CyberUp Campaign Response to DCMS Consultation

Embedding Standards and Pathways Across the Cyber Profession by 2025

As outlined in the Department's consultation, we agree that the Department's work on developing the cyber profession is closely intertwined with the Home Office's work on reforming the outdated Computer Misuse Act – something the CyberUp Campaign has long advocated for. This is because:

- **Computer Misuse Act reform will be a core enabler of the Department's ambition to widen the diversity of the UK's talent pool and address the remaining skills shortage**. A reformed Computer Misuse Act, providing greater legal protections for UK cyber security professionals through a new statutory defence, would improve the attractiveness of the profession for everyone with the right aptitude and attitude, by removing the risk of legal jeopardy for those in the profession.
- **The proposals for professionalisation support a consistent application of a statutory defence** that ensure that ethical professionals' actions are defensible while those of criminals remain punishable. An actor's competence, we believe, should be a factor for consideration when judging the defensibility of their actions. Implementation of the Department's proposal to regulate the use of professional titles, through UK Cyber Security Council led assessments of competence, could facilitate the judgment of competence (though cannot come at the exclusion of other proof of competence). Similarly, inclusion on any future register could offer supporting evidence of an actor's ethics. In turn, a reformed Computer Misuse Act could incentivise cyber security researchers to pursue membership of the proposed Register of Practitioners or use of a professional title as known ways of demonstrating competence.

We therefore believe that the Department's and the Home Office's work should proceed hand in hand as the desired outcomes have significant potential to offer solutions to respective challenges; however, we also believe that this cooperation should not come at the expense of kicking Computer Misuse Act reform into the long grass. We would welcome if the Department's response to the consultation provided an update on how its proposals will correspond to the Home Office's considerations.

Background

The CyberUp Campaign is pushing for reform of the UK's outdated Computer Misuse Act, to update and upgrade cyber crime legislation to protect our national security and promote international competitiveness.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 Home Office conducted a Call for Information into the effectiveness of the Act, which finished in June 2021. As the Department may be aware, two thirds of respondents to the Home Office's Call for 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.

We believe (and as is implied in the Department's own consultation) that the Department's work on developing the cyber profession is closely intertwined with the Home Office's work on reforming the outdated Computer Misuse Act, and outline below why that is the case:

Why reforming the Computer Misuse Act would support the Department's aims to make cyber security a more attractive, more accessible profession and reduce the skills gap

In 2018, Parliament's Joint Committee on the National Security Strategy concluded that the shortage of "deep technical expertise" was one of the "greatest challenges faced by the UK…in relation to cyber security,"[1] and while the skills gap has begun to decrease, the workforce is still short 3.21 million people[2]. As the Department acknowledges, the skills shortage affects public and private organisations alike, and tackling it is imperative for the long-term security and success of the UK.

In order to attract and nurture the skills the sector requires, it needs to be able to offer talented young people confidence that a career in cyber security would be a worthwhile and comfortable way to make a living. In this context, the impact of the outdated Computer Misuse Act and the potential legal jeopardy it puts professionals in is a concern.

Case Study

UK-based engineer Rob Dyke has shared his experience of his legal dispute with the Apperta Foundation, following a vulnerability disclosure he made to the organisation in February 2021. The dispute concluded after Mr Dyke made the reasonable undertakings requested.

So as to offer a complete representation of events, the CyberUp Campaign shares Rob Dyke's account before offering the Apperta Foundation's perspective.

Rob Dyke's experience

[1] https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/1658/1658.pdf
[2] https://blog.isc2.org/isc2_blog/2020/11/2020-isc2-cybersecurity-workforce-study-skills-gap-narrows-in-an-unusual-year.html

Rob Dyke has argued that his experience with the Apperta Foundation offers an example of the legal risk that cyber security researchers acting in the public interest are presented with.

Having discovered that two public GitHub repositories, belonging to a third party, exposed application source code, user names, passwords and API keys, Mr Dyke made a confidential report to the Foundation in February 2021.

The Foundation thanked him for the vulnerability disclosure and removed the exposed public source repositories.

In March 2021, however, Mr 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. He was also contacted by a Northumbria Police cyber investigator who inquired about a report of computer misuse by the Foundation. Law enforcement chose not to pursue a criminal case against Mr. Dyke, but unfortunately there was protracted correspondence between his lawyers and the Apperta Foundation's. Mr. Dyke chose to crowdfund money towards what he claims to be £25,000 worth of legal bills to fund this correspondence before eventually agreeing to the reasonable undertakings requested.

Apperta Foundation's perspective

The Apperta Foundation has argued that the case of Rob Dyke related to the unnecessary extraction and retention of confidential data as opposed to vulnerability disclosure. The Foundation has stated that it recognises good faith disclosures, acts according to industry standards and works productively and positively with individuals who responsibly inform organisations of security issues.

The Apperta Foundation has not contested that data exposure occurred but describe it as a relatively trivial breach. It has described the more significant aspect of the incident as relating to how Mr Dyke accessed and retained "considerably more confidential data than required to make the disclosure", and expressed concern that Mr Dyke republished links to archive sites containing the repositories, beyond the spirit of a responsible disclosure. The Apperta Foundation also notes that Mr Dyke, prior to his report, had publicly criticised the organisation.

The Foundation agrees that it thanked Mr Dyke for disclosing the vulnerability and took immediate action to remove the repositories from public view. It also asked Mr Dyke to confirm the extent of the information he had accessed and requested he delete any confidential information from his systems – something he did not do, but attached conditions and "arbitrary" retention timescales to doing, and which, the Foundation says, was the cause of the legal dispute. This was eventually resolved after Mr Dyke made an appropriate undertaking, having been presented with evidence against him.

The Apperta Foundation supports the objectives of the CyberUp Campaign and broadly agrees with the Campaign's principles-based Defence Framework (see below) to assess whether individuals who identify and report vulnerabilities have good intentions, act proportionately, do not cause more harm than is necessary, and are sufficiently competent in ethical research.

In its view:

- The harm of Mr Dyke's actions to store more confidential data than necessary outweigh the benefits of informing the Foundation immediately upon finding the GitHub repositories;
- Mr Dyke's intent was to cause turbulence and his conduct, including his failure fully to cooperate with relevant organisations in a timely manner, raised concerns about the intended use of the retained data.

While the CyberUp Campaign will not judge the merits of this case, it does believe that this example illustrates the relevance of an agreed principles-based approach that facilitates judgement of the defensibility of a security researcher's actions, as a core component of introducing further protections for cyber security researchers.

Closing the skills gap

If the UK is to meet the challenge of closing the cyber skills gap - and consequently grow its share of a global cyber security services market, currently dominated by North America, and bolster cyber resilience and defend the UK - it needs to stop criminalising the work and ultimately talent that is needed to promote the industry. Indeed, our research shows that 4 out of 5 UK cyber security professionals worry about breaking the law when researching vulnerabilities or investigating cyber threat actors. We believe the way to do this is by reforming the Computer Misuse Act to include a statutory defence (see more below).

To go alongside reform of the Act, we have advocated for a Government-backed information campaign to make clear what conduct the Government intends to legalise (or legitimise) with any proposed reforms, and what the intention is behind any such changes. This would be useful in helping to alleviate the widespread sense of anxiety in the industry over the possibility that any action of theirs might suddenly land them in legal jeopardy, and gradually thaw the freezing effect that stifles innovation and international competition in the sector. A public-facing communications campaign would also have the benefit of clearing up misunderstandings about the sector and send a clear marker to the industry that the Government values the contribution to national security and the economy that the cyber security sector makes and that it intends to help them successfully navigate the bounds of legal and legitimate activity under a reformed Computer Misuse Act. We believe this would send a strong signal to everyone that cyber security is a worthwhile and secure path for a career, thus helping the UK bridge its cyber skills gap.

Why the Department's proposals for professionalisation support a consistent application of a statutory defence under a reformed Computer Misuse Act

> *"This route [a register of practitioners] does open up potential opportunities to underpin and align with existing legislative frameworks. We know, at the time of writing, that there is work being explored around potential reform of the Computer Misuse Act. While this work is a separate process upon which no link can be fully defined at this point, there is potential to ensure a prominent role for defined professional competence to expand the scope of what changes may be possible where considered appropriate to ensure professionals are sufficiently clear on the legal confines of their activity."*

The above passage in the consultation document was, unsurprisingly, of particular interest to us. We agree that a reformed Computer Misuse Act is closely linked to the Department's work to define professional competence.

As we have noted above, we want to see the inclusion of a statutory defence in the Act so that cyber security professionals can defend themselves from unjust prosecution and civil litigation. To support the application of this defence – and in response to understandable feedback we received that emphasised the need to ensure there were safeguards to prevent nefarious actors or actions that are *prima facie* criminal acts from being decriminalised by our proposed reforms – we have developed a principles-based framework. The framework establishes a set of principles to be taken into account when determining whether an action should be defensible (see full summary below).

One such principle - the 'Competence Principle' – recommends that an actor's level of qualification/accreditation and/or membership of a professional body becomes one of a number of factors to consider when applying a statutory defence. In the context of the Department's proposals, being a member of the Register of Practitioners and/or using a statutory professional title could mean that a researcher was likely to satisfy the Competence Principle. It would then be for the courts to determine, on the basis of the remaining principles, whether the defence should ultimately apply.

We have not proposed that qualification, certification, accreditation or membership of a professional body act as a precondition for eligibility for a statutory defence, but rather that the existence of these proficiencies, alongside the other principles, could all act as supporting factors in the actor's favour when determining the defensibility of their acts. Indeed, this is because an individual may be highly qualified —and even be on a Register of Practitioners —and have a track record of successful research that led to actionable intelligence or otherwise improved general cyber resilience, and still commit a *prima facie* criminal act (an act we would want to remain criminalised under a reformed Computer Misuse Act).

We also chose in the defence framework to include factors beyond just simply whether a cyber security professional was accredited after reflecting on feedback that many cyber security researchers are self-taught and lack official qualification, though may still be highly skilled. However, we are open to a system that ties defensibility of an action more closely to a cyber security researcher's (potentially UK Cyber Security Council) accreditation.

It follows from the fact that qualification, certification, accreditation or membership of a professional body are neither necessary nor sufficient conditions for defensibility that we do not envisage that the proposed steps to embed standards in the cyber security sector are a necessary pre-cursor to reform of the Computer Misuse Act. The new system under a reformed Act could be established before any legislation (or other interventions) that underpins the UK Cyber Security Council comes into force, with the system built on a thoroughly updated DCMS / Home Office guidance on the practice of applying a statutory defence.

A summary of the CyberUp Campaign's principles-based framework for a statutory defence

What is the framework?

1. The principles-based framework aims to demonstrate that courts are capable of successfully and consistently applying an assessment of whether an act of unauthorised access was defensible, and thereby inform an evolving understanding of what constitutes legitimate conduct in cyber space.
2. The details of the framework are not intended to be included in primary legislation as part of a reformed Computer Misuse Act. Instead, we advocate for updated legislation to mandate the courts to "have regard to" Home Office or DCMS guidance on applying a statutory defence that would, ideally, be based on the framework we propose. We would also want courts to be upskilled on cyber matters over time. As is standard practice in criminal law, courts could seek evidence from independent expert bodies, such as, in this case, the UK Cyber Security Council, to understand technical details before them in the course of their work.
3. Our view is that, over time with case law, and ideally with clear guidance from Government departments and prosecutors, the boundaries of legal conduct will be clear enough that new norms of what is and is not acceptable conduct will be established within the industry.

The four guiding principles

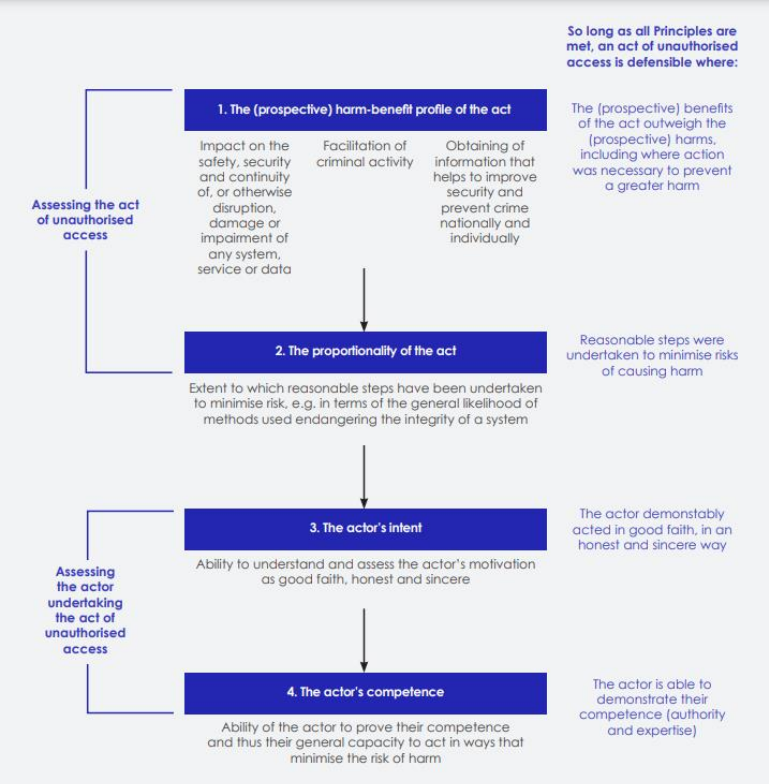

Figure 1: Overview of the CyberUp principles-based defence framework for applying a statutory defence in the cyber context.

The Competence Principle

We argue that there is a series of factors that ought to serve as a proxy to determining an actor's competence, and thus their general capability of acting in a way that minimises the risk of harm to the greatest extent possible. These include:

- An actor's level of qualification, certification, or accreditation
- An actor's membership of a professional organisation and compliance with a code of ethics
- An actor's professional capacity during the act in question — whether an actor was acting under commercial, academic, research, or other contracts, or participating in a bug bounty or other kind of product attack challenge programme
- An actor's prior track record of work, research and investigations — self-taught ethical hackers may not have any qualifications or be affiliated with any accrediting body, but this doesn't necessarily mean that the defence shouldn't apply to them
- An actor's previous associations — similarly, successful participation in schemes like bug bounty programmes should count towards competence

Please find the framework in full here: www.cyberupcampaign.com/news/a-proposal-for-a-principles-based-framework-for-the-application-of-a-statutory-defence-under-a-reformed-computer-misuse-act