CyberUp Campaign Submission to the Product Security and Telecommunications Infrastructure Bill Committee

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The CyberUp Campaign is pushing for reform of the UK's outdated Computer Misuse Act, to update and upgrade cyber crime legislation to protect our national security and promote international competitiveness.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). This includes HackerOne, one of the leading providers of Bug Bounty and crowd-sourced vulnerability and security research services.

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 and unlock the world-leading UK cyber industry's full potential, and will improve the general cyber resilience of UK systems.

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 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 to that Call for Information is available here: https://www.cyberupcampaign.com/news/cyberup-campaign-submits-to-the-government-call-for-information

We believe that the principles underpinning rationale for parts of the Product Security and Telecommunications Infrastructure (PSTI) Bill would be better complemented by reform of the Computer Misuse Act to include a statutory defence, which would allow the legislation to be more successful in achieving its aims. We set out why in this submission.

We are not seeking to have the PSTI Bill amended but would be grateful for consideration from Ministers at Report Stage or Third Reading as to the progress of the Computer Misuse Act review and how that policy development process will interact with this legislation.

The need for a cohesive cyber security legislative framework

As the Committee will be aware, under the regulations that will be introduced following the passage of the Bill, manufacturers of connectable consumer products will be required to provide a public point of contact to report vulnerabilities. The CyberUp Campaign believes this is an important step forward in ensuring that vulnerability disclosures by cyber security researchers are encouraged, leading to improved cyber resilience across systems. Indeed, the Government response to the consultation on these proposals mentioned the importance of legal certainty for security researchers in the context of vulnerability disclosure. The PTSI Bill is a step in the right direction in this regard.

However, the CyberUp Campaign has been clear that, without a statutory defence in the Computer Misuse Act, cyber security researchers can still face spurious legal action for reporting a vulnerability to a company which can decide on a whim to ignore its vulnerability disclosure policy – a practice known as liability dumping. If, as the PSTI Bill and accompanying discussion seems to recognise, encouraging greater vulnerability reporting is an important part of cyber resilience, then the Government should go further to reform the Computer Misuse Act and put in law a basis from which cyber security researchers can defend themselves.

Vulnerability Disclosure Policies of public bodies

Many UK public bodies already have vulnerability disclosure policies that include reference to the term 'good faith' as being necessary when a security researcher is reporting a vulnerability. We conducted a series of Freedom of Information request to ask these public bodies to define good faith.

The results showed clearly that there is, at the very least, a common working definition of good faith security research that, we argue, should provide the basis for updated Computer Misuse Act legislation that increases the certainty of what are legitimate cyber security activities and reduces the ability of entities to engage in the practice of liability dumping.

Please find that research in full here: https://www.cyberupcampaign.com/news/new-research-public-bodies-are-already-defining-good-faith

Case Study

UK-based engineer Rob Dyke – who recently met with MPs in Parliament – has been involved in an ongoing and expensive legal tussle with the Apperta Foundation, a UK-based clinician-led non-profit 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 in the healthcare sector, having previously 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 CMA. Nevertheless, the Apperta legal team have 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 need for further protections for cyber security researchers beyond the encouraging steps taken in the PSTI Bill.

Principle of primary legislation followed by guidance

We support the PSTI Bill's design in allowing the Secretary of State to make regulations to introduce mandatory security requirements for connectable products sold in the UK.

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'. In our principles-based Defence Framework (see 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), we state clearly that do not intend for the details of the framework 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 Department for Digital, Culture, Media and Sport (DCMS) guidance on applying a statutory defence that would, ideally, be based on the framework we propose.

The logic for this is the same, we believe, as that which lies behind the decision to give the Secretary of State power to make regulations to introduce mandatory security requirements for connectable products – it prevents the legislation from becoming dated in what is an area in which there is rapid technological development.