Towards a supportive legal environment for global cybersecurity: the case for a public interest defence in international legal instruments on cybercrime

Accepted for publication in Global Cybersecurity and International Law

Towards a supportive legal environment for global cybersecurity: the case for a public interest defence in international legal instruments on cybercrime.

Author: Dr Audrey Guinchard, University of Essex, abguin@essex.ac.uk

Vulnerabilities, these flaws in software and systems,[1] have long been recognised as an unwanted but inevitable outcome of coding and implementing network and information (NI) systems.[2] When discovered and exploited by criminal hackers, they compromise the security of NI systems. The resulting unauthorised access often leads to the commission of further crimes, notably fraud and the spread of ransomwares and spywares.[3] Conversely, the responsible disclosure and removal of vulnerabilities significantly contribute to the closure of the security gap, and consequently to the prevention of cybercrime and the protection of individuals and their rights, notably privacy and freedom of expression.[4] Over the last fifteen years, the race to fix vulnerabilities has led to the development of a complex vulnerability environment in the Global North, progressively extending to the Global South.[5] At its heart is the vital role that independent security researchers play in finding and timely reporting vulnerabilities to vendors who supply or implement IT products.

Yet, when not invited to hack by vendors, they face significant criminal law challenges under national cybercrime legislations.[6] In Europe and the US, some have already been

[1] The first legal definition of a vulnerability in the world is in Article 6(15) of the Directive 2022/0383 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive 2016/1148 2022 *OJ* . See also, European Network and Information Security Agency (ENISA), *Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations* (2015) 14-15

[2] OECD, 'Encouraging Vulnerability Treatment. Overview for Policy Makers', *OECD Digital Economy Papers*, No. 307, February 2021, (OECD Publishing, Paris) pp10-12, 31-32 https://doi.org/10.1787/0e2615ba-en; ENISA (n 1) and *Economics of vulnerability disclosure* (2018) 15-16; 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, 410.

[3] ENISA (n 2) 7, 56-57

[4] European Parliament, LIBE, *Report on the fight against cybercrime*, (2017/2068 (INI), 25 July 2017, para 1, 27, 30, 31, 55, at <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2017-0272+0+DOC+PDF+V0//EN>; Adamantia Rachovitsa, 'Engineering and lawyering privacy by design: understanding online privacy both as a technical and an international human rights issue.' (2016) 24(4) *International Journal of Law and Information Technology* 374, 375, 393-395.

[5] For an analysis of countries' readiness in the world, S. Creese and others, 'Cybersecurity capacity-building: cross-national benefits and international divides' (2021) 6 Journal of Cyber Policy 214

[6] This chapter focuses on the computer-dependent offences and excludes the computer-aided offences such as fraud or forgery, which the Council of Europe Convention on cybercrime n. 185 defines but which the Directive 2013/40/EU leaves aside. Interception will also be overlooked, as it is often tackled through procedural national laws and tends to concern government surveillance. The chapter will also exclude the wide range of offences, other than unauthorised access, to be criminalised in the 2022 draft UN Convention on cybercrime, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (hereinafter, Ad Hoc Committee), Fourth session 9-20 January 2023, A/AC.291/16 *Consolidated negotiating document on the general provisions and the provisions on criminalization and on procedural measures and law enforcement of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes* (7 November 2022)
https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_fourth_session/main.html

convicted for the commission of unauthorised access or hacking.[7] Slowly, national legal authorities in these regions start to confront the 'chilling effect' of cybercrime laws,[8] but the emerging changes are fragmented and unsatisfactory.[9] The same pattern of overreaching criminalisation and underwhelming consideration of the criminal law's impact on security research underpins the international legal instruments on cybercrime, including the current proposals for a UN Convention on Cybercrime.[10] In effect, calls for a safe harbour have emerged, but without details. They are on the margins of computer science and the law, in an effort to clarify the technical, rather than legal, framework of vulnerability treatment.[11]

This chapter argues that these efforts are unlikely to yield any legal certainty for security researchers, since the technical and legal understandings of which searches would be or not authorised do not align. More importantly, the misalignment masks the real focus of the technical debates, which is on identifying the necessity and proportionality of vulnerability research activities. The criminal law best recognises these considerations, not in the structure of its offences, but in defining defences to legitimise otherwise illegal conducts.

Therefore, to establish a legal environment effective in its support of global cybersecurity research, this chapter proposes to add a public interest defence to the computer-dependent offences. [12] And in recognition of the global nature of security research, which calls for a harmonised protection of security researchers, the chapter argues for adding a public interest defence in the current and future cybercrime international instruments, namely: the Directive 2013/40/EU on attacks against information systems, the Convention on Cybercrime n. 185 which is currently the *de facto* international treaty on cybercrime[13] ; and the future UN Convention on cybercrime currently discussed.

---

[7] UK: *R v Cuthberth* (Crown Court, 2005, unreported); Peter Sommer, 'Two Recent Computer Misuse Cases', (2006) 16/5 *Computers & Law*, http://www.pmsommer.com/CLCMA1205.pdf accessed 02 August 2019; *R v Mangham* [2012] EWCA Crim 973. Both were analysis by this author in 'The Computer Misuse Act 1990 to support vulnerability research? Proposal for a defence for hacking as a strategy in the fight against cybercrime', 2018 Journal of Information Rights, Policy and Practice, 2(2), p.1 DOI: http://doi.org/10.21039/irpandp.v2i2.36. In the US: US v. Auernheimer, 748 F.3rd 525 (3rd Cir. 2014); 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, Alana Maurushat, *Disclosure of Security Vulnerabilities: Legal and Ethical Issues* (Springer 2013) 35-52; OECD (n 2) 29-30

[8] OECD (n 2); ENISA reports (n 1, 2); ENISA, *Coordinated Vulnerability Disclosure Policies in the EU* (13 April 2022) <https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu> p74-75; Centre for European Policy Studies (CEPS), *Software Vulnerability Disclosure in Europe, Report (2018)* *https://www.ceps.eu/ceps-publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges/*

[9] For some of the changes, ENISA (n 7) pp14-47; Audrey Guinchard, 'Better cybersecurity, better democracy? The public interest case for amending the Convention on cybercrime n.185 and the Directive 201340EU on attacks against information systems', in Ricardo Pereira, Annegret Engel and Samuli Miettinen, The Governance of Criminal Justice in the European Union (Edward Elgar, 2020) chapter 8, p148

[10] Ad Hoc Committee (n 6)

[11] OECD (n 2) 31-36; ENISA (n 2) 66 and (n 8) 42

[12] This chapter deepens the analysis undertaken in a previous work, with a particular focus on authorisation, Guinchard (n 9)

[13] Report on the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, A/CONF.213/18 (18 May 2010), para. 46-49, 65, 203-204. Similarly, Recital 15 Directive 2013/40/EU. The situation may change if the draft UN Convention on cybercrime comes to fruition in the next few years.

The conflation of hacking with crime, notably unauthorised access, brought the unwarranted criminalisation of a wide range of legitimate security practices, with little protection afforded to these independent security researchers.[14] At international level, neither the Council of Europe since the drafting of the Budapest Convention, nor the EU Commission with regard to the Directive 2013/40/EU, have mentioned the criminal law challenges security researchers face.[15] While the UNDOC Ad Hoc Committee expressly raised the question of 'legal protections of vulnerability researchers',[16] the responses of Member States have so far ignored the matter, as does the current common draft.[17] In effect, concerns about the legal risks security research entails have received attention mostly outside the sphere of cybercrime, in cybersecurity circles, usually as part of a reflexion on how the vulnerability research ecosystem could carve a space for independent security researchers to improve global cybersecurity.[18] In particular, the last decade has witnessed an impetus among policy makers to develop coordinated vulnerability disclosure (CVD) policies. The objective is to establish best practice and clarify the technical and financial boundaries of security research, notably which search can be authorised in a multi-stakeholders environment. [19] In doing so, they aim to promote cooperation between researchers and vendors, and subsequently mitigate security researchers' exposure to criminal liability. This movement has culminated in the EU in the NIS2 Directive requiring Member States to adopt policies on 'managing vulnerabilities',[20] and encourag[ing] them to adopt guidelines as 'regards the non-prosecution of information security researchers'.[21] While welcomed for its recognition of the problem, this approach has a major flaw: guidelines are no substitute for reforming the criminal law, as ENISA and the OECD clearly stated.[22] In fact, the OECD argues that guidelines on vulnerability treatment will not yield their full benefits until and unless the legal framework is modified. [23] Nevertheless, their call for amending the Budapest Convention (for the OECD) and the Directive 2013/40/EU (for ENISA) remains vague, with no details as to how the criminal law should be amended.[24] A few law academics, as well as a European think tank, have also analysed the threat, proposing a 'safe harbour' but without details as to its precise shape.[25] This chapter proposes to do just that. After an overview of the vital contribution independent security researchers bring to the governance of (cyber)crime, it will outline the patterns of

[14] ENISA (n 1, 2); OECD (n 2); Maurushat (n 7)

[15] Lorenzo Picotti and Ivan Salvadori, *National legislation implementing the Convention on Cybercrime – Comparative analysis and good practices, Discussion paper*, 28 August 2008; EU Commission*, Report from the Commission to the European Parliament and the Council 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 evaulati Framework Decision 2005/222/JHA*, 23 September 2017, COM (2017)474, 13

[16] Letter from the Chair of the Ad Hoc Committee, including guiding questions (25 May 2022), *Letter from the Chair of the Ad Hoc Committee, including guiding questions* (25 May 2022) <https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Documents/Letter_from_AHC_Chair_-_2nd_session_methodology_and_guiding_questions4115.pdf >

[17] Ad Hoc Committee (n 6) and the second session for Member States' proposals

[18] ENISA reports (n 1, 2, 8); OECD (n 2); Centre for European Policy Studies (CEPS) (n 8)

[19] ENISA (n 8) reviewing practices beyond the EU, in China, Japan and the US

[20] Article 7(2)(c) NIS2 (n 1)

[21] Recital 60 NIS2 (n 1)

[22] ENISA (n 8) 74-75 ; OECD (n 2) 35

[23] OECD (n 2) 27, 35-36

[24] Ibid ; ENISA (n 7) 74-75

[25] CEPS (n 8) 42-45, 79. Notably, Maurushat (n 7) and her references.

criminalisation of security research, explaining why the current structure of the criminal law, notably its concept of authorisation, is particularly ill-suited to protect security researchers and why a public interest defence should be preferred to recognise the necessity and proportionality of legitimate security practices . The chapter will then demonstrate the limits of reforms at national level and review the reasons for amending the Budapest Convention and the EU Directive 2013/40/EU. It will draw on the lessons learned from these two influential international instruments to inform the current discussions on a UN Convention on cybercrime and argue that a public interest defence constitutes an effective mechanism to establish a delicate balance between providing a safe haven to security researchers and maintaining the effectiveness of cybercrime legislations in deterring criminal hackers.

1. The vital contribution of independent security researchers to global cybersecurity

Cutting across a variety of products created by different code and/or system owners, vulnerabilities are ubiquitous.[26] Consequently, they need to be found and fixed. The same interconnectedness which compounds the impact of a vulnerability increases the positive effects of removing vulnerabilities, benefiting all stakeholders.[27] The question is thus who should be in charge of finding and fixing vulnerabilities. An obvious answer is for vendors who supply IT products and/or are system owners to bear the costs of improving the security of their products and systems. National governments, whether linked to national intelligence agencies or to law enforcement forces, also actively search for vulnerabilities in computer systems, for offensive purposes. Whether they are authorised to do so, and, if so, to what extent, is a grey area, outside the direct scope of this chapter.[28]

The other actors engaged in vulnerability research are security researchers. This very diverse group can include students, companies, academics, free-lance professionals or just amateurs in computer science who may be knowledgeable but work in their spare time.[29] They can be hired by vendors (and governments) or work independently. The necessity of their work as independent researchers was initially contested. Their reporting of vulnerabilities was to be for free and rewards to be entirely at the discretion of vendors. Vendors were expected to drive the finding and patching vulnerabilities, a model which the Council of Europe still supported in 1990.[30] Some vendors have recognised the necessity to find and patch vulnerabilities. Consequently, they employ, permanently or temporarily, one or several

[26] OECD (n 2) chapter 1; see also Guinchard (n 7).
[27] 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
[28] See section 4.2
[29] 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
[30] ENISA (n 1) 18-25; Council of Europe, *Computer-related crime*, 1990, 95-98, and its Recommendation R(89)9 on computer-related crime.

persons to search for vulnerabilities. [31] Unfortunately, however, many vendors abide by the 'penetrate [the market] first and patch later' motto, externalising the cybersecurity costs and harms to their customers. [32] Relying on vendors has thus in practice failed to significantly improve the security of IT products.[33]

The security industry in the US and in Europe reacted to this failure by contributing to the emergence of a complex vulnerability market, so that independent security researchers, not just those hired by vendors, could find an outlet for their work and be paid for it. The first intermediaries or brokers in these legitimate markets appeared after the Convention's signature in 2001, approximately when the 2005 EU Council Framework Decision on cybercrime was enacted.[34] Progressively, vendors have accepted the work of independent security researchers. Many have put in place vulnerability disclosure policies, to establish the conditions for searching for and disclosing vulnerabilities. Some resort to hacking contests through intermediaries such as HackerOne, effectively authorising hacking to a number of chosen security researchers.[35] Vendors may also have bug bounty programmes to create a financial incentive to report vulnerabilities.[36]

As this complex vulnerability research ecosystem matured, the need for less variations in the processes and for the promotion of best practices emerged. It has led over the past fifteen years to the development, often through national Computer Security Incident Response Teams (CSIRTs), of CVD policies to assist organisations in their dealings with independent security researchers.[37] In the EU, it culminated in the NIS2 Directive requiring Member States to establish a CVD policy for the sectors within the Directive's scope.[38] That the first guiding question set by the Ad Hoc Committee expressly asked about their protection from cybercrime offences is a testimony to how far stakeholders have come to accept independent security research as an essential element of cybersecurity and of the fight against cybercrime.[39]

To explain this vital role of independent security researchers, the computer science and economics literature on vulnerability research and markets has identified a range of factors. I have explained these more substantially in a previous work.[40] Here I would like to highlight the effectiveness of independent security research compared to that done by in-house cybersecurity teams. Rewarding independent security research is technically as efficient, if not

[31] 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.
[32] ENISA (n 2) 18-21
[33] The draft EU Cyber Resilience Act published in September 2022 attempts to remedy this situation, see https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
[34] ENISA (n 1) 18-25
[35] Notably, Omer Akgul and others, *The Hackers' Viewpoint: Exploring Challenges and Benefits of Bug-Bounty Programs* (6th Workshop on Security Information Workers, 2020)
[36] OECD (n 2); ENISA (n 2)
[37] Ibid. The US CERT-CC was the first CSIRT and exists since 1988.
[38] Article 7(2)(c) and Recital 60 NIS2 (n 1)
[39] Letter from the Chair (n 17)
[40] Guinchard (n 7)

more so, than hiring full-time employees.[41] Financially, it is from 2 to 100 times more effective than having one's permanent security team.[42] The reason lies in the diversity of vulnerabilities and the breadth of knowledge and skills needed to find them and which are unlikely to be entirely mastered by a single individual or by a team of cybersecurity researchers.[43]

Even organisations which have at their heart strong cybersecurity standards and practices cannot afford the luxury of side-lining independent security researchers. The Pegasus scandal is a case in point. Apple's ability to bring privacy and security to 99% of users has long been reflected in the market price of zero-day vulnerabilities.[44] The corollary has also been that the work of independent security researchers has not been central to Apple's strategy of securing its products, with its bug bounty programme criticised for its failure to adequately reward researchers.[45] In 2019, this approach threatened to damage Apple's reputation for privacy and security, when independent security researchers established the breach of security due to a vulnerability.[46] Since, Apple has certainly learnt its lesson. In July 2022, it was offering $ 2 million to anyone finding a vulnerability in the new 'lockdown' mode it created to counter mercenary spyware such as Pegasus.[47]

The Pegasus scandal illustrates what the academic literature of the last two decades has demonstrated: that the vendors' role in maintaining and promoting high cybersecurity standards is crucial, but that independent security researchers remain vital in improving cybersecurity. It also brings to light another aspect of the vulnerability ecosystem, often subdued in the discussions on security research and cybercrime: that Governments can hack for offensive purposes, and law enforcement authorities for investigative purposes, two grey areas that potentially leave security researchers in a difficult position.[48] Cybersecurity is indeed more than just a technical standard to meet the requirements of confidentiality, integrity and availability of NI systems. Digital technologies are nowadays ubiquitous to every activity in our societies. Depending on the actors involved in the exploitation of vulnerabilities and their objectives, lack of security will not just threaten individuals' privacy and/or access to information if a website is made inaccessible. It also has the potential to threaten the physical safety of individuals, their exercise of freedom of expression, and their ability to make governments accountable. Security research sits uncomfortably between these two

[41] Mingyi Zhao, Jens Grossklags and Peng Liu, 'An empirical study of web vulnerability discovery ecosystems', In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (ACM 2015) 1105, 1115.
[42] Matthew Finifter, Devdatta Akhawe and David Wagner, 'An Empirical Study of Vulnerability Rewards Programs', in (2013) 23 *USENIX Security* 273, 279-280, 286.
[43] On the tendency for security researchers to specialize in certain types of vulnerabilities, Zhao, Grossklags and Liu, (n 42) 1108-1112; Hafiz and Fang (n 30).
[44] Andy Greenberg, 'Why 'Zero Day' Android Hacking Now Costs More Than iOS Attacks' *The Wired* (03 September 2019) <https://www.wired.com/story/android-zero-day-more-than-ios-zerodium/>
[45] Alex Hern, 'Why Apple's walled garden is no match for Pegasus spyware' *The Guardian* (21 July 2021) <https://www.theguardian.com/technology/2021/jul/21/why-apples-walled-garden-is-no-match-for-pegasus-spyware>
[46] In fairness, Apple's security coding facilitated the discovery. Hern (n 46)
[47] David Milmo and Stephanie Kirchagessner, 'Apple to launch 'lockdown mode' to protect against Pegasus-style hacks' *The Guardian* (Manchester 6 July 2022) <https://www.theguardian.com/technology/2022/jul/06/apple-to-launch-lockdown-mode-to-protect-against-pegasus-style-hacks>
[48] OECD (n 2) 19-21; CEPS (n 8)

dimensions, the law recognising neither. Security researchers may have a certain level of protection under the Whistle-blowing Directive 2019/1937/EU and the Council of Europe's Recommendation on the protection of whistleblowers, but their finding of vulnerabilities needs to be within 'a work-related context'. When they are independent, not employed by vendors, that is when they contribute most to cybersecurity, they will naturally be excluded from the scope of these legal instruments. They are then exposed to the full force of the criminal law as cybercrime legislations criminalise their work, despite their vital contribution to closing the security gap.

2. Patterns of criminalisation of independent security researchers

The vulnerability research process has three stages: the discovery of vulnerabilities through the inspection and testing of the information systems and software, with the help of dual-use hacking tools; their verification by creating a proof of concept; and the disclosure or reporting of the vulnerability to the vendor, to an intermediary, and/or to the public. Each stage raises its own technical issues, but not all represent the same legal risks. A first overview of these risks will be followed by a specific focus on the concept of authorisation in the technical field and in law. The developments focus on the Budapest Convention and the EU Directive as implemented by their respective Member States.[49]

2.1 From low to high risks: an overview of the criminal law threats

The main risk of the last two stages, verification and disclosure, stems from security researchers posting publicly, before a patch is available, sufficient information on the vulnerability for criminal hackers to exploit the security gap. This practice might trigger accessorial liability to unauthorised access (Article 11 Convention; Article 8 Directive) or constitute the offence of misuse of tools (Article 6 Convention; Article 7 Directive).[50] Overtime, however, consensus has built around coordinated disclosure where vendors are given enough time to patch the vulnerabilities before the information is released. Consequently, the risk of prosecution is low, although not impossible.[51]

By contrast, the discovery stage concentrates most of the risks security researchers can face, although these will depend on the offence considered. Ranking from low to high risk are: intentional damage and interference (Articles 4 and 5 Convention; Articles 5 and 4 Directive); misuse of tools; and unauthorised access (Article 2 Convention; Article 3 Directive).

When searching for vulnerabilities, security researchers, contrary to criminal hackers, aim to avoid the exploitation of vulnerabilities and the ensuing damage of, or interference with, systems and data.[52] Some techniques for finding vulnerabilities are not without risk though;

[49] For a more detailed comparative law analysis, see Guinchard (n 9).
[50] Guinchard (n 7) and (n 9)
[51] OECD (n 2) 23
[52] Notably, A Nehaluddin, 'Hackers' Criminal Behaviour and Laws Related to Hacking' (2009) 15(7) *Computer and Telecommunications Law Review* 159, 159-160.

when national legislations criminalise recklessness, their actions may fall within the scope of these national laws.[53] Overall, however, the risk of the discovery process involving intentional damage or interference remains low.

The risk of prosecution substantially increases for the misuse of tools offence, not because the international texts failed to provide safeguards to independent security researchers, but because their implementation has been fragmented and inadequate, Member States adopting various broad versions of the offence without the express safeguards of Articles 6 Convention and without the more subdued protection in Article 7 Directive and its interpretative Recital 17.[54] The only exception is France, which explicitly transposed Article 6(2) Convention. Consequently, the issue does not lie in the structure of the offence but in the unwillingness of Member States to comply with the letter and spirit of the international texts.[55]

By comparison, the offence of unauthorised access is far more contentious in its structure, both at international and national levels. It also brings the highest risk of prosecution and conviction to independent security researchers since 'the terms 'unauthorised' and 'access' do not produce a similar set of shared assumptions in the technical, legal or ethical fields' among all stakeholders.[56] The first difficulty lies with the concept of access. Security researchers are unlikely to know with enough certainty which conducts constitute access or attempted access in a given country, even when the conducts are technically necessary to find a vulnerability.[57] The second difficulty concerns the requirement of acting without authorisation or, in the international texts, 'without right'. The literature in law and in cybersecurity does not articulate how the legal concept of authorisation fits within its technical understanding in security research. The following developments are an attempt to do just that.

2.2 Authorisation in the technical field: uncertainties and fragmentation

Three sets of stakeholders can convey authorisation to independent security researchers: national CSIRTS when a state has one, vendors, and the intermediaries managing bug bounty programmes. The national CSIRTs act as voluntary or mandatory co-ordinator between vendors and researchers. To facilitate this role, they may establish a national CVD policy explaining how vulnerability treatment from discovery to disclosure should be approached by all sides. When they do so, their policy is understood as an authorisation, independently of what vendors do within their own organisations.[58]

Vendors, both in the private and public sector, may have their own vulnerability disclosure policies, with or without a bug bounty programme. These policies are considered as authorising vulnerability research within the parameters they set. Vendors may work in close

[53] For a detailed analysis, see Guinchard, 'Better Cybersecurity' (n 9) 156
[54] Ibid.
[55] Criminal Law Reform Now Network (CLRNN), *Reforming the Computer Misuse Act 1990* (2020) 57
[56] Maurushat (n 7) 49.
[57] Guinchard (n 9)
[58] ENISA (n 8); OECD (n 2)

collaboration with the national CSIRTs, but not necessarily, especially if the CSIRT has no established CVD policy. [59]

The third group is those involved as intermediaries, running bug bounty programmes. The research process is often structured in detail, intermediaries proposing templates vendors adapt to their needs and specific objectives. The OECD qualified them as 'open contracts', highlighting how the authorisation to find vulnerabilities is the closest to the 'gold standard' of mandated testing, that is of a contract expressly negotiated and agreed by vendors and security researchers *before* the search starts.[60]

Therefore, researchers face a fragmented landscape that places a significant onus on them finding the document possibly authorising their search. Not all vendors have vulnerability policies, and even less so, bug bounty programmes, often because these are costly and difficult to run.[61] Authorisation through national CVD policies is not a widespread practice either. In the EU, as per April 2022, only four Member States had implemented a national CVD policy; nine had none; and fourteen were at different stages of implementing one. The NIS2 Directive in requiring Member States to adopt a CVD policy will bring a certain level playing field in Europe, but beyond Europe and the US, fragmentation reigns. To compensate, researchers may choose to report to a different CSIRT than that of their country, if more suitable to their findings and to their risks, but the onus is still on them to identify the relevant CSIRT and its policy if there is oneany.[62]

In the absence of any of the documents mentioned above, no prior authorisation exists to search and access the system or product. National CSIRTs and vendors give authorisation retrospectively, when they receive the report, but independent security researchers will not know about their perspective until after having committed the offence of unauthorised access. Researchers are particularly exposed to vendors' retributive actions, unless the national CSIRT receives first the report and provides anonymity to security researchers.

Furthermore, assuming they found an authorisation, researchers will not know with a high degree of certainty whether their conducts were fully authorised. A CVD policy and a vendor's policy provide an express structure to engage in vulnerability research, but significant grey areas remain. Typically, a policy bans specified conducts, such as denials of service attacks, installing malwares, spamming, phishing and brute force attacks to obtain log in details. The ban is uncontroversial and uninformative: independent security researchers would not

[59] Ibid.
[60] OECD (n 2) 26.
[61] OECD (n 2) 17, 26 ; Uldis Ķinis, 'From Responsible Disclosure Policy (RDP) towards State Regulated Responsible Vulnerability Disclosure Procedure (hereinafter – RVDP): The Latvian approach' (2018) 34 Computer Law & Security Review 508, 518
[62] OECD (n 2) 20-21

normally engage into these conducts. [63] For bug bounty programmes, a long list of prohibited actions is actually counter-productive, leading to less vulnerability submissions.[64]

National CVD policies often encourage vendors to identify and restrict vulnerability research to certain assets and/or types of vulnerabilities. They also advise the insertion of a safe harbour clause stating researchers will not be prosecute should they comply with the terms set. The problem is that compliance with the policy is not along clear-cut lines. Policies usually do not list acceptable behaviours. Instead, they tend to set out a general duty for security researchers to act proportionally and to report the vulnerability responsibly, by contacting the vendor and/or the CSIRT within a certain time frame. Authorisation relies on a shared understanding between stakeholders as to which conducts are proportionate and which are not. In practice, this interpretation will vary depending on, notably: the ease of access and the extent to which security measures are lacking; the researchers' background, expertise and related knowledge of the potential lack of authorisation; the depth of exploration in the information system (the more depth, the more vendors will recoil); the vendors' (im)maturity and (lack of) familiarity with disclosure; the possibility to have a CSIRT as a coordinator to ease tensions between vendors and security researchers.[65] Consequently, policies can leave enough space for security researchers to contend that their actions complied with its terms and for vendors to argue the opposite, that the action was disproportionate and thus unauthorised.[66]

Furthermore, researchers must contend with variations across policies, even if most have the above common features of banned conducts and proportionality duty. Consequently, one policy may be specific enough to authorise a search, another may ban it or stay silent; while another may encourage the researcher to seek clarification before engaging into the conduct unaddressed by the policy.[67]

Finally, with regards to vendors, '[t]he power dynamics is not in favour of security researchers'.[68] While they are often consulted by national CSIRTs, researchers do not set the rules in vendors' policies. Vendors set them, often to protect themselves, not security researchers.[69] Furthermore, researchers frequently lack legal expertise to counteract vendors' threat to rescind *a posteriori* the authorisation researchers believed was given in the policy.[70] They are thus in a weak position when they wish to argue they were authorised.

[63] ENISA (n 1) 66; Didier Jacquet-Chiffelle and Michele Loi, 'Ethical and Unethical Hacking' in Markus Christen, Bert Gordijn and Michele Loi (eds), *The ethics of cybersecurity* (The International Library of Ethics, Law and Technology, Springer Nature 2020) 179

[64] Yuni Li and Ling Zhao, 'Collaborating with Bounty Hunters: How to Encourage White Hat Hackers' Participation in Vulnerability Crowdsourcing Programs through Formal and Relational Governance' (2022) 59 Information & Management 103648, 10

[65] ENISA (n 8) 62-66; OECD (n 2) 31-35

[66] For a detailed demonstration of the tensions, see the analysis of *R v Mangham* in the UK involving Facebook, Guinchard (n 7)

[67] ENISA (n 8) 31, 41

[68] OECD (n 2) 24; ENISA (n 8) 62

[69] Ibid.

[70] ENISA (n 2) 31; Guinchard (n 7) 13-14

From this summary, it becomes apparent that authorisation in the technical field is not a straightforward matter. So is the criminal law cognisant of this complex landscape and can it provide a degree of protection to independent security researchers?

2.3 – The ill-suited legal concept of authorisation and its criminalising effect

The Convention does not define 'without right', the expression Article 2 uses for lack of authorisation. Its Explanatory Report, more specific, excludes 'authorised testing' from the scope of the offence.[71] The problem is that 'authorised testing' captures the least controversial aspect of security research, when security researchers are formally contracted by vendors. It is unsurprising though. At the time of drafting the Convention, vulnerability markets have not yet emerged. Furthermore, while security researchers criticised draft Article 6 Convention, - and were listened to by the Council of Europe-, they did not articulate the possibility of liability for unauthorised access.[72] The Council of Europe had thus no possibility to articulate how the law would fit the future vulnerability ecosystem. Its Explanatory Report however provides elements for the Convention to be interpreted favourably to independent security researchers. In its general explanation of 'without right', for all offences, it refers to 'classical legal defences [such as] consent, […] self-defence or necessity'. [73] Consent is indeed one element the UK uses to define authorisation. Policies and bug bounty programmes could thus be interpreted as reflecting CSIRTs' and vendors' prior consent to vulnerability research. Whether consent would be an adequate legal concept is examined below.

In contrast to the Convention, by the time the Directive was adopted, the vulnerability research ecosystem has considerably matured. Were the EU institutions cognisant of this and did they intent to authorise the practices? Recital 12 acknowledges that vulnerability research 'is a pertinent element of effective prevention of, and response to, cyber attacks', calling for Member States to 'endeavour to provide possibilities, so as to allow the legal detection and reporting of security gaps'. Yet, the Directive itself is unlikely to provide a safe harbour. Article 2(d) defines 'without right' as 'not authorised by the owner'. Recital 17 only mentions 'mandated testing' with the uncontroversial example of a contract, where risks of prosecution would be low. The final version of Article 3 and Recital 17 is the result of rejecting several amendments to incorporate a liability exemption for responsible vulnerability disclosure. [74] LIBE thus concluded that, despite the debate, the Directive leaves security researchers without protection. [75] Have national laws chosen the same path?

National legislations preferred the word 'authorisation' to the expression 'without right', but 23 EU Member States have not transposed Article 2(d) Directive and most have provided no further guidance. Hence, the EU Commission's call for its transposition to clarify the scope of

[71] Explanatory Report to the Convention on cybercrime, para 47 at https://www.coe .int/en/web/conventions/full-list/-/conventions/treaty/185 (accessed 03 August 2022). Similarly for interception and interference, para 58 and 62

[72] See Draft no 22 REV 2, 2 October 2000, 6-7; also CVE, Panel on Cybercrime treaty, 5 October 2000, at https://cve.mitre.org/data/board/archives/2000-10/msg00007.html

[73] Explanatory Report (n 72) para 38

[74] EU Parliament, Amendments 34-128, Draft Report 2010/0273 (COD), 27 January 2012, amendments 45 and 86 (MEP Albrecht), 85 (MEP Vergiat)

[75] Group briefing, 2010/273, June 2012, 3

the offences.[76] Yet, even if they were to do so, clarification is unlikely to be achieved, for the reasons just explained. Among the current non-EU Member States signatories of the Budapest Convention, definitions of authorisation are also hard to come by, the UK being an exception. Predating the Convention and the Directive, at a time where vulnerability markets were inexistent, its definition describes authorisation as having 'consent to access' or being 'entitled to control access'.[77] Is consent nevertheless suited to define authorisation in the context of vulnerability research? At first sight, yes: a published policy seems to indicate both explicit lack of consent, with its list of prohibited conducts, and implicit consent for the conducts not listed but potentially covered by the duty of proportionality. There are however two issues.

First, the security industry's practice of associating authorisation with the publication of vulnerability policies, often drafted by the private sector, is likely to violate the principle of legality. In European criminal laws, private entities do not have the power to unilaterally decide what is or not criminal.[78] Recital 17 Directive excludes criminal liability for violation of a 'user policy or terms of service' or in 'labour disputes'. Why treat vulnerability policies differently from a user policy for the purpose of defining the scope of a criminal offence? Legality should prevail.

Assuming this first difficulty on legality could be resolved, a more fundamental one remains: is the vendors' implicit consent in a policy the same as assessing the proportionality of security researchers' actions? The technical debate on authorisation focuses indeed on different elements: the objective proportionality of the search (are the actions in line with the major practices in the field?); and security researchers' reasonable belief that the policy authorised them to act in the way they did. In UK law, discussing reasonable belief goes beyond the scope of 'legal' consent and is to be excluded from the understanding of consent. Consent negates the *actus reus*, the material element; reasonable belief in consent negates the *mens rea*, that is the intention to commit the offence. Where an offence, such as unauthorised access, does not have in its constitutive elements a requirement of reasonable belief, the latter plays no role in the analysis of consent. Without a reform, authorisation provides no defence in UK law.[79]

Whether other European cybercrime laws understand the concept of authorisation as excluding reasonable belief is extremely difficult to ascertain. Like in UK law, the two conceptualisations of consent (*actus reus* only; or with reasonable belief in *mens rea*) co-exist in other national laws, depending on the context and the interests underpinning the criminalisation of each specific offence.[80] In the absence of a detailed study in cybercrime which would establish that the UK's distinction between consent and reasonable belief were to be an exception, it is reasonable to conclude that the legal interpretation of authorisation/consent of the EU and Council of Europe is likely to exclude aspects of the discussion used in the technical field to consider the search as proportionate and legitimate.

[76] EU Commission (n 16) 6, 12
[77] S17(5) Computer Misuse Act 1990
[78] Christina Peristeridou, *The principle of legality in European criminal law* (Intersentia 2015) ch 4, 8
[79] CLRNN (n 56) para 3.5.3-3.5.6
[80] Jeroen Blomsma, *Mens Rea and Defences in European Criminal Law* (Intersentia 2012) 415-417; Jeremy Horder, *Ashworth's principles of criminal law* (9th edn, Oxford University Press 2019), 151-152

Would redefining authorisation to include a reasonable belief in consent suffice to protect security researchers?[81] It is unlikely. When no policy and no formal authorisation exist, the questions about the search's necessity and proportionality do not disappear. In fact, vendors' consent becomes indifferent to the assessment of necessity and proportionality. When CSIRTs act as coordinators and choose to anonymously report to vendors a vulnerability, vendors have to accept the report, whether they agree or not with the search. Not that vendors' perspective should be ignored, but what truly lies behind the question of authorisation is not a question of consent but a question of reasonable belief in public interest in the search and an issue of balancing the different rights and interests of the various stakeholders, vendors and researchers alike. The theoretical structure of criminal law traditionally takes into account these elements not through consent as an element of the offence but through the concept of a defence.[82] Hence, my proposal to introduce a public interest defence. The criminal law would then align with the focus of CVD policies and vendors' policies on a proportionality duty.

A defence would also better reflect the terms of the prosecutorial guidelines the Netherlands adopted along with a national CVD policy. The 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?[83] They establish what is in effect a public interest defence at the prosecutorial stage. They bring a degree of certainty but even if they could be adopted by most countries,[84] they may not suffice to protect security researchers once a case has reached the courts. Security researchers may not feel confident enough, or have the means, to challenge the prosecutorial interpretation that their actions were unauthorised and thus criminal. The courts may equally be reluctant to interpret the activities as authorised for fear of not protecting vendors and letting potential criminal hackers walking free. The Council of Europe was cognisant of these difficulties for the misuse of tools offence. It considered that the careful wording of the offence would not suffice once a case would reach a court; consequently, it introduced Article 6(2) Convention which urges the courts not to impose criminal liability on security researchers using hacking tools. There is no equivalent to Article 6(2) in Article 2 Convention. For all these reasons, I argue that only a public interest defence to cybercrime offences would protect effectively researchers. In addition, the reform would be in line with the Council of Europe's initial attempts at defining authorisation twenty years ago when it defined 'without right' by reference to legal defences such as self-defence and necessity.[85]

To summarise, this section has demonstrated the multiple risks security researchers face, with a specific focus on the offence of unauthorised access and its concept of authorisation. In the technical field, authorisation is a multi-faceted notion which varies according to the stakeholders' diverse practices. The drive for national CVD policies, as represented in the EU by the NIS2 Directive, is a welcome step towards more alignment among stakeholders as to

[81] CLRNN (n 56) para 3.5.4. The Report also recommends a public interest defence to protect security researchers.
[82] George P Fletcher, *Basic concepts of criminal law* (Oxford University Press 1998); Horder (n 81) 129-155
[83] ENISA (n 1) 52; (n 8) 64-65
[84] Guinchard (n 9)
[85] Explanatory Report (n 72)

what could be authorised. Yet, some fundamental difficulties remain. Assuming the principle of legality could be complied with, the concept of authorisation in law does not align with that in the technical field, leading to the criminalisation of vulnerability research. The technical discussions centre on whether security researchers act proportionally in the reasonable belief their search is authorised in a policy. Behind the belief in consent lies a different debate: the assessment of the necessity and proportionality of the search, independently of whether a particular vendor agrees with the search. Even if the legal concept of authorisation present in national and international legal instruments were defined, or better defined, it would remain ill-suited to capture the technical discussions. The introduction of a public interest defence should be preferred. The first step would be to do so at national level.

3 – The first step towards effective global cybersecurity: national approaches to support independent security researchers, and their limits

Regarding the offence of misuse of tools, transposing the safeguards Article 6 Convention and Article 7 created would significantly improve the protection of security researchers. Article 323-3-1 French penal code, with its concept of legitimate reason, is, in that respect, a good example of how to restrict the offence, as noted by ENISA. [86]

By contrast, as the previous section demonstrated, amending the offence of unauthorised access is likely to prove very difficult. A preferable option would be for national laws to introduce a public interest defence. It would also force prosecutorial authorities to consider, before prosecuting, whether the defence would apply. Consequently, the defence would limit the opportunities to prosecute, independently of the existence of prosecutorial guidelines on vulnerability research. An additional effect would be to protect against the misuse of tools offence, which rests on the intention to commit unauthorised access, even if national criminal laws do not have a specific exclusionary clause like the French one.

To the best of my knowledge, no legal system has so far established a public interest defence to computer-dependent offences. Yet, such a defence does exist outside the cybercrime laws, ironically for offences structurally overlapping with the cybercrime offence of unauthorised access. For example, the UK Data Protection Act 2018, enacted to complement the GDPR, provides a defence to a form of unauthorised access. S172 provides a defence to security researchers who search for vulnerabilities that would allow for the unauthorised re-identification of individuals whose data was previously anonymised. The legislative provision requires several conditions to be fulfilled: conditions of necessity (a 'reasonable belief that the testing was justified as being in the public interest'), and of proportionality (no intentional damage, and disclosure without undue delay). Whether the parallels between data protection and cybercrime will push the UK to adopt a similar defence in its cybercrime for security researchers is difficult to assess. The UK 2022 submission to the UN for the purpose of drafting

[86] ENISA, *The Directive on attacks against information systems. A Good Practice Collection for CERTs on the Directive on attacks against information systems* (2013) 13-14 at https://www.enisa.europa.eu/publications/the-directive-on-attacks-against-information-systems (accessed 02 August 2022)

the UN Convention on cybercrime makes no mention of a possible defence, beyond, a possible, but very vague, difficult to interpret, reference to Member States having reserved competence to determine the lawfulness of conducts.[87] It is also difficult to quantify whether other countries would do so. The current national proposals before the UN Ad Hoc Committee, entirely silent on a defence, are disappointing. Yet, the global nature of vulnerability research warrants a common approach across Member States, in Europe and beyond, rather than piecemeal reforms dependent on individual countries' willingness to provide legal safeguards. Consequently, I argue that the way forward is for international organisations to agree on a public interest defence in their cybercrime legal instruments.

4 – Towards a more supportive legal environment: integrating a public interest defence in international instruments on cybercrime

The legitimacy of international legal instruments depends on their ability to satisfy the principles of subsidiarity and proportionality.[88] Other considerations are also advanced: the protection of human rights. This section argues that a public interest defence to the cybercrime offences is likely to meet these two sets of requirements. The demonstration will start with justifying amending the Directive 2013/40/EU and the Budapest Convention, before concluding on the implications for a future UN Convention.

4.1 – Meeting the requirements of subsidiarity and proportionality

Under the principle of subsidiarity, which the Council of Europe also recognises,[89] the Union's objective 'cannot be sufficiently achieved by the Member States, either at central level or at regional and local level [and would] be better achieved at Union level'.[90] As demonstrated in sections 2 and 3, the objective to fight cybercrime underpinning the Directive and the Convention is unlikely to be achieved by their respective Member States alone, with sufficient coordination. The current implementation of the texts in national criminal laws is fragmented; their inconsistent interpretations of 'without right', a concept ill-equipped to serve as a defence, brings uncertainty. For the Convention, the initial concept of 'without right' is even confusing since the Explanatory Report explains authorisation by reference to legal defences. These weaknesses in the legal framework have a cross-border dimension and involve serious risks to security since vulnerability research is transnational. By contrast, protecting security researchers from criminal liability across Member States would directly help closing the security gap and would strengthen the enforcement of the Directive 2013/40/EU and the Convention, thus fulfilling their core objective to fight cybercrime.

[87] Article 14(6) in Ad Hoc Committee (n 6) 62 (second session)
[88]The EU has these principles enshrined in the Treaty; the principles are not formally recognised before the Council of Europe and the UN, but shape their respective actions; see notably, Kai Ambos, *European Criminal Law* (Cambridge University Press 2018) ch 2 & 3
[89] Ambos (n 89)
[90] Article 5(3) TEU

The international action must also be proportionate and not exceed what is necessary to achieve its objectives.[91] The proposed defence would not go beyond what is necessary to achieve the objective of strengthening the enforcement of the Directive 2013/40/EU and of the Convention. The cost of implementation by Member States is likely to be limited, beyond the transposition of the amendment to the legal texts. It could even be argued that the reform would reinstate some proportionality into the original EU and Council of Europe's actions in two ways. First, a defence would restrict and thus reduce the scope of criminal law to those criminal hackers who are not security researchers. Secondly, facilitating global cybersecurity practices will, in the medium to long term, reduce the pool of vulnerabilities and thus the number of data breaches and opportunities for criminal hackers to commit cybercrime. The costs associated with the prosecution and convictions of the latter would be progressively reduced. For those countries with a less mature cybersecurity environment, an explicit protection of security researchers is likely to help them developing a significant part of their cybersecurity industry, which in turn will have a positive effect on their fight against cybercrime.

Justificatory defences are less familiar in international law than in national laws, but they are not unknown.[92] The defence could be modelled, for example, on the UK data protection laws or on the Netherlands' implicit defence in its prosecutorial guidelines. What matters is not to leave its definition to Member States; otherwise, they are likely to adopt widely different wordings, fragmenting the implementation of the international instruments and thus defeating the purpose of the reform at international levels.

The defence would provide minimum standards, with Member States able to offer more protection. Noteworthily, in the EU, the CJEU has required, in several instances that domestic authorities ignore domestic criminal law when 'Community law sets certain limits to their power' and the behaviour is for example permitted by EU law.[93] EU law could thus be used as a defence against prosecution and conviction in the event that no justificatory defence exists in a Member State or when the national law defence would be too restrictive. For obvious reasons, the same mechanism is not available within the Council of Europe, but the incorporation of a defence would still provide a guide to the interpretation of the offences, should a Member State fail to adequately implement the safeguard of a public interest defence.

To summarise, amending the Directive 2013/40/EU and the Budapest Convention is very likely to satisfy the principles of subsidiarity and proportionality that must underpin EU legal actions and those of the Council of Europe. The human rights dimension of cybersecurity research may however create more of a political challenge.

4.2 – Fulfilling human rights obligations and political challenges

As the Pegasus scandal demonstrates, vulnerabilities do not just allow for privacy to be compromised, but also threaten the physical safety of individuals, their exercise of freedom

[91] Article 5(4) TEU. See André Klip, *European Criminal Law. An Integrative Approach* (Intersentia, 2009) 35-56
[92] For the EU, Klip (n 92) 210-211; Blomsma (n 81).
[93] Samuli Miettinen, *Criminal law and policy in the European Union* (Routledge 2012) 11

of expression, and their ability to make governments accountable. To incorporate a public interest defence to all computer-dependent offences could thus be argued to foster human rights and strengthen democracy. The Budapest Convention, in its preamble, and Directive 2013/40/EU (Recital 21) acknowledge the Council of Europe and EU's human rights obligations and that of their Member States. A public interest defence would thus enable the international organisations to fulfil their obligations and help their respective Member States meeting their own human rights engagements.

This argument is however likely to be contentious even among those countries keen to promote human rights. To introduce a public interest defence is to introduce an unprecedented level of transparency and accountability in the security industry. Governments which exploit vulnerabilities, legitimately or illegally, would have less latitude to threaten security researchers with prosecution to stop them reporting vulnerabilities. For these reasons, the introduction of a public interest defence for security researchers may be politically less savoury. It might explain why none of the written submissions to the UNODC Ad Hoc Committee tackled the protection of security researchers (even to reject it) despite an express question as to whether or not security researchers should be protected. It might also explain why the EU has not incorporated in NIS2 Directive an Article on the protection of security research against criminal law, leaving it to its Recital 60. The Council of Europe is also not immune to these tensions. It has repeatedly been criticised for giving too much power to governments and law enforcement authorities and not listening enough to civil society representatives, when drafting the Budapest Convention and its two additional protocols.[94] Furthermore, the sheer number of states having accepted the Budapest Convention (66 in 2022) renders amendments or additional protocols challenging to draft and adopt.

Consequently, it may be more realistic to push for the Council of Europe to adopt some detailed guidance notes on what 'without right' means in the context of vulnerability research, as it has done for example on the concept of 'computer system' or the situation of 'electoral interference'.[95] In the same spirit, the EU may find it easier to amend the NIS2 Directive, or the cybercrime Directive, to incorporate a legal 'safe harbour' provision for Member States to implement, without specifying its exact terms. Yet, it cannot be overstated that these reforms or guidance notes would not yield the full benefits that a specific public interest defence would bring to the work of security researchers. This is probably why ENISA, for the EU, and the OECD, for beyond Europe, have both reached the same conclusion: the need to amend the existing cybercrime instruments of respectively the EU and the Council of Europe, along with the recommendation to better regulate the role of governments in security research.

The context of these calls for legal reform is here important. The political dimension of vulnerability research, rather subdued in the early analyses of the vulnerability research ecosystem, has progressively gained prominence in recent works on national CVD policies.[96]

---

[94] Notably Cyber-Rights, *An advocacy Handbook for the Non Governmental Organisations*, 2003, at http://www.cyber-rights.org/cybercrime/ ; European Digital Rights (EDRi) submission to the Council of Europe's Second Protocol to the Convention on cybercrime, 20 February 2019 at https://edri.org/safeguarding-fundamental-rights-in-the-new-cybercrime-protocol/

[95] https://www.coe.int/en/web/cybercrime/guidance-notes

[96] Compare ENISA's 2015 report which has half a page (n 1, 54), its 2018 report, three pages (n 2, 39-41); its 2022 report tackles China which vulnerability evaluation process is in the sole hands of the intelligence

In the EU, the CEPS Task force argued that 'it is critical for governments to have robust, accountable and transparent policies in place [regarding the purchase and exploitation of vulnerabilities by government agencies] in order for companies and users to have trust and confidence that governments are responsibly managing any vulnerabilities that they learn about.'[97] It is not about forbidding governments to buy and/or use vulnerabilities for offensive ends or intelligence purposes. It is about creating a framework which brings back a certain degree of transparency and accountability. The two can co-exist: a public interest defence for security researchers and a soft-law approach to governments' role in searching and exploiting vulnerabilities. In 2021, the OECD made a similar assessment, calling for the regulation of how Governments find and exploit vulnerabilities for offensive ends, along with the creation of legal safeguards in national laws and the amendment of the Budapest Convention to 'add a safe harbour provision'.[98] These reflections have implications for the current discussions before the UNODC Ad Hoc Committee on a future UN Convention on cybercrime.

4.3. Implications for the future UN Convention on cybercrime

The UNODC Ad Hoc Committee has expressly asked Member States and other participants to reflect on whether security researchers should be protected from the impact of cybercrime offences.[99] The responses are underwhelming. National proposals have been entirely silent on the possibility of a public interest defence. Furthermore, their definitions of computer-dependent offences raise more questions than they resolve. They tend to adopt the same wording as that of Budapest Convention and/or the EU Directive, even when their own national laws do not align with the terms of these international legal instruments and increase the scope of the criminal law. For example, countries define the offences of damage and interference by reference to intention, with no mention of recklessness as an option, even when their current national law criminalises recklessness and no national reform is currently underway to restrict the offence's *mens rea* to intention. [100] The offence of misuse of tools copies the wording of Article 6 Convention, including the protection of Article 6(2) Convention, even when a country, such as the UK, has implemented none of the safeguards present in Article 6 Convention and has not headed a single call for reform.[101] This dissonance between the Member States' choice of overcriminalisation and their national proposals for the UN Convention, often aligned on the Budapest Convention and the Directive 2013/40/EU, raises questions as to whether the future UN Convention, should it be adopted, will yield a more harmonised legal landscape. The common draft agreed for negotiations in November 2022 contains no definitions of the key terms of 'access', 'attempted access', and 'authorisation', and side-steps the question on security research.

services; 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 08 July 2022)

[97] CEPS (n 8) 63

[98] OECD (n 2) 34-36

[99] Letter from the Chair (n 17)

[100] Australia, and the UK, in Ad Hoc Committee (n 6) 4-5, 58-59

[101] CLRNN (n 56) for the UK; for EU member states, Guinchard (n 9)

Consequently, the reasons underpinning my call for a public interest defence in the Budapest Convention and the EU Directive remain entirely valid for the purpose of drafting the future UN Convention. Whether the Ad Hoc Committee will explore this option is a different matter. The vulnerability research ecosystem does not have the same degree of readiness across its Member States; therefore, some countries may be less aware of the patterns of criminalisation affecting security research and how they impact on cybersecurity and the fight against cybercrime.

Furthermore, the political challenges mentioned earlier may prove a formidable obstacle to adopt a public interest defence, although the recent common draft gives a beacon of hope. The push for a safe harbour comes from civil society organisations and private companies. They were expressly integrated into the drafting process in order to bring a more balanced view on the fight against cybercrime, not solely reliant on state law enforcement's perspectives. [102] So far they seem to have been successful in bringing some of their concerns to the attention of the Ad Hoc Committee, whose common draft has just adopted a requirement for Member States to respect human rights in their implementation of the future Convention. [103] The momentum may not extend yet to integrating a safe harbour for security researchers, but inspiration could be taken from the security community when twenty years ago it raised the alarm about the Council of Europe's initial draft on the misuse of tools offence. Their detailed representations led to the adoption of a number of safeguards, including that of Article 6(2) Convention. Incorporating a public interest defence in the future UN Convention could benefit from submissions providing an outline of the public interest defence. This could be along the lines of the defence in the current UK Data Protection Act. There could be a clause on necessity, with a 'reasonable belief that the search was justified as being in the public interest' and a requirement of proportionality with no intentional damage committed and the disclosure of the vulnerability without undue delay.

Conclusion

After having demonstrated the vital contribution of independent security research to the fight against cybercrime and the protection of human rights, this chapter has outlined the patterns of criminalisation adopted by the respective Member States of the EU and the Council of Europe when they implemented the Directive 2013/40/EU and the Budapest Convention. Member States brought a certain minimum harmonisation but have also and often broadened the scope of their criminal law, creating some significant variations among national laws. The resulting fragmentation has fuelled uncertainties as to which conducts under cybercrime laws would be or not criminalised across Member States. While risks of prosecution are low for the unauthorised damage and interference offences, and, to a lesser extent, for the misuse of tools offence, they do increase substantially for unauthorised access. The concept of authorisation is particularly ill-suited for the criminal law to protect independent security researchers. Not only the security industry's reliance on vulnerability policies to decide authorisation may violate the principle of legality, but the technical discussions on authorisation cannot be reflected in the legal concept of authorisation understood as consent.

[102] Resolutions 74/247 and Resolution 75/282
[103] Article 5(1) draft, Ad Hoc Committee (n 6)

Consequently, this chapter has argued that a public interest defence would be far better suited to reflect the considerations of necessity and proportionality which underpin the controversy around 'authorisation'. So far, no Member States in the EU and signatories of the Budapest Convention seem to have considered and implemented such defence. The problems are not completely ignored. Data protection laws offer some protection, in some countries, to security researchers. Nevertheless, this protection remains limited and legislative reform at national level, even if it were to start, is likely to be fragmented. Hence, the proposal to amend the Budapest Convention and the EU Directive. It would provide a legal environment supportive of global security practices, well beyond the shores of Europe, since a number of countries in North America, Latin and Central America, Africa, Asia and Australasia, have signed the Budapest Convention. Such reform would also pave the way for the future UN Convention on cybercrime to integrate a public interest defence. Yet, challenges lie ahead. The Pegasus scandal demonstrated that cybersecurity is more than just a technical standard: it is an essential condition for human rights to thrive. A public interest defence would avoid cybercrime laws to be weaponised against those contributing to the fight against cybercrime and indirectly protecting human rights. It may not be politically very palatable as it will push for stronger clarification of the governments' role in the search and use of vulnerabilities for national security and/or law enforcement purposes. Yet, momentum towards reform is gaining strength. Calls for establishing policies for governments' role sit alongside those for legal reforms at national and international law. Let us hope that the future UN Convention on cybercrime will be successful in establishing a defence.