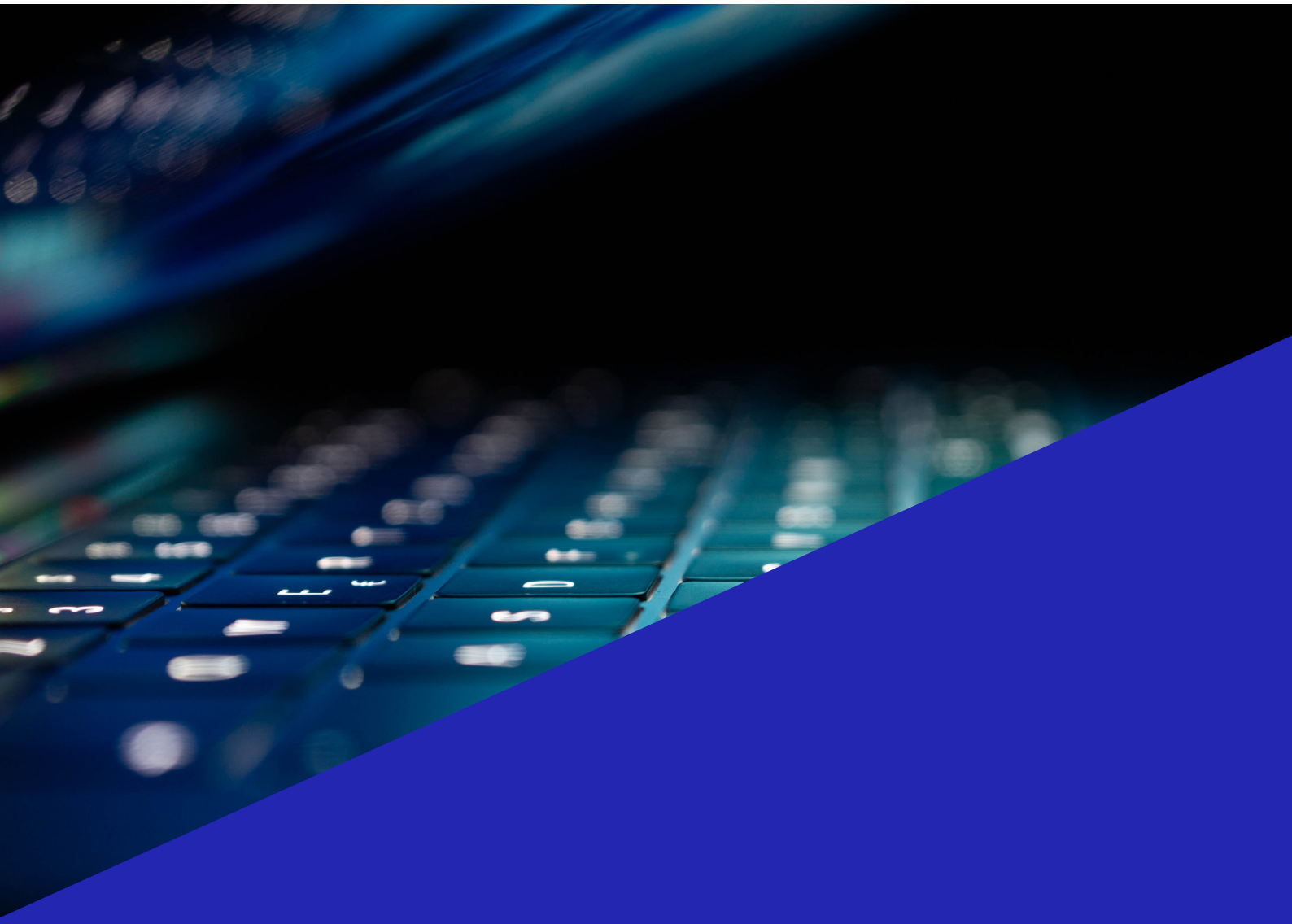


CyberUp response to the UK National Cyber Strategy 2022

How CMA reform will drive a whole-of-society approach to cyber resilience

January 2022

Whilst the publication of the UK Government's National Cyber Strategy (NCS) marked a missed opportunity to introduce much needed changes to the Computer Misuse Act 1990 (CMA), 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 ambitions set out in the NCS would be furthered by a UK cyber crime law fit for the 21st century. In this short report we detail how a reformed CMA would help to deliver the UK Government's aims, in support of its national goals.

What are we calling for?

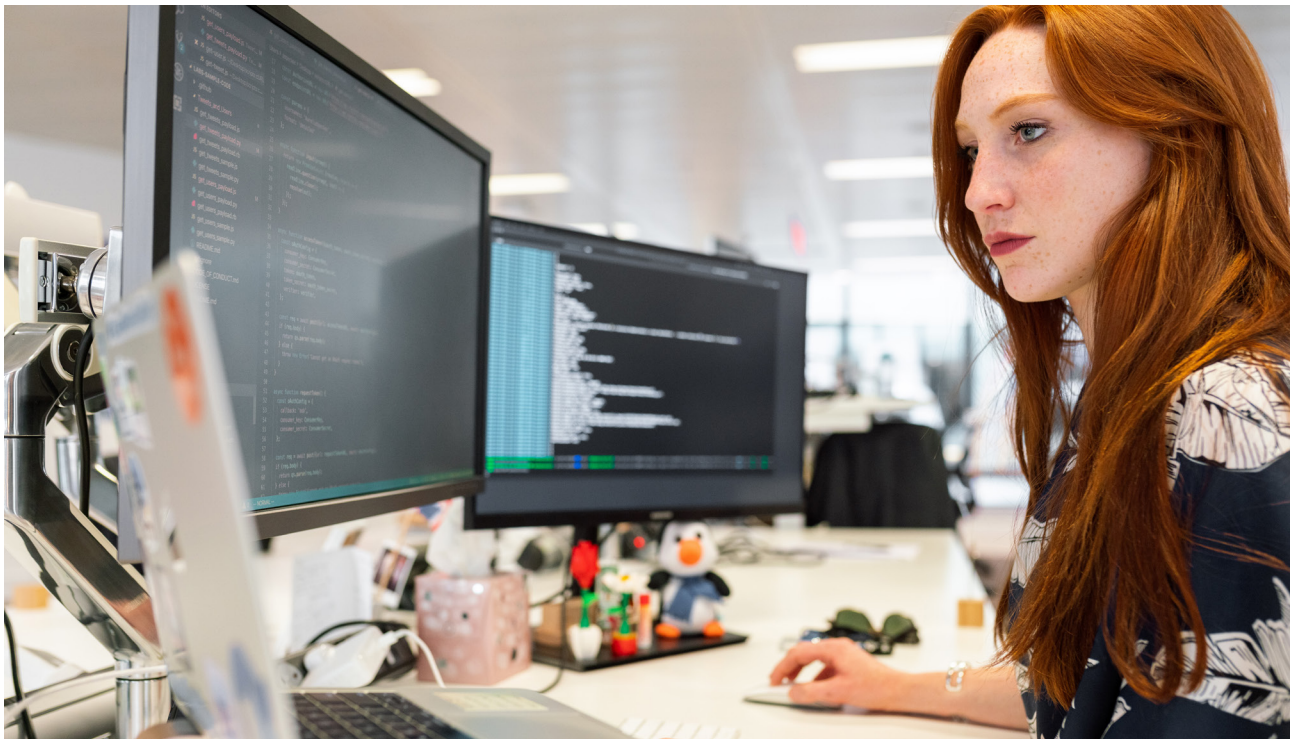
Much of the threat intelligence and vulnerability research that cyber security professionals are able to carry out to protect the country is criminalised. This is because the CMA blanketly prohibits all unauthorised access to computer material, irrespective of intent or motive. This leaves the UK's cyber 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.
The CyberUp Campaign has been pushing for the inclusion of a 'statutory defence' in the CMA, so that cyber security researchers 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, better enabling ethical cyber security researchers to support national cyber resilience, strengthening law enforcement response to cyber crime, and promoting the growth of a burgeoning industry.

How would this help to deliver the National Cyber Strategy's aims?

UK Government National Cyber Strategy commitment(s) or aim(s)	How a reformed Computer Misuse Act will help
NATIONAL GOAL A more **secure and resilient nation**, better prepared for evolving threats and risks and using our cyber capabilities to protect citizens against crime, fraud and state threats	
The Government will take action in and through cyberspace to **support our national security and the prevention and detection of serious crime**.	**A reformed Computer Misuse Act will make the UK safer and more secure** by allowing cyber security professionals to improve cyber security and detect and protect crime in the public interest without the threat of prosecution, whilst remaining tough on cyber criminals. The CyberUp Campaign has published a detailed paper on how this can work in practice through a principles-based framework[1].
Central to the strategy will be a **whole-of-society** approach to cyber. We need to build an enduring and balanced partnership across the public, private and third sectors, with each playing an important role in our national effort. The Government will seek to benefit from the cyber security sector's capabilities and expertise, including by establishing a new National Cyber Advisory Board.	**A reformed Computer Misuse Act will ensure an essential component of a truly whole-of-society approach – the cyber security sector – is able to do its job effectively**, plugging gaps the public sector is unable to fill and protecting the UK from hostile actors. The Government's recognition of the important role of the partnership between the public and private sectors in the UK's national cyber defence is welcome. Indeed, we note that the Strategy mentions 'private sector' or 'industry' 71 times across its 130 pages. But the current Computer Misuse Act limits this kind of collaboration and constrains its full potential. UK cyber security professionals are operating with one hand tied behind their back and in fear of prosecution – meaning a core component of the whole-of-society approach is presently hampered. Reform will provide much needed clarity and legal protections.
The Government will invest in the UK's **cyber intelligence capabilities**, improving threat detection coordination, ensuring investigations are supported by intelligence from all sources, and leveraging skills and knowledge across the private sector.	**A reformed Computer Misuse Act will unleash the full potential of the cyber industry to bolster UK threat intelligence.** The cyber security industry works closely with law enforcement and intelligence agencies to defend the UK against cyber crime and geo-political threat actors. But the current legal restrictions in gathering high quality actionable intelligence make it highly challenging to stay ahead of hostile threat actors and cyber criminals as governments alone cannot provide the required capacity.

[1] New Research: a proposal for a principles-based framework for the application of a statutory defence under a reformed Computer Misuse Act — CyberUp (cyberupcampaign.com)

UK Government National Cyber Strategy commitment(s) or aim(s)	How a reformed Computer Misuse Act will help
We will establish a cross-Government **Vulnerability Reporting Service** (VRS) [that] will aim for **valuable and trusted relationships with the security researcher community**, delivering a reduction in vulnerabilities across the government estate.	**A reformed Computer Misuse Act will remove uncertainty for cyber security researchers as they look to help government, and other targeted organisations, identify and tackle vulnerabilities.** The logic of the prospective VRS – and proposals in the *Product Security and Telecommunications Infrastructure (PSTI) Bill* – is that the Government sees private sector vulnerability research as part of the solution to improved cyber resilience across society. A reformed Computer Misuse Act will give proper expression to the value security researchers bring and establish certainty beyond reliance on trusted relationships, hoping organisations adhere to their own stated policies, and prosecutorial discretion.
The UK's cyber security **legislation must remain effective** in the light of evolving risk and technologies.	**A reformed Computer Misuse Act will bring UK cyber crime laws into the 21st century.** The Computer Misuse Act, though world-leading at the time of its introduction, 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.



[1] New Research: a proposal for a principles-based framework for the application of a statutory defence under a reformed Computer Misuse Act — CyberUp (cyberupcampaign.com)

UK Government National Cyber Strategy commitment(s) or aim(s)	How a reformed Computer Misuse Act will help
NATIONAL GOAL A **Science and Tech Superpower**, securely harnessing transformative technologies in support of a greener, healthier society	
For this strategy to succeed, we must have an **internationally competitive cyber sector**. The Government will continue to support the sector's **growth**.	**A reformed Computer Misuse Act will provide the opportunity to not only put the UK's cyber industry on a level footing with global competitors, but introduce a truly world-leading legislative regime, driving growth and cementing the UK's position as a global cyber power.** The restrictions put in place by the Computer Misuse Act 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. Our research[2] found 91 per cent of businesses had been put at a competitive disadvantage, and 90 per cent believed that if the UK moved closer to what their ideal, world leading regime would be, then their organisation would experience significant productivity improvements, growth and resilience benefits. Mapped on to data about the current size of the UK's cyber security industry, this would amount to an additional £1.6 billion in annual sector revenue, and an added 6,200 mostly high-skilled jobs.
The Government will focus on advancing the **secure use of digital technologies**.	**A reformed Computer Misuse Act will help to enable the secure use of digital technologies.** Businesses and organisations – including the UK's critical national infrastructure – are increasingly dependent on digital technologies and online services to operate, innovate and grow. By preventing cyber security professionals from carrying out important threat intelligence research without fear of prosecution, the current legal system leaves ever more digitalised organisations at increased risk. A reformed Computer Misuse Act will better protect the UK at a time when our reliance on safe and resilient digital technologies has never been greater.

[2] 4 out of 5 cyber security professionals worry about breaking the law when defending UK, report finds — CyberUp (cyberupcampaign.com)

UK Government National Cyber Strategy commitment(s) or aim(s)	How a reformed Computer Misuse Act will help
NATIONAL GOAL An **innovative, prosperous digital economy**, with opportunity more evenly spread across the country and our diverse population.	
The Government will enhance and expand the nation's cyber skills at every level, including through a **world class and diverse cyber security profession** that inspires and equips future talent.	**A reformed Computer Misuse Act will lift a significant disincentive for aspiring cyber security researchers to join the profession.** Our research shows 4 out of 5 UK cyber security professionals worry about breaking the law when researching vulnerabilities or investigating cyber threat actors[3]. This actively discourages UK talent from pursuing a career in cyber. Changing the UK's cybercrime laws could be coupled with a positive and proactive information campaign to communicate that the Government values ethical cyber security research to help further de-mystify the profession.
Underpinned by Royal Charter, the UK Cyber Security Council will establish **professional standards and pathways** into and through a cyber career.	**A reformed Computer Misuse Act could incentivise cyber security researchers to seek chartered status and drive recognition of and for the profession.** In the CyberUp Campaign's proposed principles-based framework for a statutory defence[4], we set out that an actor's competence should be considered when determining whether an act (of unauthorised access) was defensible. Factors to assess competence can include an actor's level of qualification, certification or accreditation, and/or an actor's membership of a professional organisation and compliance with a code of ethics. This could involve tying an actor's eligibility for a statutory defence to the UK Cyber Security Council's Royal Charter, thus incentivising professionals to seek chartered status. The CyberUp Campaign is in ongoing discussions with the UK Cyber Security Council about how accreditation might be linked to a statutory defence.

[3] 4 out of 5 cyber security professionals worry about breaking the law when defending UK, report finds — CyberUp (cyberupcampaign.com)
[4] New Research: a proposal for a principles-based framework for the application of a statutory defence under a reformed Computer Misuse Act — CyberUp (cyberupcampaign.com)

UK Government National Cyber Strategy commitment(s) or aim(s)	How a reformed Computer Misuse Act will help
NATIONAL GOAL A more **influential and valued partner on the global stage**, shaping the future frontiers of an open and stable international order while maintaining our freedom of action in cyberspace	
The UK will continue to be a leading responsible and democratic **global cyber power**.	**A reformed Computer Misuse Act will enact a world-leading piece of cyber crime legislation, cementing the UK's position on the global stage.** A recent report[5] by the Criminal Law Reform Now Network (CLRNN) found that the Computer Misuse Act is "out of step" with equivalent European legislation. Although the UK is currently behind the curb, the report also highlights that the steps taken in other European states remains somewhat piecemeal. The CLRNN argue that reforming the Act to include a statutory defence would allow the UK to have a world-leading piece of cyber crime legislation, concluding "the UK has a unique opportunity to lead in this area." Efforts to reform cyber security legislation to put in place protections for private sector researchers are gaining traction in other democratic countries. Being the first mover would give the UK significant credibility and influence as a global cyber power. With the UK having left the European Union, and with a review of the Computer Misuse Act having already been undertaken by the Government, now is the time to take that opportunity with both hands and enact reform.

[5] http://www.clrnn.co.uk/media/1028/clrnn-1a-comparative-report-on-computer-misuse-defences.pdf