In defense of offense: information security research under the right to science

van Daalen, O.

DOI
10.1016/j.clsr.2022.105706
Publication date
2022
Document Version
Final published version
Published in
Computer Law and Security Review

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

In defense of offense: information security research under the right to science ☆

Ot van Daalen*

University of Amsterdam

ARTICLE INFO

Keywords:
Information security
Coordinated vulnerability disclosure
Right to science
Communications freedom
Duty to disclose
Vulnerabilities
Information security research

ABSTRACT

Information security is something you *do*, not something you *have*. It's a recurring process of finding weaknesses and fixing them, only for the next weakness to be discovered, and fixed, and so on. Yet, European Union rules in this field are not built around this cycle of making and breaking: doing offensive information security research is not always legal, and doubts about its legality can have a chilling effect. At the same time, the results of such research are sometimes not used to allow others to take defensive measures, but instead are used to attack. In this article, I review whether states have an obligation under the right to science and the right to communications freedom to develop governance which addresses these two issues. I first discuss the characteristics of this cycle of making and breaking. I then discuss the rules in the European Union with regard to this cycle. Then I discuss how the right to science and the right to communications freedom under the European Convention for Human Rights , the EU Charter of Fundamental Rights and the International Covenant on Economic, Social and Cultural Rights apply to this domain. I then conclude that states must recognise a right to research information security vulnerabilities, but that this right comes with a duty of researchers to disclose their findings in a way which strengthens information security.

1. Introduction

Information security is something you *do*, not something you *have*. It's a recurring process of finding weaknesses and fixing them, only for the next weakness to be discovered, and fixed, and so on. Yet, European Union rules in this field are not built around this cycle of making and breaking: doing offensive information security research is not always legal, and doubts about its legality can have a chilling effect. At the same time, the results of such research are sometimes not used to allow others to take defensive measures, but instead are used to attack. In this article, I review whether states have an obligation under the right to science and the right to communications freedom to develop governance which addresses these two issues. I first discuss the characteristics of this cycle of making and breaking. I then discuss the rules in the European Union with regard to this cycle. Then I discuss how the right to science and the right to communications freedom under the European Convention for Human Rights (the Convention), the EU Charter of Fundamental Rights (the Charter) and the International Covenant on Economic, Social and Cultural Rights (the Covenant) apply to this domain. I then conclude that states must recognise a right to research information se-

☆ This work was supported by the Netherlands Organisation for Scientific Research (NWO/OCW), as part of the Quantum Software Consortium programme (project number 024.003.037/3368). It is based on a forthcoming PhD on information security, encryption, quantum computing and human rights by the author. The author would like to thank his PhD supervisors, Joris van Hoboken and Mireille van Eechoud, for their comments on earlier drafts.

* Corresponding author: Mr Ot van Daalen, Institute for Information Law, Netherlands
E-mail address: o.l.vandaalen@uva.nl

https://doi.org/10.1016/j.clsr.2022.105706
0267-3649/

curity vulnerabilities, but that this right comes with a duty of researchers to disclose their findings in a way which strengthens information security.

2. Information security as a cycle of making and breaking

In the literature, information security is often framed in terms of desirable security properties, such as confidentiality, integrity and availability.[2] And information security measures are intended to safeguard these properties against attacks. Many organisations will, at some point in their development, take these kind of information security measures. But it can be difficult to determine which measures make the most sense. Over the past decades, standard practices have emerged to help organisations make the best choices, even in the face of changing circumstances. These are generally subsumed under the *plan-do-check-act* cycle.[3]

In the first phase of the cycle, the *plan*-phase, an organisation will decide which measures are necessary in view of the risks. These decisions are usually laid out in an information security policy. In the second phase, the *do*-phase, the organisation then implements these measures. That does not mean, of course, that these measures are always sufficient. That's why information security policies need to be tested and reviewed periodically – the *check* and *act* phases of the cycle. You periodically check whether the measures are commensurate with the risks, then adjust as needed. This approach reflects the reality of the continuous cycle of making and breaking.

An important part of this cycle centres around the "vulnerability" or weakness, in software or hardware. An attacker can exploit such a vulnerability to make a system act in a way which it is not supposed to do, or to be more precise: to violate a *security policy*. And while you might in theory be able to make software and hardware without vulnerabilities, in practice it's virtually impossible. It is not doable to independently verify all components of a system.[4] And even such verification only provides limited assurance that a component can actually be trusted.[5]

2.1. Research and discovery

As a result, many vulnerabilities are found in most widely used products after they are shipped, and even if they're shipped without vulnerabilities, the deployment by users might create new weaknesses. One particular type of vulnerability is called the "zero day vulnerability", or simply the "zero day". It's a weak spot for which no fix has been created yet, usually because the vendor doesn't know of its existence. Of all vulnerabilities, zero days are the most coveted by attackers, because by definition there is not yet a direct defence for them. And that's why zero days can also wreak the most havoc.

After inception, these vulnerabilities will often lie dormant, undiscovered for months, if not years. But researchers are continuously on the lookout for bugs, and they generally have the upper hand. They hunt by disassembling hardware, trawling through lines of code and remotely testing online services. This used to be done manually, and still often is. However, many tools and services have come available which enable automatic testing.[6] And since the information security of a system is as strong as its weakest link, attackers generally only need one vulnerability to gain access, whereas the defender needs to close every potential gap.

So, after the research has started, there usually comes the moment of discovery, and – in most cases – subsequent disclosure. When the vendor itself discovers a weakness in its own product, it might fix it before others become aware of it. But most vulnerabilities are in fact discovered by *others* than the vendor. In that case, several scenarios are possible.

2.2. Different forms of disclosure

Some researchers will not disclose the vulnerability to the outside world, but only disclose it to the *vendor*. There are, for example, many companies and researchers which offer security assessments as a consulting service. These researchers often also do research on their own initiative, not on the basis of an engagement, sometimes to collect bounties.[7]

Intelligence agencies also look for vulnerabilities. If such an organisation found a zero day, it may not disclose it to others but instead keep it to itself, to use it to attack. Likewise, some researchers only focus on the in-house development of zero days *without* disclosure to the vendor and the public, instead

[2] See Axel M. Arnbak, *Securing Private Communications: Protecting Private Communications Security in EU Law: Fundamental Rights, Functional Value Chains, and Market Incentives* (Kluwer Law International 2016) ch 5 for an in depth discussion of these concepts; and A. J. Menezes, Paul C. Van Oorschot and Scott A. Vanstone, *Handbook of Applied Cryptography* (CRC Press 1997) 4 for the definition of the first two.

[3] See for example Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016 OJ L 119/1), Art. 32(1)(d).

[4] Edlyn V. Levine, "The Die Is Cast: Hardware Security Is Not Assured" (2020) 18 ACMqueue.

[5] See Ken Thompson, "Reflections on Trusting Trust" (August) 1984 Communications of the ACM 761 for a principled argument; and Georg T. Becker and others, "Stealthy Dopant-Level Hardware Trojans: Extended Version" (2014) 4 Journal of Cryptographic Engineering 19 for a practical example.

[6] See on this Dr Sven Herpig, "Securing Artificial Intelligence: Part 1: The Attack Surface of Machine Learning and Its Implications" (Stiftung Neue Verantwortung 2019); Ben Buchanan and others, "Automating Cyber Attacks" (Center for Security and Emerging Technology (CSET) 2020); and Bruce Schneier, "The Coming AI Hackers" (Belfer Center for Science and International Affairs 2021) Essay for a discussion of artificial intelligence in information security.

[7] For example, Security Research Lab, which has done extensive work on the security of mobile phone communications, calls itself "a hacking research collective and think tank working on consultancy and in-house projects as well as tools at the cutting edge of security research"; Security Research Labs, "Security Research Labs" (*Corporate Website*); See for an early empirical study on bug bounties Matthew Finifter, Devdatta Akhawe and David Wagner, "An Empirical Study of Vulnerability Rewards Programs" 16.

opting to sell what they've found to interested parties.[8] This business of selling vulnerabilities is controversial, sometimes compared to the arms trade.[9] It is also a world about which we know very little. What we *do* know, is that this market is driven by some serious money – with six-figure prices being paid for some zero days.[10] The reason organisations pay these kinds of sums, will in many cases be because these will be used to attack systems.

This weaponisation is done by converting the vulnerability into a working 'exploit': executable code which allows for the circumvention of a security policy. For instance, the is known to stockpile vulnerabilities and has created an automated system for infecting targets – but other intelligence services likely do the same.[11] And not only governments and criminals do this: there are also companies which make money by weaponising vulnerabilities, and then selling services around them. For instance, mobile spyware suite Pegasus, developed by the Israel-based group, allows for the remote surveillance of mobile phones with zero days. It gained notoriety for being used by governments around the world to spy on opponents, including, as recently has been discovered, against European politicians.[12] This why the European Parliament started an investigation into the use of Pegasus and other spyware.[13]

2.3. *Coordinated vulnerability disclosure*

Not all vulnerability discoveries are used to attack, however – many researchers, from academia to corporates and individuals, instead aim for public disclosure, usually after giving the vendor time to fix the problem. These security researchers opting for public disclosure have to perform a tricky balancing act. They will want to push knowledge of the vulnerability out in the open quickly – if only because they want to make users aware of the existence of the vulnerability. While they are waiting for a patch, users can then decide to either not use the service or tool, or develop a patch themselves. This need for a speedy release becomes more pressing as knowledge of the vulnerability spreads, because the risk of exploitation by others then also increases.[14] If a vulnerability is being exploited in the wild, immediate release might even be called for.[15] And in some high-stakes cases, the longer security researchers have to sit on a vulnerability, the greater the risk that they might themselves become a target.[16] On the other hand, disclosing a vulnerability which is not fully fixed exposes users to serious security risks, because others might exploit it.

This is why *coordinated vulnerability disclosure* (CVD) procedures have been developed. CVD processes are the outcome of a fierce debate over the past decades on the best approach to disclosure. Some in this debate feared that waiting for the vendor to develop remediating measures before publicly disclosing a vulnerability would stall the process. They argued for full disclosure. Full disclosure means publishing all information on a vulnerability to everyone at the same time, usually before the vulnerability is fixed.[17] Others were highly critical of full disclosure, arguing that it creates "information anarchy" and only helps the attackers.[18] Disclosing vul-

[8] See Lillian Ablon and Andy Bogart, *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits* (RAND Corporation 2017); and for earlier reports Marilyn Fidler, "Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis" (2015) 11 I/S: A Journal of Law and Policy for the Information Society 405; Andy Greenberg, "Inside Endgame: A Second Act for the Blackwater of Hacking" (*Forbes*, March 3, 2014); Lillian Ablon, Martin C. Libicki and Andrea A. Golay, "Zero-Day Vulnerabilities in the Black and Gray Markets," *Markets for Cybercrime Tools and Stolen Data* (RAND Corporation 2014); Andy Greenberg, "Meet the Hackers Who Sell Spies the Tools to Crack Your PC (and Get Paid Six-Figure Fees)" *Forbes* (2012); Andy Greenberg, "Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits" *Forbes* (March 23, 2012); Thierry Zoller, "The Rise of Vulnerability Markets - History, Impacts, Mitigations" (OWASP Benelux, 2011); J. Radianti, E. Rich and J.J. Gonzalez, "Vulnerability Black Markets: Empirical Evidence and Scenario Simulation," *2009 42nd Hawaii International Conference on System Sciences* (2009); Charlie Miller, "The Legitimate Vulnerability Market" 10.

[9] Fidler; The Economist Staff, "The Digital Arms Trade" [2013] *The Economist*.

[10] Zerodium, formerly called Vupen, touts itself the world's leading zero-day acquisition platform, and offers to pay up to 2.5 million for weaknesses in systems. Zerodium, "About Us and Our Bug Bounties" (*Zerodium*); Zerodium, "How to Sell Your 0day Exploit to ZERODIUM" (*Zerodium*, September 3, 2019); Although it expected prices to drop mid-2020 because of surplus in iOS-exploits; Zerodium, "Tweet of 13 May 2020 on 2:05PM" (*Twitter*, May 13, 2020).

[11] See the description of the FOXACID system; Bruce Schneier, "Attacking Tor: How the NSA Targets Users' Online Anonymity" *The Guardian* (October 4, 2013); Bruce Schneier, "How the NSA Thinks About Secrecy and Risk" [2013] The Atlantic. In 2017, WikiLeaks released a trove of documents, allegedly from the CIA, which also contained exploits, including one zero day for Cisco routers, which Cisco investigated and then patched; Cisco, "The Wikileaks Vault 7 Leak – What We Know so Far" (*blogs@Cisco - Cisco Blogs*, March 7, 2017); Cisco, "Cisco IOS and IOS XE Software Cluster Management Protocol Remote Code Execution Vulnerability" (March 17, 2019).

[12] See John Scott-Railton and others, "CatalanGate: Extensive Mercenary Spyware Operation Against Catalans Using Pegasus and Candiru" (Citizen Lab 2022) on the hacking of politicians who are in favour of independence of Catalonia.

[13] European Parliament, "EP inquiry committee for Pegasus and other spyware launched" (*European Parliament website*, April 19, 2022).

[14] For example, researchers at the Vrije Universiteit reported that after not publishing their findings on CPU-weaknesses, they were getting reports that information on the vulnerabilities was being shared; Kim Zetter, "Intel Fixes a Security Flaw It Said Was Repaired 6 Months Ago" *The New York Times* (November 12, 2019).

[15] For example, Google Project Zero employed a seven day-deadline for disclosure of vulnerabilities which were being exploited in the wild; Maddie Stone, "Bad Binder: Android in-the-Wild Exploit" (*Project Zero*, November 21, 2019).

[16] There is one reported incident of a Belgian cryptography professor, Jean-Jacques Quisquater, being hacked, but is uncertain who was behind the hack; Lucien Constantin, "Prominent Cryptographers Targeted by Malware Attacks" (*PCWorld*, February 3, 2014); Mark Eeckhout and Nikolas Vanhecke, "Belgian professor in cryptography hacked (English Summary)" *De Standaard* (February 1, 2014); see more recently for a campaign targeting security researchers; Adam Weidemann, "New Campaign Targeting Security Researchers" (*Google*, January 25, 2021).

[17] See Bruce Schneier, "Full Disclosure of Security Vulnerabilities a 'Damned Good Idea'" (*Schneier on Security*, January 2007).

[18] See for example Scott Culp, "It's Time to End Information Anarchy" (*Microsoft Security Response Center*, October 2001).

nerabilities does indeed increase the frequency of attacks.[19] But on the other hand, it also incentivises vendors to release patches.[20] CVD is a middle-ground solution that gives vendors time to come up with a fix, after which the vulnerability will be disclosed.[21]

2.4. *The challenges of coordinated vulnerability disclosure*

Not all disclosure through CVD will proceed without a hitch. There are several examples of security researchers being sued for exposing vulnerabilities in their research.[22] Sometimes, researchers are denied the opportunity to present their work with other experts at conferences.[23] And there are examples of employers prohibiting their employees from presenting their findings at security conferences.[24]

But even when there is no court case, no conference blocking publication and no employer taking measures, the application of CVD procedures is not always straightforward. Firstly, the increasing interdependence of all parties in the supply chain makes it difficult to coordinate disclosure processes, let alone assign responsibility for making a patch available. When researchers at Radboud University found a vulnerability in the hardware encryption of Samsung, Crucial and Sandisk SSDs, it wasn't the harddrive vendors who made a patch. It was Microsoft. That's because Microsoft had been turning off software-based encryption automatically if it determined that an SSD already offered hardware-based encryption. So *Microsoft* could most easily provide a patch for what was essentially a hardware problem. And ultimately, they did.[25]

Moreover, some vulnerabilities cannot be fixed, are very hard to fix, or can be fixed only with a significant performance hit. This is particularly the case with hardware based-vulnerabilities, because it is more difficult to replace chips than programs.[26] Meanwhile, many cheap embedded devices have only limited support from their vendor: a Chinese producer of connected children's toys will not always bother with pushing updated firmware to its devices if a bug is found.[27]

Because it is sometimes difficult to develop a patch, and because some companies go into damage control mode when confronted with a vulnerability, the period that security researchers grant to vendors for fixing a vulnerability is still heavily contested. The desired policy is rather delicate, because in the phases between the discovery of a vulnerability and the deployment of remediation measures, the vulnerability remains exposed. The window of exposure opens

[19] Ashish Arora, Anand Nandkumar and Rahul Telang, "Does Information Security Attack Frequency Increase with Vulnerability Disclosure? An Empirical Analysis" (2007) 8 Information Systems Frontiers 350.

[20] Dmitri Nizovtsev and Marie Thursby, "To Disclose or Not? An Analysis of Software User Behavior" (2007) 19 Information Economics and Policy 43; Ashish Arora, Rahul Telang and Hao Xu, "Optimal Policy for Software Vulnerability Disclosure" (2008) 54 Manage. Sci. 642; Ashish Arora and others, "An Empirical Analysis of Software Vendors' Patch Release Behavior: Impact of Vulnerability Disclosure" (2010) 21 Information Systems Research 115. It might even spur further research into the security of a product; Arrah-Marie Jo, "Software Vulnerability Disclosure and Security Investment (Preliminary Draft Presented at WEIS 2019)" 33. See for other analyses; Jay Pil Choi, Chaim Fershtman and Neil Gandal, "Network Security: Vulnerabilities and Disclosure Policy" (2010) 58 The Journal of Industrial Economics 868; Sam Ransbotham and Sabyasachi Mitra, "The Impact of Immediate Disclosure on Attack Diffusion and Volume," *Economics of Information Security and Privacy III* (Springer New York 2013).

[21] There have been several initiatives to standardise coordinated vulnerability disclosure. See for example ENISA's guide; ENISA, "Good Practice Guide on Vulnerability Disclosure: From Challenges to Recommendations." (ENISA 2015); the standard; ISO, "ISO/IEC 27001:2013: Information Technology - Security Techniques - Information Security Management Systems - Requirements" (ISO/IEC 2013); and the Dutch 's revised guidelines; NCSC, "Coordinated Vulnerability Disclosure: The Guideline" (2018); see also the overview in Chapter 3 of Marietje Schaake and others, "Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges" (Centre for European Policy Studies 2018).

[22] See *NXP/RUN (Mifare-chip)* [2008] District Court of Arnhem ECLI:NL:RBARN:2008:BD7578; see also Flavio D. Garcia and Bart Jacobs, "The Fall of a Tiny Star" in Peter Y. A. Ryan, David Naccache and Jean-Jacques Quisquater (eds), *The New Codebreakers: Essays Dedicated to David Kahn on the Occasion of His 85th Birthday* (Springer Berlin Heidelberg 2016); in another high-profile case, Volkswagen was granted an injunction in a UK high court relating to the publication of research into keyless theft; *Volkswagen Aktiengesellschaft v Garcia & Ors* [2013] EWHC 1832 (Ch) HC13C02168; Lisa O'Carroll, "Scientist Banned from Revealing Codes Used to Start Luxury Cars" *The Guardian* (July 26, 2013); Roel Verdult, Flavio D. Garcia and Baris Ege, "Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer" Supplement to the Proceedings of the 22nd USENIX Security Symposium 1; after two years of negotiation, Volkswagen eventually agreed the paper could be published, albeit with one sentence struck out; Jamie Grierson, "Security Flaw Affecting More Than 100 Car Models Exposed by Scientists" *The Guardian* (August 18, 2015).

[23] In 2017, the US denied two researchers visas, although it is not clear, merely suggested in the reporting that it was because of their profession; Zack Whittaker, "Black Hat Speaker Denied Entry to US in Another Needless Hit to Security Research" (*ZDNet*, July 25, 2017).

[24] Mike Lynn, a former researcher at Internet Security Systems, was threatened by his former employer and Cisco, if he were to publish his findings on vulnerabilities in Cisco routers in 2005; Kim Zetter, "Whistle-Blower Faces FBI Probe" [2005] *Wired*. Security researcher Barnaby Jack was pressured by his employer, Juniper Networks, to delay his presentation on jackpotting ATMs by one year; Kim Zetter, "Researcher Demonstrates ATM 'Jackpotting' at Black Hat Conference" [2010] *Wired*; Henry Schwarz, "Black Hatted" (*Henry Schwarz's ATM & EFT-POS Security Blog*).

[25] Carlo Meijer and Bernard van Gastel, "Self-Encrypting Deception: Weaknesses in the Encryption of Solid State Drives," *2019 IEEE Symposium on Security and Privacy (SP)* (IEEE 2019).

[26] We have seen multiple attacks on Intel and AMD s, allowing for unauthorised reading of memory, which could only be remedied (partly) by software which slowed the processor down significantly, which then also were circumvented, and required additional mitigations; Paul Kocher and others, "Spectre Attacks: Exploiting Speculative Execution," *2019 IEEE Symposium on Security and Privacy (SP)* (IEEE 2019); Moritz Lipp and others, "Meltdown: Reading Kernel Memory from User Space" 18; Michael Larabel, "A Look at the CPU Security Mitigation Costs Three Years After Spectre/Meltdown" (*Phoronix website*, January 6, 2021); Xida Ren and others, "I See Dead μops: Leaking Secrets via Intel/AMD Micro-Op Caches" 14; University of Virginia School of Engineering and Applied Science, "Computer Scientists Discover New Vulnerability Affecting Computers Globally" (*ScienceDaily*, April 30, 2021).

[27] See for an analysis of manufacturers' firmware update provision; Elsa Rodríguez and others, "Superspreaders: Quantifying the Role of IoT Manufacturers in Device Infections" 18.

when a vulnerability is discovered, and grows as knowledge of the vulnerability spreads. Only when remediation measures are developed and applied, does the window start closing again.[28] From a security perspective, the idea is to keep the window of exposure as short as possible – by delaying disclosure while patching swiftly. The period granted for fixing a vulnerability depends in part on how likely it is that a vulnerability will be discovered independently. This is called the "collision rate" – the likelihood of two people finding the same vulnerability.[29] Where there is already evidence that a vulnerability is actively being exploited, this would favour speedy disclosure. But even when a company is confronted with attacks using its vulnerability in the wild, it may still hold off with bringing out a patch: Microsoft waited two years before patching a serious vulnerability in the program signature validation code of Windows.[30]

Still, even when a patch has been developed, users will have to apply the patch, something they often fail to do in time, or fail to do at all. Although most operating systems have automated systems for installing security updates, they too require an action on the part of the user. Many people do not install security updates as a result.[31] Large organisations will generally only install updates in regular update cycles, in order to first test the effects of an update and only then roll it out across the system. These cycles may take months, and the internal processes are not always in place to identify high priority security updates which require quicker fixes.[32] Smaller organisations may not have an update policy in place, and some organisations will avoid updating their systems because they fear it might break something. Furthermore, many embedded devices are coming online which are more difficult to patch.

This all means that while the risk that a zero day poses might be mitigated in theory when a vendor offers a patch, the vulnerability can still live on in systems that fail to apply the patch. This is sometimes called an N-day. And while zero day vulnerabilities might often be more newsworthy because of their novelty, these will eventually become N-days, and many of the breaches we read about can be attributed to these particular kinds of vulnerabilities.

2.5. *The effects of zero days*

Many of these breaches may seem harmless – clever digital tricks affecting an abstract, mathematical world. But that does not do justice to the severity of their consequences. These attacks affect people and organisations in real ways. Take data breaches, for instance.[33] Some breaches, such as the Yahoo-breach of 2013, involve data on *billions* of users, and many affect *millions*.[34] Meanwhile, for each record obtained, there is potential for misuse. This data can be used by criminals to steal an identity, open accounts or make fraudulent purchases.[35] This can lead to financial loss, emotional distress and lost time (to deal with the incident).[36] Exploits are also used by intelligence services to intercept communications and do other kinds of spying. The NSA for instance uses these technologies to inject exploits into rerouted communications, enabling them to take over the computer of a target.[37]

Some exploits are not used to gather data, but to gain control over a system. These can be industrial targets, such as critical infrastructure. The 2015 attack on the Ukranian power grid is an example.[38] Another high-profile example is Stuxnet, the malware used to disrupt uranium enrichment facilities in Natanz, Iran, which exploited four zero-day vulnerabilities in Microsoft Windows.[39] And many systems are in fact vulnerable: a 2019 study found that almost one thousand industrial control systems in the Netherlands have multiple, highly severe vulnerabilities, which could be fixed by taking measures

[28] Bruce Schneier, "Managed Security Monitoring: Closing the Window of Exposure" (Counterpane 2000).

[29] See on this Ablon and Bogart; Trey Herr, Bruce Schneier and Christopher Morris, "Taking Stock: Estimating Vulnerability Rediscovery" (Harvard Kennedy School/Belfer Center for Science and International Affairs 2017); Andy Ozment, "The Likelihood of Vulnerability Rediscovery and the Social Utility of Vulnerability Hunting," *Fourth Workshop on the Economics of Information Security (June 2–3 2005* (2005).

[30] Michael Krebs, "Microsoft Put Off Fixing Zero Day for 2 Years — Krebs on Security" (*Krebs on Security*, August 20, 2020).

[31] See for example Matthijs Koot, "Field Note on CVE-2019-11510: Pulse Connect Secure SSL-VPN in the Netherlands" (2020) 1 Digital Threats: Research and Practice 13, which describes the situation where a security-critical patch was not installed by large organisations, even months after a patch was made public.

[32] For example, a high-risk vulnerability in VPN software was already discovered and fixed in April 2019 by the vendor, but turned out to be exploited in August 2019, with hundreds of large organisations not having installed the patch; Matthijs Koot, "Kwetsbare Pulse Connect Secure SSL-VPNs in Nederlandse IP-adresruimte: bevindingen en gedachten" (*Matthijs R. Koot's notebook*, September 1, 2019); Huib Modderkolk, "Intern netwerk honderden bedrijven en ministerie lag maandenlang wagenwijd open" *De Volkskrant* (September 28, 2019).

[33] Many data breaches have occurred because the information systems were badly secured and a good number became accessible through the use of exploits: of the top ten data breaches between 2005 and 2018 in terms of quantity of leaked data, seven are a result of hacking; Hicham Hammouchi and others, "Digging Deeper into Data Breaches: An Exploratory Data Analysis of Hacking Breaches over Time" (2019) 151 Procedia Computer Science 1004, 1006.

[34] See Nicole Perlroth, "All 3 Billion Yahoo Accounts Were Affected by 2013 Attack" *The New York Times* (October 3, 2017); Hammouchi and others 1006. Data breaches are a recurring theme in the Internet Organised Crime Threat Assessment of Europol; see Europol, "Internet Organised Crime Threat Assessment (IOCTA) 2019" (Europol 2019) and earlier years.

[35] ENISA, "Preventing Identity Theft" (April 3, 2010).

[36] See for example Yuan Li and others, "Responding to Identity Theft: A Victimization Perspective" (2019) 121 Decision Support Systems 13.

[37] Bruce Schneier, "How the NSA Attacks Tor/Firefox Users with QUANTUM and FOXACID" (*Schneier on Security*, October 7, 2013).

[38] See Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid" [2016] *Wired*; see also Andy Greenberg, *Sandworm. A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (First edition, Doubleday 2019).

[39] Ryan Naraine, "Stuxnet Attackers Used 4 Windows Zero-Day Exploits" (*ZDNet*, September 14, 2010); Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (1st edn, Crown Publishers 2014).

that are relatively easy to deploy.[40] Attackers have also been able to (remotely) take over a car while it was being driven, steering the wheel, braking and shutting off the transmission.[41]

Finally, exploits can be used for targeted abuse and murder, often of political dissidents. In 2019, multiple zero-days were found on a website targeting the Uyghur community, just as stories on Uyghur muslim concentration camps run by the Chinese government were coming out.[42] A phone could become infected simply by visiting the website, and then the attackers – likely to be the Chinese government – would gain full access to all data on the phone, including messages, pictures and locations. Another example is the tale of Saudi-Arabian dissident and writer Jamal Khashoggi, who in 2018 was lured into the Saudi consulate in Istanbul, never to re-emerge. It was later discovered that he had been killed inside and dismembered with a bone saw. When Citizen Lab investigated the phone of Khashoggi's friend Omar Abdulaziz, a Saudi dissident living in Canada, they found it infected with NSO's Pegasus spyware.[43] The United Nations special rapporteur investigating his murder subsequently linked the infection of this phone to the interception of chat messages betweeen Abdulaziz and Khashoggi, and it is believed that the interception played a role in his murder.[44]

It would be a mistake, though, to conclude that exploits are always bad. At their core, information security technologies enable control over devices and information. In some cases, it may be in the public interest to circumvent this control. If the NSA had taken far-reaching security measures to ensure near-total control over its internal files, then Snowden would have never been able to exfiltrate the vast amounts of documents he did.[45] Another example comes from rules prohibiting the circumvention of certain copy-protection measures for copyrighted works. In the US, the Copyright Office decides each three years which activities are exempt from this circumvention prohibition for reasons of public interest.[46] Currently, these exceptions range from jailbreaking iPads and Alexa home devices, to software that reads text aloud for the blind, from the ability to modify and repair cars, to using third party feedstock for 3D printers. And many of these activities are made possible by actually using vulnerabilities to circumvent information security measures (something I discuss further below).

3. The governance of the information security cycle

In order to understand the human rights obligations of governments in the field of information security research, it is necessary to review what the rules currently are.[47] I discuss two sets of laws: intellectual property rules and cybercrime laws. This is not necessarily an exhaustive overview, but already serves to make my point – finding and disclosing vulnerabilities may sometimes currently be illegal, and there is at the same time no duty to disclose vulnerabilities you have found.

3.1. *Intellectual property protection rules*

Article 11 of the WIPO Copyright Treaty obliges contracting parties to provide adequate legal protection against the "circumvention of effective technological measures."[48] These rules have been transposed in the 2001 European Copyright Directive and implementing legislation.[49] Information security measures are almost always such "effective technological measures", because they restrict access to information or restrict the copying of information without authorisation.[50] The scope of these rules is broad, extending to fields far beyond

[40] J.M. Ceron and others, "Online Discoverability andVulnerabilities of ICS/SCADADevices in the Netherlands" (Universiteit Twente for the WODC 2019).

[41] Jordan Golson, "Jeep Hackers at It Again, This Time Taking Control of Steering and Braking Systems" (*The Verge*, August 2, 2016); Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway—with Me in It" [2015] *Wired*.

[42] Zack Whittaker, "Sources Say China Used iPhone Hacks to Target Uyghur Muslims" (*TechCrunch*, September 1, 2019); Nicole Perlroth, Kate Conger and Paul Mozur, "China Sharpens Hacking to Hound Its Minorities, Far and Wide" *The New York Times* (October 22, 2019); Austin Ramzy and Chris Buckley, "'Absolutely No Mercy': Leaked Files Expose How China Organized Mass Detentions of Muslims" *The New York Times* (November 16, 2019); see later Lorenzo Franceschi-Bicchierai, "Mysterious Bugs Were Used to Hack iPhones and Android Phones and No One Will Talk About It" (*Vice*, November 10, 2020) for similar zero-days. See for how malware has been used to spy on politicans; Stephanie Kirchgaessner, "WhatsApp Confirms Catalan Politician's Phone Was Target of 2019 Attack" (*The Guardian*, July 28, 2020); Stephanie Kirchgaessner, "Israeli Spyware Used to Target Moroccan Journalist, Amnesty Claims" (*The Guardian*, June 21, 2020).

[43] Bill Marczak and others, "The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil" (The Citizen Lab 2018).

[44] Special Rapporteur on extrajudicial, summary or arbitrary executions, "Annex to the Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions: Investigation into the Unlawful Death of Mr. Jamal Khashoggi" (2019) A/HRC/41/CRP.1 ch I.I; David D. Kirkpatrick, "Israeli Software Helped Saudis Spy on Khashoggi, Lawsuit Says" *New York Times* (December 2, 2018); and Nina dos Santos and Michael Kaplan, "Jamal Khashoggi's Private WhatsApp Messages May Offer New Clues to Killing" (*CNN*, December 4, 2018).

[45] See Edward Snowden, *Permanent Record* (Henry Holt and Company 2019), in particular ch. 20 on Heartbeat.

[46] Exemptions under 17 U.S.C. 702 (CFR).

[47] See for a similar mapping exercise Gloria González Fuster and Lina Jasmontaite, "Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights" in Markus Christen, Bert Gordijn and Michele Loi (eds), *The Ethics of Cybersecurity* (Springer International Publishing 2020); Schaake and others; OECD, "Encouraging Vulnerability Treatment" (OECD 2021) 307, par. 3.3; see also "Challenges to Effective EU Cybersecurity Policy" (European Court of Auditors 2019) Briefing Paper.

[48] WIPO Copyright Treaty 1996. See also Art. 18 WIPO Performances and Phonograms Treaty 1996.

[49] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society 2001 (2001 OJ L 167/10), Art. 6(1); Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC 2019 (2019 OJ L 139/92), rec. 7.

[50] See *Nintendo/PC Box* [2014] CJEU Case C-355/12, par. 27.

movies and songs, such as the verification of printer cartridges and keycard systems for locks. Furthermore, not only do the rules apply to virtually every kind of information with some security measure around it. The rules also apply to all circumvention, regardless of why you're doing it.

This is why some room for exceptions has been built into these laws. The EU prohibits all circumvention, but at the same time obliges member states to take measures to ensure that rightholders under certain circumstances make available to users the means of benefiting from copyright exceptions.[51] It is furthermore clarified in recitals that these provisions "should respect proportionality and should not prohibit those devices or activities which have a commercially significant purpose or use other than to circumvent the technical protection", and in particular, "should not hinder research into cryptography."[52] These measures, however, do not adequately address the problem that circumvention in the public interest is prohibited in the EU. A recital does not have the same binding force as actual provisions. And more importantly, information security research is not necessarily commercial in nature, while technological measures are not always cryptographic.

In addition, member states must under the Copyright Directive also provide legal protection against the production, distribution or possession for commercial purposes of certain circumvention "devices, products or components."[53] Whether these tools are prohibited, depends on whether they are *promoted* as circumvention tools, have only a limited commercially significant *purpose* other than circumvention or are primarily *designed* to circumvent. Vulnerabilities, exploits and tools used for information security research could in theory fall within the scope of this provision, because they allow for the circumvention of security measures. Some vulnerability research will be done for commercial gain, for example in order to attract attention with the research. And many security research tools and exploits will be designed to circumvent; that is their main function. The fact that this circumvention also takes place for legitimate purposes, such as interoperability, legitimate copyright use, or installing other apps, does not matter for its legality. There have been numerous cases where this provision has been used to restrict the sale of devices which remove copy protection measures.[54] Given how broadly these provisions have been interpreted in the past, this could mean that for example an exploit which allows for the jailbreaking of a phone is considered a product or service intended to circumvent an "effective technological measure".

3.2. *Cybercrime rules*

The copyright rules discussed above are enforced primarily through civil law. But when a researcher does not own the system or have permission to study it, they may also face criminal liability under cybercrime rules – through the regulation of unauthorised access and of unauthorised interception.

3.2.1. *Regulation of unauthorised access*

Firstly, member states are under the Cybercrime Directive obliged to criminalise the intentional access to an information system (basically everything with a), by infringing a security measure without the right to do so.[55] *Mere access* falls within the scope of this provision. It doesn't matter what will be done after having gained access, despite the fact that the drafters of the Cybercrime Convention were aware that access could be harmless or even beneficial, leading to "the detection of loopholes and weaknesses of the security of systems."[56] As a result, the scope of this provision is broad, potentially including many activities carried out in the public interest, including information security research.[57] The term "without right" is defined as conduct "which is not authorised by the owner or by another right holder of the system or of part of it, or not permitted under national law."[58] Most of the information security research performed at the initiative of a third party will be done without authorisation. The third condition is that a "security measure" must be circumvented. It is likely that the bar for effectiveness of such a measure is not high, because if the security measures were really effective, then it would not be necessary to prohibit their circumvention (because they couldn't be circumvented).

Meanwhile, there is no clear carve-out for the public interest, let alone for security researchers. The recitals mysteriously consider that the directive is "without prejudice to the right of access to information as laid down in national and Union law, while at the same time it may not serve as a justification for unlawful or arbitrary access to information" – a hollow phrase, as it does not clarify how to strike the balance between the two.[59] It is further clarified in the recitals that there is no criminal intent, and thus no criminal liability, "in the case of mandated testing or protection of information systems, such as where a person is assigned by a company or vendor to test the strength of its security system", the operative word being "mandated" (e.g. consultancy security research).[60] This leaves out information security research performed by outsiders. It is furthermore observed that the "identification and reporting of threats and risks posed by cyber attacks and the related vulnerability of information systems is a pertinent element of effective prevention of, and response to, cyber attacks and to improving the security of information systems",

[51] Copyright Directive, Art. 6(4).
[52] See rec. 48 of the ibid.
[53] Ibid, Art. 6.
[54] See for example *Nintendo/PC Box; Nintendo modchips* [2010] District Court of The Hague ECLI:NL:RBSGR:2010:BN1963; *Kabushiki Kaisha Sony Computer Entertainment Inc v Ball (Application for Summary Judgment)* (2004) [2004] EWHC 1738 (Ch); *Nintendo Co Ltd v Playables Ltd* [2010] High Court of Justice HC09C00988, [2010] EWHC 1932; *TubeBox* [2012] Landgericht München 7 O 10502/12.
[55] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA 2013 (OJ) 7, Art. 2(a) and 3.
[56] See Council of Europe, "Explanatory Report to the Convention on Cybercrime" (Council of Europe 2001), par. 44.
[57] See for a discussion Pedro Miguel F. Freitas and Nuno Gonçalves, "Illegal Access to Information Systems and the Directive 2013/40/EU" (2015) 29 International Review of Law, Computers & Technology 50.
[58] Cybercrime Directive, art. 2(d).
[59] Ibid, rec. 17.
[60] Ibid, rec. 17.

suggesting that "Member States should endeavour to provide possibilities for the legal detection and reporting of security gaps."[61] But these suggestions are not further operationalised in the directive.

3.2.2. *Regulation of unauthorised interception*

Not only does the Cybercrime Directive regulate unauthorised access. It also criminalises the intentional and unauthorised interception of "non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions from an information system carrying such computer data."[62] This basically encompasses all information flowing through and between computers.

Three types of information security research are implicated in this provision. Firstly, the testing of communication protocols could run afoul of these laws: if one is to test the security of mobile communications, this will necessarily involve the interception (and perhaps even a *man-in-the-middle attack*) of communications traffic between a cell phone and a cell tower. Even if the researcher has gained authorisation from the owner of the cell phone, this does not necessarily imply that it also has gained authorisation from the telecommunications company operating the tower. A second, more common example concerns the interception of traffic between a client and a server in order to better understand the traffic itself, not the protocol. This applies where a researcher wants to, for example, understand telemetry data sent by an operating system, which is transmitted encrypted to a server. In order to understand the data, one will have to intercept (and decrypt) the stream going to the server. A third kind of research involves examining offline systems, for example to extract keys from security components. This is sometimes done by intercepting the communications with other parts of a computer, for example through what are called *side-channel attacks*. In side-channel attacks, a researcher attempts to gain information on the working of one channel through a related channel, such as power consumption. Since the directive also specifies the interception of "electromagnetic emissions", side-channel attacks may in some cases also fall within the scope of this provision.

Here again, an important qualification is that, in order to fall within the scope of this provision, the interception must be done "without right" – e.g. without consent from the owner or right holder of (part of) the system. As we've seen above, this qualification still leaves room for snaring computer security research in its ambit.[63]

3.2.3. *Dealing with knowledge of vulnerabilities*

When a vulnerability has been found, the next question is how organisations are required to handle this knowledge. Broadly speaking, one can distinguish between two kinds of required responses: fixing the security issue and notifying stakeholders. What is absent, however, is a a general duty on the part of information security researchers to disclose their findings.

The predominant response that may be required is patching the vulnerability. For instance, under the GDPR, this follows from the requirements to "ensure" the "ongoing" security, and to implement a procedure for testing, evaluating and assessing the security of systems.[64] This is even more pronounced in the NIS directive, where there is an explicit requirement to take measures to "prevent and minimise the impact of incidents affecting the security of their network and information systems", with a view to ensuring the continuity of services.[65] Under the NIS2 proposal, where a measure is not in compliance, the responsible organisation shall take all necessary measures to remedy this situation.[66]

The second response is notification. Under the GDPR, controllers are obliged to document all data breaches (as defined in the GDPR), report most data breaches to the applicable data protection authorities and inform data subjects in the case of high-risk data breaches.[67] Under the NIS directive, operators of essential services are required to report, without undue delay, incidents having a significant impact on the continuity of the essential services they provide to the competent authority.[68] Under the NIS2 proposal, regulated entities will without undue delay notify the competent authority of incidents and threats, and shall in certain circumstances, also notify the recipients of the services.[69] In the Cybersecurity Act, ENISA is accorded the task of strengthening capacity building in coordinated vulnerability disclosure, but this is voluntary.[70] There is no obligation to notify when you have *found* a vulnerability in the systems of someone else.

Here, the NIS2 proposal opens up a promising new avenue of policymaking, as it would strengthen the obligations of member states to devise policies on information security. Most importantly, the European Commission has proposed to oblige member states to adopt a policy to promote and facilitate coordinated vulnerability disclosure.[71] This CVD process would be supported by an organisation designated to coordinate the disclosure process in each member state, and

[61] Ibid, rec. 12.
[62] Ibid, Art. 6.
[63] Council of Europe, "Explanatory Report to the Convention on Cybercrime," par. 58.
[64] GDPR, Art. 32(1)(b) and (d).
[65] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union 2016 (2016 OJ L 194/1), Artt. 14 and 16.
[66] Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity across the Union, repealing Directive (EU) 2016/1148 2020, Art. 20; at the time of writing a compromise has been accepted in trilogue, but the final text has not yet been published.
[67] GDPR, Artt. 32 and 33.
[68] NIS I Directive, Art. 14(3) and (4).
[69] Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity across the Union, repealing Directive (EU) 2016/1148 NIS II Directive Proposal, Art. 20.
[70] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act) 2019 (2019 OJ L 151/15), Art. 6(1)(b).
[71] Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity across the Union, repealing Directive (EU) 2016/1148 NIS II Directive Proposal, Artt. 5(1) and 5(2).

would also provide for co-operation between each national organisation.[72] Furthermore, ENISA shall develop and maintain a vulnerability registry. At the same time, it is unfortunate that member states are given a lot of leeway to devise their own approach in this respect. Given the significance of these policies, one can question whether the European legislator should not take the design of these policies more into its own hands.

Finally, there is one framework under which it may be obligatory to *share* vulnerabilities: *vulnerabilities equities processes*, or VEPs. These rules are intended to determine under what circumstances governments must use knowledge of weaknesses in the IT-infrastructure to strengthen it, instead of exploiting it. In the EU, discussions on these VEPs are gaining steam. A 2018-report recommended that all member states implement policies and practices on how to deal with knowledge of vulnerabilities, to be codified in law, with a default policy to disclose.[73] In another report, a detailed set of best practices for VEPs was described.[74] In the same year, GCHQ published a blog on its VEP, noting that the "default position is to disclose the problem and there has to be a very good reason not to - either an overriding intelligence case or the fact that disclosing could reduce the security of people who use the product."[75] In the Netherlands at the time of writing, legislation for a VEP has been proposed which would contain a "bias towards disclosure", but which allows for temporary secrecy under certain circumstances.[76] Similarly, while it has been reported that Germany is also working on a formal policy, it appears to not have adopted one yet.[77]

So, in short, current EU governance with regard to information security research does not provide a general carve out for doing information security research in the public interest. At the same time, it also does not provide a duty to disclose vulnerabilities you may have found while doing information security research. The question is whether both a security research exception and a duty to disclose can be construed on the basis of the human rights to science and communications freedom. I discuss this below.

4. The right to science: supporting science as an iterative process

With regard to the right to science, I base my analysis on two instruments: the Covenant and the Charter. Article 15 of the Covenant reads:[78]

1 The States Parties to the present Covenant recognize the right of everyone:
   a To enjoy the benefits of scientific progress and its applications;
   b To benefit from the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author.
2 The steps to be taken by the States Parties to the present Covenant to achieve the full realization of this right shall include those necessary for the conservation, the development and the diffusion of science and culture.
3 The States Parties to the present Covenant undertake to respect the freedom indispensable for scientific research and creative activity.
4 The States Parties to the present Covenant recognize the benefits to be derived from the encouragement and development of international contacts and co-operation in the scientific and cultural fields."

The right has subsequently been protected under the European Charter of Fundamental Rights in Article 13, which provides that the "arts and scientific research shall be free of constraint. Academic freedom shall be respected". The emphasis on academic freedom in the Charter is also discussed below.

4.1. *Interpretation of the right to science under the Covenant*

Under the Covenant, the right to science is generally considered to have three components.[79] The first is the *freedom of science* – this is about the activity of science, being able to choose your own lines of inquiry. This is relevant for information security researchers – allowing them to also do *offensive* security research and share the results. The second is the right to enjoy the *benefits of science* – this is about sharing the positive results of science, and it aligns well with the iterative nature of the information security cycle, arguably implying a duty to disclose your findings under certain circumstances. And the third is the obligation to *protect against the risks of science* – this is about the negative effects of science. For the information security cycle, this implies that scientists must minimise the impact of disclosure of vulnerabilities. These themes can be found in four guiding documents which have been drafted over the years.

The first report is the Venice Statement, drawn up by human rights experts between June 2007 and July 2009.[80] The Venice Statement laid a foundation which has subsequently

[72] Ibid, Art. 6(1).
[73] Schaake and others 74.
[74] Sven Herpig, "Governmental Vulnerability Assessment and Management" (Stiftung Neue Verantwortung 2018).
[75] Ian Levy, "Equities Process" (*GCHQ*, November 29, 2018).
[76] Kees Verhoeven, Voorstel van wet van het lid Verhoeven houdende een regeling voor een afwegingsproces voor het gebruik van kwetsbaarheden in geautomatiseerde werken door de overheid (Wet Zerodays Afwegingsproces) 2018 [35257] 4.
[77] Sven Herpig and Ari Schwartz, "The Future of Vulnerabilities Equities Processes Around the World" (*Lawfare*, January 4, 2019); see *IT-Sicherheitslücken* [2021] 1 BvR 2771/18 (BVerfG) for a German constitutional case on a VEP of the *Land* Baden-Württemberg.
[78] International Covenant on Economic, Social and Cultural Rights 1976.
[79] Klaus D. Beiter, "Where Have All the Scientific and Academic Freedoms Gone? And What Is 'Adequate for Science'? The Right to Enjoy the Benefits of Scientific Progress and Its Applications" (2019) 52 Israel Law Review 233, par. 2.
[80] UNESCO, "The Right to Enjoy the Benefits of Scientific Progress and Its Applications" (Experts' meeting 2009); see Amrei Müller, "Remarks on the Venice Statement on the Right to Enjoy the Benefits of Scientific Progress and Its Applications (Article 15(1)(b) ICESCR)" (2010) 10 Human Rights Law Review 765 for a discussion of the Venice Statement; see also "Report of the Experts' Meeting on the Right to Enjoy the Benefits of Scientific Progress and Its Applications" (UNESCO 2007) for one of the reports leading up to the ultimate statement.

been worked out in the other guiding documents. Under the statement, states firstly have an obligation to respect scientific freedom: the obligation "to respect the freedoms indispensable for scientific research and creative activity, such as freedom of thought, to hold opinions without interference, and to seek, receive, and impart information and ideas of all kinds". Secondly, this freedom is not unfettered: states should at the same time take "appropriate measures to prevent the use of science and technology in a manner that could limit or interfere with the enjoyment of the human rights and fundamental freedoms."[81] And lastly, the experts emphasise the importance of knowledge sharing and diffusion, while respecting human rights: states have an obligation to "adopt a legal and policy framework and to establish institutions to promote the development and diffusion of science and technology in a manner consistent with fundamental human rights" and "to promote access to the benefits of science and its applications on a non-discriminatory basis."[82]

Special Rapporteur Farida Shaheed then developed this foundation further in her 2012-report on the right to science.[83] She identified a strong connection between the right to science and the right to freedom of expression, self-determination and the right to participate in public affairs, noting that it imposes on states an obligation to allow people to reconsider, create, and contribute to "knowledge that is testable and refutable, including revisiting and refuting existing theorems and understandings."[84] She agreed with the Venice Commission that scientific freedom includes the right to freedom of inquiry, and underlines the importance of the freedom of sharing. And the rapporteur suggested where scientific progress should ultimately lead: the concept of "access to the benefits of science" points to "the idea of a positive impact on the well-being of people and the realization of their human rights."[85] Conversely, states should protect from harm arising from the misuse of science.[86]

In 2017, UNESCO then adopted the Recommendation on Science and Scientific Researchers, setting out a detailed agenda for the right to science.[87] At the heart of the guidance lies the conceptualisation of science as a dynamic, iterative process – both the freedom of inquiry and the freedom to share results are a theme central to the report.[88] It is recommended that researchers "work in a spirit of intellectual freedom to pursue, expound and defend the scientific truth as they see it, an intellectual freedom which should include protection from undue influences on their independent judgement."[89] Member states should encourage and facilitate publication of results, data, methods and software, as well as access to knowledge.[90] Restrictions on publications must be strictly minimised and surrounded by appropriate safeguards.[91] Finally, the recommendations acknowledge the importance of scientific, social and ecological responsibility in science. This responsibility is informed by the promotion of themes such as peace, sustainable development, human welfare, dignity and human rights.[92]

Lastly, in 2020, the Committee on Economic, Social and Cultural Rights (CESCR) adopted a General Comment on Science and Economic, Social and Cultural rights.[93] The CESCR has the authority to interpret the Covenant, and its guidance thus carries significant weight. The General Comment devotes significantly less attention to the scientific process than the preceding documents, focusing more on issues such as gender-based and disability-based discrimination in science, perhaps because the earlier documents already described this process in detail. It does, however, emphasise the importance of freedom of research, noting that science is dependent on its "robust protection", and considering that this freedom includes the freedom to determine the direction and method of research and to share the results wherever possible.[94] Like the earlier documents, the CESCR considers that the development of science in the service of peace and human rights should be "prioritized" over other uses.[95] In particular, limitations on the applications of science "can be used to guarantee the safety and quality of products used by persons", for example through human rights impact assessments and limitations on the research process.[96] But, the report continues, "any limitation on the content of scientific research implies a strict burden of justification by States, in order to avoid infringing freedom of research".

---

[81] UNESCO, "The Right to Enjoy the Benefits of Scientific Progress and Its Applications," par. 14(a) and (d).

[82] Ibid, art. 16(a) and (b).

[83] Farida Shaheed, "The Right to Enjoy the Benefits of Scientific Progress and Its Applications" (United Nations General Assembly 2012) A /HRC/20/26.

[84] Ibid, par. 18 and 21.

[85] Ibid, par. 24.

[86] Ibid, recommendation (m).

[87] UNESCO, "Recommendation on Science and Scientific Researchers" (UNESCO 2017).

[88] It is defined as "the enterprise whereby humankind, acting individually or in small or large groups, makes an organized attempt, by means of the objective study of observed phenomena and its validation through sharing of findings and data and through peer review, to discover and master the chain of causalities, relations or interactions; brings together in a coordinated form subsystems of knowledge by means of systematic reflection and conceptualization; and thereby furnishes itself with the opportunity of using, to its own advantage, understanding of the processes and phenomena occurring in nature and society"; ibid, par. I(1)(a). The terms "research and development" are defined as "scientific research and experimental development for which"scientific research" signifies those processes of study, experiment, conceptualization, theory-testing and validation involved in the generation of scientific knowledge (…) and thus including both fundamental and applied research".

[89] Ibid, par. 16.

[90] Ibid, par. 35 and 36.

[91] Ibid, par. 38.

[92] ibid, par. 18, 20.

[93] CESCR, "General Comment No. 25 (2020) on Science and Economic, Social and Cultural Rights (Article 15 (1) (B), (2), (3) and (4) of the International Covenant on Economic, Social and Cultural Rights)" (United Nations 2020) E /C.12/GC/25.

[94] Ibid, par. 13.

[95] ibid, par. 6.

[96] Ibid, par. 22.

4.2. *Interpretation of the right to science under the Charter*

The extensive guidance on Article 15 Covenant is in contrast to the cursory explanation given on its equivalent in the Charter, Article 13. It is merely noted in the explanatory memorandum that this right is deduced primarily from the right to freedom of thought and expression, to be exercised having regard to Article 1 (on human dignity) and subject to the limitations under Article 10 of the Convention.[97] I add to this, that Article 13 should of course be understood in light of the guidance on this right in the context of the Covenant.

There is, however, one difference between the two provisions: Article 13 not only protects "scientific research", but also explicitly protects "academic freedom". The relation between the right to science and academic freedom is unclear: both academic freedom and the right to science protect institutional and individual elements of the scientific endeavour.[98] The most relevant question for this article is whether research performed by academics is accorded *extra* protection, compared to research performed by others. According to Beiter, this is the case: academic freedom is a special, "enhanced" kind of scientific freedom, only applicable to academics.[99] The reasoning is that academics have the particular role of performing research in the public interest, but because of this role, they also require extra protection.[100] This is not convincing, if only because non-academic researchers *also* perform research in the public interest. In fact, a significant amount of information security research takes place outside of academia. This is why I conclude that the concept of academic freedom merely *emphasises* the role of the right to science in the context of academia, but does not accord it extra protection. Thus, the relevance for the information security cycle of this particular element of Article 13 is limited.

5. The right to communications freedom: mitigating the negative impact of scientific research

Not only the right to science is relevant to information security research: it is complemented by the right to communications freedom as protected by Article 10 of the Convention and Article 11 of the Charter. Strictly speaking, there is no right to communications freedom: under Article 10 of the Convention and Article 11 of the Charter everyone has the right to "freedom of expression". "Expressing" is something most people do in public, so the term "freedom of expression" on the surface might suggest that it only refers to the public dimension of communication. But people also communicate less freely in private if they are under surveillance. Furthermore, the term "expression" refers to the sending phase of communications, whereas the right protected under the Convention and the Charter also includes the phase of receiving information. I therefore instead use the term "communications freedom", to emphasise not only the public dimension of communication, but also its private aspects, and to underline its importance throughout all phases of communication. And as we will see, many information security research practices fall squarely within the protection provided by those provisions.

5.1. *The qualification of interferences with regard to information security research*

Article 10 protects "information and ideas". In practice, a broad range of types of information is protected. This can vary from trivial information, to information which is only in the public interest, to information which is merely damaging.[101] One topic not yet handled by the Court, is whether information which is both expressive and functional is also protected. This is relevant because an executable exploit contains information (it is expressive) and does things as well (it is functional). Given the sweeping considerations of the Court in its case law on the scope of this right, however, the fact that information not only conveys knowledge, but also *does* something, should not exclude it from protection.

Furthermore, the form through which you express yourself also does not matter. The Court has considered that it follows from Article 10 that everyone is free to choose the form for expressing information and ideas which they consider the most effective to reach the most persons.[102] This can range from text to pictures, from speech to symbols, from literary heritage to the right not to speak.[103] The Court even considers that protesting by physically impeding activities of which

[97] Explanations Relating to the Charter of Fundamental Rights 2007.

[98] See on the difficulties of articulating the concept of academic freedom; E. M. Barendt, *Academic Freedom and the Law: A Comparative Study* (Hart Pub 2010) ch 2; see further on this topic Beiter; Klaus D Beiter, Terence Karran and Kwadwo Appiagyei-Atua, "'Measuring' the Erosion of Academic Freedom as an International Human Right: A Report on the Legal Protection of Academic Freedom in Europe" (2016) 49 Vanderbilt Journal of Transnational Law 597; Klaus D Beiter, Terence Karran and Kwadwo Appiagyei-Atua, "Yearning to Belong: Finding a 'Home' for the Right to Academic Freedom in the U.N. Human Rights Covenants" 11 Intercultural Human Rights Law Review 107; Klaus D. Beiter, Terence Karran and Kwadwo Appiagyei-Atua, "Academic Freedom and Its Protection in the Law of European States" (2016) 3 European Journal of Comparative Law and Governance 254; Robert Quinn and Jesse Levine, "Intellectual-HRDs and Claims for Academic Freedom Under Human Rights Law" (2014) 18 The International Journal of Human Rights 898; J.R. Groen, "Academische Vrijheid En Wetenschappelijke Integriteit: Een Onderzoek Naar Vrijheid En Verantwoordelijkheid in Wetenschappelijk Onderwijs En Onderzoek" (NVOR 2015) Preadvies 9–10. The Court on Article 13 has underlined that academic freedom also incorporates an "institutional and organisational dimension"; *European Commission v Hungary* [2020] CJEU Case C-66/18, par. 227.

[99] Beiter 237.

[100] See also Beiter, Karran and Appiagyei-Atua, "Yearning to Belong" 173.

[101] CLSR105710.

[102] *Women on Waves and others v Portugal* [2009] ECHR Application no. 31276/05, par. 38.

[103] See Dominika Bychawska-Siniarska, *Protecting the Right to Freedom of Expression Under the European Convention on Human Rights: A Handbook for Legal Practitioners* (Council of Europe 2017) 17–18.

the applicants disapproved, constitutes expressions of opinion within the meaning of Article 10.[104]

This is also relevant to information security. The practice of publishing information security vulnerabilities is highly diverse. Some vulnerabilities are published in academic papers which have gone through peer review. Other vulnerabilities have been published in online fora, or on mailinglists. Sometimes the authors merely state that there is a vulnerability, without alluding to the details. In other disclosures, the authors provide actual exploits to demonstrate their findings (which can of course be easily used for malicious purposes). Given the broad protection afforded by these instruments, all these practices arguably fall within the scope of this provision.

The second question is to what extent restrictions on the information security cycle should be considered an interference. Under Article 10, "formalities, conditions, restrictions or penalties" are mentioned as examples of an interference. Thus, criminal convictions, orders to pay damage and publication prohibitions should, in principle, all be assessed under Article 10.[105] Furthermore, where there is a *potential* of a chilling effect on communications freedom, for example because an order is not yet enforced, this will often be considered an interference as well.[106]

This is relevant to information security as well. As noted above, there are a number of restrictions on information security research. Only a few are outright prohibitions under criminal law – many are restrictions under civil law, such as copyright law, and some are imposed via contractual obligations (that is: service providers, or product manufacturers prohibit research in the contracts they conclude with their customers). And most of these provisions have a chilling effect – it may lead to experts not doing the research at all, or not publishing parts of the research out of fear of repercussions. As a result, many of these restrictions should be considered an interference under Article 10.

Finally, not only is the act of publication covered by Article 10: the Court considers the research and disclosure stage to be highly intertwined. As discussed, Article 10 protects all phases of the communications cycle: "receiving" as well as "imparting" information. The Courts have interpreted this to mean that the preparatory stages of communication also fall within the scope of this provision. The Court has for example considered that in circumstances where access to government information is instrumental for the exercise of an applicant's right to receive and impart information, its denial may constitute an interference with that right.[107] Research activities in preparation of a publication, such as doing an investigation, are also covered by the right to communications freedom.[108] The Court has lastly repeatedly underscored that academic freedom, both in the research and publication phase, is protected under Article 10 of the Convention.[109] This, of course, is also relevant to information security – most publications of vulnerabilities are the result of actual research. These activities fall within the scope of the rights to communications freedom as well.

5.2. *Proportionality of restrictions on the information security cycle*

Having established that many information security research restrictions constitute an interference, the next question is whether these are proportionate, or, in the words of Article 10, whether an interference is "necessary in a democratic society."[110] This necessity must, according to the Court, be a "pressing social need" and, where the press is concerned, the most careful scrutiny is applied, which means that the margin of appreciation is restricted.[111] In its case law, the Court affirmed in strong language the central role of freedom of expression in the human rights framework: it constitutes one of the essential foundations of a democratic society and one of the basic conditions for its progress and for each individual's self-fulfilment.[112] The Court speaks of restrictions which could "only have been justified by imperative necessities since exceptions to the freedom of expression must be interpreted narrowly", and in another case notes that "supervision must be strict because of the importance – frequently stressed by the Court – of the rights in question", which means that the necessity for any restriction must be convincingly established.[113]

[104] *Steel and others v the United Kingdom* [1998] ECHR 67/1997/851/1058, par. 92.

[105] See ECHR, *Guide on Article 10 of the European Convention on Human Rights* (Council of Europe 2020), par. 50; for example *Lindon, Otchakovsky-Laurens and July v France* [2007] ECHR Applications nos. 21279/02 and 36448/02; *Tolstoy Miloslavsky v the United Kingdom* [1995] ECHR Application no. 18139/91; *Cumhuriyet Vakfi and others v Turkey* [2013] ECHR Application no. 28255/07.

[106] See for example *Financial Times Ltd and others v the United Kingdom* [2009] ECHR Application no. 821/03, par. 56; *Goodwin v the United Kingdom* [1996] ECHR Application no. 17488/90, par. 28; *Voskuil v the Netherlands* [2007] ECHR Application no. 64752/01, par. 49; *Telegraaf Media Nederland Landelijke Media BV and others v the Netherlands* [2012] ECHR Application no. 39315/06, par. 84-88; *Becker v Norway* [2017] ECHR Application no. 21272/12, par. 59; *Sanoma v The Netherlands* [2010] ECHR Application no. 38224/03, par. 67.

[107] *Magyar Helsinki Bizottság v Hungary* [2016] ECHR Application no. 18030/11, par. 155.

[108] See e.g; *Dammann v Switzerland* [2006] ECHR Application no. 77551/01, par. 52.

[109] See Julia Laffranque, "A Look at the European Court of Human Rights Case Law on Moral Issues and Academic Freedom" (2017) 26 Juridica International 34; *Cox v Turkey* [2010] ECHR Application no. 2933/03; Council of Europe, "Cultural Rights in the Case-Law of the European Court of Human Rights" 42, par. 91; *Mustafa Erdoğan and Others v Turkey* [2014] ECHR Application nos. 346/04 39779/04, par. 40; *Aksu v Turkey* [2012] ECHR Application nos. 4149/04 41029/04, par. 71; *Hasan Yazici v Turkey* [2014] ECHR Application no. 40877/07, par. 55; and *Sorguç v Turkey* [2009] ECHR Application no. 17089/03; *Magyar Helsinki Bizottság v. Hungary*, par. 168. @echrBaskayaOkcuogluTurkey1999, par. 65; *Kenedi v Hungary* [2009] ECHR Application no. 31475/05, par. 43; *Wille vs Liechtenstein* [1999] ECHR Application no. 28396/95; *Sorguç v. Turkey; Sapan vs Turkey* [2010] ECHR Application no. 44102/04, par. 34; *Kula v Turkey* [2018] ECHR Application no. 20233/06, par. 38.

[110] *Handyside v. the United Kingdom*, par. 49.

[111] Ibid, par. 49; *Observer and Guardian v the United Kingdom* [1991] ECHR Application no. 13585/88, par. 60; *the Sunday Times v the United Kingdom* [1991] ECHR Application no. 13166/87, par. 51.

[112] *Handyside v. the United Kingdom*, par. 49.

[113] *Vereinigung Demokratischer Soldaten Österreichs and Gubi v Austria* [1994] ECHR Application no. 15153/89, par. 37; *Informationsverein*

But while restrictions on communications freedom need to be subject to strict scrutiny, not all information is protected to the same degree. This involves a balancing exercise, weighing the interests in interference against the interests in communications freedom. This also requires an analysis of the subsidiarity of the interference: there must be no other means of achieving the same end that would interfere less seriously with the fundamental right concerned. Furthermore, where Article 10 conflicts with another right under the Convention, such as the right to privacy, these rights deserve equal respect, and a wide margin of appreciation will usually be afforded by the Court in striking a balance between the two.[114]

At the heart of the proportionality analysis of the Court in the context of communications freedom lies the concept of the *"public interest"*. The more the dissemination of information is in the public interest, the more it can count on protection. According to the Court, the "public interest relates to matters which affect the public to such an extent that it may legitimately take an interest in them, which attract its attention or which concern it to a significant degree, especially in that they affect the well-being of citizens or the life of the community."[115] This is also the case with regard to "matters which are capable of giving rise to considerable controversy, which concern an important social issue, or which involve a problem that the public would have an interest in being informed about."[116] Furthermore, the quest by the public to find *solutions* to problems through dialogue also thrives on freedom of expression.[117]

All these considerations are relevant for the information security cycle: while vulnerabilities may appear to be highly technical issues only interesting to a limited group of experts, these can deeply affect individuals, organisations and governments alike. They have, in other words, a strong public interest dimension. Research and disclosure are an important way to address these vulnerabilities and the related public interest issues. This is particularly the case where information security measures support the enjoyment of fundamental rights, for example in the case of encryption technologies which protect the confidentiality of communications.

Another factor considered by the Court is the extent to which information contributes to the quest for truth: it has considered that "it is an integral part of freedom of expression to seek historical truth."[118] Similarly, the Court has considered that a criminal law system should allow for the *exceptio veritatis* – the defence of truth – with regard to provisions protecting the reputation of heads of state.[119] It follows that information that contributes to the quest for truth, or can be proven to be true, should be accorded more protection.

Research and publication of information security vulnerabilities contributes to a better understanding of the working of software and hardware, and thus of truth. This already is an important argument, but it becomes even more important because software and hardware play such a central role in our society, also for the enjoyment of other fundamental rights. Improving our understanding of the digital infrastructure we rely on everyday, also contributes to the enjoyment of these other fundamental rights.

Case law on the right to freedom of expression in relation to the publication of *confidential information* is also relevant. This is because some policy interventions in this cycle are predicated on the assumption that keeping information with regard to information security measures secret, is a good way to advance information security. The Court notes, however, that in the context of confidential information, there is "little scope" for restrictions on a debate of matters of public interest.[120] Furthermore, the Court is realistic when it comes to the question of whether information is still confidential – it looks to the actual dissemination and also takes into account the probability that information might not be confidential anymore.[121] This is relevant, because most vulnerabilities will eventually be published, sometimes anonymously, regardless of the existence of confidentiality obligations.

Lastly, the case law on who can profit from Article 10 is highly relevant. The Court initially accorded an important role to journalists working in the press media in spurring the debate on matters of public interest. According to the Court, the press played the vital role of "public watchdog."[122] But as the internet became widely available, it gradually recognised that others could also perform this role. What matters is whether the activities of an organisation are an essential element of informed public debate.[123] In the context of information security, this "informed public debate" is fed by researchers from diverse backgrounds, some are self-taught independents, some are working in the commercial sector, some

Lentia and Others v Austria [1993] ECHR Application no. 13914/88; 15041/89; 15717/89; 15779/89; 17207/90, par. 35.

[114] *Von Hannover v Germany (no 2)* [2012] ECHR Applications nos. 40660/08 and 60641/08, par. 106; *Case of Delfi AS v Estonia* [2015] ECHR Application no. 64569/09, par. 139.

[115] *Magyar Helsinki Bizottság v. Hungary*, par. 162.

[116] Ibid, par. 162. As an example, information meets a public-interest test where, inter alia, disclosure provides transparency on matters of interest for society as a whole and thereby allows participation in public governance by the public at large; ibid, par. 161.

[117] *United Communist Party of Turkey and Others v Turkey* [1998] ECHR Application nos. 133/1996/752/951, par. 57: see also @echrStankovUnitedMacedonian2001, par. 97.

[118] *Chauvy and Others v France* [2004] ECHR Application no. 64915/01, par. 69. Conversely, "denying the reality of clearly established historical facts, such as the Holocaust […] does not constitute historical research akin to a quest for the truth", and the Court considered such "attempts to deflect Article 10 of the Convention from its real purpose by using his right to freedom of expression for ends which are contrary to the text and spirit of the Convention"; *Garaudy v France* [2003] ECHR Application no. 65831/01; see also *Morice v France* [2015] ECHR Application no. 29369/10, par. 126; *Lingens v Austria* [1986] ECHR Application no. 9815/82, par. 46; and later *Oberschlick v Austria* [1991] ECHR Application no. 11662/85, par. 63; *Salov v Ukraine* [2005] ECHR Application no. 65518/01, par. 113.

[119] *Colombani and others v France* [2002] ECHR Application no. 51279/99, par. 66.

[120] *Stoll v Switzerland* [2007] ECHR Application no. 69698/01, par. 106; ibid, par. 110.

[121] See *the Sunday Times v. the United Kingdom; Observer and Guardian v. the United Kingdom; Vereniging Weekblad Bluf! v the Netherlands* [1995] ECHR Application no. 16616/90, par. 45; *Telegraaf Media Nederland Landelijke Media B.V. and others v. the Netherlands*, par. 130; *Plon v France* [2004] ECHR Application no. 58148/00.

[122] *Observer and Guardian v. the United Kingdom*, par. 59; *the Sunday Times v. the United Kingdom*, par. 50.

[123] *Magyar Helsinki Bizottság v. Hungary*, par. 167.

are from academia. All these researchers should be considered a "public watchdog" for the state of information security of our digital infrastructure, as long as they work towards strengthening this infrastructure, and as such are accorded the same protection under Article 10.

All in all, disclosure of vulnerabilities in digital infrastructure by researchers is a good example of an activity protected under Article 10 of the Convention.

5.2.1. *Duties and responsibilities and the information security cycle*

Now, the fact that communication may be protected under Article 10 of the Convention, does not mean that its beneficiaries can publish information at will. Article 10 emphasises the obligations of the person invoking the right: the exercise of these freedoms carries with it "duties and responsibilities". The question is how these duties and responsibilities apply to information security research. In fact, since the information security cycle is predicated on improving information security in the long run, but publication may pose a risk in the short term, the brunt of the proportionality assessment in this context will in most cases be bourne by the scope of these duties and responsibilities.

Case law on the due diligence required by journalists when publishing information suggests that information security researchers have a duty of care when researching and disclosing vulnerabilities.[124] Journalists can profit from Article 10 when reporting on issues of general interest, but only as long as they are acting in good faith in order to provide accurate and reliable information in accordance with the ethics of journalism.[125] In the context of defamation by a newspaper, the due diligence required depends on different factors.[126] Where the allegations are particularly serious, for example allegations that a person supervised the deportation of Jews in the Second World War, "the utmost care and particular moderation" was required.[127] And while most of the case law concerns journalists, the Court has determined that the same principles also apply to others, such as people distributing campaigning leaflets.[128]

This case law implies that information security researchers will in many cases have a duty to mitigate the risks associated with disclosure. The most important way to mitigate the risks, is by allowing a period of time to bring out a patch or fix a vulnerability before publishing it. But how much time should researchers grant the organisations to bring out a patch? The reference to the *ethics* in the case law above, could be read to imply that for journalists, this is partly a matter of what the profession itself considers to be acceptable. And the same would apply to information security researchers – commonly accepted standards should be considered relevant for this assessment.

However, the Court's case law also provides some pointers. On the one hand, the *urgency* of publication is relevant – in other words, what would happen if publication were to be delayed? This question is mostly relevant in the context of so-called prior restraints: prohibiting a publication altogether, instead of interfering *after* a publication. Such prior restraints are not prohibited *per se*, but "the dangers inherent in prior restraints are such that they call for the most careful scrutiny on the part of the Court. This is especially true so as far as the press is concerned, for news is a perishable commodity and to delay its publication, even for a short period, may well deprive it of all its value and interest."[129] Where there is less urgency in publishing information, for example in the case of archives, the duty to "act in accordance with the principles of responsible journalism by ensuring the accuracy of historical, rather than perishable, information is likely to be more stringent."[130]

Now, to be clear, there have also been cases where research and publication have gone too far. Sometimes, this is because of the damage resulting from a publication. For example, in *Hadjianastassiou* (1992), the Court considered that "the disclosure of the State's interest in a given weapon and that of the corresponding technical knowledge, which may give some indication of the state of progress in its manufacture, are capable of causing considerable damage to national security" and it found a five month-prison sentence for disclosing information justified.[131] This can also be the case where there are alternatives which achieve the same effect – something which is particularly relevant for performing research.[132] This means information security researchers must not go further than necessary, not with their methods, and not with their disclosure. So: no downloading a file if you just needed to show that the server was badly secured; no providing an exploit if you could prove your point with a description of what you

[124] The Court has also touched on the duties and responsibilities of others, such as employees towards their employers, see for example *Wojtas-Kaleta v Poland* [2009] ECHR Application no. 20436/02.
[125] *Stankiewicz and others v Poland* [2014] ECHR Application no. 48723/07, par. 62; see before *Bladet Tromsø and Stensaas v Norway* [1999] ECHR Application no. 21980/93, par. 65; *Fressoz and Roire v France* [1999] ECHR Application no. 29183/95, par. 54.
[126] *Stankiewicz and others v. Poland*, par. 63 and cited case law.
[127] *Radio France and others v France* [2004] ECHR Application no. 53984/00, par. 39; See also *Europapress Holding DOO v Croatia* [2009] ECHR Application no. 25333/06, par. 68.
[128] *Steel and Morris v United Kingdom* [2005] ECHR Application no. 68416/01, par. 90.
[129] *Ahmet Yildirim v Turkey* [2012] ECHR Application no. 3111/10, par. 47; see before *the Sunday Times v. the United Kingdom*, par. 51; and *Observer and Guardian v. the United Kingdom*, par. 60.
[130] *Times Newspapers Ltd v the United Kingdom (Nos 1 and 2)* [2009] ECHR Applications nos. 3002/03 and 23676/03, par. 45.
[131] *Hadjianastassiou v Greece* [1992] ECHR Application no. 12945/87, par. 45.
[132] See ECHR, par. 284 for an overview; for example, the Court did not deem it necessary for journalists to actually buy a firearm (in violation of criminal law) in order to demonstrate that it was easy to purchase one, because this could have been illustrated in other ways; *Salihu and others v Sweden* [2016] ECHR Application no. 33628/15, par. 57; the conviction of a journalist for carrying a weapon on an airplane (wanting to prove that airport security was bad) was also considered disproportionate, because the journalist could have revealed the security flaws at the airport without committing a criminal offence, for example by disposing of the knife after the security check-points; *Erdtmann v Germany* [2016] ECHR Application no. 56328/10, par. 23; similarly, the conviction of journalists who owned and used scanners to intercept police traffic (to arrive at a crime scene in time) was also deemed proportionate, although the reasoning is succinct; *Brambilla and others v Italy* [2016] ECHR Application no. 22567/09.

found; and always documenting what you did, for later reference.

5.2.2. *Positive obligations flowing from the right to communications freedom*

Lastly, case law on a so-called "right to reply" provides some inspiration for the question of whether states have an obligation to adopt rules on coordinated vulnerability disclosure processes. The Court in one case notes that the state has a positive obligation to ensure that an author had a reasonable opportunity to exercise his right of reply in a newspaper, and to ensure that he had an opportunity before the domestic courts to contest the newspaper's refusal.[133] The Court considers that the right of reply, as an important element of freedom of expression, flows from the need not only to be able to contest untruthful information, but also to ensure a plurality of opinions, especially in matters of general interest such as literary and political debate.[134] In both cases, the national law provided for a right to reply, and the case centred around the question of whether its application was in line with Article 10, focusing on the role of the press. But the cases arguably also underline that states have an obligation to structure other publication processes, not only of the press, in such a way that damage is minimised and the goals of this process – truth-seeking, plurality – are maximised. This broader understanding is also relevant for information security research – it is likely that states have a positive obligation to embed coordinated vulnerability disclosure procedures in their legal frameworks to ensure that information security research is channeled in the right direction.

5.2.3. *The right to communications freedom under the Charter*

The meaning and scope of Article 11 of the Charter are the same as those guaranteed under the Convention.[135] And the Court of Justice also often refers to the European Court of Human Rights in its decisions. In its case law to date, the European Court of Justice has furthermore not deviated from the line set out by the European Court of Human Rights. The European Court of Justice has called the principle of freedom of expression "one of the fundamental pillars of a democratic society", and has underlined the "essential role played by the press in a democratic society", communicating information and ideas and the public's right to receive them.[136] Restrictions on the press informing the public must thus be "strictly necessary."[137] Similar to the case law on Article 10 of the Convention, whether a publication contributes to the public interest is an important factor.[138] Other factors include "the content, form and consequences of the publication, and the manner and circumstances in which the information was obtained and its veracity", as well as the possibility for an organisation "to adopt measures to mitigate the extent of the interference."[139] Conversely, when publication does not contribute to a discussion of public interest – as in the case of commercial information –, member states have a broader discretion in determing which measures are appropriate, and review is limited to an examination of the reasonableness and proportionality of the interference.[140] In other words – it is not necessary to draw a clear line between the communications freedom case law under the Charter and under the Convention when it comes to assessing restrictions on the information security cycle.

5.3. *Relation between the right to science and communications freedom*

As noted above, an important part of the right to science is scientific freedom: the right to determine your own lines of inquiry and share the results of this inquiry with others. This obviously is strongly related to the right to communications freedom under the Convention and the Charter, as is also clear from the Court of Justice's considerations on Article 13 in *European Commission v. Hungary* (2020):[141]

> [A]cademic freedom in research and in teaching should guarantee freedom of expression and of action, freedom to disseminate information and freedom to conduct research and to distribute knowledge and truth without restriction, although it should be made clear that that freedom is not restricted to academic or scientific research, but that it also extends to academics' freedom to express freely their views and opinions.

Although this quote focuses on academic freedom due to the particulars of the case, one could easily replace *academic* with *scientific* and it would still work. So what does the right to science add to the right to communications freedom?

First, the right to science protects all phases of scientific inquiry equally. The research stage is explicitly mentioned in the Covenant: it includes an undertaking on member states to "respect the freedom indispensable for scientific research and creative activity."[142] By contrast, the activities traditionally protected under the right to communications freedom are mostly related to the disclosure phase, and the protection of the preparatory stages can be derived from protection of the disclosure phase (see above). This further extends protection to research activities in the information security context.

Second, not only do scientists have a right to perform research, but everyone has a right to enjoy the benefits of that research, of "scientific progress". You can enjoy the benefits through products and services which are based on the insights of that research. And you can also enjoy scientific progress by learning about the state of science, and, where necessary, im-

[133] *Melnychuk v Ukraine* [2007] ECHR Application no. 28743/03.
[134] Ibid, par. 2; *Eker v Turkey* [2017] ECHR Application no. 24016/05, par. 43.
[135] Explanations Relating to the Charter of Fundamental Rights.
[136] *Damgaard* [2009] CJEU Case C-421/07, par. 26; *GC/CNIL* [2019] CJEU Case C-136/17 21, par. 76.
[137] *Spiegel Online GmbH v Volker Beck* [2019] CJEU Case C-516/17, par. 72; *Painer* [2011] CJEU Case C-145/10 45, par. 113; *Satamedia* [2008] CJEU Case C-73/07, par. 56; see similarly *Sky Österreich GmbH/Österreichischer Rundfunk*, [2013] CJEU Case C-283/11, par. 52.
[138] *Sergejs Buivids v Datu valsts inspekcija* [2019] CJEU Case C-345/17, par. 66; see also *Google Spain* [2014] CJEU Case C-131/12, par. 81.
[139] *Sergejs Buivids v. Datu valsts inspekcija*, par. 66.
[140] *Damgaard*, par. 27; see also *Neptune Distribution SNC v Ministre de l'Économie et des Finances (Minister for Economic Affairs and Finance)* [2015] CJEU Case C-157/14, par. 76.
[141] *European Commission v. Hungary*, par. 225.
[142] CLSR105710.

prove on it. This iterative nature of the scientific process is at the heart of the right to science. But the state of science can of course only improve, if researchers indeed *contribute* their findings to what is already known.

6. In defense of research and disclosure

This leads me to the core of my argument: offensive information security research must be put on equal footing with defensive information security research. This means three things. Firstly, it imposes on states an obligation to introduce an information security research exception, applicable across all information security domains. At the same time, it also obliges states to recognize a duty to disclose the findings of this research, under certain circumstances. And this means that governments are required to embed CVD-processes in their legal framework. These obligations square with a fundamental idea underlying the right to science: the pursuit of truth in service of humanity.[143] And this becomes even more clear if read in conjunction with the "duties and responsibilities"-clause under the right to communications freedom.

6.1. *A research exception*

Now, under what circumstances are there such obligations? I argue that the right to science, read together with the right to communications freedom, requires states to adopt a general information security research exception, in order to prevent researchers from fearing criminal or civil persecution. One way of doing this, would be to simply make circumvention of security measures lawful, under both criminal and civil law, regardless of intent and regardless of what you do with your knowledge of the vulnerability. But this would not be in line with other human rights obligations which states have under the Convention: states are for instance also required to provide practical and effective protection to if not exclude, then at least minimise the risk of unlawful access.[144] Technical and organisational measures are one way to provide such protection; prohibiting circumvention of these measures is another way. And there is, of course, an interaction between both levers: if you have strong security measures, you need less law enforcement, and if you have strong law enforcement this may decrease the need for good security. But you will always need some legal rules aimed at prohibition: instead, what is crucially important for the information security cycle, is that knowledge of vulnerabilities are fed back into the system, to strengthen security measures.

A more proportionate approach is therefore to introduce a conditional exception to liability for information security research in the public interest, as worked out below.[145] Such an exception should extend to both criminal and civil liability – which means that researchers cannot be prosecuted, or held liable in any other way for doing their research. This also means that contractual restrictions on research and disclosure in line with the exception should be considered void, and, in their contracts with suppliers, states should not restrict research which falls within this exception.

The exception can be modelled along the lines of the guidelines for the non-prosecution of information security research by the Dutch public prosecutor.[146] This means that information security research and disclosure is in the public interest if three conditions are met. Firstly, the activities may not go further than necessary for the goal of demonstrating the existence of vulnerabilities (proportionality). If research causes damage to a system, this should be considered disproportionate. Secondly, there is no other way to demonstrate the existence of vulnerabilities with less impact (subsidiarity). And lastly, the findings of the research must be disclosed in line with applicable coordinated vulnerability disclosure policies (more on this below). For evidence purposes, this also means that researchers will have to structure their research in such a way that they will subsequently be able to demonstrate that they acted in line with these principles. Putting the public interest at the core of this exception also implies that there is room to take into account the positive human rights impacts of disclosing a vulnerability in some cases.

6.2. *A duty to disclose*

Making the exception dependent on the disclosure of vulnerabilities is important: this is a translation of the idea under the right to science that research is dependent on an iterative process of sharing information and falsification. Merely doing information security research without disclosing your findings would not do justice to this principle. But I contend that this obligation to disclose on the basis of the right to communications freedom and the right to science goes further: it should apply, regardless of how you obtained knowledge of vulnerabilities, not only when you claim protection under these rights.

This duty to disclose means two things. First, governance measures should be aimed at rapid disclosure and patching of vulnerabilities to strengthen security measures. It also means that states may not keep vulnerabilities found through research under wraps for offensive purposes (and holds even more for *inserting* vulnerabilities). This doesn't mean, by the way, that *all* information needs to be disclosed: perhaps it is sufficient to publicly disclose just the information needed to allow organisations to determine whether they are affected, whereas vendors also need to obtain a working exploit. If on

[143] See also Beiter, Karran and Appiagyei-Atua, "Yearning to Belong" ch IV.B.

[144] The Court speaks of "unauthorised" access, but for clarity I use the same terminology as in the sections above; *I v Finland* [2008] ECHR Application no. 20511/03, par. 47; *KU v Finland* [2008] ECHR Application no. 2872/02, par. 49.

[145] See also ENISA, "Economics of Vulnerability Disclosure" (ENISA 2018); ENISA, "The Directive on Attacks Against Information Systems: A Good Practice Collection for CERTs on the Directive on Attacks Against Information Systems" (ENISA 2013), par. 2.4.3; Schaake and others, par. 6.2.2; and OECD, par. 3.3; see also Mingyi Zhao, Aron Laszka and Jens Grossklags, "Devising Effective Policies for Bug-Bounty Platforms and Security Vulnerability Discovery" (2017) 7 Journal of Information Policy 372 which suggests the same because it would support the effectiveness of bug-bounty programs.

[146] CLSR105710 Dutch Public Prosecutor, "Beleidsbrief Coordinated Vulnerability Disclosure" (December 14, 2020).

the other hand, disclosing would merely increase the risk of unauthorised access, but not allow people to mitigate this risk, this would argue against publication.

This is why I contend that researchers are not expected to determine entirely on their own how they should give effect to these duties. Given the interests at stake, and the complex balancing required when devising CVD-processes, there is also a governmental obligation to devise CVD-policies and embed them in a legal framework. By doing so, states can further ensure that research towards vulnerabilities is used to strengthen security measures, especially those which protect human rights. I work this out in the last section.

The duty to disclose logically should also apply to states: states should – *in principle, see below* – no longer be able to hoard vulnerabilities, and should instead disclose those vulnerabilities they are aware of. This particular policy follows as much from the right to science as it follows from the rights to privacy and communications freedom (because hoarding vulnerabilities increases the risk of unlawful access too much). One important question is what would the impact be on the work of national intelligence agencies when accessing adversaries' systems: to what extent do they rely on non-disclosed vulnerabilities, or can they simply rely on disclosed vulnerabilities which have not yet been patched and badly configured infrastructure? In 2021, the German Constitutional Court concluded that the fundamental right to confidentiality and integrity of IT systems does not require authorities to notify "any IT security vulnerabilities immediately and in all circumstances."[147] According to the Court, delaying notification must, however, be based on a legal framework that resolves the conflict between the different interests involved:

> It must be ensured that every time the authority decides whether to keep an unknown security vulnerability open, it assesses the risk of the vulnerability's existence becoming more widely known and it determines, in qualitative and quantitative terms, the benefit of potential state infiltration measures exploiting the vulnerability. Following a weighing of the risks and benefits, the authority must report the security vulnerability to the developer unless the interest in keeping it open outweighs the risks.

Whether this conclusion is correct requires further research. My initial assessment is that the German Court gives too much leeway to states in this regard: on balance, the public interest favours immediate disclosure, and the burden rests on governments to demonstrate otherwise. This, given the poor state of information security, will be difficult to accomplish.

There is one important exception to the duty to disclose: if this is a vulnerability in a configuration of a single system of one organisation, disclosing would not necessarily help others with improving their own systems (unless this is a common mistake). In that case, it is questionable whether this can be derived from human rights obligations, because it does not affect the right to science, and the right to privacy and communications freedom do not call for such transparency. Thus, private organisations would not have to disclose the results of their own security testing (unless they uncover an actual, notifiable security breach, not a mere vulnerability). But if this is a vulnerability which is present across many organisations – a form of *class break* –, then disclosing enables others to patch their systems.

I recognise that such a duty to disclose may have side effects. First, it may lead to less research n vulnerabilities. If you need to disclose a vulnerability, you might not want to be aware of its existence it in the first place – so you'd rather not investigate it.[148] It would also be likely to lower the price for bug bounties significantly – you have to disclose vulnerabilities anyway, so there's no point in asking for remuneration.[149] This measure will lastly limit the market for zero day exploits.[150] It also means that it is not useful for governments to insert vulnerabilities in systems on purpose. But what if some states are obliged to do this, but others aren't, for example? A cynic might conclude that in that case, EU citizens would be less secure than the citizens of their adversaries, because EU intelligence agencies could not use knowledge of vulnerabilities as leverage against their counterparts. These are all relevant considerations, but not considerations which are easily assessed under the right to science and the right to communications freedom and are interesting topics of further research.

6.3. *Embedding CVD-processes in a legal framework*

Finally, the framework for the research of vulnerabilities should be complemented with a framework for disclosing and acting on knowledge of vulnerabilities. At the core of this framework lies the idea that CVD-policies (which are currently voluntary principles), should be embedded in a legal framework. This framework should apply to all organisations which play a role in the attack surface – the operator, vendor and supplier – and contain at least three main elements.[151]

First, it is important that each organisation should create a publicly available contact point for disclosing vulnerabilities and that reporting of vulnerabilities is standardised – this could, for instance, be done through an online form on the website of the organisation, through which everyone

[147] *IT-Sicherheitslücken*, par. 43-44.

[148] See for an older economics analysis of mandatory disclosure Choi, Fershtman and Gandal.

[149] See on the economics of the market for bug bounties; Zhao, Laszka and Grossklags; Jiali Zhou and Kai-Lung Hui, "Bug Bounty Programs, Security Investment and Law Enforcement: A Security Game Perspective" 28.

[150] See Fidler for another approach to the market for zero days, advocating more enforcement for possession and use of exploits, as well as export control. See further Trey Herr and Paul Rosenzweig, "Cyber Weapons and Export Control: Incorporating Dual Use with the PrEP Model" (2014) 8 Journal of National Security Law and Policy 301, also advocating export control of exploits.

[151] This paragraph sets out the major elements of such a framework – useful standards for details, such as how to secure the submission of vulnerabilities, are for example worked out in ISO, "ISO/IEC 29147:2014 - Information Technology - Security Techniques - Vulnerability Disclosure" (ISO/IEC 2014). See also for similar suggestions ENISA, "Economics of Vulnerability Disclosure."; Schaake and others; Herpig; OECD (although the authors argue for voluntary, not mandatory notification of vulnerabilities).

could submit vulnerabilities.[152] This would allow researchers to easily submit vulnerability reports, and allow organisations to ensure they receive the right information. Researchers would at the same time, be required to submit vulnerability reports through these reporting mechanisms, to ensure that the knowledge of a vulnerability would reach the right person quickly.

A second element of this framework would be an obligation on the part of these organisations to act on the knowledge of a vulnerability.[153] This could be partly construed via a clarification of the obligation to take security measures – when you learn something has a weakness, and you do not act on it, this may imply that your level of security is no longer appropriate. But since the system also extends to other parties who play a role in the attack surface, this means that these parties would now have a joint responsibility to act on this knowledge – coordinating and sharing information among themselves where necessary. This also requires that these organisations should not be held liable for sharing information on vulnerabilities for coordination purposes. Some have suggested that CERTs should play this role.[154] Whether this is a good idea would depend on the institutional governance structure – something which is beyond the scope of this article, but is a worthy topic for further research.

The speed with which organisations have to handle a vulnerability report would depend on a number of factors, with the potential risk of exploitation being the primary factor. This risk depends partly on the severity of the impact: where for example this affects many devices, or many people, or important infrastructure, or human rights, this calls for a swift response. And it depends in part on the likelihood of exploitation: where a vulnerability has already been exploited in the wild, this implies that a quick response is necessary, although one generally should assume that vulnerabilities are already being exploited.[155] Another factor is the costs of implementing a fix, and – related to this – the complexity of the coordination between different organisations in the attack surface. In order to ensure that organisations cannot drag this process out, the burden of proof to demonstrate that a response was appropriate would rest with the organisation which has learned of the vulnerability.

A third element of a legal CVD framework would consist of measures to increase transparency about vulnerabilities. This could be done by officially recognising a central repository of vulnerabilities, to which operators, vendors and suppliers must report vulnerabilities they have learned of, including when they have been fixed. There are already central registers, such as the CVE register, but these are privately run and not recognised in legislation. This officially recognised repository would not only keep track of all vulnerabilities, but would also disclose them for easy reference and provide aggregate reports on the time it takes to fix a vulnerability. This would improve the possibilities for enforcement and allow for further tweaking of the CVD-framework in the future.

Declaration of Competing Interest

None.

Data Availability

No data was used for the research described in the article.

[152] See also Frederico Oliveira da Silva, "Keeping Consumers Secure. How to Tackle Cybersecurity Threats Through EU Law" (ANEC and BEUC 2019) Position paper BEUC-X-2019-066 for a similar recommendation.

[153] This has already been proposed as early as 2008; Ross Anderson and others, "Security Economics and the Internal Market" (ENISA 2008), par. 6.5.1.

[154] See for example ENISA, "Good Practice Guide on Vulnerability Disclosure.", par. 6.4.

[155] See also ISO, "ISO/IEC 29147:2014.", par. 5.9.