Briefing on the Crime and Policing Bill: a critical opportunity to improve national resilience against cyberattacks and grow the domestic cyber security sector – March 2025

The CyberUp Campaign is calling for a long-overdue update to the **Computer Misuse Act 1990** (CMA)—a law that **currently prevents UK cyber security professionals from undertaking vital work** to protect national infrastructure without fear of legal repercussions, putting the domestic cyber security sector at a significant disadvantage. **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.

Despite widespread recognition of the need for change—including from Lord Vallance in his Pro-Innovation Regulation of Technologies Review, successful examples of updated legislation in other countries, widespread industry and cross-parliamentary consensus, and readily available policy safeguards—**legislative time is still urgently needed to update our cyber security legislation.** This urgency was echoed by the National Cyber Security Centre's (NCSC) 2024 Annual Review, which warned of a growing gap between the UK's cyber risks and its defences, stressing the need to update legislation, including the CMA, to address modern threats.

With the Crime and Policing Bill now at committee stage in the House of Commons, we are hoping that the **committee will be able to address this issue by tabling an amendment that would introduce a statutory defence for cyber security professionals.** Similar amendments were tabled by the Labour Party, then in Opposition, as part of the previous government's Criminal Justice Bill 2023-24.

The CyberUp Campaign is backed by a broad coalition of cyber security businesses, trade associations (including the CBI and techUK), and legal experts—and has prepared draft amendments (included below). These legislative changes are also backed by BT, Ciaran Martin (former CEO-NCSC), The Internet Services Providers'Association, Which?, and many others.

This latest Bill further reinforces the appropriateness of our proposed approach (i.e. statutory defence for legitimate action) by introducing a range of new public interest defences to proposed criminal offences. The inclusion of these defence mechanisms across different areas of law highlights an important inconsistency: while other offences are accompanied by statutory safeguards, the CMA still lacks a similar provision for cyber security professionals. Without a public interest defence, those working to identify and report vulnerabilities continue to face legal uncertainty and risk. **Given the clear precedent set by other defences in this Bill, it is only logical that the CMA should be updated to reflect the same principles. We hope the committee will consider championing this crucial change to strengthen the UK's cyber resilience and support the growth of its cyber security sector.**

Suggested Computer Misuse Act amendments:

"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."

"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 justified 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.""

Summary

- The Computer Misuse Act 1990 (CMA) is 35 years old. Despite being unfit for purpose in the wake of 21st century technologies, threats and the evolution of the domestic cyber security industry, the law still governs how we tackle cyber criminals today.
- As it is currently written, the Act inadvertently criminalises crucial cyber security research. This includes vulnerability research, threat intelligence activities and academic research – all of which are critical in protecting the UK from increasingly sophisticated cyberattacks.
- 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. It will also unlock growth in this already successful British tech industry —with a potential increase revenue of £2.4 billion each year.
- Lord Vallance—in his previous role as Government Scientific Adviser—recognised this and called on the previous government to urgently update the CMA, recommending the introduction of a statutory public interest defence in the CMA as part of his Digital Technology Regulation Review in March 2023. He also highlighted the move by global partners to update their legal frameworks in similar ways, and the need for the UK to do the same so our cyber industry is able to compete on a level playing field.
- Since the Vallance Review report, countries like Belgium, Malta, Germany, and Portugal haver confirmed they would be updating their legal frameworks in similar ways, while others like the Netherlands, France and the US already have more adequate legal regimes.
- The Crime and Policing Bill provides an opportunity to deliver on this much-needed update. The Bill introduces new powers for law enforcement to suspend domain names and IP addresses used for criminal purposes. 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 cyber security activities.

Key statistics

- **9 million** instances of cybercrime against UK businesses and charities since the review into the CMA began in May 2021 (based on DSIT's 2024 Cyber Breaches Survey, published April 2024).
- The same Cyber Breaches Survey showed **50% of businesses and 32% of charities suffered a cyber breach or attack** last year.
- The **total cost of cybercrime to the UK economy** is estimated to be **£27 billion per year**, with businesses accounting for a significant proportion of this cost. The **National Fraud Authority** estimates that fraud—including online fraud—costs the UK over **£38 billion annually**.
- **£2.4 billion** estimated increased revenue potential post-update for the sector.
- **17,750 (or +2 GCHQs)** worth of cyber defenders are estimated to be lost due to outdated cyber laws.
- Analysis based on the CyberUp's recent industry report, suggests:
    - **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.
- **Two-thirds of UK adults are inclined to support a change in the law** to allow cyber security professionals to carry out research to prevent cyberattacks.

Background to the CyberUp Campaign

The CyberUp Campaign is the UK's leading cyber coalition calling for an update to the UK's outdated Computer Misuse Act 1990 (CMA). It brings together a broad base of supporters from across the UK cyber security sector, academia and beyond. Together, we advocate for updating and upgrading cybercrime laws to protect our national security, enhance our resilience to digital crime, and promote the UK's international competitiveness in the rapidly evolving global technology sector (https://www.cyberupcampaign.com/).

The Policy Solution: 'Statutory Defence' with strong and appropriate safeguards

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. Countries like Malta, Germany and Belgium are updating their legal frameworks in similar ways, while others like the Netherlands, France and the US already have more adequate legal regimes.

This proposal has also been backed by Sir Patrick Vallance, during his previous role as the Government's Chief Scientific Advisor, in his Pro-Innovation Regulation of Technologies Review: *"amending the CMA to include a statutory public interest defence that would provide stronger legal protections for cyber security researchers and professionals".* We also note the ICO's recommendation to the Home Office on the need for exemptions for legitimate actors built into the legislation.

In response to understandable questions about how an updated CMA would work in practice—striking the right balance between protecting the cyber security ecosystem and prosecuting criminals effectively—the CyberUp Campaign, in consultation with industry and legal experts, has developed a framework that could guide the application of a 'statutory defence'. This has been supplemented with additional research that establishes an industry consensus of which legitimate cyber security activities should be legally permissible.

This 'Defence framework' establishes a set of principles to be taken into account when determining whether an action should be defensible and by whom. Actions should be justifiable if their benefits outweigh potential harms, especially when preventing greater harm (*Harm-Benefit Principle*), and actors must take reasonable steps to minimise harm (*Proportionality Principle*). Defensible actions require good faith, honesty, and sincerity (*Intent Principle*), and an actor's qualifications, accreditation, or professional memberships should also be considered (*Competence Principle*).

The proposal is proportionate, includes appropriate safeguards, and has widespread backing from industry, academia and parliament, including:

- **Extensive stakeholder engagement:** Over the past four years, the Home Office has conducted extensive stakeholder engagement. The outcome of all these exercises has demonstrated overwhelming support for an update to the Act - with two-thirds of respondents to the initial call for evidence stating that they did not believe that the current Act offered sufficient protections.

- **Support within the cyber security sector is clear and unequivocal:** A recent industry survey by the CyberUp Campaign, 100% of respondents from across the UK cyber security industry were also in support of the introduction of a statutory defence for good faith research. The CyberUp Campaign is backed by a growing coalition of industry representatives from NCC Group, LRQA, F-Secure, techUK, CREST, the Cyber Scheme, Cyber Defence Alliance, Cyber security Advisors Network (CyAN), CyberLondon and many others. Darktrace —a global leader in cyber security artificial intelligence—also confirmed its support of an update to the CMA.

- **A statutory defence is supported by wider services businesses and consumer groups,** including BT Group, Which?, and The Internet Services Providers' Association—which represents BT, Virgin Media and Sky.

- **Independent voices have endorsed updating the CMA to provide further legal protections for cyber security professionals, including** the former CEO of the National Cyber Security Centre Ciaran Martin, and the ICO.

- **Cross-Party Parliamentary Support:** This includes recommendations for updating the CMA in the Joint Committee on the National Security Strategy's ransomware inquiry and the Science, Innovation and Technology Committee's Legacy Report.

State of Play: The Road to a CMA Review

More than three years have now passed since the previous Government first announced its review of the CMA. The Campaign felt as though cyber security had fallen off the political agenda just as the threats were reaching unprecedented levels. Indeed, despite two public consultations, a Home Office industry working group, and the strong recommendation to update the Act in Lord Vallance's review, the previous government repeatedly postponed addressing this issue.

The Campaign has welcomed this Labour Government's commitment thus far to improving cyber security through the introduction of the Cyber Security and Resilience Bill in the King's Speech, the designation of data centres as CNI, an additional £1.3m cyber skills grant as well as Labour's prior support for updating the Computer Misuse Act 1990, by tabling amendments during the Criminal Justice Bill (NC18 NC19), and the Security Minister Dan Jarvis's positive comments while in Opposition. At the recent Predict Conference, the Security Minister, Dan Jarvis, confirmed that the government is considering reforming the CMA as one of several policy options to strengthen the UK's response to cyber threats.

There is **clear evidence that an update 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.

How the Computer Misuse Act relates to the Crime and Policing Bill

The Crime and Policing Bill introduces new powers for law enforcement to suspend domain names and IP addresses used for criminal purposes. 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 cyber security 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.

These provisions have been carried over from the previous government's Criminal Justice Bill 2023-24. During the Committee and Report Stage of the Criminal Justice Bill in the House of Commons, the Campaign were delighted to see the amendments tabled by then Shadow Minister for Policing, Alex Norris MP (now Minister), to introduce a public interest defence to the CMA. This was lent further support by the then Shadow Labour Security Minister Dan Jarvis MP, who highlighted Labour's support for an urgent update to the CMA and called on the previous government to address the continued delays to reform. He stated in his speech that: *"[this] is why the Opposition tabled an amendment to the Criminal Justice Bill that would reform the CMA by introducing a statutory defence for cyber-security researchers and professionals involved in ethical hacking. […] If this Government do not deliver, the next one should. Until that happens, the legislative lag will have consequences."*

This latest Bill further reinforces the appropriateness of our proposed approach (i.e. statutory defence for legitimate action) by introducing a range of new public interest defences to proposed criminal offences. These defences cover offences related to both possession and provision of objects, such as child sexual abuse image generators, SIM farms, and other specified articles, as well as actions and conduct, including wearing items, climbing on war memorials, or taking photographs in specific contexts.

A few key features stand out in the way these defences have been structured. First, there is clear legislative intent to codify defences rather than relying solely on prosecutorial discretion, ensuring greater legal certainty

for individuals. Second, the Bill makes extensive use of flexible 'good reason' defences, recognising that rigid statutory definitions may not account for legitimate activities in complex cases. Finally, it incorporates reverse burdens of proof, or at least evidential burdens, which places on the defendant the brunt of the burden to provide justification for their actions and the application of the defence.

The inclusion of these defence mechanisms across different areas of law highlights an important inconsistency: while other offences are accompanied by statutory safeguards, the CMA still lacks a similar provision for cyber security professionals. Without a public interest defence, those working to identify and report vulnerabilities continue to face legal uncertainty and risk. **Given the clear precedent set by other defences in this Bill, it is only logical that the CMA should be updated to reflect the same principles. We hope the committee will consider tabling and championing this crucial change to strengthen the UK's cyber resilience and support the growth of its cyber security sector.**

Further information

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