APPG ON CYBER SECURITY MEETING ON THE COMPUTER MISUSE ACT

Title: To review the Computer Misuse Act and debate whether or not it is still fit for purpose.

Chairman's welcome – Chairman welcomed everyone and encouraged debate. Aim is to meet with the Minister responsible when back from leave.
Present: Simon Fell MP (Chair), Lord Mackenzie of Framwellgate OBE, LL. B, the Rt Hon the Lord Arbuthnot of Edrom,
Apologies: Rt Hon Sir George Howarth MP, Lord West of Spithead, Tony Lloyd MP
Speakers:

1. Ollie Whitehouse, NCC

Ollie Whitehouse is Chief Technical Officer at NCC Group PLC, a UK headquartered cyber multinational, where he is responsible for the Group's technical strategy, research and development. A technology focused executive with over two decades of experience in cyber security working in consultancy, applied research and service delivery.

Ollie is also a research and science advisor to UK Government on cyber security and is also a non-Executive Director for PortSwigger a UK software company.

The context to the Act was in response to events in 1983 when two individuals broke into a royal inbox. The act came into force at the time of the First Gulf War to put it into context. Act was written to seek authorization from the system owner which made sense at the time. 30+ years later the world is radically different. Those changes which have happened could not have been foreseen and these represent the challenges.

We have bad actors as well as hostile states who are mis-using computing. Cyber Security is not the purview of police forces and government agencies alone. The Act constrains the private sector when responding to incidents. Customers want to understand who, what and why when an incident takes place. The Act forces NCC Group when responding to an incident to ask the perpetrator for permission to interact their machine in certain ways. There is much talk in our cyber security strategy about partnership between the public and the private sectors. Yet NCC sees competitors in the private sector behaving very different in other countries and the UK is therefore behind the game.

2. Daniel Cuthbert

Daniel is currently a global head of cyber security research and I've been a hacker for over two decades and sit on the Blackhat review board and also one of the original early contributors of the OWASP security project.

Part of a small club of people who have been convicted under the CMA, many years ago. Was looking at how criminals put together phishing websites. Clear that the law has not been kept up to date. Criminals do not care about the law and they know this and use it against law enforcement. The Act ties people's hand.

Also makes people shy of reporting bugs in case they are persecuted. The industry relies on the good will of bug hunter to report them. Many have been put off in the UK, people of good intent who are put off reporting legitimate bugs.

Law has struggled with the notion of "good intent". Looking forward to seeing how we can change this law.

3. Robert Carolina, BA, JD, LL.M

Robert Carolina is a Senior Fellow at Royal Holloway University of London, where he has taught legal and regulatory aspects of cyber security for more than two decades. Robert is a lawyer licensed to practice in England and the US who has spent his career specialising in the application of law to information and communications technologies. He is the author of the "Law and Regulation Knowledge Area" in the UK government-sponsored work CyBOK: Cyber Security Body of Knowledge.[1]

Act came into force just after my arrival in London in 1992, and I've always been intrigued since then.

Prosecution history and theory: seems to me that the Govt has shifted the focus of law enforcement away from what we think of as computer misuse and more towards historical crimes that we were familiar with before the Internet. The focus is more on where computers and the internet are simply an instrumentalities of some other crime such as blackmail or bank robbery.

In terms of legal risk management, I always warn my students do not annoy a sovereign state as they have more resources than you. They will also come after you! The CMA may have gained a reputation (fairly or unfairly) as the kind of legislation that can be used when the UK Government wants to go after somebody. Just a few year's after Daniel's brush with enforcement of the Act, BBC Click broadcast someone filming themselves which contravened the CMA. Showed the person taking over a botnet of 20,000 machines, all in the name of security education. The presenter did not explain that it was a criminal act and the consequences from law enforcement and government were…nothing to be heard[2]. Challenges of reforming the law: how do we distinguish between "legitimate" research and "criminal" hacks? This applies to academics and business equally. How do

[1] Available at www.cybok.org

[2] BBC - The Editors: Click's botnet experiment. For a contrasting view of the incident, see Carolina, "Opinion: BBC Click exploited world's poor and vulnerable"

you find a statutory provision to distinguish between hacking and research? Principle of "I know it when I see it" is difficult to apply and unpredictable in application. as it may be hard to find a public interest exception.
Might be better if criminal liability were somehow linked to harm caused, or risk of harm created.

Measuring what we are trying to achieve with this law. What is the harm to society that we are trying to minimise. The concern has shifted over time. If we look to US sentencing guidelines the length of sentence is linked to provable economic loss.

As we think about the harm, a significant change is the Internet of Things with an always connected world. People connect to the internet nowadays systems which have the capacity to threaten life and health as well as consumer technology which control systems that could injure people (especially vulnerable individuals) such as a thermostat. Those who hack them can threaten lives.

Open questions and discussion -
Simon Fell – what is the impact of this on UK plc? Are there are a group of people in the UK operating in this grey area or do we outsource?

DC – take traditional card skimming, working with the British Transport Police to solve cases is a grey area as we gain access to stolen credit card details. We cannot share the data with 3rd parties partly due to trust, the data is valuable but also stolen so cannot be shared.

OW – clear that competitors use this data and sell it on to other private sector firms.

Lord Arbuthnot – took part in the original debates. Clearly out of date and something has to happen to it. No-one has come up with the new law needed.

GDPR is based on concepts of consent. No-one really understands the consequences to ticking yes to cookies and to agreeing to advertising or data sharing requests. Consent seems to be an improper basis for the legislation. Need something else, like Azimov's 3 rules of robotics, any suggestions, what do other countries do?

OW – we have Dr John Child in the meeting, Reader in Criminal Law at Birmingham Law School, and Director of the Criminal Reform Network (CLRNN - Criminal) that published a set of recommendations for the new laws.

Dr John Child – The Network is a Research Council funded group that has looked at the CMA – 3-year project, based on 35 different authors from academia, legal practice (solicitor and barristers, including CPS), journalists, computer expert witnesses and investigators, as well as those from cyber security. The report – available here open-access – was launched at Westminster in 2020. CMA ties the hands of those who are trying to combat cyber crime.

Recommended a number of changes, across offences, defences, prosecutorial and sentencing guidance. On defences/exemptions, it is necessary to clarify the enforcement exemptions in section 10 to cover Court Orders etc.; but most importantly, the report recommends the creation of a new public interest defence (modelled in line with overlapping regulations of data protection in the DPA 2018. Public interest or consent defences are common in criminal law (e.g. theft, criminal damage), but are narrowed considerably in the DPA 2018 in a way that they also recommend for computer misuse: The defendant must prove (reverse burden) that what they did was in the public interest (objective standard), so simple assertions or beliefs in public interest would not be sufficient. Believes that the recommendations would provide the assurance for 'good actors' (cyber security, researchers, etc.); legal consistency and coherence (both across domestic offences, and international obligations); whilst providing robust offences to tackle 'bad actors'.

SF – looking at where other countries have updated their legislation, are there any examples.

Dr John Child – no, less call for these types of defences. Other European countries have narrower offences (e.g. requiring an intention to cause harms etc.) and so additional defences are not as necessary – though some, notably the Netherlands, have defences. Our range of offences are much wider, so we catch more people. Options are to narrow those offences. The idea of pitching for a dramatic narrowing of offences gives no wriggle room and would be out of step with the DPA 2018 – better, instead, to do the work with defences that put a burden on the defendant to demonstrate a public interest in their actions.

OW – 17000 reported cases of computer misuse of which 54 went onto prosecution in 2019.

DC – cases are technical, in his case has to explain how the internet works. CPS tends to shy away from the more technical cases, esp. when the criminals are not in the UK. Struggle with criminal gangs who have spread their bases across several European countries.

RC – jurisdiction is a key point. A majority of these cases would have been generated outside the UK. This means triggering mutual assistance and this generates costs and delay. If there is some other crime that has produced harm, the CPS will go for this. Thirdly, explaining how the Internet worked 15 years ago was one thing, 30 years ago a suspect had to explain how software worked! I tend to disagree with the opinion that "The law does not keep pace with technology." I believe instead that the law is reasonably flexible, but lawyers fall behind technology changes and by extension judges fall behind. [Clarification after-the-fact: Law is misapplied when lawyers do not understand the environment that confronts them.]

Simon Fell – my background is fraud prevention. The UK fraud prevention system triages through the City of London police and then the NCA who try to connect the dots. Not fantastic, what does the legislative framework look like?

OW – yes, the sharing of this data is encouraged within UK law enforcement agencies such as the NCA.

DC – worked for Monzo and on the first fraud case, did the normal stuff to report it. Put together a dossier on the case and could not get it investigated. Never picked up and the criminal got away with it.

Daniel Dresner – found that criminals are well up the regulatory side of things. Is the Online Harms bill, ever-shrinking, an opportunity?

RC – Would point out that the Bill addresses the kind of harms that do not easily map onto a discussion on computer misuse. The harms addressed by the Bill and referred to are very self-evident. Those types of cyber crimes are about the criminals not the computers.

The DCMS paper excluded financial predation from the bill.

Looking at where the CMA should focus is to fill gaps in the law because it developed over the centuries without computers. In *The Cuckoos Egg (1989)*, the author, Clifford Stoll, was constantly criticized for spending time investigating a computer intrusion crime with no obvious harm. [He subsequently uncovered the first known international Internet spy ring.] Internationally one thing that is viable is in the European Directive which states that everyone in our club is required to define the number of crimes, you do not need to define activity that causes only de minimis harm or risk. Part of the problem with the CMA is a feature: a strategic choice by law enforcement to lobby Parliament to adopt a hair trigger approach.

OW- echoed Robert's comment on de-coupling the computer. Take Xenobots[3] now a new area of computing, this sector moves quickly and laws need to be agile.

Prof Keith Mayes – seems to be a practical need for good people to do things without consent that look like criminal things. A good person would highlight an issue, a bad person would not broadcast the vulnerability which is not obviously doing something bad. It is like preparing for a burglary is not necessarily a crime until the burglary happens. Legitimate users should have a get out of jail free.

OW – Successful Dutch prosecutions have been based on this idea, looking at whether the person shared the vulnerability and to the extent they leveraged the vulnerability.
RC – these comments provide a wonderful case for the licensure of cyber security activities. Moves the question into a new field as some kind of organisation is then needed to police good behaviour by licensed professionals. CREST[4] has got some of that under control.

[3] Xenobots: First living robots created from stem cells - CNN
[4] CREST (crest-approved.org)

Dr John Child – the idea of carving our exemptions is appropriate for State Authorities, dangerous outside of the public context. Caution against defining ideas of harms too closely as it becomes out of date quickly.
Need to look at people who are making claims and gaining access. Once you have gained access to someone else's computer you must explain yourself adequately to a jury, if not you are open to prosecution – this is the basis of a public interest defence. This goes further than the current law which criminalises you from the start, leaving 'good actors' to rely on the uncertainties of prosecutorial discretion; and in most cases, simply to stop doing the securities work for fear of prosecution/for lack of insurance.

James Eaton-Lee – lots of instances outside of the UK of the uses of cyber security legislation to remove rights. In terms of future proofing, cyber law needs to be inoculated against the removal of rights.

OW – worth consideration as reform happens.

RC – if we are talking about reigning in a Govt that is out of control, will not be solved in the context of computer legislation.

Robin Oldham – no-one is arguing against reform. How much of computer crime is just crime committed using a computer and how much is genuine computer crime that could not be done in a different way?

DC – just crime! Most crime against banks is now performed on a computer, just criminals.
RC – Main area where the CMA continues to have currency are those areas where we see a risk to good order in society that are not appropriately addressed in other areas of law. Comes back to the concept of trespass.

When we look at state sponsored intrusions, we see actions that do not merit a kinetic response. We can say that it is a violation of domestic criminal law – computer misuse legislation.

OW – CMA is used when no other law can be used. Some criminals break in and then sell the access to others to trespass.

Conclusions – Simon Fell thanked the speakers and other contributors. Will be taking the comments on board and will have a conversation with the Security Minister.

Next meeting – March – Artificial Intelligence