

It's time to CyberUp!

Update our laws, Upgrade our defences, Upskill our workforce

What is the CyberUp campaign?

The CyberUp campaign – which brings together a broad coalition of supporters including cross-party parliamentarians and industry bodies such as CBI and techUK – is calling for urgent reform of the Computer Misuse Act 1990 (CMA) to protect the cyber security professionals working hard to keep Britain safe and secure in today's digital world. 32 years after its introduction, the CMA remains the main legal regime covering cybercrime in the UK. As it is currently written, it inadvertently criminalises a large proportion of vulnerability and threat intelligence research that UK cyber security professionals are capable of carrying out to protect the UK from rising cyber threats such as ransomware attacks.

What do cyber security professionals do and why is this important?

Vulnerability and threat intelligence research is undertaken for defensive purposes. Researchers identify vulnerabilities in products and services and work with manufacturers and vendors to fix them. They also detect cyber attacks, gain insight into attackers and victims, lessen the impact of incidents, and prevent future ones. The UK Government's National Cyber Strategy 2022 recognises the value of this important work, committing to build valuable and trusted relationships with the security researcher community to deliver a reduction in vulnerabilities.

How does the CMA impact cyber security professionals?

The CMA blanketly prohibits all unauthorised access to computer material, irrespective of intent or motive. This leaves the UK's cyber defenders having to act with one hand tied behind their back because much of their defensive work requires the interaction with compromised victims' and criminals' computer systems where owners have not, or are unlikely to, explicitly permit or authorise such activities.

What are we calling for?

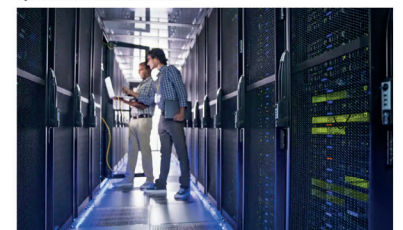
The CyberUp campaign wants to see the inclusion of a 'statutory defence' in the CMA, so that cyber security professionals who are acting in the public interest can defend themselves from prosecution by the state and from unjust civil litigation. This will provide much needed legal clarity and unlock the world-leading UK cyber industry's full potential.

MailOnline
EXCLUSIVE: UK's 'outdated' cyberlaws preventing experts infiltrating cybercriminals' networks without THEIR permission must be reformed, campaigners say, as two thirds of Britons back call to update Computer Misuse Act

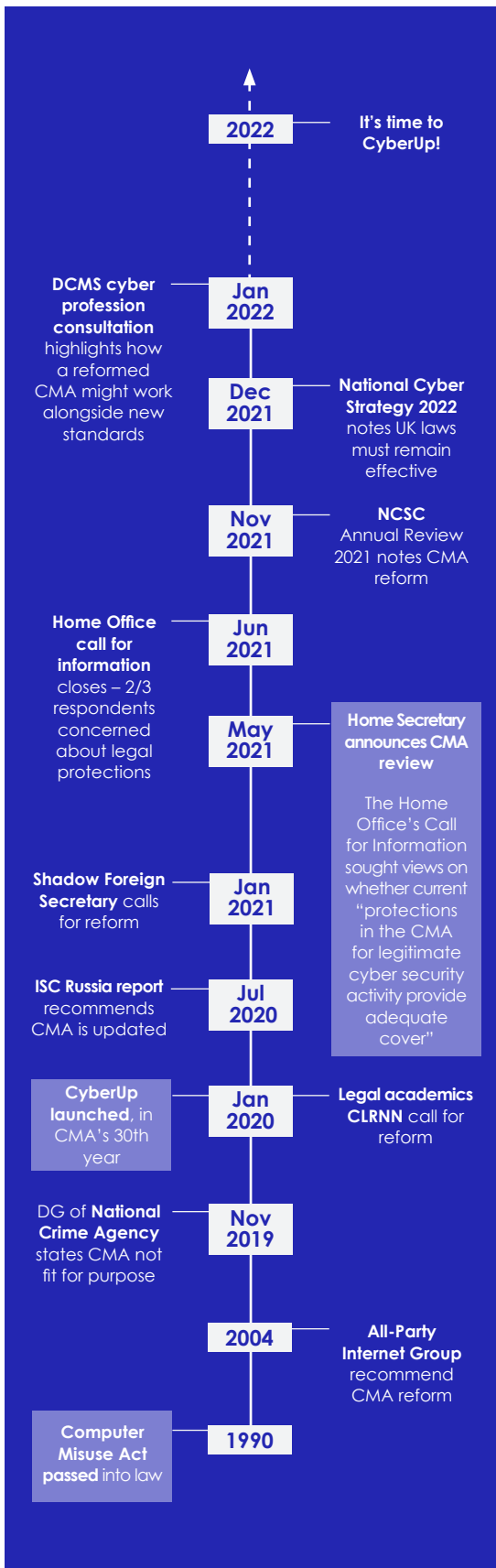
The Guardian
News website of the year

Cybercrime laws need urgent reform to protect UK, says report

Lawyers say ineffectiveness of act exposes UK to harm by 'cybercriminals and hostile nations'



CyberUp



What does this look like in practice?

In response to understandable questions about how a reformed CMA 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'. That means that when judging a cyber security professionals' actions to see if a cyber crime was committed, the following would be taken into account:

| The (prospective) harm-benefit profile of an act | The proportionality of the act | The actor's intent | The actor's competence |
|--|--|--|---|
| <i>"A defence should be considered where the (prospective) benefits of the act outweigh the (prospective) harms, including where action was necessary to prevent a greater harm"</i> | <i>"A defence should be considered where reasonable steps were undertaken to minimise risks of causing harm"</i> | <i>"A defence should be considered where the actor demonstrably acted in good faith, in an honest and sincere way"</i> | <i>"A defence should be considered where the actor is able to demonstrate their competence (authority and expertise)"</i> |

Why is reform needed?

A reformed CMA will strengthen the essential building blocks needed to be a leading democratic and responsible global cyber power – an ambition the UK Government set out in the Integrated Review and reiterated in the National Cyber Strategy 2022.

- It will make the UK **safer and more secure** by allowing cyber security professionals to improve cyber security and detect and prevent crime in the public interest without the threat of prosecution. The government has repeatedly emphasised the crucial role of the UK's public-private sector partnership in keeping UK cyberspace safe, as part of a whole-of-society approach. But, the longer we wait to reform the CMA, the longer the UK's private sector cyber defenders must operate with one hand tied behind their back. As the digital threat landscape continues to evolve in intensity, complexity and severity – now is the time for reform!
- It will bring UK cyber crime laws into the **21st century**. The CMA was put on the statute book when 0.5% of the population used the internet. The digital world has since changed beyond recognition and the Act must be updated to reflect that.
- It will put the UK on a **level footing** with global competitors and **drive growth**. The restrictions put in place by the CMA put the brakes on what has the potential to be one of the biggest growth areas in the UK's burgeoning tech sector. This is because companies headquartered in jurisdictions that offer more permissive legislative regimes, such as France, the US and Israel, are able to supply the market with a rich supply of threat intelligence gathered abroad, putting UK businesses at a competitive disadvantage. Each year the Government fails to update the CMA, the UK cyber industry is at risk of falling behind its international competitors, losing out on up to 20 per cent additional revenue.
- It will help to tackle the **cyber skills shortage** (estimated at 10,000 per year) by lifting a significant disincentive for aspiring cyber security researchers to join the profession.

80%
of businesses
indicate the CMA
has inhibited their
employees from
preventing harm

66%
of the public would
support a change
in the law

91%
of UK cyber
businesses put
at a competitive
disadvantage

£1.8bn
additional annual
sector revenue, and
7,000
new jobs

66%
of respondents to the
Call for Information
stated that they had
concerns over the
current protections
in the act for
legitimate cyber
activity

The CyberUp campaign remains optimistic that reform is imminent. That is because, as we await the outcome of the Home Office review of the CMA, so many of the UK's ambitions would be furthered by a UK cyber crime law fit for the 21st century. But the more we delay, the longer our cyber security industry is held back from fulfilling its full potential.

We would be grateful for anyone who felt able to write to the Home Secretary in support of our ask and to press for a timeline. Join us and find out what more you can do to help make CMA reform a reality by emailing contact@cyberupcampaign.org