The Computer Misuse Act 1990 to support vulnerability research? Proposal for a defence for hacking as a strategy in the fight against cybercrime.

Introduction

Despite the recent push towards security by design and the progress made in achieving more secure IT products, most software and hardware on the market still includes numerous vulnerabilities or flaws.[1] These weaknesses, when discovered and exploited by criminal hackers,[2] compromise the security of networked and information systems (systems). They affect millions of users, as acknowledged by the UK government in its Cybersecurity Strategy launched on 1st November 2016.[3]

Conversely, the removal of these weaknesses significantly contributes to the fight against cybercrime,[4] and, more widely, to the management of digital security and privacy risks, as recognised by the Organisation for Economic Co-operation and Development in 2015.[5] In the race to fix vulnerabilities, security researchers are key actors. Through finding and timely disclosure of vulnerabilities to vendors who supply or service IT products, they help to close the security gap. Nevertheless, when not invited by vendors to hack,[6] they face

[1] In the absence of official definition of vulnerabilities, see the list established by the European Network and Information Security Agency (ENISA) in *Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations* (2015) 14-15 <https://www.enisa.europa.eu/publications/vulnerability-disclosure>, accessed 20 July 2017.

[2] Nicknamed black hats, criminal hackers act alongside script kiddies who lack programming expertise and resort to others' scripts and tools to hack. Alisdair A. Gillepsie, *Cybercrime. Key issues and debates* (OUP 2016) 43-44; Pedro Miguel F. Freitas and Nuno Gonçalves, 'Illegal access to information systems and the Directive 2013/40/EU.' (2015) 29(1) *International Review of Law, Computers & Technology* 50, 56; David Wall, *Cybercrime: The transformation of crime in the information age* (Polity, 2007), .53-56

[3] UK National Cybersecurity Strategy 20, 22-23, <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/564268/national_cyber_security_strategy.pdf> accessed 20 July 2017.

[4] European Parliament, LIBE, *Report on the fight against cybercrime*, (2017/2068 (INI), 25 July 2017, para 21, 34, at <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2017-0272+0+DOC+PDF+V0//EN>; Benoît Dupont, 'Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime', (2016) *Crime Law and Social Change* 1, 2; Amanda Craig and Scott Shackelford, 'Hacking the Planet, the Dalai Lama, and You: Managing Technical Vulnerabilities in the Internet Through Polycentric Governance' (2014) 24 *Fordham Intellectual Property, Media & Entertainment Law Journal* 381; Michael Levi and Matthew Leighton Williams, 'Multi-agency partnerships in cybercrime reduction' (2013) 21(5) *Information Management & Computer Security* 420; Scott J. Shackelford, Scott Russell and Jeffrey Haut, 'Bottoms up: A Comparison of Voluntary Cybersecurity Frameworks' (2015) 16 UC Davis Bus. LJ 217.

[5] OECD, *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document* (OECD, 2015) 14. On the Governments' use of vulnerabilities to conduct mass surveillance: Stefan Schuster, Melle Van Den Berg, Xabier Larrucea, Ton Slewe, and Peter Ide-Kostic, 'Mass surveillance and technological policy options: Improving security of private communications' (2017) 50 *Computer Standards & Interfaces* 76, 79-80; European Parliament, LIBE, 'Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices', (2017) PE 583.137, at <http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf> accessed 20 July 2017; European Data Protection Supervisor (EDPS), *Dissemination and use of intrusive surveillance technologies*, Opinion 8/2015, 6-7 <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-12-15_Intrusive_surveillance_EN.pdf> accessed 20 July 2017.
DOI: http://dx.doi.org/10.1787/9789264245471-en accessed 20 July 2017.

[6] The terminology referring to these security researchers is not clear, and therefore will not be used in this article. Some consider them to be grey hats because they ask for rewards (Freitas (n 2); C. Kirsch, 'The Grey

significant criminal law challenges. Taking stock of these issues, which remain substantially understudied in the UK,[7] this paper proposes a new defence of public interest to offences under the Computer Misuse Act.

In November 2015 the European Network and Information Security Agency (ENISA) concluded that, in the US and the EU, the threat of prosecution under computer misuse legislations 'can have a chilling effect'. [8] Security researchers are 'discentivise[d]' to find vulnerabilities, especially when working independently without vendors' prior authorisation. They potentially violate hacking laws criminalising unauthorised access to systems, and run the risk of being treated like criminal hackers. In the UK, like in other countries,[9] the risk has already been realised. Two independent security researchers were sentenced for unauthorised access to systems under the Computer Misuse Act 1990 (CMA).[10] Yet, one judge has expressed 'some considerable regret' in having to find 'the case proved against' the defendant.[11]

This paper argues that this challenging situation in the UK results from a conscious recommendation in 1989 to criminalise hacking, without exceptions, including when done for security purposes.[12] This choice needs revisiting so that criminal law can 'appropriately facilitate […] rather than inappropriately obstruct' security research.[13]

Only a handful of law academics, mostly focusing on US federal criminal law, have addressed ways to transform criminal law into a supportive tool for independent security researchers. They have argued for a 'safe harbour' without being clear about whether this would take the form of a defence justifying the commission of crime or of an exemption

Hat Hacker: Reconciling Cyberspace Reality and the Law' (2014) 41(3) *New Kentucky Law Review* 383), because they do not have authorisation (Thomas Wilhem, Professional Penetration Testing (Elsevier, 2013)) or because they sell the information to Governments (Marilyn Fidler, 'Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis.' (2015) 11 *I/S Journal of Law and Policy for the Information Society* 405, 410-412); others may consider them as white hats if they act ethically (Trevor A. Thompson, 'Terrorizing the Technological Neighborhood Watch: The Alienation and Deterrence of the White Hats under the CFAA.' (2008) 36 *Fla. St. UL Rev.* 537).

[7] The only existing analysis of UK criminal law is that of Andrew Cormack, 'Can CSIRTs Lawfully Scan for Vulnerabilities.' (2014) 11:3 *SCRIPTed* 308 <http://script-ed.org/?p=1671> accessed 20 July 2017. Gillepsie mentions the issue in passing, (n 2). Non-UK authors referred briefly to UK law: Thompson (n 6); Alana Maurushat, *Disclosure of Security Vulnerabilities: Legal and Ethical Issues* (Springer 2013) ch 4

[8] ENISA (n 1) 65-66.

[9] For other countries: US v. Auernheimer, 748 F.3rd 525 (3rd Cir. 2014), commented upon in C Kirsch (n 6); France, Cour de cassation, Crim. 20 May 2015, Olivier Laurelli, Pourvoi 14-81336, at Legifrance.gov.fr, with the first instance case reported in English language by Megan Geuss, 'French journalist 'hacks' govt by inputting correct URL, later fined $4,000+', *Ars Technica* 09 February 2014, https://arstechnica.com/tech-policy/2014/02/french-journalist-fined-4000-plus-for-publishing-public-documents/ ; for other cases, notably in New Zealand and the US, Maurushat (n 7) 35-52.

[10] *R v Cuthberth* (Crown Court, 2005, unreported); John Oates, 'Tsunami hacker convicted. Fine + costs for Daniel Cuthbert', The Register, 06 October 2005 at http://www.theregister.co.uk/2005/10/06/tsunami_hacker_convicted/; Peter Sommer, 'Two Recent Computer Misuse Cases', (2006) 16/5 *Computers & Law* January, https://www.pmsommer.com/CLCMA1205.pdf accessed 20 July 2017; *R v Mangham* [2012] EWCA Crim 973; Graham Cluley, 'Jail for "ethical" hacker who bypassed Facebook security from his bedroom', *Sophos*, 20 February 2012, at https://nakedsecurity.sophos.com/2012/02/20/jail-facebook-ethical-hacker/ accessed 20 July 2017.

[11] *R v Cuthbert,* in John Oates (n 10).

[12] ENISA (n 1) 65-66.

[13] ENISA (n 1) 70.

whereby no crime would be *a priori* committed because security researchers would be considered authorised to hack.[14]

In contrast, my proposal for a defence for CMA offences clearly shifts the discussion away from the controversial question of authorisation, and would provide security researchers, when prosecuted, with a mechanism to demonstrate to the courts that, contrary to criminal hackers, they have acted in the public interest and proportionately.

This paper will start by explaining why independent security researchers are needed, so as to underline how their work contributes to the public interest. After a presentation of the current criminal law challenges inherent in the process of vulnerability research, three options for tackling these challenges will be explored. First is modifying the structure of the current CMA offence of unauthorised access, along the lines explored by the Scottish and English Law Commissions in 1987 and 1988. The second option of improving the current CPS guidelines would be a first step in the right direction. However, only the third option, a public interest defence, would provide a statutory basis for security researchers to argue before the courts that their actions were proportionate to the public interest objective they sought to achieve. A defence for all CMA offences would allow criminal law to recognise security researchers' fundamental contribution to the disruption of the technical infrastructure on which the criminal underground relies.[15]

1 – The need for vulnerability research and independent security researchers

Vulnerability research is a response to a persistent and ubiquitous lack of security in IT systems. Various actors engage in vulnerability research, with independent security researchers representing just one of the many groups searching for vulnerabilities. The latter's contribution to vulnerability research should be recognised as essential to a strategy of securing products for the benefit of the wider public.

1.1 - The persistence of ubiquitous insecurity

The 'Achilles' heel of information systems',[16] vulnerabilities can cut across a variety of products created by different vendors[17]. They exist in all types of devices (desktops, laptops,

[14] Brent Wible, 'A site where hackers are welcome: Using hack-in contests to shape preferences and deter computer crime.' (2003) 112(6) *The Yale Law Journal* 1577, 1601-1602, with the exemption only during hacking contests; Thompson (n 6) 578-580; Kirsch (n 6) 400-401; outside the US, Maurushat (n 7); without discussion of the exemption, Taiwo A Oriola, 'Bugs for sale: Legal and ethical proprieties of the market in software vulnerabilities.' (2010) 28 *J. Marshall J. Computer & Info. L.* 451, 507. For Germany, Dominik Brodowski does not suggest a reform, '(Ir-)responsible disclosure of software vulnerabilities and the risk of criminal liability', (2015) *Information technology: IT* 357.

[15] UK Cybersecurity Strategy (n 3) 20, 22-23; see also, B Dupont (n 4).

[16] Schuster, Van Den Berg, Larrucea, Slewe, and Ide-Kostic (n 5) 79; Kirsch (n 6) 395.

[17] Notably, Antonio Nappa, Richard Johnson, Leyla Bilge, Juan Caballero and Tudor Dumitras, 'The attack of the clones: A study of the impact of shared code on vulnerability patching', in *2015 IEEE Symposium on Security and Privacy (SP)* 692; Amiangshu Bosu, Jeffrey C. Carver, Munawar Hafiz, Patrick Hilley and Derek Janni, 'Identifying the characteristics of vulnerable code changes: An empirical study', in *Proceedings of the 22nd ACM SIGSOFT International Symposium on Foundations of Software Engineering* (ACM 2014) 257, 262; Ashish Arora, Chris Forman, Anand Nandkumar and Rahul Telang, 'Competition and patching of security

mobile phones, IoT) and affect all hardware and software: operating systems - whether Linux, Apple, Windows or Android, applications, internet protocols, access routers, even anti-virus software and firewalls.[18] Given that they can remain undiscovered for long periods they tend to accumulate over the years, despite increasing efforts to detect and remove them.[19]

The ever-increasing complexity of software (Windows 7 contains 40 millions lines of code), and the emphasis on interoperability to facilitate communications and transfer of data between operating systems, impede the ability to design secure products.[20] '[M]ore attention [is paid] to features than to fundamental security'.[21] Other factors contribute to insecurity being ubiquitous: the Internet not being designed with security in mind,[22] and the exponential 'growth of societal dependency on globally interconnected technology'.[23]

Since as far back as 1949 functionality bugs and security vulnerabilities have been recognised as an unwanted but inevitable outcome of creating software and hardware. [24] They need to be found and fixed even after the product has been released onto the market.[25] However, establishing effective strategies to mitigate the creation of vulnerabilities has remained

vulnerabilities: An empirical analysis' (2010) 22(2) *Information Economics and Policy* 164, 166; Kirsch (n 7) 395.

[18] For an overview, Craig and Shackelford (n 4); Meiring De Villiers, 'Enabling Technologies of Cyber Crime: Why Lawyers Need to Understand It.' (2011) 11 *Pitt. J. Tech. L. & Pol'y* 1, 43; Ravi Sen and Sharad Borle. 'Estimating the Contextual Risk of Data Breach: An Empirical Approach' (2015) 32(2) *Journal of Management Information Systems* 314, 333.

[19] Oriola (n 14) 466; ENISA (n 1) 32-36.

[20] Code is a set of rules or instructions made of numbers, symbols and/or words, and which forms part of a programme. Ross Anderson, 'Why information security is hard-an economic perspective' in *Computer security applications conference, 2001. acsac 2001. proceedings 17th annual* (IEEE, 2001) 358, 363; Craig and Shackelford (n 4) 410; Jay P. Kesan and Carol M. Hayes, 'Bugs in the Market: Creating a Legitimate, Transparent, and Vendor-Focused Market for Software Vulnerabilities' (2016) 58 *Ariz. L. Rev.* 753, 787; Oriola (n 14) 466. Lessig has used the term in a more general sense, to mean the Internet technical architecture of software and hardware, *Code 2.*0, 2006, <http://codev2.cc/> accessed 20 July 2017.

[21] Bell, author of the influential cybersecurity models of the 1970s and 1980s, David Elliott Bell, 'Looking back at the bell-la padula model' In *Computer Security Applications Conference, 21st Annual* (IEEE 2005) 15, para. 7.2 ; Oriola (n 12) 467 fn 101 and 102

[22] Craig and Shackelford (n 4) 395; Sandra Braman, 'The framing years: Policy fundamentals in the Internet design process, 1969–1979.' (2011) 27(5) *The Information Society* 295, 300-302; Yanyan Li and Keyu Jiang, 'Prospect for the future internet: A study based on TCP/IP vulnerabilities.' In *Computing, Measurement, Control and Sensor Network (CMCSN), 2012 International Conference*, IEEE, 2012, 52; Malte Ziewitz and Ian Brown, 'A Prehistory of Internet Governance', in Ian Brown (ed.), *Research Handbook on Governance of the Internet* (Edward Elgar, 2013) 3.

[23] Rolf H. Weber and Evelyne Studer, 'Cybersecurity in the Internet of Things: Legal aspects' (2016) 32(5) *Computer Law & Security Review* 715, 716

[24] In 1949, Wilkes, British computer scientist, recognized that debugging will be part of his job of creating code, cited in Craig and Shackelford (n 3) 410; Robert W Hahn and Anne Layne-Farrar, 'The law and economics of software security' (2006) 30 *Harv. JL & Pub. Pol'y* 283, 296-297; Oriola (n 14) 465; Jaziar Radianti and Jose J. Gonzalez, 'A preliminary model of the vulnerability black market', in *25th International System Dynamics Conference at Boston, USA* 2007, 5 <http://www.academia.edu/download/42408398/RADIA352.pdf> accessed 20 July 2017. See also, security and cryptography expert, Bruce Schneier, *Secrets and lies: digital security in a networked world* (John Wiley & Sons, 2011) 209-210.

[25] Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau, 'Lawful hacking: Using existing vulnerabilities for wiretapping on the Internet.' (2014) 12 *Nw. J. Tech. & Intell. Prop.* 27, para 67; Nuthan Munaiah, Felivel Camilo, Wesley Wigham, Andrew Meneely and Meiyappan Nagappan, 'Do bugs foreshadow vulnerabilities? An in-depth study of the chromium project' (2016) *Empirical Software Engineering* 1, 34.

challenging. Security by default remains often an after-thought in the design of IT products.[26] Due to insufficient (or a lack of) training and experience in cybersecurity, most software developers cannot recognise and avoid creating vulnerabilities.[27] To compound the problem, internationally recognised technical standards for good quality software have not always integrated security as a formal requirement[28] and are still on-going.[29] Moreover, economic incentives for security by design have so far failed to significantly improve the security of IT products. Vendors continue to mostly abide by the 'penetrate [the market] first and patch later' motto.[30] Although good security can be part of a marketing strategy to increase brand trustworthiness, most vendors continue to consider that 'the harm as experienced by the individual user [because of the security flaw] is […] an externality not borne by the vendor'.[31] This behaviour, denounced as a threat to security as early as in the late 1960s,[32] runs counter to security by design, which requires time to create and analyse products.[33]

To reduce the number of vulnerabilities created, emphasis is put on better software hygiene or assurance – i.e. better processes in the designing of products - and closing the gap in security skills, as notably acknowledged in the UK Cybersecurity Strategy in November 2016.

[26] Ari Takanen, Petri Vuorijärvi, Marko Laakso and Juha Röning, 'Agents of responsibility in software vulnerability processes' (2004) 6(2) *Ethics and Information Technology* 93, 108; Daniel Hein and Hossein Saiedian, 'Secure software engineering: Learning from the past to address future challenges' (2009) 18(1) *Information Security Journal: A Global Perspective* 8, 11; Karina Curcio, Andreia Malucelli, Sheila Reinehr and Marco Antônio Paludo, 'An analysis of the factors determining software product quality: A comparative study.' (2016) 48 *Computer Standards & Interfaces* 10; Nabil M. Mohammed, Mahmood Niazi, Mohammad Alshayeb and Sajjad Mahmood, 'Exploring software security approaches in software development lifecycle: A systematic mapping study' (2017) 50 *Computer Standards & Interfaces* 107, 113.

[27] Malik Aleem Ahmed and Jeroen van den Hoven, 'Agents of responsibility—freelance web developers in web applications development' (2010) 12(4) *Information Systems Frontiers* 415; Andrew Austin and Laurie Williams, 'One technique is not enough: A comparison of vulnerability discovery techniques', in *2011 International Symposium on Empirical Software Engineering and Measurement* (IEEE 2011) 97; Bosu, Carver, Hafiz, Hilley and Janni (n 17) 264, 265; Muhammad Adnan, Mike Just, Lynne Baillie, Hilmi Gunes Kayacik,'Investigating the work practices of network security professionals' (2015) 23(3) *Information & Computer Security* 347.

[28] Rahul Telang and Sunil Wattal, 'An empirical analysis of the impact of software vulnerability announcements on firm stock price' (2007) 33(8) *IEEE Transactions on Software Engineering* 544, 545; Sanjay Bahl and O.P. Wali, 'Perceived significance of information security governance to predict the information security service quality in software service industry' (2014) 22(1) *Information Management & Computer Security* 2.

[29] As acknowledged in its draft Recital 9 of the future Directive 2013/40/EU, by Rapporteur Monika Hohlmeier, for the EU Parliament, *Draft Report on the proposal for a directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA*, 2010/0273 (COD), 24 November 2011, 'Brian Henderson-Sellers, Cesar Gonzalez-Perez, Tom Mcbride and Graham Low, 'An ontology for ISO software engineering standards: 1) Creating the infrastructure' (2014) 36(3) *Computer Standards & Interfaces* 563; Richard Kemp, 'ISO 27018 and personal information in the cloud: First year scorecard' (2015) 31(4) *Computer Law & Security Review* 553.

[30] Rainer Böhme, 'Vulnerability Markets. What Is the Economic Value of a Zero-day Exploit?' *Paper Held at the 2005 Chaos Communication Congress Berlin, Germany*. 2005, in *22C3: Private Investigations*. *Chaos Computer Club, Berlin, Germany,* 2005, 1; Ashish Arora, Jonathan P. Caulkins and Rahul Telang, 'Research Note—Sell First, Fix Later: Impact of Patching on Software Quality', (2006) 52(3) *Management Science* 465; Telang and Wattal, (n 31) 545; Ross Anderson, Rainer Böhme, Richard Clayton and Tyler Moore, 'Security economics and the internal market' *Study commissioned by ENISA* (2008), <https://www.enisa.europa.eu/publications/archive/economics-sec> accessed 20 July 2017; Oriola (n 14) 469-473.

[31] Kesan and Hayes (n 20) 781; Hasan Cavusoglu, Huseyin Cavusoglu and Jun Zhang, 'Security Patch Management: Share the Burden or Share the Damage?' (2008) 54(4) *Management Science* 657.

[32] Bell (n 21) para. 2 and 7.2.

[33] Hein and Saiedian (n 26) 10.

However, 'software security is essentially relative'.[34] Vulnerability-free products are 'virtually impossible'.[35] To compound the problem, the interconnectedness of systems multiplies the impact a single vulnerability can have. Yet, the same interconnectedness increases the positive effects of removing vulnerabilities. Vulnerability research benefits all stakeholders in cyberspace. Hence, the need for it to be undertaken effectively.

Many vendors who supply IT products and/or are system owners using these products have recognised this necessity to find and patch vulnerabilities. Consequently, they employ and authorise one or several persons to search for vulnerabilities.[36] They also resort to hacking contests through intermediaries such as HackerOne, effectively authorising hacking to a number of chosen security researchers.[37] In these circumstances, issues of criminal law are unlikely to arise.[38]

National governments, whether linked to national intelligence agencies or to law enforcement forces, also actively search for vulnerabilities in computer systems. Whether they are authorised to do so, and, if so, to what extent, is a grey area. Those questions are outside the scope of this paper, for they raise particular issues of national security and policing.

The other actors engaged in vulnerability research are independent security researchers. This very diverse group can include students, academics, free-lance professionals or just amateurs in computer science who may be knowledgeable but work in their spare time.[39] As they have not been hired by vendors they may appear to be vigilantes, taking the issue of cybersecurity into their own hands instead of leaving the discovery of vulnerabilities to vendors. However, the work of independent security researchers is essential to the improvement of the security of IT products, .

1.2 - The need for independent security researchers

It could be argued that vendors and system owners should be the only ones deciding who is allowed to penetrate their IT systems to discover vulnerabilities.[40] However, several factors demonstrate the need for independent vulnerability research.

To the best of our knowledge the necessity of *independent* researchers' work has not yet been clearly articulated in the legal literature,[41] despite some references to the concept of public

[34] Oriola (n 14) 472; Thompson (n 6) 543-548.

[35] Jay Pil Choi, Chaim Fershtman and Neil Gandal, 'Network security: Vulnerabilities and disclosure policy' (2010) 58(4) *The Journal of Industrial Economics* 868, 869.

[36] The practice originates from the US Government, especially the Department of Defence, Bell (n 21) para 2; Edward Hunt, 'US Government Computer Penetration Programs and the Implications for Cyberwar' (2012) 34(3) *IEEE Annals of the History of Computing* 4, 6, 15. The practice then spread to the private sector, D. Russell and G.T. Gangemi, *Computer Security Basics* ('O'Reilly Media, Inc.' 1991) 23-31.

[37] Wible (n 14).

[38] Maurushat (n 7) 10.

[39] ENISA (n 1) 20-21; Munawar Hafiz and Ming Fang, 'Game of detections: how are security vulnerabilities discovered in the wild?' (2015) *Empirical Software Engineering* 1, 12; Serge Egelman, Cormac Herley and Paul C. Van Oorschot, 'Markets for zero-day exploits: Ethics and implications', in *Proceedings of the 2013 workshop on New security paradigms workshop* (ACM 2013) 41, 44.

[40] Infra section 3.4

[41] Kesan and Hayes (n 20) 787-791; Craig and Shackleford (n 4); Thompson (n 6) 543-555; Kirsch (n 6) 383-392; Wible (n 14); Mailyn Fidler, 'Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis' (2015) 11 *I/S Journal of Law and Policy* 405, which is a summary of her PhD, *Anarchy or Regulation:*

interest.[42] Concerning the abundant computer science and economics literature on vulnerability research and markets, the picture is more complex. The benefits independent security researchers bring have been articulated[43] at times but generally they tend to be assumed and/or conflated with other matters, such as the benefits of vulnerability markets and how they should be organised or regulated,[44] and the benefits of full disclosure of vulnerabilities and their exploits.[45] The benefits of legitimate vulnerability research can also emerge through studies on the black markets in which criminal hackers participate[46] or grey markets where governments buy vulnerabilities to exploit them.[47]

The literature points to four factors explaining why the work of independent security researchers is indispensable to preventing cybercrime.

Firstly, as the US government found with the 'tiger teams' in the late 'sixties, different teams discover different vulnerabilities simply because of the diversity of skills within the hired teams.[48] In other words, no single security researcher is likely to find all vulnerabilities in a product, not the least because of the diversity of vulnerabilities and related discovery techniques available.[49] Even vendors such as Microsoft or Google, with an important team of

Controlling The Global Trade in Zero-Day Vulnerabilities. Diss. Master Thesis. Stanford University, 2014, https://d1x4j6omi7lpzs. cloudfront. net/live/wp-content/uploads/2014/06/Fidler-Zero-Day-Vulnerability-Thesis.pdf accessed 20 July 2017.

[42] Maurushat (n 7) 48-51.

[43] Andy Ozment, 'The Likelihood of Vulnerability Rediscovery and the Social Utility of Vulnerability Hunting.' *Worshop on the Economics of Information security* 2005 <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.479.7888&rep=rep1&type=pdf> accessed 20 July 2017; Egelman, Herley and Van Oorschot (n 36).

[44] Notably, Andy Ozment, 'Bug Auctions: Vulnerability Markets Reconsidered,' *Workshop on the Economics of Information Security 2004* 19, and his PhD, *Vulnerability discovery & software security*, PhD diss., University of Cambridge, 2007, <http://andyozment.com/papers/ozment_dissertation.pdf > accessed 20 July 2017; Böhme (n 26); Charlie Miller, 'The legitimate vulnerability market: Inside the secretive world of 0-day exploit sales' *Sixth Workshop on the Economics of Information Security* 2007, < http://weis07.infosecon.net/papers/29.pdf > accessed 20 July 2017; Sam Ransbotham, Sabyasachi Mitra and Jon Ramsey, 'Are markets for vulnerabilities effective?' *ICIS 2008 Proceedings* 24; Pankaj Pandey and Einar Arthur Snekkenes, 'An assessment of market methods for information security risk management' *16th IEEE International Conference on High Performance and Communications, WiP track*. 2014; Andreas Kuehn and Milton Mueller, 'Shifts in the Cybersecurity Paradigm: Zero-Day Exploits, Discourse, and Emerging Institutions' In *Proceedings of the 2014 workshop on New Security Paradigms Workshop* (ACM 2014) 63; ENISA (n 1) 55. Contra Karthik Kannan and Rahul Telang, 'Market for software vulnerabilities? Think again.' (2005) 51(5) *Management Science* 726.

[45] Pu Li and H. Raghav Rao, 'An examination of private intermediaries' roles in software vulnerabilities disclosure' (2007) 9(5) *Information Systems Frontiers* 531; Jukka Ruohonen, Sami Hyrynsalmi and Ville Leppănen, 'Trading exploits online: A preliminary case study', in *2016 IEEE Tenth International Conference on Research Challenges in Information Science (RCIS)* (IEEE 2016) 1.

[46] Jaziar Radianti and Jose J. Gonzalez, 'Understanding hidden information security threats: The vulnerability black market', in *HICSS 2007. 40th Annual Hawaii International Conference on System Sciences* (IEEE 2007) 156c; Radianti and Gonzalez (n 22); Jaziar Radianti, Eliot Rich and Jose J. Gonzalez, 'Vulnerability black markets: Empirical evidence and scenario simulation', in *2009. HICSS'09. 42nd Hawaii International Conference on System Sciences* (IEEE 2009) 1; Jaziar Radianti, Jose J. Gonzalez and Eliot Rich, 'A quest for a framework to improve software security: Vulnerability black markets scenario' *Proceedings of the 27th International Conference of the System Dynamics Society* 2009 < https://pdfs.semanticscholar.org/0f29/b736c7787eaca6cd13a7fa670e258a1fdcf4.pdf> accessed 20 July 2017.

[47] Jart Armin, Paolo Foti and Marco Cremonini, '0-Day Vulnerabilities and Cybercrime', in *2015 10th International Conference on Availability, Reliability and Security (ARES)* (IEEE 2015) 711, 716-717; Schuster, Van Den Berg, larrucea, Sleew and Ide-Kostic (n 4) 80.

[48] Bell (n 19); Egelman, Herley and Van Oorschot (n 39).

[49] On the diversity of techniques, Austin and Williams (n 27). On the tendency for security researchers to specialize in certain types of vulnerabilities, Mingyi Zhao, Jens Grossklags and Peng Liu, 'An empirical study

experts dedicated to security research, will miss vulnerabilities through no fault of their own. Better security depends on independent security researchers filling the gaps and sharing this information[50]. Vendors may want to rely on a number of well-known security researchers but they should accept a wider pool of independent researchers submitting reports to improve security. [51]

Secondly, recent academic studies have demonstrated that, from vendors' point of view, the work of independent researchers is particularly cost-effective, from 2 to 100 times more cost-effective than hiring a security researcher full-time. The rewards that vendors, such as Google and Mozilla, pay to independent security researchers when averaged over one year cost less than employing one security researcher.[52]

Thirdly, vulnerabilities are bound to be discovered by anybody looking for them.[53] As noted above, a diversity of skills and experience is needed to find a wide range of vulnerabilities in a product. Being a vendor, even with a big team, does not guarantee discovering the vulnerability first. A criminal hacker may well discover and exploit the vulnerability without the vendor's knowledge, conducting what is called a zero-day attack.[54] Independent security researchers play an integral part in this race against criminal hackers.

Finally, vulnerability research must be placed in the wider context of cybersecurity practices. Good security for digital products is not necessarily achieved through obscurity but through openness and thus exposure to hacking, whether by criminal hackers or independent security researchers. Cryptography[55] and open-source software[56] are two areas where openness prevails. Counter-intuitively, the security of these products tends to be better than that of the average proprietary product. Openness increases the risk of harm since, for open-source products, criminal hackers can access the code at any time and find vulnerabilities. However,

of web vulnerability discovery ecosystems', In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (ACM 2015) 1105, 1108-1112; Hafiz and Fang (n 39).

[50] MITRE, at https://cve.mitre.org/about/faqs.html#cve_identifier_descriptions_created> accessed on 26 July 2017

[51] Zhao, Grossklags and Liu (n 49) 1115; Matthew Finifter, Devdatta Akhawe and David Wagner, 'An Empirical Study of Vulnerability Rewards Programs', in (2013) 23 *USENIX Security* 273, 279, 273-288.

[52] Finifter, Akhawe and Wagner (n 51) 280, 286. See also Aron Laszka, Mingyi Zhao and Jens Grossklags, 'Banishing misaligned incentives for validating reports in bug-bounty platforms' In Ioannis Askoxylakis, Sotiris Ioannidis, Sokratis Katsikas and Catherine Meadows (eds), *European Symposium on Research in Computer Security* (Springer 2016) 161.

[53] Kesan and Hayes (n 20) 801; Miller (n 44); Ian Brown, Lilian Edwards and Christopher Marsden, 'Information security and cybercrime', in Lilian Edwards and Charlotte Waelde (eds), *Law and the Internet* (3rd edn, Hart 2009), 671, 687-692; Fidler, 'Regulating the Zero-Day Vulnerability Trade' (n 41) 462-465.

[54] Stefan Frei, Martin May, Ulrich Fiedler, and Bernhard Plattner, 'Large-scale vulnerability analysis' in *Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense* (ACM 2006) 131; Leyla Bilge and Tudor Dumitras, 'Before we knew it: an empirical study of zero-day attacks in the real world', in *Proceedings of the 2012 ACM conference on Computer and communications security* (ACM, 2012) 833.

[55] Bruce Schneier, 'Open Source and Security' 15 September 1999, <https://www.schneier.com/crypto-gram/archives/1999/0915.html> accessed 20 July 2017. The US Government's initial approach to cryptography favouring secrecy gave way to full openness due to the failure to create valid encryption.

[56] Successful OSS are Linux, Firefox Mozilla, and Oracle products. Guido Schryen and Eliot Rich, 'Increasing software security through open source or closed source development? Empirics suggest that we have asked the wrong question' in *2010 43rd Hawaii International Conference on System Sciences (HICSS)* (IEEE, 2010) 1; confirmed in Orcun Temizkan, Ram L. Kumar, Sungjune Park and Chandrasekar Subramaniam, 'Patch release behaviors of software vendors in response to vulnerabilities: an empirical analysis' (2012) 28(4) *Journal of management information systems* 305, 328-329; Mario Silic, Andrea Back, and Dario Silic, 'Taxonomy of technological risks of open source software in the enterprise adoption context' (2015) 23(5) *Information & Computer Security* 570, 571.

openness fosters strong collaboration between stakeholders, who feel responsible for the security of all users. Thus, they internalise the costs of attacks instead of externalising them to the users. In other words, openness increases security.[57]

In light of all these elements, independent security researchers significantly contribute to improving the security of IT systems. Their work is necessary and benefits the wider public, not just vendors. These concepts of necessity and public interest are familiar to criminal law defences[58] but have only just started to be recognised in cybercrime.[59] So far, the legal challenges inherent in the process of vulnerability research have dominated the conversation.

2 – The criminal law challenges inherent in vulnerability research carried out by independent security researchers

Vulnerabilities' impact on security corresponds to the harms which the UK CMA and international instruments such as the Convention on Cybercrime aim to prevent. Thus, security researchers are no more than a step away from committing crime. A more detailed review of the process of vulnerability research demonstrates that the process can trigger the application of criminal law even when security researchers have no intention of becoming criminal hackers.

2.1 - Vulnerabilities' impact and corresponding harms: the triad of confidentiality, integrity and availability (CIA)

Vulnerabilities are assigned two identifiers, both created by the US MITRE organisation and which have become the industry standard worldwide[60]: a CVE identifier that lists the vulnerabilities' characteristics,[61] and a Common Weaknesses Enumeration (CWE) ID that

[57] Supra notes 54 and 55; Peter P. Swire, 'A model for when disclosure helps security: What is different about computer and network security.' (2004) 3 *J. on Telecomm. & High Tech. L.* 163, reproduced in M. Grady and Francisco Parisi (eds), *The law and economics of cybersecurity* (Cambridge University Press 2006) 29, 45; Steven Michael Bellovin and Randy Bush, *Security Through Obscurity Considered Dangerous*, Working draft for the Internet Engineering Task Force, 2002 at http://hdl.handle.net/10022/AC:P:9172

[58] Notably the defences of self-defence and duress, where the defendant may be found not guilty if his actions were strictly necessary and proportionate to the threat faced. Jeremy Horder, *Ashworth's Principles of Criminal Law* (8th edn, OUP 2016) 134-142, 147-153, 227-237; David Ormerod and Karl Laird, *Smith and Hogan's Criminal Law* (14th edn, OUP 2015) 322-324, ch 12; John Gardner, *Offences and Defences. Selected Essays in the Philosophy of Criminal Law* (OUP 2007) ch 4 and 5; George P Fletcher, *The Grammar of Criminal Law, American, Comparative and International. Volume One: Foundations* (OUP 2007) 165-66, 197, 310, 321-324.

[59] Infra section 4. See also Maurushat (n 7) 48-51..

[60] ITU endorsed the CVE standard in 2011 "as a part of its new "Global Cybersecurity Information Exchange techniques (X.CYBEX)" by issuing Recommendation ITU-T X.1520 Common Vulnerabilities and Exposures (CVE), that is based upon CVE's current Compatibility Requirements," (see CVE website, https://cve.mitre.org/about/). The other databases of vulnerabilities also use the CVE repository (see next footnote).

[61] Two databases using CVE exist: the National Vulnerability Database (NVD) and the OVAL database hosted now by GitHub. The Open Source Vulnerability Database (OSVDB) created in 2004 to aggregate all information closed on 5 April 2016. On those dabatases, see notably Sugandh Shah and Babu M. Mehtre, 'An overview of vulnerability assessment and penetration testing techniques' (2015) 11(1) *Journal of Computer Virology and Hacking Techniques* 27; Sushama Karumanchi and Anna Cinzia Squicciarini, 'In the wild: a large

describes the vulnerabilities' impacts on security in terms of a possible breach of the confidentiality, integrity and/or availability of an IT system.[62]

Discovering a vulnerability endangering the confidentiality of a system will enable the disclosure of information which is usually private or confidential. A potential breach of integrity facilitates compromising the system owner's ability to maintain, ensure and account for the accuracy and consistency of the systems and data held. A wide range of situations are covered: attempts to access an IT system without the owner's authorisation, unauthorised exploration of the accessed system or network, damage to data, and installation of malware with subsequent impacts on the trustworthiness and veracity of the data. Finally, a breach of availability is associated with impaired or impossible access to a computer system or program.

This triad of confidentiality, integrity and availability (CIA) describes what the language of criminal law would call the harms resulting from the exploitation of vulnerabilities.[63] The Council of Europe's Convention 185 on cybercrime expressly acknowledged the link between the CIA and criminal law by classifying computer misuse offences under Title 1's heading of 'offences against the confidentiality, integrity and availability of computer data and systems'. In contrast, the UK CMA does not refer to these three possible harms but, like other computer misuse legislations, it was drafted with some, if not all, of those harms in mind.[64]

The offence of 'unauthorised access' under s1 CMA aims to deter a hacker from committing any act with intention to secure access to data, programs or computer systems. This act, on its own, breaches the integrity of the IT system, and could lead to breaches of confidentiality and/or availability. The offences of s3 CMA and, when critical infrastructures are involved, of s3ZA CMA, prohibit any act with intent to, or recklessness as to impairing, the operation of a computer or reliability of data. Thus, they protect against breaches of integrity and availability, for example where the vulnerability would enable the installation of malware or the triggering of a denial of service attack.

As vulnerabilities are so closely related to harms, from the system owner's point of view, the discovery of vulnerabilities may at the very least create a risk of harm. Thus, the security researcher is no more than a step away from committing a crime. A more detailed analysis of the process of vulnerability research reveals that the independent security researcher's legal position is even worse than the vulnerabilities' impact surmises.

2.2 - The process of vulnerability research: harms and criminal liability

scale study of web services vulnerabilities', in *Proceedings of the 29th Annual ACM Symposium on Applied Computing* (ACM 2014) 1239.

[62] R. A. Martin, 'Non-Malicious Taint: Bad Hygiene is as Dangerous to the Mission as Malicious Intent' Report for MITRE, n.13-4399, at 6 Table 1 <https://www.mitre.org/publications/technical-papers/non-malicious-taint-bad-hygiene-is-as-dangerous-to-the-mission-as.> accessed 20 July 2017. On the CWE, Hein and Saiedian (n 26) 17-18.

[63] On the triad, James P Anderson, *Computer security technology planning study*, 1972. L.G. Hanscom Field, Bedford (MA): Deputy for Command and Management Systems, HQ Electronic Systems Division (AFSC). Report No.: ESD-TR-73-51, Vol. I, NTIS AD-758 206, <http://nob.cs.ucdavis.edu/history/papers/ande72a.pdf > accessed 20 July 2017.

[64] Infra section 3.4

The process of vulnerability research includes three stages: discovery, verification and disclosure of the vulnerability. At each stage the security researcher's activities may be harmful to the vendor. Given that the CMA offences were designed to protect against those harms, the security researcher may be criminally liable for at least one if not several of those offences.

2.2.1 - The discovery of vulnerabilities

A detailed analysis of the complex process of discovery is difficult in the space of this article but it is still possible to pinpoint where the process may harm or create a risk of harm to the vendor, and thus where the security researcher may be criminally liable.

2.2.1.1 - The harms

Since neither the independent security researcher nor the criminal hacker are likely to have contacted the vendor prior to the search the vendor cannot attribute actions to a particular person. Vendors must rely on objective analysis of conduct to understand who is who. The problem is that the security researcher's actions at the discovery stage often resemble the initial stages of an attack by a criminal hacker in terms of the objectives, nature and proportionality of actions, and/or harms created.[65] Vendors do not know whether or not the intrusion is 'friendly'.

For the vendor, both the security researcher and criminal hackers share the same initial objective: to explore the IT system so as to secure an access the vendor has not authorised. Thus, both compromise the integrity and confidentiality of the system. In the initial stages of discovery they may also adopt similar approaches to the search for vulnerabilities, albeit for different reasons. Both may be very careful not to intentionally alter or delete data or programs: the criminal hacker in order to avoid detection by the vendor, the security researcher out of respect for the vendor.[66] Only after having found a vulnerability will a criminal hacker, for example, install malware that will control the IT system, and/or damage the data held. Thus, during the discovery stage, lack of damage may not indicate clearly to the vendor whose actions they are: those of a security researcher or of a criminal hacker.

Conversely, the methods and hacking tools security researchers use to discover vulnerabilities are rarely without a risk, even if a very low risk, of creating damage. The same tools are available to criminal hackers, often on an open-source basis.[67] Causing intentional

[65] R J Potts, 'Hacking: The Threats', (1989) 2(1) *Computer Audit Update* 14, 15; Jen. Ellis, 'How Do We De-Criminalize Security Research? AKA What's Next for the CFAA?', 26 January 2015, at https://community.rapid7.com/community/infosec/blog/2015/01/26/how-do-we-de-criminalize-security-research-aka-what-s-next-for-the-cfaa, cited in ENISA (n 1) 66, fn 228; Bryan Smith, William Yurcik and David Doss, 'Ethical hacking: the security justification redux', in *2002 International Symposium on Technology and Society, 2002 (ISTAS'02)* (IEEE, 2002) 374, 377; Stephen Northcutt, Jerry Shenk, Dave Shackleford, Tim Rosenberg, Raul Siles and Steve Mancini, 'Penetration testing: Assessing your overall security before attackers do.' *SANS Institute* (2006), 4 <http://www.sans.org/reading_room/analysts_program/PenetrationTesting_June06.pdf > accessed 20 July 2017. The SANS Institute is a private US for-profit organisation, reknown for its training and guidance in cybersecurity matters. See also, Thompson (n 6) 556.

[66] Northcutt, Shenk, Shackleford, Rosenberg, Siles, and Mancini (n 65) 4.

[67] Hafiz and Fang (n 39) 24-25.

damage has always been presented as the hallmark of criminal hackers.[68]. In contrast, expert security researchers will take reasonable care and notably avoid using certain techniques known in the security industry to cause a higher risk of damage.[69] However, damage may be caused without intention. Vendors themselves acknowledge the risk of damage by security researchers. Their vulnerability disclosure policies and bug bounty programmes recommend that security researchers act in good faith to avoid destroying data or impairing the operation of their services if they want to escape criminal prosecution.[70]

Thus, from the vendor's point of view, the search for vulnerabilities, whether by criminals or by independent security researchers, leads to a breach of integrity and confidentiality. Only when the security researcher discloses his/her findings to the vendor will the vendor know, retrospectively, that the 'attack' was not by a criminal hacker. Meanwhile, the vendor may find it difficult to distinguish a security researcher from a criminal hacker through the natures and proportionality of their respective actions.[71]

2.2.1.2 - Preventing harms: the risk of criminal liability

This process of discovery may trigger the security researchers' liability for s1 CMA. The offence of unauthorised access was designed to protect users against any potential intrusion into their systems well before hackers' conduct could be identified as 'harmless' or, on the contrary, harmful, causing damage to systems and/or data. It is a conduct offence. The threshold for triggering criminal liability is very low. No access needs to be secured for the offence to be committed. It suffices that the defendant 'causes a computer to perform any function with intent to secure access'. Thus, to commit s1 CMA *actus reus*, security researchers do not need to find a vulnerability that would enable them to secure access. Exploration, with its objective to find a vulnerability that secures access to the system, can constitute the conduct of the offence,.

[68] As far back as 1984, Steven Levy, *Hackers: Heroes of the computer revolution*. Vol. 4 (New York: Penguin Books, 2001) 4; Hugo Cornwall (pseudonym for Peter Sommer), *The Hacker's Handbook* (1st edn, Century 1985) 3; Richard C. Hollinger, 'Hackers: Computer heroes or electronic highwaymen?' (1991) 21(1) *ACM SIGCAS Computers and society* 6; Reid Skibell, 'The myth of the computer hacker' (2002) 5(3) *Information, Communication & Society* 336, 350-352; Jim Thomas, 'The moral ambiguity of social control in cyberspace: a retro-assessment of the "golden age" of hacking' (2005) 7(5) *New Media & Society* 599, 618; Orly Turgeman-Goldschmidt, 'Hackers' accounts: Hacking as a social entertainment' (2005) 23(1) *Social Science Computer Review* 8, 17, 21; Kirsty Best, 'Visceral Hacking or Packet Wanking? The Ethics of Digital Code, Culture' (2006) 47(2) *Theory and Critique* 213, 218, 223; A Nehaluddin, 'Hackers' Criminal Behaviour and Laws Related to Hacking' (2009) 15(7) *Computer and Telecommunications Law Review* 159, 159-160; Tim Jordan, 'A genealogy of hacking' (2016) *Convergence: The International Journal of Research into New Media Technologies* 1, 8-10.

[69] For penetration testing, Karen Scarfone, Murugiah Souppaya, Amanda Cody and Angela Orebaugh, 'Technical guide to information security testing and assessment.' 2008 *NIST Special Publication 800-115*, 5-2 , https://www.nist.gov/publications/technical-guide-information-security-testing-and-assessment> accessed 20 July 2017; Bryan Smith, Yurcik and Doss (n 65) 377. With regards to the specific risks of damage when finding one type of vulnerabilities, the buffer overflow, OWASP, *Buffer overflow*, 2009, <https://www.owasp.org/index.php/Buffer_Overflow> accessed 20 July 2017; Andrew Cormack (n 7) 317.

[70] For example, Facebook's vulnerability disclosure policy, < https://www.facebook.com/whitehat/> accessed 20 July 2017; US Department of Defense, *Vulnerability disclosure policy*, published on the website of Hacker One, an intermediary between vendors and independent security researchers, <https://hackerone.com/deptofdefense> accessed 20 July 2017, also reported by reputable security expert, Krebs, 'DoD Opens .Mil to Legal Hacking, Within Limits,' 23 November 2016, <https://krebsonsecurity.com/tag/department-of-defense/ > accessed 20 July 2017.

[71] Thompson (n 6) 556-558, 571.

With regard to the *mens rea*, two elements need to be satisfied. Firstly, the conduct must be intentional, direct intention being defined as the aim or purpose of committing the prohibited act,[72] with motives being irrelevant.[73] Since security researchers 'actively explore for these vulnerabilities'[74] they act with the aim and purpose of securing access to data, i.e. with the intention of securing access as per s1 CMA. Motives being irrelevant to the definition of intention, they are unable to argue that their reasons for securing access are to improve security. Secondly, security researchers need to know that the access they intend to secure is at the time unauthorised. Under s17(5) CMA lack of authorisation results from the defendant not being 'entitled to control access' and 'not hav[ing] consent to access by a person' entitled to control access. Independent security researchers are not hired by vendors and will not seek their express authorisation prior to the exploration of the IT systems and networks. Thus, they do not have consent to access or to secure access.[75]

Hence, in 2005, Cuthbert was convicted under s1CMA for having searched for vulnerabilities on a website.[76] He did not find any but he actively searched with the aim of securing access and thus acted intentionally. He also knew the access was unauthorised. His motives – to improve security by checking whether the charity website he gave money to was fraudulent - were irrelevant.[77] As the Crown Court judge acknowledged, Cuthbert met the requirements of the offence.[78] Yet, Cuthbert was a security researcher. An active member of the international OWASP organisation supporting the security community, he initiated the first guidelines regarding testing systems for vulnerabilities.[79] However, in the absence of a defence for hacking, the judge had to find him guilty for s1 CMA despite his 'considerable regret' about doing so.[80]

In some circumstances whether vendors authorised or not security researchers to access the system may be difficult to ascertain. Vendors such as Microsoft, Google and Facebook publish a vulnerability disclosure policy, often in conjunction with a bug bounty programme to financially reward security researchers for their findings of vulnerabilities. Their vulnerability disclosure policy determines the boundaries of what vendors consider to be acceptable searching for vulnerabilities. Such authorisation could constitute consent to search and thus to access a system as per s17(5) CMA[81].

However, vulnerability disclosure policies are not systematically detailed as to what is or is not authorised. Beyond the conditions they may expressly establish, the policies may be

[72] *R v Moloney* [1985] AC 905

[73] *A-G's Reference (no 1 of 2002)* [2002] EWCA Crim 2392. See J Horder, 'On the Irrelevance of Motive in Criminal Law', in J Horder (ed), *Oxford Essays in Jurisprudence* (OUP 2000) 173.

[74] Hafiz and Fang (n 39) 23-24; Zhao, Grossklags and Liu (n 49) 1109-1111.

[75] Cormack (n 7) 318-319; Ian Walden also cites *Cuthbert* but does not explain the defendant's background, , *Computer crimes and digital investigations* (2nd, OUP 2015) 164, para 3.239. For the US, Kesan and Hayes (n 20) 791; Oriola (n 14) 501-507; Kirsch (n 6) 392-394; Thompson (n 6) 560-568; Wibble (n 14) 1581-1584. More generally, Maurushat (n 7) 38-44.

[76] Oates (n 10)

[77] P Sommer, 'Computer Misuse Prosecutions' (2005) 16(5) *Computers and Law* 24-26; Cormack (n 5) 311.

[78] Oates (n 10)

[79] Between 2003 and 2005, OWASP, *Testing Guide Frontispiece,* <https://www.owasp.org/index.php/Testing_Guide_Frontispiece > accessed 20 July 2017.

[80] Oates (n 8)

[81] In *R v Lennon* [2006] EWHC 1201 (Admin), the Court accepted that for the purpose of s17(5) CMA, consent to receive bona fide email communications could be granted in general terms. This implied consent would not extend to communications that were not bona fide because they demonstrated on the contrary the purpose of interrupting the proper operation and use of the system._

vague enough to allow for different interpretations as to what they authorise. For example, they often ban intentional damage, but remain silent as to whether non-intentional damage, which may happen, would still be tolerated.[82] This imprecision leaves space for the security researcher to contend that his/her actions complied with the terms of the policy and for the vendor to argue the opposite, that the action was not authorised. As Maurushat put it, 'the terms 'unauthorised' and 'access' do not produce a similar set of shared assumptions in the technical, legal or ethical fields'.[83] In that case, which perspective should be taken into account? Walden has indicated that, generally, it should be the controller's perspective, hence here the vendor's, as objectively assessed by the Courts.[84] No UK court has yet discussed the concept of authorisation in this particular context. Nevertheless, indirectly, the 2012 UK case of *R v Mangham* illustrates the difficulties of interpretation and of relying on the vendor's perspective to define authorisation.[85] Because Mangham pleaded guilty to charges under s1 and s3 CMA offences,[86] the question of what constitutes authorisation could not be raised before the court. However, the elements that would matter to determine authorisation or lack of are present in the discussion on the mitigating factors the Court of Appeal could take into account to quash the original sentence of a serious crime prevention order and 8 months imprisonment.

Mangham found vulnerabilities in one of Facebook's servers. He explored further these initial vulnerabilities with the help of a program he created to utilise a Facebook employee's identity. He then accessed the source code owned by the company. He copied part of an email archive, as well as part of the source code.[87] Facebook realised that Mangham had gained access to its system before he could write and disclose his report on the vulnerabilities.[88] It had a vulnerability disclosure policy but no bounty programme rewarding security researchers like Mangham.[89]

Clearly 'upset' by this repeated access, including to its source code, Facebook argued a lack of authorisation and interpreted his actions as industrial espionage, not as vulnerability research conducted within the terms of its vulnerability disclosure policy.[90] Upon review of the events, the Crown Prosecution Service decided it was in the public interest to prosecute Mangham. For the prosecution, Mangham had stolen 'invaluable' intellectual property and 'acted with determination, undoubted ingenuity and it was sophisticated, it was calculating', costing Facebook $200,000 (£126,400) for the investigation. [91] In contrast, Mangham claimed to be an ethical hacker and security consultant who had previously reported vulnerabilities either for free or against fee, [92] a fact acknowledged by the Court. [93] His aim 'was to identify

[82] Supra n 67

[83] Maurushat (n 7) 49.

[84] Walden (n 75) para 3.237-3.238, without mentioning vulnerability research.

[85] [2002] EWCA Crim 973

[86] He refused to plead guilty to charges for committing s3A offences on making and adapting hacking tools, *Mangham* (n 85) para 2.

[87] *id*, para 4.

[88] *id*, paras 8, 22.

[89] Facebook launched its bug bounty programme after Mangham's arrest, <https://www.facebook.com/security/posts/238039389561434> accessed 20 July 2017. Yet, Facebook's chief security officer Joe Sullivan (@joesullivana, 21 February 2012) claimed the opposite in an official comment about *Mangham* as reported by reputable security consultant Graham Cluley (n 10).

[90] Maurushat (n 7) 41-42.

[91] BBC news, 'York Facebook hacking student Glenn Mangham jailed', 17 February 2012, <http://www.bbc.co.uk/news/uk-england-york-north-yorkshire-17079853> accessed 20 July 2017.

[92] *ibid*.; Ben Quinn, 'Facebook hacker jailed for eight months', *The Guardian* 18 February 2012 <https://www.theguardian.com/technology/2012/feb/17/facebook-hacker-glenn-mangham-jailed> accessed 20

vulnerabilities in the system so I could compile a report that I could then bundle over to Facebook and show them what was wrong with their system.'[94]

Mangham certainly accessed the system and confidential data. Given that s1 and s3 CMA are designed to protect against breaches of integrity and confidentiality Mangham's prosecution seemed justified. However, Mangham also operated in the knowledge of Facebook's vulnerability disclosure policy. The December 2010 policy, made of three lines, stated that Facebook 'will not bring any lawsuit against you or ask law enforcement to investigate you for that research' if 'in the course of the research you made a good faith effort to avoid privacy violations, destruction of data, or interruption or degradation of our service', and if the vulnerability was not revealed to the public before Facebook had the chance to fix it.[95] Arguably, a vulnerability disclosure policy cannot establish a legal test, but the policy indicates that Facebook authorises access to its system to find vulnerabilities upon four conditions: not to violate privacy, destroy data, interrupt or degrade the service, and not to reveal the vulnerability to the public. The question can thus be whether Mangham breached any of the conditions Facebook established in its vulnerability disclosure policy. The answer is more nuanced and ambiguous than the guilty plea for s1 and s3 CMA offences would suggest.

Undoubtedly, Mangham destroyed the data revealing his trail, whereas Facebook's policy expressly prohibits the destruction of data. This action can thus be considered not to be authorised and contrary to s3 CMA criminalising any unauthorised act with intent to damage or impair the reliability of data.

The lack of authorisation is however less obvious for other activities. Mangham intentionally used an employee's log-in credentials to explore further the potential impacts of the initial vulnerability. This is likely to be problematic as Mangham hid behind another's identity. However, the policy itself does not expressly prohibit such action. Furthermore, the use of the identity was not followed by a violation of privacy; it was only to secure access, rather than to peak at the employee's personal or professional life, or to impersonate the employee in other circumstances. Facebook itself accepted in Court that 'no personal use of data […] was compromised'.[96] Thus, it could be argued that Mangham avoided in, 'good faith', violations of privacy, and thus stayed within the boundaries of Facebook's policy.

Furthermore, the Court noted as a mitigation factor that Mangham did not interrupt or degrade Facebook's service.[97] Facebook admitted in Court that it suffered no loss as it retrieved the source code in its entirety.[98] In that respect, Mangham could be said to have complied with Facebook's policy not to destroy data, or interrupt or degrade the service.

Moreover, as the Court noted again as a mitigation factor, Mangham did not disclose the copy of the source code he held for three weeks. In spite of the likely high commercial

July 2017; Mangham's own blog, 'The Facebook Hack. What really happened', *Blog Ebor' Hack'em*, 23 April 2012, <http://gmangham.blogspot.co.uk/2012/04/facebook-hack-what-really-happened.html> accessed 20 July 2017.

[93] *Mangham* (n 85) para 7.

[94] Quinn (n 92)

[95] Marcia Hofman, 'Knowledge is Power: Facebook's Exceptional Approach to Vulnerability Disclosure', EFF 17 December 2010, <https://www.eff.org/deeplinks/2010/12/knowledge-power-facebooks-exceptional-approach> accessed 20 July 2017; Oriola (n 14) 505.

[96] *Mangham* (n 85) para 5.

[97] *ibid*.

[98] *id.* para 23.

value of the code on the black market he did not seek to gain any financial advantage. [99] Thus Mangham did not reveal the vulnerability to the public, in compliance with Facebook's policy. In addition, Mangham held the copy on a secure storage medium unconnected to the Internet. The source code was thus inaccessible to hackers and more secure than Facebook's own storage.

Thus, many of Mangham's actions seem proportionate to his objective of finding vulnerabilities to benefit the wider public. They appear to support his claim that he searched ethically for vulnerabilities in accordance with Facebook's short vulnerability disclosure policy. The remaining question is whether Mangham should have stopped and immediately reported to Facebook, as the Crown Court judge suggested. No clear guidance exists but three elements point towards accepting further exploration. Firstly, 'the security mindset involves thinking like an attacker, an adversary or a criminal'.[100] A criminal hacker would not stop at the first vulnerability. S/he would try to find other vulnerabilities. Further exploration can be appropriate.[101] The difference would be that the security researcher would not exploit the vulnerabilities, which was precisely what Mangham refrained from doing. Secondly, Mangham claimed he wanted to analyse the source code as a means of finding further vulnerabilities. The claim cannot be easily dismissed in light of the OWASP testing guide for the security industry, in which such analysis is presented as possibly the sole means to find some vulnerabilities in a system.[102] Thirdly, Facebook itself changed its policy after Mangham's conviction, and currently states 'You do not exploit a security issue that you discover for any reason. (This includes *demonstrating additional risk, such as attempted compromise of sensitive company data or probing for additional issues*.)'.[103] Facebook's previous policy applicable to Mangham did not contain this prohibition and thus could have been interpreted as not forbidding Mangham's further exploration.[104]

Facebook may have felt aggrieved by the finding of the source code, which breached confidentiality, and consequently justified in its decision to withdraw authorisation. However, the terms of the vulnerability disclosure policy and the practices of vulnerability research leave, after the event, enough room to argue that Facebook's policy, at the time of its publication, authorised many of Mangham's activities at the discovery stage, and that his search for vulnerabilities was genuine.[105] The next stage in the process of vulnerability research is not without its own legal challenges either.

2.2.2 - The verification of the vulnerability

To verify the vulnerability the security researcher will write a proof of concept that demonstrates how the vulnerability could lead to a breach of confidentiality, integrity and/or

[99] Mangham's blog (n 92).
[100] Bruce Schneier, testifying to the Science and Technology Committee, *Personal Internet Security* (HL 2006-07, 165-II) p184, Q565.
[101] Supra section 2.2.1.
[102], at https://www.owasp.org/index.php/Testing_Guide_Introduction#Source_Code_Review, accessed 20 July 2017
[103] Our emphasis, <https://www.facebook.com/whitehat/> accessed 20 July 2017.
[104] Maurushat (n 7) 42.
[105] Maurushat (n 7) 41-42.

availability. For example, the proof of concept may demonstrate how, at the most basic level, a vulnerability affects the functioning of an application and thus violates the availability of the IT system and network.[106]

In the process the security researcher may violate s3 and s3A CMA. The execution of the proof of concept could constitute an unauthorised act aimed at impairing the functioning of a computer, as per s3 CMA. The proof of concept could constitute an 'article' or a computer program aimed at impairing the operation of a computer, as per s3A CMA. The security researcher created it and executed it intentionally, with the aim and purpose of doing so, thus violating s3 and s3A CMA.

Furthermore, finding a vulnerability may coincide with a breach of confidentiality and/or integrity. The security researcher may then access confidential or personal data and copy the data onto an external drive to evidence the vulnerability, as Mangham did when copying a selection of Facebook's email archives. According to s17(2)(b) CMA copying the data 'on any storage medium' would constitute an act to secure access, and thus would constitute s1 CMA. S55 Data Protection Act 1998 may also be violated when the security researcher copies and thus obtains personal data without consent.[107]

Therefore, the security researcher is expected to establish a proof of concept, before, so as to ensure that the vulnerability exists and demonstrate potential or existing harm. Yet, this process may fall within the scope of criminal law.

2.2.3 - The disclosure of the vulnerability

Disclosure can be done in many ways: to vendors exclusively or to third parties which will relay the information to the vendors (coordinated disclosure), to vendors for a given period of time and then to the public (delayed full disclosure), or directly to the public (full disclosure).

Disclosure is certainly a contentious issue within the security industry, and practices vary enormously across security researchers. When established in late 1988 the CERT, in the US, promoted and continues to favour disclosure to vendors until vendors have fixed the vulnerability and are in a position to release the patch to the public.[108] Then the vulnerability will be reported to the public and available for all to see. This form of disclosure should demonstrate that the security researcher did not intend to exploit the found vulnerability or to harm the vendor. It could also be presumed to be the most effective method for enabling the patching of the vulnerability but vendors do not always take the information seriously, and/or may unnecessarily delay the release of the patch.[109]

Thus, many security researchers choose the option of full disclosure, i.e. disclosing to the public by various means: hacking conferences, the use of media and, mostly, public lists such as Bugtraq, which was created in 1993 in reaction to the CERT's own disclosure policy and with the aim of forcing vendors to fix vulnerabilities quickly. Full disclosure can be immediate or delayed. Delayed is when disclosure is first to vendors, then to the public when vendors, lacking 'maturity', either do not respond or are too slow in responding.[110] Google's

[106] Hafiz and Fang (n 39) 21-22, 26-27, 30-31.

[107] On the possible use of s55 DPA for criminal hackers, CPS, *Legal guidance on Cybercrime*, <http://www.cps.gov.uk/legal/a_to_c/cybercrime/#a07 > accessed 20 July 2017.

[108] ENISA (n 1) 26; CERT, <http://www.cert.org/faq/> accessed 20 July 2017.

[109] Arora, Caulkins and Telang, 'Research Note—Sell First, Fix Later…' (n 30); Ashish Arora, Rahul Telang and Hao Xu, 'Optimal Policy for Software Vulnerability Disclosure' (2008) 54(4) *Management Science* 642.

[110] ENISA (n 1) 52-53, 63-64; Hafiz and Fang (n 39) 29-30, 34.

Project Zero, for example, gives ninety days for vendors to fix vulnerabilities or face public disclosure after the stated period.[111]

This disclosure to the public, whether immediate or delayed, has been demonstrated to be effective, with vendors taking a more active stance towards fixing vulnerabilities.[112] However, it may be problematic with regard to criminal law. By posting the information about the vulnerability to the public the security researcher provides information to criminal hackers about which vulnerabilities they could exploit to commit other crimes. The disclosure may trigger accessorial liability under section 8 of the *Accessories and Abettors Act* 1861, whereby the security researcher has intentionally aided and abetted criminal hackers. Intention can be direct, with the accessory aiming to assist or influence the principal, or oblique, the accessory having foresight about the principal's offence as a virtual certainty.[113] Disclosure to the public is known among the security industry to increase the number of attacks.[114] In legal terms their knowledge could amount to the definition of oblique intention: it is 'virtually certain' that the information will be used by some hackers for criminal endeavours. Therefore, disclosure of vulnerabilities to the general public may trigger the security researcher's accessorial liability for crimes committed by hackers maliciously exploiting the disclosed vulnerabilities.[115]

The security researcher's disclosure may constitute the offence of s 3A (2) CMA 1990. A person who supplies an article believing that it is likely to be used to assist with the commission of offences under the CMA may be liable for up to two years imprisonment upon indictment. Belief is considered to be more than mere suspicion but less than knowledge and certainly less than intention.[116] For the same reasons as above security researchers are likely

[111] <https://googleprojectzero.blogspot.co.uk/> accessed 20 July 2017; ENISA (n 1) 60.

[112] Arora, Forman, Nandkumar and Telang (n 15); Ashish Arora, Ramayya Krishnan, Anand Nandkumar, Rahul Telang and Yubao Yang, 'Impact of vulnerability disclosure and patch availability-an empirical analysis' in (2004) 24 *Third Workshop on the Economics of Information Security* 1268; Ashish Arora, Ramayya Krishnan, Rahul Telang and Yubao Yang, 'An Empirical Analysis of Vendor Response to Disclosure Policy', in 2005 *Workshop on the Economics of Information Security* < http://infosecon.net/workshop/pdf/41.pdf> accessed 20 July 2017; Jeremy D. Seideman, Bilal Khan and Ghassen Ben Brahim, 'Determining vulnerability resolution time by examining malware proliferation rates', in *2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC)* (IEEE, 2013) 1678; Ryan W. Gardner, Matt Bishop and Tadayoshi Kohno, 'Are patched machines really fixed?' (2009) 7(5) IEEE Security & Privacy 82.

[113] *National Coal Board v Gamble* [1959] 1QB 11; *R v Bryce* [2004] EWCA Crim 1231; Ormerod and Laird (n 58) 225-226. The definition of oblique intention is in *R v Hyam* [1975] AC 55; *R v Woollin* [1999] AC 82.

[114] Ashish Arora, Anand Nandkumar and Rahul Telang, 'Does Information Security Attack Frequency Increase with Vulnerability Disclosure? An Empirical Analysis' (2006) 8(5) *Information Systems Frontiers* 350; Ashish Arora, Rahul Telang and Hao Xu, 'Timing Disclosure of Software Vulnerability for Optimal Social Welfare,' in 2004 *Third Workshop on Economics of Information Systems* 1, 13-15. Even when disclosure is done by vendor, attacks will increase in the subsequent days, because users are slow to update their systems, Geraldine Vache Marconato, Vincent Nicomette and Mohamed Kaâniche, 'Security-related vulnerability life cycle analysis', in *2012 7th international conference on Risk and security of internet and systems (crisis)* (IEEE 2012) 1; Yogita Kansal, P. K. Kapur and Deepak Kumar, 'Assessing optimal patch release time for vulnerable software systems', in *2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH)* (IEEE 2016) 308.

[115] Maurushat (n 7) 44-45. See with regard to the draft EU Directive 2013/40/EU, amendments 96 and 97 respectively by MEPs Jan Albrecht and Marie-Christine Vergiat. They proposed to delete future Article 8 on accessorial liability to protect security researchers. EU Parliament, Amendments 34-128, Draft Report 2010/0273 (COD), 27 January 2012. For the US, Electronic Frontier Foundation, 'Coders' Rights Project Vulnerability Reporting FAQ', <https://www.eff.org/issues/coders/vulnerability-reporting-faq#faq12 > accessed 20 July 2017.

[116] CPS, Legal Guidance to Computer Misuse Act 1990, <http://www.cps.gov.uk/legal/a_to_c/computer_misuse_act_1990/#an05 > accessed 20 July 2017; Ormerod and

to meet the test since it could be argued that they believe, if not know, that their proof of concept 'is likely to be used' by others to commit crime. To avoid disclosure to the public, and thus to criminals, mailing lists could be restricted to vetted security researchers. However the legal challenges raised by full disclosure to the public would not completely disappear. Even intermediaries, such as ZDI, which use vetted mailing lists are likely to resort to full disclosure if vendors do not provide a patch within the time-frame proposed.[117]

2.2.4 - Conclusion

Full disclosure – delayed or immediate - is not without its own ambiguities. Not surprisingly, discussions of its pros and cons have been present over the past thirty years in the security industry, with security researchers seen alternatively as promoting a more secure ecosystem or as 'vigilantes' there to 'humiliate' vendors.[118] At the heart of these ambiguities, though, is a lack of adequate channels to pressurise vendors into fixing vulnerabilities by means other than full disclosure. Security researchers would be less inclined to use full disclosure if a regulatory framework were to effectively promote what ENISA called vendors' maturity in responding adequately and in a timely manner to disclosure. This aspect of the problem is beyond the scope of this article but it shows that, of all the ambiguities of the process of vulnerability research, those at the disclosure stage could be resolved by security researchers adopting other conduct whilst still reporting vulnerabilities.

In contrast, a change of behaviours cannot dispel the ambiguities at the discovery and verification stages. Security researchers could be more careful and their search more constrained, as *Mangham* partially illustrates, but vulnerability research remains about learning how to open a door which nobody was meant to open. Security researchers cannot stop hacking, i.e. exploring systems to gain unauthorised access, and they cannot stop verifying vulnerabilities without at times creating a proof of concept which may trigger liability under the CMA.

Based on this review of the process of vulnerability research this paper argues that the controversial aspects of the process are the discovery and verification stages. At the discovery stage the thorniest issue is that of the authorisation at the heart of s1 CMA and also s3 CMA. In the absence of a vulnerability disclosure policy and/or bug bounty programme the security researcher will act without authorisation and thus violate the law even if s/he has taken reasonable care and is acting in the public interest, as per *Cuthbert*. A vulnerability disclosure policy and/or bug bounty programme would grant authorisation under certain conditions and if the policy is adequately written. However, the security researcher may face uncertainty, as in *Mangham*. Furthermore, at the verification stage the security researcher may commit several CMA offences even if s/he discloses responsibly the information and proof of concept to the vendor. Thus, criminal law treats the security researcher as if s/he were a malicious hacker intending to commit crimes, in the process ignoring the objective of public interest s/he aims to promote. The challenge will be to reconcile the need for vendors to protect the confidentiality, integrity and availability of their systems with the need to establish a space for security researchers to act without the fear of criminal liability.

Laird (n 58) 1190; Gillepsie (n 2) 73; Jonathan Clough, *Principles of Cybercrime* (2nd edn, Cambridge University Press 2015) 143-144; Walden (n 75) 201-202.

[117] See ZeroDayInitiative (ZDI) disclosure policy at http://www.zerodayinitiative.com/advisories/disclosure_policy/ (accessed 20 November 2017)

[118] Kirsch (n 6) 390-391; ENISA (n 1) 25-26.

Three options are possible: modifying the structure of the current offences, establishing adequate prosecutorial guidelines, or a public interest defence. The first option was explored in the discussions that preceded the Computer Misuse Bill of 1990.

3 - Revisiting the past: the UK's failed attempts to recognise vulnerability research prior to the Computer Misuse Bill of 1990

The expression 'vulnerability research' never featured in discussions on the criminalisation of hacking and the potential need for an offence of unauthorised access. Nevertheless, the idea that hacking, notably for security purposes, might be recognised as a legal activity permeated the debates at regular intervals until the start of parliamentary debates on the Computer Misuse Bill in February 1990.

The Scottish Law Commission (SLC) and the English Law Commission (ELC) first proposed making hacking – unauthorised access - partially legal in their respective reports of 1987 and 1988. Subsequently, MP Emma Nicholson tabled a Private Member's Bill in April 1989 with terms which were very similar to the Law Commissions' proposals. However, the Bill's subsequent withdrawal in July 1989 signalled a change of policy. The reasons for this change hold the key to why adopting similar proposals would not be a viable option.

3.1 - The Scottish Law Commission's proposal to recognise hacking for security purposes

In its 1987 draft Bill the SLC adopted a nuanced position towards hacking and hackers in general. For the SLC the term 'hacking' covered a wide range of behaviours and motives: from the hacker's mere curiosity 'to test their electronic and technological skills' with a lack of 'nefarious motive in mind', to the 'unscrupulous person' aiming to access data to 'use for his own advantage'.[119] The structure of its proposed offences constituted an 'attempt to distinguish between the 'probably harmless' hacker and the malicious one'.[120]

This reference to 'harmless' hacking echoes passages of its first report of 1986, where the SLC acknowledged that a hacker could be a highly skilled 'computer enthusiast',[121] and that hacking could be 'no more than a harmless sport [the hacker] engaged in simply for the intellectual challenge which it presents'.[122] This discourse corresponds to the original meaning of 'hacking' before it became associated predominantly with crime, in the UK, by late 1989. [123]

Nevertheless, this discourse is partially misleading. The SLC had little doubt that gaining unauthorised access led the hacker to view data he was not supposed to see in the first place.[124] However, in contrast to its 1986 proposal,[125] in 1987 the SLC refused to

[119] Scottish Law Commission, *Report on Computer Crime* (Scot L Com No 106) para 2.8

[120] id. para 3.19

[121] Scottish Law Commission, *Computer Crime* (Scot Law Com CM 68, 1986) para 4.5 also 2.38-2.39. Cornwall (n 63) 1 and also in the third edition, p7; Chris Frost, 'Hacking: Bulletin Boards as Sources of Information', (1989) 2(1) *Computer Audit Update* 16; Wible (n 12) 1590. Enthusiasm is also the word in the Oxford English Dictionary to describe the first meaning of a hacker. OED *V.* Hacker.

[122] Cornwall (n 68) VI.

[123] Levy (n 68) 26-27; Jordan (n 68); Helen Nissenbaum, 'Hackers and the contested ontology of cyberspace' (2004) 6(2) *New media & society* 195, 197; Wible (n 14) 1590.

[124] Scottish Law Commission (n 121) paras 3.6 and 4.15.

[125] Scottish Law Commission (n 121) para 4.6 - 4.8, 6.2 - 6.9.

recommend the criminalisation of unauthorised access just because the hacker would have accessed personal data and invaded the person's privacy. Hacking 'in order to inspect or otherwise to acquire knowledge of the program or the data' would have been legal. Similarly, the SLC rejected the criminalisation of unauthorised access in order 'to add to, erase or otherwise alter the program or the data'.

Hacking would have become illegal only in three situations: when the hacker intended to 'procur[e] an advantage for himself or another person, […when s/he would intentionally] damag[e] another person's interests' (clause 1), or when s/he 'recklessly' damaged another person's interests by 'altering, corrupting, erasing or adding to a program or data' (clause 2). Penalties were up to 6 months imprisonment on summary conviction, 5 years on indictment (clause 3).

It is difficult to know to what extent the SLC was cognisant of the precise impact of its proposals on hackers engaged in vulnerability research. In particular, the SLC did not explain the test for recklessness.[126]. It also did not mention whether security industry standards could be used, although some had already emerged at the time.[127] On the other hand, the SLC's choice of words, notably the verb 'to inspect', implied an awareness of hacking for security purposes, where hacking leads the hacker to analyse the security strengths and weaknesses of an IT system.

3.2 - The English Law Commission's proposals of 1988

In its Working Paper 110, whose structure is very similar to that of the SLC's reports, the ELC also extensively reviewed the pros and cons of criminalising hacking. Contrary to the SLC, it did not reach 'any provisional conclusions' as to the principle and scope of criminalisation of unauthorised access,[128] and thus proposed four very different wordings for the offence of unauthorised access.[129]

The fourth and broadest option recalls the SLC's first proposal of 1986. It would have criminalised any unauthorised access, whatever the 'subsidiary purpose' of the hacker and independently of whether the hacker 'took reasonable care to avoid causing damage to the computer system'. The ELC clearly stated there would be 'no defence' offered to the hacker, whatever the motive.[130] The first option was similar to the fourth in that unauthorised access would be criminalised whatever the purpose, although access was restricted to specific types of data, such as personal data.[131]

Conversely, the second and third options were closer to the SLC's 1987 Bill in scope and spirit. It refused to recommend the criminalisation of unauthorised access in order 'to inspect' computer systems unless the 'inspection' was 'done for the purpose of either gaining

[126] Scottish Law Commission (n 121) para 4.11. On the Scottish test, notably Joshua Samuel Barton, 'Recklessness in Scots Criminal Law: Subjective or Objective?' (2011) 2 *Juridical Review* 143.

[127] Notably, for penetration testing, see the well known study in security circles of Richard C. Attanasio, Peter W. Markstein and Ray J. Phillips, 'Penetrating an operating system: a study of VM/370 integrity' (1976) 15(1) *IBM Systems Journal* 102.

[128] Law Commission, *Computer Misuse* (Law Com WP 110, 1988) paras 6.2 and 8.5

[129] For an analysis, Hugo Cornwall (alias Peter Sommer), 'Hacking away at computer law reform.' (1988) 138 *New Law Jo*urnal 702.

[130] Law Commission (n 128) para 6.36.

[131] Law Commission (n 128) para 6.25.

an advantage for oneself or another, or of damaging another person's interests' (option B) or unless damage existed, on a strict liability basis (option C). [132]

With its option B the ELC took the same position as the SLC with regard to invasion of privacy. Invasion of privacy not exploited or not intended to be exploited by a hacker for his own benefit or another's benefit would have been legal. Breaching confidentiality was not sufficient to justify criminalisation without evidence of the hacker's further intention to create harm.

Regarding the harm of damage, in its option B the ELC proposed tolerating reckless damage. This included hackers whose only motive was 'to overcome security devices'[133] but who would have been cautious not to create intentional harm. Conversely, its option C would have criminalised hacking causing damage on a strict liability basis, even when the hacker had taken reasonable care in his exploration, the ELC asking for clarification on the likelihood of this risk of harm by hacking.[134]

The novelty of the SLC's and ELC's proposals hardly attracted any comment at the time. In 1987 Professor Smith indicated that hacking for security purposes was a 'controversial' question Parliament needed to discuss.[135] Another author considered that these hackers 'have served at least one useful social purpose'.[136] Yet, the impact the proposals would have had on security researchers remained undiscussed. Whether this silence meant acceptance of the proposals and reasoning is difficult to tell but in April 1989 MP Emma Nicholson presented a Bill which drafted the offence of unauthorised access in very similar terms to these of the SLC and ELC.

3. 3 - The unsuccessful April 1989 Bill

Put forward a few months after the ELC 1988 report, Nicholson's Private Member's Bill proposed an offence of unauthorised access with a slightly broader scope than that of the SLC's proposal. Reckless damage would have been criminalised, in addition to recklessly gaining an advantage or causing prejudice (clause 1(1)). The Bill also proposed to 'outlaw[…] the possession of anything intended to be used to gain unauthorised access to a computer as defined in clause 1' (Clause 1(2)) [137], which would have criminalised hacking tools and possession of information on to how to gain unauthorised access which was circulating on bulletin boards. Penalties would have been up to ten years imprisonment or five years if acts were committed recklessly (clause 2).

Nicholson's own discourse is unclear regarding which behaviours her Bill intended to criminalise. She argued that the law should signal to hackers that unauthorised access was not acceptable.[138] Hence, it could be interpreted as an absolute condemnation of all forms of hacking. However, the terms of her draft Bill, very similarly to the SLC's proposal, would

[132] Law Commission (n 128) paras 6.31-6.32.

[133] Law Commission (n 128) para 6.31

[134] Law Commission (n 128) para 8.5; see also paras 3.39, 3.68, 6.4, 6.11, 6.12, 6.15, 6.17

[135] 'Computer Crime: A Reply', (1987) 3 *Y.B. L. Computers & Tech.* 204, 206.

[136] Y I Cole-Wilson, 'Old Bailey Hacks: Some Reflections on R v Gold and Schifren', (1987) 137 NLJ 1118, 1121

[137] Emma Nicholson, 'Computer Misuse: Fact or Invention', (1989) 2(1) *Computer Audit Update* 2, 4.

[138] *Id.* 2.

have left space for security researchers acting with reasonable care to explore and test a security system. They could also have possessed hacking tools in the absence of further intent to commit crime.

How this Bill was received is difficult to tell, in the absence of discussions before Parliament. Two lawyers argued in favour of the non-criminalisation of security researchers, one noting their vital role of assisting the police in the fight against cybercrime.[139] Peter Sommer, alias Hugo Cornwall, an 'Oxford-trained lawyer' and expert in digital forensics, considered that the Bill's objectives were misaligned with the reality of hacking. The Bill did not tackle real issues such as system owners' lax security practices, theft of information or the difficulties in using computer files as evidence.[140] Yet, Sommer also recognised it had become impossible to talk of hacking as an educational challenge as he did in 1985 when quoted by the SLC in its 1986 report.[141] The context had changed. In November 1988, the Morris worm brought down much of the internet. Hacking had become a controversial activity which had to be criminalised [142].

Nicholson withdrew her Bill in July 1989 on the promise that the Government would present one once the ELC had published its final report.[143] In effect, the Bill's withdrawal signalled the end of the idea of exempting hackers from criminal liability, even if they hacked for security purposes and did so responsibly, with reasonable care. The ELC became adamant that security researchers should also be criminalised.

3.4 - The final decision to criminalise security researchers

By the time the ELC published its final report in October 1989 its approach to hacking had changed dramatically, influenced by the surrounding context. The tone and discourse about hacking had changed dramatically during the year 1989. Comments widely called for the criminalisation of hacking without exceptions, with barely a mention of the Law Commissions' other proposals or of Nicholson's Bill.[144]. Behind this change in tone lies a

[139] Kelman, QC, who represented the hackers Gold and Schiffren before the Court of Appeal and House of Lords in 1987, A. Kelman, 'Case Law and Implications of Hacking' (1989) 2(1) *Computer Audit Update* 5. The other lawyer was Chris Pounder, from Hopskins Law firm, specialised in data protection. Both Kelman and Pounder were cited in Matthew May, 'How a hacking law could weaken security' *The Times* 20 April 1989 and in 'News' (1989) 1(6) *Computer Audit Update* 18, 19.

[140] The Guardian, 13 April 1989

[141] <http://www.pmsommer.net/page10.html> accessed 20 July 2017.

[142] Eugene H. Spafford, 'The Internet Worm Program: An Analysis' (1988) *Computer Science Technical Reports. Paper 702*, <http://docs.lib.purdue.edu/cstech/702> accessed 20 July 2017; Jon A. Rochlis and Mark W. Eichin, 'With Microscope and Tweezers: The Worm from MITS Perspective' (1989) 32(6) *Communications of the ACM* 689; David Davies, 'Computer risk management' (1990) 5(6) *Computer Law & Security Review* 2, 7; Eugene H. Spafford, 'Are computer hacker break-ins ethical?' (1992) 17(1) *Journal of Systems and Software* 41; Douglas Thomas, *Hacker Culture*, University of Minnesota Press 2002, pp 43-44; Nissenbaum (n 123); Michael Warner, 'Cybersecurity: a pre-history' (2012) 27(5) *Intelligence and National Security* 781, 794.

[143] Matthew May, 'Hold back the hackers', *The Times* 6 July 1989.

[144] Frost (n 121); John Court (for the Institute of Chartered Accountants in England and Wales), 'Hacking and the law: The Way Forward', (1989) 2(1) *Computer Audit Update* 18. Sommer and Wasik did not express any views, just presenting the pros and cons of criminalisation. Peter Sommer, 'Hacking away at computer law reform' (1988) 138 NLJ 702; Martin Wasik, 'Law reform proposals on computer misuse' [1989] Crim L.R. 257. 'The CBI Submission. Part 1' (1988-90) 1 *Computer Law and Security Report* 14.

transformation in the reality of hacking. Motivated by greed and power, hackers stopped being mostly security researchers.[145]

The initial hacking culture and mindset of expanding one's knowledge of IT systems to improve security had not disappeared but it was superseded by the image of the 'black hat', the criminal hacker.[146] Hacking became associated solely with crime, pushing aside the idea that security researchers could act responsibly.

Therefore, the ELC expressly rejected Nicholson's Bill, as well as the SLC's 1987 proposal.[147] The entire report was a condemnation of hacking, including for the purpose of security: 'the hacker who genuinely was merely (unauthorised) testing the system's defences would still in our view be someone whom the law should seek to discourage'.[148] For the ELC, the mischief that criminal law should tackle was not that which the ELC and SLC previously identified: the invasion of privacy, and the damage the hacker could inflict.[149] It was instead that attempts by unknown hackers to secure unauthorised access breach the integrity of an IT system, 'whatever the motive behind those attempts'.[150]

Therefore, the offence of unauthorised access, which was to become s1 CMA 1990, 'seeks to catch those who actively interfere with the system itself, in order to inspect its contents or test its access procedures'[151]. This would prohibit both the exploration that precedes gaining access - when the hacker tries to gain access through various methods - and the exploration that follows the gaining of unauthorised access, even if done with reasonable care and without an intention to commit crime. The offence would also, through accessorial liability, prohibit the use of bulletin boards when the publication of information would facilitate hacking by criminals.[152]

Due to time constraints the ELC did not draft a Bill but its conclusions were widely accepted.[153] In the absence of a government Bill MP Colvin, having obtained the government's support, deposited a Private Member's Bill in December 1989 along the same lines outlined by the ELC in 1989.[154] His Bill became the Computer Misuse Act.

3.5 – Lessons from the past

Although not identical, the Law Commissions' proposals and Nicholson's Bill had clear advantages. They did not focus on (un)authorised access, which is often a contentious issue. Instead, they shifted the debate to the proportionality of the security researcher's actions in relation to the objective sought –finding a vulnerability. Both Law Commissions made

[145] Hollinger (n 68); Nissenbaum (n 123); Wible (n 12).

[146] Nissenbaum (n 123); Jeffrey Bardzell, Shaowen Bardzell and Austin Toombs, 'Now that's definitely a proper hack: self-made tools in hackerspaces', in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (ACM 2014) 473, 475; Jeremy Hunsinger and Andrew Schrock, 'The democratization of hacking and making' (2016) 18(4) *New Media & Society* 535.

[147] Law Commission, *Computer Misuse* (Law Com No 186, 1989) para 1.12.

[148] Id. para 3.18; see also para 2.17.

[149] Id. para 1.29, 1.37, 2.15, 3.9 with footnote 52, 3.10 and 3.36.

[150] Id. para 1.29 and footnote 52 page 17.

[151] Id. para 3.29.

[152] Id. para 2.23; 1.36.

[153] Matthew May, 'Call to arms against the computer virus', *The Times* 12 October 1989.

[154] Nick Nuttall, 'MP takes up fight on computer tampering; Michael Colvin', *The Times*, 16 December 1989.

several references to hacking as a harmless pursuit. Nevertheless, the structure of their recommended offences indicated that hacking could cause two types of harms without systematically attracting criminal liability. These harms were invasion of privacy, as a breach of confidentiality, and damage to IT systems, a breach of integrity.

The proposals did not provide a blank cheque for hackers to do as they pleased, as the ELC acknowledged a year later in its 1989 report. The discovery stage would have been legal providing the hacker took reasonable care and did not intend to cause damage. The proposals would also have constrained the verification process and choice of disclosure. Since the hacker could not take advantage of his findings, s/he would have had to disclose to the vendor only, and not to the public or on bulletin boards, so as not to damage another's interest. In addition, the security researcher would have had to disclose to the vendor without intent to be financially rewarded by the vendor as this could have been interpreted as 'procuring himself an advantage'.

Implicitly, the proposals recognised that a security researcher and a criminal hacker might behave very similarly at the discovery stage but that further actions would allow for distinguishing between them. Both would initially inspect data or programs and gain unauthorised access but the criminal hacker would then move, for example, to writing a virus or worm program, whilst the security researcher would inform the vendor in order for the vulnerability to be fixed.

Suitable for security researchers, the proposals had one weakness though. They would not have protected vendors well enough against criminal hackers until it was too late. For the ELC, in 1989, the breach of integrity which hacking created justified the criminalisation of both criminal hackers and security researchers. The testing the security of the systems should be a decision left to the 'operators', who would alone grant authorisation to do so.[155]

Thirty years later, the development of vulnerability markets, unforeseen in 1989, shows that the ELC's conclusion to leave to vendors alone the finding of vulnerabilities was mistaken. Vendors themselves acknowledge the need for independent security researchers to search for vulnerabilities without having obtained prior permission to do so. Security researchers should be able to hack. On the other hand, today, in the age of cybercrime as a service, the ELC's 1989 assessment about the need to protect systems against breaches of integrity has increased, not decreased, in relevance.[156] Exempting security researchers from criminal liability, by restricting the scope of the unauthorised access offence, is likely to give criminal hackers too much freedom to investigate IT systems and too much incentive to remain undetected until they can cause damage and feel the full weight of criminal law. As a matter of policy it is important that criminal law recognises this harm to the vendor.

The question is thus how the law should be drafted to reconcile two opposite objectives: protecting vendors and thus tackling criminal hackers' activities before they commit further crimes; allowing security researchers to find and report vulnerabilities without vendors' prior authorisation. Both at international and national levels, the question appears only in the margin of the discussions on cybercrime. Yet, in the UK, criminal law's impact on security research has significantly intensified since the original CMA was enacted in 1990. Driven by

[155] Law Commission (n 147) para 2.17. The ELC also put forward the ensuing 'substantial costs' borne by the victims in detecting those attempts and in mitigating their effects, para 1.29-1.30.

[156] Derek Manky, 'Cybercrime as a service: a very modern business' (2013) 6 *Computer Fraud & Security* 9; Aditya K. Sood and Richard J. Enbody. 'Crimeware-as-a-service—a survey of commoditized crimeware in the underground market' (2013) 6(1) *International Journal of Critical Infrastructure Protection* 28.

compliance with the Cybercrime Convention in 2006, and the EU Directive 2013/40/EC in 2015, the reforms of the CMA in 2006 and in 2015 have increased the penalties for existing offences, extended the scope of s3 CMA, and created two new offences: in 2006, the new offence of making and distributing hacking tools of s3A CMA, which scope was extended in 2015; and in 2015, the s3ZA offence when the systems targeted are those of critical infrastructures, and to which is attached a penalty of life imprisonment. Thus, security researchers in the UK face criminal liability for a range of offences not limited to unauthorised access and three months imprisonment as the ELC initially envisaged. Any reform of the law would have to take into account this changed landscape. The problem is that so far, the discussions on security researchers' criminal liability at international and national levels have been sporadic and restricted to essentially one offence, that of misuse of hacking tools, with at times some debates on the structure of unauthorised access.

Regarding the misuse of hacking tools offence, the Council of Europe attempted to qualm the concerns of the security industry by adding an interpretation clause in Article 6(2).[157] Article 6 should not 'be interpreted as imposing criminal liability [...when the tools are used' for authorised testing or protection of a computer system'. Such a clause did not find its way into UK law when the UK created its s3A CMA in 2006. It was not adopted either in the EU Directive 2013/40. To protect security researchers, the EU only excluded possession of hacking tools and passwords from the scope of criminalisation, reiterating in its Recital 16 that a specific intent to commit crime must be proven. At national level, s3A CMA has been criticised, in particular s3A(2) CMA. A reverse burden of proof has been proposed.[158] However, the proposal still focuses on whether the defendant has or not committed the elements of the offence, which is precisely what is difficult to prove. In addition, it ignores the other legal challenges security researchers face, notably liability for s1 CMA.

Regarding unauthorised access, at international level, how to structure the offence of unauthorised access to protect security researchers has been at times discussed. The Council of Europe acknowledged that some Member States have rejected the criminalisation of mere access when 'acts of hacking have led to the detection of loopholes and weaknesses of the security of systems'.[159] The Convention itself offers the options to restrict unauthorised access when security measures are infringed and/or when the defendant has intent to obtain computer data or other dishonest intent.[160] Whether these options would avoid criminalisation of security research has not been articulated by the Council of Europe.

The first option is unlikely to exempt security researchers from criminal liability. Vulnerabilities do not necessarily correspond to a system being openly accessible, with no security policy implemented.[161] Thus finding vulnerabilities may still lead security researchers to infringe security measures. Adopting this restriction will not protect security

[157] Dorothy Denning, 'Reflections on Cyberweapons Control' (2000) 16(4) *Computer Security Journal* 43, 50-52; Stuart Staniford, reporting to the CVE board on 05 October 2000, at <http://www.cve.mitre.org/board/archives/2000-10/msg00007.html>; Jason Wallace, 'The Cybercrime Treaty' IThell 2 November 2000, at <http://www.ithell.com/Opinion/Cybercrime_Treaty/Cybercrime_Treaty_page_2/cybercrime_treaty_page_2.html>

[158] Gillepsie (n 2) 73-74

[159] Explanatory notes, para 49.

[160] There is also the option to restrict hacking to interconnected computers. In most cases, security research involves interconnection with computers; thus the option is irrelevant to this analysis.

[161] Freitas (n 2) 53-55

researchers. In addition, it is likely not to protect vendors either. As Freitas demonstrated, systems and their owners deserve protection even if systems owners fail to implement adequate security measures.[162] In that sense, that the EU Directive 2013/40 has introduced it as a mandatory element to its Article 3 offence of illegal access remains problematic.

The second option in the Cybercrime Convention, not present in the EU Directive, may be more appropriate. Security researchers do not aim to obtain computer data other than the data describing the vulnerability. They may access confidential data, but they would not keep and use this data for illegal purposes. Thus the second option could be worded to protect security researchers. It is not dissimilar to the Law Commissions' proposals of 1987 and 1988, of not criminalising unauthorised access where the hacker has showed no dishonest intent to procure an advantage for oneself. Like these past proposals, its main flaw is that vendors would not be protected against criminal hackers until it was too late. In any case, the UK has not envisaged any of the two options in the Cybercrime Convention, and the mandatory restriction established by the EU Directive. Like many member states, the UK is not alone in having kept the broader offence of unauthorised access. [163]

Interestingly, during the drafting of the Directive 2013/40/EU, two MEPs proposed in an amendment to Article 3 in order to grant to security researchers what one of the MEPs named 'whistleblower protection'.[164] The offence would have been committed only when 'the operator or vendor of the system is not fully informed of the vulnerability in a timely manner'. Effectively, the proposal incorporated the practice of responsible disclosure as an objective element to exempt security researchers from criminal liability. It was a step in the right direction. However, the proposal would not have resolved other legal challenges security researchers may face. Even if disclosure to vendor and operator has been timely, security researchers may still be liable as accessories to unauthorised access if they subsequently choose to disclose to the public because the vendor has failed to fix the vulnerability timely disclosed. Modifying the offence of unauthorised access is thus not sufficient to protect security researchers from criminal liability; no more than modifying the offence of misuse of hacking tools is.

A more holistic approach is needed, that embraces all the cybercrime offences security researchers may be liable for. Furthermore, two competing interests need to be balanced: that to find vulnerabilities, security researchers may breach the confidentiality and integrity of the systems criminal law aims to protect; that vendors need protection from criminal hackers. The Law Commissions' past proposals attempted to establish a balance through the structure of the offence of unauthorised access. Their main weakness was that by allowing exploration of the systems, criminal hackers would also escape criminal liability. Structuring the offence of unauthorised access proved equally difficult at international level. The options offered by the Cybercrime Convention, even if the UK were to adopt them, as well as the EU Directive restrictive definition of unauthorised access would not provide sufficient protection to security researchers.

A first step could be the use of vulnerability disclosure policies from vendors in order to set the boundaries for acceptable hacking, but, as *Mangham* illustrated, they also have their

[162] (n 2) 59-60.

[163] The UK is not isolated in that respect, see Europen Commission, Report assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, COM (2017) 474 at <http://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-474-F1-EN-MAIN-PART-1.PDF>

[164] European Parliament (n 115), Amendment 85 (MEP Vergiat) and 86 (MEP Albrecht) at 33-34.

limits. Could the use of prosecutorial guidelines filter cases so that independent security researcher would not be prosecuted? Or would a public interest defence be more appropriate?

4 – Choosing an appropriate response: the proposal of a defence for hacking

To reduce criminal law's impact in the UK, and in other jurisdictions, ENISA suggested drafting prosecutorial guidelines along the lines of the Dutch model implemented in 2013 so that all stakeholders would understand how prosecutorial authorities would exercise their discretion to prosecute security researchers.[165] The suitability of these guidelines needs to be assessed before sketching the benefits of a public interest defence.

4.1 – The suitability of prosecutorial guidelines

Resorting to prosecutorial guidelines is not a new idea. The OECD 1986 report on cybercrime had already recommended not prosecuting security researchers in the presence of the following two elements: the security researchers' 'inten[t] to improve data security', and their 'immediate notice of [the] access and of the loopholes used in the data system to the victim or to state authorities'.[166]

In the UK the Crown Prosecution Service issued some guidelines on prosecution for CMA offences in late December 2007. The guidelines followed the CMA reform of 2006 by the Police and Justice Act. They aimed to fulfil the government's promise during the 2006 parliamentary debates to quell concerns about unwarranted prosecution of security researchers for making, distributing or obtaining hacking tools as per the new section 3A CMA.

The guidelines set out a series of questions as a test for deciding to prosecute. Criticised at the time of publication by security researchers and academics,[167] their effectiveness remains difficult to gauge. In *R v Mangham* the defendant was charged under s3A CMA, in addition to s1 and s3 CMA, but he refused to plead guilty for the s3A CMA offence. The reasons for the refusal were not provided and it could be speculated that Mangham used the guidelines to demonstrate that he did not commit the offence. However, the fact remains that the guidelines failed to stop the prosecution for s3A CMA, even though the final decision was to lie the charge on file. This could be indicative of the difficulties of relying on guidelines to avoid the threat of prosecution. Furthermore, the guidelines on

[165] ENISA (n 1) 65-66.

[166] Organisation for Economic Co-operation and Development, *Computer-related crime: analysis of legal policy* (OECD 1986) 63

[167] Richard Clayton, "Hacking tool guidance finally appears", Blog 31 December 2007 at <https://www.lightbluetouchpaper.org/2007/12/31/hacking-tool-guidance-finally-appears/> accessed 27 November 2017; Mark Barwise, "UK Crown Prosecution Service publishes Computer Misuse Act guidance" 04 January 2008 at <https://web.archive.org/web/20080107070650/www.heise-security.co.uk/news/101286> accessed 27 November 2017; Vasilios Katos, and Steven Furnell, 'The security and privacy impact of criminalising the distribution of hacking tools' (2008) 7 *Computer Fraud & Security* 9, 15; Anonymous, 'UK Crown Prosecution Service publishes Computer Misuse Act guidance' 4 January 2008, at <http://www.h-online.com/security/news/item/UK-Crown-Prosecution-Service-publishes-Computer-Misuse-Act-guidance-735749.html> accessed 27 November 2017, cited in Andrew Murray, *Information Technology Law* (3rd ed., OUP 2016) 385.

security researchers only concern s3A CMA. Certainly, the DPP needs to consider the public interest in prosecution as a general rule but the absence of guidance as to how this public interest plays for security researchers accused of committing s1, s3 and s3ZA CMA may prove difficult to articulate, as *Mangham* partially suggests. Thus, could the gaps be filled by adopting the model ENISA suggested in 2015?

The Dutch prosecutorial guidance emerged after two high-profiles incidents in 2011. Academics who had unveiled serious vulnerabilities in the Dutch public-transport chip card were investigated for violating the Dutch Computer Misuse Act. To avoid similar situations arising the Dutch National Cyber Security Centre (NCSC) issued guidance for both vendors and security researchers on responsible disclosure policy in 2013. The policies are far more detailed than Facebook's 2010 policy in Mangham, although the NCSC recognises that they cannot be too prescriptive. The NCSC did not act in isolation. The Dutch Ministry of Security and Justice publicised the guidance[168] and the Dutch prosecutorial authority published its own guidance.[169]

The terms of the prosecutorial guidelines illustrate this concerted approach. The test for prosecution strongly echoes the terms of vulnerability disclosure policies that the NCSC promoted and by which the vendor authorises the security researcher to hack providing his/her actions remain proportionate.

The Dutch prosecutorial guidelines contain the following three-part test: were the security researcher's actions necessary within a democratic society (general interest)? Were the actions proportionate to the goal to be achieved? Could the security researcher have taken other possible courses of action that were less intrusive?[170] In particular, the security researcher should not use brute force attacks or compromise further the security of the system; s/he should also avoid copying, modifying or deleting files, the alternative, whenever possible, being to create a directory listing for the system as proof of concept of the vulnerability.[171] In other words, the prosecutorial test looks at how independent security researchers can achieve an objective of public interest and how their activities are proportionate to the objective sought. The effect is to set limits on security researchers' activities whilst carving a space for security researchers to find vulnerabilities without undue fear of criminal prosecution. In this sense the test strongly echoes the structure of the proposed offences of unauthorised access in the SLC 1987 draft Bill, the ELC's 1988 options B and C and Nicholson's 1989 Bill.

How effective the test has been in reducing investigations has not been documented so far. The effect of the NCSC guidance has been to increase the number of organisations publishing their disclosure policies and 'paying attention to the legal implications' of their policy in light

[168] <https://www.ncsc.nl/english/security>; see also The National Cyber Security Centre, The Netherlands, 'Introducing Responsible Disclosure. Experiences in The Netherlands: A Best Practice Guide', in *Global Conference on CyberSpace 2015*, 9-10 < https://www.gccs2015.com/documents/introducing-responsible-disclosure-experiences-netherlands-best-practice-guide> accessed 27 November 2017.

[169] Openbaar Ministerie, Letter to: Aan alle parkethoofden, 18 March 2013, <https://www.om.nl/publish/pages/22742/03_18_13_beleidsbrief_college_responsible_disclosure.pdf> accessed 2017. Translation in English, ENISA (n1) 52.

[170] ENISA (n 1) 52.

[171] The National Cyber Security Centre, *Policy for arriving at a practice for Responsible Disclosure*, 2013, 8 < https://www.ncsc.nl/english/current-topics/news/responsible-disclosure-guideline.html> accessed 27 November 2017.

of the prosecutorial guidelines.[172] In this sense, the coordinated approach of good vulnerability disclosure policies and prosecutorial guidelines could be said to be effective. It would probably be suitable for the UK CPS to adopt a similar approach. Strong guidelines would potentially help hackers such as Mangham, who are on the autism spectrum.[173]

However, for the security researcher, prosecutorial guidelines may not suffice to significantly reduce the risk of criminal liability. They should decrease the risk of prosecution. However, if the prosecution authority nevertheless decides to go ahead there is uncertainty as to whether the security researcher could rely on prosecutorial guidelines and/or on the vulnerability disclosure policy to convince the judge s/he is not guilty of having committed computer misuse offences.

As per *Cuthbert*, the structure of the CMA offences, especially of s1 CMA, does not allow for integrating the proportionality of the security researcher's actions into the analysis of the *actus reus*. The motive of public interest cannot be taken into account either as part of the *mens rea*. Arguably, in *Cuthbert* no prosecutorial guidelines existed but Cuthbert was leading one of the key organisations in the process of establishing standards in security research. Although it is unclear from the news reports whether he referred to these standards in Court he chose to plead not guilty, thus arguing he should not be convicted. Yet, he was unable to convince the judge *not* to find him guilty despite the judge regretting the conviction. Whether prosecutorial guidelines would have changed the situation is unclear.

At a more practical level it is also uncertain whether the security researcher would feel confident enough to challenge before the court the prosecutorial interpretation that his/her actions were illegal. Mangham explained he felt compelled to plead guilty to most charges.[174] Yet, this paper demonstrated that most of his actions could be considered compliant with Facebook's vulnerability disclosure policy. Again, no prosecutorial guidelines existed but, given that the suggested guidelines put forward criteria essentially similar to those of vulnerability disclosure policies, would Mangham have felt able to challenge before a judge both the vendor's and the prosecution's interpretation of the facts and law?

Put differently, prosecutorial guidelines are strongly desirable because security researchers can read them and understand better the boundaries of legal and illegal actions. However, in the event that security researchers are prosecuted, guidelines would still leave uncertainty as to whether the security researchers could demonstrate to the court that they did not commit CMA offences. A public interest defence would enable security researchers to argue the proportionality of their actions with regard to the public interest they have pursued.

[172] The National Cyber Security Centre, 'Introducing Responsible Disclosure' (n 168) 20, 22-23.

[173] *R v Martin* [2013] EWCA Crim 1420; Gary McKinnon who was not extradited to the US, *McKinnon v The United States of America and another*, [2008] UKHL 59; but Lauri Love was, Kevin Lawrinson, 'Amber Rudd orders Lauri Love extradition to US on hacking charges' *The Guardian* 14 November 2016, <https://www.theguardian.com/law/2016/nov/14/amber-rudd-approves-lauri-love-extradition-to-us-on-hacking-charges> accessed 2017; Lachlan Urquhart, 'Should having autism be a legal defence to hacking charges?', *Sophos Naked Security* 10 February 2012, <https://nakedsecurity.sophos.com/2012/02/10/should-having-autism-be-a-legal-defence-to-hacking-charges/> accessed 2017; Punit Shah, 'People with autism make more logical decisions' The Conversation 13 October 2016, < http://theconversation.com/people-with-autism-make-more-logical-decisions-66946> accessed 2017; and the related research, Punit Shah, Caroline Catmur and Geoffrey Bird, 'Emotional decision-making in autism spectrum disorder: the roles of interoception and alexithymia' (2016) 7(1) *Molecular autism* 43.

[174] Penny Darbyshire, 'The mischief of plea bargaining and sentencing rewards' (200) *Criminal Law Review* 895; Nuno Garoupa and Frank H. Stephen, 'Why plea-bargaining fails to achieve results in so many criminal justice systems: A new framework for assessment.' (2008) 15(3) *Maastricht Journal of European and Comparative Law* 323.

4.2 – Sketching a public interest defence

In the last thirty years sole reliance on vendors' willingness to improve the security of their systems, as advocated by the ELC in 1989, has failed to significantly contribute to the security of IT systems. If prosecuted, security researchers need a mechanism to discuss before the courts the implications of their work and the methods used. To do so at mitigation stage does not suffice. When sentenced, security researchers are left with a criminal record and are likely to spend some time in prison. A mechanism needs to allow security researchers to demonstrate that they acted in the public interest and proportionately, so that they could be found not guilty.

Article 6 of the Cybercrime Convention represented a first step in this direction. It allowed parties to criminalise the creation, distribution and possession of hacking tools but indicated in Article 6(2) that the courts should not interpret the provisions to impose criminal liability on security researchers. However, Article 6(2) only concerns one offence, in the UK that of section 3A CMA. Furthermore, it does not articulate what the courts should take into account.

In contrast, available to all CMA offences, the defence, which could be called as a short-hand a defence for hacking, would give a statutory basis for discussing before the courts what constitutes technically and ethically responsible vulnerability research. It would take stock of vendors' understandable reluctance to authorise violations of integrity whilst recognising that independent security researchers can undertake work of public interest under certain conditions.

Its terms could mirror the prosecutorial guidelines that the UK could implement as suggested above, as well as the current terms of many bug bounty programmes and vulnerability disclosure policies. The focus would stop being on whether the vendor has or has not authorised hacking. Instead, the discussion would shift to the proportionality of the security researchers' actions and the public interest in vulnerability research.

The defence could be integrated into a more coherent legal and technical framework for the security researcher. A CMA amendment would bring to light government practices of buying vulnerabilities from independent security researchers. It would push for a debate on whether governments should do so and, if so, how they and security researchers selling to them should be regulated.[175]

Furthermore, because security researchers are akin at times to whistle-blowers,[176] the defence would provide additional momentum to re-examine a public interest defence for journalists and whistle-blowers. Such defence for journalists has already been raised in

[175] EDPS (n 5); Bellovin, Clark and Landau (n 25); C. Alden Pelker, 'Permission to Come Aboard (an Adversary's Network)-Ensuring Legality of Enhanced Network Security Measures through a Multilayer Permission Acquisition Scheme' (2016) 53 *Am. Crim. L. Rev.* 437; Jesse Jacob McMurdo, 'Cybersecurity Firms-Cyber Mercenaries' (2016) 4 *Homeland & Nat'l Sec. L. Rev.* 35.

[176] Schneier (n 100); MEP Jan Albrecht, EU Parliament, Draft report (n 115) p38; see also *Bolton v Evans* [2006] EWCA (civ) 1653

1989/1990, suggested in the Leveson inquiry,[177] and discussed in Parliament in 2014 before an amendment to the CMA was withdrawn.[178] In 2015, former DPP Keir Starmer has called for journalists to benefit from a public interest defence for a variety of offences among which the CMA offences. He felt that the prosecutorial guidelines for the media –drafted when he was DPP- were insufficient to protect journalists in difficult cases.[179] Similar arguments could be put forward for security researchers, although there are differences between security researchers reporting vulnerabilities and journalists writing, for example, on tax evasion as in the Paradise papers. Whereas journalists may report on wrongdoing, security researchers are unlikely to report on others' activities that would be illegal *per se*. As demonstrated, even if good security were to be systematically part of products' design, vulnerabilities would remain and would have to be discovered. Public interest in security research does not lie necessarily in the interest of the public to be informed of vulnerabilities, but on security researchers being able to investigate and report vulnerabilities to vendors without fear of prosecution.

5 - Conclusion

This paper outlined the existing tensions between the public interest in security researchers engaging in vulnerability research and the legal challenges they currently face along the three phases of vulnerability research – discovery, verification and disclosure-. This paper then proceeded to demonstrate that three options could be available with regards to criminal law.[180]

The first option would be to modify the structure of the CMA offences, notably the offence of unauthorised access, along the lines that the Scottish and English Law Commissions proposed in 1987 and 1988. Their choice was to legalise unauthorised access when the hacker took reasonable care not to damage the computer system and did not intentionally act to gain an advantage for himself or for another. This was a significant step forward. Security researchers would have avoided criminal liability whilst being constrained in their actions, notably at the verification and disclosure stage. Yet it had serious drawbacks which have not faded over the years as the discussions on the structure of these offences in the Cybercrime Convention and in the EU Directive 2013/40/EU have demonstrated. Should these past proposals be implemented criminal law would be unable to send the important signal that malicious hackers should not hack and that public interest also lies in protecting the integrity of vendors' IT systems.

[177] *Leveson Inquiry, Cultures, practices and ethics of the press*, 2012, HC 780-IV, Part J, Chapter 2; see also George O'Malley, 'Hacktivism: Cyber Activism or Cyber Crime' (2013) 16 *Trinity CL Rev.* 137, 147-148; Alison Powell, 'Hacking in the public interest: Authority, legitimacy, means, and ends.' (2016) 18(4) *New Media & Society* 600. A defence of public interest for journalists already exist in s55 DPA, HC *Privilege: Hacking of Members' mobile phone* – 14th Report HC 628, 2011, para. 19; L. Webley, 'The Former Legal Director of the London Times, Legal Professional Privilege and the Duty Not to Mislead the Court in England and Wales' (2014) 17(2) *Legal Ethics* 310.

[178] HL Deb 20 October 2014, cols 539-546

[179] The speech is available at <http://www.keirstarmer.com/the_london_press_club_debate> and reported by Roy Greenslade, 'Keir Starmer to call for journalists to have aa public interest defence', *The Guardian* 13 July 2015, at ,https://www.theguardian.com/media/greenslade/2015/jul/13/keir-starmer-to-call-for-journalists-to-have-a-public-interest-defence> accessed 27 November 2017.

[180] For a study on vendors' liability for bad design in software and the correlative need for standardization, Roksana Moore, 'Standardisation: A tool for addressing market failure within the software industry' (2013) 29(4) *Computer Law & Security Review* 413.

The second option would be to modify the CPS current guidelines along the lines of the Dutch model, as suggested by ENISA in 2015. This would require a concerted approach between the CPS and the UK equivalent of the Dutch National Cybersecurity Centre. Vendors would be pushed to adopt best practices in drafting vulnerability disclosure policies that outlined the obligations of all stakeholders, not just the security researchers. Better drafted policies and prosecutorial guidelines could even contribute to reducing the risk of prosecution for hackers on the autism spectrum, who are disproportionally represented in hacking cases. Nevertheless, this option does not provide certainty as to what security researchers could argue before the courts should they be prosecuted.

Thus, this paper proposed a third option: creating a public interest defence for the security researcher. The tension between the public interest in security researchers finding vulnerabilities and the private interests of the vendors in protecting the integrity of their IT systems is only apparent. They are two sides of the same coin: the fight against cybercrime. Thus, the defence would allow independent security researchers to take an active part in the fight against cybercrime, to the benefit of the wider public. Finally, a defence would fit within the wider debate on whether journalists and whistle-blowers would benefit from a public interest defence for hacking.