxonomy’, in *Digital Investigation*, vol. 3, no. 2, 2006, pp. 97–102

MR11 Rogers, M., ‘The Psyche of Cybercriminals: A Psycho-Social Perspective’, in Ghosh, S., and Turrini, E., *Cybercrimes: A Multidisciplinary Analysis* (Springer, Berlin; 2011), pp. 217-235

JR54 Rousseau, J., *Discourse on the Origin and Basis of Inequality Among Men*, 1754; available at https://www.aub.edu.lb/fas/cvsp/Documents/DiscourseonInequality.pdf879500092.pdf

SH12 Schell, B., and Holt, T., ‘A Profile of the Demographics, Psychological Predispositions, and Social/Behavioral Patterns of Computer Hacker Insiders and Outsiders’, in *Information Resources Management Association: Cyber-crime: Concepts, Methodologies, Tools and Applications, Volume 3* (IGI Global; 2012), pp. 1461-1484

SM12 Schell, N., and Melnychuk, J., ‘Female and Male Hacker Conference Attendees: Their Autism-Spectrum Quotient (AQ) Scores and Self-Reported Adulthood Experiences’ in *Information Resources Management Association: Cyber-crime: Concepts, Methodologies, Tools and Applications, Volume 2* (IGI Global; 2012), pp. 1975-1099

SLC8 Scottish Law Commission, *Report on Computer Crime - Report No. 106,* 1987; available at https://www.scotlawcom.gov.uk/files/1812/7989/7451/rep106.pdf

RS15 Seebruck, R., ‘A Typology of Hackers: Classifying Cyber Malfeasance using a Weighted Arc Circumplex Model’, in *Digital Investigation*, vol. 14, 2015, pp. 36-45

SCA1 Serious Crime Act 2015; available at http://www.legislation.gov.uk/ukpga/2015/9/contents/enacted

RS07 Sharma, R., ‘Peeping Into A Hacker’s Mind: Can Criminological Theories Explain Hacking?’ in *SSRN Electronic* Journal, 2007, pp.1-20; available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1000446

SRP9 Shaw, E., Ruby, K., Post, J., ‘The Insider Threat to Information Systems: The Psychology of the Dangerous Insider’, in *Security Awareness Bulletin*, no. 2, 1998; available at https://www.semanticscholar.org/paper/The-Insider-Threat-to-Information-Systems-Shaw-Ruby/d806df7d5cd61c686a35fa694757059d14faffbc

SGU0 Smith, R., Grabosky, P., and Urbas, G., *Cyber Criminals on Trial* (Cambridge University Press, Cambridge; 2004)

KS16 Steinmetz, K., *Hacked: A Radical Approach to Hacker Culture and Crime* (New York University Press, New York; 2016)

PT99 Taylor, P., *Hackers: Crime in the Digital Sublime* (Routledge, London; 1999)

PT00 Taylor, P., ‘Hackers - Cyberpunks and Microserfs?’ in Thomas, D., and Loader, B. (eds.) *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age,* (Routledge, London; 2000), pp. 36-55

PT01 Taylor, P., ‘Hacktivism: In Search of Lost Ethics?’ in Wall, D. (ed.), *Crime and the Internet: Cybercrime and Cyberfears* (Routledge, London; 2001), pp. 59-74

TFL1 Taylor, R., Fritsch, E., and Liederbach, J., *Digital Crime and Digital Terrorism, 3rd edition* (Pearson, New Jersey; 2015)

TLY1 Tianji, C., Li, D., Yanyu X., and Chang, L., ‘Characteristics of Cybercrimes: Evidence from Chinese Judgment Documents’, in *Police Practice and Research*, vol. 19, no. 6, 2018, pp. 582-595

TL00 Thomas, D., and Loader, B., ‘Cybercrime in the Information Age’ in Thomas, D., and Loader, B. (eds.), C*ybercrime: Law Enforcement, security and surveillance in the Information Age,* (Routledge, London; 2000) pp. 1-13

TG11 Turgeman-Goldschmidt, O., ‘Identity Construction Among Hackers’, in Jaishanker, K. (ed.), *Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour,* (CRC Press, Boca Raton; 2011), pp. 31-51

TG12 Turgeman-Goldschmidt, O., ‘Between Hackers and White- Collar Offenders’, in *Information Resources Management Association: Cyber-crime: Concepts, Methodologies, Tools and Applications, Volume 3* (IGI Global; 2012), pp. 1528-1547

MTCE Turner, M., www.computerevidence.co.uk
USSS U.S. Secret Service, *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*, 2004; available at http://www.ustreas.gov/usss/ntac_its.shtml
USSS US Secret Service, I*nsider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*, 2005; available at http://www.ustreas.gov/usss/ntac_its.shtml
IW00 Walden, I., 'Computer Crime', in Reed C., and Angel, J. (eds.), *Computer Law, Fourth Edition* (Oxford University Press, Oxford; 2000), pp. 277-298
IW16 Walden, I., *Computer Crimes and Digital Investigations* (Oxford University Press, Oxford; 2016)
WLD1 Wada, F., Longe, O., and Danquah, P., 'Action Speaks Louder than Words- Understanding Cyber Criminal Behavior using Criminological Theories', in *The Journal of Internet Banking and Commerce*, vol. 17, no. 1, 2012, pp. 1-12
DW99 Wall, D., 'Cyber-crimes: New wine, no Bottles?' in Davies P., Francis P. and Jupp V., (eds.), *Invisible Crimes: Their Victims and their Regulation* (Macmillan, London; 1999), pp. 105-139
DW01 Wall, D., 'Cybercrimes and the Internet' in Wall, D. (ed.), *Crime and the Internet: Cybercrime and Cyberfears* (Routledge, London; 2001), pp. 1- 17
DW07 Wall, D., *Cybercrime: The Transformation of Crime in the Information Age* (Polity, Cambridge; 2007)
DW09 Wall, D., 'Introduction', in Wall, D. (ed.), *Crime and Deviance in Cyberspace* (Ashgate, Farnham; 2009), pp. xv-xxx
MW90 Wasik, M., *Crime and the Computer* (Oxford University Press, Oxford; 1990)
MW12 Wasik, M., 'The Emergence of Computer Law', in Jewkes, Y., and Yar, M. (eds.), *Handbook of Internet Crime* (Routledge, New York; 2012), pp. 395-412
MWK1 Weulen Kranenbarg, M., 'Cyber-offenders Versus Traditional Offenders: An Empirical Comparison', Vrije Universiteit Amsterdam, 2018; available at https://research.vu.nl/en/publications/cyber-offenders-versus-traditional-offenders-an-empirical-compari
HW03 Woo, H-J., 'The Hacker Mentality: Exploring the Relationship Between Psychological Variables and Hacking Activities', The University of Georgia; available at https://www.semanticscholar.org/paper/The-hacker-mentality-%3A-exploring-the-relationship-Woo/3302e173939ae434ad30f91d4c60d69f5e4a05e3
WKD0 Woo, H-J., Kim, Y., and Dominick, J., 'Hackers: Militants or Merry Pranksters? A Content Analysis of Defaced Web Pages', in *Media Psychology*, vol. 6, no. 1, 2004, pp. 63-82,
KW86 Wong, K., 'Computer Fraud in the UK - The 1986 Picture', in *Computer Fraud and Security Bulletin*, vol. 9, no. 1, 1986, pp. 3-11
KW90 Wong, K., 'A Survey of the BIS Casebook', in *Computer Fraud and Security Bulletin*, vol. 1990, no. 11, 1990, pp. 9-15
VBS0 Voiskounsky, A., Bahaeva, J., and Smyslova, O., 'Attitudes towards computer hacking in Russia', in Thomas, D., and Loader, B. (eds.), C*ybercrime: Law Enforcement, security and surveillance in the Information Age* (Routledge, London; 2000), pp. 57-84
MY06 Yar, M., *Cybercrime and Society* (Sage, London; 2006)
YS19 Yar, M., and Steinmetz, K., *Cybercrime and Society, 3rd Edition* (Sage, London; 2019)

Student Number: 100910920
James Crawford

The Computer Misuse Act and Hackers: A review of those convicted under the Act

Appendix A

Supervisor: Dr. Rikke Bjerg Jensen

Table 1

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Tony Spencer	https://www.essexlive.news/news/essex-news/sexual-predator-filmed-children-getting-3802832	Yes	January 2020	Low skill (used open source software to access accounts)	He was sentenced for nine counts of voyeurism, five counts of taking indecent photographs of a child and 12 counts of Computer Misuse Act offences. He was found guilty of gaining unauthorised access to multiple iCloud accounts and obtaining sexual images before sharing them online. During several searches of his home address, officers found computer equipment containing the victims' pictures as well as software used to access these accounts. Twelve victims were identified and they were informed. He also filmed children and young women getting changed at a leisure centre. [CCCD]	Sexual Obtained images intended for sexual gratification	Outsider	38	Male	Lone operator	None identified
Daniel Moonie	https://www.dailymail.co.uk/news/article-7898807/Hospital-administrator-sacked-using-NHS-computer-download-10-000-records-spared-jail.html https://www.theregister.co.uk/2020/01/20/stoke_on_trent_hospital_hacker_9000_cardiac_images/	Yes	January 2020	Low skill (used open source software and known credentials to commit criminality	He pleaded guilty to causing a computer to secure unauthorised access to computer data contrary to Section 1(1) and (3) of the Computer Misuse Act 1990, and causing a computer to perform function to secure unauthorised access to a program/data. While a Royal Stoke Hospital employee, he used malicious software to crack the passwords of his co-workers and access over 10,000 confidential hospital files. He stole confidential information including patient and employee records. When it was discovered he had gained unauthorised access to the hospital's computer network, he was dismissed from the hospital and cautioned by police. He agreed as part of the terms of the police caution that he would not access any IT system within the hospital, enter the hospital (unless a patient, visiting a patient or for HR reasons), or contact staff unless at the request of the HR department. However, after the caution, he again gained unauthorised access to the hospital's computer systems, obtaining and saving confidential material. During his arrest officers searched his home and discovered two hard drives with over 10,000 files including jpeg images of cardiac tests on patients, sensitive patient records and confidential employee files. [CCCD]	Revenge He was motivated by a desire to put right his previous sacking for accessing unauthorised material; he believed he had been unfairly treated and that he was not alone in his earlier hacking behaviour and thought he could demonstrate this through further activity	Insider	27	Male	Lone operator	None identified
Vladimir Yanpolsky	https://perma.cc/WR3N-FNRA	Yes	January 2020	Low skill (no evidence of how he gained access, but he used his home IP address)	An IT specialist, he accessed the computer system of a company he had been previously dismissed from months earlier and caused an outage. He was found guilty of an offence under section 3(1) of the Computer Misuse Act 1990. The London-based IT services company experienced a critical system failure, and enquiries revealed that these had been caused by network intrusions from someone gaining access remotely. An analysis of the IP addresses of computers that had accessed the company's computer network around the time of the system failure, found several were linked to his home address and new place of work. Devices seized from his premises linked him to the offences. [CCCD]	Revenge Motivated to exact revenge following his dismissal from victim company.	Insider	45	Male	Lone operator	None identified

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Anwar Batson	https://www.birminghammail.co.uk/news/midlands-news/crook-who-tried-hack-national-17548431; computer evidence https://www.theregister.co.uk/2019/11/13/anwar_batson_national_lottery_accounts_court_case/	Yes	January 2020	Low skill (used open source tool)	Anwar Batson, 29, used hacking tool Sentry MBA to attack UK National Lottery operator Camelot's database of 9m customer accounts. Guilty pleas to four counts under CMA. Jailed for nine months. [MTCE]	Money Criminality was conducted with sole aim of obtaining money.	Outsider	29	Male	Group (low level criminal group)	None identified
Scott Cowley	https://www.liverpoolecho.co.uk/news/liverpool-news/pervert-hacked-webcams-watch-women-17521033 https://www.infosecurity-magazine.com/news/uk-man-jailed-for-using-rat-to-spy/	Yes	January 2020	Low skill (used open source software, purchased using own PayPal account)	Scott Cowley, 27, purchased Imminent Monitor RAT (IM-RAT) that he used to spy on three women's webcams and secretly film them undressing and having sex. Guilty pleas to four counts under CMA. Jailed for two years and ordered to sign on the Sex Offenders Register and comply with a Sexual Harm Prevention Order for 10 years. [MTCE]	Sexual Criminality was aimed at obtaining sexual images of victims.	Outsider	27	Male	Lone operator	None identified
Scott Burns	https://www.bbc.co.uk/news/uk-england-leeds-50843669 https://www.theregister.co.uk/2019/12/18/jet2_hacker_scott_burns_prison_sentence/	Yes	December 2019	Low skill (used home IP address and known login credentials to conduct criminality)	Disgruntled former Jet2 IT contractor Scott Burns, 27, deleted an entire domain's user accounts in a revenge attack that shut down Jet2's systems for 12 hours in January 2018 and accessed the email account of Jet2's chief executive. Recovery from the attack cost the company £165,000. Guilty pleas to eight counts under CMA. Sentenced to imprisonment for 10 months. Laptop order to be destroyed. Judge referred to the "pernicious and far-reaching impact" of this type of attack. [MTCE]	Revenge Criminality conducted following curtailment of employment. Judge stated: 'This was a revenge attack for a perceived slight you had suffered'.	Insider	27	Male	Lone operator	None identified
Grant Morton	https://www.scotsman.com/news/uk-news/it-expert-installed-spy-cameras-his-home-watch-teenage-house-guests-use-bathroom-1403136	Yes	November 2019	Unskilled (hands on access to unlocked devices)	He pleaded guilty to voyeurism, taking an indecent image of a child, distributing indecent images, having indecent images of a child and an offence under the Computer Misuse Act. He installed spy cameras in his home to watch three teenage house guests. He also stole private photos from a girl's phone while charging it from his laptop and images from a woman while he fixed her computer. He shared some of the images with friends over Skype. When police raided his home they found more than 55,000 indecent images, including 125 in the most serious category. [CCCD]	Sexual Stole sexual images for own viewing, and shared with others.	Outsider (known to victim)	46	Male	Lone operator	None identified
Sherry Bray	https://www.cps.gov.uk/wessex/news/statement-following-sentencing-sherry-bray-and-christopher-ashford https://www.bbc.co.uk/news/uk-england-wiltshire-48929607	No	September 2019	Unskilled (unauthorised use of authorised access)	Bray (49) a Director of Camera Security Services Limited Chippenham and her employee Ashford (62) were driven by morbid curiosity and accessed CCTV footage of the post mortem of footballer Emiliano Sala. Guilty Pleas. Bray sentenced to 14 months in prison. [MTCE]	Curiosity Examining footage of incident gaining national coverage	Insider	49	Female	Group	None identified

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Chris Ashford	https://www.cps.gov.uk/wessex/news/statement-following-sentencing-sherry-bray-and-christopher-ashford https://www.bbc.co.uk/news/uk-england-wiltshire-48929607	No	September 2019	Unskilled (unauthorised use of authorised access)	Bray (49) a Director of Camera Security Services Limited Chippenham and her employee Ashford (62) were driven by morbid curiosity and accessed CCTV footage of the post mortem of footballer Emiliano Sala. Guilty Pleas. Ashford to 5 months in prison. [MTCE]	Curiosity Examining footage of incident gaining national coverage	Insider	62	Male	Group	None identified
Elliott Gunton	https://www.bbc.co.uk/news/uk-england-norfolk-47790458 https://krebsonsecurity.com/tag/elliott-gunton/ https://www.theregister.com/2016/11/15/talktalk_h1_fy2017_results_hacker_teen_pleads_guilty/ https://www.edp24.co.uk/news/crime/teen-computer-hacker-pleads-guilty-to-offences-at-norwich-crown-court-1-6143474 https://www.theregister.com/2019/04/03/elliott_gunton_denies_instagram_login_sales_bitcoin/ https://www.theregister.com/2019/08/19/elliott_gunton_400k_repay_instagram_hacking_telstra/ https://www.theregister.com/2019/09/26/talktalk_hacker_indicted_in_us/	Yes	August 2019	Semi-skilled (prolonged and effective use of open source hacking tools; but committed some basic security errors)	Convicted hacker (aged 16 at time of TalkTalk attack) Gunton, 19, used a suite of hacking tools to penetrate network providers and take over high profile social media accounts before offering them for sale on hacker forums. Australian telecoms provider Telstra attack yielded an Instagram account with a following of 1.3m users whose credentials were sold on. Sentenced to 20 months in prison, ordered to pay £407k and given a three and a half year Criminal Behaviour Order. [MTCE] Also stole funds from cryptocurrency exchange EtherDelta.	Money, Entertainment, Status, Ego Gunton stole data/instagram accounts and sold them, and stole money from bitcoin wallets. He also took control of an instagram account with 1.2 million followers and sent abusive messages to those interacting with the account.	Outsider	19	Male	Lone operator	None identified

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Liam Watts	https://www.theregister.co.uk/2019/08/15/liam_watts_dos_cheshire_greater_manchester_police_jailed/ https://www.bbc.co.uk/news/uk-england-lancashire-48054973 https://www.dailymail.co.uk/news/article-7349207/Hacker-20-jailed-16-months-revenge-cyber-attacks-police-websites-bomb-hoax.html	Yes	August 2019	Low skill (purchased botnet for one off criminality)	Convicted hacker Watts, 20, used SYN flood DDoS denial of service attacks on GMP and Cheshire police public websites that made them inaccessible. Claimed one attack was in retaliation for a separate conviction for a bomb hoax days after Manchester Arena bombing. Guilty pleas. Sentenced to 16 months in a young offenders' institution, five year restraining order to prevent him from deleting browser history, police inspections and destruction of computers. [MTCE]	Revenge Clearly stated revenge as motivation on Twitter: "@Cheshirepolice want to send me to prison for a bomb hoax I never did, here you f****** go, here is what I'm guilty of."	Outsider (known to victim)	20	Male	Lone operator	ADHD and alcohol-related neurodevelopment disorder
Okechukwu Efobi	https://www.theregister.co.uk/2019/07/11/met_police_sgt_pleads_guilty_computer_misuse_crimes/ https://www.policeprofessional.com/news/former-officer-who-monitored-investigation-into-himself-found-guilty-of-gross-misconduct/	No	3 July 2019	Unskilled (unauthorised use of authorised access)	Serving Met Police officer Sergeant Efobi accessed Met police databases to check progress of a criminal investigation of his own conduct. Guilty plea to three offences. Sentenced to 12 month community order, 150 hours of community service and payment of £90 victim surcharge and £450 costs. [MTCE]	Curiosity Desire to know how investigation into his own conduct was progressing.	Insider	Unknown	Male	Lone operator	None identified
Michael Lawrence	https://www.birminghammail.co.uk/news/midlands-news/shamed-pcso-blew-up-childhood-16568630	No	July 2019	Unskilled (unauthorised use of authorised access)	A former PCSO for Staffordshire Police, he pleaded guilty to fraud and computer misuse. He admitted making false claims about his annual leave and misusing police systems. In May 2018 concerns had been raised about his time-keeping and the booking of annual leave. Audits were subsequently carried out and identified that he had booked leave and then made false claims on the force's HR management system that he was at work. An internal investigation also discovered that he had accessed the force's incident log and viewed 879 incidents without a lawful policing purpose. [CCCD]	Personal gain/Curiosity Over-rode system to input additional working hours, and searched system in order to gain (according to sentencing judge) 'gossip out of the computer and tittle tattle about people in your local area'.	Insider	29	Male	Lone operator	None identified
Graeme Brandon	https://www.bbc.co.uk/news/uk-england-dorset-48199225 https://www.mirror.co.uk/news/uk-news/royal-marine-sobs-man-who-14999510	No	May 2019	Unskilled (downloaded photos from Facebook and set up fake account)	Brandon, 44, stole a user's identity from a Facebook account and used it to send WhatsApp messages with indecent images of himself to 27 women whose mobile numbers he had harvested from Gumtree. [MTCE]	Sexual Conducted criminality in order to send sexually explicit images of himself to victims.	Outsider	44	Male	Lone operator	None identified

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Zain Qaiser	https://www.bbc.co.uk/news/uk-47800378 https://nationalcrimeagency.gov.uk/news/hacker-from-russian-crime-group-jailed-for-multi-million-pound-global-blackmail-conspiracy https://www.cps.gov.uk/cps/news/hacker-behind-ps500k-online-blackmail-campaign-jailed	Yes	April 2019	Semi-skilled (prolonged, sophisticated campaign involving ransomware and DOSing)	Multi-million pound global blackmail conspiracy. Between 2012 and 2014 Computer Science student Qaiser, 24, planted ransomeware attacks (using Angler Exploit Kit) on porn websites designed to display threatening warning messages from the FBI or local police force and to lock users' computers (using Reveton or Cryptolocker). [MTCE]	Money Criminality was conducted with sole aim of obtaining money.	Outsider	24	Male	Group (part of organised criminal group)	Mental health issues mentioned
Scott Willey	https://www.lawgazette.co.uk/news/fake-barrister-pursuing-dream-career-jailed-after-working-in-chambers-for-months/5069841.article https://www.standard.co.uk/news/crime/fraudster-who-took-on-18-cases-in-two-years-as-bogus-barrister-jailed-for-27-months-a4106941.html	Yes	March 2019	Unskilled (access to colleague's email- no indication of how obtained)	Willey, who had failed law examinations and with no legal qualifications accessed a barrister colleague's email account to copy his Practising Certificate in order to produce a faked copy in his own name. [MTCE]	Other (personal gain) Computer misuse was intended to augment wider criminality aimed at fraudulently pursuing his career as a barrister despite lack of necessary qualifications.	Insider	27	Male	Lone operator	None identified
Zammis Clark	https://www.theregister.co.uk/2019/03/29/buildfeed_malwarebytes_guilty_hacking_microsoft_nintendo/ https://www.standard.co.uk/news/crime/autistic-man-24-spared-jail-for-nintendo-cyber-attacks-after-court-is-told-he-cant-help-himself-a4104211.html; https://www.theverge.com/2019/3/28/18286027/microsoft-nintendo-vtech-security-hack-breach-researcher-guilty	Yes	March 2019	Semi-skilled (persistent access to Windows over significant period)	Security researcher Clark, 24, aka Slipstream / Raylee and Hounsell, 26, hacked into Microsoft OS software development systems, downloaded 43,000 files and shared details of their exploits online with other hackers; damage estimated at $2M. Clark also hacked into Nintendo systems and stole 2,000 user ID credentials; damage estimated at £1.4M. Autistic Clark pleaded guilty to three CMA charges. Sentenced to 15 month prison sentence suspended for 18 months, rehabilitation activity order (25 days), 5 year serious crime prevention order and £140 victim surcharge. [MTCE]	Entertainment, Ego, Entrance to social group, Status He shared his access and hacks on IRC chatrooms so that others would recognise and utilise his achievements. Clark's barrister also stated that his hacking is akin to an addiction and he "couldn't help himself."	Outsider	24	Male	Group (shared details of hack with others so they could participate)	Autistic

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Thomas Hounsell	https://www.theregister.co.uk/2019/03/29/buildfeed_malwarebytes_guilty_hacking_microsoft_nintendo/; https://www.standard.co.uk/news/crime/autistic-man-24-spared-jail-for-nintendo-cyber-attacks-after-court-is-told-he-cant-help-himself-a4104211.html https://www.theverge.com/2019/3/28/18286027/microsoft-nintendo-vtech-security-hack-breach-researcher-guilty	Yes	March 2019	Low skill (used Clark's hack to conduct own research)	Security researcher Clark, 24, aka Slipstream / Raylee and Hounsell, 26, hacked into Microsoft OS software development systems, downloaded 43,000 files and shared details of their exploits online with other hackers; damage estimated at $2M. Hounsell pleaded guilty to one CMA charge. Sentenced to 6 month prison sentence suspended for 18 months, unpaid work order (100 hours) and £115 victim surcharge.[MTCE]	Entertainment Hounselll was interested in Windows build strings as part of his work running the website Buildfeed. He used Clark's access to run searches to inform his work.	Outsider	26	Male	Group (piggy backed off Zammis Clark's hack)	None identified
Steffan Needham	https://www.theregister.co.uk/2019/03/20/steffan_needham_aws_rampage_prison_sentence_voova/ https://www.getreading.co.uk/news/reading-berkshire-news/man-jailed-after-hack-caused-15992318#	Yes	March 2019	Low skill (did not obfuscate IP, no evidence of complex techniques used)	Sacked IT consultant Needham, 36, used a former IT colleague's Login ID to delete client data on his former employer Voova's 23 servers. Losses estimated at £500,000 and several redundancies resulted. Found guilty. Sentenced to two years in prison Appeal dismissed. [MTCE]	Revenge Carried out attack in response to sacking.	Insider	36	Male	Lone operator	None identified
Norman Stephens	https://www.bbc.co.uk/news/uk-england-coventry-warwickshire-47232767	No	February 2019	Unskilled (unauthorised use of authorised access)	Warwickshire Police Detective Constable Stephens, 47, used force incident management, intelligence and ANPR SYSTEMS to check colleagues' personal data. Guilty plea. Sentenced to 12 month community order, ordered to do 150 hours unpaid work and pay £270 costs. [MTCE]	Curiosity Snooping on colleagues' personal data.	Insider	47	Male	Lone operator	
Samir Desai	https://leamingtonobserver.co.uk/news/computer-hacker-who-targeted-former-employer-ordered-to-pay-20000-compensation-10809/ https://www.birminghammail.co.uk/news/local-news/samir-desai-sutton-coldfield-warwickshire-15676312	Yes	January 2019	Low skill (no evidence of complex hacking techniques)	Desai, 41, attacked his former employer's computer system and caused "significant disruption and financial loss". Guilty plea. Sentenced to 15 month prison suspended for two years, ordered to pay compensation of £20,000 and £1,800 of costs. [MTCE]	Other (unable to identify) Police explicitly stated that they were 'unable to identify a motive' for the crime.	Insider	41	Male	Lone operator	None identified

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Daniel Kaye	https://www.bbc.co.uk/news/uk-46840461 https://krebsonsecurity.com/2019/01/courts-hand-down-hard-jail-time-for-ddos/#more-46248 https://www.bloomberg.com/news/features/2019-12-20/spiderman-hacker-daniel-kaye-took-down-liberia-s-internet https://krebsonsecurity.com/2017/07/who-is-the-govrat-author-and-mirai-botmaster-bestbuy/	Yes	January 2019	High skill (controlled botnet Mirai#14; alleged to have developed govRat software by security researcher Krebs)	"Hacker for hire" Kaye, 30, was paid $30,000 by a competitor to attack Liberian mobile phone company Lonestar systems using a zombie botnet to execute DDoS attacks that brought down Lonestar's servers. Guilty plea. Sentenced to 32 months imprisonment. Investigation by the NCA's National Cyber Crime Unit (NCCU). [MTCE]	Money Kaye conducted his hacking activity off the back of tasking from others; he was paid to carry out the attacks that he did and had no other personal motivation for carrying out those specific attacks.	Outsider	30	Male	Tasked by third parties	None identified
Jane Denmark	https://www.leicestermercury.co.uk/news/leicester-news/leicestershire-police-control-room-employee-2302130	No	December 2018	Unskilled (unauthorised use of authorised access)	Civilian employee Denmark, 56, used her privileged access as a control room call handler at Leicestershire Police to access police computer systems to find her son's address. Guilty plea. Six months community order. [MTCE]	Curiosity Locating estranged son's address.	Insider	56	Female	Lone operator	
Ernest Edjeren	https://www.readingchronicle.co.uk/news/17206617.reading-crown-court-was-told-that-edjeren-attempted-a-scam-that-cost-the-orange-county-employees-retirement-scheme-pensions-fund-almost-200000/	Yes	November 2018	Low skill (used victim details to set up on online bank payments via VPN)	Edjeren, 39, attempted to steal the pensions of retired public sector workers in Orange County USA by breaking into their accounts and setting up payments using his own Paypal account. Pension company defrauded of £100,00 and spent £200,00 on fixing their software. Found guilty of Unauthorised access by a majority verdict. Found guilty of fraud by unanimous verdict. Sentenced to three years in prison. SEROCU Cyber Crime Unit investigation. [MTCE]	Money Criminality was conducted with sole aim of obtaining money.	Outsider	39	Male	Lone operator	None identified
Mustafa Kasim	https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/six-month-prison-sentence-for-motor-industry-employee-in-first-ico-computer-misuse-act-prosecution/ https://www.bbc.co.uk/news/technology-46185667	Yes	November 2018	Unskilled (used known login credentials)	Kasim used a former co-worker's login credentials to steal personal details (names, phone numbers, vehicle and accident details) from his former employer's vehicle repair software package. Guilty plea. Sentenced to six months in prison. First successful CMA prosecution brought by the Information Commissioner's Office (ICO). July 2019 hearing found that Kasim had benefitted financially and ordered to pay a £25,500 confiscation order and £8,000 costs. [MTCE]	Money Criminality was conducted with sole aim of gaining an unfair business advantage.	Insider	NA	Male	Lone operator	None identified

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Matthew Hanley	https://www.bbc.co.uk/news/uk-england-stoke-staffordshire-39725208?ocid=socialflow_twitter https://www.theregister.co.uk/2017/04/27/talktalk_hack_duo_cop_pleas/ https://www.theguardian.com/uk-news/2018/nov/19/two-men-jailed-talktalk-hacking-customer-data [2019] EWCA Crim 95	Yes	November 2018	Semi-skilled (concerted hacking into Talk Talk, although did not identify vulnerability)	Hanley, 23, and Allsopp, 21, stole more than 150,000 customer records in the £77 million 2015 attack on TalkTalk website vulnerabilities to DDoS and SQL injection attacks. Guilty pleas. Hanley sentenced to 12 months jail. [MTCE]	Status; Ego; Entrance to Community On Appeal, the Judge accepted the point that Hanley and Allsopp were motivated by 'bravado within a community of like-minded souls, rather than financial gain.'	Outsider	23	Male	Group (with Allsopp)	Social anxiety disorder
Connor Allsopp	https://www.bbc.co.uk/news/uk-england-stoke-staffordshire-39725208?ocid=socialflow_twitter https://www.theregister.co.uk/2017/04/27/talktalk_hack_duo_cop_pleas/ https://www.theguardian.com/uk-news/2018/nov/19/two-men-jailed-talktalk-hacking-customer-data [2019] EWCA Crim 95	Yes	November 2018	Semi-skilled (concerted hacking into Talk Talk, although did not identify vulnerability)	Hanley, 23, and Allsopp, 21, stole more than 150,000 customer records in the £77 million 2015 attack on TalkTalk website vulnerabilities to DDoS and SQL injection attacks. Guilty pleas. Allsopp sentenced to eight months Allsopp's appeal against sentence failed. [MTCE]	Status; Ego; Entrance to Community On Appeal, the Judge accepted the point that Hanley and Allsopp were motivated by 'bravado within a community of like-minded souls, rather than financial gain.'	Outsider	21	Male	Group (with Hanley)	None identified

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Philip Tong	https://www.bbc.co.uk/news/uk-england-derbyshire-45995907	Yes	October 2018	Unskilled (basic social engineering techniques to obtain ID)	Owner/Directors and managers at employment firm Smart Recruitment AKA Workchain Ltd made bogus telephone calls to obtain employees' account IDs. Then used the IDs to log onto the NEST online system to opt the workers out of their pension schemes, thus avoiding the firm making pension payments on their behalf. Owner/Directors Phillip Tong and Adam Hinkley received four month prison terms suspended for two years, ordered to complete 200 hours community service and were ordered to pay costs of £11,250 each. Workchain LTD was fined £200,000. Prosecution by The Pensions Regulator. Largest financial penalties to date and first fine of a corporate entity. On appeal Court of Appeal amended the fine handed down to Workchain from £200,000 to £100,000. [MTCE]	Money Criminality aimed at saving business costs via defrauding employees	Insider	41	Male	Group (with Hinkley)	None identified
Adam Hinkley	https://www.bbc.co.uk/news/uk-england-derbyshire-45995907	Yes	October 2018	Unskilled (basic social engineering techniques to obtain ID)	Owner/Directors and managers at employment firm Smart Recruitment AKA Workchain Ltd made bogus telephone calls to obtain employees' account IDs. Then used the IDs to log onto the NEST online system to opt the workers out of their pension schemes, thus avoiding the firm making pension payments on their behalf. Owner/Directors Phillip Tong and Adam Hinkley received four month prison terms suspended for two years, ordered to complete 200 hours community service and were ordered to pay costs of £11,250 each. Workchain LTD was fined £200,000. Prosecution by The Pensions Regulator. Largest financial penalties to date and first fine of a corporate entity. On appeal Court of Appeal amended the fine handed down to Workchain from £200,000 to £100,000. [MTCE]	Money Criminality aimed at saving business costs via defrauding employees	Insider	39	Male	Group (with Tong)	None identified
Dominik James	https://www.harwichandmanningtreestandard.co.uk/news/south_essex_news/16611052.essex-police-operation-sees-hacker-who-stole-30-people-private-photos-get-eight-months-sentence/	Yes	August 2018	Low skill (used software to access accounts)	James, 31, hacked into over 30 women's iCloud accounts to take private information and photographs and share them online. Guilty plea to five s1 counts. Sentenced to eight month concurrent sentences. [MTCE]	Sexual Criminality aimed at obtaining personal photographs of women and posting them online.	Outsider	31	Male	Lone operator	None identified
Sadiya Dakri	https://www.leicestermercury.co.uk/news/leicester-news/agency-worker-illegally-accessed-leicestershire-1693148	No	July 2018	Unskilled (unauthorised use of authorised access)	Dakri, 22, a temp at Leicestershire Police accessed police systems without authorisation, photographing sensitive police documents relating to her brother in law. Guilty plea to four counts of unauthorised access to computer material. Sentenced to 12 months in prison. [MTCE]	Criminality Activity conducted in order to try and find out information related to further criminality.	Insider	22	Female	Group	

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Daniel Thompson	https://www.businesscloud.co.uk/news/naive-cyber-criminals-jailed-after-13-lottery-heist	Yes	July 2018	Low skill (used brute forcing application to attack National lottery)	He pleaded guilty to unauthorised computer access with intent to commit other offences, and two counts of obtaining an article for the commission of a computer misuse offence. They used an online application to gain access to National Lottery customer accounts. He had the application used for the brute force attack on his laptop, and evidence of unauthorised access. He admitted downloading files and said he was unaware that he was responsible for tens of thousands of login attempts. [CCCD]	Money Criminality was conducted with sole aim of obtaining money.	Outsider	27	Male	Group (with Kayode)	None identified
Idris Kayode Akinwunmi	https://www.businesscloud.co.uk/news/naive-cyber-criminals-jailed-after-13-lottery-heist	Yes	July 2018	Low skill (gained access to one National Lottery account alongside Thompson)	He pleaded guilty to unauthorised computer access with intent to commit other offences and fraud by false representation. They used an online application to gain access to National Lottery customer accounts. He gained access to one customer account and removed £13. [CCCD]	Money Criminality was conducted with sole aim of obtaining money.	Outsider	21	Male	Group (with Thompson)	None identified
Grant West	https://www.bbc.co.uk/news/uk-england-44249888 https://www.bbc.co.uk/news/uk-england-kent-49450676 https://www.cps.gov.uk/cps-london-north-london-south/news/prolific-computer-hacker-jailed-10-years	Yes	May 2018	Semi-skilled (used open source software for brute force and phishing attacks, but in a concerted fashion against hundreds of websites in order to sell the data)	West, 26, used Brute force attacks (Sentry MBA) in August and September 2017 to target some 100 companies' websites (including Just Eat, Sainsburys, Nectar, Groupon, AO.com, Ladbrokes, Coral betting, Uber, Asda, T mobile and Argos) to harvest tens of thousands of customers' email addresses, passwords and financial data to be sold on the dark web. Guilty pleas. Sentenced to 10 years eight months in jail. [MTCE]	Money Criminality was aimed at obtaining data to sell.	Outsider	26	Male	Lone operator	None identified
Kane Gamble	https://www.telegraph.co.uk/news/2017/10/06/teen-admits-bid-hack-cia-chiefs-computer-leicestershire-home/ https://www.bbc.co.uk/news/uk-england-leicestershire-43840075 https://www.bbc.co.uk/news/uk-england-leicestershire-41527941 https://www.theguardian.com/technology/2018/apr/20/two-years-detention-for-uk-teenager-who-cyberterrorised-us-officials-kane-gamble	Yes	May 2018	Semi-skilled (concerted effort against prominent targets and using a variety of techniques)	15 year-old Leicester male founder of Crackas With Attitude (CWA) used Social engineering to target email accounts of US government chiefs including John Brennan (CIA), James Clapper and Mark Giuliano (FBI) and their families. Guilty plea to eight s1 and two s3 offences. Sentenced to two years in youth detention. Order for seizure of his computers. [MTCE]	Cause, Entertainment, Ego The sentencing judge stated that: 'This was an extremely nasty campaign of politically motivated cyberterrorism'. His boasting of his exploits on social media show that he was also motivated by a desire to prove himself, as well as the fact he enjoyed the activity. Tweets used #freepalestine.	Outsider	18	Male	Group (member of CWA)	Autistic

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Michelle Denne	https://www.bbc.co.uk/news/uk-england-stoke-staffordshire-43665907	No	April 2018	Unskilled (unauthorised use of authorised access)	PC Denne, 44, accessed Staffordshire Police computer systems to obtain information on her partner's ex-wife and children, and her neighbours. Guilty plea to six CMA counts. Sentenced to a six month community service order, ten days of community rehabilitation work. Ordered to pay £185 court costs and £85 victim surcharge. [MTCE]	Curiosity Accessed systems in order to find out information relating to her personal relationships.	Insider	44	Female	Lone operator	No
Andrew Howe	https://www.chroniclelive.co.uk/news/north-east-news/police-howe-criminal-computer-hero-14497318	No	April 2018	Unskilled (unauthorised use of authorised access)	PC Howe accessed Northumbria Police computer systems to obtain information to pass on to a female publican with who he was having an "inappropriate relationship". Guilty pleas. Sentenced to four months prison suspended for 12 months and ordered to pay £1,460 costs. [MTCE]	Personal relationship Obtained information in order to satisfy individual with whom he was in a relationship.	Insider	50	Male	Group	None
Adam Mudd	https://www.bbc.co.uk/news/uk-england-beds-bucks-herts-43541534 https://www.bbc.co.uk/news/uk-england-beds-bucks-herts-39705068 https://www.cybersecurity-insiders.com/teenage-hacker-makes-400000-by-hacking-1-7-million-xbox-live-and-minecraft-accounts/ https://krebsonsecurity.com/2017/04/uk-man-gets-two-years-in-jail-for-running-titanium-stresser-attack-for-hire-service/ [2017] EWCA Crim 1395	Yes	March 2018	High skill (developed own DDOS software, Titanium Stresser, and sold to others)	Teenager Mudd wrote Titanium Stresser DDoS malware and used it for 595 DDoS attacks against 181 IP addresses. Also received Rental Income of some £386,000 from 112,000 registered users. Guilty plea. Sentenced to two years in a young offenders institute. Ordered (27 March 2018) to pay back £70k within three months or face further two years detention. [MTCE]	Money; Ego; Status; Entrance to Community Received significant sums for renting out Titanium Stresser. However, a pre-sentence report stated that: 'While a large amount of money had flowed into his PayPal account, the appellant's motivation was more to do with a perception he gained about himself as a clever person, rather than the failure he had lived with as he was growing up.' A further report stated his offending "had a function of meeting his emotional and social needs rather than being for financial gain".	Outsider	20	Male	Tasked by third parties	Aspergers
Craig Steinberg	https://www.sunderlandecho.com/news/trusted-sunderland-bar-boss-made-money-hacking-womens-private-pictures-and-posting-them-porn-sites-334144 https://www.chroniclelive.co.uk/news/north-east-news/apple-icloud-hacker-craig-steinberg-14371722	Yes	March 2018	Low skill (used software of others to commit criminality)	31 year-old Bar manager hacked into 272 Apple iCloud accounts to grab private, sexual photographs that he posted on his websites and charged members to access. Steinberg used software and guesswork to gain access to photographs of Apple iCloud customers' most intimate moments. Guilty plea. Jailed for 34 months. [MTCE]	Money; Sexual Stole images for his own sexual gratification and also set up a website where he charged others to view them.	Outsider	31	Male	Lone operator	None identified

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Gavin Paul Prince	https://www.dailypost.co.uk/business/business-news/jailed-cyber-crook-threatened-future-14377752 https://www.dailypost.co.uk/news/north-wales-news/sacked-expert-who-launched-revenge-14349923	Yes	February 2018	Low skill (deleted items and locked accounts)	37 year-old IT expert launched revenge cyber attack on previous employer company LetsXL of Colwyn Bay in April 2017. Over a four day period he changed the passwords and accessed mailboxes of five company employees. Guilty plea to five CMA offences. Sentenced to 10 months in prison. [MTCE]	Revenge Carried out attack after relationship with victim company soured.	Insider	37	Male	Lone operator	None identified
Goncalo Esteves	https://www.infosecurity-magazine.com/news/av-evasion-website-mastermind-gets/ https://www.theregister.co.uk/2018/02/15/refud_cryptex_kingpin_goncalo_esteves_jailed/	Yes	February 2018	Semi-skilled (ran counter anti-virus service and sold RATs)	Esteves (aka KillaMuvz) ran the reFUD.me website which charged hackers for testing whether their malware would evade Anti Virus and Malware scanners from 2011 to 2015. Sentenced to two years in jail. [MTCE]	Money Made an estimated £500,000 through his activities running the CAV site.	Outsider	24	Male	Tasked by third parties	None identified
Alex Bessell	https://www.bbc.co.uk/news/uk-england-42733638 https://www.cybersecurity-insiders.com/man-uses-9k-zombie-computers-to-cyber-attack-skype-google-and-pokemon/ https://www.spamfighter.com/News-21354-Alex-Bessell-The-Hacker-is-put-Behind-Bars-for-the-Offense-of-Cyber-Crime.htm	Yes	January 2018	High skill (wrote own software and Crypter services)	Bessell, 21, created malware sold on the dark web that allowed others to conduct Distributed Denial of Service (DDoS) attacks. Had remote control of over 9,083 bots. Guilty plea. Sentenced to two years imprisonment and given a Serious Crime Prevention Order. [MTCE]	Money Carried out attacks for clients in exchange for payment.	Outsider	21	Male	Tasked by third parties	None identified
Abiola Ajibade	https://www.theregister.co.uk/2018/01/17/santander_manager_guilty_computer_misuse/ https://www.itwiser.co.uk/news/former-bank-manager-pleads-guilty-to-computer-misuse	No	January 2018	Unskilled (unauthorised use of authorised access)	Ex Santander branch manager gave boyfriend customer information used for fraudulent transactions worth £15k. Guilty plea. Sentence not known. [MTCE]	Money Obtained information to enable fraudulent transactions.	Insider	24	Male	Group	

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Jack Chappell	https://www.theregister.co.uk/2017/12/20/stockport_ddoser_given_suspended_sentence/ https://www.bbc.co.uk/news/uk-england-manchester-40484890 https://krebsonsecurity.com/2017/12/u-k-man-avoids-jail-time-in-vdos-case/	Yes	December 2017	Semi-skilled (helped to run attack for hire service vDOS over a significant period of time and helped to launder money for vDOS)	Chappell, 19, launched 2,000 Distributed Denial of Service (DDoS) attacks including on Amazon, NatWest and Netflix. Guilty plea. Sentenced to 16 months in youth custody, suspended for two years, and ordered to undertake 20 days rehabilitation. [MTCE]	Money Rented out his services for money, running a commercial enterprise.	Outsider	19	Male	Tasked by third parties	Autistic
Karen Enabafio	https://www.dailymail.co.uk/news/article-5131937/Office-worker-hacked-computer-colleagues-salaries.html	No	November 2017	Unskilled (unauthorised use of authorised access)	43 year-old Private Hospital financial administrator accessed colleagues' payroll data to find out their salaries. Guilty plea. Sentenced to twelve weeks imprisonment suspended for one year and ordered to complete ten days of rehabilitation. [MTCE]	Curiosity Finding out about colleagues' salaries.	Insider	43	Female	Lone operator	
Nigel Mungur	https://www.bbc.co.uk/news/uk-england-merseyside-41531324	No	October 2017	Unskilled (unauthorised use of authorised access)	Police Constable accessed Lancashire Constabulary systems 21,802 times over 7 years to obtain personal details of car crash victims to sell on to ambulance chasing claims firms. Proceeds totalled £363,000. Guilty plea. Sentenced to five years in prison. [MTCE]	Money Sold information to ambulance chasing legal firms.	Insider	40	Male	Group	
Pardeep Parmar	https://www.theregister.co.uk/2017/08/30/ex_harrods_man_pardeep_parmar_computer_misuse_plea/	No	October 2017	Unskilled (conducted no activity himself)	Ex-Harrods IT worker asked computer repair shop to help him retrieve personal files (including his National Insurance number) on his company-issued laptop. Guilty plea to CMA s1 charge. Fined £135 for the CMA s1 offence, ordered to pay £85 costs and £30 victim surcharge. [MTCE]	Retrieval of own data Attempting to obtain personal information from devices that he no longer had access to .	Insider	30	Male	Lone operator	
Grant McCabe	https://www.liverpoolecho.co.uk/news/liverpool-news/disgraced-cop-used-police-intelligence-13682666	No	September 2017	Unskilled (unauthorised use of authorised access)	Merseyside PC accessed police intelligence systems to snoop on two girlfriends and their previous partners. Guilty plea. Sentenced to nine months in jail suspended for two years, 200 hours of unpaid work, six month curfew 7pm and 7am (monitored by a tag) and 20 rehabilitation activity days. [MTCE]	Curiosity To find information on personal realationships.	Insider	43	Male	Lone operator	
Alexander Akinyele	https://www.nwemail.co.uk/news/barrow/16436195.barrow-fraudster-who-threw-bogus-credit-cards-out-of-the-window-is-jailed/	Yes	September 2017	Unskilled (purchased stolen details in order to commit fraud)	ID Theft. 37 year-old found in possession of 500 BT and 500 Sky usernames and passwords. NCA investigation. Guilty plea. Sentenced to two years 4 months in prison. [MTCE]	Money Criminality aimed at obtaining personal details in order to commit credit card fraud.	Outsider	37	Male	Lone operator	None identified

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Jason Polyik	https://www.nottinghampost.com/news/local-news/hacker-cost-sports-direct-50000-3431164 https://www.theregister.co.uk/2017/02/13/sports_direct_arrest/	Yes	August 2017	Semi-skilled (hacked into Sports Direct via unpatched vulnerabilities in DNN platform)	Hacker accessed two websites including Sports Direct and shut it down for half an hour. Sentenced to 10 months in prison suspended for a year. [MTCE]	Other (personal gain) Criminality was committed in an attempt at finding a job.	Outsider	27	Male	Lone operator	Autistic
Sean Caffrey	https://www.bbc.co.uk/news/uk-england-birmingham-40292156 https://www.itv.com/news/central/2017-09-14/birmingham-hacker-spared-a-prison-sentence-us-department-of-defence-sean-caffrey/ https://www.theregister.co.uk/2017/06/16/us_mil_sat_hack_plea/	Yes	June 2017	Semi-skilled (obtained access to US military systems through unknown vector)	25 year-old accessed a US military satellite communications system in June 2014 and stole 800 users' usernames, ranks and email addresses and details of about 30,000 satellite phones. US Department of Defense (DoD) estimated cost to fix the damage at about $628,000 (c. £450,000). Guilty plea. Sentenced to 18 months in prison, suspended for 18 months. [MTCE]	Ego; Status Summing up, the judge stated: 'this was a serious crime but your motives were not seriously criminal. You did what you did just to show that you could"	Outsider	25	Male	Lone operator	Severe Asperger's Syndrome
Daniel Devereux	https://www.bbc.co.uk/news/uk-england-norfolk-40307003 https://www.edp24.co.uk/news/crime/hacker-known-as-his-royal-gingerness-admits-cyber-attacks-on-norwich-airport-and-norfolk-and-norwich-university-hospital-1-5035255 https://www.anomali.com/blog/anomali-weekly-threat-intelligence-briefing-june-20-2017	Yes	June 2017	Semi-skilled (used SQL injection attacks against hospital and airport websites)	Devereux aka "His Royal Gingerness" hacked into the websites of Norwich airport and the Norfolk and Norwich hospital in 2015. The airport's website was down for three days and said the breach cost £40,000 to fix. Guilty plea. Sentenced to 32 weeks in prison, issued with a Criminal behaviour Order (CBO) preventing him from owning an internet enabled device unless he follows a set of strict rules for five years and ordered to pay £150 as a victim surcharge. [MTCE]	Ego; Status Devereux called BBC Radio Norfolk and was interviewed about the attacks anonymously, boasting of how quickly he carried them out.	Outsider	30	Male	Lone operator	None identified

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Christopher Hutcheson	https://www.theguardian.com/uk-news/2017/jun/07/gordon-ramsay-father-in-law-chris-hutcheson-jailed https://www.dailymail.co.uk/news/article-4579794/Gordon-Ramsay-s-laws-sentenced-hacking.html	Yes	June 2017	Low skill (used key logger software to obtain passwords)	Restaurateur Gordon Ramsay family feud. After a series of toxic civil disputes, father-in-law Christopher Hutcheson (Snr) and his two sons used key logger to capture passwords and hacked into Gordon Ramsay Holdings Ltd systems to access email accounts of employees, financial data and details of intellectual property (IP) rights. Guilty pleas. Hutcheson (Snr) sentenced to six months imprisonment. [MTCE]	Revenge Criminality conducted following family dispute.	Outsider (known to victim)	69	Male	Group (Hutcheson family group)	None identified
Chris Hutcheson	https://www.theguardian.com/uk-news/2017/jun/07/gordon-ramsay-father-in-law-chris-hutcheson-jailed https://www.dailymail.co.uk/news/article-4579794/Gordon-Ramsay-s-laws-sentenced-hacking.html	Yes	June 2017	Low skill (used key logger software to obtain passwords)	Restaurateur Gordon Ramsay family feud. After a series of toxic civil disputes, father-in-law Christopher Hutcheson (Snr) and his two sons used key logger to capture passwords and hacked into Gordon Ramsay Holdings Ltd systems to access email accounts of employees, financial data and details of intellectual property (IP) rights. Guilty pleas. Chris Hutcheson (Jnr) given four-month prison sentence, suspended for two years. [MTCE]	Revenge Criminality conducted following family dispute.	Outsider (known to victim)	37	Male	Group (Hutcheson family group)	None identified
Adam Hutcheson	https://www.theguardian.com/uk-news/2017/jun/07/gordon-ramsay-father-in-law-chris-hutcheson-jailed https://www.dailymail.co.uk/news/article-4579794/Gordon-Ramsay-s-laws-sentenced-hacking.html	Yes	June 2017	Low skill (used key logger software to obtain passwords)	Restaurateur Gordon Ramsay family feud. After a series of toxic civil disputes, father-in-law Christopher Hutcheson (Snr) and his two sons used key logger to capture passwords and hacked into Gordon Ramsay Holdings Ltd systems to access email accounts of employees, financial data and details of intellectual property (IP) rights. Guilty pleas. Adam Hutcheson given four-month prison sentence, suspended for two years. [MTCE]	Revenge Criminality conducted following family dispute.	Outsider (known to victim)	47	Male	Group (Hutcheson family group)	None identified
Paul Dixon	https://www.bbc.co.uk/news/uk-england-tyne-39482304 https://www.thenorthernecho.co.uk/news/15444123.seaham-computer-geek-bragged-hacking-durham-police-british-airways-costing-airline-100-000/	Yes	April 2017	Low skill (used botnet to DDOS a number of websites)	South Shields man mounted DoS attacks against CeX, Durham Constabulary, Police Scotland and British Airways websites in October 2014. British Airways site down for an hour at an estimated cost of £100,000. Guilty plea. Sentence not known. [MTCE]	Ego; Status; Entrance to Community Bragged about exploits on Twitter; prosecution stated: "He could not resist boasting about his activities online on his Twitter account. Indeed, this appears to be the sole motivation behind his actions." Also requested others recommend targets for him;	Outsider	22	Male	Lone operator	None identified

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Thomas Fendall	https://www.bbc.co.uk/news/uk-england-manchester-39306738	No	March 2017	Unskilled (unauthorised use of authorised access)	PCSO with a personal grievance accessed restricted material on the GMP police intelligence computer system to try to frame an innocent man for attempted murder. Guilty plea. Sentenced to nineteen months imprisonment. [MTCE]	Personal dispute Accessed information to enable further criminality	Insider	26	Male	Group	
Shaun Turner	https://www.cambridge-news.co.uk/news/cyber-pervert-watched-women-via-12528678 https://www.itv.com/news/anglia/2017-01-31/man-who-spied-on-victims-through-their-webcams-jailed-for-three-years/	Yes	January 2017	Low skill (used RAT malware to access his victim's computers)	29-year-old man spied on female victims using their personal webcams and used RAT malware to download intimate and personal files held on their computers. Refused to provide key to two encrypted hard drives. Guilty plea. Sentenced to three years imprisonment (including 10 months consecutive for Failure to comply with RIPA section 49 notice to provide encryption key). [MTCE]	Sexual Criminal activity aimed at obtaining sexual images for personal gratification.	Outsider	29	Male	Lone operator	None identified
Paul Andre	https://www.chroniclelive.co.uk/news/north-east-news/northumbria-police-worker-faces-sack-12496521	No	January 2017	Unskilled (unauthorised use of authorised access)	43 year old Crime prevention officer at Northumbria Police used force IT system to find out about an incident involving tenants at his flat without authorisation. Guilty plea. 12-month conditional discharge, ordered to pay £85 costs and a £30 victim surcharge. [MTCE]	Personal dispute Accessed information relevant to a personal dispute.	Insider	43	Male	lone operatorT	
Christopher Topliss	https://www.newsandstar.co.uk/news/16755816.carlisle-online-predator-jailed-after-being-caught-by-national-crime-agency/ [2017] EWCA Crim 1747	Yes	December 2016	Low skill (downloaded and operated malicious software to abuse his victims)	Topliss used open source software to access victims mobile handsets, as well as conducted an online relationship with a minor.	Sexual Criminality conducted in order to develop inappropriate relationships with minors.	Outsider	29	Male	Lone operator	None identified

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Daniel Kelley	https://www.bbc.co.uk/news/technology-38300106 https://www.bbc.co.uk/news/uk-wales-48120428; https://www.telegraph.co.uk/news/2019/06/10/talktalk-hacker-blackmailed-executives-77million-cyber-attack/ https://www.birminghammail.co.uk/news/midlands-news/cruel-calculating-talktalk-hacker-daniel-16409800	Yes	December 2016	Semi-skilled (concerted hacking against major targets, but no indication of own tool development)	19 year old man involved in 2015 attack on ISP TalkTalk when more than 150,00 customers' data was stolen and demanded a payment of 465 bitcoins. DDoS attack on Coleg Sir Gar website where he was a student. Guilty pleas to 11 charges. Sentenced to four years' detention in a young offenders institution. [MTCE]	Revenge; Money Demanded payment following Talktalk hack. Initially hacked college out of spite.	Outsider	19	Male	Group (others participated in hacking activity)	Aspergers
Paul Whitehead	https://www.thecomet.net/news/bedfordshire-police-officer-jailed-after-defrauding-cleaner-out-of-more-than-30-000-1-4739531	No	October 2016	Unskilled (unauthorised use of authorised access)	Police officer misused Bedfordshire Police systems to locate his victim (a cleaner at Luton Police Station) and defraud him out of his inheritance. Guilty plea. Sentenced to five years, seven months imprisonment. [MTCE]	Money Information used to enable fraud.	Insider	32	Male	lone operator	
Paul Streeter	https://www.oxfordmail.co.uk/news/14776162.cynical-hackers-laddish-firm-sentenced-spying-rival/	Yes	September 2016	Unskilled (used known credentials to commit hack)	"The Quadsys Five" hacked into a business rival IT security reseller's computer system to access customer and pricing data. Guilty pleas. Directors Barnard, Cox and Streeter sentenced to 10 months imprisonment, suspended for two years, three month curfew, 150 hours of unpaid work and victim surcharge of £100. [MTCE]	Money Criminality was conducted with purpose of obtaining business advantage over their rivals.	Insider (via co-conspirator Davies)	40	Male	Group (Quadsys Five)	None identified
Paul John Cox	https://www.oxfordmail.co.uk/news/14776162.cynical-hackers-laddish-firm-sentenced-spying-rival/	Yes	September 2016	Unskilled (used known credentials to commit hack)	"The Quadsys Five" hacked into a business rival IT security reseller's computer system to access customer and pricing data. Guilty pleas. Directors Barnard, Cox and Streeter sentenced to 10 months imprisonment, suspended for two years, three month curfew, 150 hours of unpaid work and victim surcharge of £100. [MTCE]	Money Criminality was conducted with purpose of obtaining business advantage over their rivals.	Insider (via co-conspirator Davies)	40	Male	Group (Quadsys Five)	None identified
Alistair Barnard	https://www.oxfordmail.co.uk/news/14776162.cynical-hackers-laddish-firm-sentenced-spying-rival/ https://www.theregister.co.uk/2016/09/30/quadsys_five_sentencing/	Yes	September 2016	Unskilled (used known credentials to commit hack)	"The Quadsys Five" hacked into a business rival IT security reseller's computer system to access customer and pricing data. Guilty pleas. Directors Barnard, Cox and Streeter sentenced to 10 months imprisonment, suspended for two years, three month curfew, 150 hours of unpaid work and victim surcharge of £100. [MTCE]	Money Criminality was conducted with purpose of obtaining business advantage over their rivals.	Insider (via co-conspirator Davies)	38	Male	Group (Quadsys Five)	None identified

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Steve Davies	https://www.oxfordmail.co.uk/news/14776162.cynical-hackers-laddish-firm-sentenced-spying-rival/ https://www.channelpro.co.uk/news/10146/sophos-cuts-ties-with-quadsys-after-reseller-hit-by-guilty-verdicts	Yes	September 2016	Unskilled (used known credentials to commit hack)	"The Quadsys Five" hacked into a business rival IT security reseller's computer system to access customer and pricing data. Guilty Plea. Manager Steve Davies sentenced to nine months imprisonment, suspended for two years, 150 hours of unpaid work, and victim surcharge of £100. [MTCE]	Money Criminality was conducted with purpose of obtaining business advantage over their rivals.	Insider	34	Male	Group (Quadsys Five)	None identified
Jon Townsend	https://www.oxfordmail.co.uk/news/14776162.cynical-hackers-laddish-firm-sentenced-spying-rival/	Yes	September 2016	Unskilled (used known credentials to commit hack)	"The Quadsys Five" hacked into a business rival IT security reseller's computer system to access customer and pricing data. Guilty plea. IT Security Consultant Jon Townsend a 12-month community order, 275 hours of unpaid work, three month curfew and victim surcharge of £60. [MTCE]	Money Criminality was conducted with purpose of obtaining business advantage over their rivals.	Insider (via co-conspirator Davies)	36	Male	Group (Quadsys Five)	None identified
Nazariy Markuta	https://www.theregister.co.uk/2016/09/23/yahoo_hacker_gets_11_years/ https://www.wired-gov.net/wg/news.nsf/articles/Key+member+of+international+cyber+crime+collective+jailed+for+2+years+23092016151500?open	Yes	September 2016	Semi-skilled (concerted hacking over a significant period to obtain data for sale)	Founder member of international cyber crime network D33Ds used SQL injection attacks to obtain 300k usernames and passwords from Yahoo and offered them for sale. Also attacked a website selling computer game codes that were obtained for resale. Investigation by the National Crime Agency. Jailed for two years after guilty pleas to three offences under CMA 1990 s3 and fraud. [MTCE]	Money Obtained data in order to sell it for profit.	Outsider	23	Male	Group (member of D33Ds)	None identified
Adam Penny	https://www.standard.co.uk/news/london/canary-wharf-computer-hacker-jailed-for-stealing-thousands-of-pounds-in-gold-a3343241.html https://www.theregister.co.uk/2016/09/15/hacker_jailed_over_gold_bar_theft_scam/	Yes	September 2016	Low skill (hacked gold bullion company-criticised for poor security by police- for information around deliveries)	Unemployed hacker accessed a gold bullion firm website to obtain names, addresses and tracking numbers of customers to enable associates to intercept the gold deliveries. Pleaded guilty to conspiracy to steal, unauthorised access to a computer and blackmail and sentenced to five years and four months in jail. [MTCE]	Money Criminality was conducted with the sole purpose of facilitating further criminality, the aim of which was to steal gold.	Outsider	25	Male	Group (part of OCG)	None identified
Neil Hempsell	https://www.thenorthernecho.co.uk/news/14724412.former-policeman-sentenced-using-force-computer-help-contact-sex-workers/	no	September 2016	Unskilled (unauthorised use of authorised access)	Police officer trawled police computers to contact sex workers, track down a former lover and make 195 checks on a Gateshead gangster who he had fallen out with following a Christmas day brawl. Sentenced to 255 hours unpaid work and ordered to pay costs. [MTCE]	Sexual Accessing information related to sex workers and previous lover in order to enable further contact	Insider	48	Male	Lone operator	

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
David Buchanan	https://www.bbc.co.uk/news/uk-england-surrey-36954673 https://www.itpro.co.uk/security/26598/surrey-teenager-charged-over-misogynist-mumsnet-hack https://www.scmagazine.com/home/security-news/surrey-teenager-charged-under-computer-misuse-act-over-mumsnet-hack/ https://www.dailymail.co.uk/news/article-3720350/Bored-schoolboy-hacked-popular-social-networking-site-parents-led-vicious-hoax-bomb-threats-fabricated-claims-kidnappings-avoided-jail.html	Yes	August 2016	Semi-skilled (developed own scripts to disrupt Mumsnet; also DDOS on site)	Bored 17 year-old developed scripts to help harvest Mumsnet usernames and passwords and hacked into his school intranet. Sentenced to a 12-month community order and 200 hours of unpaid community work. [MTCE]	Entertainment Buchanan claimed to have committed the attacks in order to alleviate boredom. His choice of	Outsider (known to victim)	18	Male	Group (others took advantage of his scripts)	Aspergers
Kyoji Mochizuki	https://www.eastbourneherald.co.uk/news/crime/county-news-man-sentenced-cyber-attacks-police-contact-centre-869728	Yes	August 2016	Low skill (DDOS attacks on police and insurer systems)	Man aka Tariq Elmughrabi bombarded Sussex Police's contact centre with 3,000 emails in six hours. Pleaded guilty and sentenced to ten months jail, suspended for 18 months. [MTCE]	Revenge Criminality committed as revenge for Sussex police force seizing his electronic property in connection with another case.	Outsider (known to victim)	28	Male	Lone operator	None identified
16-year-old from Plymouth	https://www.bbc.co.uk/news/uk-england-devon-36844957 https://www.theregister.co.uk/2016/06/29/seaworld_plymouth_teen_hacker_pleads_guilty_denies_airline_bomb_hoax_tweets/	Yes	July 2016	Low skill (DDOS attacks, traced via Twitter account linked to home address)	14-year old Plymouth boy launched DDoS attacks against animal rights target websites and Devon and Cornwall Police and tweeted bomb hoaxes to American Airlines and Delta Air Lines. Three offences under Computer Misuse Act Section 3 (the DDoS attacks) admitted. Convicted of two offences under Section 51 of the Criminal Law Act (the bomb hoaxes). District Judge Diana Baker had considered 12 month jail but sentenced him to a two year Youth Rehabilitation Order and ordered his laptop to be destroyed. [MTCE]	Cause; Entertainment; Ego Teenager told the court that a number of his targets were chosen as he was 'fighting for animal rights.' The sentencing judge stated "I think you got carried away, you thought you were cool and clever"	Outsider	16	Male	Lone operator	None identified
Matthew Oaten	https://www.bbc.co.uk/news/uk-england-oxfordshire-36478513	No	June 2016	Unskilled (unauthorised use of authorised access)	Thames Valley police officer accessed information on police computer system without authorisation. Sentenced to 150 hours community service and £1,000 costs. [MTCE]	Unable to identify motive. Sentencing judge: "There was no gain to himself by doing so. The defendant accepts he must have sent the offending emails but he cannot say why he did so. His father has no memories of receiving or opening them. He had no ulterior motive or gain."	Insider	30	Male	Group	

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Helen Logins	https://www.bbc.co.uk/news/uk-england-nottinghamshire-36174542	No	April 2016	Unskilled (unauthorised use of authorised access)	Nottingham City Council manager used council computer systems to search confidential records and case files. Sentenced to twelve months in prison, suspended for 18 months and 250 hours community service. [MTCE]	Personal use Searching in relation to specific case against her husband.	Insider	52	Female	Group	
John Sabatina	https://www.liverpoolecho.co.uk/news/liverpool-news/snooping-merseyside-police-sergeant-face-11018436	No	March 2016	Unskilled (unauthorised use of authorised access)	Merseyside police officer accessed information on police computer system over eight years without authorisation. Sentenced to two months in prison, suspended for 12 months. [MTCE]	Curiosity Prolonged misuse of systems to obtain a large amount of information on non-specific issues.	Insider	49	Male	Lone operator	
Matt Swash	https://www.bbc.co.uk/news/uk-england-cambridgeshire-35597834	No	February 2016	Unskilled (unauthorised use of authorised access)	Cambridgeshire police officer accessed information on a police computer system without authorisation. Sentenced to two months in prison, suspended for 12 months. [MTCE]	Curiosity Accessed information about a colleague.	Insider	41	Male	Lone operator	
Ian Sullivan	https://www.dailymail.co.uk/news/article-3316347/Hacker-attacked-300-websites-month-long-revenge-spree-children-care-jailed.html https://www.theregister.co.uk/2015/11/13/brit_gets_eight_months_for_ddos_spree/	Yes	November 2015	Low skill (DDOS vs 300 sites using RageBooter, identified via Twitter account)	51-year old father of six launched DDoS attacks against over 300 websites after his five children were taken into social care. Guilty plea to 21 offences. Sentenced to eight and a half months in prison. [MTCE]	Revenge; Cause Sullivan was connected with Anonymous, but the sites he chose were linked to institutions and services that he had perceived had done him wrong in taking his children into social care.	Outsider	51	Male	Group (linked to Anonymous)	Diagnosed with a variety of mental health disorders
Sundar Banerjee	https://www.windsorobserver.co.uk/news/13953731.former-met-police-detective-from-old-windsor-jailed-for-trawling-polices-criminal-database/	No	October 2015	Unskilled (unauthorised use of authorised access)	Former Met Police detective used MPS computer systems for 230 searches between 2009 and 2013 for private use. Sentenced to nine months in prison. [MTCE]	Curiosity/Private use Searches across a wide variety of information, including his own car.	Insider	33	Male	Lone operator	

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Charlton Floate	https://nakedsecurity.sophos.com/2015/08/24/teen-nabbed-after-attacks-on-uk-government-and-fbi-sites/ https://www.bbc.co.uk/news/uk-england-birmingham-34555291 https://www.dailymail.co.uk/news/article-3203894/British-teenager-team-hackers-caused-government-websites-UK-USA-crash.html	Yes	October 2015	Semi-skilled (created botnet in order to conduct DDOS; concerted activity; gained access to devices of individuals webcams etc)	Teenager launched global distributed denial-of-service (DDoS) attacks against UK Home Office and FBI websites. Guilty plea to the DDoS attacks and two counts of possessing 111 prohibited images. Eight month sentence suspended for 18 months, an order restricting his access to the internet and computer activity and an order to complete 250 hours unpaid of work. [MTCE]	Status; Ego; Entrance into community Floate bragged about the attacks on an internet forum frequently used by hackers and also on Twitter.	Outsider	19	Male	Group (worked alongside others)	None identified
Stefan Rigo	https://www.actionfraud.police.uk/news/cybercriminal-hacked-victims-webcams-and-spied-on-them-having-sex https://nakedsecurity.sophos.com/2015/10/09/blackshades-webcam-voyeur-spared-jail-over-stolen-webcam-images/	Yes	October 2015	Low skill (used Blackshades RAT - purchased using ex-girlfriend's details- to gain control of individual devices)	Webcam voyeur used Blackshades Remote Access Trojan (RAT) malware to spy on people through their webcams. Sentenced to a 40 week suspended sentence, seven years on the sex offenders register, 200 hours of unpaid work and the forfeiture of all his computer equipment. [MTCE]	Sexual Criminality intended to obtain sexual images and content for personal use.	Outsider	33	Male	Lone operator	None identified
Richard Neale	https://www.bbc.co.uk/news/technology-34052408 https://www.dailymail.co.uk/news/article-3209256/Computer-firm-boss-hacked-900-mobile-phones-belonging-Aviva-insurance-employees-act-revenge-leaving-job-bad-terms-jailed-18-months.html https://www.theregister.co.uk/2015/08/26/aviva_phone_hacker_jailed/	Yes	August 2015	Low skill (stolen, as well as legitimate but mistakenly unrevoked, credentials were the main agents in the attack)	Revenge attacks by ex-Director on former network security company Esselar and its client Aviva over five months. 900 Aviva employees' phones hacked; Expenses claims rejected. Esselar Twitter account defaced. Esselar lost Aviva contract. Aviva recovered from attack within 24 hours. Pleaded guilty to four counts of unauthorised or reckless acts with intent to impair computer operation. Actions had "damaged confidence and reputations in a way that can be far-reaching and serious". Sentenced to 18 months. [MTCE]	Revenge Prosecuting judge stated: "The prosecution describe these offences as revenge; you use the expression causing mischief. What form of words you use is beside the point: it was plainly borne of your resentment.	Insider	40	Male	Lone operator	None identified

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Andrew Skelton	https://www.bbc.co.uk/news/uk-england-leeds-33566633	No	July 2015	Unskilled (unauthorised use of authorised access)	Senior Internal Auditor at Morrisons supermarket accessed and uploaded confidential personal data (including employees' names, addresses, NI and bank details) of nearly 100,000 employees to newspaper and data sharing websites. Found guilty of fraud by abuse of position of trust, securing unauthorised access to computer material and disclosing personal data. Data breach cost the company more than £2m to rectify. Sentenced to eight years. [MTCE]	Revenge Activity carried out due to disillusionment with employer.	Insider	43	Male	Lone operator	
Seth Nolan-McDonagh -	https://www.bbc.co.uk/news/technology-33480257 https://www.theregister.co.uk/2015/07/10/spamhaus_ddos_teen_sentenced/ https://krebsonsecurity.com/2014/12/spamhaus-cloudflare-attacker-pleads-guilty-to-computer-abuse-child-porn-charges/	Yes	July 2015	Semi-skilled (while he launched DDOS attacks, at the time this was the world's largest ever and, said the Judge, 'was so sophisticated and unprecedented in scope they had a worldwide effect')	Teenager using the nickname Narko launched a series of crippling global distributed denial-of-service (DDoS) attacks against internet exchanges and services including Spamhaus. Guilty plea to two counts of an unauthorised act with intent to impair computer operation. Sentenced to 240 hours of community service. [MTCE]	Money Conducted attacks in exchange for payment from third parties.	Outsider	18	Male	Tasked by third parties	Suffered from a severe mental illness at the time of the attack
Lee Rees	https://www.itv.com/news/wales/2015-12-07/lee-phillip-rees-pretended-to-be-a-13-year-old-girl-in-online-chatrooms-so-he-could-blackmail-the-men-who-contacted-him/ https://www.theregister.co.uk/2015/12/08/blackmail_paedo_hunter_jailed/	Yes	June 2015	Low skill (posed as an underage girl in order to get paedophiles to download malware alongside indecent images)	Self-styled paedophile hunter posed as underage girls in chatrooms to entice men to send indecent images of themselves that he exchanged for other indecent images that concealed malware to obtain their personal details for blackmail. £40,000 proceeds. Guilty pleas. Sentenced to nine years in prison. [MTCE]	Money; Entertainment The sentencing judge said: "Having read all of the evidence and, in particular, the chat logs, I have reached the conclusion that you derived much enjoyment and satisfaction in controlling and manipulating these individuals, preying on their fears and extracting for yourself significant financial gain.	Outsider	48	Male	Lone operator	None identified
Zoe Gregory	https://www.bbc.co.uk/news/uk-england-norfolk-33013773	Yes	June 2015	Unskilled (no evidence as to how obtained access to student's email account)	Teaching Assistant hacked into the school email system at Ormiston Victory Academy and used pupil's account to send email "There will be a bomb in school Monday". Guilty plea to one count of communicating false information and one count of unauthorised computer access. Sentenced to 15 months imprisonment for both offences. [MTCE]	Revenge Crime seemingly carried out in order to cause distress to victims	Insider	26	Female	Lone operator	None identified
Imran Uddin	https://www.dailymail.co.uk/news/article-3053639/Cheating-student-hacked-university-computer-better-degree-jailed.html	Yes	April 2015	Low skill (bought keyboard spying equipment on the internet which he then connected to a number of university computers in order to find out staff credentials)	Adult student at University of Birmingham installed four keyboard spying devices to steal staff passwords used to obtain access to his examination results and improve grades. Guilty plea to six CMA charges - unauthorised access to computer material, intent to commit further offences and impairing the operation of a computer. Four-month prison sentence. [MTCE]	Other (unable to identify motivation) Sentencing Judge Burbridge said: 'For reasons not entirely clear to me, whether it was monetary, or pride, or a desire to outperform others, you decided to cheat and you formed a settled intention to do that. I consider your actions were planned and persistent.'	Outsider (known to victim)	25	Male	Lone operator	None identified

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Mark Johnson	https://www.bbc.co.uk/news/uk-england-stoke-staffordshire-29958425	Yes	November 2014	Unskilled (enabled Anonymous DDOS attacks by posting links on his Twitter account)	44 year old Casino croupier and supporter of Anonymous published DDoS cyber attack links to UK Home Office and Home Secretary Theresa May websites on Twitter. Charged with encouraging or assisting an offence. Found Guilty. [MTCE]	Cause Action was carried out in support of Anonymous activity.	Outsider	44	Male	Group (member of Anonymous)	None identified
Anthony Elliott	https://www.examinerlive.co.uk/news/west-yorkshire-news/disgruntled-ex-employee-anthony-elliott-jailed-7744048	Yes	September 2014	Low skill (knew credentials that facilitated attack, and uploaded script to disrupt cameras)	Disgruntled ex-employee used access credentials to disable 120 of former employer's time-lapse cameras at construction sites around the world. Unauthorised acts with intent to impair operation of a computer. Cost to restore the service, by sending an engineer to each location, was estimated at around £50,000. Jailed for 10 months. [MTCE]	Revenge Ex-employee committed criminality aimed at causing disruption to victim company following dispute.	Insider	33	Male	Lone operator	None identified
Andrew Meldrum	https://www.itv.com/news/update/2014-05-30/man-freed-after-bugging-computers-to-spy-on-women/ https://nakedsecurity.sophos.com/2014/03/05/man-guilty-of-fixing-womens-computers-to-spy-on-them-via-webcam/	Yes	May 2014	Low skill (used physical access to target devices in order to uploaded RAT software)	Cyber-stalking Peeping Tom installed iCamSource software to spy on three young women in their bedrooms. Guilty plea to three counts of unauthorised access to computer material and found guilty of two counts of voyeurism. 12-month suspended sentence. Ordered to forfeit his computer and pay a contribution to prosecution costs of £2,100 plus a £100 victim surcharge. [MTCE]	Sexual Criminality aimed at obtaining images/ videos for sexual gratification.	Outsider	30	Male	Lone operator	None identified
Piotr Smirnow	https://www.theregister.co.uk/2013/12/19/casino_cyber_extortionists_jailed/ https://www.bbc.co.uk/news/uk-england-manchester-25436558	Yes	December 2013	Unskilled (claimed to use services of Ukraine-based hacker to conduct activity)	Blackmailers threatened a £30M online casino with DDoS denial of service attacks. Guilty plea. Sentenced to five years and four months in prison. [MTCE]	Money Criminality was conducted with the sole purpose of making money.	Outsider	31	Male	Group (alongside Surmacki)	None identified
Patrick Surmacki	https://www.theregister.co.uk/2013/12/19/casino_cyber_extortionists_jailed/ https://www.bbc.co.uk/news/uk-england-manchester-25436558	Yes	December 2013	Unskilled (claimed to use services of Ukraine-based hacker to conduct activity)	Blackmailers threatened a £30M online casino with DDoS denial of service attacks. Guilty plea. Sentenced to five years and four months in prison. [MTCE]	Money Criminality was conducted with the sole purpose of making money.	Outsider	35	Male	Group (alongside Smirnow)	None identified
Alan Thorpe	[2013] EWCA Crim 2559	Yes	November 2013	Low skill (Using a password to which he had been privy whilst working for the company, he used instructions to create files for a shut down, edited the internet firewall and made unauthorised searches on computer files)	Thorpe was made redundant in circumstances which gave rise to resentment on his part. Just over 3 months later, he hacked into his ex-company's computer system and disrupted the transferring of data from an old database to a new system. As a result a number of critical servers shut down and there were problems with system failures that delayed completion of the operation. [[2013] EWCA Crim 2559]	Revenge Appeal documents state his actions were malicious and he was motivated by revenge.	Insider	45	Male	Lone operator	None identified

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Stephen Burrell	https://www.dailymail.co.uk/news/article-2519425/Computer-hacker-stole-virtual-property-online-fantasy-gamers-pay-REAL-gambling-debts.html	Yes	November 2013	Low skill (used databases and password cracking software to access other peoples' accounts)	Burrell unlawfully accessed the accounts of 3,872 players of online game Runescape with intent to steal gaming resources and actually modified 105 player accounts	Money; Status 'The prosecution stated that his principal motivation was to gain kudos among people on the internet. Once a player has lost gaming resources, there is no redress.' [Daily Mail]	Outsider	21	Male	Lone operator	None identified
Tyrone Ellis	https://www.bbc.co.uk/news/av/uk-england-london-24950721/online-job-advert-fraudsters-jailed	Yes	November 2013	Low skill (used social engineering to get individuals to download key logging malware)	Fraudsters posted fake job adverts for Harrods on Gumtree. Respondents were sent a link to an online application form that downloaded malware to capture financial and personal data. National Crime Agency (NCA) investigation.	Money Criminality was conducted with the sole purpose of making money.	Outsider	27	Male	Group (part of low level criminal group)	None identified
Lewys Stephen Martin	https://www.bbc.co.uk/news/uk-england-22558151 http://www.bailii.org/ew/cases/EWCA/Crim/2013/1420.html https://www.theregister.co.uk/2012/05/18/call_of_duty_vxer_jailed/ [2013] EWCA Crim 1420	Yes	May 2013	Low skill (used widely available software - Jaindos and Cyberghost - to carry out attacks)	NullCrew hacktivist Lewys Martin aka sl1nk launched Denial of Service (DOS) attacks on the websites of Kent Police (site temporarily unavailable to the public) and universities of Oxford and Cambridge; both universities estimated that around two person weeks were spent dealing with the attacks. Guilty plea to five counts of Unauthorised modification, two counts of Unauthorised access and two counts of Making, supplying or obtaining articles. Sentenced to two years imprisonment. [MTCE]	Ego; Entrance to the community Martin's lawyer, stated on appeal, that his client's motivation was youthful bravado to a like-minded community. Though it is acknowledged that the offences were planned and persistent, they were not financially motivated. This explanation was accepted by the judge.	Outsider	21	Male	Group (member of NullCrew)	None identified

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Ryan Cleary	https://www.independent.co.uk/news/uk/crime/lulzsec-hackers-sentenced-for-sophisticated-global-cyber-attacks-8619462.html https://nakedsecurity.sophos.com/2013/05/16/lulzsec-hackers-wait-sentence/ https://www.theguardian.com/technology/2013/may/16/lulzsec-hacking-fbi-jail https://thehackernews.com/2012/06/lulzsec-hacker-brit-ryan-cleary-charged.html https://web.archive.org/web/20110619214911/http://arstechnica.com/tech-policy/news/2011/06/lulzsec-heres-why-we-hack-you-bitches.ars	Yes	May 2013	Semi-skilled (ran own botnet and his services were used by Lulzsec for a wide variety of activity, although described as a peripheral member of the group)	LulzSec collective hactivists Ryan Ackroyd, Jake Davis, Mustafa Al-Bassam and Ryan Cleary used DDoS attacks to crash websites of major global institutions including USAF, CIA, FBI, SOCA, Sony and Nintendo and stole personal data including passwords and credit card details belonging to millions of people that was posted online en clair. Damages estimated in millions of pounds. Ryan Cleary (aka ViraL), 21, to six charges and was jailed for 32 months. [MTCE]	Cause; Entertainment Lulzsec's main stated motivation was to have fun by causing mayhem; however, their activities and choice of targets show a clear underlying political ideology (e.g. hacking the Westboro Church, targeting CIA/FBI/SOCA with DDOS)	Outsider	21	Male	Group (member of LulzSec)	Aspergers
Jake Davis	https://www.independent.co.uk/news/uk/crime/lulzsec-hackers-sentenced-for-sophisticated-global-cyber-attacks-8619462.html https://nakedsecurity.sophos.com/2013/05/16/lulzsec-hackers-wait-sentence/ https://www.theguardian.com/technology/2013/may/16/lulzsec-hacking-fbi-jail https://www.theguardian.com/technology/2013/sep/09/jake-davis-topiary-lulzsec-answers	Yes	May 2013	Unskilled (has said of himself that he was a spokesperson with no hacking knowledge)	LulzSec collective hactivists Ryan Ackroyd, Jake Davis, Mustafa Al-Bassam and Ryan Cleary used DDoS attacks to crash websites of major global institutions including USAF, CIA, FBI, SOCA, Sony and Nintendo and stole personal data including passwords and credit card details belonging to millions of people that was posted online en clair. Damages estimated in millions of pounds. Jake Davis (aka Topiary), 20, was jailed for 24 months. [MTCE]	Cause; Entertainment Lulzsec's main stated motivation was to have fun by causing mayhem; however, their activities and choice of targets show a clear underlying political ideology (e.g. hacking the Westboro Church, targeting CIA/FBI/SOCA with DDOS)	Outsider	20	Male	Group (member of LulzSec)	None identified

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Ryan Ackroyd	https://www.independent.co.uk/news/uk/crime/lulzsec-hackers-sentenced-for-sophisticated-global-cyber-attacks-8619462.html https://nakedsecurity.sophos.com/2013/05/16/lulzsec-hackers-wait-sentence/ https://www.theguardian.com/technology/2013/may/16/lulzsec-hacking-fbi-jail https://web.archive.org/web/20110619214911/http://arstechnica.com/tech-policy/news/2011/06/lulzsec-heres-why-we-hack-you-bitches.ars	Yes	May 2013	High skill (widely seen as one of the most skilled members of Lulzsec)	LulzSec collective hactivists Ryan Ackroyd, Jake Davis, Mustafa Al-Bassam and Ryan Cleary used DDoS attacks to crash websites of major global institutions including USAF, CIA, FBI, SOCA, Sony and Nintendo and stole personal data including passwords and credit card details belonging to millions of people that was posted online en clair. Damages estimated in millions of pounds. Ryan Ackroyd (aka Kayla), 26, was jailed for 30 months. [MTCE]	Cause; Entertainment Lulzsec's main stated motivation was to have fun by causing mayhem; however, their activities and choice of targets show a clear underlying political ideology (e.g. hacking the Westboro Church, targeting CIA/FBI/SOCA with DDOS)	Outsider	26	Male	Group (member of LulzSec)	None identified
Mustafa Al-Bassam	https://www.independent.co.uk/news/uk/crime/lulzsec-hackers-sentenced-for-sophisticated-global-cyber-attacks-8619462.html https://nakedsecurity.sophos.com/2013/05/16/lulzsec-hackers-wait-sentence/ https://www.theguardian.com/technology/2013/may/16/lulzsec-hacking-fbi-jail https://web.archive.org/web/20110619214911/http://arstechnica.com/tech-policy/news/2011/06/lulzsec-heres-why-we-hack-you-bitches.ars	Yes	May 2013	High skill (widely seen as one of the most skilled members of Lulzec)	LulzSec collective hactivists Ryan Ackroyd, Jake Davis, Mustafa Al-Bassam and Ryan Cleary used DDoS attacks to crash websites of major global institutions including USAF, CIA, FBI, SOCA, Sony and Nintendo and stole personal data including passwords and credit card details belonging to millions of people that was posted online en clair. Damages estimated in millions of pounds. Mustafa Al-Bassam (aka tFlow), 18, was sentenced to 20 months suspended for two years, and 200 hours of unpaid community work. [MTCE]	Cause; Entertainment Lulzsec's main stated motivation was to have fun by causing mayhem; however, their activities and choice of targets show a clear underlying political ideology (e.g. hacking the Westboro Church, targeting CIA/FBI/SOCA with DDOS)	Outsider	18	Male	Group (member of LulzSec)	None identified

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Matthew Beddoes	https://www.dailymail.co.uk/news/article-2295948/Black-Dragon-cyber-criminal-tried-hack-UN-computers-steal-6-5million-carbon-credits-jailed-years.html https://www.tripwire.com/state-of-security/featured/inside-the-mind-of-a-former-black-hat-hacker/	Yes	March 2013	High skill (created own Trojan for use in infiltrating UN/EU carbon credit systems; long history of previous hacks)	Zeus Trojan developed by Beddoes a.k.a Black Dragon, 32, used in attempted transfers of some 750,00 carbon credits worth £6.5m from accounts at the UN in Bonn and Spain's Carbon Credit Registry to a UK broker co-defendant. Guilty plea to six counts of conspiring to do unauthorised acts, with intent to impair computer programs, four counts of unauthorised access to business computers, three counts of possessing electronic files containing data from 3,000 credit cards. Sentenced to 2 years and 9 months imprisonment. [MTCE]	Money; Entertainment Was approached by others in order to attack UN, motivated by profit. Beddoes' lawyer stated that the scheme appealed to him as it was a new challenge.	Outsider	32	Male	Group (committed criminality in concert with others)	None identified
Christopher Weatherhead	https://www.bbc.co.uk/news/uk-20449474 https://www.theguardian.com/technology/2013/jan/24/anonymous-hackers-jailed-cyber-attacks https://www.dailymail.co.uk/news/article-2267763/Anonymous-members-jailed-denial-service-attacks-Visa-Mastercard-PayPal-websites.html https://www.theregister.co.uk/2012/12/14/uk_anon_investigation/	Yes	January 2013	Low skill (used LOIC - Anonymous-linked DDOS tool- to carry out attacks. Poor security around use of his nickname)	Hacking group Anonymous members Christopher Weatherhead a.k.a "Nerdo", 22, Ashley Rhodes, 28, Peter Gibson, 24, and Jake Burchall, 18 carried out DDoS attacks in retaliation for withdrawal of services to WikiLeaks by PayPal, Visa and Mastercard between August 2010 and January 2011; one online attack was said to have cost PayPal at least £3.5m. All four convicted. Weatherhead sentenced to 18 months in prison, Rhodes to seven months in prison and Gibson to six months prison (suspended). Sentencing of Burchall adjourned. [MTCE]	Cause Subscribed to core Anonymous ideology, and picked their targets according to this (e.g. attacked Paypal for refusing to process payments on behalf of Wau Holland Foundation, that was raising funds for Wikileaks; Operation Payback was launched against music industry companies after proceedings were brought against Pirate Bay)	Outsider	22	Male	Group (member of Anonymous)	None identified
Ashley Rhodes	https://www.bbc.co.uk/news/uk-20449474 https://www.theguardian.com/technology/2013/jan/24/anonymous-hackers-jailed-cyber-attacks https://www.dailymail.co.uk/news/article-2267763/Anonymous-members-jailed-denial-service-attacks-Visa-Mastercard-PayPal-websites.html	Yes	January 2013	Low skill (used LOIC - Anonymous-linked DDOS tool- to carry out attacks)	Hacking group Anonymous members Christopher Weatherhead a.k.a "Nerdo", 22, Ashley Rhodes, 28, Peter Gibson, 24, and Jake Burchall, 18 carried out DDoS attacks in retaliation for withdrawal of services to WikiLeaks by PayPal, Visa and Mastercard between August 2010 and January 2011; one online attack was said to have cost PayPal at least £3.5m. All four convicted. Weatherhead sentenced to 18 months in prison, Rhodes to seven months in prison and Gibson to six months prison (suspended). Sentencing of Burchall adjourned. [MTCE]	Cause Subscribed to core Anonymous ideology, and picked their targets according to this (e.g. attacked Paypal for refusing to process payments on behalf of Wau Holland Foundation, that was raising funds for Wikileaks; Operation Payback was launched against music industry companies after proceedings were brought against Pirate Bay)	Outsider	27	Male	Group (member of Anonymous)	None identified

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Peter Gibson	https://www.bbc.co.uk/news/uk-20449474 https://www.theguardian.com/technology/2013/jan/24/anonymous-hackers-jailed-cyber-attacks https://www.dailymail.co.uk/news/article-2267763/Anonymous-members-jailed-denial-service-attacks-Visa-Mastercard-PayPal-websites.html	Yes	January 2013	Low skill (used LOIC - Anonymous-linked DDOS tool- to carry out attacks)	Hacking group Anonymous members Christopher Weatherhead a.k.a "Nerdo", 22, Ashley Rhodes, 28, Peter Gibson, 24, and Jake Burchall, 18 carried out DDoS attacks in retaliation for withdrawal of services to WikiLeaks by PayPal, Visa and Mastercard between August 2010 and January 2011; one online attack was said to have cost PayPal at least £3.5m. All four convicted. Weatherhead sentenced to 18 months in prison, Rhodes to seven months in prison and Gibson to six months prison (suspended). Sentencing of Burchall adjourned. [MTCE]	Cause Subscribed to core Anonymous ideology, and picked their targets according to this (e.g. attacked Paypal for refusing to process payments on behalf of Wau Holland Foundation, that was raising funds for Wikileaks; Operation Payback was launched against music industry companies after proceedings were brought against Pirate Bay)	Outsider	24	Male	Group (member of Anonymous)	None identified
Jake Burchall	https://www.bbc.co.uk/news/uk-20449474 https://www.theguardian.com/technology/2013/jan/24/anonymous-hackers-jailed-cyber-attacks https://www.dailymail.co.uk/news/article-2267763/Anonymous-members-jailed-denial-service-attacks-Visa-Mastercard-PayPal-websites.html	Yes	January 2013	Low skill (used LOIC - Anonymous-linked DDOS tool- to carry out attacks)	Hacking group Anonymous members Christopher Weatherhead a.k.a "Nerdo", 22, Ashley Rhodes, 28, Peter Gibson, 24, and Jake Burchall, 18 carried out DDoS attacks in retaliation for withdrawal of services to WikiLeaks by PayPal, Visa and Mastercard between August 2010 and January 2011; one online attack was said to have cost PayPal at least £3.5m. All four convicted. Weatherhead sentenced to 18 months in prison, Rhodes to seven months in prison and Gibson to six months prison (suspended). Sentencing of Burchall adjourned. [MTCE]	Cause Subscribed to core Anonymous ideology, and picked their targets according to this (e.g. attacked Paypal for refusing to process payments on behalf of Wau Holland Foundation, that was raising funds for Wikileaks; Operation Payback was launched against music industry companies after proceedings were brought against Pirate Bay)	Outsider	18	Male	Group (member of Anonymous)	None identified
James Marks	https://www.pinsentmasons.com/out-law/news/sony-music-hackers-given-suspended-prison-sentence http://www.bbc.co.uk/newsbeat/article/20983940/michael-jackson-fans-sentenced-for-sony-music-hacking https://www.dailymail.co.uk/news/article-2260983/British-hackers-broke-Sony-Musics-servers-steal-unreleased-Michael-Jackson-tracks-escape-jail.html	Yes	January 2013	Semi-skilled (used a known vulnerability to get into Sony systems, but wrote own scripts to expedite exfiltration of files)	James Marks, 27, and James McCormick, broke into Sony Music's servers and downloaded 7,900 files including tracks recorded by Elvis, JLS and Beyoncé and unreleased Michael Jackson tracks. Guilty pleas. Both sentenced to six month in prison, suspended for one year and ordered to do 100 hours of unpaid community service. [MTCE]	Cause; Money McCormick and Marks claimed that they were motivated to prove that some of the tracks on Michael Jackson's record, Michael, had not been sung by him (a bizarre Cause, but still a Cause). Chatlogs seized by the police show the pair had discussed the prospect of selling music/data that they had illegally downloaded.	Outsider	27	Male	Group (alongside McCormick)	None identified

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
James McCormick	https://www.pinsentmasons.com/out-law/news/sony-music-hackers-given-suspended-prison-sentence http://www.bbc.co.uk/newsbeat/article/20983940/michael-jackson-fans-sentenced-for-sony-music-hacking https://www.dailymail.co.uk/news/article-2260983/British-hackers-broke-Sony-Musics-servers-steal-unreleased-Michael-Jackson-tracks-escape-jail.html	Yes	January 2013	Semi-skilled (used a known vulnerability to get into Sony systems, but wrote own scripts to expedite exfiltration of files)	James Marks, 27, and James McCormick, broke into Sony Music's servers and downloaded 7,900 files including tracks recorded by Elvis, JLS and Beyoncé and unreleased Michael Jackson tracks. Guilty pleas. Both sentenced to six month in prison, suspended for one year and ordered to do 100 hours of unpaid community service. [MTCE]	Cause; Money McCormick and Marks claimed that they were motivated to prove that some of the tracks on Michael Jackson's record, Michael, had not been sung by him (a bizarre Cause, but still a Cause). Chatlogs seized by the police show the pair had discussed the prospect of selling music/data that they had illegally downloaded.	Outsider	26	Male	Group (alongside Marks)	None identified
Matthew Higgins	https://www.bbc.co.uk/news/uk-wales-north-west-wales-20557579	Yes	November 2012	Low skill (used social engineering to obtain credentials for school's parent portal)	Revenge attack after bullying at school. Sixth form pupil hacked into his school computer system and accessed personal data on a female pupil. Sentenced to a 12 month community order with supervision and 120 hours unpaid work. [MTCE]	Ego; Entrance to the community; Revenge The Recorder believed that part of Higgins' motivation was to "show-off" to those in the computer hacking field, and that there was an element of attention seeking. But she was satisfied Higgins had also wanted to "get back" at the school and used his computer talents to do so.	Insider	20	Male	Lone operator	None identified
James Goodwill	https://www.bbc.co.uk/news/uk-england-cambridgeshire-19341195	No	August 2012	Unskilled (unauthorised use of authorised access)	Cambridgeshire Police officer attracted to a female witness used force computer system to obtain her phone number. Guilty plea. Sentenced to four months imprisonment. [MTCE]	Sexual To enable personal relationship with witness.	Insider	27	Male	Lone operator	
Astrid Curzon	https://www.swindonadvertiser.co.uk/news/9881311.former-beauty-queen-spied-on-headteachers-email/	Yes	August 2012	Unskilled (used known credentials to access email system not her own)	Business manager of Royal Wootton Bassett Academy had recently been made redundant when she accessed the school email system using the login and password of another school employee and read private emails from the Head. Defendant convicted. Fined £200. Ordered to pay court costs of £675 and £15 to a victim. [MTCE]	Other (curiosity) Accessed email account that she retained access to; no clear reason given for doing so.	Insider	49	Female	Lone operator	None identified
Junaid Hussain	https://www.theregister.co.uk/2012/07/27/teen_hacker_six_months/ https://ctc.usma.edu/british-hacker-became-islamic-states-chief-terror-cybercoach-profile-junaid-hussain/	Yes	July 2012	Semi-skilled (as a member of TeaMP0ison, concerted period of exploiting vulnerable websites and DDOSing targets)	18 year-old TeamP0ison hacker Junaid Hussain aka TriCk hacked into a Gmail account used by Katy Kay, a former special advisor to Tony Blair and accessed and published personal details of 150 contacts including Tony Blair and family. Also used Skype to swamp UK anti-terrorism hotline with hoax calls. Guilty plea. Six months youth detention sentence. [MTCE]	Cause Hussain's hacking, alongside other members of TeamP0ison, was inspired by anti-establishment views, feelings of persecution, and against UK/US activity in the 'Global War on Terror'.)	Outsider	18	Male	Group (member of TeaMp0isoN)	None identified

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Pavel Cyganok	https://www.bbc.co.uk/news/technology-18672068 https://www.theregister.co.uk/2012/07/02/ebanking_fraudsters_jailed/ https://threatpost.com/three-baltic-men-jailed-after-using-spyeye-malware-070212/76758/	Yes	July 2012	Semi-skilled (systematic exploitation of victims for financial gain using SpyEye malware)	SpyEye trojan used to steal login credentials for online banking accounts and then uploaded to servers controlled by Cyganok and Zakrevski. Tip-off by Estonian Police led Metropolitan Police's Central E-Crime Unit (PCEU) to seize one of the UK-based servers. An estimated 1,000 computers had been infected with victims in the UK, Denmark, The Netherlands and New Zealand. Guilty pleas. Pavel Cyganok was jailed for five years. [MTCE]	Money Hacking activity aimed solely at obtaining profit.	Outsider	28	Male	Group (alongside Zakrevski)	None identified
Ilja Zakrevski	https://www.bbc.co.uk/news/technology-18672068 https://www.theregister.co.uk/2012/07/02/ebanking_fraudsters_jailed/ https://threatpost.com/three-baltic-men-jailed-after-using-spyeye-malware-070212/76758/	Yes	July 2012	Semi-skilled (systematic exploitation of victims for financial gain using SpyEye malware)	SpyEye trojan used to steal login credentials for online banking accounts and then uploaded to servers controlled by Cyganok and Zakrevski. Tip-off by Estonian Police led Metropolitan Police's Central E-Crime Unit (PCEU) to seize one of the UK-based servers. An estimated 1,000 computers had been infected with victims in the UK, Denmark, The Netherlands and New Zealand. Guilty pleas. Ilja Zakrevski for four years. [MTCE]	Money Hacking activity aimed solely at obtaining profit.	Outsider	26	Male	Group (alongside Cyganek)	None identified
Mahdiya Khan	https://www.bbc.co.uk/news/uk-england-lancashire-23907268 [2012] EWCA Crim 2032	No	July 2012	Unskilled (unauthorised use of authorised access)	Accessed social care records in order to assist her partner who was on charge for grooming crimes [[2012] EWCA Crim 2032]	Specific access reasons in relation to a rape charge against her boyfriend	Insider	22	Female	Group	
Gareth Crosskey	https://www.theregister.co.uk/2012/05/17/facebook_account_hacker_jailed/ https://www.dailymail.co.uk/tvshowbiz/article-2147556/Selena-Gomez-Jailed-Facebook-hacker-Gareth-Crosskey-21-read-emails-Justin-Bieber.html [2012] EWCA Crim 1645	Yes	May 2012	Low skill (used social engineering in order to obtain passwords)	19 year-old McDonald's employee hacked into the Facebook account of Justin Bieber's girlfriend Selena Gomez by posing as the actress' step-father/manager to persuade Facebook staff to change the password to the account. After accessing and copying her private emails he contacted celeb magazines offering to reveal information about her. Guilty plea. Sentenced to twelve months imprisonment. Sentence reduced to eight months on appeal. [MTCE]	Ego; Status; Entrance to Community. The author of a pre-sentence report formed the view that the offences appeared to have been the product of youthful bravado and a desire to prove himself to his peers	Outsider	21	Male	Lone operator	Attention Deficit Disorder and a Hyperactivity Activity Disorder

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
James Jeffrey	https://www.judiciary.uk/wp-content/uploads/JCO/Documents/Judgments/james-jeffery-sentencing-remarks-13042012.pdf https://www.theregister.co.uk/Print/2012/04/16/anon_jailed_over_abortion_site_hack/ https://www.alphr.com/life-culture/1000788/what-happened-to-the-hacktivists https://www.bbc.co.uk/news/uk-17325182	Yes	April 2012	Semi-skilled (arrested for attack on BPAS, but had been involved in numerous other attacks previously. Claims to have been caught only due to an FBI informant (Sabu))	Defendant associated with Anonymous group used log-on details of a system admin to access 10,000 database records from abortion provider BPAS (British Pregnancy Advisory Service) and post anti-abortion messages on its home page. Sentenced to 2 years 8 months imprisonment. [MTCE]	Cause; Ego; Entertainment; Status Jeffrey boasted on twitter about his activity; believed abortion was morally wrong; defaced website with Anonymous logo; in a later interview talked of the adrenaline buzz he got from hacking	Outsider	27	Male	Group (member of Anonymous)	Suffering from depression at time of criminal activity; Aspergers
Richard Mundle	https://www.bbc.co.uk/news/uk-england-nottinghamshire-14554567 [2014] EWCA Crim 887	No	February 2012	Unskilled (unauthorised use of authorised access)	Nottingham City Council community protection officer. He had access to the police computer systems and used that in breach of restrictions notified to staff, and without authorisation, to make checks on two addresses outside his beat, namely his home address and that of a complainant in sexual allegations. [[2014] EWCA Crim 887]	Specific access reasons in relation to a rape charge against himself	Insider	32	Male	Lone operator	
Glenn Mangham	https://www.zdnet.com/article/british-student-jailed-for-hacking-into-facebook/ [2012] EWCA Crim 973 https://www.theregister.co.uk/2012/02/20/facebook_hacker_jailed/ https://www.bbc.co.uk/news/uk-england-york-north-yorkshire-17079853 https://www.casemine.com/judgement/uk/5a8ff70560d03e7f57ea5e98#	Yes	Feb 12	Semi-skilled (Used relatively sophisticated techniques to hack into Facebook, although was tracked back to his parents' IP address. Previously provided Yahoo with information around a vulnerability).	Software development student from York repeatedly hacked into Facebook and extracted internal material in Spring 2011 using the account of a Facebook employee who was on holiday. His targets included Facebook Puzzle and Mailman servers and a restricted area of the Facebook Phabricator server. Guilty plea on two counts. Sentenced to 8 months imprisonment. Serious Crime Prevention Order (SCPO) made restricting access to the internet and forfeiture of computer. [MTCE]	Entertainment The judge in Mangham's case stated that he done the crime solely for the intellectual challenge.	Outsider	26	Male	Lone operator	Aspergers and mental health issues identified
Oliver Baker	https://www.thefreelibrary.com/Prison+term+halved+for+IT+scammer.-a0252306658 [2011] EWCA Crim 928	Yes	March 2011	Low skilled (hacked into Welsh Assembly system - where he had worked previously - in order to read emails. Obtained access via a computer he had retained from previous employment).	Defendant IT contractor sacked by Welsh Assembly (for producing fake pay and display parking tickets) hacked into the Assembly's computer system on twenty occasions to read sensitive emails. Sentenced to four months imprisonment. Sentence upheld on appeal. [MTCE]	Revenge Hacked into systems in order to obtain information on previous dismissal.	Insider	28	Male	Lone operator	None identified

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Zachary Woodham	https://www.theregister.co.uk/2011/05/16/hacker_duo_sentenced/ https://www.databreaches.net/uk-computer-hacker-who-ruined-strangers-internet-business-for-a-game-and-stole-bank-account-details-is-spared-jail/ https://www.dailymail.co.uk/news/article-1387564/Hacker-Zachary-Woodham-ruined-strangers-web-business-game-spared-jail.html	Yes	May 2011	Semi-skilled (hacked into a small business in order to stop it trading; disrupted websites; conducted fraud using stolen credit cards; gave tutorial on Gh0stMarket about 'rooting servers')	Teenager using alias Colonel Root repeatedly attacked Punkyhosting web hosting company and caused it to cease trading. Guilty plea. Sentenced to 12 months' imprisonment suspended for two years and 240 hours unpaid work. [MTCE]	Ego; Entertainment; Money Boasted that he took down a company 'for a game'; redirected traffic from a church to pornographic images; obtained money through his criminality	Outsider	19	Male	Group (alongside another teenager)	None identified
Paul McLoughlin	https://www.theregister.co.uk/2011/05/18/gaming_trojan_conviction/	Yes	May 2011	Low skill (used Istealer software to obtain credentials of victims by uploading it disguised to file sharing site. Used credentials to log into accounts).	Student used Istealer password-stealing kit to create Trojan that he wrapped in several malware programs. Users tricked into downloading which enabled Defendant to harvest login credentials of over 100 web users via an FTP server. Charged with adapting an article intending it to be used to commit, or to assist in the commission of, an offence under section 1 or 3. Guilty plea. Sentenced to eight months' imprisonment suspended for 12 months. [MTCE]	Other (personal gain) Investigators reckon the miscreant was motivated by a desire to get free gaming facilities rather than enrich himself via the ruse. Personal gain.	Outsider	22	Male	Lone operator	None identified
Gary Paul Kelly	https://www.theguardian.com/uk/2011/mar/02/ghostmarket-web-scam-teenagers https://threatpost.com/four-face-jail-time-ghost-market-crime-forum-030411/74996/	Yes	March 2011	High skill (helped design malware to hack into thousands of computers; ran web platform for Gh0stMarket)	Creators of Gh0stMarket forum used by thousands to trade unlawfully obtained credit/debit card details, confidential personal information and malware tools. Guilty pleas. Kelly sentenced to five years imprisonment. [MTCE]	Money Used proceeds from criminality to pay for bills and sustain family.	Outsider	21	Male	Group (member of Gh0stMarket)	None identified

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Nicholas Webber	https://www.theguardian.com/uk/2011/mar/02/ghostmarket-web-scam-teenagers https://www.dailymail.co.uk/news/article-2287138/Public-schoolboy-hacker-masterminded-15m-fraud-jails-IT-class--hacks-prisons-system.html https://threatpost.com/four-face-jail-time-ghost-market-crime-forum-030411/74996/	Yes	March 2011	High skill (ran Gh0stMarket forum, involved in wide-scale fraud, and ran a botnet using a variant of a Zeus Trojan)	Creators of Gh0stMarket forum used by thousands to trade unlawfully obtained credit/debit card details, confidential personal information and malware tools. Guilty pleas. Webber sentenced to five years imprisonment. [MTCE]	Money; Ego; Status Used stolen credit cards and earned a significant amount through Gh0stMarket. His defence barrister said he had set the site up more for kudos and notoriety than for personal gain	Outsider	19	Male	Group (member of Gh0stMarket)	None identified
Ryan Thomas	https://www.theguardian.com/uk/2011/mar/02/ghostmarket-web-scam-teenagers https://threatpost.com/four-face-jail-time-ghost-market-crime-forum-030411/74996/	Yes	March 2011	Unskilled (a forum moderator for Gh0stMarket)	Creators of Gh0stMarket forum used by thousands to trade unlawfully obtained credit/debit card details, confidential personal information and malware tools. Guilty plea, four years. [MTCE]	Money Profited from Gh0stMarket activity	Outsider	18	Male	Group (member of Gh0stMarket)	None identified
Shakira Ricardo	https://www.theguardian.com/uk/2011/mar/02/ghostmarket-web-scam-teenagers https://threatpost.com/four-face-jail-time-ghost-market-crime-forum-030411/74996/	Yes	March 2011	Low skilled (active in the laundering of the proceeds from Gh0stMarket. While the judge claimed she was skilled in running malware from a phone, articles say she was learning the ropes around hacking)	Creators of Gh0stMarket forum used by thousands to trade unlawfully obtained credit/debit card details, confidential personal information and malware tools. Guilty plea, 18 months. [MTCE]	Money Profited from Gh0stMarket activity	Outsider	21	Female	Group (member of Gh0stMarket)	None identified
Ashley Mitchell	https://www.theregister.co.uk/2011/03/22/poker_chip_hacker_jailed/	Yes	February 2011	Semi-skilled (was able to exploit vulnerabilities in Zynga's website, although caught through use of own personal facebook page)	Poker addict hacked into American poker company Zynga and stole £7m worth of virtual poker chips for resale on Facebook. Guilty plea. Sentenced to two years imprisonment (including term for breach of previous suspended sentence for hacking). [MTCE]	Money Hacking was aimed solely at obtaining profit via obtaining/selling chips	Outsider	27	Male	Lone operator	None identified
Daniel Woo	https://www.theregister.co.uk/2010/11/25/fake_student_hacker_scam/	Yes	August 2010	Low skill (installed Cain & Abel on university computers in order to harvest credentials)	Bulgarian pretending to be a student installed key logging software to capture passwords and access emails containing personal and financial data. Guilty plea. Sentenced to eight months imprisonment, suspended for two years. Two year supervision order, 200 hours unpaid work and £21,000 costs and compensation ordered. [MTCE]	Money Targeted bank accounts linked to email addresses.	Outsider	23	Male	Lone operator	None identified

Name	Source (all websites accessed in July 2020)	Hacker	Date of conviction	Skill level	Description of Case	Motivation	Insider or Outsider	Age (at conviction)	Gender	Lone operator or part of Group	Mental Health Issue
Matthew Anderson	https://www.theregister.co.uk/2010/10/25/scots_xver_warpigs_jailed/ https://www.theregister.co.uk/2010/11/23/matthew_anderson_warpigs_sentence/ https://www.theguardian.com/technology/2010/nov/23/computer-expert-jailed-hacking-webcams	Yes	October 2010	Semi-skilled (involved in a wide variety of sophisticated hacking activity, although had to commission others to develop viruses and create botnets)	Franchise manager aka Warpigs virus writer used malware attached to spam to spy on victims using their webcams and steal personal information. Guilty plea. Sentenced to eighteen months imprisonment. [MTCE]	Money; Entertainment While he earned profit off his hacking, he also seemingly conducted some activity for amusements sake (e.g. making a teenage girl cry via taking control of her computer).	Outsider	33	Male	Group (member of m00p)	None identified
Keziah Stubbs	[2011] EWCA Crim 926	No	October 2010	Unskilled (unauthorised use of authorised access)	Civilian employee of Gloucestershire Constabulary who made enquiries on the system for information in relation to people known to her and a second party with the intention of passing that information on to others outside the police service. Also made searches of the official database for personal use [[2011] EWCA Crim 926].	Further criminality Accessing information in order to advance further criminality.	Insider	32	Female	Group	
Dale Trever	https://www.theregister.co.uk/2010/10/05/hull_man_snoop/	No	September 2010	Unskilled (unauthorised use of authorised access)	Primary Care Trust data manager accessed confidential female NHS patient medical records. Guilty plea. Sentenced to six months imprisonment, suspended for two years. [MTCE]	Curiosity Accessed medical data of female victims known to him personally.	Insider	22	Male	Lone operator	
Balwinder Basran	https://www.birminghammail.co.uk/news/local-news/west-midlands-police-detective-fined-131491	No	September 2010	Unskilled (unauthorised use of authorised access)	Police officer accessed police computer records for private use. Guilty plea. Fined £2,000. [MTCE[	Curiosity/personal use Obtained personal details of a female colleague	Insider	47	Male	Lone operator	
Robert Campbell	https://www.independent.co.uk/news/uk/crime/pc-used-force-computer-to-become-sexual-predator-2028435.html	No	June 2010	Unskilled (unauthorised use of authorised access)	Sexual adventurer Police officer accessed police computer records for private use. Guilty plea. 18 month Conditional Discharge and ordered to pay £1,200 costs. [MTCE]	Sexual Accessed details of women	Insider	42	Male	Lone operator	