RAPID7

Rapid7 Position on the Computer Misuse Act 1990

June 2021

In May 2021, the UK Home Office opened a Call for Information[1] on the Computer Misuse Act 1990 (CMA)[2], the UK's anti-hacking law. This paper focuses on Rapid7's positions on issues related to legitimate cyber security activity and authorisation. Specifically, Rapid7 recommends the Home Office 1) retain helpful aspects of the CMA; 2) clarify protections for defensive security tools; 3) avoid authorising private sector hack back; 4) provide clearer protections for independent security research; and 5) clarify the definition of "authorisation".

Retain helpful aspects of the CMA

The CMA was passed in 1990 and since then has been updated multiple times (through amendment bills in 1998, 2005, and 2008, and through the Police and Justice Act 2006 and by the Serious Crime Act 2015). Despite these updates, many critics assert that the legislation is out of date and in need of reform in a variety of ways. Rapid7 believes anti-hacking laws in general are useful and necessary to deter malicious attacks, though it is always important to work to ensure such laws are not overbroad, vague, or misused. As detailed below, Rapid7 agrees the CMA has areas where updates to the legislation would be welcome, but the CMA is also not unfit for the purpose of deterring and prosecuting malicious attacks in its current form.

We appreciate that the CMA contains only criminal causes of action, not civil. In our view, this helps avoid aggressive or inappropriate uses of the law by self-protective technology owners and operators, which can result in a chilling effect on security research.[3] We urge the Home Office to retain this aspect of the CMA. We also appreciate that several offenses under the CMA require evidence of harm or malicious intent, and urge against weakening these standards, however these standards should be considered in

[1] https://www.gov.uk/government/consultations/computer-misuse-act-1990-call-for-information
[2] https://www.legislation.gov.uk/ukpga/1990/18/contents
[3] In contrast, US anti-hacking laws like the Computer Fraud and Abuse Act and Section 1201 of the Digital Millennium Copyright Act include private causes of action independent of government enforcement, requiring discretion from both prosecutors and private parties to avoid over-aggressive use. 18 USC 1030(g), 17 USC 1203.

Section 1 and 3A(2) (see below for more information).

We also appreciate that the text is relatively easy to understand - this should not be underestimated as computer laws can have a tendency to be overly complex and hard to interpret, which makes it harder for individuals to ensure compliance.

While the legislation has received criticism for its lack of definitions, we believe the decision to *"not provide a definition of a computer because rapid changes in technology would mean any definition would soon become out of date"*[4] is pragmatic and reasonable. Conversely, the lack of a clear definition for "authorisation" creates a lack of clarity in what activity specifically is being prohibited. We urge the Home Office to clarify this with clearer language around expectations for authorisation (see below for more details).

Protect legitimate security testing tools

Rapid7 urges the Home Office to consider clarifying Section 3A(2) to ensure it protects tools, code, and other dual use technologies that are used defensively to test security. This issue is acknowledged by the Crown Prosecution Service guidelines on Section 3A(2), and we suggest the Home Office draw from the guidelines to provide clear protection[5] for "articles" supplied for security purposes.

An important part of a robust security programme is testing your own defences and understanding the impact of an attack on your systems[6]. This activity is so standard in security that it is a requirement of many cybersecurity standards and regulations around the world, including the Payment Card Industry Data Security Standard[7]. In order to conduct this kind of testing, security professionals need testing tools that enable them to emulate the activity of attackers, as well as exploit proof-of-concept code to test whether their own assets are vulnerable.[8]

These tools are often shared collaboratively within the security community, or sold commercially. Some of these tools may be made widely available as open source software to help ensure a broad range of organisations (not just well-resourced organisations) have access to these tools to defend themselves, and so that a community of contributors can help ensure the tools stay up to date with the latest attacker trends and capabilities. The purpose and value of open source penetration testing programs are well understood across the security community, yet by nature of them being open source and widely available,

[4] https://www.cps.gov.uk/legal-guidance/computer-misuse-act

[5] https://www.cps.gov.uk/legal-guidance/computer-misuse-act

[6] https://www.ncsc.gov.uk/guidance/penetration-testing

[7] https://www.pcisecuritystandards.org/

[8] Computer programs, code, and electronic data are covered by the CMA's definition of 'articles' at section 3A(4). This definition makes no distinction with regard to whether the article has a dual use for testing or auditing hardware and software for security purposes.

it is impossible to say that these defensive tools could not be used by malicious actors for nefarious purposes.

The same issue applies to proof-of-concept exploit code, which may be widely shared to help others in the security community investigate how a vulnerability may be exploited in practice, and to test whether one's own assets are vulnerable to the exploit (or if a mitigation will successfully prevent exploitation). This is a very standard part of how the security community works together to build collective knowledge that enriches the whole and advances security. While the intent of the development and sharing of the code is defensive, there is always a risk that exploit code could be accessed and used by malicious actors - yet this makes the wide availability of testing tools all the more important so organisations can identify and mitigate their exposure.

To ensure that the Computer Misuse Act does not inadvertently prohibit or chill defensive use of dual use technologies and code which are helpful for strengthening cybersecurity, we suggest the Home Office establish clearer protections under Section 3A(2)[9]. The Home Office should consider modifying 3A(2) to exempt "articles" that are:

1. *Capable of being used for legitimate purposes[10]; and*
2. *Intended by the creator or supplier of the article to be used for a legitimate purpose; and*
3. *Widely available[11]; unless*
4. *The article is deliberately developed or supplied for the sole purpose of committing a CMA offence.*

It is worth noting that the CMA would still retain 3A(1) as a means to prosecute those who supply articles with the intent that it will be used to commit CMA offenses.

Avoid authorising private sector hack back

Some proposals for computer crime reform make an argument that security professionals should be able to interrogate or interact with third party systems engaged in an attack, or even take action to deter or stop attacks. This sounds like an argument for the authorisation of private sector hack back activities, which is hugely concerning and will likely lead to a wild west situation where organisations hire digital gunslingers to fight battles for them with little oversight or repercussions for unintended harms. There are a number of reasons that private sector hack back is not practical, as detailed below[12].

[9] "3A(2) A person is guilty of an offence if he supplies or offers to supply any article believing that it is likely to be used to commit, or to assist in the commission of, an offence under section 1, 3 or 3ZA."
[10] See the discussion of dual use articles in the Crown Prosecution Service guidance for section 7 of the Fraud Act of 2006, https://www.cps.gov.uk/legal-guidance/fraud-act-2006#a13
[11] https://www.cps.gov.uk/legal-guidance/computer-misuse-act#_Toc532920184
[12] https://hbr.org/2017/05/why-companies-shouldnt-try-to-hack-their-hackers

For the purposes of this document, we understand hack back to mean an organisation taking action against a cyber-attacker on technical assets or systems not owned by the person taking action or their client. The action may be taken to neutralise the threat, recapture lost data, better understand the nature of the attack, or as an act of revenge. We do not include hacking activities undertaken by or on behalf of the government in this classification, only those undertaken specifically for private sector entities. Rapid7 does not support hack back for the following reasons:

Impracticalities of attribution and application

One of the most widely stated and agreed upon tenets in security is that "attribution is hard." We can go further – in many cases, it is essentially impossible to know for certain that we have accurately attributed an attack. Even when we find indications that point in a certain direction, there is no way to ensure they are not red herrings intentionally planted by the attacker to either throw suspicion off themselves, or to specifically incriminate another party for some purpose. We like to talk about "digital fingerprints," but the reality is that there is no such thing: in the digital world there is nothing that cannot be spoofed or obfuscated with enough time, patience, skill, and resources. Attackers are constantly evolving their techniques to stay one step ahead of defenders and law enforcement, and the emergence of deception capabilities is just one example of this. So being certain we have the right actor before we take action is extremely difficult.

In addition, where do we draw the line in determining whether an actor or computing entity could be considered a viable target? For example, if someone is under attack from devices that are being controlled as part of a botnet, is it reasonable for them to take action against those devices in order to neutralise the threat against themselves? Surely those devices – and their owners – are as much victims of the attacker as the target of the attack. Rapid7's Project Heisenberg[13] honeypots often pick up traffic from legitimate organisations whose systems have been compromised and leveraged in malicious activity[14]. Action mistakenly taken against one of these entities could be catastrophic.

Motivations, which are often unclear or easy to misunderstand, should surely also be taken into account. For example, research projects that scan ports on the public-facing internet do so in order to help others understand the attack surface so exposure and opportunities for attackers can be reduced. This activity is benign and often results in security disclosures that have helped security professionals reduce their organisation's risk. However, it is not unusual for these scans to encounter a perimeter monitoring tool, throwing up an alert to the security team. What would happen if an organisation saw the alerts and

[13] https://www.rapid7.com/research/project-heisenberg/
[14] https://www.rapid7.com/c/icer-ftse/?x=Tj1DVo

decided to take a “shoot first and ask questions later” approach – would the researcher end up being attacked for undertaking a research project designed to advance better cybersecurity?

Impracticalities of limiting reach and impact

The internet does not operate in neatly defined and clearly demarcated boundaries. If we take action targeted at a specific actor or group of actors, how can we be sure that we will not unintentionally impact innocent others? Many people have likened hack back to the idea of a homeowner defending their property against an intruder. They evoke images of malicious, armed intruders breaking into your home to do you and your loved ones harm. They call to you to arm yourself and stand bravely in defense, refusing to be a victim in your own home. It’s an appealing idea; however, the reality is more likely to be akin to standing by your fence spraying bullets out into the street hoping to get lucky and stop an attacker as they flee the scene of the crime. With such an approach, even if you do manage to reach your attacker, you’ll almost certainly cause terrible collateral damage too.

Rapid7 believes the possibility of unintended consequences should not only concern lawmakers, they should also disincentivise participation. Organisations that believe they can avoid negative outcomes in the majority of cases need to understand that even just one or two errors could be extremely costly. Imagine for example that a high-value target organisation, e.g. a bank, undertakes 100 hack backs per year and makes a negatively impactful error on two occasions. A two percent fail rate may not seem that terrible; however, if either or both of those errors resulted in compromise of another company or harm to a group of individuals, the hack-backer could then see themselves tied up in expensive legal proceedings, reputational damage, and loss of trust. Attempts to make organisations exempt from this kind of legal action are problematic as it raises the question of how we can spot and stop abuses.

The potential negative consequences of a hack back gone awry could be far reaching. We frequently discuss damage to equipment or systems, or loss of data, but in the age of the Internet of Things, there is always the potential that negative consequences could include physical harm to individuals. And let’s not forget that cyberattacks can be considered acts of war.

Impracticalities of providing appropriate oversight

To date, proposals to legalise hack back have been overly broad and non-specific about how such activities should be managed, and what oversight would be required to ensure there are no abuses of the system. Indeed, creating a framework and system for such oversight is completely impractical and costly. Who would run it? How would it be funded? How would accountability and oversight be guaranteed to avoid abuses? Who will determine where the line should be on what action is acceptable?

When the UK government takes action against attackers, it is with a high degree of oversight and accountability. They must meet a very stringent burden of proof for attribution, and even when that has been done, there are strict parameters determining the types of targets that can be pursued, and the kind of action that can be taken. Private sector organisations may be contracted by the government to participate in these operations, but again, this will always occur under the necessary oversight. Authorising the private sector to participate in these activities without this oversight makes a mockery of the checks and balances in place for the government and is likely to lead to unintended harms.

Impracticalities of legal liability and jurisdiction

While the internet is a borderless space accessed from every country in the world, each of those countries has its own legal system and expects its citizens to abide by it. It would be very risky for companies and individuals who hack back to avoid running afoul of the laws of another country and international law.

When national governments take this kind of action, it tends to occur within existing international legal frameworks and under some regulatory oversight, but this would not apply in the private sector, begging the question of where the liability rests. For example, what if a company hacks back and accidentally hurts another company or individual? The company that hacked back could incur expensive legal proceedings, reputational damage, and loss of trust. Making organisations exempt from this kind of legal action around unintended consequences is problematic. How could we spot and stop accidental or intentional abuses of the system? Should the government authority that approves private sector entities to participate in hack back instead bear the liability? This leads us back to the issues around the impracticalities of applying oversight, detailed above.

It is also worth noting that once one major power authorises private sector hack back, other governments will likely follow and legal expectations or boundaries may vary. How would the UK government respond when its citizens are being attacked as part of a private sector hack back gone wrong?

Inequalities of applicability

Should a viable system be developed, and hack back authorised, effective participation is likely to be costly as it will require specialist skills. Not every organisation will be able to participate. If the authorisation framework is not stringent, many organisations may try to participate with insufficient expertise, which is likely to be either ineffective or damaging, or potentially both. However, there are other organisations that will not have the maturity or budget to participate even in this way.

These are the same organisations that sit below the "cybersecurity poverty line"[15] and cannot afford a great deal of in-house security expertise and technologies to protect themselves – in other words, these organisations are already highly vulnerable. As organisations that do have sufficient resources start to hack back, the cost of attacking these organisations will increase. Profit-motivated attackers will eventually shift towards targeting the less-resourced organisations that reside below the security poverty line. Rather than authorising a measure as fraught with risk as hack back, we should instead be thinking about how we better protect these vulnerable organisations, for example, by subsidising or incentivising security hygiene.

Reducing uncertainty for security researchers

Independent security research comes in many forms and flavours, but at its core, good faith, legitimate security research shares a common goal of protecting technology users from cyber-risks. By increasing the general awareness of how technical systems can be exploited, we can build better defences against attackers and deploy mitigations to reduce risk. This offers a significant benefit to society, yet there are claims that security research is being chilled by the CMA[16] as it makes no provision for legitimate, good faith testing.

While Section 1(1) does address intent, it makes no mention that the intent must be malicious, only that the actor intended to gain access without authorisation:

1 Unauthorised access to computer material.

> *(1) A person is guilty of an offence if—*
>
> *(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer, or to enable any such access to be secured;*
>
> *(b) the access he intends to secure, or to enable to be secured, is unauthorised; and*
>
> *(c) he knows at the time when he causes the computer to perform the function that that is the case.*

You could perhaps make an argument here that a good faith researcher hopes not to gain access as they would prefer systems not to be exposed to attack; however, the actions taken to test whether this is the case would be designed to gain access, so it is unlikely this argument would be persuasive as a defence.

How this works in practice - vulnerability research

[15] https://duo.com/blog/rising-above-the-security-poverty-line

[16] https://www.cyberupcampaign.com/about

Vulnerability research is the practice of testing software or systems to identify potential flaws, bugs or misconfigurations that provide opportunities for malicious actors to gain access to the systems themselves or the information they may handle. The goal of good faith vulnerability research is to disclose the information to the owners or operators of the technology so they can take steps to mitigate the risk for their end users. Further, information on known vulnerabilities is shared publicly to build a corpus of knowledge that enables others to avoid the same pitfalls in the future.

The UK Government's recent Code of Practice for consumer IoT security[17] appears to acknowledge the value of security research in its inclusion of vulnerability disclosure policies and security patching as its second and third principles. Both activities hinge on the disclosure of discovered security vulnerabilities in products, which often results from independent security research. Conducting this kind of research is less controversial when IoT devices can be bought and tested in non-production environments. Yet when researchers want to look at the back-end systems supporting these IoT offerings, or their apps - which often control functionality and store sensitive data - this testing would likely violate the CMA. This extends to identifying vulnerability in any other websites, software, or systems on the internet.

How this works in practice - port scanning

This issue also applies to some forms of port scanning[18], an activity undertaken to investigate, analyse, and measure the exposed attack surface of the internet. For example, when investigating the exposure landscape, security researchers may look for whether the Simple Network Monitoring Protocol (SNMP)[19] is being exposed as it can be a good source of information for would-be attackers. As the protocol has been around for decades, there are a number of known vulnerable versions, so researchers often want to understand whether organisations are continuing to use these vulnerable versions, or if they are moving to more secure versions and reducing their exposure to attack.

A notorious aspect of SNMP is that it may use either 'public' or 'private' community strings for authentication. Public strings are generally known and easy to find and will give requesters read-only access to sensitive information. In order to understand and document exposure, security researchers want to be able to identify whether users are leveraging the more secure private community string, or whether they are leaving data exposed by leaving the public community string in place. In order to test for

[17] https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security

[18] https://whatismyipaddress.com/port-scan#:~:text=Port%20Scanning%20is%20the%20name,by%20hackers%20to%20target%20victims.

[19] https://www.advancedcyber.co.uk/it-security-blog/what-is-snmp-and-is-it-secure#:~:text=SNMP%20is%20without%20a%20doubt,authentication%20is%20almost%20non%2Dexistent.

this, researchers would need to prompt the protocol to take an action, in violation with Section 1 of the Computer Misuse Act. Even automated mass scanning where no sensitive data is being viewed or captured, would be considered a violation.

Similarly some users set up certain ports to automatically take an action when they are contacted. For example, a redirect from one port to another. In this instance, if a researcher were to ping the port, it could trigger an action even though that was not the researcher's intention or expectation.

Possible approaches to a security research exemption

Creating a carve out for good faith, legitimate security research is challenging. We must avoid inadvertently creating a backdoor in the law that provides a defence for malicious actors, or permits types of activity that can create unintended harms. As legislators consider some options of paths forward on this, we strongly recommend considering the following questions:

- **How do you determine whether research is legitimate and justified?** Some considerations include whether sensitive information was accessed, and if so, how much - is there a threshold for what might be acceptable? Was any damage or disruption caused by the action? Did the researcher demand financial compensation from the technology manufacturer or operator?

  For example, for a similar effort to update the Computer Fraud and Abuse Act (CFAA) - the U.S. equivalent of the CMA - Rapid7 proposed the following language be considered to indicate what is understood by "good faith security research":

  > *"The term "good faith security research" means good faith testing or investigation to detect one or more security flaws or vulnerabilities in software, hardware, or firmware of a protected computer for the purpose of promoting the security or safety of the software, hardware, or firmware.*
  >
  > *(A) The person carrying out such activity shall*
  >
  > *(i) carry out such activity in a manner reasonably designed to minimise and avoid unnecessary damage or loss to property or persons;*
  >
  > *(ii) take reasonable steps, with regard to information obtained without authorisation, to minimise the information the person obtains, retains, and discloses to only that information which the person reasonably believes is directly necessary to test, investigate, or mitigate a security flaw or vulnerability;*
  >
  > *(iii) wait a reasonable amount of time before publicly disclosing the security flaw or vulnerability, taking into consideration the following:*

> > > *(I) the severity of the vulnerability,*
> > >
> > > *(II) the difficulty of mitigating the vulnerability,*
> > >
> > > *(III) industry best practices, and*
> > >
> > > *(IV) the willingness and ability of the owner of the protected computer to mitigate the vulnerability;*
> >
> > *(iv) not publicly disclose information obtained without authorisation that is*
> >
> > > *(I) a trade secret without the permission of the owner of the trade secret; or*
> > >
> > > *(II) the personally identifiable information of another individual, without the permission of that individual; and*
> >
> > *(v) does not use a nonpublic security flaw or vulnerability derived from such activity for any primarily commercial purpose prior to disclosing the flaw or vulnerability to the owner of the protected computer or the [government vulnerability coordination body].*
>
> *(B) For purposes of subsection (A), it is not a public disclosure to disclose a vulnerability or other information derived from good faith security research to the [government vulnerability coordination body]."*

- **What happens if a researcher does not find anything to report?** Some proposals for reforming the CFAA have suggested requiring coordinated disclosure as a predicate for a research carve out. This only works if the researcher actually finds something worth reporting. What happens if they do not - is the research then not defensible?

  For the language proposed for the CFAA, Rapid7 addressed this issue as follows:

  > *"(C) Nothing in subsection (A) shall be construed to prohibit or require public disclosure of security flaws or vulnerabilities derived from good faith security research."*

- **Are we being consistent with other areas of legislation?** For example, does increasing authorities for security researchers align with privacy legislation? Do specific requirements or balancing controls need to be indicated to ensure alignment, such as those proposed in the language above.

Clarify authorisation

At its core, the CMA effectively operates as a law prohibiting digital trespass and hinges on the concept of authorisation. Four of the five classes of offenses laid out in the CMA involve "unauthorised" activities:

1. Unauthorised access to computer material.

2. Unauthorised access with intent to commit or facilitate commission of further offences.

3. Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.

3ZA.Unauthorised acts causing, or creating risk of, serious damage

The challenge here is that the CMA does not define authorisation (or its lack) or detail what authorisation should look like. As a result, it is hard to understand where the legal line is truly being drawn in the context of the internet, where lengthy terms of service are not read or understood by many users, and data and services are frequently publicly accessible for a wide variety of novel uses. Many take a view that if something is made accessible in public spaces on the internet, authorisation to access it is inherently granted. In this view, the responsibility lies with the owner/operator to ensure that if they do not wish something to be accessed, they are not making it publicly available.

That being the case, the question becomes how systems owners/operators can indicate a lack of authorisation for accessing systems or information in a way that scales while still enabling broad access and innovative use of online services. In the physical world, we have an expectation that both public and private spaces exist. If a space is private and the owners do not want it to be accessed, it is common for them to indicate this through signage or physical barriers (walls, fences, gates etc). Yet there is currently no accepted standard way for owners and operators to set out a 'No Trespassing' sign for publicly accessible data or systems on the internet that truly serves the intended purpose.

While a website's Terms of Service (TOS) can be legally enforceable in some contexts, the Home Office should be skeptical that violation of TOS alone should not qualify as an "unauthorised act." TOS are almost always ignored by the vast majority of internet users, and ordinary internet behavior may routinely violate TOS (such as using a pseudonym where a real name is required). Reading TOS also does not scale for internet-wide scanning, as in the case of automated port scanning and other services that analyse the status of millions of publicly accessible websites and online assets. In addition, if TOS is "authorisation" for the purposes of the CMA, it gives the author of the TOS the power to define what is and is not a hacking crime under CMA section 1. It is notable that multiple US cases have rejected the notion that TOS violations alone qualify as "exceeding authorisation" under the CFAA,[20] creating a split in US courts. In its recent Van Buren decision, the US Supreme Court noted that if TOS violations alone

[20] "Several other courts, including the Second, Fourth, and Ninth Circuits, have more narrowly interpreted "without authorisation" and "exceeds authorised access," based on an understanding that the CFAA's central purpose is to criminalise hacking. These courts apply CFAA liability only to those who lack any authorisation to access a computer or website or those who are "authorised to access only certain data or files" but access "unauthorised data or files." As a result, the narrow view exempts from CFAA liability those who have merely violated ToS agreements." https://crsreports.congress.gov/product/pdf/LSB/LSB10423/6 , pgs. 3-5.

qualify as an “unauthorised act” for computer crime purposes, “then millions of otherwise law-abiding citizens are criminals.”[21]

To address this lack of clarity, the CMA needs a clearer explanation of what constitutes authorisation for accessing technical systems or information through the internet and other forms of connected communications.

*   *   *

[21] Van Buren v. United States https://www.supremecourt.gov/opinions/20pdf/19-783_k53l.pdf No. 19-783, 593 U.S. _ (June 3, 2021)