The Computer Misuse Act and the characteristics of convicted hackers

Authors
James Crawford, MSc (Royal Holloway, 2020)
Rikke Bjerg Jensen, ISG, Royal Holloway

Abstract

The Parliamentary debates that preceded the introduction of the Computer Misuse Act in 1990 provided some initial views on who criminal hackers were believed to be, and against whom the Act was aimed. Emma Nicholson MP commented that hackers 'support a drug-based lifestyle on their activities', while Dr Moonie MP, a psychiatrist by profession, believed that 'a profound sexual inadequacy is often related to such behaviour'. This article attempts to go beyond these somewhat absurdist stereotypes by analysing the characteristics of 132 of the individuals convicted under the CMA between 2008 and 2018. Who are the convicted hackers in the UK?[a]

[a] This article is published online by Computer Weekly as part of the 2021 Royal Holloway information security thesis series https://www.computerweekly.com/ehandbook/Royal-Holloway-The-Computer-Misuse-Act-and-the-characteristics-of-convicted-hackers. It is based on an MSc dissertation written as part of the MSc in Information Security at the ISG, Royal Holloway, University of London. The full thesis is published on the ISG's website at https://www.royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/research/explore-our-research/isg-technical-reports/.

The Computer Misuse Act (CMA) entered its 30s in June 2020. To celebrate, a group of cyber security experts (under the CyberUp campaign) wrote a letter to Boris Johnson calling for its reform. Ironically, the letter laments the shackles that the CMA places on the ability of cyber security professionals to respond to threats. That it is no longer seen as fit for purpose is hardly surprising. The analysis of its birth, in the dissertation that underpins this article, shows that the nature of the threat was poorly understood by those legislating against it. In fact, it was intended as a PR statement as much as to enable prosecutions. Nevertheless, the CMA did have some teeth and, as explained to the House of Commons by Gary Waller MP, was expected to 'plug a loophole in the law' by forbidding unauthorised access or modification to/of computer material. Who these hackers were, though, appears to have been another blind spot. The Parliamentary debates around the introduction of the Act perceived of a sprawling, conspiratorial threat carried out by individuals who were claimed to be supporting drugs-based lifestyles or attempting to offset profound sexual inadequacies.

Despite its inauspicious start, the CMA *has* led to some convictions: Ministry of Justice statistics show that 303 individuals were convicted under the provisions within the CMA between 2008 and 2018. These numbers are low compared to the number of relevant crimes believed to have been committed over this period (for numerous reasons, including that individuals have been prosecuted under other laws), and hence the sample size is extremely small compared to the delinquent population (and, perhaps, unrepresentative by the very fact of being caught). Yet, there are enough convictions to start to understand who is behind the criminality and move beyond the Parliamentary caricatures. This article is based on an analysis of 132 of these individuals (accessible as part of the underlying dissertation), assessing their key characteristics (skill, motivation, demographic etc.) in order to provide some insight into who they are and what threats they may pose. These 132 individuals were identified primarily through Michael Turner's `computerevidence.co.uk` website, with further analysis done on each individual through media reporting, security websites and public court documents. An accurate and concrete understanding of who is being convicted has implications for both government policy and law enforcement attempts to deal with these threats. It can also serve as a reflection on the effectiveness of the CMA and efforts to enforce it, a complex issue in itself.

Hackers?

There is no agreed definition of a hacker in the academic literature. The one used in this article is 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). The provision of a definition is not just an academic exercise; of the 132 cases examined, 32 involved unauthorised access to, or use of, data without getting round any security controls. This also includes where this authorisation had been presumed to be removed. These individuals fall outside the definition and cannot be considered hackers in any sense of the word. Indeed, they are predominantly law enforcement officials who misused police systems. They make up a substantial proportion of those analysed (almost 25%) and were clearly not the intended targets of the Act; but, still, have fallen foul of it. This boost in prosecutions significantly inflates conviction rates under the CMA, leading to an inaccurate reflection - and understanding - of the CMA's effectiveness against the external hacking threat.

Skill

Across the remaining 100 convicted individuals there is a large variation in skill levels. Using Holt and Kilger's[1] divisions of hackers into highly skilled, semi-skilled, low or unskilled hackers, it is clear that the majority of individuals showed little or no hacking skill in the crimes that secured their convictions. From retweeting a link to an anonymous DDOS (distributed denial of service) tool to using known credentials of third parties to gain illegal access, the group of unskilled individuals have a fairly nebulous claim to belong to the hacking fraternity. Those in the low skill category are largely ex-IT employees who employed their knowledge of the systems that they used to operate in order to damage their previous employers, and other individuals using open-source software or rented botnets (usually coupled with a lack of obfuscation techniques) in order to conduct their activity. Twenty-eight of the 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 perhaps more common perception of a hacker. 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. Eight of the individuals convicted under the CMA are classed as high skilled actors. This includes those who wrote their own malware, controlled and rented out destructive botnets, or were high-performing members of prominent hacktivist groups. These individuals uniformly carried out a wide array of criminal activity, both for their own ends and, more often, on behalf of others.

Table 1: Skill level of convicted hackers.

Unskill	Low skill	Semi-skilled	High skill
18	46	28	8

The Act was meant for use in catching the highest profile remote hackers; but, with only 35 of the 100 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. 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 (those who did not circumvent security controls) cannot even be considered as such 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 limited knowledge; the large number of individuals using widely available remote access trojans or DDOSing services is a testament to this. It is clear in a number of cases that individuals have used

[1] 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`

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.

Motivation

Analysis of any individual's motivation is always a fraught exercise, especially when done through media representations as in this case. Nevertheless, some important conclusions can be drawn from these 100 individuals. Kilger, Arking and Stutzman[2] 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). These are the classic motivations attributed to the hacking fraternity. However, only 68 of the individuals examined are linked to a motivation under the MEECES framework. The bulk of the rest of the individuals (27) were motivated by either criminal sexual activity or revenge, with the remaining five evading classification. The interesting division in this data is around the skill level correlated against the motivations. All of the highly or semi-skilled individuals are linked to at least one of the motivations under the MEECES framework; while all but one of the individuals linked to sexual motivation or revenge were low or unskilled. 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.

Table 2: 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

Note: ego-centric includes Ego, Entertainment, Entrance to Social group and Status.

An attractive conclusion from this 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. However, the absence of these motivations may be explained by the fact that 26 of the 27 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. Still, 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.

[2] 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

Demographics

The common hacker stereotype of young males is supported by the results of this analysis. Of the 100 hackers, three in the data are women. All of the semi-skilled or high skilled hackers are male. As for those not considered to be hackers, eight of the 32 are women; a significant difference in proportion. As for age, 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 demographic stereotype is a link between hackers and high-functioning autism and other mental health disorders. 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. This is 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.

The greater the skill level, the more pronounced these demographic characteristics become. Indeed, this reflects a clear 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 and popular consciousness, 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.

Table 3: 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

Insiders and groups

This division in the data is echoed when considering who the convicted hackers worked alongside, and who they targeted. Of the 100 criminal hackers, over half acted with at least one accomplice, with the preponderance of hackers to act together becoming greater the higher their skill level, indicating there is merit in the claims that the most dangerous hackers act in collectives. 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 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.

Table 4: Comparing skill level to hackers' relationships (with associates and victims).

	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

Conclusion

As demonstrated here, 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, such as status, entertainment, entrance to community, larger numbers are indicative of more common criminal concerns, including preponderance of financial motivations, criminal sexual motivation, revenge. These hackers are not, by and large, aligned with organised crime groups 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.

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. 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.

Biographies

James Crawford is a Civil Servant who has recently completed an MSc in Information Security at Royal Holloway University of London.

Rikke Bjerg Jensen is a social scientist and ethnographer in the Information Security Group at Royal

Holloway University of London. Her research focuses on collective security practices. Specifically, it explores the different security needs, perspectives and practices amongst groups of people living and working on what we might call *the edge* of society.

Series editor: S.- L. Ng