CyberUp Campaign | Cyber Security and Resilience (Network and Information Systems) Bill submission | January 2026

Overview

The CyberUp Campaign welcomes the Cyber Security and Resilience Bill as a landmark step towards strengthening the UK's defences. However, **the Bill fails to address a major vulnerability in the sector, the decades-old Computer Misuse Act 1990 (CMA)**.

This outdated law criminalises good-faith cyber security research, weakening national resilience, limiting economic growth, and leaving the UK exposed to increasingly complex cyber threats. In its current form, the CMA inadvertently criminalises critical activity such as vulnerability research and threat intelligence, both of which are essential for defending the nation's digital systems.

CMA reform is essential for the delivery of the Cyber Security and Resilience Bill. Many of the security requirements regulated entities will have to comply with will require skilled cyber professionals, including threat intelligence and vulnerability researchers. By effectively criminalising much of the work these professionals are able to undertake, the ability of regulated entities to fulfil their obligations is compromised, potentially encouraging them to use non-UK services.

The Government has committed to exploring a statutory defence for cyber security researchers under the CMA. Security Minister Dan Jarvis MP highlighted this need in a recent speech, stating, *"We've heard the criticisms about the Computer Misuse Act, and how it can leave many cyber security experts feeling constrained in the activity that they can undertake. [...] We shouldn't be shutting these people out, we should be welcoming them and their work."*[1]

The necessary amendment (below) is already drafted and ready to implement. It is a simple, straightforward step that ensures both vulnerability research and threat intelligence are fully protected, giving the professionals safeguarding the UK the legal certainty they need.

As the UK's first ever 'cyber' Bill, this is a historic opportunity that must be seized**. Updating the CMA is a straightforward and necessary step which improves the Cyber Security and Resilience Bill by updating the legal foundations of UK cyber security.** It strengthens the regulatory framework, empowers the professionals defending the nation, supports growth in the cyber security sector, and demonstrates the Government's commitment to resilience and innovation.

---

[1] Keynote address to FT Cyber Resilience Summit 2025, 3rd December 2025, https://www.gov.uk/government/speeches/keynote-address-to-ft-cyber-resilience-summit-2025

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.""

Nature of the issue

The Computer Misuse Act 1990 (CMA) was created to criminalise unauthorised access to computer systems. However, as it is currently written, the CMA produces a perverse situation where industry specialists who are acting in the public interest to defend computer systems are at risk of being defined as criminals if they access them without permission. It blanketly prohibits all forms of unauthorised access to computer material, irrespective of intent or motive to act in the public interest and assist in the prevention of a crime.

This outdated legislation restricts the UK's cyber industry, which collaborates with law enforcement, the public sector, academia, and private firms to create a more secure digital environment. By banning all unauthorised access, the CMA ties the hands of UK cyber defenders, including those working in-house within our critical infrastructure.

The 'chilling effect' that the fear of legal prosecution brings to the cyber industry is well documented. Our 2023 survey found that 71% of threat intelligence researchers were concerned about inadvertently breaching the CMA. The UK Home Office's own call for evidence found that two-thirds of respondents believed the current Act does not provide sufficient protection for legitimate cyber security activity.

Conversely, failure to update the law could result in a loss of £4 billion and the departure of more than 18,400 skilled professionals—the equivalent of losing more than two entire GCHQs—to international competitors with modern, fit-for-purpose cybercrime laws.

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

The CyberUp Campaign is calling for the inclusion of a legal defence in the CMA, 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.

In consultation with industry, academia and legal experts, the CyberUp Campaign 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 regarding 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 and academia. In addition to the supporters of the CyberUp Campaign and legal academics from the Criminal Law Reform Now Network, others who have backed a statutory defence include BT, Which?, and former CEO of the National Cyber Security Centre Ciaran Martin.

This proposal has also been backed by Lord Patrick Vallance during his previous role as the Government's Chief Scientific Advisor. In his Pro-Innovation Regulation of Technologies Review, he recommended "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.

The UK Cyber Security Sector is being left behind

The Cyber Security and Resilience Bill will update the NIS regulations, helping to align with the EU's NIS2 framework. If the UK is aligning its NIS framework with the EU, this is a clear opportunity to reform other areas of cyber law that impact the sector, including the currently limited CMA.

Other countries have already taken action. The EU's Cyber Resilience Act (clause 75) calls on States to support responsible cyber research, with Belgium having adopted reforms, Malta and Germany drafting theirs, and the Netherlands and France providing clear protections for legitimate cyber security activity. Portugal even used its equivalent of the Cyber Security and Resilience Bill to strengthen legal protections for researchers, creating a creating a framework where strict conditions have to be met: the sole purpose must be identifying vulnerabilities and contributing to cybersecurity, similar to the Campaign's proposed 'statutory defence'.

Beyond the EU, the US has an established legal framework, and Australia has consulted on measures to reduce barriers for researchers. Most recently, Hong Kong's Law Reform Commission recommended introducing bespoke cybercrime legislation to provide specific defences to permit unauthorised access made for cyber security purposes. It is therefore possible that this territory, which was still under UK governance when the CMA was introduced, will have changed hands and updated its own cybercrime legislation before the UK does so itself.

The message is clear and obvious. Nations around the world have modernised their cyber laws to protect researchers and promote innovation. The UK cannot afford to lag behind. Updating the CMA now is the straightforward, necessary step to ensure our laws protect those defending the nation, support the cybersecurity sector, and keep the UK globally competitive.

How does this relate to the Cyber Security and Resilience Bill?

The Cyber Security and Resilience Bill is a landmark step for the UK, being the first legislation to explicitly put cyber security in its title. It updates the NIS Regulations, aligning with the EU's NIS2 framework, strengthening oversight, and improving incident reporting across essential services. While these are important steps forward, the Bill misses a crucial opportunity by not updating the Computer Misuse Act.

CMA reform is essential for the Bill to deliver on its objectives. Many of the security requirements regulated entities must comply with rely on skilled cyber professionals, including threat intelligence analysts and vulnerability researchers. Currently, the CMA criminalises much of the work these professionals undertake, limiting their ability to support regulated organisations and potentially driving UK entities to rely on services outside the country.

Reforming the Act would ensure these professionals can operate confidently and legally, making compliance with the Bill both feasible and effective.

The UK cyber industry already generates over £13 billion in revenue and supports 58,000 skilled jobs. Modernising the CMA could unlock £2.6 billion in additional economic value and create 9,555 new jobs. This would directly strengthen national cyber resilience and signal the Government's commitment to supporting the professionals responsible for protecting the UK's digital infrastructure. Threat intelligence and vulnerability research are essential to preventing cyber incidents before they impact essential services. Ensuring these activities are clearly protected in law is a straightforward and necessary step to make the Bill effective in practice.

About the CyberUp Campaign

The CyberUp Campaign has long been advocating for reform of the UK's outdated CMA 1990, to update and upgrade cybercrime legislation to protect our national security and resilience to digital crime, and to promote the UK's international competitiveness in the rapidly evolving global technology sector. The campaign brings together a broad coalition of supporters across the UK cyber security sector and beyond.

For more information about the CyberUp campaign, please see: www.cyberupcampaign.com or email at contact@cybercampaign.com.