techUK

CyberUP

Time for reform?

Understanding the UK cyber security industry's views of the Computer Misuse Act

November 2020

Contents

1.	Foreword	3
2.	Introduction to the Computer Misuse Act	5
3.	Summary and Analysis of survey	9
4.	Amendment and legal analysis	20
5.	Conclusions and recommendations	28

1

Foreword

Ruth Edwards MP

As a former cyber security professional myself, I am delighted to be able to present this important report in conjunction with the CyberUp Campaign and techUK.

The Computer Misuse Act went on the statute book in 1990 – when 0.5 per cent of the UK's population used the internet regularly. I know from my time in this industry that there are now real concerns among the cyber security community that this law is impeding professionals' ability to protect the nation from the ever-evolving range of cyber threats we face, and preventing the sector from establishing its leadership position on the international stage.

The two main strands to this report therefore fill an important gap in the cyber security policy landscape. First, this survey is the first assessment of its kind into the views of those on the frontline navigating the current legal framework. The results of this survey render a definitive verdict that the current regime is in significant need of an update. Across the survey, 93 per cent of respondents didn't believe the Computer Misuse Act was a piece of legislation fit for this century.

Second, the report builds on survey respondents' feedback and provides suggested amendments to the Act – based on considered analysis from legal academics and practising lawyers – seeking to address those faults. These proposed changes provide a solid foundation from which to design a piece of legislation that equips cyber security professionals with legal certainty while ensuring malicious actors can still be prosecuted and punished appropriately.

The Computer Misuse Act needs urgent attention from policy makers. If ever there was going to be a time to prioritise the rapid modernisation of our cyber legislation, it is now, when our reliance on safe, reliable and resilient digital technologies has been brought into stark relief by the coronavirus pandemic.

This provides an opportunity to step back and ensure that we are doing all we can to promote the security of the digital spaces in which more of our lives now take place.

Between the Integrated Review of Security, Defence, Development and Foreign Policy and the forthcoming next iteration of the National Cyber Security Strategy, there is a body of work taking place across government at the moment to assess the effectiveness of existing policies and processes and what ought to be prioritised in the post-pandemic world. We also see a growing recognition in recent legislation that, in the pursuit of doing the right thing, there are circumstances in which otherwise criminal offences ought to be defensible. The Law Commission's recent review of the Official Secrets Act proposes the introduction of a public interest defence for unauthorised disclosure, and the Covert Human Intelligence Sources Bill provides the legal basis to authorise the criminal conduct of members of the security services where their actions serve the national and economic security of the United Kingdom, such as preventing a cyber attack on critical national infrastructure.

"We have a duty to ensure that those trying to defend and protect us are able to do so unencumbered from the burden of outdated legislation"

As we accept that the threats facing our country and its citizens are continuously evolving, we have a duty to ensure that those trying to defend and protect us are able to do so unencumbered from the burden of outdated legislation.

With that in mind, now is the time to be ensuring that the legal framework for UK cyber security professionals is fit for the modern age, allowing them to defend our digital infrastructure from threat actors and foster a flourishing cyber sector on these shores and beyond.

Ruth Edwards MP

2 Introduction

About the report

This report has been produced by the CyberUp Campaign in conjunction with techUK to offer additional evidence underpinning the case for reform of the Computer Misuse Act 1990.

The CyberUp Campaign brings together a coalition of groups from the cyber security industry, and techUK is the main trade body representing the interests of the UK technology sector. This collaboration is born out of the desire by both organisations to see a legal environment in the UK that will be conducive to a thriving and internationally competitive cyber security sector, as well as one that is best able to assist UK law enforcement and the intelligence services in their work defending the UK's critical national infrastructure and public services from an ever-evolving array of cyber threats.

The production of this report has involved two evidence gathering processes which correspond to the its two main chapters:

1. A survey of representatives of the cyber security industry, asking a series of qualitative and multiple choice questions to better understand the way that cyber security professionals interact with the Computer Misuse Act in their daily work, and to assess the way that institutions and organisations as a whole navigate the legal environment created by the Computer Misuse Act.
2. Feedback and analysis on specific proposals for reform of the Computer Misuse Act from a collection of legal academics and practising lawyers and barristers who the CyberUp Campaign approached for their evaluation and insights.

Summary and analysis in these two sections is followed by a concluding discussion and a series of recommendations for Government on how best to ensure the UK cyber security legal regime is fit for the 21st century.

This report will recommend that:

1. **The Government launch a review of the Computer Misuse Act as soon as possible**

2. **The Government consult widely to design future-proof legislation that offers legal certainty to cyber security professionals acting in good faith.**

History

In 1984, Robert Schifreen and Stephen Gold used home computers and modems to gain unauthorised access to a BT dataset, after they "shoulder surfed" to observe an engineer's password. The pair explored the dataset, eventually gaining access to Prince Phillip's personal message box.

They were initially convicted under the Forgery and Counterfeiting Act 1981, but appealed and were acquitted – an acquittal that was eventually upheld by the Law Lords, with Lord Chief Justice Brandon saying whether or not to criminalise this behaviour was a "matter for the legislature". The Law Commission subsequently came to the conclusion that new legislation was needed.

In response, an initial Private Member's Bill was introduced to Parliament by Emma Nicholson MP (now Baroness Nicholson); eventually, in 1990, a Private Member's Bill was brought forward by the late Michael Colvin MP, section 1 of which sought to address the central issue of *R v Gold & Schifreen* by criminalising unauthorised access to computer material.

Background to contemporary calls for reform

As mentioned, section 1 of the Computer Misuse Act criminalises unauthorised access to computer material.

Section 1, together with Section 17 of the Act, make it an offence for anyone who is not entitled to do so, or does not have the right consent, to "cause a computer to perform any function with intent to secure access to any programme or data held".

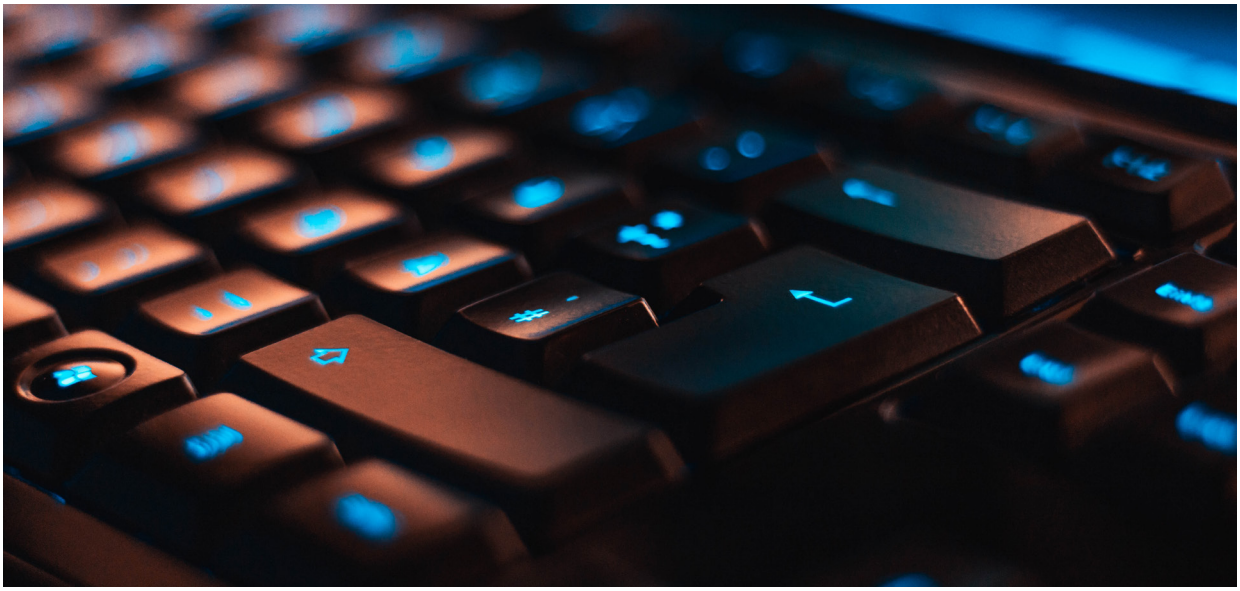
In brief, without permission, anyone altering or erasing data, copying or moving it, using it, or even displaying output from a computer, is acting illegally.

The argument for reform is that this aspect of the legislation – passed in 1990 when 0.5 per cent of the UK population were on the internet – did not foresee the expansion of the internet and the advent of modern cyber security practices, which includes techniques like vulnerability and threat intelligence research.

The Computer Misuse Act was created to criminalise unauthorised access or illegal hacking. It entered into force before the cyber security industry, as we know it today, developed in the UK. The methods used by cyber criminals and cyber security professionals are often identical; the main differentiator being that the former lack authorisation where the latter usually have it. Yet, as cyber criminals' actions evolve, so do those of cyber security experts, regularly requiring actions for which explicit authorisation is difficult, if not impossible, to obtain.

"Without any regard for individuals' motivations, the outdated Computer Misuse Act creates the perverse situation where cyber security professionals, acting in the public interest to prevent and detect cyber threats, risk being criminalised by a law created to punish cyber criminals."

As a result, the Computer Misuse Act now criminalises at least some of the cyber vulnerability and threat intelligence research and investigation by UK based cyber security professionals in the private and academic sectors, essentially creating the perverse situation where cyber security professionals, acting in the public interest to prevent and detect crime, are held back by the legislation which should at the very least not be standing in their way.



Modern vulnerability and threat intelligence research, more generally described as defensive cyber activities, often involve the scanning and interrogation of compromised victims' and criminals' systems to lessen the impact of attacks and prevent future incidents. In these cases, criminals are obviously very unlikely explicitly to authorise such access; to do so would be akin to asking a thief for permission to try to thwart their criminal scheme. Cyber security professionals can therefore find themselves in the position of not being able to follow through on investigations which may ultimately yield actionable intelligence that could have meaningfully prevented harm or expense.

Chapter 3 of this report – by providing a summary and analysis of a survey of the cyber security industry – seeks more precisely to assess the extent to which the Computer Misuse Act constrains cyber security professionals. It also makes determinations about the real world impact of these constraints on businesses in the UK cyber security sector and their international competitiveness, as well as for the UK's efforts to defend against a myriad of cyber threats.

The objection to the Computer Misuse Act in its current form is that the law punishes behaviour without any regard for the motivation of those carrying it out. The argument is that it lacks any mechanism for accounting for cyber security and threat intelligence researchers acting in good faith, or for other legitimate, or defensible reasons.

As part of the evidence gathering process for Chapter 4, we worked with the Criminal Law Reform Now Network (CLRNN) , who earlier in 2020 published their own proposals for reform of the Computer Misuse Act, to draw up specific amendments targeted at addressing the motivation issue highlighted here, and aimed at creating a legal regime that allows for more certainty amongst cyber security professionals and organisations alike.

3 Survey – Summary and Analysis

The following results are based on a 31-question survey that ran from 29 September until 14 October 2020. The survey was circulated via the CyberUp Campaign and techUK newsletters, mailing lists and social media channels. It was also distributed to their membership by the APPG on Cyber Security and we are grateful for their assistance.

Profile of respondents

There were a total of 46 respondents to the survey. Of those who responded representing organisations (11), the total number of employees their organisation represented was 25,120. This is more than half of the approximately 43,000 Full Time Equivalents (FTEs) working in a cyber security related role across the cyber security firms identified by the UK Government's most recent analysis of the cyber security sector.[1]

The survey comprised two sets of questions: one for individual cyber security researchers to give testimony based on their personal experience, and one for those responding on behalf of organisations.

Two-thirds of respondent researchers worked for cyber firms

Of those that responded as individuals to the survey, a significant majority of more than two thirds worked at a cyber security consultancy. Other respondents included in-house IT and cyber security engineers, as well as specialist cyber researchers at universities.

The size of the businesses that respondents work for vary, between small start-ups of less than 5 people to large multinationals of around 500,000 people worldwide, but the majority of respondents work for companies that employ between 2000-5000 people.

Businesses that responded had between 5 and 2,000 customers

There were 11 respondents who answered on behalf of organisations. These respondents hold leadership positions as Managers, Directors, CEOs and Owners of a range of cyber security consultancies which vary in size. The size of the organisations that these respondents were answering on behalf of represented a similar cross section as the employees who were responding individually, and the number of clients they had ranged from five to up to 2,000. The companies were headquartered around the UK, including in London, Surrey, Reading, York and Manchester. Two company headquarters are abroad, in Canada and the US West Coast.

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/861945/UK_Cyber_Sectoral_Analysis__2020__Report.pdf

An outdated law which is not fit for the 21st century

As outlined in Chapter 2, the Computer Misuse Act became law in 1990 – more than 30 years ago, before wider uptake of the internet and other modern communications technologies amongst the UK (and global) population. One argument that proponents of reform – including the CyberUp Campaign – make is that the passage of time and advances in technology have rendered the law out of date and ill-fitting for a world in which vulnerability and threat intelligence research exists as one of the main tools in the fight against cyber crime.

It was therefore striking that on this question, those who must navigate the boundaries of this 30-year old law offered such a clear verdict. Of those responding in an individual capacity, more than 9 in 10 (91 per cent) said they did not believe that the Computer Misuse Act represented a world leading example of 21st century cyber crime legislation. Even more emphatic was the judgment rendered by those responding on behalf of businesses, who unanimously also do not believe that the Computer Misuse Act 1990 represents a world leading example of 21st century cyber crime legislation.

It is clear that those working in the cyber security sector believe that the UK's legal framework does not represent an up to date and functioning piece of legislation. One might question what those responding are using as a basis when considering an ideal regime. Researchers and managers are likely to know and be aware of colleagues and competitors that operate in different jurisdictions under different sets of rules, and are likely to comment on the UK regime with those as points of reference.

Understanding of the current legal regime is varied and views on what is legal divergent

As has been outlined, one of the key arguments made by proponents of reform is that the Computer Misuse Act acts as a barrier to their work. Beyond that though, proponents also make the case that the uncertainty itself has a negative impact, with researchers who are unsure if they are breaking the law often opting not to take the risk because they cannot be sure of the repercussions of their activities. On this basis, the survey asked a series of questions to try to assess the level of understanding around the Computer Misuse Act – and what exactly constitutes a breach of the law – within the industry.

The survey asked respondents if they believe they or their colleagues have a firm understanding of what is legal and illegal behaviour according to the Computer Misuse Act 1990. The responses to this question were mixed, indicating that there is ambiguity within the community of cyber security professionals about what activities are against the law: 19 respondents (59 per cent) stated they believe they do have a firm understanding of what is legal and illegal under the Computer Misuse Act, whereas 6 (19 per cent) stated they do not, and 7 (22 per cent) were unsure.

When asked to give examples of what constitutes a clear breach of the Computer Misuse Act, there was a set of common answers given, which included:

- Trying to get into a system
- Attempting to gain access to something unauthorised
- Intent in actions
- Hacking
- Acting without permission

These answers themselves involve some confusion, with respondents who argued that malicious intent in one's actions constitutes a clear breach having revealed they have a misunderstanding of the Act. However, the majority of respondents largely conveyed that they understood what was a clear-cut breach of the Act.

However, the survey also put a series of scenarios and behaviours that cyber security professionals carry out routinely in the course of their day-to-day work, and asked whether any of these constituted a breach of the Computer Misuse Act.

These activities included:

- Web scraping – facilitating analysis and discovery of various types of malicious activity
- Port scanning – for the discovery of malicious infrastructure as well identifying possible susceptible hosts
- Other open source internet scanning activities – use of search engines to identify open source information
- Honeypot investigations – systems intended to be hacked by malicious threat actors to observe their activities and collect intelligence
- Malware detonation – to understand how malware behaves, where it connects to (its C2 infrastructure) and what it is instructed to do by its operators
- C2 interaction – for purposes of identification and also potentially extraction of information about victims and/or its operators to facilitate understanding
- Vulnerability research on products with no published vulnerability disclosure policy – to identify weaknesses in order to proactively report them
- The use of default credentials in login panels exposed to the public internet – to identify victims of a particular malware campaign

The answers to these questions indicate there is confusion about what, in fact, counts as a criminal offence under the Computer Misuse Act. The only three activities where there was a reasonable level of consensus were:

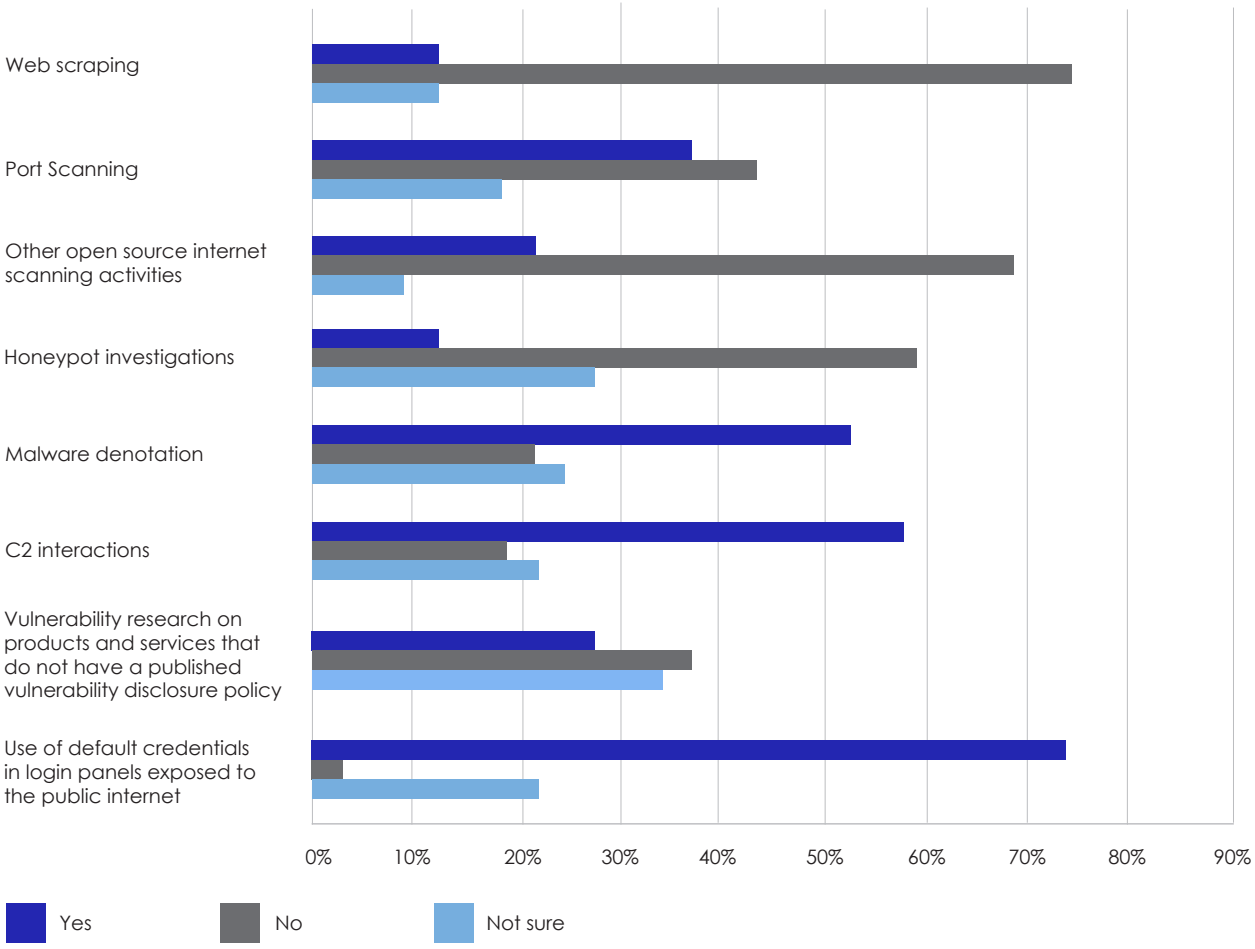
- Web scraping - 74 per cent believe it is not a breach
- Open source internet scanning activities - 68 per cent believe it is not a breach
- Use of default credentials in login panels exposed to the public internet - 74 per cent believe it is a breach

"The findings present a damning picture of the functioning of the legal regime that governs cyber crime in the UK - 80 per cent of respondents worry about breaking the law when researching vulnerabilities or investigating cyber threat actors"

Otherwise, some activities were split largely evenly between those who thought it was a breach and those who thought it wasn't, including:

- Port scanning activities - 38 per cent a breach versus 44 per cent not a breach
- Vulnerability research absent a disclosure policy - 28 per cent a breach versus 38 per cent not a breach

Do you believe that this activity constitutes a breach of the Computer Misuse Act?



Perhaps most tellingly, nearly all activities received around 25 per cent or more of responses indicating they did not know if it constituted a breach, with 6 per cent of respondents answering 'not sure' for every question.

These findings present a damning picture of the state of the understanding of the Computer Misuse Act and the functioning of the legal regime that governs cybercrime in the UK. It's clear that while researchers will say that they feel they understand the perimeters of legal conduct, upon closer examination those lines are very blurred and there are considerable misconceptions. That there is such widespread disagreement among cyber security researchers about what constitutes a breach of the Act is worrying in itself.

But the crucially important question that follows must be, to what extent this level of misunderstanding has affected cyber security researchers in the course of their work. The survey results here indicate that the predicted stifling effect may be taking place, with 81 per cent of researchers having discussed the Computer Misuse Act with their colleagues, and 80 per cent of respondents having worried about breaking the law when researching vulnerabilities or investigating cyber threat actors.

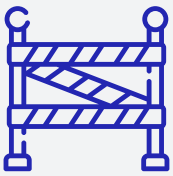
The impact on national security and the wider national response to organised crime

One consequence of the Computer Misuse Act's ambiguity and restrictiveness is its effect on the UK's national security, and domestic capabilities to safeguard against adversarial cyber threat actors both state and criminal in nature.

The cyber security industry works closely and in concert with law enforcement and intelligence agencies to defend the UK against cyber crime and geo-political threat actors. This is a settled public-private partnership that helps keep the UK – its citizens and its institutions – and its international partners safe from harm. But if it is the case that current legal restrictions are holding back cyber security researchers from carrying out certain activities, impeding their ability to supply rich threat intelligence to support national cyber defence operations and law enforcement, then it is possible that the Computer Misuse Act is having a detrimental impact on the UK's national security.

This detrimental impact is because the restrictions in gathering high quality actionable intelligence or proactively identify certain vulnerabilities make it challenging to stay ahead of hostile threat actors and cyber criminals as governments alone cannot reasonably provide the required capacity and capabilities given the scale of the challenge.

This survey sought evidence to make an assessment of this hypothesis. Its findings confirmed that the restrictions are having an impact, with 58 per cent of researchers revealing that the Computer Misuse Act has acted as a barrier to them or their colleagues conducting cyber security or threat intelligence research. Separate answers also suggested that 23 per cent of researchers indicated that they believed the Computer Misuse Act had indeed inhibited them from preventing harm to businesses or citizens, whereas a smaller percentage (10 per cent) believed that the Act had inhibited them from preventing a threat to national security.



58%

of researchers revealed the Computer Misuse Act has acted as a barrier to them or their colleagues

40%

of businesses indicated the Computer Misuse Act had inhibited employees of their organisation from preventing harm

The figures were higher for those responding on behalf of organisations, with 40 per cent indicating the Computer Misuse Act had inhibited employees of their organisation from preventing harm to businesses or citizens, and 20 per cent that the Act had inhibited employees of their organisation from preventing a threat to national security.

The clear majority of researchers who indicated the Act had prevented them from carrying out activities indicates there is support for the claim that the Computer Misuse Act is having a constraining effect.

While there was, perhaps, less support for the claims that these constraints had led to them being unable to prevent harm and threats to national security, there were still significant numbers who believed this had been the case. It is interesting that the proportions increase for those responding on behalf of organisations. It is worth considering whether those in managerial positions are likely to have a better sense of the wider impact of the work of their organisations, because they are perhaps more likely to be involved with coordinating cyber security consultancies' engagement with law enforcement and intelligence agencies.

The effect on growth and investment in relation to the UK cyber security sector

Another area where the constraints posed by the Computer Misuse Act could be having an impact is on the prosperity of the UK cyber security sector. Proponents of reform claim that the UK cyber sector is currently held back by the competitive advantage of companies headquartered in jurisdictions that offer more permissive legislative regimes, such as France, the US and Israel (and who may not have the same relationship/obligations to the UK Government). The argument is that the rich supply of threat intelligence gathered by those companies headquartered abroad floods the UK market and puts UK businesses at a disadvantage.

This argument is particularly noteworthy given how much the UK Government already spends on trying to foster a constructive business environment for technology companies broadly and cyber security companies specifically. Just one example from earlier in 2020 was when nine firms were revealed as the latest recipients as part of Department of Digital, Culture, Media and Sport and the UK Research and Innovation's Digital Security by Design programme, securing £10 million of investment between them. The programme's stated aim is to help the tech infrastructure of UK organisations and digital devices be more resilient to cyber attacks. Reforming the Computer Misuse Act, by contrast, would cost the Exchequer nothing (aside from the administrative costs of designing, passing and implementing the change).

The CyberUp Campaign has, in a previous piece of work, estimated that reform of the Computer Misuse Act would unlock growth in the UK cyber industry, thereby leading to an additional 4,000 high-skilled jobs and increasing the sector's worth to around £500 million by 2023.

Again, this survey sought to make an assessment of the extent to which there is evidence for these arguments based on how those who work in the cyber security industry feel the Computer Misuse Act affects their business. It is worth also making the point that it is on questions about business development where this survey is likely to have most value in assessing the views of industry, given that businesses are likely to be in the best place to have a firm understanding of how legal restrictions are affecting their bottom lines.

As stated before, 58 per cent of researchers believe the Computer Misuse Act has acted as a barrier to them or their colleagues conducting cyber security or threat intelligence research. This corresponds with responses to a similar question put to those responding on behalf of organisations, where 67 per cent believed the Computer Misuse Act had been a barrier for cyber research and innovation activities they had been planning to undertake in the UK.

UK consultancies believe they are at a disadvantage because of the Computer Misuse Act

91%

of businesses believed that the Computer Misuse Act puts UK consultancies at a competitive disadvantage with other countries

The ramifications of these constraints were also made plain: 91 per cent of respondents believed that the Computer Misuse Act puts UK-based cyber security consultancies at a competitive disadvantage relative to other countries. When asked, respondents broadly claimed they were unable to quantify the scale of any loss to their business, but several indicated that the Computer Misuse Act meant they just left certain workstreams and projects to international competitors. 45 per cent of respondents were aware of reports written by overseas competitors that would clearly have been impossible to write in the UK, and 27 per cent were sure they had lost contracts to other companies based abroad, while only 27 per cent could say for sure that they hadn't.

Most emphatically, 90 per cent believed that if the UK moved closer to what their ideal, world leading 21st century cyber security and cyber regime would be, then their organisation would experience significant productivity improvements, growth and resilience benefits.

Additionally, there were strong majorities for the proposition that such a move would lead to an increase in annual revenue (75 per cent), the number of clients (63 per cent) and the number of employees (88 per cent).

There were strong majorities for the proposition that such a move would lead to an increase in

75%

annual revenue

63%

clients

88%

employees

The same question also asked respondents to put a specific value, in percentage terms, of the amount a change would increase the revenue and number of employees of their organisation. On the question of an increase in revenue, of those that responded, 33.33 per cent suggested that they would see an increase of 1-10 per cent, 16.67 per cent suggested they would see an increase of 10-20 per cent, and 50 per cent suggested they would see an increase of 20+ per cent. Averaging these[2], the expected revenue increase would be nearly 20 per cent across the entire sector. Multiplying this by the most recent estimation of the total revenue of the cyber sector in the UK of £8.3bn, gives an increased revenue of £1.6bn for the sector from a change in legislation.

A similar calculation for responses about increases in numbers of employees found an average increase in percentage terms of nearly 15 per cent. When multiplied by the existing work force of the sector, this leads to an increase of about 6,200 jobs resulting from a change in legislation.

6,200 jobs

created from reforming the Computer Misuse Act, and a £1.6bn increase in cyber security sector revenue

[2] Taking the midpoint for each option and also 30 per cent as reasonable assumption for the 20+ per cent bracket. Not including don't knows.

These results bring into focus that there is clearly a feeling within in the cyber security industry that the UK is being held back by the current legal framework. The people who are responsible for taking strategic decisions about the revenues of their businesses believe decidedly that an up to date legal regime would be beneficial for them. In a climate where the UK Government's stated ambition is to support the country's burgeoning tech sector, and to become the world's leading research and science superpower, it would seem these findings represent a strong addition to the case for reform.

Designing a framework fit for the 21st Century

The survey also sought qualitative views on what features respondents believed an ideal world leading 21st century cyber security and cyber crime regime would contain. There were three themes that ran through the answers.

"At the moment, innovation is stifled by a lack of clarity over what is and is not acceptable in the UK."

First, the need for more clarity for researchers and managers over what constitutes a breach of the Act: One respondent put the argument succinctly when they said, "*At the moment, innovation is stifled by a lack of clarity over what is and is not acceptable in the UK.*" The word 'clear' came up in several other responses.

Second, the need to have a system that is able to account for an actor's good faith / good intentions / motivations: the word 'intent' featured in several of the answers; one respondent commented that a better legal regime would have "*the ability to protect researchers who are trying to protect their [/their clients] systems' from compromised ones attacking them.*"

And third, the need for an open and permissive system that enabled researchers and businesses to do more than they are currently able to do. One respondent claimed that what they were looking for was, simply, the freedom to carry out their research activities and defensive investigations free from the '*fear of litigation.*'

These themes are taken up in more detail in Chapter 4 as part of the feedback from lawyers on specific proposals for reform, but the views of the cyber security businesses are clear and should be taken into account when designing a new legal framework – whether via an amendment to the Computer Misuse Act or otherwise.

4 Amendments and legal analysis

A second body of work that went into the production of this report involved producing and assessing a set of concrete proposals for reform of the Computer Misuse Act that would enable the creation of legal framework that has the features that those surveyed within industry describe as likely to enable them to grow their businesses and better protect UK citizens and institutions from harm: clarity, and legal certainty, and the ability to take account of actors' motivations when assessing their behaviours and activities.

We worked with the Criminal Law Reform Now Network (CLRNN), who earlier in 2020 published their own proposals for reform of the Computer Misuse Act, to draw up specific amendments. We then approached a collection of legal academics and practising barristers for feedback on these proposals. The results are the draft amendments suggested here, with some analysis and commentary of why their implementation would represent a piece of legislation that addresses the deficiencies in the current system.

"Concrete proposals for reform seek to create a legal framework that offers clarity, legal certainty and the ability to take account of actors' motivations, enabling UK cyber security professionals to better protect UK citizens and institutions from harm"

The central flaws of the current Act are twofold:

1. As outlined repeatedly, the Computer Misuse Act in its current form does not allow for an actor's motivation to be taken into account: the law punishes behaviour without any regard for the motivation of those carrying it out, and therefore offers no protection for cyber security and threat intelligence researchers acting in good faith, or for other legitimate, or defensible reasons.
2. As demonstrated previously, the Computer Misuse Act creates significant legal ambiguity: the current parameters of what is and is not legal under the Act are unclear. This arises out of its authors' failure to foresee the rise of the internet and the advent of modern cyber security practices. The result is a regime in which the lack of clarity itself has a stifling effect on security researchers.

Accordingly, the amendments suggested here have two primary aims:

i. Create clear legal definitions to ensure that cyber security researchers based in the UK who reasonably believe they have authorisation to act can legitimately do so;

ii. Introduce statutory defences to allow cyber security researchers to justify their actions under specific circumstances.

The proposed changes to the legislation are set out in **blue** below.

I. Definition of what constitutes unauthorised access: inserting new subsections to 17(5)

17 Interpretation

{…}

(5) Access of any kind by any person to any program or data held in a computer is unauthorised if—

a. he is not himself entitled to control access of the kind in question to the program or data; and

b. he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled;

c. he does not reasonably believe that the person entitled to control access of the kind in question to the program or data would have consented to that access if he had known about the access and the circumstances of it, including the reasons for seeking it;

d. he is not empowered by an enactment, by a rule of law, or by the order of a court of tribunal to access the kind question to the program or data.

Guidance and commentary

This proposed amendment seeks to address the fact that the boundaries of authorisation as per the provisions of the Computer Misuse Act have always been difficult to predict or control. It seeks to directly address some of the problems revealed in the previous chapter by the questions about what constitutes a breach of the act, and the lack of consensus on those points, as well as qualitative comments about the need for a future system to offer more clarity.

The qualifications proposed here are available elsewhere in the law. Their explicit inclusion in an amended Computer Misuse Act 1990 would permit cyber security and threat intelligence professionals to rely on their professional experience when deciding their course of action.

In addition to attempting to clarify for cyber security and threat intelligence professionals what constitutes a breach, it also begins to deal with the issue of good faith and intent. The inclusion of the concept of including reasons for seeking consent, as this would afford cyber security professionals' actions in good faith.

To disqualify any attempts at their inappropriate use, and to address concerns raised as to how subjectively these qualifications might be applied, their inclusion is further qualified by a requirement of reasonable belief i.e. they will be subject to a reasonableness test. This could be further supported via an agreed industry standard of documentation, to develop common principles for cyber security professionals' approach to establishing reasonable belief prior to undertaking cyber defensive and investigative activities.

At present, the reasonableness test is set out under Section 11 (1) of the Unfair Contract Terms Act (UCTA) 1977, asking whether it is "fair and reasonable to be included, having regard to the circumstances which were, ought reasonably to have been, known to or in contemplation of the parties when the contract was made".

Crown Prosecution Service (CPS) guidance regarding the issue of consent in relation to the Sexual Offences Act 2003 describes the test of reasonable belief as a "subjective test with an objective element", containing two questions:

1. (subjective element) Did the defendant believe the complainant consented? (in relation to the defendant's personal capacity to evaluate consent)
2. (objective element) If so, did the defendant reasonably believe it? (the jury will decide if the defendant's belief was reasonable)

Considerations for policy-makers

Further discussion is required as to how any abstract concept would be applied in practice, and whether a requirement of reasonable belief will sufficiently cover cyber security professionals unless, or until, a body of jurisprudence has been accumulated to establish how courts will seek to prove reasonable belief in a third party's potential consent.

However, the reasonableness test is a well-established principle of the law, and forms a useful starting point for reforms aimed at tackling the shortcomings of the Computer Misuse Act as it currently exists.

II. Introduction of statutory defences

Section 18 Defences

(1) It will be a defence for a person charged with an offence under sections 1 and 3 to prove that in the particular circumstances unauthorised access to computer material, or any unauthorised act in relation to a computer with intent to impair, or with recklessness as to impairing, operation of computer –

a. Was necessary for the detection of crime;

b. Was proportionate to the harm caused by the crime in question.

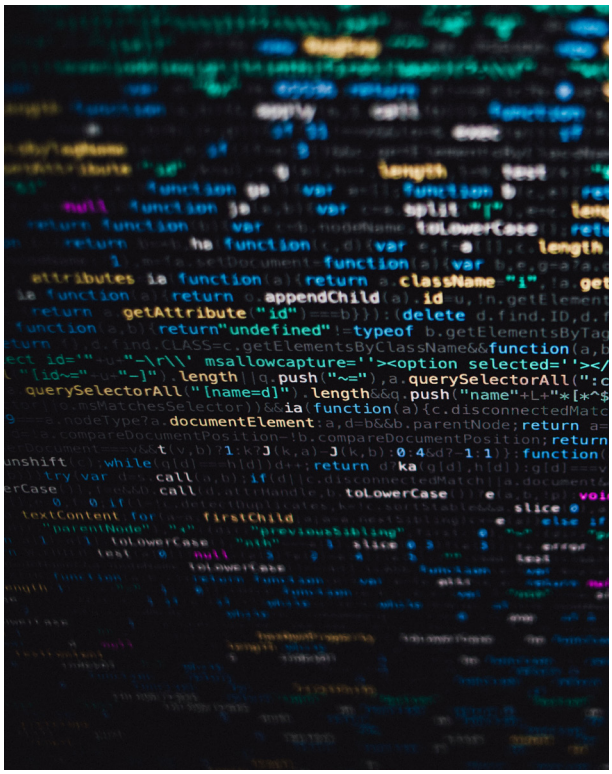
Guidance and commentary

The above amendment details the statutory defences that are being proposed to be inserted into the Act. They seek to make clear the circumstances under which a cyber security or threat intelligence researcher may be protected from prosecution. They chiefly attempt to address the issue that the Act, as it is currently written, does not account for the motivations of these groups, one of the key issues raised by respondents to the survey asked to describe their ideal system. The following sections provide further background and discussion for why this amendment has been proposed.

Importance of statutory defences

The CLRNN report[3] on reforming the Computer Misuse Act provides detailed arguments for the inclusion of a statutory defence. Additionally, the inclusion of a statutory defence in the Computer Misuse Act 1990 would bring this area of the law into line with comparative issue spaces and jurisdictions:

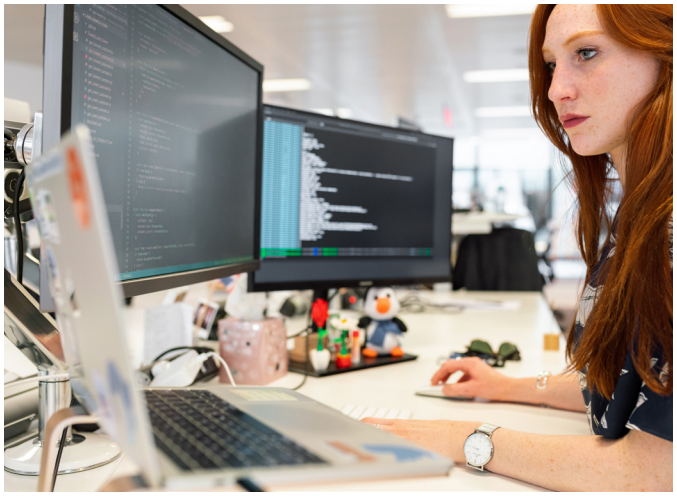
- As per Article 6(2) of the Cybercrime Convention and Recital 16 to Directive 2013/40/EU, a statutory defence would mean that UK law finally reflects international best practice of the kind we see across Europe;
- As outlined in the Law Commission's report on the Official Secrets Act[4], the UK Government has recently recognised the importance of protections in the Digital Economy Act 2017 (sections 42(4); 51(4); 59(4); 67(9); 68(9); and 69(9))[5] and the Data Protection Act 2018 (sections 170(2,3); 171(3,4,6,7) and 173(5))[6], thereby highlighting the absence of statutory defences in many other (disclosure) offences.
- The proposed Covert Human Intelligence Sources Bill stipulates that criminal conduct authorisations can be granted in the interests of national security, for the purposes of preventing or detecting crime, and in the interests of the economic wellbeing of the UK, including the possibility of a hostile cyber attack against UK critical national infrastructure, financial institutions, or government, where conduct is part of efforts to prevent more serious criminality, and no other practicable means are available to achieve the same outcome.



[3] http://www.clrnn.co.uk/media/1018/clrnn-cma-report.pdf
[4] https://www.lawcom.gov.uk/reform-of-the-criminal-law-needed-to-protect-victims-from-online-abuse-says-law-commission/
[5] https://www.legislation.gov.uk/ukpga/2017/30/pdfs/ukpga_20170030_en.pdf
[6] https://www.legislation.gov.uk/ukpga/2018/12/part/6/crossheading/offences-relating-to-personal-data/enacted

Extent of statutory defences

While there is debate regarding the extent of a new statutory defence, there is agreement that balance needs to be struck between enabling cyber security and threat intelligence professionals and ethical hackers to work lawfully, and avoiding the unintended consequence of affording a defence to malicious individuals.



A blanket public interest defence is seen by some as too broad and nebulous to provide sufficient protection from bad actors, as well as encouraging vigilantism, taking account of the role of the appropriate authorities, with appropriate checks and balances in place.

The Law Commission, in recommending the introduction of a statutory public interest defence in the Official Secrets Act in relation to unauthorised disclosures also finds that:

- The legal burden on proving the defence should rest on the defendant;
- The court needs to find that the act in question was, in fact, in the public interest, considering whether (1) the subject matter of disclosure was in the public interest and (2) the manner of disclosure was in the public interest.
- Defining factors to determine public interest is a political matter for Government and Parliament.

Eligibility of statutory defences

There are comments that further clarification would be required of what activities would be covered by any statutory defence; this, it is argued, can be established either in time, through case law, or through additional guidance. Some considerations include:

- Existing discussion and commentary:
  Previous reports[1] suggest a list of factors that indicate defensible conduct, including: a motive to prevent crime, or to reveal security flaws and methods known by the offender to be unlikely to endanger the integrity of the system; or a motive to obtain information in the course of responsible cyber threat intelligence collection.

- The US framework:
  In the context of the US Digital Millennium Copyright Act (DMCA), the concept of "good faith security research" is explained as "accessing a computer program solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability, where such activity is carried out in an environment designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices or machines on which the computer program operates, or those who use such devices or machines, and is not used or maintained in a manner that facilitates copyright infringement."[7]

  The proposed US Active Cyber Defence Certainty Act (ACDCA)[8] (despite concerns regarding its intentions) proposes a general defence for active cyber defence measures that are defined as: the unauthorised access to an attacker's computer where that is aimed at establishing contribution and passing it on to authorities, monitoring attackers' behaviour to help develop future defences, and disrupting criminal activity, but specifically excludes conduct that destroys, or renders inoperable information, causes reckless injury or creates a public threat. This proposed legislation includes a notification requirement by which any defenders using ACD measures must notify FBI authorities and receive acknowledgement of notification, including: type of cyber breach, intended target, steps to preserve evidence, and steps to prevent damage.

- A licensing scheme:
  There are suggestions of using secondary legislation to create a licensing scheme for cyber security and threat intelligence professionals to whom any defences would apply, and list any obligations as part of this. This is in line with previously raised ideas of cyber security and threat intelligence professionals signing up to a binding code of ethics, committing to sharing any information gained with public authorities, and keeping auditable logs to have their activities reviewed on a regular basis, or as and when required.

[7] https://www.federalregister.gov/documents/2018/10/26/2018-23241/exemption-to-prohibition-on-circumvention-of-copyright-protection-systems-for-access-control
[8] https://www.congress.gov/bill/116th-congress/house-bill/3270?s=1&r=1

There is already work going on by government-funded institutions to this end that would not necessarily need to be replicated. The UK Cyber Security Council has drafted a widely applicable code of ethics for the cyber security profession and is currently consulting on the document. These could be tied to a reformed Computer Misuse Act regime that links defences to a commitment by approved industry professionals to act in good faith.

- Eligibility of actors rather than actions:
  An alternative view of eligibility would focus on the actor rather than the action. It is possible to consider fraud prevention clauses contained in the Serious Crime Act 2007 and the Data Protection Act 2018 as the basis for drafting defences for cyber security professionals. Section 68 of the Serious Crime Act 2007 defines as anti-fraud organisation any unincorporated association, body corporate or other person which enables or facilitates any sharing of information to prevent fraud or a particular kind of fraud or which has any of these functions as its purpose or one of its purposes. It is possible to argue that cyber security firms should be presumed to be, or formally be classified as anti-fraud organisations.

Considerations for policy-makers

Again, more discussion of these issues is required as to how a defence like the one proposed would operate in practice. However, the proposal draws on well-established legal principles and provides a solid starting point for any draft legislation.

5 Conclusions and Recommendations

The survey of representatives of the cyber security industry – the results of which are presented in Chapter 3 – is important in that it is the first piece of work to get the views of those who are tasked with navigating the boundaries of the Computer Misuse Act as to its effectiveness.

The survey's findings emphatically demonstrate that there is appetite for reform. 93 per cent of respondents do not believe the Computer Misuse Act is a law fit for this century. Further, detailed analysis reveals there is widespread confusion about what types of activities and behaviours do and do not constitute a criminal offence under the Act. The impact that this confusion – and the restrictions themselves – have on the ability of researchers to prevent harm and threats to national security are still significant. There is strong evidence that a move towards a better, more permissive system would be of economic benefit. All told, these findings add meaningfully to the weight of evidence pointing towards reform of the Computer Misuse Act. The first recommendation of this report is therefore as follows:

1. **The Government should launch a review of the Computer Misuse Act as soon as possible.**

Respondents to the survey were also clear about what type of legal framework they would like to see established in place of the current Computer Misuse Act. The future legal regime ought to offer clarity, so cyber security professionals can be certain about what behaviours would put them on the wrong side of the law. Cyber security professionals also sought a regime that takes into account the intent and motivation of their actions. The amendments to the Computer Misuse Act that we propose in Chapter 4 are motivated by these findings, and, following consultation with a collection of practising lawyer and legal academics, offer a solid foundation from which to begin to design an up-to-date piece of legislation. Our second and final recommendation is therefore:

2. **The Government should consult widely to design future-proof legislation that offers legal certainty to cyber security professionals acting in good faith.**

techUK

CyberUP