It's time to CyberUp.

UPdate our laws, UPgrade our defences, UPskill our workforce

The CyberUP campaign is pushing for reform of the UK's outdated Computer Misuse Act 1990 (CMA). We need to update and upgrade the UK's cyber crime legislation to protect our national security and seize the economic opportunity presented by cyber professionals. The current legislative framework runs counter the UK's stated policy objective to promote public-private partnerships to combat cyber crime. The UK's cyber security industry is unable to deploy its full threat intelligence and investigative capabilities in the pursuit of national security. Reform is needed to:

• Amend the law to allow cyber security researchers acting in the public interest, or for the detection and prevention of crime to explain and justify their actions;

• Create clear legal definitions to ensure that cyber security researchers who reasonably believe they have authorisation to act can legitimately do so.

What do threat intelligence researchers do?

• Threat intelligence is undertaken for defensive purposes, to detect cyber-attacks, gain insight into attackers and victims, lessen the impact of incidents, and prevent future ones. Activities require the scanning, interrogation and (limited) interaction with compromised victims' and criminals' systems where owners have not, or are unlikely to, explicitly permit, or authorise, such access.

• For example, in recent years, threat intelligence researchers based in Bratislava, have worked with US-based organisation Censys to conduct a large-scale scan of the Internet and identified that an Asian mobile hardware and software manufacturer had been infected with Trojan malware. They were able to warn the manufacturer and prevent a global supply chain cyber attack, a clear example of the benefits of cyber threat intelligence research and investigation.

UPdate our laws - the Computer Misuse Act (CMA)

• The CMA criminalises individuals who attempt to access or modify data on a computer without authorisation. This often involves cyber-attacks like malware or ransomware attacks which seek to disrupt services, obtain information illegally or extort individuals or businesses. But the law in the UK has failed to keep pace with technological and market developments in the cyber security sector in the 30 years since it went on the statute books - when less than 0.5% of the population used the Internet.

• Section 1 of the Computer misuse Act 1990, prohibiting unauthorised access to computers, inadvertently criminalises a large proportion of cyber threat intelligence research and investigation by UK cyber security professionals. This is because the law punishes behaviour without any regard for the motivation of those carrying it out. There is no protection whatsoever for cyber security and threat intelligence researchers acting in good faith.

UPgrade our defences - protecting our national security

• 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 force UK companies to act with one hand tied behind their backs, significantly reducing their ability to supply rich threat intelligence to support national cyber defence operations. It puts the UK's national security at risk by impeding the ability of the private sector threat intelligence industry to assist law enforcement and intelligence agencies.

• The restrictions in gathering high quality actionable intelligence make it challenging to stay ahead of hostile threat actors and cyber criminals as governments alone cannot provide the required capacity and capabilities.

UPskill our work force - the economic case for reform

• Demand for cyber security services is growing rapidly. The global threat intelligence market is predicted to be worth 10bn by 2023.

• At present, non-UK threat intelligence firms operating under more permissive regimes - in the US and Israel - flood the market with high quality intelligence they have obtained using methods illegal under the UK's Computer Misuse Act. This puts the UK at a competitive disadvantage and leads to a lack of investment domestically in the necessary skills and capabilities - 1 in 5 UK companies at present report significant threat intelligence skills shortages.

• We estimate that reform would unlock growth in the UK cyber industry, leading to an additional 4,000 high-skilled jobs and increasing the sector's worth to around £500 million by 2023.

Reform

• It essential that reform takes place in a way that addresses the risk of misuse or exploitation of any legal changes by individuals with dishonest or criminal motives. We propose exploring options to create a regime of approval and accreditation of eligible providers, signing of an individually applicable strict ethics code of conduct, a commitment to maintain and share auditable logs of all activities and an obligation to pass on all intelligence and information to the appropriate authorities.

• We have been very clear that we do not support 'hacking back' - where a security researchers' activities entail the disruption or degradation of the investigated systems and infrastructure. These 'offensive' cyber activities should remain the prerogative of the state.

Threat intelligence in action - an example of when the CMA hindered national security

• NCC Group, one of the UK's biggest cyber security companies, and a leading member of the CyberUP campaign, worked jointly with the National Cyber Security Centre (NCSC) to research newly registered Internet domain names to identify potential malicious activities.

• One of the domains was found to point at an incompletely configured web server that showed a list of files, one of which included source code that made it obvious that the server belonged to an adversary with nefarious motives and offered insight into the adversary's motives, targets and methods.

• Because the files were directly, and thus publicly accessible from the web server, the access to them was de facto authorised, and therefore allowable, under the Computer Misuse Act. Through monitoring the adversary's activities, NCC Group was able to work out that the adversary was targeting an overseas UK diplomat, and could warn them and thus prevent harm in time.

• However, briefly after the diplomat had been warned, the adversary changed the configuration of their web server which now included a login screen. While the original web address to the server was still known to NCC Group, the existence of a login screen meant the files were no longer publicly accessible; instead, in line with the provisions of the Computer Misuse Act, authorisation was required to continue investigating the adversary. The lack of permission to do so meant that, to avoid breaking the law, NCC Group had to stop all investigative activities immediately.

Help us make reform of the Computer Misuse Act a reality by joining the CyberUp Campaign contact@cyberupcampaign.com

CyberUP