The CRA and the Challenges of Regulating Cybersecurity in Open Environments: The Case of Free and Open Source Software

Lucas Lasota

Abstract

This chapter provides a bird's eye view of the Cyber Resilience Act (CRA) from the perspective of the policy, legal, and socio-economic elements that prompted regulators to intervene in the digital markets. Its focus centres on the market and regulatory failures regarding cybersecurity, treating the regulatory path taken by the EU as a reaction. An interdisciplinary approach is proposed as a methodology for listing the technical aspects of cybersecurity and the nature of vulnerabilities, and balancing economic factors with ethical and legal concerns. A practical context is given with the study case of a stakeholder intervention during the CRA's legislative process: the liability issue raised by Free and Open Source Software (FOSS) stakeholders. The collective intercession of different FOSS organisations galvanised broad changes in the text of the law. This chapter concludes with the recommendation that policymakers should not lose touch with civil society during the implementation phase and monitoring process.

1. Introduction – making cybersecurity a priority for digital markets

Recognising that *any connected device can be maliciously hacked* is one of the hard pills that digital users must swallow nowadays. As the Internet has now spread to over 66% of the world's population (Statista, 2024), and digital products are more pervasive than ever in all spheres of life, a sensation of impotence subtly imposes a perception that it is too late for any adequate reaction by policymakers. This feeling is accentuated when noting that cybercrime involving digital products has cost trillions of euros in recent years (European Commission, 2022a, p. 2), and that current EU legislation does not comprehensively impose mandatory cybersecurity for economic actors. Indeed, securing the vast number of elements in the internet value chain – composed of interconnected devices, encryption,

software and hardware interoperability, and integration of networks and data streams – is one of the significant challenges of the contemporary world.

This sombre attitude stands in stark contrast to the enthusiastically progressive view proposed by the *cyberculture*. After all, *cyberspace* was thought to be a civilising refuge from traditional oppressive state-led forces (Barlow, 1996). Admittedly, as early as the beginning of the 1990s, disenchanted whistleblowers warned about how the *cyber-rhetoric*, with its articulated dichotomous discourse of immunity from sovereignty of traditional state forces, ended up being co-opted by capitalist interests (Curtis, 2016). The resulting neoliberal-style interventionism facilitated an intimate relationship of co-dependence between liberal governments and corporations favouring profitability and dominance over distributed economic welfare and efficiency in digital markets (Powers and Jablonski, 2015). This symbiosis produced a contradictory outcome: an overemphasis on cybersecurity for surveillance and law enforcement that contrasts with a lack of regulatory oversight of corporate control, leading to the persistent, structural market failures in the realm of cybersecurity (European Commission, 2022a, p. 17).

The opposition to the status quo encompasses far-reaching reactions, ranging from voices demanding deep structural reorganisation over the production and ownership of wealth in the digital age to reformist approaches via legislative and regulatory updates (Lasota, 2023). The Cyber Resilience Act (CRA) (Regulation (EU) 2024/2847) emerged from this content, as the European Union (EU) seized the regulatory momentum to complement product safety and liability legislation by forcing tech companies to improve the security of their products through compliance with the CE quality marking.[1] The CRA is the outcome of a regulatory approach which evolved to conceive of cybersecurity as a cross-sector policy for digital markets. This complementary addition to the safety of digital products marks the EU taking a more interventionist approach in digital markets, aiming towards stricter behaviour rules for economic activities (Bygrave, 2024).

This chapter, therefore, seeks to understand the conditions under which the CRA emerged. The editorial contour skips an in-depth legal analysis

1 CE marking indicates that a product has been assessed by the manufacturer and deemed to meet EU safety, health, and environmental protection requirements. For more information, please see Your Europe (2024).

and favours an interdisciplinary approach merging legal, social-economic, and historical analysis. As a portrait of the codification of cybersecurity into law, a particular aspect of the public debate is here reported: the contributions from Free and Open Source Software (FOSS) stakeholders reacting to new, CRA-imposed liability regimes. The choice for this portrayal is relevant. As the CRA's envisioned scope applies to commercialised products with digital elements – from small internet of things (IoT) devices to operating systems and security hardware – the rules necessarily touch both embedded and non-embedded software. Since up to 90% of software developed today has FOSS elements (Nagle et al, 2022, p. 4), the law necessarily relates to FOSS. Nevertheless, as revealed by the fierce reaction from different FOSS stakeholders, the European Commission's 2022 CRA Proposal fell short on understanding the dynamics of the production, distribution, and maintaining of FOSS (BEUC, 2022; Hendrick and Mckeay, 2022; FSFE, 2023; Phipps, 2023; Sander, 2024). The diverse legislative iterations that followed display a valuable dialectical experience among policy makers and FOSS stakeholders, shedding light on the intricacies of the FOSS economy and developing new legal constructions to accommodate the responsibilities tailored for the sector in relation to liability and cybersecurity rules.

The line of argument follows the above-stated objectives. Cybersecurity is presented not only as a technical discipline, but also as a complex social-economic phenomenon with deep political consequences. Then, security vulnerabilities and the efforts required for their mitigation are considered. Later parts dive deeper into the emergence of the CRA as legislation by addressing three topics: how cybersecurity has been historically regulated in the EU, the CRA as a solution for security as a *quality* of digital products, and, finally, a case study of the entanglement of the CRA and FOSS. The concluding remarks reflect on how cybersecurity is negatively affected by corporate influence on fragile communities, and how policymakers and regulators will need to take this reality into consideration when implementing the CRA.

2. Cybersecurity is broader than computer security

Cybersecurity is a broad discipline involving technology, information, and, above all, people developing processes for the security of computer systems (Christen, Gordjin and Loi, 2020). The diverse aspects of creating,

operating, analysing, and testing digital systems involve such subjects as law, policy, ethics, risk management, computer science, networking, and data science (ACM et al, 2017). As a field of endeavour, cybersecurity emerged with mainframe computers in the 1960s as a safeguard for data storage, and grew to include device integrity, infrastructure protection, and internet security (Warner, 2012). In its origins, cybersecurity was practiced in terms of the physical security of devices to prevent theft and sabotage, and document classification to prevent espionage. The Internet increased complexities to new heights: mass connectivity translated into software and devices being presented in all spheres of life, requiring a multidisciplinary approach to encompass the profound risks (DeNardis, 2020).

However, this is not to say that cybersecurity should be seen as an absolute value. More than a matter of individual effort, cybersecurity is a social project. Its multifaceted characteristics cannot, and should not, be oversimplified with binary assumptions of *more is good, less is bad*. Instead, depending on the context, other values may be supportive or conflicting. Overemphasising cybersecurity may violate fundamental values, such as equality, fairness, freedom, or privacy (van de Poel, 2020). At the same time, neglecting cybersecurity could also undermine privacy and safety, and detrimentally impact trust and confidence in digital infrastructure and institutions (Christen et al, 2020, p. 2). For instance, increasing cybersecurity measures for accessing devices by requiring users to provide personal data may decrease their level of privacy. At the same time, the anonymisation of users in a system may create difficulties for monitoring their activities, and thus the security of the whole system (Van de Poel, 2020).

The term *cybersecurity* itself is ideologically charged. Before 1989, discussions instead focused on *computer security*. The word *cyber* originates from *cybernetics* – a transdisciplinary philosophy of the 1940s, but was etymologically linked to security in the 1990s under the auspices of the *cyberculture* (Newitz, 2013). With that, cybersecurity fell under the online-offline dichotomy within the broader concepts of digital libertarian claims that the Internet had to be immune from the regulation of the offline (Barlow, 1996). This mindset permeated the following two decades, creating a regulatory gap between security and safety (as explained in the next sections). Strangely enough, starting in the 2010s, the naming of legislative and regulatory initiatives began to reclaim the term *cyber*, as the denomination of several laws and policies in this chapter illustrates. However, legally speaking, Art. 2(1) of the Cybersecurity Act (2019) defines cybersecurity in the EU as:

"activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats".

The dimensions of cybersecurity are technical, ethical, political, economic, and legal (ACM et al, 2017; Papakonstantinou, 2022). Traditionally, the technical aspects of cybersecurity relate to the protection of such valuable assets as hardware, software, and data by (i) information security and (ii) system security. System security is not limited to information and can refer to so-called digital systems with physical components, such as personal devices or larger equipment used in industrial manufacturing, finance, energy, healthcare and infrastructure. Both aspects comprise the following values (Herrmann and Pridöhl, 2020, pp. 13–14):

Confidentiality: Only authorised users and processes should be able to access or modify the system's data or parameters. Example: encrypting emails and messages so that only intended recipients can read the contents;
Integrity: Accuracy and completeness of the data and the system during their entire lifecycle. Example: implementing measures to detect and prevent unauthorised alterations to files;
Availability: Ensuring that information and resources are accessible to authorised users when needed. Example: deploying redundant servers to keep a website online even during malicious attacks or hardware failures;
Authenticity: Verifying that data and communications are genuine and have not been tampered with. Example: using digital signatures to confirm a document's origin.

The ethical dimension of cybersecurity is multifaceted. Issues prompting ethical consideration include legitimacy of hacking, dilemmas involving vulnerability reporting, access grants, privacy, conflicting attitudes in law enforcement, and encryption (Christen, Gordjin and Loi, 2020).

Due to its inherent focus on power in the information society, cybersecurity raises diverse political issues as well (Guiora, 2017). Such topics as the regulation of information flows, the protection of civil and political rights, privacy, security of government systems, and market issues necessarily invoke political consideration from decision makers. International relations, interstate competition related to technology, economical aspects, internet governance, and national security are also areas in which states, governments, and public agencies have a stake in cybersecurity (Ishikawa and Kryvoi, 2023).

The economic dimension in cybersecurity has been a convergence point in EU law-making. Security services compose an entire industry, ranging from hardware production to software development, consultancy, penetration testing, cyberdefence, and encryption technologies. How economic actors prioritise cybersecurity involves complex trade-offs between security and other values, asymmetries of defence and attack, social gains and losses, and the costs of adopted strategies (Grady and Parisi, 2006). The several market failures involving cybersecurity have been subject to scrutiny from policymakers, and will be analysed further.

Legal and regulatory aspects of cybersecurity can include rules imposed on individuals, organisations, and governments related to the protection of information technology and computer systems (Schreider and Noakes-Fry, 2020). Regulations aim to minimise security risks and enhance protection, as well as determine the legality of security and encryption technologies. Many diverse legal areas fall under the overarching scope of cybersecurity, such as cybercrime, liability and accountability, certification, security of critical infrastructures, and goods (Fuster and Jasmontaite, 2020).

Cybersecurity's corpus of legal and standards frameworks in relation to software products and services took longer to develop and mature than those for safety and privacy *precisely because of* how the above-mentioned elements differentiate cybersecurity from safety and data protection (Vedder, 2019). Product safety is a subset in the larger area of consumer protection and includes procedures to minimise the likelihood of accident or injury (Ruohonen, 2022). Cybersecurity is concerned with diminishing vulnerabilities and protecting against intentional and non-intentional harm caused by human and technical factors and cyberattacks. Cybersecurity measures include human-related preventive activities and technical elements, such as firewalls, anti-virus software, intrusion detection and prevention systems, encryption, and login passwords. In software engineering, cybersecurity includes best practices, guidelines, quality control, and standardisation for securing software and diminishing vulnerabilities (ACM, 2017). However, as the importance of artificial intelligence (AI) and the IoT increases, so too does cybersecurity become more connected to consumer safety and critical industrial infrastructure, as well as to the digital economy and democratic systems (DeNardis, 2020). In its turn, although data protection has similarities and often overlaps with cybersecurity, it has a closer relation to privacy. Cybersecurity and privacy have historically shared a common ground in protecting confidentiality, integrity, and access to data, but many cybersecurity problems have lesser implications for pri-

vacy, and vice versa (Porcedda, 2023, p. 130). For instance, the collection of non-personalised industrial data can be sensitive from a cybersecurity perspective, but has less of an impact on individuals' privacy. Similarly, advertising in social media prompts serious privacy concerns and other social risks, whereas cybersecurity threats can be of lesser concern (Grotto and Schallbruch, 2021).

Prevention and resilience are two foundational elements of cybersecurity. When attacks are not prevented, resilience means withstanding, recovering, and evolving from them (Bendiek et al, 2017, p. 2). Resilience in this sense complements prevention by involving procedures to respond and recover in case of a cyberattack (Bygrave, 2024). Anticipating attacks means understanding vulnerabilities, how they occur, and what is necessary to mitigate them. The following section delves more deeply into these aspects.

3. Vulnerabilities are inescapable in the digital world

When related to software, cybersecurity is considered a *software quality* that spans all stages of the software life cycle (Salvaggio and González, 2023). As such, it refers to software's capabilities to: prevent unauthorised actions in relation to information and other resources of the system; tolerate security-related attacks and violations of the system; and quickly and securely recover from an attack.

Vulnerabilities are failures in these qualities that can be exploited against the system's security policy (Shirey, 2007). Vulnerabilities in software are also characterised by the information asymmetry between creation and detection. Exploitable vulnerabilities have been repeatedly shown to be easy to introduce in the code base, but their detection and remediation are not only difficult, but can take weeks or months (Hendrick and Mckeay, 2022, p. 3). Vulnerabilities are often found in systems composed of multiple components or in the interactions between components and systems. Infections derived from supply chain compromises are one of the most relevant challenges for cybersecurity nowadays (ENISA, 2023, p. 5). However, not all vulnerabilities are necessarily exploited. A *cyberthreat* refers to the hypothetical event wherein an invader or attacker uses the vulnerability (Paulsen and Byers, 2019). Common examples of vulnerabilities include:

Broken authentications: With authentication credentials compromised, identities can be hijacked. Other attacks may trick an authenticated user

into performing an action they did not intend. This, paired with social engineering,[2] can deceive users into providing a malicious actor with sensitive data (Feil and Nyffenegger, 2008);

SQL injections[3] **and malicious scripts (malware)**: Intentional malicious or defective code can be inserted into software to grant unauthorised access to databases, websites, and other assets (Aslan and Samet, 2020);

Misconfiguration and outdated software: A configuration error can be used to violate security. Unpatched or outdated software is a common source of vulnerability exploitation (Mugarza et al, 2020);

Unsecured Application Programming Interfaces (APIs):[4] Due to how APIs can share data and functionalities among connected devices, they can also create a broad attack surface through insufficient monitoring, configuration errors, and excessive data exposure (OWASP, 2019). If an API lacks proper authentication, authorisation, or encryption, it would be vulnerable to attacks and unauthorised data access.

Once a vulnerability is identified, it can either be kept secret or reported. There are ethical, policy, and legal issues to be considered here. Motivations for keeping a vulnerability secret may include its illegal exploitation or planned further legal action. Disclosures can be made publicly or privately in coordination with the software developer. Unreported vulnerabilities – also called *zero days* – may remain unfixed for a long time. Vendors, manufacturers, and developers respond to such reporting in different ways. For instance, they can react positively and expeditiously to fix the issue or disregard the report. Some have even taken a defensive approach and

2 Social engineering in this context refers to manipulations that exploit human error to trick someone into divulging specific information or performing a specific action for fraudulent purposes. "Phishing" is a common example where an attacker sends an email posing as a trusted entity to trick the recipient into clicking a malicious link or providing sensitive information, such as passwords or credit card numbers. More can be found at Wang, Z. Sun, L. and Zhu, H (2020).

3 SQL injections refer to a technique used to attack data-driven applications and systems. SQL is a language used to manage data bases, including access to, and the recording, control, manipulation, and deletion of data. SQL injections allow attackers to interfere with the queries that an application makes to its database. For more, please see OWASP (2025).

4 An application programming interface (API) is a connection between computers or between computer programs. It is a type of software interface, offering a service to other pieces of software.[1] A document or standard that describes how to build such a connection or interface is called an API specification. A computer system that meets this standard is said to implement or expose an API. The term API may refer either to the specification or to the implementation. More at Wikipedia (2025).

retaliated with legal actions. Discoverers may find themselves in a delicate position due to the grey area of the methods used to discover the vulnerability and how it was disclosed (ENISA, 2015, p. 7). Furthermore, keeping vulnerabilities secret or threatening the reporter can be considered immoral and illegal in some cases (van de Poel, 2020). For instance, a company could behave immorally and illegally by offering a bribe to a security engineer who discovered a vulnerability in the system in order to gain time to fix it without alerting its customers. Although there are competing and conflicting interests in disclosures between companies, researchers, the media, and the general public, it is recommended to protect the discoverer by recognising their whistleblower status and creating safeguards for researchers involved in vulnerability and ethical hacking (ENISA, 2022, p. 74). It is also recommended that cybersecurity agencies and governments establish policies fostering responsible disclosures to promote research, discovery, and transparency (ENISA, 2022, p. 8).

Vulnerabilities can be found by testing, auditing, and discovery efforts. Access to source code is helpful for security audits (Hermanowski, 2015). In the case of proprietary software, analyses may involve reverse engineering[5] (Payne, 2002, p. 68). The process for handling vulnerabilities differs by company and organisation, but generally involves detection, assessment, reporting, and mitigation (ENISA, 2015). Once the vulnerability has been detected, it should be assessed to determine the risks and threat levels. Next, it can be directly reported to those affected, as well as in public catalogues. Vulnerabilities in widely deployed products can be included in public databases, such as the "Common Vulnerabilities and Exposures (CVE)", "Open Source Vulnerabilities (OSV)", and "National Vulnerability Database (NVD)" (Townsend, 2024). There they receive a unique identifier (i.e., an alphanumeric code) and a score to reflect the potential risk they represent.[6] Public catalogues serve as reference points for vulnerability management for the general public.

After being discovered, assessed, and reported, vulnerabilities should be fixed. The release and integration of new updates and patches require further scanning, testing, and new iterations to avoid new vulnerabilities. Best practices indicate that organisations should have necessary process

5 Reverse engineering involves analysing a system, software, or device to discover its design, architecture, or code, often to duplicate or enhance the system without access to the original source. For more, see Wikipedia (2025a).

6 See, for example, the CVE process for recording vulnerabilities (CVE, no date).

in place, including responsible teams, short reaction times, and structured schedules, and publish as much information as possible to allow their users to accurately assess any risks to which they may be exposed (ENISA, 2015).

Remediation processes tend to be long and resource-consuming. Due to the impossibility of developing completely flawless software, *security by design* principles are important for saving remediation resources (OWASP, 2020). Managing and resolving vulnerabilities aim to reduce *attack surfaces*, which refer to every point or area in a system where an attacker could attempt to break in, extract data, or cause harm to the system.[7] Surface attack possibilities encompass the various vulnerabilities that attackers can exploit. For instance, in a web application, attack surfaces include user input fields, API endpoints, and network interfaces. If a web application has multiple outdated plugins, each could serve as a potential entry point for attackers to exploit. The existence of vulnerabilities does not necessarily translate into inevitable attack, so a risk assessment is useful for determining its probability and the consequent prioritisation for remediation (NIST, 2012). Risks can be avoided by eliminating the software feature or mitigated by implementing security measures. Risks can be transferred to users or covered by insurance (European Commission, 2022a, p. 10). Risks can also be accepted when a fix cannot be performed because the equipment cannot be replaced (OWASP, 2020, p. 15) or when the choice is made to cover the costs of an attack (Shostack, 2014).

There are several elements to consider in the risk assessment process. For instance, competitive pressure to bring products quickly to market, design factors, and requirements related to energy, power, size, speed, portability, and interoperability are decisive factors for developers and manufacturers when implementing security mechanisms (DeNardis, 2020). As the next section elaborates, industrial policies adopted for the tech sector have caused a market and regulatory failure for cybersecurity. Tracking how the EU regulatory approach reacted can elucidate how the CRA came to fruition.

7 See more at Computer Security Resource Center (no date).

4. From safety to security – understanding the EU's cybersecurity regulatory path

While expansionist policies for the Internet have brought connectivity to over 5 billion users (Statista, 2024), a collateral effect resulted in deprioritising security in favour of availability (ACM, 2017, p. 16; Powers and Jablonski, 2015, p. 22). This prioritisation affected how cybersecurity has been regulated. Although some aspects of computer security have been covered under data protection, national defence, law enforcement, and criminal law, regulation concerning *security as a quality of digital products* has lagged behind, and not accidentally so. Fostered by the waves of economic deregulation in the 1990s and 2000s in the US and EU, manufacturers and vendors of digital products have enlarged profit margins at the cost of better cybersecurity policies, commercialising products with exploitable vulnerabilities, which not only jeopardised the correct functioning of the markets (Lasota, 2023), but also negatively affected fundamental rights and safety (Chiara, 2022).

The neoliberal status quo established in the 1990s dominated the technology industry and boosted a symbiosis between corporations and governments in relation to security policies. The massive surveillance practices revealed by Edward Snowden in 2013 have demonstrated that, especially since 9/11, a *security hyperprevention mindset* has allowed governments and corporations to intervene and operate in many cases outside the law and due process to enforce security mechanisms (Lemke, 2014). *Surveillance capitalism* is the outcome of this symbiosis permeating digital societies (Zuboff, 2019), facilitating an intimate relationship of co-dependence between liberal governments and corporations in areas of surveillance, control, defence, and law enforcement (Powers and Jablonski, 2015). The overemphasis on cybersecurity for surveillance and law enforcement contrasts with the lack of regulatory oversight in digital markets, which creates an environment of less security and privacy that privileges corporate profit over distributed economic welfare and efficiency. The situation is rather puzzling: while surveillance capitalism misuses concepts of cybersecurity, capable of bypassing traditional constitutional safeguards and human rights (Lemke, 2014), consumers are increasingly exposed to faulty digital products with low levels of privacy and security due to regulatory and market failures.

Indeed, market aspects related to cybersecurity are characterised by diverse failures: information asymmetries, negative externalities, and inad-

equate levels of private investment (Carr and Tanczer, 2018; European Commission, 2022a). Heightening the security of digital products is no trivial task, and leaving it to market forces has historically led to suboptimal and inconsistent levels of confidentiality, integrity, and authenticity in said products (ENISA, 2011; Chung, 2017; DeNardis, 2020; Hendrick and Mckeay, 2022). Besides, turning from the security sector to a broader consideration, the extreme returns to scale, network externalities, and dependence on data pose challenges to digital markets' efficiency (Crémer, Montjoye and Schweitzer, 2019). The focus on internet expansion led policy makers to deviate from their traditional regulatory role, resulting in weakened oversight and accountability of industry in favour of profitability and dominance (Powers and Jablonski, 2015, pp. 22–24).

Safety regulations followed a different path from security. Liability derived from safety regulations was already a reality in the '80s, while the chronological gap for security was not closed in the next decades, leaving the behaviour of suppliers of digital products in the markets out of regulatory scope (European Commission, 2022a, p. 11). Unlike safety in the energy, finance, medical, and pharmaceutical sectors, cybersecurity as a quality of digital products remained under the auspices of industry self-regulation (Moore, 2013) and took a long time to be established in the EU, leaving consumers exposed to threats due to an absence of harmonised regulation (ENISA, 2022, p. 12). The legislative and regulatory landscape for cybersecurity in the EU scaled up from fragmented initiatives addressing specific domains to the latest large-scale horizontal regulations covering practically all elements of digital products. Security laws benefited from advancements in data protection and product safety regulation. Data protection norms emerged in Europe in the 1960s, mainly with the public sector's regulation of the collection and processing of data by public institutions, which, at the time, possessed the largest data banks and were the main processors. The *rediscovery* of the economic value of data at the end of the 1990s, coupled with the expansion of the Internet and the industrial strategies derived from it, led to a renewed concern about privacy in digital environments, raising concerns about cybersecurity as well (Mantelero, 2022, pp. 139–159). A risk-based approach to regulation emerged from product safety in the 1980s (Ruohonen, 2022). While chemicals and cosmetics required a more rigorous approach, software was permitted more lax supervision, leaving it industry players to self-assess their own standards, documentation, engineering practices, quality controls, and safety verification. The Product Liability Directive (Council Directive 85/374/EEC) represented a landmark

mechanism to incorporate four strategic goals (known at the time as the *New Approach*): fair trading, public health, public controls, and consumer information, as unified by standardisation. The Directive also strengthened consumer law by introducing some aspects of strict liability for producers, but software liability was left for a 2022 review (European Commission, 2022b).

The EU's cybersecurity institutional apparatus emerged at the end of the 1990s as a technical, engineering-driven governance system among various national teams responsible for network and computer security, known as Computer Emergency Response Teams (CERTs). The modus operandi of some European CERTs served as an initial base for further regulatory actions by the EU (Ruohonen et al, 2016). However, CERTs, including the coordination hub ENISA – founded in 2004 – followed a different track from other law enforcement agencies, such as Europol. The Cybersecurity Act (Regulation (EU) 2019/881) granted ENISA a permanent mandate with decision-making powers regarding policy issues and tasks, including technical supervision, certification frameworks, and dealing with large-scale cross-border cyberattacks and crises.

With the 2013 Cybersecurity Strategy (European Commission, 2013), cybersecurity became an official policy area in the EU by collating and combining sectoral rules for defence and law enforcement under a unified umbrella. Five years later, the revised 2017 strategy called for a complex approach to resilience that encompasses economic, societal, and political actors, enlarging the traditional and limited technical aspect of cybersecurity (European Commission, 2017). Although both strategies identified principles that would later be incorporated in legislative proposals, they did not include mandatory roles for the EU in the protection of the digital internal market (Bendiek et al, 2017). This changed with the third EU cybersecurity strategy of 2020, which evolved from being an essentially declarative policy to an operational document proposing concrete regulatory solutions by conceiving cybersecurity as a horizontal or cross-cutting policy for digital markets (Robles-Carrillo, 2023). This move integrates with other policy frameworks, marking the EU's more interventionist approach in digital markets, with the aim of stricter behaviour rules on economic activities (European Union, 2023). The next section dwells upon the CRA itself and contextualises the new law in a broader picture of other related legislation.

5. CRA: setting far-reaching cybersecurity rules for digital products

Over the last 20 years, cybersecurity rules have been established in sector-specific legislation related to cybercrime,[8] mobility and transport,[9] healthcare,[10] finance,[11] telecommunications,[12] and critical infrastructure.[13] However, as already mentioned several times in this chapter, an economics-led approach to cybersecurity as a quality of digital products was still notably absent. For instance, the GDPR (Regulation (EU) 2016/679) contains several provisions regarding information security, but does not deal with the cybersecurity of products. The Cybersecurity Act (Regulation (EU) 2019/881) concerns itself with certification and the ENISA's mandate, but does not establish any mandatory requirements for economic actors. The NIS 2 Directive (Directive (EU) 2022/2555), while serving as a follow-up to the first piece of EU-wide legislation on cybersecurity, does not entail requirements for the design, development, and security support of prod-

8 The Budapest Convention (Council of Europe, 2001) is the first binding instrument of international law aimed at harmonising domestic legislation related to cybercrime, dealing with copyright infringements, fraud, pornography, and network security violations. The convention has been signed by the 26 EU member states except Ireland.

9 Examples include the Vehicle General Safety Regulation (Regulation (EU) 2019/2144), the Common Rules in Civil Aviation Regulation (Regulation (EC) No 216/2008), and the Machinery Regulation (Regulation (EU) 2023/1230).

10 The Medical Device Regulation (Regulation (EU) 2017/745) and the In Vitro Diagnostic Medical Devices Regulation (Regulation (EU) 2017/746) are examples containing some aspects of cybersecurity.

11 The Regulation on Digital Operational Resilience for the Financial Sector (DORA) (Regulation (EU) 2022/2554) addresses this trend and aims to strengthen the cyber resilience of financial entities, such as banks, insurance companies, investment firms, and crypto-asset service providers.

12 Before the CRA, the Radio Equipment Directive (Directive 2014/53/EU) was the legislation with broad cybersecurity rules regarding transmitting devices (routers, smartphones, etc). Similarly, the European Electronic Communications Code (Directive (EU) 2018/1972) regulates how telecom operators should safeguard the security of their networks and services.

13 The European Network and Information Security Directive (NIS 1 Directive) (Directive (EU) 2016/1148) promulgated a minimum set of security requirements, including reporting obligations, for critical infrastructure in the EU. The NIS 2 Directive (Directive (EU) 2022/2555) expanded the sectors considered critical to encompass digital infrastructure, public administration, and space. The updated rules mandate more rigorous security requirements, which include enhanced cybersecurity risk management and reporting obligations. For more information on the NIS 2 Directive, see Chapter 17 'Unpacking the NIS 2 Directive: enhancing EU cybersecurity for the Digital Age' by Eyup Kun.

ucts. While the Radio Equipment Directive (Directive 2014/53/EU)[14] does include security requirements for network and fraud protection, it only covers wireless products (hardware and their embedded software), leaving other products and non-radio components (e.g., processors) out of the equation. Such safety laws as the Product Liability Directive (European Commission, 2022c) and Machinery Regulation (Regulation 2023/1230) address aspects of risk management and liability derived from flawed products, but do not include requirements of duty of care and other specific aspects of cybersecurity. The CRA has come to close this regulatory gap.

The CRA is a legislative initiative to regulate economic operators producing and commercialising products with digital elements (PDEs) in the EU internal market (Recital 2). Cybercrime involving such products has cost trillions of euros in recent years and the market dynamics have not been able to improve the situation for business and consumers (European Commission, 2022a, p. 2). The law addresses two main issues: (i) how to elevate the level of cybersecurity and (ii) how to provide better cybersecurity information to consumers (European Commission, 2022a, p. 4). Admittedly, these are not simple tasks, because:

Cross-border dimension: Cybersecurity has a strong cross-border dimension, as products are manufactured and used by consumers in different countries (European Commission, 2022a, p. 7);
Commercial interests: Cybersecurity has been not a commercial priority for manufacturers, as the emphasis on product security can be occasionally detrimental to corporate interests (European Commission, 2022a, p. 11). The development of new features is aimed towards market access and compatibility with existing products, with security properties suffering in the process (Burri and Zihlmann, 2023, p. 5). Security support (updates and handling of vulnerabilities) has been neglected or not provided for the product life cycle (European Commission, 2022a, p. 13);
Risk transfer to consumers: The higher switching costs and vendor lock-ins shift the costs of security vulnerabilities to consumers (European Commission, 2022a, p. 7). Although device providers can suffer reputational damage, consumers do not necessarily change the product or leave the provider's ecosystem (FSFE, 2023a, p. 22);
Lower security levels involving IoT: The massive number of smaller connected devices, IoT gadgets, toys, sensors, and other systems not run-

14 See also the Commission Delegated Regulation (EU) 2022/30, which further implemented cybersecurity requirements in the RED.

ning traditional operating systems have substantially lower levels of security protection. They present an entry gate to networks and may serve as hideouts in more complex environments (Meneghello et al, 2019). Besides, the apparent simplicity of such devices hides the complexity of their purpose and configuration, lowering the awareness of consumers (Palmer, 2021);

Information asymmetries: There are information asymmetries involved among manufacturers and consumers. Manufacturers have not provided adequate information about security features, vulnerabilities, and how to use a device safely (European Commission, 2022a, p. 13). Coupled with the fact that consumers generally lack even the most basic cybersecurity skills, this information asymmetry affects businesses as well: decision makers cannot properly evaluate risks posed to their organisation (European Commission, 2022a, p. 14).

Among the diverse possible regulatory approaches to deal with these issues, in 2021 the EC concluded that a strong interventionist approach would the most suited to improving the functioning and harmonisation of the internal market (Georgiev et al, 2021, p. 10). Therefore, the CRA aims to (European Commission, 2022b, p. 96):

Establish "security by design" for PDEs by requiring higher levels of confidentiality, integrity and availability;

Ensure "security support" for the whole life-cycle of the PDE by requiring mechanisms for updates and reporting vulnerabilities;

Foster "transparency of security information" by requiring the identification of dependencies and vulnerabilities, including the composition of software used and supply-chain-related information.

With that, the CRA affects all market participants involved in PDE supply chains: manufacturers (Art. 13), importers (Art. 19), distributors (Art. 20), and FOSS stewards (Art. 24).[15] Depending on their role and responsibility within the supply chain, these economic actors will have to fulfil several obligations before and while they place products on the market. Manufacturers bear the largest number of obligations as they are assumed to form the beginning of the supply chain, thus typically having the greatest influence on the conception, design, and development of their products (Burri and Zihlmann, 2023, p. 29). Some examples of obligations for manufactur-

15 The definition of FOSS Stewards and their obligations are detailed in Section 6.

ers include (Art. 13 and following provisions): they should ensure appropriate levels of cybersecurity by design and avoid delivering products with known exploits; they are also expected to adequately handle vulnerabilities throughout a product's life cycle, conduct due diligence and conformity assessments, and comply with reporting obligations. Importers and distributors are assigned a *watchdog* function by being permitted only to import or distribute products that meet the essential cybersecurity requirements outlined by the Regulation (Burri and Zihlmann, 2023, p. 36). They also should report vulnerabilities expeditiously if they become aware of them. However, if an importer or distributor modifies products or uses its own trademark, manufacturer obligations will apply (Art. 15).

The material scope of the CRA refers to PDEs – any commercialised product in the EU containing digital elements (Art. 2) – end-devices, such as laptops, smartphones, routers, cameras, sensors; software, including operating systems, mobile apps, video games; and components, such as chips, video cards, and software libraries. AI systems classified as high risk[16] are also included (Art. 12).[17] PDEs are classified in two groups based on their level of risk (Arts. 7 and 8), and subject to less or more stringent obligations ranging from a simple cybersecurity self-assessment to a third-party conformity assessment. Exceptions include products covered by sector-specific legislation, such as medical, aviation, and military devices. The underlying logic is that horizontal cross-sector overarching legislation will help significantly reduce products' attack surfaces by implementing a systematic approach to cybersecurity, such as security by design, conformity assessments, transparency obligations, and standard harmonisation (Georgiev et al, 2021, p. 10).

Compliance monitoring will be done by the European Commission, ENISA, and market surveillance authorities (Art. 52). The EU Member States shall be responsible for applying penalties (Art. 64). Non-compliance

16 The AI Act classifies AI according to its risk. Unacceptable risk is prohibited (e.g., social scoring systems and manipulative AI), while the law addresses mostly high-risk AI systems. Limited risks are subjected to transparency obligations (e.g., chatbots), and minimal risks are not regulated (e.g., AI in videogames). High-risk AI systems are those which can significantly impact individuals' rights and safety, such as systems used in critical infrastructures, employment processes, or law enforcement. See Section 2 of the AI Act (Regulation (EU) 2024/1689).

17 Products falling under the scope of the CRA which are eventually classified as high-risk AI systems according to Art. 6 of the AI Act shall comply with the essential requirements of the CRA (Recital 51).

may result in fines of up to 15 million EUR or 2,5% of the company's annual turnover.

The CRA aims to reach social goals, such as reducing cybercrime, increasing data protection and privacy, raising the population's overall awareness level, and creating a new market for cybersecurity-trained specialists (European Commission, 2022b, p. 69). However, admittedly, the 2022 Proposal was unable to capture some of the complexities of software development in open environments. The 2022 Proposal addressed FOSS, misapplying liability and compliance burdens onto those who could not reasonably be expected to deal with them. The analysis in the next section shows how the CRA affects FOSS, and how the rich debates during the legislative phase shaped a completely different result in the final approved version of the law.

6. The challenge of regulating FOSS cybersecurity

Considered by some to be the most impactful driver of innovation in the world today (Herstatt and Ehls, 2015), FOSS emerged as an idealistic movement to become a foundational element of the economy of the Digital Age (Benkler, 2006) and its notion of democracy (Foletto, 2021). Technically, FOSS refers to licensed source code guaranteeing the *four freedoms* to use, study, share, and improve the source code of a computer program.[18] From software running in devices, such as drivers, operating systems, apps, and embedded software of IoT devices, to software running less obviously in servers, digital libraries, APIs, operating system kernels, and encryption and security applications, FOSS has become a critical element of up to 90% of the software developed today (Nagle et al, 2022, p. 4). FOSS differs from proprietary software in its licensing. When a license does not grant these four freedoms, the software is considered proprietary (FSFE, 2020). In comparison with proprietary security by obscurity, where the details or mechanisms of a system are concealed and cannot be openly discovered and fixed, the open and transparent approach of FOSS is generally highly regarded due to the benefits of responsible disclosure and collaborative repair (NIST, 2008, p. 15; Smith, 2012; Norwood, 2023). Nevertheless,

18 The CRA follows this traditional definition in Art. 3 (40a): "'free and open-source software' means software the source code of which is openly shared and which is made available under a free and open-source license which provides for all rights to make it freely accessible, usable, modifiable and redistributable".

open environments where FOSS operates still have their own challenges. Hendrick and Mckeay (2022) listed the following:

> **Diversity of approaches**: FOSS communities can vary significantly in their development of practices and techniques to reduce the risk of defects in code, or to respond quickly and safely when one is discovered by others;
> **Security as low priority**: Organisations have been negligent in managing security of their software dependencies, opening more surface attack possibilities. Smaller FOSS organisations and communities bear disproportionate risks due to the lack of security policies covering FOSS;
> **Slow responses**: Depending on the project's organisation and staffing, responsive actions to fix vulnerabilities can take months with open review processes.

Nagle et al (2022) added:

> **Lack of security review**: Although FOSS benefits from transparent and open review for vulnerabilities, and their collaborative repair, not all FOSS projects are regularly reviewed equally. Vulnerabilities in widely used projects with smaller maintainer bases can remain unnoticed;
> **Lack of standardisation**: The lack of standardised software component naming schemas as a time-delaying issue mean that organisations are unable to share such information with each other on a large scale;
> **Versioning challenges**: Software versioning issues create incompatibilities in supply chains when organisations maintain internal versions of a package and do not contribute their changes back to the upstream repository;
> **Legacy technology**: FOSS, similarly to proprietary software, suffers from persistent legacy technology. As technology (both software and hardware) ages, it loses support. The number of developers working to ensure updates – including feature improvements, as well as security and stability updates – decreases over time;
> **Lack of human capacity**: Heavy reliance upon individual developers has legal, bureaucratic, and security consequences, as individuals may have fewer protections than companies. To illustrate, Koebler (2024) reported that bullying against individual developers can also impact volunteer-led projects when malicious actors conduct long campaigns in contribution processes to introduce vulnerabilities.

Since the CRA comprehensively affects digital products, the law has deep implications for FOSS. The CRA's impact assessment concluded that, in 2019 alone, investments in FOSS surpassed 1 billion euros, and small and micro enterprises could attribute over half their revenues to FOSS (European Commission, 2022b, p. 30). The software industry in the EU is almost entirely composed of small and medium-sized enterprises (SMEs), the vast majority of which (94%) are micro enterprises with fewer than nine employees (European Commission, 2022b, p. 29). Against this background, the European Commission's 2022 Proposal established an exception for FOSS in Recital 10: "in order not to hamper innovation or research, free and open-source software developed or supplied outside the course of a commercial activity should not be covered by this Regulation. [...] In the context of software, a commercial activity might be characterized not only by charging a price for a product, but also by charging a price for technical support services [...]".

However, the proposed distinction made for "commercial activity" prompted fierce criticism from some FOSS organisations about the potential chilling effects caused by liability consequences imposed on individuals and not-for-profit entities developing, curating, and distributing FOSS (Phipps, 2023). The core of the complaints deemed the EC's Proposal to disrupt the FOSS ecosystem by deterring volunteer contributors with strict liability regimes and compliance overload, affecting the entire software industry (Phipps, 2023). Demands highlighted the role of hobbyists, volunteers, and developer communities contributing to critical FOSS projects on a non-commercial basis. For instance, those receiving micro donations or small financial contributions for project maintenance would unduly and disproportionately bear the same level of responsibility and compliance costs as companies and corporations commercialising software (FSFE, 2023). Indeed, development models involving FOSS approaches cybersecurity differently from proprietary ones. FOSS is produced in a decentralised and distributed manner, meaning that there is no central authority to ensure quality and maintenance (Hendrick and Mckeay, 2022). FOSS is provided at zero cost to the consumer, decoupling its intrinsic value from its sale price. The huge quantity of FOSS systems made publicly available at no cost supports multi-billion-euro ecosystems (Milinkovich, 2023). Against this backdrop, although diverse FOSS stakeholders were displeased by the solution proposed for "commercial activity", they acknowledged the need for such a law, recognising that FOSS-related cybersecurity suffered from deregulation (Phipps, 2023). For instance, security incidents that affected

the entire FOSS industry, such as SolarWinds and Apache Log4j, have demonstrated the urgent need for improvement (Alkhadra et al, 2021; Feng and Lubis, 2022).

The following two years of the legislative process were marked by a transition to an updated regulatory attitude towards FOSS. While some civil-society and consumer-protection organisations supported the role of regulation to enhance cybersecurity as a public good, corporate-oriented deregulatory rhetoric was a source of concern by demanding the full exclusion of liability regimes (BEUC, 2022; Sander, 2024). The dialectical exchange during the Trilogues ultimately led to the incorporation of substantial changes that addressed concerns over exclusions and carved out specific roles and new legal constructions to address developer liabilities (Aertsen, 2024). The debates focused on improving clarity in terms of the liability of contributors acting outside of commercial activities (Art. 16 of the Proposal). Imposing stricter liability regimes on small or non-profit entities would undermine the consolidated logic of FOSS developers providing the software for free to the public, but accepting no liability or provision of warranty for its use. Since individual developers still represent the majority of the workforce in FOSS projects, the chilling effect could be tragic (FSFE, 2023). FOSS stakeholders demanded that businesses commercialising software and significantly profiting from the code should be the ones to bear liability for security flaws and provide warranties to their customers (Phipps, 2023). The incorporation of such demands substantially changed the structure of the law. If the CRA Proposal FOSS was timidly mentioned in Recital 10, the term now appears 57 times in the official text, permeating 10 Recitals and 13 Articles (Regulation (EU) 2024/2847). The applicability of the CRA to commercialised FOSS was clarified, and "FOSS Stewards" as a new regulatory category for organisations providing sustained support for the development of FOSS products was introduced.

The scope of application is explained in Recital 18:

> In relation to economic operators that fall within the scope of this Regulation, only free and open-source software made available on the market, and therefore supplied for distribution or use in the course of a commercial activity. The mere circumstances under which the product with digital elements has been developed, or how the development has been financed, should therefore not be taken into account when determining the commercial or non-commercial nature of that activity. More specifically, [...] to ensure that there is a clear distinction between the de-

> velopment and the supply phases, the provision of free and open-source software products with digital elements that are not monetised by their manufacturers is not considered a commercial activity.

To address the specific nuances of the FOSS industry, the legislators proposed a new "light-touch and tailor-made regulatory regime" of FOSS Stewards. Recital 19 provides a verbose explanation justifying the novel institution, mentioning that:

> Taking into account the importance for cybersecurity of many products with digital elements qualifying as free and open-source software that are published, but not made available on the market within the meaning of this Regulation, legal persons who provide support on a sustained basis for the development of such products which are intended for commercial activities, and who play a main role in ensuring the viability of those products (open-source software stewards), should be subject to a light-touch and tailor-made regulatory regime. Open-source software stewards include certain foundations as well as entities that develop and publish free and open-source software in a business context, including not-for-profit entities. [...] Given that the light-touch and tailor-made regulatory regime does not subject those acting as open-source software stewards to the same obligations as those acting as manufacturers under this Regulation, they should not be permitted to affix the CE marking to the products with digital elements whose development they support.

FOSS stewards are counterparts to manufacturers who ship products to market. They play an essential role in enabling manufacturers to deliver their products, but are subject to fewer requirements. Art. 3 (14) defines a FOSS Steward as: "a legal person, other than a manufacturer, that has the purpose or objective of systematically providing support on a sustained basis for the development of specific products with digital elements, qualifying as free and open-source software and intended for commercial activities, and that ensures the viability of those products". The obligations of FOSS Stewards differ from manufacturers (Art. 24): the former should develop cybersecurity policies for FOSS projects, handle vulnerabilities, help report incidents, and cooperate with market surveillance authorities to mitigate the cybersecurity risks posed by a PDE qualifying as FOSS. The CRA also allows the Commission to further establish voluntary security attestation programmes for FOSS developers and users to assess conformity with the CRA (Art. 25, Art. 32 (5)). The monitoring of FOSS Stewards'

activities should be done by market surveillance authorities (Art. 52 (3)). In case FOSS Stewards are not compliant with the law, corrective actions should be undertaken by such authorities. However, the CRA has excluded FOSS Stewards from administrative fines when the law is infringed (Recital 120 and Art. 64 (10b)).

In sum, the clarification of the liability regime and the introduction of FOSS Stewards reflect the EU's deeper understanding of how FOSS collaborative environments function. However, the practical implementation of the law will still face relevant challenges in relation to FOSS, especially involving different standardisation efforts related to conformity assessments, security policies and procedures, supply chain risk management (e.g., software bills of materials), documentation, and reporting (European Commission, 2024).

7. Conclusion and future research

As the old adage reminds us: *with great power comes great responsibility*. The ambitious CRA has a long way to go to accomplish its desired effect of raising the cybersecurity bar for digital markets. As discussed in the first sections of this chapter, cybersecurity is a multidisciplinary subject that cannot approached simplistically. Fundamental rights and values should be balanced in the process of increasing security measures in the digital society to improve and eliminate the contradictions of surveillance capitalism. Cybersecurity should be an instrument with which to promote the common good (Bendiek et al, 2017), and its effects across data protection, platform regulation, and consumer protection should conform to democratic principles. The CRA is inserted in a regulatory momentum that confront corporate power. As seen, market forces alone have not been able to promote safer and more secure digital environments. This historical experience should not be dismissed when corporate pressure defies reasoning that privileges consumer protection, digital commons, and human rights.

This chapter has served as an introduction to the CRA and focused on some of the history that led to its creation. It leaves now as a follow-up task the analysis of its implementation, but with a caveat: as has happened with other large and far-reaching legislation, its enforcement can be more challenging than the legislative process itself, and expectations should be adjusted accordingly. Regulators will struggle to make sense of the solutions proposed by affected parties, prompting strict monitoring (especially from

civil society) to confirm whether the interests of consumers and citizens are being prioritised. As concluded in the preceding section, the regulatory interaction with FOSS stakeholders reveals how open innovation depends on complex intricate dynamics that escape the traditional classifications of industrial economic actors (Phipps, 2023a). Volunteers, not-for-profit communities, and non-commercial actors are frail key players in environments that are highly exposed to corporate power and domination (Birkinbine, 2020; Brazeal, 2024). Such fragility impacts cybersecurity and will require special care and attention from policymakers.

Acknowledgments

This study was enriched by the invaluable contribution of several people. I am grateful to Elisabetta Biasin, Alexander Sander and Carlo Piana for their insights and comments. I thank the participants of the 2024 Workshop "Digital Decade: How the EU shapes digitalisation research" at the Weizenbaum Institute who interacted and provided feedback on a previous version of this paper. I am grateful to Prof. Dr. Christoph Rademacher and Prof. Dr. Jyh-An Lee for allowing me to present and discuss the outcome of this research at the Waseda University in Tokyo. My appreciation is also extended to Richard Schmeidler for his thorough and meticulous volunteer proofreading. Mariam Sattorov's compilation of EU legislation and literature review was instrumental, for which I am sincerely appreciative. I thank also the reviewers, the official proofreader and the editors, in particular Marie-Therese Sekwenz and Rita Gsenger, who dedicated time and expertise to improving this paper. Any inconsistency and imprecision in the text is my sole responsibility.

References

ACM et al (2017) *Cybersecurity curricula 2017: curriculum guidelines for post-secondary degree programs in cybersecurity*. ACM, IEEE, AIS SIGSEC, IFIP WG [Online], 11 August. Available at: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf (Accessed: 11 April 2024).

Aertsen, M. (2024) *What I learned in Brussels: the Cyber Resilience Act*. NLnet Labs [Online]. Available at: https://blog.nlnetlabs.nl/what-i-learned-in-brussels-the-cyber-resilience-act/. (Accessed: 1 May 2024).

Alkhadra, R., Abuzald, J. and AlShammari, M. (2021) 'Solar winds hack: in-depth analysis and countermeasures', in *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, pp. 1–7.

Apache Foundation (2023) *Save open source: the impending tragedy of the Cyber Resilience Act* [Online]. Available at: https://news.apache.org/foundation/entry/save-open-source-the-impending-tragedy-of-the-cyber-resilience-act (Accessed: 9 May 2024).

Aslan, A. and Samet, R. (2020) 'A comprehensive review on malware detection approaches', *IEEE Access*, 8, pp. 6249–6271.

Barlow, J. (1996) *A declaration of the independence of cyberspace*. Electronic Frontier Foundation [Online]. Available at: https://www.eff.org/cyberspace-independence (Accessed: 1 May 2024).

Bendiek, A., Bossong, R. and Schultze, M. (2017) *The EU's revised cybersecurity strategy*. SWP Comments [Online]. Available at: https://www.swp-berlin.org/publications/products/comments/2017C47_bdk_etal.pdf (Accessed 9 May 2024).

Benkler, Y. (2006) *The wealth of networks: how social production transforms markets and freedom*. New Haven: Yale University Press.

BEUC (2022) *Cyber Resilience Act: cybersecurity of digital products and ancillary services. BEUC response to public consultation*. BEUC [Online]. Available at: https://www.beuc.eu/position-papers/cyber-resilience-act-cybersecurity-digital-products-and-ancillary-services (Accessed: 1 May 2024).

Birkinbine, B. (2020) *Incorporating the digital commons: corporate involvement in free and open source software*. London: University of Westminster Press.

Brazeal, F. (2024) *The threat to open source comes from within*. Good Tech Things [Online]. Available at: https://newsletter.goodtechthings.com/p/the-threat-to-open-source-comes-from (Accessed: 11 April 2024).

Burri, M. and Zihlmann, Z. (2023) 'The EU Cyber Resilience Act – an appraisal and contextualization', *Zeitschrift für Europarecht (EuZ)*, 2, pp. 2–37.

Bygrave, L.A. (2024) 'The emergence of EU cybersecurity law: a tale of lemons, angst, turf, surf and grey boxes', *Computer Law & Security Review*, 56, 106071 [Online]. Available at: https://doi.org/10.1016/j.clsr.2024.106071 (Accessed: 29 January 2025).

Carr, M. and Tanczer, L. (2018) 'UK cybersecurity industrial policy: an analysis of drivers, market failures and interventions', *Journal of Cyber Policy*, 3(3), pp. 430–444.

Chiara, G. (2022) 'The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements', *International Cybersecurity Law Review*, 3, pp. 255–272.

Christen, M., Gordjin, B. and Loi, M. (eds.) (2020) *The ethics of cybersecurity*. London: Springer Nature.

Chung, J. (2017). 'Critical infrastructure, cybersecurity, and market failure', *Oregon Law Review*, 96, pp. 441–474.

'Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e), and (f), of that Directive' (2022) *Official Journal* L 7, 12 January, pp. 6–10 [Online]. Available at: http://data.europa.eu/eli/reg_del/2022/30/oj (Accessed: 29 January 2025).

Computer Security Resource Center (no date) *attack surface* [Online]. Available at: https://csrc.nist.gov/glossary/term/attack_surface (Accessed: 29 January 2025).

'Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products' (1985) *Official Journal* L 210, 7 August, pp. 29–33 [Online]. Available at: http://data.europa.eu/eli/dir/1985/374/oj (Accessed: 1 May 2024).

Council of Europe (2001) *Convention on Cybercrime. European Treaty Series – No. 185*. Council of Europe [Online]. Available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention (Accessed: 11 April 2024).

Crémer, J., Montjoye, Y. and Schweitzer, H. (2019) *Competition policy for the digital era*. European Commission Publications Office [Online]. Available at: https://data.europa.eu/doi/10.2763/407537 (Accessed: 5 May 2024).

CVE (no date) Process [Online] Available at: https://www.cve.org/About/Process (Accessed: 29 January 2025).

DeNardis, L. (2020) 'Cyber-physical security' in Denardis, L. (ed.) *The internet in everything: freedom and security in a world with no off switch*. New Haven: Yale University Press, pp. 93-131.

'Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC' (2014) *Official Journal* L 153, 22 May, pp. 62–106 [Online]. ELI: http://data.europa.eu/eli/dir/2014/53/oj (Accessed: 5 May 2024).

'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) *Official Journal* L 194, 19 July, pp. 1–30 [Online]. ELI: http://data.europa.eu/eli/dir/2016/1148/oj (Accessed: 5 May 2024).

'Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code. Recast. Text with EEA relevance' *Official Journal* L 321, 17 December, pp. 36–214 [Online]. ELI: http://data.europa.eu/eli/dir/2018/1972/oj (Accessed: 05.05.24).

'Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)' (2022) *Official Journal* L 333, 27 December, pp. 80–152 [Online]. ELI: http://data.europa.eu/eli/dir/2022/2555/2022-12-27 (Accessed: 11 April 2024).

ENISA (2011) *The working group contribution, economics of security: facing the challenging*. ENISA [Online]. Available at: https://www.enisa.europa.eu/topics/risk-management/files/EoS%20Final%20report/view (Accessed 1 May 2024).

ENISA (2015) *Good practice guide on vulnerability disclosure: from challenges to recommendations*. ENISA [Online]. Available at: https://www.enisa.europa.eu/publications/vulnerability-disclosure (Accessed: 1 May 2024).

ENISA (2022) *Coordinated vulnerability disclosure policies in the EU*. ENISA [Online]. Available at: https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu (Accessed 1 May 2024).

ENISA (2023) *Good practices for supply chain cybersecurity*. ENISA [Online]. Available at: https://op.europa.eu/en/publication-detail/-/publication/866c8abe-1ba8-11ee-806b-01aa75ed71a1 (Accessed: 11 April 2024).

European Commission (2017) *State of the Union 2017 – cybersecurity: Commission scales up EU's response to cyberattacks*. European Commission [Online]. Available at: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_17_3193/IP_17_3193_EN.pdf (Accessed: 9 May 2024).

European Commission (2020) *Joint communication to the European Parliament and the Council: the EU's cybersecurity strategy for the digital decade. JOIN(2020) 18 final*. European Commission [Online]. Available at: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 (Accessed 9 May 2024).

European Commission (2021) *2030 digital compass: the European way for the digital decade. COM(2021) 118 final*. European Commission [Online]. Available at: https://commission.europa.eu/system/files/2023-01/cellar_12e835e2-81af-11eb-9ac9-01aa75ed71a1.0001.02_DOC_1.pdf (Accessed: 11 April 2024).

European Commission (2022) *Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending regulation (EU) 2019/1020. COM(2022) 454 final 2022/0272(COD)*. European Commission [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454 (Accessed: 11 April 2024).

European Commission (2022a) *Commission Staff Working Document. Impact Assessment Report. Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. COM(2022) 454 final, SEC(2022) 321 final, SWD(2022) 283 final. Part 1/3*. European Commission [Online]. Available at: https://ec.europa.eu/newsroom/dae/redirection/document/89545 (Accessed: 11 April 2024).

European Commission (2022b) *Commission Staff Working Document. Impact Assessment Report. Annexes to the Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. COM(2022) 454 final, SEC(2022) 321 final, SWD(2022) 283 final. Part 2/3*. European Commission [Online]. Available at: https://ec.europa.eu/newsroom/dae/redirection/document/89546 (Accessed: 11 April 2024).

European Commission (2022c) *Proposal for a Directive of the European Parliament and of the Council on liability for defective products. COM(2022) 495 final 2022/0302(COD)*. EUR-Lex [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0495 (Accessed: 5 January 2024).

European Commission (2024) *Draft on the Commission Implementing Decision on standardisation request to European Standards Organisations in support of Union policy on cybersecurity requirements for products with digital elements. Notification under Article 12 of Regulation (EU) No 1025/2012*. European Commission [Online]. Available at: https://ec.europa.eu/docsroom/documents/58974. (Accessed 23 May 2024)

European Union (2013) *Cybersecurity strategy of the European Union: an open, safe and secure cyberspace (JOIN/2013/01 final)*. EDPS [Online]. Available at: https://www.edps.europa.eu/data-protection/our-work/publications/opinions/cyber-security-strategy-european-union-open-safe-and_en (Accessed: 5 May 2024).

European Union (2023) *European Declaration on digital rights and principles for the digital decade 2023/C 23/01. Official Journal* C 23, 23 January, pp. 1–7 [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001. (Accessed: 11 April 2024)

Feil, R. and Nyffenegger, L. (2008) 'Evolution of cross site request forgery attacks', *Journal in Computer Virology*, 4(1), pp. 61–71.

Feng, S. and Lubis, M. (2022) 'Defense-in-depth security strategy in log4j vulnerability analysis', in *2022 International Conference Advancement in Data Science, E-learning and Information Systems (ICADEIS)*, pp. 1–4.

Foletto, L. (2021) *A cultura é livre: uma história da resistência antipropriedade*. São Paulo: Autonomia Literária [Online]. Available at: https://rosalux.org.br/wp-content/uploads/2021/03/aculturaelivre-1.pdf (Accessed: 19 May 2024).

FSFE (2020) *What is free software*. Free Software Foundation Europe [Online]. Available at: https://fsfe.org/freesoftware/ (Accessed: 15 April 2024).

FSFE (2023) *CRA & PLD: EU: proposed liability rules will harm free software*. Free Software Foundation Europe [Online]. Available at: https://fsfe.org/news/2023/news-20230323-01.html (Accessed: 11 April 2024).

FSFE (2023a) *Router Freedom Survey Report – the end-user perspective on freedom of terminal equipment in Europe*. Free Software Foundation Europe [Online]. Available at: https://download.fsfe.org/routers/rf-survey-report-2023.pdf. (Accessed: 11 April 2024)

Fuster, G. and Jasmontaite, L. (2020) 'Cybersecurity regulation in the European Union: the digital, the critical and fundamental rights' in Christen, M., Gordjin, B. and Loi, M. (eds.) *The ethics of cybersecurity*. London: Springer Nature, pp. 97–115.

Georgiev, S. et al (2021) *Study on the need of cybersecurity requirements for ICT products – No. 2020-0715 Final Study Report*. Luxembourg: Publications Office of the European Union.

Grady, F. and Parisi, F. (2006) *The law and economics of cybersecurity*. Cambridge: Cambridge University Press.

Grotto, J. and Schallbruch, M. (2021) 'Cybersecurity and the risk governance triangle', *International Cybersecurity Law Review*, 2, pp. 77–92. Available at: https://doi.org/10.1365/s43439-021-00016-9 (Accessed: 11 April 2024).

Guiora, N. (2017) *Cybersecurity: geopolitics, law, and policy*. Abingdon: Routledge.

Hendrick, S. and Mckeay, M. (2022) *Addressing cybersecurity challenges in open source software*. Report from Linux Foundation & Snyk [Online]. Available at: https://www.linuxfoundation.org/research/addressing-cybersecurity-challenges-in-open-source-software (Accessed: 11 April 2024).

Hermanowski, D. (2015) 'Open source security information management system supporting it security audit', *2015 IEEE 2nd International Conference on Cybernetics*, pp. 336–341.

Herrmann, D. and Pridöhl, H. (2020) 'Basic concepts and models of cybersecurity' in Christen, M., Gordjin, B., and Loi, M. (eds.) *The ethics of cybersecurity*. London: Springer Nature, pp. 11-44.

Herstatt, C. and Ehls, D. (2015) *Open source innovation: the phenomenon, participant's behaviour, business implications*. Abingdon: Routledge.

Hypernormalisation (2016) Directed by Adam Curtis [Documentary]. London: BBC Documentary. Available at: https://www.bbc.co.uk/programmes/p04b183c (Accessed: 19.04.2024).

Ishikawa, T. and Kryvoi, Y. (eds.) (2023) *Public and private governance of cybersecurity: challenges and potential*. Cambridge: Cambridge University Press.

Koebler, J. (2024) *Bullying in open source software is a massive security vulnerability*. 404 Media [Online]. Available at: https://www.404media.co/xz-backdoor-bullying-in-open-source-software-is-a-massive-security-vulnerability/ (Accessed 11 April 2024).

Kryvoi, Y. (2023) 'Responding to public and private cyberattacks: jurisdiction, self-defence, and countermeasures' in Ishikawa, T. and Kryvoi, Y. (eds.) *Public and private governance of cybersecurity: challenges and potential*. Cambridge: Cambridge University Press.

Lasota, L. (2023) 'Regulating corporate behaviour in digital ecosystems: increasing fairness and contestability of digital markets with free software', *Toward Green, Inclusive, and Digital Growth* [Online]. Available at: https://doi.org/10.26493/978-961-293-306-7 (Accessed: 11 April 2024).

Lemke, T. (2014) 'The risks of security: liberalism, biopolitics, and fear' in Lemm, V. and Vatter, M. (eds.) *The government of Life: Foucault, biopolitics, and neoliberalism*. New York: Fordham University Press, pp. 59-74.

Mantelero, A. (2022). *Beyond data: human rights, ethical and social impact assessment in AI*. The Hague: Springer.

Meneghello, F. et al. (2019) 'IoT: internet of threats? A survey of practical security vulnerabilities in real IoT devices', *IEEE Internet of Things Journal*, 6(5), pp. 8182–8201.

Milinkovich, M. (2023) *Cyber Resilience Act: good intentions and unintended consequences*. Eclipse Foundation [Online]. Available at: https://blogs.eclipse.org/post/mike-milinkovich/cyber-resilience-act-good-intentions-and-unintended-consequences (Accessed 11 April 2024).

Moore, R, (2013) 'Standardisation: a tool for addressing market failure within the software industry', *Computer Law & Security Review*, 29(4), pp. 413–429.

Mugarza, I., Flores, J.L., Montero, J.L. (2020) 'Security issues and software updates management in the Industrial Internet of Things (IIoT) era', *Sensors*, 20(24), 7160 [Online]. Available at: https://doi.org/10.3390/s20247160 (accessed: 29 January 2025).

Nagle, F. et al (2022) *Census II of free and open source software – application libraries*. The Linux Foundation and The Laboratory for Innovation Science at Harvard [Online]. Available at: https://www.linuxfoundation.org/tools/census-ii-of-free-and-open-source-software-application-libraries (Accessed 11 April 2024).

Newitz, A. (2013) *The bizarre evolution of the word "cyber"*. Gizmodo [Online]. Available at: https://gizmodo.com/today-cyber-means-war-but-back-in-the-1990s-it-mean-1325671487 (Accessed: 23 April 2024).

NIST (2008) *Guide to general server security: recommendations of the National Institute of Standards and Technology*. National Institute of Technology and Standards [Online], v.800-123. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf (Accessed: 19 May 2024).

NIST (2012) *Guide for conducting risk assessments*. National Institute of Technology and Standards [Online]. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (Accessed: 1 May 2024).

Norwood, D. (2023) *Debian public statement about the EU Cyber Resilience Act and the Product Liability Directive*. Bits from Debian [Online]. Available at: https://bits.debian.org/2023/12/debian-statement-cyber-resillience-act.md.html (Accessed: 1 May 2024).

OWASP (2019) *API security top 10 2019: the ten most critical API security risks*. The Open Worldwide Application Security Project [Online]. Available at: https://owasp.org/API-Security/editions/2019/en/dist/owasp-api-security-top-10.pdf (Accessed: 11 April 2024).

OWASP (2020) *OWASP Vulnerability Management Guide (OVMG)*. The Open Worldwide Application Security Project [Online]. Available at: https://owasp.org/www-project-vulnerability-management-guide/OWASP-Vuln-Mgm-Guide-Jul23-2020.pdf (Accessed: 1 May 2024).

OWASP (2025). *SQL Injection* [Online] Available at: https://owasp.org/www-community/attacks/SQL_Injection (Accessed: 29 January 2025).

Palmer, D. (2021) *Critical IoT security camera vulnerability allows attackers to remotely watch live video – and gain access to networks*. Zdnet [Online]. Available at: https://www.zdnet.com/article/critical-iot-security-camera-vulnerability-allows-attackers-to-remotely-watch-live-video-and-gain-access-to-networks/ (Accessed: 1 May 2024).

Papakonstantinou, V. (2022) 'Cybersecurity as praxis and as a state: the EU law path towards acknowledgement of a new right to cybersecurity?', *Computer Law & Security Review*, 44, 105653 [Online]. Available at: https://doi.org/10.1016/j.clsr.2022.105653 (accessed: 29 January 2025).

Paulsen, C. and Byers, R. (2019) *Glossary of key information security terms*. National Institute of Technology and Standards [Online]. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf (Accessed: 1 May 2024).

Payne, C. (2002) 'On the security of open source software', *Information Systems Journal*, 12, pp. 61–78.

Phipps, S. (2023) *The ultimate list of reactions to the Cyber Resilience Act*. Open Source Initiative [Online]. Available at: https://opensource.org/blog/the-ultimate-list-of-reactions-to-the-cyber-resilience-act (Accessed: 15 May 2024).

Phipps, S. (2023a) *What is the Cyber Resilience Act and why it's dangerous for open source*. Open Source Initiative [Online]. Available at: https://opensource.org/blog/modern-eu-policies-need-the-voices-of-the-fourth-sector (Accessed: 15 May 2024).

Porcedda, M. (2023) *Cybersecurity, privacy and data protection in EU law: a law, policy and technology analysis*. Oxford: Hart Publishing.

Powers, M. and Jablonski, M. (2015) *The real cyber war: the political economy of internet freedom*. Champaign: University of Illinois Press.

'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) *Official Journal* L 119, 4 May, pp. 1–88 [Online]. ELI: http://data.europa.eu/eli/reg/2016/679/oj (Accessed: 5 May 2024). 'Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC' (2017) *Official Journal* L 117, 5 May, pp. 1–175 [Online]. ELI: http://data.europa.eu/eli/reg/2017/745/oj (Accessed: 5 May 2024).

'Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU' (2017) *Official Journal* L 117, 5 May, pp. 176–332 [Online]. ELI: http://data.europa.eu/eli/reg/2017/746/oj (Accessed: 5 May 2024).

'Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (Text with EEA relevance)' (2018) *Official Journal* L 212, 22 August, pp. 1 [Online]. ELI: http://data.europa.eu/eli/reg/2018/1139/2024-12-01 (Accessed: 29 January 2025).

'Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166' (2019) *Official Journal* L 325, 16 December, pp. 1–40 [Online]. ELI: http://data.europa.eu/eli/reg/2019/2144/oj (Accessed: 1 May 2024).

'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) *Official Journal* L 151, 7.6.2019, pp. 15–69 [Online]. EI: http://data.europa.eu/eli/reg/2019/881/oj (Accessed: 1 May 2024).

'Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011' (2022) *Official Journal* L 333, 27 December, pp. 1–79 [Online]. ELI: http://data.europa.eu/eli/reg/2022/2554/oj (Accessed: 11 April 2024).

'Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC' (2023) *Official Journal* L 165, 29 June, pp. 1–102 [Online]. ELI: http://data.europa.eu/eli/reg/2023/1230/oj (Accessed: 11 April 2024).

'Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)' (2024) *Official Journal* L, 2024/1689, 12 July. [Online]. ELI: http://data.europa.eu/eli/reg/2024/1689/oj. (Accessed: 3 October 2024).

'Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)' (2024) *Official Journal* L, 2024/2847, 20 November [Online]. ELI: http://data.europa.eu/eli/reg/2024/2847/oj (Accessed: 24 December 2024).

Robles-Carrillo, M. (2023) 'The European Union strategy for cybersecurity' in Moura Vicente, D., de Vasconcelos Casimiro, S. and Chen, C. (eds.) *The legal challenges of the fourth industrial revolution*. London: Springer Nature, pp. 173-192.

Ruohonen, J. (2022) 'A review of product safety regulations in the European Union', *International Cybersecurity Law Review,* 3, pp. 345–366.

Ruohonen, J., Hyrynsalmi, S. and Leppänen, V. (2016) 'An outlook on the institutional evolution of the European Union cyber security apparatus', *Government Information Quarterly*, 33(4), pp. 746–756.

Salvaggio, S.A. and González, N. (2023) 'The European framework for cybersecurity: strong assets, intricate history', *International Cybersecurity Law Review*, 4, pp. 137–146.

Sander, A. (2024) *CRA & PLD liability rules and software freedom.* Conference talk at elLibre [Online]. Available at: https://propuestas.eslib.re/2024/charlas/cra-pld-liability-rules-software-freedom (Accessed: 25 May 2024).

Schreider, T. and Noakes-Fry, K. (2020) *Cybersecurity law, standards and regulations*. Brookfield: Rothstein Publishing.

Shirey, R. (2007) 'Vulnerability'. *Internet Engineering Task Force RFC 4949 Internet Security Glossary, Version 2* [Online]. Available at: https://datatracker.ietf.org/doc/html/rfc4949 (Accessed: 1 May 2024).

Shostack, A. (2014) *Threat modeling: designing for security.* Indianapolis: Wiley.

Smith, R. (2012) 'A contemporary look at Saltzer and Schroeder's 1975 design principles', *IEEE Security & Privacy*, 10(6), pp. 20–25.

Statista (2024) *Number of internet and social media users worldwide as of January 2024*. Statista [Online]. Available at: https://www.statista.com/statistics/617136/digital-population-worldwide/ (Accessed 1 May 2024).

Townsend, K. (2024) *Vulnerabilities CVE and NVD – A weak and fractured source of vulnerability truth*. SecurityWeek [Online]. Available at: https://www.securityweek.com/cve-and-nvd-a-weak-and-fractured-source-of-vulnerability-truth/ (Accessed 1 May 2024).

Van de Poel, I. (2020) 'Core values and value conflicts in cybersecurity: beyond privacy versus security' in Christen, M., Gordjin, B. and Loi, M. (eds.) *The ethics of cybersecurity*. London: Springer Nature, pp. 45–71.

Vedder, A. (2019) 'Safety, security and ethics' in Vedder, A. et al (eds) *Security and law. Legal and ethical aspects of public security, cyber security and critical infrastructure security*. Cambridge, Antwerp, Chicago: Intersentia, pp. 11-26.

Wang, Z. Sun, L. and Zhu, H. (2020) 'Defining Social Engineering in Cybersecurity,' in *IEEE Access*, v. 8 [Online]. Available at: https://ieeexplore.ieee.org/abstract/document/9087851 (Accessed: 31 January 2025).

Warner, M. (2012) 'Cybersecurity: a pre-history', *Intelligence and National Security*, 27(5), pp. 781–799.

Wikipedia (2025) *API* [Online]. Available at: https://en.wikipedia.org/wiki/API (Accessed: 29 January 2025).

Wikipedia (2025a) *Reverse engineering* [Online]. Available at: https://en.wikipedia.org/wiki/Reverse_engineering (Accessed: 29 January 2025).

Your Europe (2024) *CE marking* [Online]. Available at: https://europa.eu/youreurope/business/product-requirements/labels-markings/ce-marking/index_en.htm (Accessed: 29 January 2025).

Zuboff, S. (2019) *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. New York: PublicAffairs.