Submission to the Bill Committee by the Cyber Up Campaign, in support of amendments NC52 and NC53 to the Criminal Justice Bill – January 2024

This submission outlines the need to amend the Criminal Justice Bill to provide a legal defence for legitimate cybersecurity activities and deliver urgent reform of the outdated Computer Misuse Act (1990).

Summary

- **Amendment NC52 and NC53, proposed by Alex Norris MP, highlight to the Government how vulnerable the UK is to cyber-attacks and how our outdated cyber laws are holding back our cybersecurity professionals in their vital work protecting the UK from cyber criminals. Continued inaction will put the UK at risk in an ever-digital world. The Criminal Justice Bill is the perfect vehicle to push for urgently needed reform.**
- The Computer Misuse Act 1990 is over 33 years old. While unfit for purpose in the context of 21st century advances in technology, the threats we face, the unique geopolitical situation we are in and the evolution of the domestic cyber security industry, the legislation still governs how the UK tackles cyber criminals today.
- Updating the Act and providing a legal defence for legitimate cyber security activities would protect cyber professionals and increase the UK's ability to combat cybercrime, fraud, and foreign interference, whilst unlocking the growth potential of this already successful British tech industry: the enhanced economic opportunities of the sector post reform are significant – with potential increased revenue of £2.1 billion each year.
- There is clear evidence that reform is urgent and necessary. What is needed now is the political will to act, and to future-proof our response to cybercrime as well as deliver real benefits to the UK's economic prosperity, criminal justice system and national security.

Amendment NC52 and NC53

NC52

To move the following Clause—

"Definition of unauthorised access to computer programs or data In section 17 of the Computer Misuse Act 1990, at the end of subsection (5) insert— "(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 or tribunal to access of the kind in question to the program or data.""

NC53 To move the following Clause—

"Defences to charges under the Computer Misuse Act 1990 (1) The Computer Misuse Act 1990 is amended as follows. (2) In section 1, after subsection (2) insert— "(2A) It is a defence to a charge under subsection (1) to prove that—

(a) the person's actions were necessary for the detection or prevention of crime; or

(b) the person's actions were justiied as being in the public interest."

(3) In section 3, after subsection (5) insert— "(5A) It is a defence to a charge under subsection (1) to prove that— (a) the person's actions were necessary for the detection or prevention of crime; or (b) the person's actions were justified as being in the public interest."

Background to the CyberUp Campaign

The CyberUp Campaign is pushing for reform of the UK's outdated Computer Misuse Act (CMA), to update and upgrade cybercrime 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 and the Road to Reform

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. But now, over 33 years later, we are in 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 legal 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.

Sir Patrick Vallance, in his recent role as the Government's Chief Scientific Advisor, backed reform in his Pro-Innovation Regulation of Technologies Review, when he recommended*, "amending the CMA to include a statutory public interest defence that would provide stronger legal protections for cyber security researchers and professionals".* In his Budget Statement 2023, the Chancellor committed to implementing all of Sir Patrick's recommendations.

Key Statistics

- **77%** increase in cyber threats in 2022 according to the ONS.
- **8 million** instances of cybercrime against UK businesses and charities since the review into the CMA began in May 2021 according to the CyberUp Campaign, as covered in the Express.
- **£2.1 billion** estimated increased revenue potential post reform for the sector.
- Analysis in CyberUp's recent industry report, as covered in the Mirror, suggests:
    - **16,850 (or 2 GCHQs)** worth of cyber defenders estimated to be lost due to outdated cyber laws.
    - **60%** of respondents said the CMA is a barrier to their work in threat intelligence and vulnerability research.
    - **80%** of respondents believed that the UK was at a competitive disadvantage due to the CMA.

The Home Office conducted a Call for Information into the effectiveness of the Act, which closed in June 2021, with two thirds of respondents stating that they did not believe that the current Act offered sufficient protections for legitimate cyber security activities. Following the Home Office's response to the Call for Information in February 2023, it convened a stakeholder working group to consider the issue of defences which concluded in October 2023. In its most recent update in November 2023, the Home Office acknowledged that several respondents would support the introduction of a defence to CMA offences but did not announce any more concrete further steps. As the Joint Committee on the National Security Strategy concluded in December 2023, the outdated CMA leaves a gap in the UK's cyber defences that requires urgent action.

The CyberUp Campaign firmly believes that the Government can be at the forefront of defending the UK from the ever-growing cyber threat with up-to-date legislation and a modern approach that is fit for the 21st century, and that this goes hand in hand with the ongoing work to improve the law enforcement response to tackle fraud and prosecute cyber criminals.

How this relates to the Criminal Justice Bill

The Criminal Justice Bill introduces new powers for law enforcement to suspend domain names and IP addresses used for criminal purposes. This announcement directly follows the Home Office consultation on the Computer Misuse Act, as described above.

While the CyberUp Campaign recognises the need to address IP takedown powers, we strongly believe that any updates should not be delivered without the introduction of a defence to protect those actually undertaking legitimate cybersecurity activities. The CyberUp Campaign has been clear that, without a legal defence, cyber security researchers can still face spurious legal action for reporting security risks to a company which can decide on a whim to ignore its vulnerability disclosure policy. This demonstrates that offences and defences cannot be considered in isolation.

The Government is aware of the need to reform the UK's outdated cyber laws:

- When the Security Minister appeared before Parliament in November 2023, he acknowledged that the Act had to be updated in line with 21st century cyber defensive practices, but excused inaction to date with the lack of parliamentary time.
- The CyberUp Campaign agrees with the Joint Committee on the National Security Strategy's conclusion that *"the Minister for Security's acknowledgement of how out of date the Computer Misuse Act is does not excuse the lack of progress which has been made to legislate in this space. It has been two-and-a-half years after its main consultation and 33 years since that dated legislation received Royal Assent. It is hard to see how the Criminal Justice Bill brought forward by the King's Speech 2023 will sufficiently cover the gap left by the outdated CMA".* Indeed, this Bill presents a key opportunity to bring the UK's cyber laws into the 21st century and bring cyber criminals to justice.
- The House of Lords Fraud Act 2006 and Digital Fraud Committee Report 'Fighting Fraud: Breaking the Chain' clearly called on the Government to urgently reform the CMA and consider immediate reform, "*including the introduction of a statutory defence to protect cyber security researchers from prosecution*".

An amendment to introduce a legal defence would increase the UK's cyber defenders' collective ability to combat cybercrime, fraud and foreign interference and unlock the growth potential of this already successful British tech industry. Conversely, continued inaction is likely to result in a growing number of abandoned threat intelligence investigations, and unreported security vulnerabilities. This puts organisations and individuals at risk of harm from cyber-attacks that could be prevented.

The risk of inaction is simply too great: amending the Criminal Justice Bill is the action that is required to keep the UK safe in cyberspace.

Further information

For any further information please contact William Woodward at the Cyber Up Campaign:
contact@cyberupcampaign.com