The Rt Hon Boris Johnson MP
Prime Minister
10 Downing St
Westminster
London
SW1A 2AA

29 June 2020

Dear Prime Minister,

We are group of businesses, organisations, academics and lawyers writing to you to call for reform of the Computer Misuse Act (CMA), which received royal assent 30 years ago today.

In 1990, when the CMA became law, only 0.5 per cent of the UK population used the internet, and the concept of cyber security and threat intelligence research did not yet exist.

Now, 30 years on, the CMA is the central regime governing cybercrime in the UK despite being originally designed to protect telephone exchanges. This means that the CMA inadvertently criminalises a large proportion of modern cyber defence practices.

The CMA prevents thousands of UK threat intelligence researchers from carrying out research to detect malicious cyber activity and prevent harm and disruption to organisations and citizens alike. In particular, section 1 of the Act prohibits the unauthorised access to any program or data held in any computer and has not kept pace with advances in technology. With the advent of modern threat intelligence research, defensive cyber activities often involve the scanning and interrogation of compromised victims' and criminals' systems to lessen the impact of attacks and prevent future incidents. In these cases, criminals are obviously very unlikely to explicitly authorise such access.

With less threat intelligence research being carried out, the UK's critical national infrastructure is left at an increased risk of cyber attacks from criminals and state actors.

But it does not have to be like this. Other countries – like the US and France – have in place far more permissive regimes, which provide well-intentioned cyber security researchers with legal certainty while retaining the ability to prosecute those seeking to abuse the system. In addition, this creates an advantage for competing cyber security sectors, which could see the UK lose out on as many as 4,000 additional high-skilled jobs by 2023 without reform.

The coronavirus crisis has brought to the fore just how reliant modern society is on secure and effective digital technologies, the delivery of essential services – like banking, utilities and health – particularly so. The government has committed to investing in the UK's digital and technology credentials and, as we move beyond the pandemic, we are calling on the government to make putting in place a new cyber crime regime part of this commitment. This will give our cyber defenders the tools they need to keep Britain safe.

Yours sincerely,

CREST

Digital Shadows

Demos

Cyber Defence Alliance

Cyber Security Research Institute

Ollie Whitehouse, CTO, NCC Group

F-Secure, UK MD, F-Secure Consulting

RaJ Samani, McAfee Fellow/Chief Scientist, McAfee

Rik Ferguson, Vice President Security Research, Trend Micro

Robert Dartnall, CEO, Security Alliance

Julian David, CEO, techUK

Phil Lynch, Managing Principal Security Consultant, Nettitude

Erhan Termukan, Principal Cyber Security Consultant

Daniel Cuthbert

Mark Deem, Partner at Cooley LLP

Abigail Bright, Practising barrister at Doughty Street Chambers

Dr John Child, Reader in Criminal Law and Co-Director of the Criminal Law Reform Now Network; University of Birmingham

Dr Audrey Guinchard, Senior Lecturer (Law), Director of Legal Skills, School of Law, University of Essex

Dr Oriola Sallavaci, Senior Lecturer in Law, School of Law, University of Essex

Professor Peter Sommer, Professor of Digital Forensics,  Birmingham City University, Expert Witness