Legitimate cyber security activities in the 21st century

Assessing the current consensus of what should constitute legitimate cyber security activity under a reformed UK Computer Misuse Act 1990

August 2022

Executive Summary

The CyberUp Campaign has been asking the UK Government to reform the Computer Misuse Act 1990 (CMA) to include a statutory defence since 2017. This is because we see that some cyber security activities that today would be classed as unauthorised access to computer material – currently illegal and without defence – could be justified if the law were updated in line with the evolution of cyberspace in the 21st century. Specifically, the UK cyber security sector is hampered today by the Computer Misuse Act in two main areas:

- **Vulnerability research** i.e. the activity of finding vulnerable systems and security vulnerabilities in systems and software.
- **Cyber threat intelligence** i.e. the activity of identifying and tracking our cyber adversaries and their victims.

By permitting these activities, we argue, the Government can enable a swathe of benefits including improved cyber resilience of the nation and its allies and accelerated growth of the UK's domestic cyber security sector.

In response to understandable questions about how a statutory defence – a well-established legal principle – would work in practice in the cyber context, we previously developed a Defence Framework, which proposed a set of principles that could be applied in any case of unauthorised access to make a judgment on whether such an action was defensible.

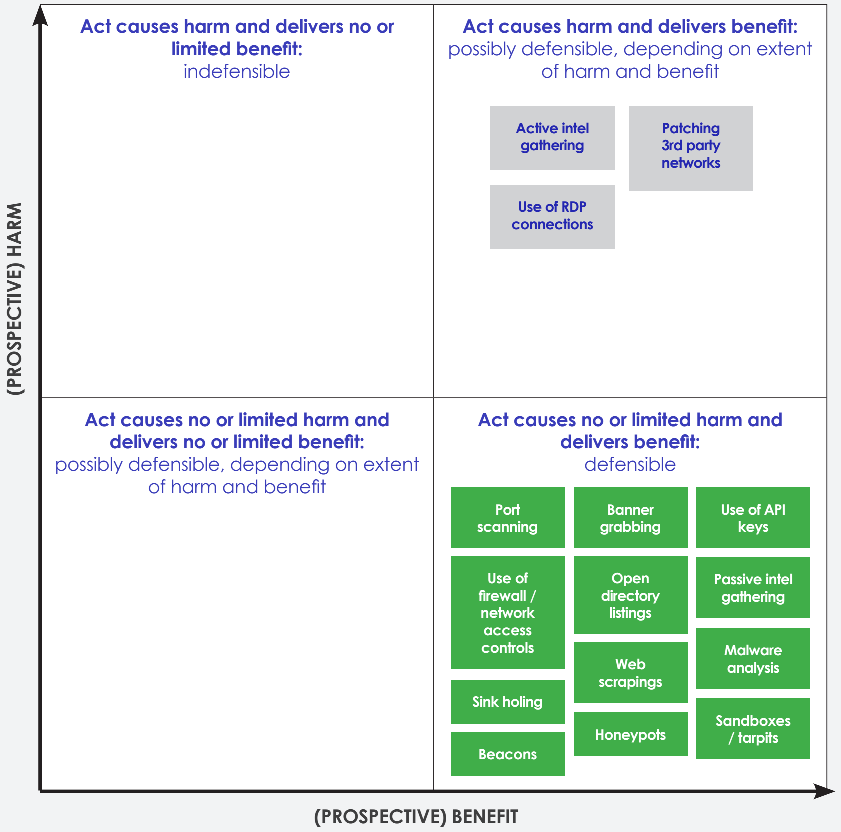
We believe this principles-based approach is the correct one. This is because trying to set out in legislation or guidance specific activities and techniques involving unauthorised access that should be defensible would quickly become outdated and thus be unsustainable. A principles-based approach guards against this as cyber security techniques and technology evolve over time.

Nevertheless, in this report we establish, through consultation with UK cyber security professionals, that a significant degree of consensus already exists about what are legitimate and illegitimate instances of unauthorised access. This consensus should offer additional confidence to policy makers that applying a statutory defence in practice is possible, and that it is therefore also possible for the courts to adjudicate clearly which behaviour and acts should continue to be punishable as criminal offences.

There remain grey areas where the question of what is legitimate remains contested by some. This research paper does not seek to offer a definitive final view on some of these edge cases; they will need to be subject to further consultation and discussion as the policy formation process develops. But, a focus on these edge cases should not be allowed to cloud the key finding of this report: that consensus exists on which acts of unauthorised access should be defensible.

Question 1: Harm / benefit profile

Respondents were asked for their views on the harm / benefit* profile of the most common cyber security activities and techniques deployed in the course of vulnerability and threat intelligence research which require unauthorised access.



Act causes harm and delivers no or limited benefit:
indefensible

Act causes harm and delivers benefit:
possibly defensible, depending on extent of harm and benefit

- Active intel gathering
- Patching 3rd party networks
- Use of RDP connections

Act causes no or limited harm and delivers no or limited benefit:
possibly defensible, depending on extent of harm and benefit

Act causes no or limited harm and delivers benefit:
defensible

- Port scanning
- Banner grabbing
- Use of API keys
- Use of firewall / network access controls
- Open directory listings
- Passive intel gathering
- Web scrapings
- Malware analysis
- Sink holing
- Honeypots
- Sandboxes / tarpits
- Beacons

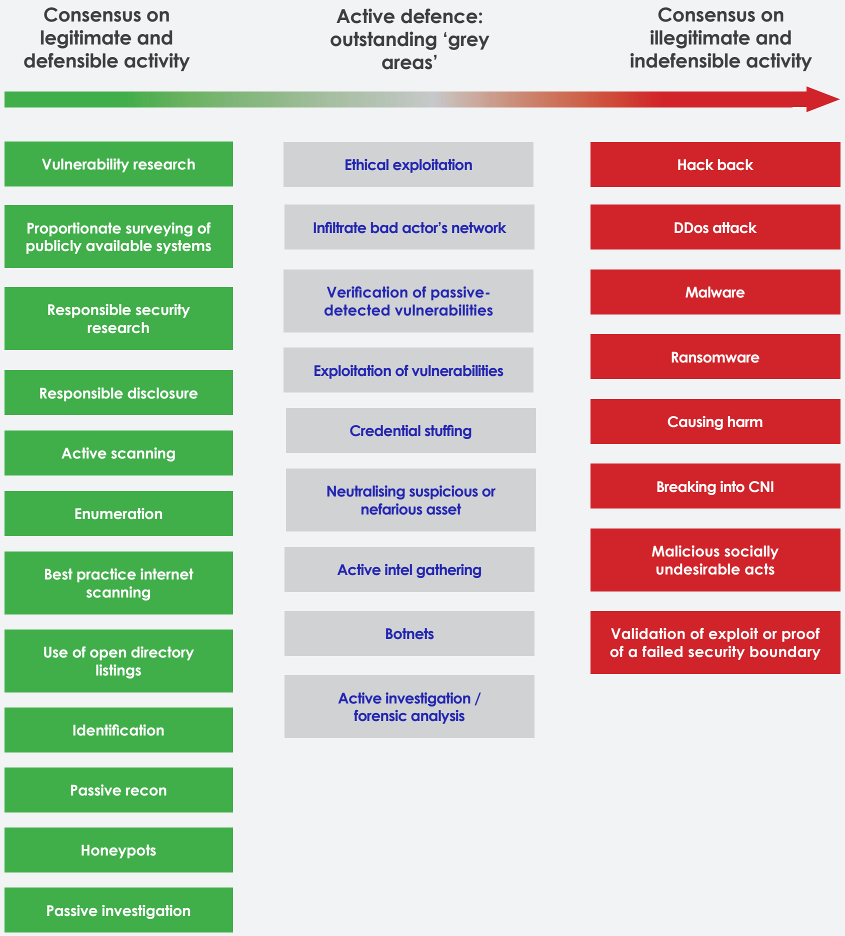
(PROSPECTIVE) HARM

(PROSPECTIVE) BENEFIT

Definitions of what constitute 'harm' and 'benefit' are outlined in section 1.3 of this paper.

Question 2: List-based assessment

Respondents were asked for their views on those cyber security activities and techniques which require unauthorised access but which should be deemed legitimate under a reformed Computer Misuse Act.



Consensus on legitimate and defensible activity

- Vulnerability research
- Proportionate surveying of publicly available systems
- Responsible security research
- Responsible disclosure
- Active scanning
- Enumeration
- Best practice internet scanning
- Use of open directory listings
- Identification
- Passive recon
- Honeypots
- Passive investigation

Active defence: outstanding 'grey areas'

- Ethical exploitation
- Infiltrate bad actor's network
- Verification of passive-detected vulnerabilities
- Exploitation of vulnerabilities
- Credential stuffing
- Neutralising suspicious or nefarious asset
- Active intel gathering
- Botnets
- Active investigation / forensic analysis

Consensus on illegitimate and indefensible activity

- Hack back
- DDos attack
- Malware
- Ransomware
- Causing harm
- Breaking into CNI
- Malicious socially undesirable acts
- Validation of exploit or proof of a failed security boundary

1.1. Introduction

Last year (2021), the CyberUp Campaign set out our Defence Framework – a proposal for a set of principles that would guide the application of a statutory defence under a reformed Computer Misuse Act. This work was borne out of understandable questions about how a reformed Computer Misuse Act would work in practice – it sought to ensure that under any reforms the right balance would be struck between protecting the cyber security ecosystem and prosecuting criminals effectively.

The principles-based framework aims to demonstrate that courts are capable of successfully and consistently applying an assessment of whether an act of unauthorised access is defensible, and thereby inform an evolving understanding of what constitutes legitimate conduct in cyber space.

For the avoidance of doubt, the techniques and activities being discussed here all involve an element of unauthorised access to computer material as defined in law today – currently prohibited by the Computer Misuse Act. Unlike lots of what cyber security professionals are able to do, such as penetration testing, vulnerability assessments or red teaming exercises, these are actions that do not involve the explicit pre-obtained permission or consent of (whoever acts as) the system owner.

In the Defence Framework, we were clear that the details of the framework are not intended to be included in primary legislation as part of a reformed Computer Misuse Act. Instead, we are advocating for updated legislation to mandate the courts to "have regard to" Home Office or Department for Digital, Culture, Media and Sport (DCMS) guidance on applying a statutory defence that would, ideally, be based on the framework we propose.

To support the application of the guidance, we would also encourage the courts to seek evidence from independent expert bodies, as is standard practice in criminal law. This could involve courts calling witnesses – such as UK Cyber Security Council representatives or other industry authorities – to understand the technical details of any cases they are called upon to adjudicate.

We resisted suggestions to include a list of typical activities or techniques that should be classed as legitimate cyber security activity under a reformed Act, because we do not consider it a sustainable or fit-for-purpose approach. That said, we do understand that it would be useful for policy makers to be presented with a summary of the current expert consensus of the types of vulnerability research and cyber threat intelligence activities that should be classed as defensible. The findings should assuage any fears policy makers have that a statutory defence will be open to abuse and have negative unintended consequences. Broadly, there are two central, related worries we have picked up in our engagement with ministers, government officials and criminal justice representatives:

1. A statutory defence will unleash a wild west of cyber vigilantism
2. A statutory defence will be abused by those with genuinely nefarious ends, and prosecutors will be unable to secure convictions in those instances.

This consultation finds that a significant degree of consensus already exists in the UK about what are legitimate and illegitimate instances of unauthorised access, and that it is therefore also possible for the courts to adjudicate clearly which behaviour and acts should continue to be punished as criminal offences. We envisage that this consensus would form the basis of the technical expertise courts will be provided with when applying a principles-based assessment of the defensibility of acts of unauthorised access. The vast majority of the acts which currently are being prosecuted under the Computer Misuse Act fall outside of this consensus to the extent that a court – drawing on this expert consensus – would be able to provide an uncontroversial and swift judgment on the criminality of the action. This expert consensus may shift over time, as new technologies and cyber security techniques emerge, but it will still be able to be drawn on by courts.

We also find that there are outstanding grey areas where the question of what is legitimate remains contested. This research paper does not seek to offer a definitive final word on some of these edge cases, which will need to be subject to further consultation and discussion as the policy formation process develops.

1.2. Methodology

The CyberUp Campaign consulted cyber security professionals on their views regarding the qualities and characteristics of different techniques and their perceived legitimacy.

Our consultation asked respondents a series of open-ended questions about what activities should be defensible (that they believed currently are not), and what should remain illegal; asked for specific views as to the harm-benefit profile of different activities; and provided respondents with the opportunity to offer any general comments.

In brief, we asked respondents for their views on:

1. the harm / benefit profile of the most common cyber security activities and techniques deployed in the course of vulnerability and cyber threat intelligence research which require unauthorised access
2. those cyber security activities and techniques which require unauthorised access, but which should be deemed legitimate under a reformed Computer Misuse Act 1990.

A full list of the questions asked is provided in an annex to this document. The number of respondents was 15. Respondents were from a wide range of key organisations across the UK cyber security ecosystem. They varied in scope and size, from independent security and defence consultants and single independent researchers through to large scale IT and security consultancies and organisations employing 85,000 people, as well as bug bounty program providers and research institutes like the Alan Turing Institute. We believe, therefore, that the outputs detailed in this paper reflect an expert consensus.

1.3. Revisiting the Defence Framework

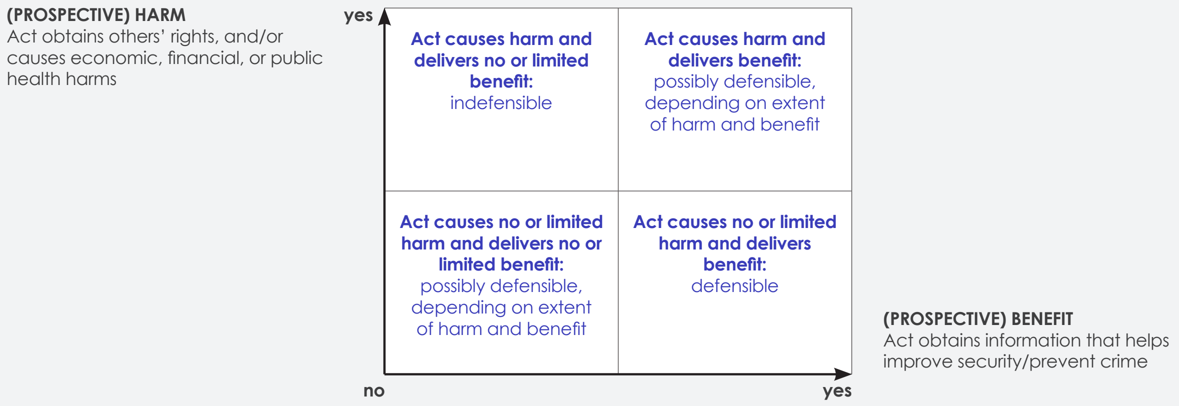
The Defence Framework set out four principles to guide the application of a statutory defence. The relevant principle for this consultation is Principle 1: the (prospective) harm-benefit profile of the act. Setting out Principle 1 in the Defence Framework, we produced a diagram that could be used to assess the (prospective) harm-benefit profile of any action, in order to allow courts to make a judgement as to whether Principle 1 had been satisfied (see below).

Harms to be weighed include:

- The infringement of the rights of another person/organisation, such as impacting the safety, privacy, security and continuity of systems, services or data
- Economic/financial harms and/or harms to public health, such as facilitating criminal activity
- Geo-political risks

Benefits to be weighed include:

- Improved cyber resilience and reduced cyber crime, for individual system owners, and at national scale, such as through obtaining information or actionable intelligence that helps improve security or prevent crime.



(PROSPECTIVE) HARM
Act obtains others' rights, and/or causes economic, financial, or public health harms

yes

Act causes harm and delivers no or limited benefit: indefensible

Act causes harm and delivers benefit: possibly defensible, depending on extent of harm and benefit

Act causes no or limited harm and delivers no or limited benefit: possibly defensible, depending on extent of harm and benefit

Act causes no or limited harm and delivers benefit: defensible

(PROSPECTIVE) BENEFIT
Act obtains information that helps improve security/prevent crime

no

yes

Figure 2: The CyberUp (prospective) harm-benefit spectrum of acts of unauthorised access.

To allow us theoretically to consider whether the techniques we set out are legitimate in isolation, we asked respondents to assume that the Defence Framework's remaining three principles are satisfied. This means:

- The act in question was proportionate – reasonable steps were undertaken to minimise risks of causing harm
- The actor demonstrably acted in good faith, in an honest and sincere way
- The actor was able to demonstrate their competence (authority and expertise), based on their:
  - level of qualification, certification or accreditation
  - membership of a professional organisation and compliance with a code of ethics
  - professional capacity during the act in question – whether an actor was acting under commercial, academic research or other contracts, or participating in a bug bounty or other kind of product attack challenge programme
  - prior track record of work, research and investigations – self-taught ethical hackers may not have any qualifications or be affiliated with any accrediting body, but this doesn't necessarily mean that the defence shouldn't apply to them
  - previous associations – similarly, successful participation in schemes like bug bounty programmes should count towards competence.

2.1 Findings

2.1.1 The question of intent

The CyberUp Campaign has been asking for reform of the Computer Misuse Act for the principal reason that the current law does not take into account the intent of the actor, and the intent of the actor remains the key dividing line for marking out an ethical hacker from the rest (once we accept that authorisation alone is not fit for purpose in the 21st century). In many cases, the techniques and tools used by cyber criminals and cyber defenders will be similar – leaving intent as the primary differentiator in making judgments about an (unauthorised) act's legitimacy.
Despite this, for this exercise, we stipulated that respondents attempt to isolate actions from the intent of the actor, in order to understand if and where consensus lies on the types of activities that should be defensible.

Nevertheless, the question of intent was, understandably, continually raised in the qualitative part of the survey. In questions about what should be defensible under a reformed Computer Misuse Act, respondents often qualified their answers with statements like:

- Do X in order to do Y (i.e. to understand more about…, to help identify… , to detect or collect data… the asset and disable/neutralise)
- Participate in X for the purpose of Y (i.e. for purposes of intelligence or data collection, or investigations)
- Undertake X in the context of Y (i.e. investigation, incident response etc)

In response to the questions about what should remain illegal, answers sometimes focussed on malicious intent as a key factor. Additionally, at the end of the survey where respondents were asked to offer any additional comments, there were reflections about the difficulty of isolating cyber security techniques from the intent of the actor, with one respondent even going so far as to claim that "techniques are irrelevant".

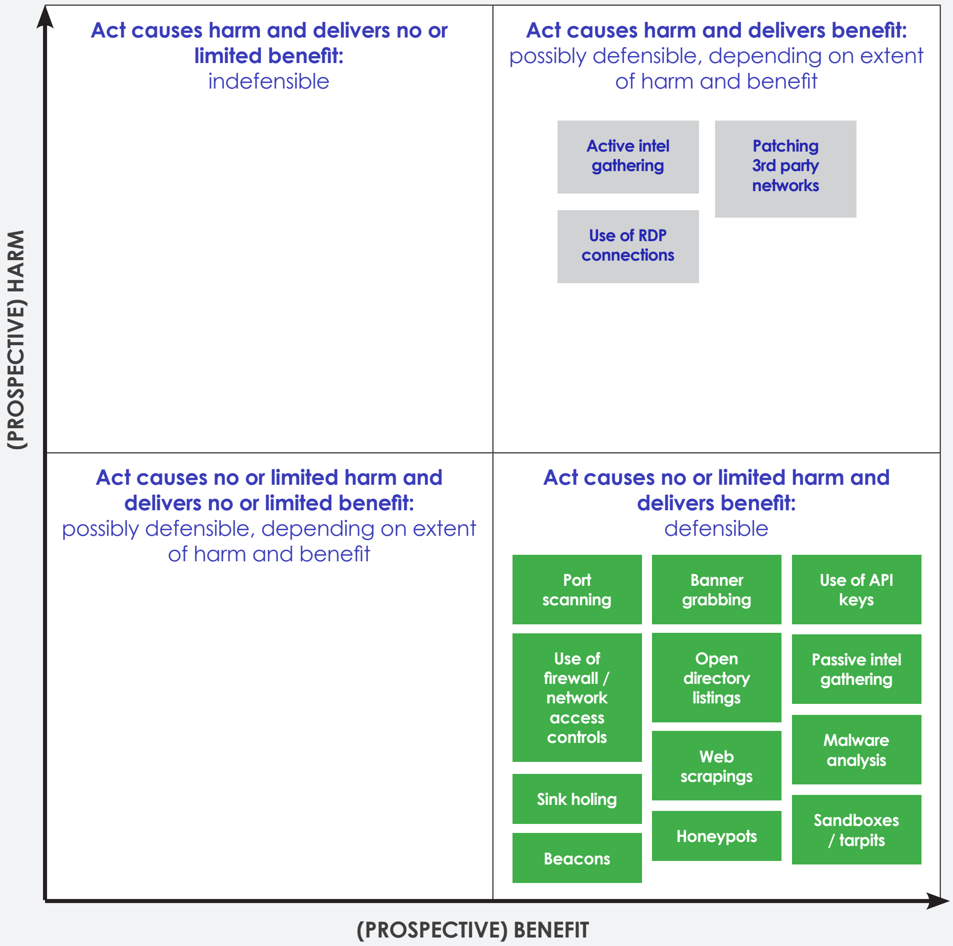
As discussed, these are sympathetic concerns. We agree that it is, ultimately, impossible to make a comprehensive judgment about the defensibility of an action based on its harm-benefit profile alone. Nevertheless, grouping activities according to potential harms and benefits is a useful exercise for demonstrating to policy makers where the current expert consensus lies as to what are legitimate techniques.

2.1.2 Harm/benefit profile of actions surveyed

Assessing the harm / benefit profile of the most common cyber security activities and techniques deployed in the course of vulnerability and threat intelligence research which require unauthorised access.

Question 1: Harm / benefit profile

Respondents were asked for their views on the harm / benefit* profile of the most common cyber security activities and techniques deployed in the course of vulnerability and threat intelligence research which require unauthorised access.



Act causes harm and delivers no or limited benefit: indefensible

Act causes harm and delivers benefit: possibly defensible, depending on extent of harm and benefit

Active intel gathering

Patching 3rd party networks

Use of RDP connections

Act causes no or limited harm and delivers no or limited benefit: possibly defensible, depending on extent of harm and benefit

Act causes no or limited harm and delivers benefit: defensible

Port scanning

Banner grabbing

Use of API keys

Use of firewall / network access controls

Open directory listings

Passive intel gathering

Web scrapings

Malware analysis

Sink holing

Honeypots

Sandboxes / tarpits

Beacons

**Definitions of what constitute 'harm' and 'benefit' are outlined in section 1.3 of this paper.*

As described above, we asked respondents to place different cyber security techniques in the four quadrants of our harm-benefit profile matrix. We define consensus as those instances where more than 50% of respondents placed the activity in one of the four quadrants.

Interestingly, activities only reached this threshold in two of the four quadrants – acts that cause harm and deliver benefit, and acts that cause little to no harm and deliver benefit. On reflection, this outcome is understandable – it is not surprising that cyber security researchers, in the aggregate, looked at the set of techniques outlined and felt they could be of benefit if deployed in the correct way. The key diving line was which of these actions – which all involved some form of unauthorised access – had the potential for harm.

2.1.2.1 Acts that cause no or limited harm and deliver benefit

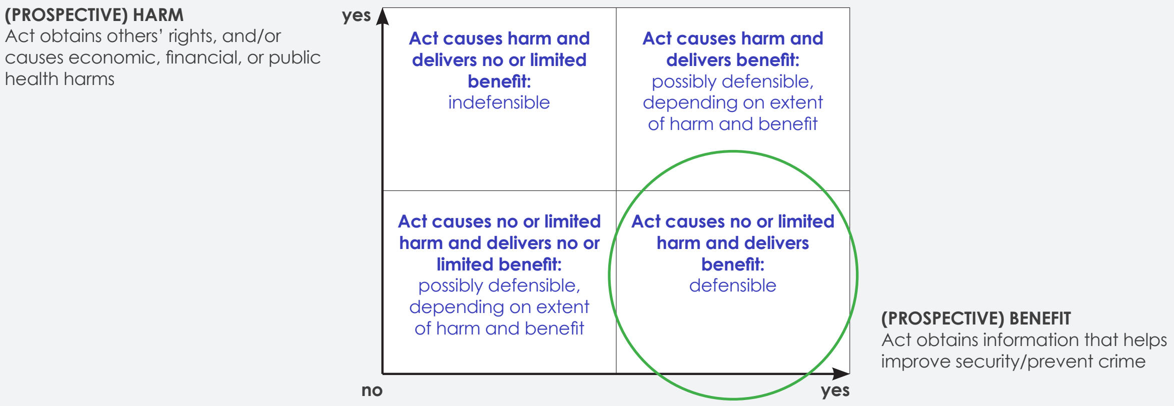

(PROSPECTIVE) HARM
Act obtains others' rights, and/or causes economic, financial, or public health harms
yes
Act causes harm and delivers no or limited benefit: indefensible
Act causes harm and delivers benefit: possibly defensible, depending on extent of harm and benefit
Act causes no or limited harm and delivers no or limited benefit: possibly defensible, depending on extent of harm and benefit
Act causes no or limited harm and delivers benefit: defensible
(PROSPECTIVE) BENEFIT
Act obtains information that helps improve security/prevent crime
no
yes

Figure 2: The CyberUp (prospective) harm-benefit spectrum of acts of unauthorised access.

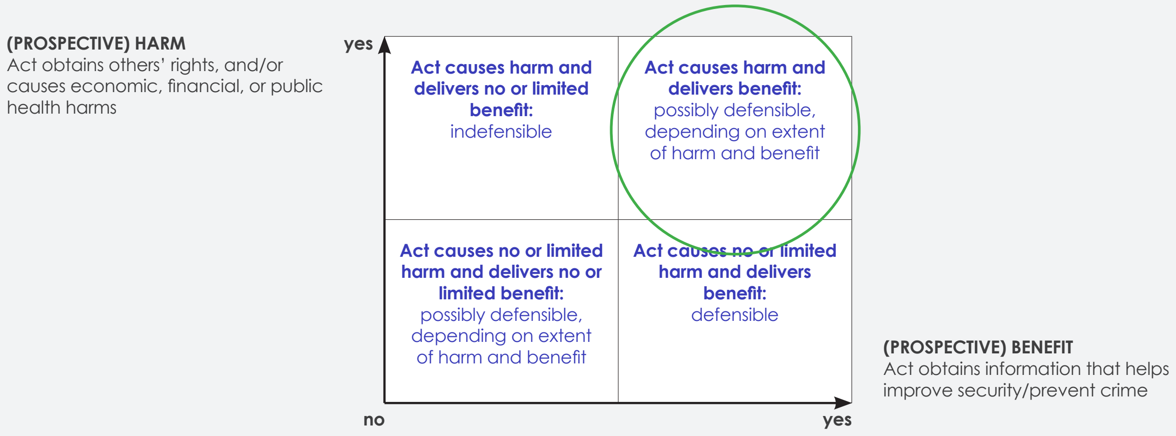
We provide here a list of the techniques that achieved a consensus (more than 50%) of respondents believing these actions caused no or limited harm and delivered benefit, with the percentages provided for each action:

- **Use of Application Programming Interface (API) keys (82%)**
- **Banner grabbing (64%)**
- **Beacons (56%)**
- **Implementation of firewalls and network access controls (90%)**
- **Use of honeypots (90%)**
- **Use of open directory listings (73%)**
- **Passive intel (intelligence) gathering (81%)**
- **Port scanning (73%)**
- **Use of sandboxes / tarpits (100%)**
- **Server/botnet take down (55%)**
- **Sink holing (73%)**
- **Web scraping (64%)**
- **Malware analysis (91%)**

Given the potential for no or only very limited harm, we argue that these techniques would satisfy Principle 1 of the Defence Framework. Assuming that the other principles are met, these actions would be defensible under the reforms we are proposing to the Computer Misuse Act.

Expanding the scope of legitimate cyber security activities to include these actions, these reforms alone would have a significant impact on improving UK cyber resilience through improved security research and improved (actionable) threat intelligence.

2.1.2.2 Acts that cause harm and deliver benefit



(PROSPECTIVE) HARM
Act obtains others' rights, and/or causes economic, financial, or public health harms

(PROSPECTIVE) BENEFIT
Act obtains information that helps improve security/prevent crime

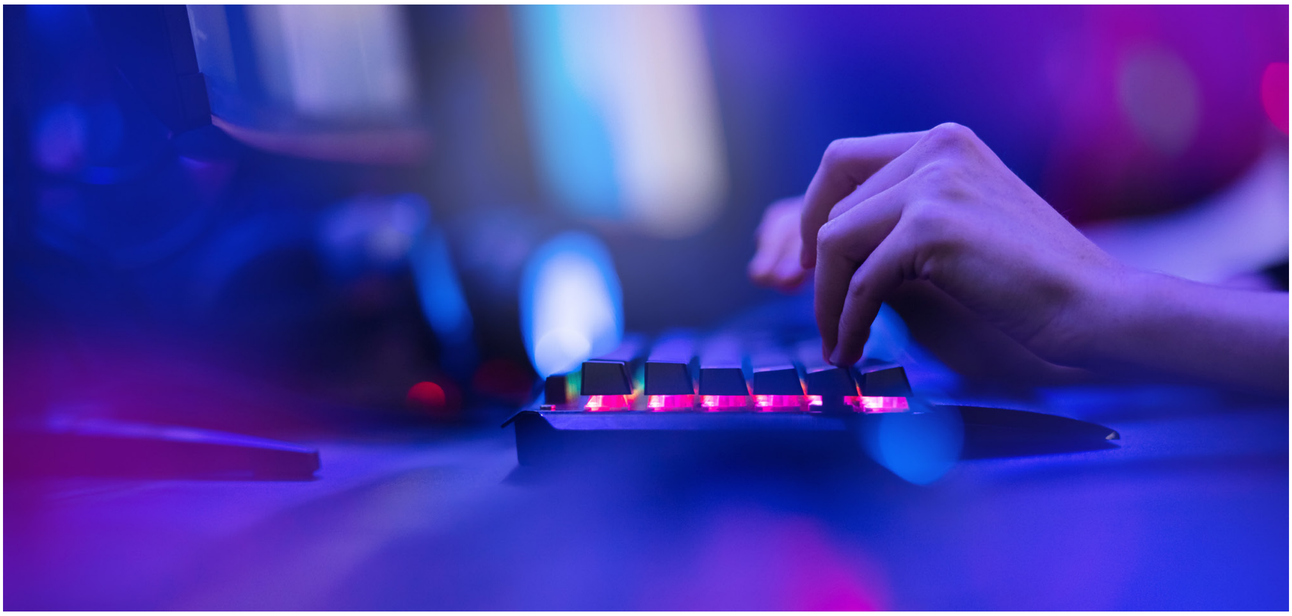
	no	yes
yes	**Act causes harm and delivers no or limited benefit:** indefensible	**Act causes harm and delivers benefit:** possibly defensible, depending on extent of harm and benefit
no	**Act causes no or limited harm and delivers no or limited benefit:** possibly defensible, depending on extent of harm and benefit	**Act causes no or limited harm and delivers benefit:** defensible

Figure 2: The CyberUp (prospective) harm-benefit spectrum of acts of unauthorised access.

We provide here a list of the techniques that achieved a consensus (more than 50%) of respondents believing these actions caused harm and delivered benefit, with the percentages provided for each action:

- **Forward/active intel (intelligence) gathering (64%)**
- **Patching third party networks (64%)**
- **Use of Remote Desktop Protocol (RDP) connections to gain information from attacker's computers (64%)**

These actions, according to the current consensus, would need to be investigated further to determine their defensibility according to the scale of the harm or benefit created in this instance. If an action fell into this category, there would also be an increased emphasis placed on the other principles being met to ensure safety and minimise harm.

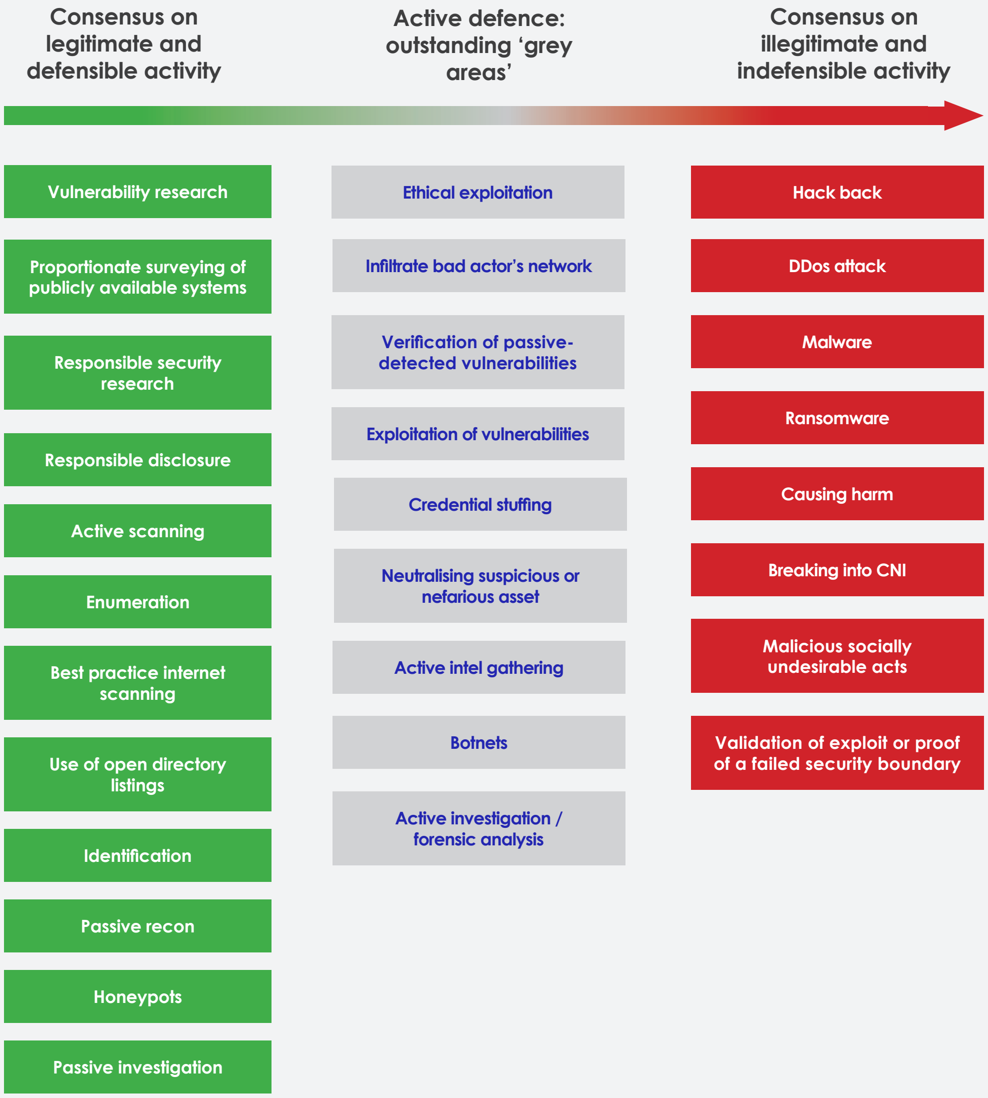


2.1.3 List-based questions

Outlining those cyber security activities and techniques which require unauthorised access but which should be deemed legitimate and remain illegal under a reformed Computer Misuse Act 1990

Question 2: List-based assessment

Respondents were asked for their views on those cyber security activities and techniques which require unauthorised access but which should be deemed legitimate under a reformed Computer Misuse Act.



Consensus on legitimate and defensible activity

- Vulnerability research
- Proportionate surveying of publicly available systems
- Responsible security research
- Responsible disclosure
- Active scanning
- Enumeration
- Best practice internet scanning
- Use of open directory listings
- Identification
- Passive recon
- Honeypots
- Passive investigation

Active defence: outstanding 'grey areas'

- Ethical exploitation
- Infiltrate bad actor's network
- Verification of passive-detected vulnerabilities
- Exploitation of vulnerabilities
- Credential stuffing
- Neutralising suspicious or nefarious asset
- Active intel gathering
- Botnets
- Active investigation / forensic analysis

Consensus on illegitimate and indefensible activity

- Hack back
- DDos attack
- Malware
- Ransomware
- Causing harm
- Breaking into CNI
- Malicious socially undesirable acts
- Validation of exploit or proof of a failed security boundary

As highlighted above, the survey also asked respondents to list techniques, acts and activities they think should be defensible under a reformed CMA, and those that definitely ought to remain illegal.

2.1.3.1 Consensus on legitimate and defensible activity

There was a consensus around similar groups of activities that were legitimate and therefore ought to be defensible. Necessarily, these answers focussed on outlining the activities in broader terms and drew out the centrality of the question of the intent of the actor (underlined below to highlight this).

We argue, in any case, that the proposed activities allow for significantly greater contextualisation as policy makers consider the inclusion of a statutory defence. As we have argued throughout this report, the degree of consensus that exists here should give policy makers confidence that in reforming the Computer Misuse Act to include a statutory defence, it will be possible to achieve a new equilibrium that makes defensible a suite of activities that involve responsible acts of unauthorised access.

Answers fell into the following two categories:

i. Security and vulnerability research and responsible disclosure, including:

- **"Vulnerability research; researchers investigating hardware items including set top boxes and other devices"**
- **"The justifiable accessing and responsible, proportionate surveying of publicly available systems for the purposes of improving their security or responsibly disclosing any potential weaknesses"**
- **"Responsible security research, including the responsible development and distribution of justifiably legitimate software and hardware tools despite their potential use for malicious purposes"**
- **"Responsible disclosure of issues located within systems"**

ii. Scanning, reconnaissance and monitoring, including:

- **"Active Scanning"**
- **"Enumeration"**
- **Identification – "active investigation to ID an unknown asset: light port scanning and active tracking of unknown assets that are suspicious (behaving outside the norm) or actively engaging with your network"**
- **"Ability to access domain name registrant information for UK ccTLD domains to help identify those with malicious intent, to allow the registry to take action e.g. in the form of an anonymised identifier for which the actual registrant details could be requested by law enforcement or investigated under Nominet T&Cs as abuse"**
- **"Broad / best practice internet scanning for general banner collection, and with targeted queries or requests in order to detect or collect specific data from systems or malware – where this data is useful for defence"**
- **"Passive reconnaissance in the context of investigations and incident response"**
- **"Conduct passive investigation to understand where the asset is coming from (information gathering tactics)"**
- **"Monitoring activity of a known bad actor in your network through the creation of a honey pot (fake asset made to look attractive to a bad actor), this can fall into entrapment types of challenges, but it can be necessary to understand the motives and goals of a bad or even suspicious actor"**

2.1.3.2 Consensus on illegitimate and illegal activity

There were also comments about the kinds of activities that definitely ought to remain illegitimate and illegal, including:

- **“Hacking back - accessing attacker infrastructure (too many complications regarding compromised infrastructure, potential access to third party data or systems, and possible unintentional targeting of Red Teams)”**
- **“Conducting a denial of service against an entire organization or multiple assets that are confirmed to be the origin of a bad actor”**
- **“Sending of malware esp. ransomware”**
- **“Causing harm to many for the suspected or even confirmed actions of a single or few actors”**
- **“Breaking into CNI [Critical National Infrastructure]”**
- **“Clearly malicious, fraudulent or otherwise clearly socially undesirable acts where the principal aim is malicious”**
- **“Social engineering of people or organizations that are suspected to be involved in an incident”**
- **“Anything available may (or may not) participate in the validation of exploit or proof of a failed security boundary”**

Many of these activities would, in our view, constitute ‘hacking back’, because they entail the subversion of security controls, disruption or degradation of the investigated systems and infrastructure. The CyberUp Campaign has been clear that there are very good reasons that these ‘offensive’ cyber activities should remain the prerogative of the state, and thereby subject to a higher degree of oversight, accountability, and, ultimately, public scrutiny. While it is possible to imagine situations where the private sector being able to conduct these operations would be in the national interest, we strongly argue that any changes to the Computer Misuse Act must still allow for activities entailing the disruption or degradation of the investigated systems and infrastructure to be criminal acts.

2.1.3.3 Active defence: outstanding ‘grey areas’

As was the case in the questions assessing the harm-benefit profile of various actions, there were techniques that were contested by some respondents in terms of whether they should be considered legitimate forms of unauthorised access.

On the one hand, the following were included by respondents as techniques that should be deemed legitimate and therefore defensible:

- **“Exploitation (including ethical exploitation such as nslookup for RCE)”**
- **“Verification of passive-detected vulnerabilities”**
- **“Credential Stuffing”**
- **“Neutralising (sandbox, disable, remove...etc) an asset that is behaving suspiciously or actively causing negative impact to your network”**
- **“Once an asset is confirmed to be nefarious from monitoring activity, log into the device (if possible) to understand more about the asset and disable/neutralise (if possible)”**
- **“Participation in botnets for the purpose of intel/data collection”**
- **“Forensic analysis of computers and other electronic devices which involve a legitimate 3rd Party taking over someone’s device for investigation purposes”**

Conversely, other respondents suggested that the following were illegitimate forms of unauthorised access, and therefore ought to remain illegal:

- **"Infiltrate the network of the bad actor"**
- **"Exploitation of vulnerabilities without informed consent from relevant third parties"**

Clearly, there is more contestation of this set of techniques – which can be broadly categorised as 'active defence':

- **'Active', because they involve a higher degree of interaction with a victim's or criminal's system than is the case for the two uncontroversial categories of security and vulnerability research and scanning, reconnaissance and monitoring (or passive threat intelligence) (as set out under 2.1.3.1.).**
- **'Defensive', nevertheless, because the interaction with the third party's system falls short of any disruption or degradation that would entail techniques that unambiguously remain off-limits (as set out under 2.1.3.2.).**

This research paper does not seek to offer a definitive final word on some of these edge cases, which will need to be subject to further consultation and discussion as the policy formation process develops. However, it is the CyberUp Campaign's view that there are qualitative differences between the 'active defence' techniques set out in this section and those set out in section 2.1.3.2. such as 'hack back'. Any approach that sought to dismiss out of hand the possibility that 'active defence' techniques could be responsible instances of unauthorised access risks restricting cyber professionals' ability to improve cyber resilience and contribute to collective national security.

Moreover, a focus on these edge cases should not be allowed to cloud the key finding of this consultation: that there exists a significant degree of consensus about what are legitimate and illegitimate instances of unauthorised access, and it is this consensus that would form the core basis of a new legal environment for cyber security professionals based on a statutory defence.

2.1.4 Opposition to reform

There were a small number of comments made by respondents questioning the overall approach of expanding the scope of defensible activity.

One respondent commented that industry/non-law enforcement should not do any of this, because it is "dangerous and could, if not done with the right authority and due diligence cause disruption of intelligence or law enforcement operations, diplomatic incidents or war". Our view as the CyberUp Campaign is that there are a set of activities, established in the consensus above, that fall short of the harms set out here and therefore should be defensible (so long as the other principles of the Defence Framework are met), bringing significant security and economic benefits to the UK. It is also evident from our analysis of legal jurisdictions where these activities can be undertaken that these worst case scenarios do not manifest.

There were also suggestions that some activities should only be conducted under license, and actors held to account where a licence has been misused, as part of greater professionalisation and offering 'powers' to appropriately qualified professionals. The CyberUp Campaign has consistently sought to make the connection between a reformed Computer Misuse Act and accreditation and standards in the cyber security sector. Our Defence Framework envisages a looser system than proposed by this respondent, where competence can be demonstrated by self-taught / non-accredited professionals. Nevertheless, recent statements by DCMS indicate that the UK Government does see the future of changes to the Computer Misuse Act as being aligned in some way to the process of embedding standards in the sector, taking place through the formation of the UK Cyber Security Council.

An even tighter system was suggested by one respondent, who suggested that the activities should only be undertaken where actors "have been certified and have a court warrant to proceed". Leaving aside that this system already exists, we still have concerns with even a vastly expanded system of pre-clearance or court warrants. This type of regime would, we believe, have the effect of stifling many of the upsides that reforming the Act according to the approach we have set out would bring. One of the main reasons we are proposing a defence is to allow cyber security professionals to have unauthorised access in some scenarios where that authorisation cannot be secured. Removing one requirement for an authorisation process and replacing it with another in the form of a pre-clearance requirement, which will still be limited by the time it will take to jump through the various hurdles, is not the right approach. Our view is that, over time with case law, and ideally with clear guidance from prosecutors, the boundaries of legal conduct will be sufficiently unambiguous to counter the need for the high degree of oversight that is sought by those who prefer a system more tightly regulated by the courts.

That said, the CyberUp Campaign has previously mentioned that it does believe that anyone undertaking an act of unauthorised access should keep documentation and technical logs of the act and any related activities, and we still believe that this is appropriate. A system of 'parallel information' – where a researcher is passing on information to relevant law enforcement bodies and intelligence agencies in a timely manner – is vastly preferable to a system of pre-clearance. Moreover, by sharing information in this manner, a researcher would go some way towards proving Principle 3 of the Defence Framework – that they were acting with the correct intent.

3.1. Conclusion

This consultation exercise has established that there is consensus around the types of cyber security activity which involve unauthorised access, but which are uncontroversial in terms of their ability to cause harm, and which therefore should be defensible under a reformed Computer Misuse Act. It is this consensus that would form the core basis of a new legal environment for cyber security professionals based on a statutory defence. This should give policy makers confidence that a reformed Computer Misuse Act need not unleash a wild west of cyber vigilantism. Rather, it will enable the UK's cyber security sector to more effectively protect the UK as part of the whole-of-society effort, whilst ensuring cyber criminals can still be prosecuted.

There was more contestation around some techniques which present a higher potential for harm, or involve a greater degree of interaction with a criminal or compromised system, and thus will need further discussion ahead of a future policy change. We would suggest that the Government use their own administrative resources and capacity to consult further on this should it be deemed necessary. But a focus on these edge cases should not be allowed to cloud the key finding of the consensus that exists. Importantly, it should also not be allowed to delay much overdue progress in reforming the Computer Misuse Act.

This exercise was conducted to establish the current consensus. We do not propose that a list of activities like that which has been established here make its way into Home Office/DCMS guidance accompanying a statutory defence, as this risks such a list becoming dated and requiring regular revisions. Instead, a court will be able to draw on the existing degree of consensus at that time about the prospective 'harm-benefit' profile of different acts and techniques, and their broader defensibility, in the application of Principle 1. Thus, any legislation and accompanying guidance will be better future proofed. We would caution against an approach based on endless consultation trying (and yet, likely ultimately failing) to establish an exhaustive list.

Unsurprisingly, the exercise also revealed the limitations of any effort to isolate techniques, activities and actions from the intent of an actor. Of course, intent remains the principal consideration of an act's legitimacy, and it is exactly for this reason that the current Computer Misuse Act falls short. In reality, intent will remain an essential component in the judgment of any act's defensibility.

4.1 Annex – survey questions

Introductory questions

Q1 Briefly describe the organisation you work for, and what it does.

Q2 How many employees does your organisation have?

Q3 What is your estimated annual turnover?

Q4 What is your role within the organisation?

List-based questions

Q5 Please list, describe and explain the techniques, acts and activities requiring unauthorised access that you think should become legitimate for UK cyber security professionals under a reformed Computer Misuse Act 1990.

Q6 Please list, describe and explain the techniques, acts and activities requiring unauthorised access that you think should definitely remain illegal. Consider that policy makers will be largely unfamiliar with technical details so an explanation of the technique in question and an example of what it might be used for will be helpful.

Harm-benefit profile questions

Q7 Use of Application Programming Interface (API) keys: An API is a software intermediary that allows two applications to talk to each other. An API key is a unique identifier used to connect to, or perform, a command – known as an API call. This technique refers to using API keys identified through research or otherwise identified on a number of applications to assess whether they are at risk.

Q8 Banner grabbing: A technique used to gain information about a computer system on a network and the services running on its open ports (see port scanning). This can allow security researchers to gather important intelligence on an attacker including the types of systems and services being used by an attacker.

Q9 Beacons: These tools allow a system owner to track data exfiltrated from its network. Beacons similarly alert the system owner when stolen data resurfaces elsewhere and can include information about the location and whereabouts of the file.

Q10 Use of default credentials: Many hardware and software products come with default credentials. These often allow users to have full administrative access to perform an initial setup. Many people don't change from the default credentials, meaning the products are vulnerable as the credentials are often available online or are easy to guess. Security researchers can use default credentials to interact with and gain intelligence from attackers' systems.

Q11 Forward/active intel (intelligence) gathering: The act of acquiring intelligence about a target by establishing contact with the target or its systems (e.g. capturing their image through their webcam).

Q12 Use of anonymous FTP: One of the oldest and still-often used methods of sharing data is FTP (File Transfer Protocol). FTP has a configuration option – often called anonymous authentication – which allows external actors to log in with a user name of FTP or anonymously. This can be used to access an FTP and interact with files as an 'anonymous' user.

Q13 Implementation of firewalls and network access controls: A network security device that monitors and controls incoming and outgoing network traffic based on a set of predetermined security rules.

Q14 Use of honeypots: A system intended to be hacked by malicious threat actors to observe their activities and collect intelligence. This can also be used for alerting defenders to the presence of attackers within a network.

Q15 Use of known paths: A known path that can be exploited by cyber actors e.g. where researchers know the URL for e.g. a control panel, and access it directly, thereby circumventing a login screen.

Q16 Use of open directory listings: Directories are lists of direct links to files stored on a web server. A directory is "open" if that directory is not protected by a username and password. This makes the directory, and all of the files contained within it, freely accessible by anyone who visits it. Open directories can be, but aren't always, a vulnerability or oversight. Security researchers can use listings of open directories to obtain information about an attacker without bypassing security or authorisation mechanisms.

Q17 Passive intel (intelligence) gathering: The act of acquiring intelligence about a target without establishing any contact with the target or its systems. The types of information that can be discovered through passive intel gathering include subdomains and public IP addresses, open directory listings and publicly available documents and files.

Q18 Security research on products without a vulnerability disclosure policy: Identifying vulnerabilities on websites, applications, or products whose owners or manufacturers have not published a vulnerability disclosure policy (VDP) that would establish a clear means of reporting and supporting the remediation of any vulnerabilities that are found as a result of the research.

Q19 Patching third party networks: The act of changing a computer program or its supporting data to update, fix, or improve it, addressing security vulnerabilities where ownership of those systems is not obvious but where the person undertaking the patching does not own the system.

Q20 Port scanning: The act of searching for a computer's ports through the use of specialised software. This software searches for 'doorways' in a computer and classifies them into one of three categories—open, closed, or filtered. Once the port scan is complete, the user will then be able to see all of the available ports on the target machine as well as their classification. This then allows security researchers to undertake banner grabbing (see banner grabbing).

Q21 Use of Remote Desktop Protocol (RDP) connections: Developed by Microsoft, RDP provides users with remote display and input capabilities over a network connection for Windows applications running on a server. This can allow security researchers to establish a connection to systems to execute commands.

Q22 Use of sandboxes / tarpits: These tools provide barriers that slow or halt and examine incoming traffic that may be suspicious.

Q23 Server/botnet take down: The act of temporarily disrupting the servers an attacker relies on or dismantling its botnets, which use networks of infected machines to launch attacks. This can be done to minimise the impact of victims and infected networks by disrupting the communication of botnets to their Command and Control servers.

Q24 Sink holing: Redirecting malicious traffic to a system under control of the defender. This can be done to minimise the impact of victims and infected networks by disrupting the communication of botnets to their Command and Control servers.

Q25 Web scraping: A term for various methods used to collect information from across the Internet. Generally, this is done with software that simulates human web surfing to collect specified bits of information from different websites.

Q26 Malware analysis: By executing malware in a sandboxed environment and observing and analysing what happens, researchers can collect relevant information about the created files, network connections, changes in the registry etc.

Q27 General Comments