Combating Cyber Dependent Crimes: The Legal Framework in the UK

Oriola Sallavaci(✉)

Anglia Ruskin University, Chelmsford CM1 1SQ, UK
Oriola.Sallavaci@anglia.ac.uk

Abstract. Computer crimes and digital investigations comprise a substantial part of criminal policy, law and practice as information becomes the cornerstone of global economy. Innovative ways of attacking, exploiting and interfering with computer and communication technologies are regularly emerging, posing increasing threats to the society, economy and security. It is essential that in tackling cybercrime the right legal framework of offences is in place and that there is clarity in how the powers that are used to investigate cybercrime interact with the offences designed to catch cyber criminals. This paper reviews the current legal framework to cyber dependent crimes in the UK, including its recent amendments, and highlights areas that remain problematic and in need of attention from policymakers.

Keywords: Cybercrime · Computer misuse · Computer security · Hacking

1 Introduction

The internet and digital technologies are transforming the world we live in by driving economic growth and providing new ways for people to connect, communicate and co-operate with one another. Cyberspace is transforming business, making it more efficient and effective by opening up markets, allowing commerce to take place at lower cost and enabling people to do business on the move. Yet, as the internet and digital technologies are becoming increasingly central to nations' economy and society, the growing role of cyberspace has also opened up new threats as well as new opportunities.

Cybercrime has increased correspondingly with the increased amount of computers and internet access. In 2015, in the UK, 22.5 million households (86%) had internet access (up from 56% in 2006) and 39.3 million adults (78%) accessed the internet every day [1]. The new and fast developing technologies provide for new opportunities to commit crime and, as technological developments become more widely available, an ever increasing number of criminals are taking advantage. The Internet Security Threat Report 2016 by Symantec shows an overall increase in cybercrime during 2015 with a 25% increase in breaches since 2013, and over 429 million global identities exposed via cyber-attacks, up 23% since 2014 [2]. Hacking continues to be the primary cause of data breaches in 2015, with the data stolen across breaches more valuable and the impact to the business greater than in previous years [2].

Whilst cyberattacks against businesses and nations hit the headlines with an overwhelming regularity, the cyber threat has been assigned a 'Tier One' threat status

H. Jahankhani et al. (Eds.): ICGS3 2017, CCIS 630, pp. 53–66, 2016.
DOI: 10.1007/978-3-319-51064-4_5

in the UK's national security strategy which indicates one of the highest priorities for action [3]. To assist in tackling the cyber threat, £860 million of public funding was set aside as part of a five-year National Cyber Security Programme. The national cyber security strategy set out the key objectives that the Government intended to achieve by 2015 in relation to cyber security and cyber-crime, to both tackle the threats and reap the benefits of cyberspace [4]. Among other measures in fighting cybercrime, having in place a national legal framework fit for purpose, has been one of the main strategic priorities of the government [4].

Cybercrime is an umbrella term used to describe two distinct, but closely related criminal activities: *cyber-dependent* and *cyber-enabled* crimes [5].[1] *Cyber-dependent crimes*, also known as computer related crimes, are offences that can only be committed by using a computer, computer networks, or other forms of information and communications technology (ICT). These acts include the spread of viruses and other malicious software, hacking, distributed denial of service (DDoS) attacks etc. Cyber-dependent crimes are primarily acts directed against computers or network resources, although there may be secondary outcomes from the attacks, such as fraud. *Cyber-enabled crimes* are traditional crimes that are increased in their scale or reach by the use of computers, computer networks or other ICT. Unlike cyber-dependent crimes, they can still be committed without the use of ICT [5].

In the UK, specific offences most commonly associated with cyber-dependent crimes, such as hacking and the creation or distribution of malware, are defined in the Computer Misuse Act 1990 (CMA) which remains the main legal instrument in combating these types of crime. CMA was drafted almost three decades ago, with no possible foresight concerning technology's evolution and its impact into creating new forms of offending [7, 8]. During the past decade CMA has undergone several amendments: initially by the Police and Justice Act 2006 (PJA) and more recently by the Serious Crime Act 2015 (SCA) in a bid to bring the legislation up to date with the outstanding developments of the digital world.

This paper provides an overview of the current legal framework on tackling cyber dependent crime with the aim of identifying the remaining problems that need be addressed to ensure an effective and robust response to cybercrime. It is hoped that this will help to drive forward policy decisions in this area which is vital in the context of emerging forms of cybercrime and technological developments.

2 Computer Misuse Act 1990: The Unauthorised Access Offences

Computer Misuse Act 1990 was introduced to deal with computer related offences and, to this day, remains the main legislative measure in force to combat cyber dependant crime. The aim of the Act is to secure computer material against unauthorised access or modification; and for connected purposes. In its initial form it established three main

[1] Other classifications include computer integrity offences, computer related offences and content related offences [6].

offences namely: unauthorised access to computer material (s1), unauthorised access with intent to commit further offences (s2) and unauthorised acts with intent or with recklessness to impairing the operation of the computer (s3). s3 which was replaced by PJA 2006 will receive attention further below alongside other important amendments to CMA.

2.1 Section 1 – The Offence of Unauthorised Access

Section 1 of the Computer Misuse Act 1990 is the main provision on hacking. It was introduced to cover all forms of unauthorised access to computer material regardless of a hacker's motives and intended to act as a deterrent to all forms of hacking, including by the so called 'innocent hackers' who break through security systems as a hobby [9]. Section 1 CMA states:

> 'A person will be guilty of unauthorised access to computer material if he causes a computer to perform any function with intent to secure access to any program or data held in any computer, or to enable any such access to be secured; if the access he intends to secure, or to enable to be secured, is unauthorised; and if he knows at the time when he causes the computer to perform the function that this is the case.'

Section 1 carries a maximum penalty of two years imprisonment on conviction on indictment or an unlimited fine, or both.

Computer Misuse Act 1990 does not provide a definition of 'computer' due to considerations that any such definition would soon become outdated given the rapid and continuous development in technology [6, 10].[2] This approach is appropriate, especially considering that we have entered the age of 'Internet of Things' where even domestic appliances, cars and any object that incorporates computer technology can become target for attack [6]. On application, courts in the UK have adopted the contemporary meaning of the word 'computer' which is defined by the Oxford Dictionary as 'an electronic device which is capable of receiving information (data) in a particular form and of performing a sequence of operations in accordance with a predetermined but variable set of procedural instructions (program) to produce a result in the form of information or signals'. According to s17(6) CMA programs and data in this sense refer to any removable storage held in the computer. For definition purposes, courts have focused on the features of a computer rather than its physical nature. In *DPP v Jones* [1997] 2 CR App R 155 a computer was defined as a device for storing, processing and retrieving information.[3]

The offence itself focuses on the functions used to gain access to any program or data held in the computer. As such, reading confidential information displayed on a screen or using forms of electronic 'computer eavesdropping', for example using embedded laptop microphone as a listening device, do not constitute offences under this section [11]. According to s17(2) *functions* can include outputting; using; copying; deleting and modifying a program or data. Most actions by computer users will fall

[2] Note that both the Convention on Cybercrime Art 1(a) and Directive 13/40/EU Art 2 (a) provide definitions which are similar to one another.

[3] At p.163 (Lord Hoffman).

under the classification 'to perform any function' including switching on/off a computer or using a non-open computer which has been left accidentally logged on by authorised users, as established in *Ellis v DPP* (No1) [2001] EWHC Admin 362 whereby the offence was deemed as sufficiently wide to cover the use of logged in terminals without permission.[4]

The *mens rea* of the offence covers two aspects. First, the defendant must know that his intended access was unauthorised and, second, the defendant must have intended to secure access to any program or data held in the computer. Intention is extended to include enabling someone else to secure unauthorised access to a computer or to enable the defendant themselves unauthorised access to a computer at a later time - s1(1)(a) CMA. Mens rea does not however extend to recklessness as s1 only deals with 'deliberate activities' whereby the offender must have knowledge that the access is unauthorised [12]. According to Section 1(2) the intent to secure access does not need to be directed at any particular program or data, a program or data of any particular kind or a program or data held in a particular computer. This is important in making the legislation enforceable, as in practice it would be very difficult for the prosecution to prove otherwise.

Access is considered unauthorised if a person is not entitled to control access to the program or data, or if no consent has been given from someone who is so entitled – s 17(5) CMA. As discussed below, the issue of authorisation has been problematic; the application of the section has been easier for external offenders but less straightforward in cases of inside hackers such as an employee [13]. In the latter situations, it is the duty of the organisation in question to clearly specify the persons with authority to access the computer or system in issue. Contracts of employment and any surrounding information such as oral advice and office practices will be looked at to determine whether an employee has exceeded the limits of the authorisation [11, 14].

Good intent will not affect the applicability of s1 CMA. The case of *R v Cuthbert* [2005] (Unreported, Horseferry Road Magistrates Court, 6 October 2006) demonstrated that ethical hackers could be found guilty of unauthorised access to computer material. Cuthbert, a computer security consultant, performed penetration tests on the Disasters Emergency Committee website as he was suspicious that the website was not authentic. It was held 'with some considerable regret' that he had committed an offence under s1 by knowingly performing unauthorised access against DEC's systems. Uninvited security testing was considered a form of vigilantism which clearly breaches the computer Misuse Act 1990 [15].

2.2 Section 2 CMA– The Ulterior Intent Offence

Section 2 CMA deals with those cases where more serious offences are intended to be committed after the gaining of unauthorised access to computer material. These ulterior offences need not be completed, merely intended by the offender. Offences such as fraud, theft and blackmail could all be ulterior offences under Section 2. If the ulterior

[4] Para 16 (Lord Wolf).

offence has actually been committed, then *that* will be the one charged. For instance, most on-line frauds (such as on-line/internet banking fraud, i.e. fraudulent withdrawals from internet bank accounts using stolen identities) are prosecuted under the Fraud Act 2006, while CMA offences are used for "pure" hacking or denial-of-service prosecutions. As discussed further below, while this could provide an explanation on the low prosecution rates under CMA, the effectiveness of CMA as a legal instrument still warrants criticism [16].

According to s2 CMA 'a person will be guilty of an offence if he commits the Section 1 offence of unauthorised access with intent to commit a further offence, or facilitate the commission of such offence'. It is not necessary for the ulterior offence to involve the use of a computer even though it usually will [9]. This section was introduced as the existing law relating to criminal attempts was deemed inadequate to address cases of hacking with intent to commit ulterior offences. The Criminal Attempts Act 1981s 1(1) requires that the offender must have done an act which is more than merely preparatory to the commission of an offence. To go beyond a purely preparatory act means 'to embark on the crime proper', that is to commence the actual commission of the offence – *R v Gullefer* [1990] 1 WLR 1063, 1065. A hacker who accesses a bank's computer system with intention to transfer funds but is unable to get past further security systems would not be guilty of an attempt of theft as the hacker's conduct at that point would be considered merely preparatory [11]. Section 2 ulterior offence makes it possible for a hacker in this situation to be found guilty under CMA.

R v Delamare (Ian) [2003] EWCA Crim 424 demonstrates the severity with which courts view the Section 2 offence as compared to the Section 1. D, a bank employee obtained and disclosed bank details to an acquaintance, who then impersonated one of the account holders to obtain £10000 from the bank. D was convicted to two charges under s2 for facilitating the commission of a further offence, in this case fraud. It did not matter that the ulterior offence took place on a different occasion to the unauthorised access under s2(3), nor did it matter that the further offence was committed by another person under s2(1)(b) [17].

2.3 Interpretative Challenges on Unauthorised Access Offences

While Computer Misuse Act 1990 achieved the criminalisation of hacking behaviour which previous legal instruments had struggled to do, there have been several key areas of complexity and uncertainty surrounding the existing law. Courts have faced considerable challenges in interpreting and applying the legislation particularly with regard to the issue of *authorisation*. There has been much inconsistency in the application of these offences and it can be argued that one of the main reasons is a lack of understanding and expertise in new and emerging areas of criminal activity [6].

Judicial interpretation emerged as one of the main difficulties in the application of unauthorised access offences especially in the early period of the Act's establishment. Such difficulties were seen in *R v Cropp* (Snaresbrook Crown Court, 4 July 1991) which was the first prosecution under the Act. The interpretation made by the judge in the case to the then Section 1(1)(a) as requiring a second computer to be involved for the offence to be committed, if upheld, would have seriously limited the scope of CMA

especially since the majority of instances of hacking are those carried out within organisations [6]. *AG-s reference* (No1 of 1991) [1992] 3WLR 432 rejected the Crown Court's interpretation and clarified that the wording of the provision 'any computer' literally meant that; there were no grounds for importing the word 'other' between 'any' and 'computer' (at para 437).

The application of unauthorised access offences to inside offenders has often been inconsistent. An offence is *not* committed under s.1 by a person who is authorised to access particular computer data, but does so for unauthorised purposes – as per *DPP v Bignell* [1998] 1 Cr. App. R. 1 whereby police officers authorised to obtain car registration details from the Police National Computer for police work purposes, accessed - via an operator - details of cars from Police National Computer for their own private/personal purposes. The defendants appealed successfully that using authorised access for unauthorised purposes was not unlawful. The court distinguished the activity of 'breaking into computers' from the 'misuse of data'. Bignells' actions would have constituted an offence under s.55 Data Protection Act 1998 but this was not charged.

Bignell has received considerable criticism. As a commentator puts it: 'authorisation relates to the giving of permission, which concerns not only the area of conduct, but the conduct itself within it' [16]. The House of Lords had an opportunity to review the *Bignell* decision in *R. v Bow Street Metropolitan Stipendiary Magistrate Ex p. Allison v United States* (No. 2) [2000] 2 A.C. 216 an extradition case involving an authorised employee of a credit card company who gained an unauthorised access to credit card details in order to create forged cards. The facts of the case were similar to *Bignell* in the sense that defendants used authorised access to gain access to unauthorised material. However unlike *Bignell*, the defendant was found guilty. The court held that, the authority to access *a particular piece of data* was not authorisation to access *similar data* in the absence of permission to do so. The ambiguity regarding the definition of "unauthorized" was resolved; the term relates to the specific data accessed rather than the same kind of data suggested in *Bignell*.

However it must be noted that, while some of the Divisional Court's reasoning in relation to s.17(5) was disapproved, the House of Lords concluded that the result in *Bignell* was 'probably right'. Authorisation was secured as the police officers 'merely requested' information from the computer operators who are authorised to access the Police National Computer. Critics of the decision note that this is problematic; due to the application of the doctrine of innocent agency, operators should not have been viewed as participants in the alleged offences [16].

In some cases such as *Ex p. Allison above and Bonnett* (November 3, 1995, Newcastle under Lyme Magistrates' Court), courts supported convictions of police officers who had themselves accessed the PNC for unauthorised purposes. However, at the same time courts denied support to convictions in cases where, like the Bignells, defendants had asked others to access the data in question for them, such as in *Farquarson* (Croydon Magistrates Court, 9 December 1993). As a commentator puts it, 'the confusion and lack of clarity in the application of the crucial concept of "authority" has somewhat undermined the Act' [16].

3 The Police and Justice Act 2006 Amendments: Impairing the Operation of a Computer and Misuse of Devices

Since the enactment of the Computer Misuse Act 1990 new forms of offending have emerged alongside the technological advancements which were not envisaged at the Act's creation. In order to deal with new types of cyber dependent offences, amendments were introduced by the Police and Justice Act 2006 which created two new offences. The previous Section 3 offence regarding unauthorised modification of computer material was replaced with a new, wider offence concerning unauthorised acts with intent to impair the operation of a computer – s36 PJA. In addition, s3A was introduced in order to criminalise the misuse of devices; namely the making, supplying or obtaining of articles for use in computer misuse offences – s37 PJA. These amendments tried to address the lack of effectiveness of CMA in coping with computer dependent crime. However it is questionable whether the broadening of the scope of the offences established by the CMA has achieved this ambition.

3.1 Section 3 Offence

The old Section 3 offence dealing with the modification of the contents of a computer was replaced by PJA 2006 due to the uncertainty as to whether the existing offence captured all types of denial of service (DoS) attacks. Many DoS attacks were not being investigated because 'no crime could be framed' [10]. With direct attacks, the nature of the communications sent to the target machine will often fall within a class of transmission which the target machine was designed to receive. As such, while there may be the necessary intention to cause modification and impairment, the modification itself may not be considered unauthorised. *DPP v Lennon* [2006] EWHC 1201 (Admin); (2006) 170 J.P. 532, clarified on its facts that there is no deemed authority/consent to send emails to a person's email address where the purpose of sending the emails is to disrupt the operation of the computer. Even though the Divisional Court was considering the original s.17(8)(b) prior to the 2006 amendment, its analysis and reasoning are still helpful.

The new s3 offence is much wider in scope so as to encompass all DoS attacks. It captures a wider range of offending conduct which will be deemed unauthorised if the person doing or causing an act to be done is not responsible for the computer, or entitled to commit an act, or if no consent has been given by any such person - s17(8) CMA. An unauthorised act for these purposes can include a series of acts - s.3(5)(b) - which is essential in making DoS attacks unlawful in cases where an attacker floods a system with multiple messages. The sending of viruses and other malware constitutes unauthorised acts under this section, just as they did under the former Section 3 offence. Interference with websites constitutes an unauthorised act, as depicted by *R v Lindesay* [2002] 1 Cr App R (S) 86 whereby the defendant was sentenced to nine months imprisonment for deleting data off of his former employer's client websites.

The main issue with the amended provision is that it hinges on *impairment* rather than *modification* [18]. CMA does not include a technical definition for 'impairment'. The term is given its ordinary meaning, defined by the Oxford dictionary as 'the state of

being diminished, weakened or damaged'. This causes interpretive problems as the offence revolves around a subjective concept rather than an objective one. Under the former modification offence, either a change was to computer data or it was not, making the modification offence relatively straightforward to establish [18]. However impairment can amount to different things due to the many characteristics of a computer [19]. CMA does not provide a way to differentiate between different types of impairment caused. The threshold to which a decline in system performance for instance, crosses the boundary into impairment, is unclear and problematic especially considering that the impairment can be temporary - s.3(5)(c) CMA [20]. Equally, evidential difficulties may arise as, once a system has been rectified, proving the requisite amount of impairment had occurred at the appropriate time and linking it to an unauthorised act could be problematic [16].

Another major change was the introduction of *recklessness* to the *mens rea* of the s3 offence. For the impairment offence to occur, merely for data to be impaired is not enough; this should be done with intent or must be foreseen by the offender. If it was foreseeable that the unauthorised act would cause impairment, prevention or hindrance to any computer, program or data, and the person involved foresaw that risk but took it anyway, s/he would be found guilty of the s 3 offence committed through recklessness. It must be noted that no other offence in CMA includes recklessness as a form of mens rea, nor was it proposed by the All Party Internet Group (APIG) in its recommendations for this offence [10]. Its inclusion was clearly made as an attempt to improve the enforceability of CMA and raise the prosecution rates, as in practice it is easier to prove the foreseeability of a risk rather than the intention to behave in a certain way to achieve particular results. However the expansion of the scope has been criticised in terms of it potentially triggering questionable attempts to prosecute and creating further interpretative difficulties [16].

3.2 Section 3A – Making, Supplying or Obtaining Articles for Use in Offences

One of the main reasons as to why computer related offences have become so common is because relevant tools and articles are freely available on the internet. Many of these tools do not require any special skill to be used. In order to deter the accessibility and subsequent use of hacking tools, Police and Justice Act 2006 added Section 3A. This was done so as to ensure compliance with Article 6 of Cybercrime Convention which requires that:

> 'Each party shall adopt such legislation and other measures as they may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: the production, sale, procurement for use, import, distribution or otherwise making available of a device …computer password … or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offences established'.

S3A establishes three offences. The first prohibits making, adapting, supplying, or offering to supply any article intending it to be used to commit, or to assist in the commission of any of ss1-3 offences. The second prohibits supplying or offering to

supply any article believing that it is likely to be used to commit, or to assist in the commission of an offence. The third offence prohibits obtaining any article with a view to it being supplied for use to commit or to assist in the commission of a ss1-3 offence.

The application of s3A has not been without controversy. The main problem concerns the legitimate use of developing and supplying tools for computer security. Many hacking tools are dual-use and are indistinguishable from utilities that are essential for the maintenance and security of computers and networks. These tools can be used for lawful and unlawful purposes. Originally the APIG advised Parliament not to legislate the criminalisation of hacking tools as it would only cause unnecessary confusion and anxiety to the legitimate users of these programs [10]. Researchers in information security, penetration testers and other professionals in the field may develop and make available such tools in the course of their study or business [6]. If these tools are then used, security researchers may fear that they can be found guilty under Section 3A(2) [21].

The criminalisation of possession, fabrication and distribution of hacking tools seems to have a broad remit, leading to problematic definitions and situations when attempting to establish one's (malicious) intent [22]. The provision allows wide powers to the law enforcement in deciding who is or not an offender. In order to establish whether s3A(2) can be applied, the *likelihood* of the article being used to commit an offence need be considered. However, how the 'likelihood' is to be determined is not clarified in the provisions themselves, which creates interpretive difficulties. As a commentator puts it 'criminal law requires clarity, not generalised ambitions; a court - a judge or a jury - needs to know what tests to apply; investigators need to know what evidence to assemble' [21].

In determining the likelihood of an article being used (or misused) to commit a criminal offence, the Crown Prosecution Service (CPS) has provided the following list of factors to be taken into consideration when prosecuting:

- Has the article been developed primarily, deliberately and for the sole purpose of committing a CMA offence (i.e. unauthorised access to computer material)?
- Is the article available on a wide scale commercial basis and sold through legitimate channels?
- Is the article widely used for legitimate purposes?
- Does it have a substantial installation base?
- What was the context in which the article was used to commit the offence compared with its original intended purpose? [14].

Prosecutors are required to look at the functionality of the article and at what, if any, thought the suspect gave to who would use it; whether for example the article was circulated to a closed and vetted list of IT security professionals or was posted openly [14]. The first factor in the guidance is helpful and could have been included in the provision itself. However the remaining factors are somewhat problematic. The second factor misses the legitimate freeware tools while answers to the third factor would not add significant insight to proving one's intent, as there are dual use tools, such as nmap, and more offensive tools, such as nessus, which are widely used for both benevolent and malicious purposes. The last question is a complex one which requires professional

expertise contribution on a case by case basis, whilst the introduction of 'context' could cause problems with respect to the dual use of the hacking tool [22].

Section 3A does not provide that legitimate users of such hacker tools will avoid liability and, as a result, security testers may stop using dual use tools until proper precedent has been made. This could cause a decrease in computer security which is the opposite of what s3A intends to achieve [22]. It is regrettable that s3A does not adopt the wording of Article 6(2) of the Cybercrime Convention (Budapest Treaty) which is as follows:

> 'an article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession…of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.'

If the wording of s3A reflected Article 6 (2) of the Cybercrime Convention then legitimate users of dual usage tools would feel less cautious about using them. Until the legitimate usages of hacking tools have been identified or s3A has been amended, the latter will continue to be 'a black hole in cyberspace rather than an efficient battleship' [23]. However it is important to note that the aim of restricting the availability of hacking tools cannot be achieved solely by finding an appropriate form of words. Informed prosecutorial policy decisions will have to be taken, balancing the need to make more difficult the casual attack on information systems against the need for tools to protect legitimate users [21].

4 Amendments to CMA Introduced by the Serious Crime Act 2015

Serious Crime Act 2015 amended Section 3A CMA so as to comply with the EU Council Directive 2013/40 EU on attacks against information systems. The aim of the Directive is to establish a set of minimum rules within the European Union on offences and sanctions relating to attacks against information systems. It also aims to improve the cooperation between competent authorities in EU Member States. The existing UK legislation was deemed compliant with the Directive save in two respects: tools used for committing offences (Article 7) and jurisdiction (Article 12). The amendments in the Serious Crime Act 2015 addressed these gaps.

According to Article 7:

> 'Member states shall take the necessary measures to ensure that the intentional production, sale, procurement for use, import, distribution or otherwise making available of … a computer programme or password… without right and with intention to commit any offence is punishable as a criminal offence, at least for cases which are not minor' [24].

The existing Section 3A met the requirements of Article 7 except in one respect: 'procurement for use' of tools to commit an offence [25, 26]. A loophole had been created by Section 3A(3) whereby it was an offence to obtain an article with a view to supplying it to another for the commission of an offence but it was not an offence to obtain it for personal use with intention of committing an offence. In other words, the

offence required the involvement (or intended involvement) of a third party. Section 42 of the Serious Crime Act extended Section 3A of the 1990 Act to include an offence of obtaining a tool for use to commit a Section 1, 3 or 3ZA offence *regardless of an intention to supply that tool* – thus removing the requirement of the involvement, or intended involvement, of a third party and ensuring that the offence covers individuals acting alone.

This amendment makes Section 3A more effective in principle, as it allows the police to intervene and interrupt an attack before it has taken place i.e. at the time the offender obtains a tool or article for usage. Before the amendment, individuals could obtain tools such as malware having the knowledge that they had a good chance not to be prosecuted unless it could be proved that they obtained the tool with the view to supply it to commit a computer misuse offence. The amendment creates a deterrent effect on such individuals as it will be easier for the prosecution to prove that they procured such tools with the intention of committing an offence due to the very nature of the tools involved.

The second amendment arising from the Directive widens the territorial scope of the Act by amending the two sections (ss.4 and 5) dealing with jurisdiction. Article 12 of the EU Directive covers jurisdiction and requires Member States to establish their jurisdiction with regards to a cyber offence being committed by one of their nationals. Before the amendment, CMA provisions concerning the arrangements for the extra territorial application of the offences (that is, the ability for the UK courts to try cases in respect of conduct committed outside their jurisdiction) required the prosecution to show a significant link to the UK – that being that either the individual or the affected/intended affected computer needed to be present in the UK at the time of the offence.

The amendments made by SCA 2015 extended the categories of "significant link to the jurisdiction" in s.5 of the Act to include "nationality". This provides a basis for the UK to prosecute a UK national who commits any s.1 to 3A offence whilst outside the UK and where the offence has no link to the UK other than the defendant's nationality, provided that the offence was also an offence in the country where it took place - Pt 2 s.43 SCA.

One of the most significant aspects of the reform is that SCA 2015 introduced a new Section 3ZA, creating an offence which covers 'unauthorised acts causing or creating risk of serious damage' – s41 SCA. This is essentially an aggravated form of the 'impairment offence' found on Section 3 but with the added *actus reus* of causing or creating risk of serious damage of a material kind [25]. Damage to material kind covers damage to human welfare, the environment, the economy or national security. If the damage is in respect of threat of life, loss of life or damage to national security, the maximum penalty is life imprisonment [25]. Considering the detrimental effects of hacking on the economy, security, environment and general wellbeing it is understandable that the high sentencing tariffs introduced in Section 3 are necessary and potentially could have a greater deterrent effect. It was deemed that the maximum sentence of 10 years' imprisonment which s3 offence carried did not sufficiently reflect the level of personal and economic harm that a major cyberattack on critical systems could cause [26].

With regard to sentencing, it is difficult to assess whether or not the increased sentencing powers under CMA, initially through PJA 2006 and then with SCA 2015,

have or will result in higher sentences. Despite the 10 year maximum sentence available for s.3 offences since 2006 for example, these offences still appear to receive relatively low sentences often measured in months rather than years [27]. One reason for this may be that, as mentioned above, many of the more serious on-line attacks resulting in significant financial loss are prosecuted and sentenced under the Fraud Act 2006 and so do not readily lend themselves to direct comparison with offences prosecuted as computer misuse. In addition, a significant proportion of modern day computer misuse offences are committed by young people under 18 who are subject to a different sentencing regime from adults, which results in lower sentences than one might otherwise have expected considering the apparent seriousness of the offences [27].

While SCA was introduced as a reform measure to ensure that the legal framework in the UK is fit for purpose, the problems with the application of CMA discussed above still remain and must receive consideration. Following the previous trends, the wording of the new sections is not sufficiently precise and could cause interpretive difficulties. Offences that would be more suited to fall under the lesser offence could be unduly classified as aggravated. Most importantly, prosecution rates have been significantly low [16] both before and after the amendments introduced by the Serious Crime Act 2015, which begs for a different approach to be taken.

5 Conclusion

The rapid development of digital information technology and its widespread use have created opportunities for new forms of criminal activity. In the UK, it was essential that the CMA 1990 was implemented in order to criminalise computer related offences. The other offences under the existing criminal law in England and Wales were not designed to encompass cyber dependent crime. However, during the past 26 years courts have faced recurring challenges in the interpretation of the law which has led in inconsistent applications. This is partly due to the drafting of the legislation as well as insufficient understanding of the complex technical concepts involved.

CMA has been trying to catch up with technology ever since its enactment. Emerging hacking techniques and the increasing threat to economy and security prompted the government to enact amendments in 2006 and 2015. By widening the scope of the Act to incorporate the new offences involving denial of service attacks and hacking tools, interpretive issues have arisen particularly surrounding the definition of impairment and dual use articles. The reform implemented by way of Serious Crime Act 2015 does not resolve any of the existing issues. It focuses in closing the legal loophole whereby an offender could obtain a tool for his own use and adds a new aggravated Section 3 offence following the previous trend of insufficiently precise terminology that could cause interpretive issues.

It is questionable whether CMA has provided an effective measure to combating cyber dependant crime considering the low prosecution rates under the Act [7, 16].[5]

[5] During 1990–2006 when amendments were introduced by PJA 2006, only 214 defendants were brought to the magistrates' courts and 161 were found guilty. In comparison with the high occurrence of computer hacking these numbers are significantly low [7, 16].

While theoretically the chances of prosecuting hackers should have been improved following the amendments made by the Police and Justice Act 2006, in practice they have not produced the desired results. Prosecutions under both offences have been rare with very few cases being reported. Section 3A only had two prosecutions in England and Wales since 2011 [28].

This state of affairs has been partly due to a reluctance to report and/or bring proceedings under CMA. Many organisations are unwilling to prosecute their employees, preferring instead to adopt internal disciplinary procedures. Arguably, if there were prospects for restitutionary damages or compensation for loss then organisations would be more willing to prosecute [7, 16]. Most importantly, organisations fear the adverse publicity that the reporting of attacks would cause as well as publicising weaknesses that could attract further attacks [2].[6]

At the same time the enforcement of legislation is beset with difficulties of a procedural and evidentiary nature. Apprehending a remote hacker can be extremely difficult due to the anonymity that the use of internet provides and the opportunity to hide the true location of the offender. If prosecutions rates are to be improved, more expertise need be provided to the police. While the legal framework on cyber dependent crime can without a doubt contribute to the control of the misuse of information technology, it cannot successfully and effectively do so in isolation.

References

1. Office for National Statistics: Internet Access – Households and Individuals 2015 (Statistical Bulletin). https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2015-08-06#main-points
2. Symantec: Internet Security Threat Report, April 2016. https://www.symantec.com/en/uk/security-center/threat-report
3. HMSO: A Strong Britain in an Age of Uncertainty: The National Security Strategy. HMSO, London (2010)
4. Cabinet Office: The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World. Cabinet Office, London (2011)
5. Home Office: Cybercrime: a review of the evidence research report 75 (2013)
6. Walden, I.: Computer Crimes and Digital Investigations. Oxford University Press, Oxford (2016)
7. Fafinski, S.: The UK legislative position on cybercrime: a 20-year retrospective. J. Internet Law **13**, 3–13 (2009)
8. Fafinski, S.: Cyber crime. New Law J. **157** (2007)
9. Dumpbill, E.: Computer misuse act 1990 – part 1. NLJ **140**, 1117 (1990)
10. All Party Internet Group: Revision of the Computer Misuse Act: Report of an inquiry by the All Party Internet Group, June 2004. https://www.cl.cam.ac.uk/~rnc1/APIG-report-cma.pdf

[6] Symantec reports that in 2015, more and more companies chose not to reveal the full extent of the breaches they experienced. Companies choosing not to report the number of records lost increased by 85 percent [2].

11. Law Commission: 'Computer Misuse' Law Com No 186 Cm 819, HMSO (1989)
12. Explanatory Notes to the Police and Justice Act 2006
13. Wasik, M.: The emergence of computer law. In: Jewkes, Y., Yar, M. (eds.) Handbook of Internet Crime, p. 395. Routledge, Abingdon (2011)
14. CPS: Computer Misuse Act 1990 Legal Guidance. http://www.cps.gov.uk/legal/a_to_c/computer_misuse_act_1990/
15. Walton, R.: The Computer Misuse Act. 11 Information Security. Technical report 39 (2006)
16. MacEwan, N.: The Computer Misuse Act 1990: lessons from its past and predictions for its future. Crim. Law Rev. **12**, 955 (2008)
17. Fafinski, S.: Access denied: computer misuse in an era of technologic change. JCL **70**, 424 (2006)
18. Fafinski, S.: Computer misuse: the implications of the Police and Justice Act 2006. J. Crim. Law **72**(1), 53 (2008)
19. Worthy, J., Fanning, M.: Denial of service: plugging the legal loopholes? CLSR **23**, 194 (2007)
20. Fafinski, S.: Hacked off. Solicit. J. **150**, 560 (2006)
21. Sommer, P.: Criminalizing hacking tools. Digit. Invest. **3**, 68–72 (2006)
22. Katos, V., Furnell, S.: The security and privacy impact of criminalising the distribution of hacking tools. Comput. Fraud Secur. **2008**, 9–16 (2008)
23. Rahman, R.: The legal measure against DoS attacks adopted by the UK legislature: should Malaysia follow suit? Int. J. Law Inf. Technol. **20**, 85–101 (2012)
24. Council Directive (EC) 2013/40/EU of 12 August on attacks against information systems, replacing Council Framework Decision 2005/222/JHA [2013] OJ L218/8
25. Explanatory notes to the Serious Crime Act 2015. http://www.legislation.gov.uk/ukpga/2015/9/notes/contents
26. Home Office: Serious Crime Act 2015 - Fact sheet: Part 2: Computer misuse. https://www.gov.uk/government/publications/serious-crime-bill-computer-misuse. Accessed 04 Aug 2016
27. Zoest, J.: Computer Misuse Offences. Sweet & Maxwell, Insight, 5 May 2015
28. Home Office: Serious Crime Bill: Amendments to Computer Misuse Act 1990 Impact assessment (2014). https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317527/2014-06-03_signed_IA_CMA_EU_Directive.pdf