CyberUp Campaign – Written evidence (FDF0005)

Background

The CyberUp Campaign is pushing for reform of the UK's outdated Computer Misuse Act, to to protect against cyber crime, strengthen our national security and promote international competitiveness. The Campaign brings together a broad coalition of supporters across the UK cyber security sector and beyond (www.cyberupcampaign.com).

The Computer Misuse Act was created to criminalise unauthorised access to computer systems, or illegal hacking. It entered into force in 1990—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—traditionally—has been that the former lack authorisation whereas the latter usually have it. Yet, as cyber criminals' techniques have evolved, so have those of cyber security experts, regularly requiring actions for which explicit authorisation is difficult, if not impossible, to obtain.

As a result, the Computer Misuse Act now criminalises at least some of the cyber vulnerability and threat intelligence research and investigation UK-based cyber security professionals in the private and academic sectors are capable of carrying out. This creates the perverse situation where cyber security professionals, acting in the public interest to prevent and detect crime, are held back by legislation that seeks to protect computer systems.

The CyberUp Campaign wants to see the inclusion of a 'statutory defence' in the Computer Misuse Act, so that cyber security professionals who are acting in the public interest can defend themselves from prosecution by the state and from unjust civil litigation. This will provide much needed legal clarity, unlocking the world-leading UK cyber industry's full potential improving the general cyber resilience of UK systems and reducing cyber crime.

The Home Office conducted a Call for Information into the effectiveness of the Act, which finished in June 2021. Two thirds of respondents to the Home Office's Call for Information agreed that they did not believe that the current Act offered sufficient protections for legitimate cyber security activities. The Home Office is yet to respond to the views gathered. Our submission is available here:

https://www.cyberupcampaign.com/news/cyberup-campaign-submits-to-the-government-call-for-information

It is impossible to consider fraud—and online fraud, which the committee has said it is paying particular attention to—without considering the role of cyber security professionals working to tackle and minimise the harm of cyber crime, and therefore the implications of the Computer Misuse Act.

Online fraud, which in itself is a form of cyber crime, is often facilitated by and is also a facilitator of many of the types of cyber crime a reformed Computer Misuse Act would help to mitigate against. For example, a phishing attack, which is a form of online fraud, can enable a cyber attack on an individual or an organisation's systems. At the same time, a nefarious actor would undertake a cyber crime when hacking into an organisation's systems to steal bank account details. What is then done with those details would be considered fraud.

We'd therefore argue that online fraud and cyber crime are two sides of the same coin, which require a holistic and joined-up response to mitigate against. Though an earlier version of the Committee's stated areas of interest include wanting views on how "the police can be better supported to prosecute criminals who engage in cyber crime," we note that the current call for evidence contains no explicit reference to cyber crime. We have therefore taken the decision to provide a written submission that touches on some of the themes of the Committee's questions, making reference to cyber crime and cyber threats and the problems with the Computer Misuse Act.

Our key suggestion to the Committee would be to recognise that online fraud cannot be tackled without tackling cyber crime, and that the Committee should therefore make a recommendation to the Government to reform the Computer Misuse Act alongside any changes it suggests be made to the Fraud Act 2006.

Fraud and cyber crime

The Committee correctly notes in its call for evidence:

> *"…fraud is the most commonly experienced crime in England and Wales, accounting for approximately 42% of all crime against individuals, causing losses of billions per year. The pandemic fuelled growth in the use of online services such as banking. This dependency on digital technology has left more and more people vulnerable to increasingly sophisticated fraudsters."*

Like fraud, cyber crime and computer misuse is a prevalent and growing threat, and is hugely under-prosecuted and prevented.

In 2020 (the latest period for which full data is available), an estimated 99.99% of total cyber crime, and roughly 99% of reported computer misuse offences went unpunished.

- ONS data shows that between October 2019 and September 2020, there were 29,293 reported computer misuse offences, about half of those relating to social media and email hacking, followed by computer viruses and malware.
- We do, however, know that cyber crime is significantly underreported. The 2020 cyber security breaches survey found that 46% of businesses reported a cyber security breach or attack. Extrapolating from the survey sample of 1,348 businesses to the UK's 6 million business population as a whole, that means that in 2020, 2.7million businesses were a victim of a computer misuse offence. This includes 662,400 that suffered virus, malware, or

ransomware attacks, and 414,000 that experienced hacking attempts of bank accounts or otherwise unauthorised access to their systems.

- However, there were only 45 prosecutions in 2020 for computer misuse offences (33 of those for section 1 offences of unauthorised access; 11 for section 2 offences of unauthorised access with intent to commit further crimes; and 1 for a section 3A offence of making, supplying or obtaining hacking tools). There were 43 convictions, the average custodial sentence was 15.7 months, the average fine £1,203.
- We don't know how many prosecutions there have been in total under the Computer Misuse Act since its entry into force in June 1990. Between 2008 and 2020, there have been 486 prosecutions, an average of 37 per year; since 2013, the average annual number of prosecutions has been 55, or less than 5 per month—and 80% of those prosecutions result in convictions. Unauthorised access offences include illegal checks on internal databases, offenders using access to accounts after passwords had not been changed, or using login information without permission. Separate analysis has concluded that 25% of unauthorised access offences involve law enforcement officials who misuse police systems. Around a third of those convicted under the Computer Misuse Act were known to their victim, in some way, either as employees, or in another capacity. Motivations for those convicted under the Computer Misuse Act were said to be predominantly financial or otherwise profit-focused, revenge for losing a job, or harassment/stalking.

The role of the private sector — threat intelligence research

The cyber security industry works closely and in concert with law enforcement and intelligence agencies, sharing information with the relevant authorities and, in turn, allowing them to take steps 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, and is widely recognised by the UK Government as part of its 'whole of society' approach to cyber resilience[1].

For example, the joint INTERPOL-Europol operation Quicksand—which was coordinated through INTERPOL's Gateway project—included private industry partners Trend Micro, CDI, Kaspersky Lab and Palo Alto Networks. Across a four-year operation, they contributed to investigations by sharing information and technical expertise which led to the disruption of a ransomware cyber crime gang and saw the arrest of seven suspects believed to be behind global malware crime operations.[2]

In the UK, this public-private partnership is being hindered by the Computer Misuse Act, which is 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, and therefore having a detrimental impact on the UK's ability to fight cyber crime (and by extension online fraud). This detrimental impact is because the restrictions in gathering high quality actionable intelligence make it challenging to stay ahead of hostile threat actors and cyber criminals as the state alone cannot reasonably provide the required capacity and capabilities given the scale of the challenge.

The role of the private sector — vulnerability research

Vulnerability research constitutes investigative activities undertaken by a cyber security researcher to attempt to find a vulnerability in a product or an IT system, in the hopes of reporting this vulnerability to the system owner and preventing harm or expense.

Best practice for system owners includes having a clearly stated vulnerability disclosure policy—which is intended to give ethical hackers

[1] National Cyber Strategy 2022 (HTML) - GOV.UK (www.gov.uk)
[2] https://www.interpol.int/en/News-and-Events/News/2021/Joint-global-ransomware-operation-sees-arrests-and-criminal-network-dismantled

clear guidelines for submitting potentially unknown and impactful security vulnerabilities to organisations. They allow organisations to have a clear communication mechanisms in place for cyber security researchers—from those working for large multinational cyber security companies to those who work independently—who are interested in reporting vulnerabilities in that organisation's products and services. The organisation can then take steps to secure its products or services, preventing criminals and other nefarious from exploiting that vulnerability to commit cyber crime and, by extension, in some cases, fraud.

But vulnerability disclosure policies have no statutory footing in law, and researchers can still be threatened with legal action even if they have acted ethically. The following case study shows the risks cyber security researchers face with every disclosure they make under the current system:

Case Study

UK-based engineer Rob Dyke—who recently met with MPs in Parliament—has been involved in an expensive legal tussle with the Apperta Foundation, a UK-based clinician-led non-profit organisation that promotes open systems and standards for digital health and social care. The dispute stems from a confidential report Dyke made to the Foundation in February 2021 after discovering that two of its public GitHub repositories exposed a wide range of sensitive data, including application source code, usernames, passwords, and API keys.

Dyke has worked extensively in the healthcare sector, having previously worked on Apperta-funded development projects to benefit the NHS and had a cordial relationship with the organisation. Initially, the Foundation thanked Dyke for disclosing the vulnerability and removed the exposed public source code repositories from GitHub. However, on 8 March 2021, Dyke received a letter from a law firm representing the Apperta Foundation that warned that he "may have committed a criminal offence under the Computer Misuse Act 1990."

Around the same time, he was contacted by a Northumbria Police cyber investigator inquiring about a report of "computer misuse" from Apperta. After interviewing Dyke, law enforcement declined to pursue a criminal case against him for violating the Computer Misuse Act. Nevertheless, the Apperta legal team continued to pursue the civil case against Dyke and his legal bills grew, forcing him to crowdfund to pay legal bills in excess of £25,000 to defend himself before Apperta eventually dropped their threats.

The case of Rob Dyke shows that, despite the responsible discretion of law enforcement officials, the Computer Misuse Act can still be used by non-state bodies to pursue individuals through the civil courts, causing considerable injury to cyber security professionals who have acted in the public interest.

The case shows the kind of disincentives that currently exist for cyber security professionals to report vulnerabilities, and thus reduce the risk of those vulnerabilities being exploited by a cyber criminal or state-based threat actor. This logic lies behind aspects of the Government's Product Security and Telecommunications Infrastructure (PSTI) Bill – which seems to recognise the role of vulnerability researchers in improving general cyber resilience, by placing a duty on manufacturers of connected products to have a vulnerability disclosure policy. But, to reiterate, vulnerability disclosure policies have no statutory footing, and, as we have illustrated in the Rob Dyke case,there is nothing stopping companies – from a legal standpoint – seeking to go after cyber security researchers with legal threats to prevent information about the vulnerability being made public.

International best practice

Cyber crime legislation in a number of countries is derived from the principles of the Council of Europe Budapest Cybercrime Convention (Budapest Convention) which establishes the concept of unauthorised access to computer systems as the basis for criminalising (illegal)

hacking. However, it also recommends the adoption of qualifying circumstances to justify criminal culpability, including the infringement of security measures and existence of dishonest intent.

The UK, on the other hand, has adopted an, arguably overly, broad approach to criminalising "hacking," choosing to exclude any of the above-mentioned qualifying elements to more narrowly define computer criminality.

There are also examples from other countries' legal statutes – such as the Netherlands, the US and Israel – that were drafted in the spirit that there are types of computer access which constitute acceptable access and therefore deserve legal protection, primarily by having found means by which to take into account actors' motivations while addressing risks of abuse or misuse. Please see a full overview in the annex of this document.

It is clear that the UK's cyber legislation is now out of step with best practice from around the world, and notably with those countries who have thriving cyber security industries. Despite this, we believe that the proposals set out below would enable the UK to have a world-leading regime.

Policy solution

The CyberUp Campaign wants to see the inclusion of a 'statutory defence' in the Computer Misuse Act, so that cyber security professionals who are acting in the public interest can defend themselves from prosecution by the state and from unjust civil litigation. Allowing industry partners to carry out these legitimate activities would have the effect of 'widening the net' that state bodies such as the National Cyber Security Centre (NCSC) and National Crime Agency (NCA) are able to cast as they look to tackle cyber threats and cyber crime.

In response to understandable questions about how a reformed Computer Misuse Act would work in practice—striking the right balance between

protecting the cyber security ecosystem and prosecuting criminals effectively—the CyberUp Campaign has developed a set of principles, in consultation with industry and legal experts, that could guide the application of a 'statutory defence.' More information on those principles is available here: https://www.cyberupcampaign.com/news/a-proposal-for-a-principles-based-framework-for-the-application-of-a-statutory-defence-under-a-reformed-computer-misuse-act

Annex - computer misuse legal regimes in other countries

Netherlands

Guidance by the Dutch Public Prosecutor's office offers a pragmatic approach to allowing the consideration of actors' motivations while providing sufficient safeguards to identify and punish illegitimate and illegal behaviour:

- The Dutch Public Prosecutor's office instruct prosecutors to take into account if:

- A defendant acted in the interest of society: by way of example, in a case where a defendant identified vulnerabilities in a hospital's internet-facing systems and subsequently breached the system, downloaded patient data, and then alerted a trusted journalist who informed the hospital, the court found that identifying security issues regarding the protection of confidential medial and personal data was in the interest of society. It concluded that the defendant's hacking highlighted the hospital system's vulnerability to third party access, and contributed to public discussion about improvements in the health sector's cyber security practices.
- A defendant acted proportionally, i.e. if he did only what was strictly necessary to act in the interest of society: In the same case, the court concluded that scanning and exploiting a system to gain access to it was proportional, but noted that the defendant's actions of multiple logins and specific searching activities covering the

defendant's friends and family was not necessary and hence not proportional.

- A defendant acted in a subsidiary fashion, i.e. if he reacted or responded to his findings in the most appropriate way, allowing those responsible to take remediation action: The court found that there were no alternative, less intrusive ways for the defendant to achieve his objectives, and highlighted that the defendant contacted a trusted journalist with his findings who allowed the hospital to take remediation action before going public, and that the defendant pledged to report any future findings to the Dutch National Cyber Security Centre. The court ultimately determined that the defendant's actions were in the interest of society and undertaken with subsidiarity, but not proportional. The defendant was sentenced to 120 hours community service.

We also understand that the Dutch Public Prosecutor's office has made significant efforts to upskill its prosecutors in understanding the evolution of technology and cyber crime, and that the reform of the Dutch Computer Crime Act in 2018 resulted in open public discussion about cyber crime and cyber defences that ultimately increased public awareness, led to a welcome increase in cyber crime reporting, and facilitated the creation of new means and channels of sharing cyber threat and vulnerability information for private sector actors more effectively to support law enforcement activities.

<u>Austria</u>

Austria has made use of the qualifying exemptions provided by the Budapest Convention on cyber crime, taking a more narrow approach to criminalising unauthorised access by offering a legal mechanism to take account of an actor's motivation:

- Austria implements 'unauthorised access to computer systems' via paragraph 118a in its federal penal law (StGB 118a) but has chosen to

take a qualified approach (as opposed to the UK's blanket one). That means that unauthorised access to computer systems constitutes a criminal offence under the law only where:

- Security protections are circumvented;
- This is done with the intent to use the data and information gained, make it available to others, or deploy it for financial advantages / to cause damages.

United States of America

While the Computer Fraud and Abuse Act (CFAA), the US equivalent to the UK's Computer Misuse Act, faces similar challenge to those of the Act, the US generally offers a more conducive operating environment to cyber threat intelligence and research companies. This is evidenced by the fact that internet and vulnerability search engines such as Shodan and Censys are headquartered in the US, and that threat intelligence research published by US-based companies often involves methods that would be illegal under the UK's Computer Misuse Act.

In addition, the US offers examples of legislation and legislative proposals that explicitly include protections for security researchers, and that would establish exemptions from computer misuse prosecutions for cyber defensive activities:

- The US Department of Justice has issued specific policy documentation to guide prosecutors trying Computer Fraud and Abuse Act (CFAA) cases, acknowledging the technical complexity and the need, therefore, to seek expert input, where appropriate.
  - Title 9 9-48.000 of the Justice Manual notes that: "Cases under the CFAA are often complex, and analysis of whether a particular investigation or prosecution is warranted often requires a nuanced understanding of technology, the sensitivity of information involved, tools for lawful evidence gathering, national and international coordination issues, and victim concerns, among other factors. JM

§ 9-50.000 sets forth general requirements for cyber prosecutions, including coordination with and notification of the Computer Crime and Intellectual Property Section ("CCIPS") of the Criminal Division in certain cases."

- We also understand that the US Department of Justice (DOJ) does acknowledge that language in the CFAA creates legal uncertainties, and that there would be benefit in creating a framework that clarifies how private companies can conduct information security research without running afoul of the CFAA.
- At state level, the Washington Cyber Crime Act, passed in 2016, recognised new categories of cyber crime and enhanced law enforcement tools to prosecute cyber criminals, using the STRIDE threat modelling approach, but includes definitions and legislative intent guidance specifically designed to protect cyber security researchers.
  - "Without authorization" is defined as to knowingly circumvent technological access barriers to a data system in order to obtain information without the express or implied permission of the owner, where such technological access measures are specifically designed to exclude or prevent unauthorized individuals from obtaining such information, but does not include white hat security research or circumventing a technological measure that does not effectively control access to a computer.
  - "White hat security research is defined as accessing a data program, service, or system solely for purposes of good faith testing, investigation, identification, and/or correction of a security flaw or vulnerability, where such activity is carried out, and where the information derived from the activity is used, primarily to promote security or safety.

- The CyberUp Campaign has met with Chad Magendanz, a former member of the Washington House of Representatives, who sponsored this piece of legislation. He told us he would be happy to speak to UK policy makers and officials about his experiences in shepherding this legislation through the Washington state assembly.

Israel

We understand that Israel has recently initiated a new approach of unprecedented cooperation between government and the private sector, effectively ensuring that private sector entities that cooperate with the state on cyber security matters obtain a level of immunity.

Zambia

The Zambian Government's Cyber security and Cyber Crimes Bill entails a number of concepts such as harm prevention, protections and licensing of investigative cyber activities, which should be evaluated more closely as options for Computer Misuse Act reform:

- The legislation defines offences such as hacking into computer systems but also contains a clause stipulating that certain actions should not be interpreted as imposing criminal liability, for example where they are not undertaken for the purpose of committing an offence, or where they serve the protection of a computer system;
- The legislation includes the concept of licensing cyber security investigative activities, suggesting that undertaking any such activities is not permitted unless a prior licence has been granted to persons who are assessed to be fit and proper, and allows for individuals with suitable qualifications or experience to act as cyber security technical experts;
- The legislation finally introduces the concept of harm prevention where certain activities are permissible in circumstances where a cyber security threat or incident severely risks harming critical information

infrastructure, disrupting essential services, or threatening national security**.**

1 April 2022