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

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.