Criminal Law Reform Now Network Comparative Report: Computer Misuse Act 1990

This Report builds on our Computer Misuse Project, and our publication *Reforming the Computer Misuse Act 1990* (CLRNN 1, 2020). We take the opportunity to expand on the comparative analysis in that publication, with a particular focus on potential defences and legal protections for legitimate cyber security and research activities. We structure the discussion across four sections:

More information about the Criminal Law Reform Now Network (CLRNN), including information about our other reform projects, can be found at our website; and by following us on Twitter @CLRNNetwork and via our YouTube Channel.

A. CLRNN Report Recommendations

In CLRNN 1, *Reforming the Computer Misuse Act 1990*, we make a series of recommendations for reform across the piste of cyber hacking regulation. This includes offences (Ch2), defences (Ch3), guidance for prosecutors (Ch4), sentencing (Ch5), and the potential for civil penalties (Ch6). The short summary below sets out our main recommendations for offences and defences only, in line with the focus of this comparative report.

Offences

1. We recommend that section 3 and 3ZA CMA, unauthorised act offences, should be narrowed to target intentional harm causing only. References to an alternative of 'recklessness' should therefore be removed – deleting s.3(3); deleting reference to recklessness in s.3(4); deleting reference to recklessness in s.3ZA(d).

NB: Narrowing these offences to intentional harm causing ensures that the conduct of bad actors will be criminalised without inadvertently catching the conduct of whistle-blowers, journalists, and others. The move would bring the law better into line with international comparators (discussed Section B and Section C below).

2. We recommend that section 3A CMA, making and supplying articles offence, should be narrowed to intentional facilitation of crimes only. References to an alternative of 'recklessness' should therefore be removed – deleting s.3A(2).

NB: Again, the current law is drafted in an overinclusive manner. In particular, here, we want to avoid the inadvertent criminalisation of cyber intelligence and threat detection materials.

3. We recommend the creation of a new corporate failure to prevent offence, to apply across all of the CMA 1990 offences in these terms:

    (a) A body corporate or partnership (B) is guilty of an offence if a person (A) commits an offence contrary to sections 1, 2, 3, 3A or 3ZA of this Act when A is acting in the capacity of a person associated with B and provided that A committed that offence for the benefit of B.
    (b) A will act in the capacity of a person associated with B where A is an employee of B, an agent of B, or any other person who performs services by or on behalf of B.
    (c) It is a defence for B to prove that B had in place adequate procedures designed to prevent persons associated with B from committing such offences.

NB: In line with developments elsewhere in the criminal law (e.g. bribery, tax evasion, etc), we believe that a corporate failure to prevent offence would provide an effective and appropriate new layer of criminal law protection. The expanding role of computer technology across all sectors makes the effective regulation of corporates particularly important in this area, and compliments recommendation for new defences discussed below.

Defences

1. We recommend that section 17(5) CMA, defining 'unauthorised' access, should be amended to include new subsections (c) and (d):

    (5) Access of any kind by any person to any program or data held in a computer is unauthorised if —
    (a) he is not himself entitled to control access of the kind in question to the program or data;
    (b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled;
    (c) he does not reasonably believe that the person entitled to control access of the kind in question to the program or data would have consented to that access if they had known about the access and the circumstances of it, including the reasons for seeking it; and
    (d) he is not empowered by an enactment, by a rule of law, or by the order of a court or tribunal to access of the kind in question to the program or data.

NB: These additions, of the kind we see elsewhere in the law, are designed to allow threat intelligence and security professionals (in particular) some discretion to use their professional judgment as to likely consent. Note, however, that they are qualified by a requirement of objective reasonableness, to avoid attempts at inappropriate use.

2. We recommend the creation of a new public interest defence, applicable to CMA offences where the defendant does not intend to commit or facilitate further crimes:

   s.18. 'It will be a defence to a charge contrary to sections 1 and 3 for a person to prove that in the particular circumstances the act or acts (i) was necessary for the detection or prevention of crime, or (ii) was justified as being in the public interest.'

NB: This recommendation provides an explicit public interest defence to allow threat intelligence and security professionals (in particular) to work lawfully for the public benefit. Note the reverse burden (i.e. it will be for the defence to prove) and the *objective* public interest and/or crime fighting requirement (i.e. good intentions by themselves will not be sufficient).

B. International Legal Obligations and Context

This section sets out the international legal context within which the current law (and any future reform) operates, focusing in particular on the potential introduction of a new public interest defence. Essentially, such defences are neither mandated nor prohibited by existing international agreements; but do provide a sensible route to meeting the broader aims articulated therein. Furthermore, since the enactment of these legal instruments, awareness of a negative legal environment for security researchers has grown and initiatives are being pursued in an attempt to devise solutions.

Council of Europe

The 2001 Convention on Cybercrime No.185 (hereafter the 'Budapest Convention') sets out a series of commitments on cybercrime, from substantive criminalisation (e.g. illegal access and trade in hacking tools), to the thematic (e.g. categories of offending related to fraud and child pornography), to the procedural. Such requirements are stated in typically generalist language and do not include a discussion of defences. However, there is recognition that the criminal law should not be applied to hinder the beneficial work of cyber security professionals and researchers; something that appears specifically in relation to the trade/use of hacking tools and more generally in the Explanatory Report (accompanying the Convention).

Article 6(1) of the Budapest Convention sets out the criminalisation of trading/using certain dual-hacking tools. In response to concerns raised by the international community of computer scientists (inc. CLRNN contributor Peter Sommer) the prohibition is qualified in Article 6(2) in a way that avoids the criminalisation of security researchers:

> This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

Article 6(2) provides an explicit recognition of the danger of overcriminalisation with regard to cyber professionals. Regrettably, it is not repeated for other Articles within the Convention.

The Explanatory Report also acknowledges and warns against overcriminalisation; and importantly, this time goes beyond Article 6 to include Article 2 (unauthorised access) and other offences (Explanatory Report, Paras 38, 47, 62). This appears when discussing the Convention term 'without right', the equivalent of 'unauthorised' within the UK Computer Misuse Act 1990. The Council of Europe describes the concept as:

> … reflect[ing] the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability.

The Council of Europe make it clear that security researchers' work should be considered as authorised, and thus 'with right'. This provides useful insight into the concerns of the Convention drafters, and a sensible prompt for national legislators to ensure that the legitimate conduct of security researchers (and the conduct of other good actors) is not criminalised. However, there is an absence of detail on *how* good actors should be protected, and focusing on the definition of 'without right' alone may not provide an appropriate mechanism (i.e. focusing debate towards complex and often uncertain technical questions about permissions within commercial agreements and practices).

The European Union

The UK has left the European Union (EU), but EU law remains a useful point of reference in this area. First, this is because for the security industry, whose work is global, EU law will continue to apply to various aspects of their work. The NCC group, for example, which also advocates for a statutory defence, has offices in the Netherlands, Denmark, Germany, Portugal, Spain, in addition to the US and Japan. Further, when considering reform of UK law, it is instructive to see similar concerns being acknowledged (if not yet acted upon) within the EU.

Directive 2013/40/EU provides the principle legal instrument for the EU. As with the Budapest Convention, the Directive provides for the criminalisation of a series of actions related to computer hacking and attacks on information systems. Again, however, the Directive does not engage explicitly with the need for criminal defences. Recital 16 makes explicit reference to the 'need to avoid criminalisation where … [where defendants have acted with] legitimate purposes', but this comment is limited to Article 7 on the misuse of tools and makes no reference to the commission of other offences.

Such deficiencies have been highlighted by several commentators, and perhaps most usefully by the European Union Agency for Cybersecurity (ENISA); and the lack of explicit protection for cyber security and other professionals has become a major focus of criticism. ENISA has discussed the issue of criminal liability (and civil liability) of the security industry as part of its report on the Directive's implementation in 2013, and as part of its work on vulnerability disclosures in 2016 and 2018. It has highlighted how regulation, as implemented at national level, has introduced great uncertainty as to the lawfulness of security researchers' work. ENISA highlights the stifling effect that *potential* criminalisation has in limiting the positive work of cyber security professionals, as well as the damage done by - albeit rare - prosecutions in fact (prosecutions for various computer misuse offences, not just for the misuse of tools offence). Relatedly, ENISA has also denounced the practice of liability dumping where companies publish a vulnerability disclosure policy to authorise work and then rescind on their alleged 'authorisation' and decide to prosecute security researchers who reported a vulnerability to the company. ENISA has repeatedly affirmed its conclusion that cybercrime-dependent offences constitute a serious obstacle to the work of the security industry, and that the law (EU and/or national) should incentivise rather than discourage vulnerability disclosure.

With growing recognition of the problem of over/inappropriate criminalisation, we have begun to see actions taken at both European and national levels. A good example of the former is the EU legislation on civil aviation and the reporting of safety concerns. Article 15(2) of Regulation (EU) 376/2014 on the reporting, analysis and follow-up of occurrences in civil aviation prohibits Member States, the Agency and organisations from being able to 'make available or use the information on occurrences [safety concerns and vulnerabilities] in order to attribute blame or liability'. This is a prohibition from prosecuting those reporting issues of safety in the civil aviation industry. It is expressed and applies in general terms, but given the predominance of software components in the industry, vulnerabilities in software represent a major aspect of these safety concerns. Article 15 thus creates a safe space for security researchers who would be working in the field.

More recently, a task force from the Centre for European Policy Studies (CEPS) worked on Software Vulnerability Disclosure in Europe and published its final report in June 2018. The Centre confirms the lack of protection offered to security researchers. It specifically recommends amending the Directive 2013/40/EU to protect security researchers from prosecution, and to create coordinated/responsible vulnerability disclosure policies as part of the NIS Directive and the GDPR. The report also discusses some national legislative responses

that have increased protections for cyber professionals – including Dutch prosecutorial guidelines and French law – as early examples of good practice. We outline these examples as part of our comparative discussion in Part C.

C. International Comparison

Headline information is provided on a range of comparator jurisdictions. The problem of potential overcriminalisation of cyber security professionals and researchers (and/or the suppression of their valuable work) is increasingly well recognised internationally. Legislative action to address the problem, however, remains slow and piecemeal.

France

French law provides perhaps the most extensive protections for cyber security professionals and researchers that we find in our sample. Such protections are contained within (i) a general exemption from being reported to the public prosecutor and (ii) a specific exemption regarding the trade of hacking tools.

(i) General exemption for cybersecurity

Article 40 of the Civil Procedure Code obliges civil servants and public authorities in France to report to the public prosecutor any information pertaining to the commission of a criminal offence. This includes hacking, and related offences. However, Article L.2321-4 from the Code of Defence provides an exemption, removing the obligation to report to the prosecutor when a cyber security professional or researcher has acted in good faith and reported a vulnerability to the ANSSI (i.e. the national agency for security of information systems). Article L.2321-4 of the Code of Defence was created by Art 47 of a 2016 statute, the Loi n. 2016-1321 of 7 October 2016 for a digital Republic. While the Article L.2321-4 is inserted in the military code, its scope solely concerns non-military law and specifically the criminal law.

Article L.2321-4 Code of Defence reads:

> Pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'article 40 du code de procédure pénale n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données.
>
> *With regards to the cybersecurity needs of information systems, the obligation in Article 40 of the Criminal Procedure Code is not applicable to the person of good faith who transferred solely to the national authority of security of information*

> *systems [ANSSI] information about an existing vulnerability related to the security of an information system. (our translation)*

By creating an exception to Article 40 CPC, Article L.2321-4 Code of Defence prohibits the reporting of a person who finds a vulnerability and provides it to the ANSSI. The provision also indirectly discourages the prosecutor from charging such a person with a crime. In that sense, the mechanism created by Article L. 2321-4 is similar to that created by Article 15 Regulation 376/22014 on civil aviation which prohibits the use of a security threat report to allocate liability or blame to the person reporting (discussed in Section B).

The parliamentary debates preceding the creation of Article L.2321-4 Code of Defence are also informative. The first option proposed by MPs was to provide a sentencing exemption for cyber security professionals and researchers to the French offence of unauthorised access (Art 323-1 Criminal Code). Criticisms came from all sides. On the one hand the proposal seemed insufficiently protective for cyber security professionals, in that it still allowed them to be prosecuted and found guilty; but on the other, a simple status-based exemption, without a public interest or reporting qualifier, was seen as having the potential to incite cybercriminals. Discussed immediately after the proposed amendments to the criminal code, Article L.2321-4 provided something of a compromise position - protecting cyber security professionals and researchers from prosecution proceedings before they really begin (i.e. stopping reporting), but only where threat information is transferred from the defendant to the ANSSI in good faith.

The French approach remains problematic, however. From the perspective of cyber security professionals and researchers (and their employers; their insurers), the exemption from reporting to the prosecutor provides only procedural and not substantive protection. Individuals, even when reporting in good faith, may still be prosecuted; the procedural rule may deter such prosecutions, but it does not prevent them, and there are no defences through which cyber security professionals and researchers may appeal to the public interest served by their work. Conversely, exemption at the reporting stage risks a lack of investigation, and the potential for bad actors to go unnoticed within the system.

(ii) Specific exemption for cybersecurity

Alongside the general exemption from reporting, a ‘legitimate purpose’ defence exists within the substantive law. This is not a general defence however, and only applies specifically to the offence of misuse of hacking tools. Despite this, its construction and rationale remain informative.

The defence is located in Article 323-3-1 of the Criminal Code, providing a justification when there is ‘a legitimate purpose, *notably of research or security*’ (emphasis added). The ‘notably of research or security’ was added in 2013 specifically for the benefit of security researchers, though not limiting the defence to such defendants alone. Article 122-6-1 of the Intellectual Property Code was also amended to the same end.

The amendment of Article 323-3-1 Criminal Code was motivated by the need to protect security researchers and to comply with Article 6(2) of the Budapest Convention (discussed in Section B). The original version of Article 323-3-1 that was introduced in 2004 was too vague and led to the criminal prosecution of legitimate security companies and researchers. Concerned that these prosecutions put the French security industry at a significant disadvantage compared to its international counterparts in a competitive market, the loi 2013-1168 of 18 December 2013 introduced the amendment and the new version of Article 323-3-1 Criminal Code.

Beyond Article L. 2321-4 Code of Defence (reporting exemption), and the new wording of Article 323-3-1 Criminal Code (defence for hacking tools), there are no defences to the other French offences of unauthorised access, unauthorised damage, and data/system interferences (Articles 323-1 to 323-3 Criminal Code). This continues to represent a problem for cyber security professionals and researchers working in France. However, note that the French offences are narrower in scope that their English counterparts, as discussed in Chapter 2 of the CRLNN 1 report (para. 3.1 – 3.59).

The Netherlands

Dutch law does not provide the same level of protection for cyber security professionals and researchers that we see in France but, exercised by similar concerns about overcriminalisation and anti-competitive legal structures, they have adopted an alternative mechanism toward the same ends. This alternative focuses on prosecutorial guidelines, and has been commended by the Centre for European Policy Studies (CEPS) taskforce on Security Vulnerability Disclosure.

The Netherlands adopted prosecutorial guidelines on the matter following two high-profile incidents in 2011. Academic security researchers who found serious vulnerabilities in the Dutch public-transport chip card were investigated for having violated the Dutch Criminal Code on computer misuse, a legally predicable outcome given the offences in place, but one that seemed plainly opposed to the public interest (i.e. identifying the vulnerabilities allowed a vital system to be secured from potential attack). To avoid similar situations arising again, the Dutch National Cyber Security Centre (NCSC) issued guidance in 2013 for both vendors and security researchers on a responsible disclosure policy. The Dutch Ministry of Security and Justice publicised the guidance (see also description), and the Dutch prosecutorial authority published its own guidance to prevent inappropriate prosecutions.

The Dutch prosecutorial guidelines contain the following three-part test on whether a prosecution should be brought:

(a) Were the security researcher's actions necessary within a democratic society (general interest)?
(b) Were the actions proportionate to the goal to be achieved?
(c) Could the security researcher have taken other possible courses of action that were less intrusive?

The guidelines focus attention on the public interest served by the security researcher's work, as well as the proportionate means they have employed to pursue that interest. In particular, the security researcher should not use brute force attacks or compromise further the security of the system; she should also avoid copying, modifying or deleting files; the alternative, whenever possible, being to create a directory listing for the system.

The guidelines are viewed internationally as an example of good practice to be followed, and we make similar recommendations for UK law in Chapter 4 of the CLRNN 1 Report. (Note, however, that our proposed guidelines go further and consider other groups whose conduct is potentially overcriminalised, such as the neurologically diverse). Despite such endorsement, it would be wrong to consider prosecutorial guidance as an *alternative* to substantive law reform. It may be easier procedurally, and it may have provided a necessarily immediate response to the problem cases in the Netherlands, but relying on prosecutorial discretion alone continues to place cyber security professionals and researchers at risk of inappropriate prosecution (a concern echoed by CEPS). Where a prosecution is initiated, even those cyber security professionals and researchers working in the public interest will have no substantive defence on which to rely. Again, this is not an acceptable way to maintain and encourage industries working for the public good; and a prosecution guideline only approach would be further strained in the UK context by the potential for private prosecutions initiated by third parties.

Austria

The Austrian approach is markedly different from both France and the Netherlands, focusing on the redefinition of hacking *offences* rather than creating new defences or procedural barriers to prosecution. Essentially, rather than defining broad over-inclusive offences that require mechanisms for exculpating good actors, the Austrian law attempts to target and criminalise only wrongful conduct. This is a laudable ambition; and one that underpins good law making across all areas of criminal law. However, as we will see, it is not at all straightforward to achieve in the context of cybercrime and hacking; and it is very unlikely to provide the full answer for UK law makers.

Austria has made use of the qualifying exemptions provided by the Budapest Convention, taking a narrower approach to criminalising unauthorised access by offering a legal mechanism to take account of an actor's motivation. This is given effect within section 118a of the Austrian Criminal Code:

> A person who, with the intent to obtain information on data for himself or for another unauthorized person, which are stored in a computer system not being destined for him, and to make them available to another person for whom they are not destined by using them or making them public, and to procure in this way an economic gain for himself or another person or causing a disadvantage for another person, obtains the access to a computer system or a part of such a system for which

> he is not permitted to dispose or not to dispose alone, by violating specific safety precautions within the computer system, is to be sentenced…

The two essential 'wrongful' elements in this definition are (i) use without right ('unauthorised'), and (ii) intent to make a financial gain or cause a loss to another.

There is much to be said for the approach taken in Austria, and we highlight again the offence narrowing recommendations for UK law included in Chapter 2 of the CLRNN 1 Report (summarised in Section A). However, two qualifications should be noted.

First, it is not clear that the Austrian legislation succeeds in its aim of protecting cyber security professionals and researchers from inappropriate criminalisation. Security professionals are likely to be working for financial gain, and so the second 'wrongful' element identified above will provide little protection. Focus instead will be upon the first element – the idea of circumventing legitimate access (i.e. being 'unauthorised') – which is left to do a lot of work in excluding good actors from the offence. The concern here is that, as with UK law, authorisation may be interpreted narrowly; and may unhelpfully focus on technical and uncertain permission giving rather than more general notions of public interest. It is possible to mitigate this concern by moving away from a focus on 'authorisation', and/or requiring some further mischief (e.g. intent to cause further harms), but these moves would lead to a significant narrowing of *potential* liability and exacerbate our second qualification.

The second qualification is that, when considering models for reform of UK law, we must acknowledge the current legal position we are working from. Rather than creating a new offence to target new conduct, we are recommending that conduct currently caught within the law should be excused. This leads to a natural concern that any change should not risk bad actors escaping liability. Focusing on the reform of defences (rather than offences) provides additional legal protections to reassure against such worries. These include (i) a reverse legal burden, requiring the defence to prove that the defendant's conduct was in the public interest (on the balance of probabilities); and (ii) the use of objective standards in assessing the defendant's conduct, rather than their subjective perceptions. This is reflected in our recommended public interest defence, set out in Section A.

United States of America

The criminal regulation of hacking and other computer crimes is provided jointly in the US across federal and state legislation. Most importantly, at the federal level, is the Computer Fraud and Abuse Act 1986 (CFAA), the US equivalent to the UK's Computer Misuse Act 1990 (CMA). Like its UK equivalent, the CFAA was created as a blanket criminalising response to early cyber threats in the 1980s (fuelled as much by science fiction as fact), setting out a series of unauthorised access and other offences, and not including defences for security professionals or researchers. The same approach is reflected in legislation across all 50 states, where again, broadly defined offences are provided with little or no qualification. [The Washington

Cybercrime Act provides a notable exception, qualifying the term 'authorization' to categorically exclude 'white hat security research'].

As with UK law, the unqualified criminalisation of cyber activities within the US CFAA is now unsustainable in the 21st Century. Rather than protecting the country from cyber threats, it is now widely recognised that application of the CFAA creates a perversely contrary impact in practice: the threat of prosecution has a demonstrable chilling effect on the work of cyber security professionals and researchers, weakening cyber defences across the country, whilst the same threat does not seem to have (sufficiently) deterred an escalating array of cyber attackers. It is little wonder, perhaps, that President Biden has highlighted improved cybersecurity as one of his 'top priorities'. The call for reform at both federal and state level is now clear and convincing, seeking to protect cyber security professionals and others in order to encourage the necessary development of such industries in the national interest.

With mounting pressure and expectation for reform, some limited progress has been made. First, in the context of copyright protection for example, section 1201 of the Digital Millennium Copyright Act (DMCA) has the potential to seriously impede the work of security researchers looking at consumer technologies. However, in this context at least, specific exemptions exist for 'good-faith security research'. It is not a perfect solution: it remains contingent on non-violation of the overlapping CFAA provisions, and the exemptions are reviewed every three years (so cybersecurity companies are unable to plan long term). Second, within the recent Supreme Court case *Van Buren v United States* (2021), the Court provide some recognition of the overbreadth of the current CFAA offences, interpreting 'exceeds authorized access' *not* to include breaking contractual agreements as to permissible computer usage. The decision, upon which three of the Supreme Court Justices dissented, provides only limited relief for the cyber industries however, and remains tied to the definition of authorisation. Third, and perhaps most successfully, the US has adopted an approach 'official reassurance' towards cyber security professionals and researchers, making clear that prosecution of good actors is not in the public interest. As the CyberUp Campaign notes in its recent response on CMA reform – in comparison to the UK, the US generally offers a 'more conducive operating environment to cyber threat intelligence and research companies', providing official reassurances against prosecution that has prompted threat intelligence research published by US-based companies that would not be undertaken in the UK.

Despite these limited steps, it is well recognised that fundamental substantive reforms are still required to adequately protect (and, indeed, to encourage) the cyber industries. In the US, however, debates about substantive law reform – and the legislative instruments emerging from them – have been broadly unsuccessful. And from our perspective, it is easy to see why. The boundaries between acceptable and unacceptable conduct in the cyber realm can be quite subtle, and will often be situation and actor specific (e.g. cyber researchers will often trade in very similar hacking tools to black hat criminals). However, rather than engaging with these subtleties, US reform debates too often focus on extreme positions; most commonly the move from blanket criminalisation (current law) to allowing active defence and hack back to the victims of cyber-attacks. We see this at the federal level, with the re-introduction of the Active

Cyber Defense Certainty Bill, a bipartisan bill that is unlikely to make progress; and we see this within various states, perhaps most notably in Georgia (SB 315) where similar proposals were initially passed by the State General Assembly, but later vetoed by the governor citing concerns about inadvertent criminalisation of good actors and the dangers of active defence.

We do not recommend reform of the kind being debated in the US. In our view, focusing on defences/exemptions to allow active defence and hack back creates an unwelcome distraction, and risks the rejection of this extreme option being conflated with rejection of reform altogether. We do not see a call for this kind of reform from the UK cybersecurity and research industries, reflected in the CyberUp Campaign's survey of industry voices. A recent academic paper in the US has also cast doubt on the potential benefits of legalising active defence for cybersecurity professionals in a broad comparative study. Essentially, we see the category-based legalisation of active defence techniques (of the kind debated in the US) as problematic on several related levels: active defence creates more danger of harms to computer systems, potentially misdirected where a false target is identified; can raise extreme public policy concerns where active defence could potentially be used against a foreign state; a lack of proportionality assessment risks escalation and abuse by bad actors taking advantage of the legal provision; and not least, identified categories and the law can become outdated quickly as technology and cyber security techniques evolve.

The public interest defence we recommend is fundamentally different (set out in Section A). Informed by industry and the state (via guidance), the legal test for acting in the public interest will be capable of evolving over time in line with best practice and the new development of technologies and security techniques. The defence test will also operate a proportionally assessment, with the same conduct potentially falling within or without the public interest depending upon the particulars of the cyber threat faced, the options available to the defendant, and the context of their role (i.e. the kinds of factors detailed in the CyberUp Campaign's Principles-Based Framework). Rather than lurching from overcriminalisation to a wild west of active defence, our recommendation offers a practical legal response that retains appropriate public safeguards and remains sensitive to an evolving field.

Israel

Similar approaches to the US, relying on soft-law reassurances, can be seen in several other jurisdictions. For Israel in particular, this has been developed into close working relationships between state and cyber security industries via the Private Protection Authority and National Cyber Directorate; and provided an environment where the industry has arguably flourished. However, though this model of operation can work effectively in smaller jurisdictions, it continues to hold back progress in places like the US and UK where clearer regulatory measures are long overdue.

D. Conclusions for the UK

The pattern of cyber regulation in the UK has remained broadly consistent with other jurisdictions since the creation of the Computer Misuse Act 1990, focusing on expanding liability through the creation of new offences to tackle developing cyber threats. However, in the last 10 years in particular, this model of expanding blanket criminalisation (albeit with few prosecutions) has looked increasingly unfit for the modern world, and multiple jurisdictions have begun to take notice. The exponential growth of cyber technologies (from mobile phones to the internet of things) brings an increasing population within the offences, complicated further by highly technical authorisation arrangements within technologies. And in particular, within this growing population, the application of blanket criminalisation to the socially beneficial conduct of cyber security professionals and researchers stands out as a paradigm of current legal failings. Cybersecurity industries have become necessary for the protection of core computer systems across the economy, and yet they are consistently compromised in their work by a hostile legal framework that criminalises without distinction. As other jurisdictions begin to address this problem – discussed in Section C – we will continue to see the UK fall behind in terms of cyber protection, as well as commercially within a global securities industry.

In tackling the problem of cyber overcriminalisation, it is clear that reliance on the concept of 'authorisation' alone (i.e. working within the current law) will not provide the necessary protections. The concept of 'authorisation' is not an appropriate tool to protect security researchers. Much testing is not expressly mandated or authorised; rather, it is tolerated through vulnerability disclosure policies. Vulnerability disclosure policies can be extremely vague, and perhaps more importantly, the apparent authorisation they give can be rescinded on a whim by the companies which issue them. ENISA called this common practice liability dumping. Uncertainties abound as to what the system owner or controller really authorises. Further, and specifically to the UK, the case of *R v Cuthbert*, and to a lesser extent that of *R v Mangham*, demonstrate that individuals not expressly mandated by a company or vendor can commit CMA offences, even if there is a vulnerability disclosure policy in place.

In line with greater recognition at regional level (Section B), we have traced a variety of jurisdictional responses (Section C) attempting to institute new protections for good actors otherwise caught by an offence. There is merit in each of these approaches, and particularly in providing clear guidelines for prosecuting authorities on how they should exercise their discretion (included within our CLRNN 1 recommendations). But whilst good practice and prosecutorial guidelines provide an important step, they do not provide a fully safe environment for the security industry; they do not protect against a conviction before the courts. It is clear (again, across jurisdictions) that substantive reform is required, not opening the door to a wild west of hack backs, but a mechanism to allow defendants the opportunity to justify their conduct as acting within established good practice in the public interest. And it is this 'public interest' defence model that we continue to endorse.

We set out our recommendations in Section A above, and in full detail within our CLRNN 1 Report. We recommend that the following should be inserted into the CMA:

> ‘It will be a defence to a charge contrary to sections 1 and 3 for a person to prove that in the particular circumstances the act or acts (i) was necessary for the detection or prevention of crime, or (ii) was justified as being in the public interest.’

The defence provided is of a familiar legal construction; and mirrors defences provided within the Data Protection Act 2018 that apply to overlapping offences related to obtaining data (section 170(2)) and re-identifying data (section 172(2)). Crucially, what counts as the public interest will remain an objective question for the court (as opposed to a subjective question for the defendant) guided by principles of industry good practice and secondary guidance as appropriate; and the burden of proving that the defendant was acting in the public interest will be his to discharge, to the civil standard. Such protections allow cyber security professionals and researchers to justify their conduct, whilst maintaining significant safeguards to prevent the defence being used inappropriately; providing a safe and effective means of untying the hands of the cyber industries.

The time for legislative action is now. We see concerns about the hostile environment for cyber security professionals highlighted again recently in the OECD 2021 Report *Encouraging Vulnerability Treatment*; and through the emergence of new global coalitions of those acting to protect the sector (e.g. the CyAN Zero day Legislative Initiative). The UK has a unique opportunity to lead in this area, towards both legally and commercially attractive ends.

Appendix: Computer Misuse Act 1990

The full statute can be accessed here. Below we set out some of the core provisions for ease of reference.

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.

[…]

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

(1) A person is guilty of an offence under this section if he commits an offence under section 1 above ("the unauthorised access offence") with intent—

(a) to commit an offence to which this section applies; or

(b) to facilitate the commission of such an offence (whether by himself or by any other person);

and the offence he intends to commit or facilitate is referred to below in this section as the further offence.

[…]

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

(1) A person is guilty of an offence if—

(a) he does any unauthorised act in relation to a computer;

(b) at the time when he does the act he knows that it is unauthorised; and

(c) either subsection (2) or subsection (3) below applies.

(2) This subsection applies if the person intends by doing the act—

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer; or

(c) to impair the operation of any such program or the reliability of any such data; or

(d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done.

[…]

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

(1) A person is guilty of an offence if—

(a) the person does any unauthorised act in relation to a computer;

(b) at the time of doing the act the person knows that it is unauthorised;

(c) the act causes, or creates a significant risk of, serious damage of a material kind; and

(d) the person intends by doing the act to cause serious damage of a material kind or is reckless as to whether such damage is caused.

[…]

3A Making, supplying or obtaining articles for use in offence under section 1, 3 or 3ZA

(1) A person is guilty of an offence if he makes, adapts, supplies or offers to supply any article intending it to be used to commit, or to assist in the commission of, an offence under section 1, 3 or 3ZA.

(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.

(3) A person is guilty of an offence if he obtains any article—

(a) intending to use it to commit, or to assist in the commission of, an offence under section 1, 3 or 3ZA, or

(b) with a view to its being supplied for use to commit, or to assist in the commission of, an offence under section 1, 3 or 3ZA.

[…]

4 Territorial scope of offences under this Act.

(1) Except as provided below in this section, it is immaterial for the purposes of any offence under section 1, 3 or 3ZA above—

(a) whether any act or other event proof of which is required for conviction of the offence occurred in the home country concerned; or

(b) whether the accused was in the home country concerned at the time of any such act or event.

(2) Subject to subsection (3) below, in the case of such an offence at least one significant link with domestic jurisdiction must exist in the circumstances of the case for the offence to be committed.

(3) There is no need for any such link to exist for the commission of an offence under section 1 above to be established in proof of an allegation to that effect in proceedings for an offence under section 2 above.

[…]

10 Savings

Sections 1 to 3A have effect without prejudice to the operation—

(a) in England and Wales of any enactment relating to powers of inspection, search or seizure or of any other enactment by virtue of which the conduct in question is authorised or required; and

(b) in Scotland of any enactment or rule of law relating to powers of examination, search or seizure or of any other enactment or rule of law by virtue of which the conduct in question is authorised or required

and nothing designed to indicate a withholding of consent to access to any program or data from persons as enforcement officers shall have effect to make access unauthorised for the purposes of any of those sections.

In this section—

“ enactment ” means any enactment, whenever passed or made, contained in—

(a) an Act of Parliament;

(b) an Act of the Scottish Parliament;

(c) a Measure or Act of the National Assembly for Wales;

(d) an instrument made under any such Act or Measure;

(e) any other subordinate legislation (within the meaning of the Interpretation Act 1978);

[…]