Information, Communication & Society

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/rics20

The regimes of ethical hacking: moral projects and the emergence of a market for vulnerability

David Bozzini

To cite this article: David Bozzini (06 May 2025): The regimes of ethical hacking: moral projects and the emergence of a market for vulnerability, Information, Communication & Society, DOI: 10.1080/1369118X.2025.2498683

To link to this article: https://doi.org/10.1080/1369118X.2025.2498683

INFORMATION, COMMUNICATION & SOCIETY
https://doi.org/10.1080/1369118X.2025.2498683

Routledge
Taylor & Francis Group

The regimes of ethical hacking: moral projects and the emergence of a market for vulnerability

David Bozzini

Department of Social Sciences, University of Fribourg, Fribourg, Switzerland

ABSTRACT

This article examines the historical evolution of ethical hacking and vulnerability disclosure practices from the 1990s to the present day. It analyzes three key disclosure regimes and their emergence: full disclosure, responsible/coordinated disclosure, and bug bounty programs. The full disclosure regime is characterized by an adversarial relationship between hackers and companies, with hackers publicly releasing vulnerability information to pressure companies to improve security. The responsible/coordinated disclosure regime formalizes collaboration between hackers and companies, introducing standards and policies to manage the disclosure of vulnerable information. Finally, the bug bounty regime established a market-based model of disclosure that partially commodified vulnerabilities and transformed ethical hacking into a form of gig work. The analysis reveals how these regimes while building upon existing models, enact distinct moral projects and govern interactions between hackers and companies. It highlights how ethical hacking has been transformed through processes of normalization, standardization, and economization and argues that these transformations resulted from complex interactions between hackers and companies shaped by broader socio-cultural trends and pre-existing practices rather than being the result of a simple co-optation by corporate interests. In doing so, this nuanced historical perspective on vulnerability disclosure regimes demonstrates how a political economy perspective contributes to developing a critical cybersecurity research agenda.

ARTICLE HISTORY
Received 22 April 2024
Accepted 23 April 2025

KEYWORDS
Hacking; cybersecurity; vulnerability; bug bounty; digital industry; socio-technical regime

From pranks to bounties: a historical tale of ethical hacking

Conventionally, the mention of a 'hacker' evokes crime rather than benevolence. However, hacker figures are manifold and one type – ethical hackers – has gained considerable visibility in recent years.[1] Ethical hacking refers to the act of searching for and reporting vulnerabilities to organizations in order to improve the security of their infrastructure or products. Vulnerability disclosure has become a crucial mechanism in cybersecurity, as it

CONTACT David Bozzini david.bozzini@unifr.ch

enables organizations to learn about existing flaws in their digital systems that could be maliciously exploited.

The idea that a team of hackers could probe computer systems by trying to break into them first appeared in the late 1960s (Hunt, 2012). 'Tiger teams' from the US Air Force and the Rand Corporation tested military time-sharing computers and over the years that followed, 'penetration testing' services would become increasingly widespread. If penetration testing can be seen as the first form of ethical hacking and a job opportunity for hackers, its model of vulnerability disclosure is limited, having no mechanism through which to accommodate unsolicited vulnerabilities, discovered outside of its authorized activities.

Focusing on the history of vulnerability disclosure, this article provides an understanding of the way in which unsolicited hacking has been transformed and integrated into the digital industry. With this intent, the article examines the models of disclosure that have been practiced since the mid-1980s, starting with the inception of 'full disclosure' to its crisis point, which set in motion 'responsible' and 'coordinated' disclosures in the 2000s, and finally the emergence of a market-led model of disclosure known as 'bug bounty,' which has thrived since the 2010s. These models didn't replace each other; rather, I argue, the modalities of disclosure have multiplied over the years via a number of different routes, with different kinds of norms, values and economic organization.

Each model of vulnerability disclosure can be understood as articulating a specific *socio-technical regime* that structures the interactions between hackers and the organizations whose software they probe. Inspired by literature on socio-technical transitions (Geels, 2002), a *disclosure regime* may be defined as a semi-coherent set of formal and informal values, norms, and rationalities that constitute the model of disclosure as well as its corresponding routines, institutions, regulations, and infrastructures. Notably, values, norms, and rationalities are semi-coherent in the sense that the regime's model is never 'stable and monolithic but subject to contestation and power battles by interested actors […].' (Fuenfschilling & Binz, 2018, p. 2). Values, such as security, transparency, efficiency or justice, are embedded differently in each disclosure regimes and delineate a specific moral project that set in motion '[…] more or less conscious efforts to categorize, normalize, and naturalize behaviors and rules that are not natural in any way' (Fourcade & Healy, 2007, p. 300). By acknowledging the existence of different moral projects, I concur with Coleman and Golub (2008) and Steinmetz (2016) about the existence of a multiplicity of hackers' ethics but, instead of locating moral projects in a hacking genre (for instance open source hacking, cracking or ethical hacking), I locate them in specific disclosure regimes. In other words, regimes of disclosure enact different moral projects to which hackers may align themselves, according to their own moral stance and circumstances. Each moral project promotes certain behaviors in line with regimes' goals such as promoting autonomy and managing reputation, enhancing collaboration and normalizing hacking or optimizing labor and information that are aligned with and justified by broader ideals and societal projects.

Through this analysis of disclosure regimes, I aim to illustrate the relevance and importance of a political economy perspective in developing a critical cybersecurity research agenda, examining how value and values are renegotiated through the changing landscape of security work. I argue that the most recent disclosure regime, the bug bounty regime, represents a new kind of market integration for ethical hacking. My

analysis expands the discussion of Delfanti and Söderberg (2018) and Söderberg and Maxigas (2022), who understand the marketization of hackers' practices as a partial and mutual co-evolution between hackers and digital industry. But instead of considering the market integration associated with bug bounties primarily as a subversion of previous moral projects, I emphasize its own moral project, and how it builds upon and coexists with other regimes.

Methodology

Two types of data collection have supported this research: first, an ongoing ethnography of bug bounty; and second, online research into the history of vulnerability disclosure. The data regarding bug bounties are of two types: semi-directed interviews and informal discussions with hackers, bug hunters and bug bounty managers in Europe and the US have been conducted during a dozen hacking events and conferences between 2018 and 2024, as well as during ethnographic research on the bug bounty programs of two Swiss companies in 2020 and 2024. This was complemented by qualitative manual data collection of online sources regarding bug bounties, mainly from bug bounty platforms and online IT magazines.

The starting point for my research on the history of vulnerability disclosure has been to document the shift from the antagonism between hackers and private companies associated with the full disclosure regime to the collaborative modus operandi of subsequent forms of disclosure. I followed the methodological technique of controversy mapping (Venturini, 2009) by first identifying relevant actors and events before gathering and analyzing texts, talks, tropes and rationales, until I reached data saturation.

Similar to Hellegren's study of crypto-discourse (2017), following controversies of vulnerability disclosure models entailed an open-ended search on a large number of online sites. Material that is still online in its original location was collected from company websites (e.g., Microsoft, SecurityFocus.com), news sites (e.g., New York Times, CNN), blogs (e.g., Schneier.com, porcupine.org), magazines (e.g., ZDNET News, PCworld.com), distribution lists archived on Seclists.org, and YouTube channels (e.g., Blackhat, DEFCON). For unavailable links, I resorted to the Wayback Machine (https://web.archive.org), which provides access to some webpages at different points in time.[2]

Despite the open-ended nature of this data collection, my reliance on intertextuality and only on internet records of what web historians call born digital and reborn digital data (Brügger, 2018) has induced at least two different biases: first, the large majority of collected materials were produced by US-based actors, but at least for the 1990s and the early 2000s, it is hard to deny that the US was a central location for both the public emergence of the ethical hacker scene and digital industry. The second bias is historical: relying on internet records has framed ethical hacking from the 1990s onwards, obscuring earlier vulnerability research practices such as penetration testing. Important datapoints have certainly been overlooked, either because of the absence of records online, or due to the initial entry points of the data collection I followed. Nevertheless, the material collected represents thick data, i.e., data densely interconnected, (Latzko-Toth et al., 2016) providing detailed descriptions and opinions about events, issues or processes at stake. Considering that the data is essentially discursive, the analyzed material only can give us partial and situated perspectives about how events, issues or processes

were unfolding in the past. Hence, the historical reconstruction in the following pages is the result of an interpretation that offers explanations of disclosure regimes but does not aim to provide a full historical series of causal inferences. The analytical concept of disclosure regimes provides a lens through which to make sense of the distinctive models, and to draw some conclusions about the relations between them.

Full disclosure regime

In the regime of full disclosure, hackers independently and publicly release all information pertaining to vulnerabilities they have found. The practice is often associated with a chivalresque figure of the hacker motivated by the desire to inform customers about the lack of security of the systems they use. Mudge, an American member of the hacking group 'The L0pht,' declared that they were making vulnerabilities public because 'Microsoft is shoving stuff down people's throats, and you don't have the ability to look and see how good it is'.[3] However, this figure of the valiant watchdog lies in the shadow of a more prosaic situation: in the early 1990s, companies were often unresponsive when hackers tried to notify them about vulnerabilities in their products.[4] Hackers justified publicizing vulnerability information as a way to force companies to acknowledge them and to fix the problems.[5] Many US hackers also felt that CERT-CC[6] – a US non-governmental institution in charge of coordinating emergency responses in the wake of major cyber-incidents and informing companies about vulnerabilities in their products – was not sufficiently pushing companies to fix identified flaws.[7] From this perspective, full disclosure was influenced by a confrontational relationship between hackers and the digital industry, as much as by more abstract ideological or moral principles such as opposition to the digital industry or capitalism at large.

Full disclosure took place online. The details of vulnerabilities were posted on public mailing lists like Bugtraq.[8] Bugtraq was founded in 1993 with the aim of providing a forum for discussions of vulnerabilities.[9] The popularity of these lists grew through the 1990s. By 2001, Bugtraq had 40,000 subscribers,[10] and hundreds of messages were posted every month. Such mailing lists created a loose community interested in vulnerability disclosure, and in addition to specific vulnerabilities, the full disclosure model itself was discussed, contested, and developed in these forums.

Full disclosure is predicated on three principles: an adversarial logic, transparency, and a gift economy. Vulnerability research and disclosure is adversarial at its core: it entails attacking a system to better defend it by reducing actionable flaws. Foundational to ethical hacking itself, the idea was enacted with penetration testing which has been practiced since the early 1970s (Hunt, 2012) and was promoted to a larger audience in 1993 when Farmer and Venema[11] published a paper entitled 'Improving the Security of Your Site by Breaking Into It' with the intention of raising awareness about security and promoting the use of SATAN,[12] a software application for testing a system for known vulnerabilities. In this sense, disclosing vulnerability information was considered to be a service offered to an imagined community of tech-savvy system administrators, who could use it to implement mitigations for weaknesses.

The principle of transparency is closely linked to the adversarial logic promoted by Farmer and Venema: to maximize the benefit for all and, consequently, to avoid the formation of potentially harmful groups of privileged actors, vulnerability information must

circulate widely. This principle often found expression in analogies between full disclosure and the free and open-source software movement:

> Full disclosure is in many ways akin to the open-source movement that's taking the computer world by storm. Open source allows for peer review, learning, and collaboration that leads to making better software. Full disclosure has similar goals. By making the details of vulnerability public, it seeks to educate and inform, and at the same time to provide a basis upon which to take further action.[13]

The practice of full disclosure was legitimated in various ways (to warn customers, to inform and educate system administrators, to pressure companies). The disclosure regime treated vulnerabilities as (ideally) freely circulating, as this also helped hackers to avoid being prosecuted for extortion. The absence of direct monetary rewards created a kind of 'gift economy' and associated moral stance. At the time, law enforcement crackdowns on illegal hacking activities were taking place[14] and growing public awareness of malicious hackers during the 1980s and early 1990s (Halbert, 1997) created the need for the articulation of a 'good' category of hacking unrelated to criminal activities or espionage. The absence of direct financial gain by unsolicited ethical hackers can be seen as an identity-oriented strategy to distinguish themselves from the ill-intentioned hacker. Thus, issues of morality, legality, and identity all contributed to the development of the first unsolicited vulnerability disclosure model as a gift economy.[15]

However, the gift economy implied in full disclosure should not eclipse other forms of benefit. If the reward wasn't financial, it was reputational. The publication of clever hacks and nasty exploits also became the means by which hackers competed for fame amongst themselves. Pranks, bravado, and mockery against companies became hackers' means of achieving glory.[16] For some, this would translate into opportunities for paid work. Hacking was presented as rebellious and contentious in the media but, as Goerzen and Coleman (2022) aptly suggest, full disclosure hackers could present themselves as 'good guys' who were committed to improving companies' digital security. This dynamic, however, did not promote a conducive environment for collaboration between hackers and the digital industry – to the contrary, it created conditions for antagonism.

The publicity generated by hackers demonstrating critical security flaws in widely distributed products garnered the attention of powerful actors. In 1998, the L0pht was invited to provide testimony on the state of digital security to the US Senate, where they famously acknowledged that they could easily turn off the Internet for the entire country in less than 30 minutes.[17] 'Security by spectacle,' as Goerzen and Coleman called the late full disclosure regime, entailed a form of 'bottom-up securitization' (Goerzen and Coleman, 2022, p. 64) in which hackers were able to outline and publicize a new type of threat to the emerging digital society.[18] Becoming more respectable, hackers involved in vulnerability disclosure gained a voice and were thus capable of reframing hacking as an important skillset (Goerzen and Coleman, 2022, p. 65). This step toward the professionalization of hacking is key to understanding how a new dialogue between hackers and companies would emerge in the early 2000s.

The full disclosure regime contained the seeds of its own eventual contestation. Between 1999 and 2001, many web defacements and viruses were engineered using information gained from full disclosure.[19] In other words, the full disclosure practice of publicizing vulnerabilities attracted new actors derogatorily termed 'script kiddies' by

hackers (Shepherd, 2003). These attacks pointed at an unavoidable problem: even if the company in question would fix the vulnerability there was an inevitable time delay before this was done, and as this became widely recognized, the practice of publishing exploit codes or hacking tools on mailing lists became increasingly difficult to morally justify.

Marcus Ranum, a hacker famous for developing cybersecurity defenses (including early firewalls and intrusion-detection systems), described the crisis in full disclosure stemming from script kiddies in a keynote speech at the Las Vegas Black Hat conference in July 2000.[20] For Ranum and several others, it was clear that the problems were of a social nature: the means of disclosing vulnerability information was due for a change[21] to prevent avoidable attacks and this meant establishing the conditions for more productive collaboration between hackers and companies. The debate around full disclosure would continue for several years and would see tensions between different moral viewpoints.[22] For instance, there were debates around the appropriate timing of disclosure (e.g., how long a company should be given to fix a vulnerability before information about it would be released publicly), what information to disclose (e.g., vulnerability only, vulnerability and exploit code), and the definition of 'the public' when it comes to vulnerability information (i.e., who gets what information and when) (Granick, 2005).

Ranum played an important role in publicising the 'script kiddies' crisis, and his arguments were also notable for framing the solutions in economic terms. He invited his peers to think in terms of cost–benefit analysis and incentivization mechanisms when it came to the practice of full disclosure.[23] As such reflexive understandings of hacking in economic terms gained traction around the turn of the century, we might associate the shift away from full disclosure as part of an increasing *economization* of hackers' practices.[24] Such processes of economization may have played a significant role in stabilizing the logics and values of a new disclosure regime at the beginning of the 2000s.

Responsible and coordinated disclosure regime

Ross Anderson and Bruce Schneier, two famous cryptographers, played a central role in problematizing digital security in economic terms, across both academic and practitioner communities. The former convened the first Workshop on Economics and Information Security (WEIS) in 2002, recalling recently that:

> When we started doing work on the economics of information security, 20 years ago, one of the first big problems that came up was responsible disclosure. Back in those days, people were split between the Bugtraq guys who wanted to disclose everything at once, and the company lawyers who want to keep everything quiet forever. And the current responsible disclosure regime has come out from that.[25]

Attempts to correct problems inherent in the practice of full disclosure emerged in the late 1990s. The seeds of responsible disclosure can be identified in hacker-authored disclosure policies produced to inform companies about what should be expected, should a vulnerability be found in their products. The earliest such policy that I identified is the NMRC policy published online in September 1999,[26] though the RFP policy[27] published in June 2000 is better known and more detailed. These policies stated that the hackers would refrain from publishing vulnerability information if companies agreed to acknowledge their notifications within a few days, develop realistic plans to address the

vulnerabilities, and negotiate their plans with the hackers who identified the vulnerability. This willingness to refrain from informing for a period of time tech-savvy fellows and system administrators who could be directly concerned about a vulnerability represented a major departure from the full disclosure practice and ideology. In a way, increased secrecy was the price hackers had to pay for companies to engage more collaboratively with them and to limit risks of 'avoidable' attacks. These policies as well as the responsible disclosure standards developed shortly thereafter were a means of limiting behavioral unpredictability by standardizing the expectations of both parties. However, the new disclosure regime did not take over wholesale. Full disclosure was still taking place in the early 2000s, and hackers could still resort to the public disclosure of vulnerability information if companies responded in an unsatisfactory manner.

The term 'responsible' has a clear moral connotation, and while full disclosure rhetoric had emphasized care for security technicalities, the main concern of responsible disclosure was social in nature. The emphasis was on facilitating collaboration between hackers and companies in setting a set of expectations about disclosures. The term 'responsible disclosure' was introduced by CERT-CC when it revised its vulnerability policy in October 2000, two months after Ranum's keynote speech,[28] to include a vulnerability information embargo period of 45 days, providing the company with an opportunity to develop a patch before the issue became widely known. The intention of the policy was 'to balance the need of the public to be informed of security vulnerabilities with the vendors' need for time to respond effectively […].' said Shawn Hernan, CERT-CC's team leader for handling vulnerabilities.[29] For many, it was no longer possible to ignore the negative outcomes of full disclosure. Furthermore, hackers and private companies found a common interest in keeping state involvement to a minimum, an incentive to address their antagonisms and to find solutions to their problems in order to retain their freedom to self-regulate.[30]

While the debate over the relevance of full disclosure was still raging, Microsoft entered the discussion through a provocative article[31] penned in 2001 by Scott Culp, the founder of the Microsoft Security Response Centre.[32] The article restated many points made by Ranum the year prior and was aligned with the basic communication rules supported by the hackers' disclosure policies mentioned above. With this article, Microsoft pushed for hackers to adopt more responsible behavior to avoid harm to users. Culp put three proposals on the table: first, the publication of exploit code should be avoided by default; second, to boost patch adoption, the publication of vulnerability information should occur around the time of the relevant patch's release; and third, to formulate an industry-wide standard for vulnerability disclosure policy, hackers should join a new coalition, the OIS (Organization for Internet Safety).

The OIS was founded one month after the publication of Culp's article and a standard proposal was submitted to the IETF[33] the year after. This proposal sought to increase effectiveness of disclosure, minimize the risks of and time required for vulnerability management, and mitigate antagonism between parties. Additional standards were drafted in the years that followed, including some by government lawyers and regulators.[34] This standardization occurred in the context of wider standardization in the field of digital security.[35] However, although the new model was built around transactions of information between hackers and companies, there was no provision for monetary rewards. Vulnerabilities were not treated in this disclosure regime as commodities to be purchased; they were treated as information to be handled carefully.

In this institutionalization process, codification became an important tool for big tech companies like Microsoft to influence disclosure's norms and surrounding narratives. In 2005, the company initiated the drafting of an ISO standard for vulnerability disclosure that was submitted in 2008 and ratified in 2014.[36] However, even before the ISO standard was published, Google and Microsoft would further revise their disclosure policies, and challenged the responsible disclosure regime. In 2010, Google published a blog post[37] raising several criticisms of responsible disclosure and raising their embargo period to 60 days. Just two days later, Microsoft renamed its standard process as 'coordinated vulnerability disclosure' (CVD).

The most significant change that Microsoft wanted to propose, however, pertained to control over 'how issues are addressed publicly.'[38] Like Google, Microsoft extended the patch-development period and thus postponed public disclosure, and since then the extension of pre-disclosure periods has become a common trend. Of course, the matter of what constitutes sufficient time to produce high-quality patches was not a new discussion.[39] What was new was that companies like Microsoft and Google exerted growing pressure to redefine the embargo time without consulting hackers and other actors as Microsoft previously did when they founded OIS. In other words, big tech companies – which had previously rejected the practice of disclosure – were now redefining the norms of vulnerability disclosure and positioned themselves as the new champions of vulnerability research by dedicating teams to searching for bugs in both their own products and those of other companies. These capacities were already in place at Microsoft in 2008,[40] and Google did something similar in founding its Project Zero in 2014.[41]

Bug bounty programs: the marketplace regime

An offensive market funneling vulnerability information to intelligence and law enforcement agencies has existed at least since the 1990s (Perlroth, 2021). As a defense measure, Netscape inaugurated a contest called bugs bounty in 1995 after several vulnerabilities were found on its browser and disclosed[42] in order to limit bad press (Ellis & Stevens, 2022, p. 33). The contest was discontinued in 1997 and no other company implemented similar initiative until Mozilla initiated a bug bounty program for its Firefox browser in 2004.[43] In the meantime, the responsible disclosure regime had emerged in 2000 and created the conditions for monetary transactions to play a greater role in the development of cyberdefense strategies in curbing the public release of vulnerabilities, and in developing institutional structures for collaboration between hackers and companies. In 2002, iDefense, a company providing 'comprehensive and actionable security intelligence' to its customers,[44] started paying hackers to postpone the public disclosure of their undisclosed vulnerability for at least one week[45] in order to sell exclusive information to its customers.[46],while the Zero Day Initiative (ZDI), another similar initiatives for vulnerability information, was founded by TippingPoint in 2005.[47] As Böhme (2006) noted, these initiatives were distinct from bug bounties: the buyers were not necessarily the company hacked but a club of subscribers (mainly government agencies and financial organizations).

Amounting sometimes to 10000 USD,[48] but still more modest than those offered by the established offensive market, the rewards of these initiatives attracted hackers selling vulnerability information to the offensive market who were frustrated by key

uncertainties.[49] Vulnerabilities were hard to price, and hard to demonstrate, without giving away the information being sold. Thus, a small group of hackers active in the offensive market started to participate to the initiatives of iDefense and ZDI at the time these companies began to organize the first Pwn2Own contest to publicize their business and to recruit more hackers while exerting renewed pressure on digital companies that could see their products hacked during the competition. What is particularly interesting to note about these initiatives is that their initiators and earliest contributors constituted a relatively small clique. Brokers, ZDI, iDefense staff, and hackers involved in 'Pwn2Own' were contributing to other initiatives as well (some of them also worked for US intelligence agencies): they constituted a dense network of actors interacting with one another.[50] This created an intermediary space between an established offensive market and the responsible disclosure practice, fomenting a debate on the possibility of a new kind of defensive market for vulnerabilities.

In 2009, three well-known hackers frustrated by both the shortcomings of the offensive market and the absence of disclosure rewards from companies decided to publicly speak out to encourage companies to pay them directly for vulnerability information. Dai Zovi, Sotirov, and Miller went onstage at the CanSecWest Conference, which was hosting 'Pwn2Own', with a placard reading 'No more free bugs.' At the same time, influential companies were ready to pay for vulnerability information to dissuade hackers from selling their discoveries to the offensive market and other buyers. Cyber incidents affecting major corporations, such as Operation Aurora at Google[51], may have increased their readiness to pay, while the success of Mozilla's bug bounty model for Firefox demonstrated an institutional form through which this commercial arrangement could be successful.

Many big tech companies began to adopt bug bounty programs in the 2010s. Google instituted its Vulnerability Reward Program in 2010, and Facebook developed its bug bounty program the following year. Microsoft followed the trend in 2013, and Apple embraced the idea in 2016. Bug bounty platforms emerged around the same time: Bugcrowd and HackerOne were founded in 2011 and 2012, respectively, hosting multiple companies' programs and gathering an online crowd of bug hunters ready to test their products and infrastructure. They have been key to publicizing the benefits of hacking to a wide range of companies across industrial sectors over the last decade.

This new model of disclosure represented a major shift from those preceding it, in particular by enabling companies to promote hacking on specific targets. Bug bounties are effectively initiatives managed by companies willing to buy vulnerability information from hackers (or, as they often refer to themselves, bug hunters) to improve the security of their products. In other words, the model turned the roles of parties upside down: while hackers had historically decided independently where to look for vulnerabilities, with bug bounties companies could now take the lead in defining the orientation of vulnerability research. In addition, as programs serve as formal invitations to hack and be rewarded for doing so, the model turned unsolicited hacking into solicited bug hunting. The monetary reward is based on the type and significance of the identified vulnerability, and hunters are paid a lump sum for a valid report – not a wage based on the time they put into their research. In the event that a valid vulnerability is reported more than once, only the hunter who submitted their report first is compensated.

Security economics presents bug bounty as an incentive mechanism for disclosure (Böhme, 2006) but they are more than that. They are complex governing instruments through which companies can manage the flow of vulnerability information and maintain a valuable reservoir of hackers at work. The two primary governing mechanisms are the scope of the program – scope being defined in terms of assets (e.g., subdomain, application, product) and the types of vulnerabilities the company is interested in – and a structure of monetary rewards attracting hunters but also limiting the submission of low value reports to avoid overloading the program team. As programs began to compete against one another, retaining the best hunters became a pressing concern, prompting companies to modify their policies, scopes, and rewards to remain attractive. Hacking events, special programs, invitations to social gatherings, and presentations on new programs at hacking conferences are now regularly organized by platforms for large tech companies to promote their bug bounty programs. In other words, the attitude of digital companies toward hackers radically changed: in the bug bounty regime, the technology companies are in control, even more so than in responsible disclosure, and hackers are considered a resource, to be managed through structured programs of incentives and reward.

Bug bounty platforms often present themselves as crowdsourced security operations involving thousands of individuals.[52] However, data on actual participation (Ellis et al., 2017) and interviews I conducted with program managers suggest that in fact a relatively small number of hunters submit the majority of paid bugs. Complex metrics used to rank hunters and their activities on the platform not only boosts competitiveness among bug hunters but also help managers to identify and retain promising and talented hunters. In the context of a perceived shortage of digital security experts, bug bounty programs are used as an instrument to shape a relevant and flexible workforce dedicated to company-specific goals.

Platforms have invested substantial energy and resources in building up online educational content to support bug bounty initiatives. Comparing these educational initiatives to the information-sharing practices among full disclosure hackers reveals a significant contrast: learning from specific vulnerability details and exploit code published on mailing lists has been replaced, for many new hackers, by learning from tutorials and commentaries. Bug bounty tutorials and other educational content contribute to the standardization of hacking beyond the definitions of any scopes, policies, or vulnerability disclosure standards by providing free online instructions and methodologies to hunt for vulnerabilities. This may indicate that through this new regime, hacking is becoming more accessible. Considering that bug bounty may serve as a training ground for novices, this could partially explain the statistics mentioned earlier (Ellis et al., 2017) indicating that few hunters submit valid reports relative to the overall number of hunters active in any given program. From this perspective, bug bounty programs, and by extension platforms, can contribute to the training of a hacker workforce exerting influence on values and behaviors related to researching and disclosing vulnerabilities.

The moral projects of ethical hacking

The history of vulnerability disclosure is a history of the transformation of ethical hacking into multiple co-existing regimes. Moreover, these regimes, saturated with norms,

provide a framework through which to understand the changing relationships between hackers and private companies. To these regimes correspond different moral projects each including a distinct set of values, practices, rules, and expectations for both hackers and companies toward vulnerability, information, and security.

The regime of full disclosure is characterized by an adversarial logic, stemming from the lack of incentives in the digital industry to invest in the production of more secure products (Anderson & Moore, 2006, p. 611; Bozzini, 2023). The adversarial attitude fueled reputational dynamics in the hackers' arena and eventually bolstered their visibility and relevance to digital security. However, pre-existing practices and values endorsed by hackers also played a part in the situation: on the one hand, transparency and curiosity were already embedded in a longstanding ethos of collaboration and information-sharing practices among computer hobbyists and software developers; on the other hand, adversarial logic and meritocratic values had been intrinsic to hacking since its inception in the 1970s. Its moral project is framed as a service to warn, inform and educate customers and pressure companies, making disclosed vulnerabilities commons, and defending liberal ideals such as freedom and autonomy.

Stemming from a crisis, the regime of responsible and coordinated disclosure did not only redefine norms and processes of disclosure (using economic language) but also codified and institutionalized them in policies and standards, formalizing collaboration and, ultimately, making vulnerability management more predictable to companies, which could, with the same stone, limit their reputational damage. The moral project emerging with this regime is tightly connected with what Foucault calls disciplinary normalization:

> Disciplinary normalization consists first of all in positing a model, an optimal model that is constructed in terms of a certain result, and the operation of disciplinary normalization consists in trying to get people, movements, and actions to conform to this model, the normal being precisely that which can conform to this norm, and the abnormal that which is incapable of conforming to the norm. (2008, p. 85).

The model of responsible disclosure is nothing more than collaboration and coordination between hackers ready (but maybe not yet willing) to disclose their hacks and the hacked companies. We see disciplinary power at play in redefining the elements of disclosure (e.g., time, information) and devising procedural sequences in the production of standards promoting compliant behaviors as the new normal, a process that I refer to later as disciplinarization of hacking.[53]

Even though hackers were involved in developing these standards and active in the institutionalization of the new norms for responsible disclosure, it is clear that a major change had taken place: whereas disclosure norms used to be entirely controlled by hackers under the model of full disclosure, without being formally institutionalized, the models of responsible and coordinated disclosure gave more power to companies to devise the norms of vulnerability disclosure. Inherent to this shift is also an increasing corporate control over vulnerability information, indicating thus that the process of privatization of vulnerability information started to take place in advance of widespread commodification of vulnerabilities instigated by the bug bounty model. Thus, shaped by normalization and institutionalization, the moral project of the responsible and coordinated disclosure regime promoted management values such as transactional

collaboration, effectiveness, predictability and control over information to achieve better security without having to pay hackers for their research and time.

The last regime took the form of bug bounty programs representing again a significant change in the disclosure model through the commodification of vulnerability information and the transformation of hacking into a form of gig work named 'bug hunting.'[54] This change was not unilaterally devised by companies; some hackers were vocal in pushing companies to pay for the information that they provided. The adoption of bug bounties by big tech and the platformization of bug hunting occuring in the same period relied on the progressive institutionalization and standardization of disclosure processes and on increased corporate control over disclosure norms and procedures, including the partial privatization of vulnerability information. Bug bounties provided a means with which to solidify corporate ownership of vulnerability information. In other words, the regime turned unsolicited disclosures into an invitation to hack a defined target, but in very different institutional conditions compared with traditional penetration testing.

Bug bounty programs and platforms have intensified the disciplinarization of hacking in various ways. Bounty policies are not only more precise than ordinary disclosure policies, but they are also commonly adjusted in order to fine-tune the flow of vulnerability information through fine-grained technical guidelines, fluctuating scopes and reward structures. Thus, bug bounty programs constitute a complex governing apparatus that enables companies to manage workflows and crowds and managers to take closer, more personal care to facilitate the work of particularly valuable bug hunters. From this perspective, bug bounty programs can be considered to be an apparatus that sorts not only technical reports but also the humans who author these reports. Beyond hunters' performances and compliance with the guidelines, harmonious relationships, widely promoted in presentations, online tutorials, and social media content, may also play an important role in the process of social sorting.[55]

In building up a bug hunter workforce by instituting educational initiatives, identifying promising hunters, and intervening in their career, platforms and programs are increasingly shaping and controlling hacking as a practice. In a context in which digital security labor is and will remain in high demand, retaining hunters and nurturing a strong reputation in hacking circles can be considered a strategy to create and maintain access to a pool of skilled labor in case of emergency. The moral project of bug bounty is articulated by monetary rewards offered in exchange for vulnerability information, but also for the control over the hackers' research, while contributing to the training of a workforce as an investment to minimize future risks. This project evidently shares some affinities with neoliberal principles such as a flexible model of entrepreneurship (Boltanski & Chiapello, 1999) and a market-based type of governance (Harvey, 2005) both in line with the historical values of autonomy and meritocracy ingrained in hacking circles.

Power and control in ethical hacking

The analysis presented in this article illustrates the importance of considering digital security from a political economy perspective. It allows us to highlight complex collective processes that have redefined vulnerability disclosure and the formation of both hacking and digital security practices. In a similar vein as Birch argues for developing a political

economy perspective of technoscience (2013), I want to stress the importance of developing such a perspective and to advance a critical research agenda (see Dwyer et al., 2022) regarding cybersecurity.

One reason to engage with contemporary political economy is to better assess how shifting regimes of disclosure are reordering people and their expectations around disclosure of vulnerability information and ultimately, to appraise the balance of power at play in these operations. The history of vulnerability disclosure highlights the increasing role of corporate control over disclosure models and, perhaps more importantly, how this control has been progressively secured.

Corporate governance has thrived since the inception of a collaborative framework between companies and hackers: regulations, terms of reference, scope, rewards, and policies are largely determined by companies, while bug hunters have had their bargaining power limited (Elazari, 2019) apart from the choice of which programs to hack for. In addition, this situation combined with the commodification of vulnerability information and the organization of flexible entrepreneurs (bug hunters) in competition with one another, may very well explain the psychological burden experienced by bug hunters evidenced in recent discussions of burnout in the bug bounty arena.[56]

Against this background, it may be easy to understand the integration and transformation of unsolicited hacking in the digital industry as a corruption of the 'traditional' form of hacking that has channeled and regimented hackers into bug bounty programs as freelance service providers for digital companies, a subjugated workforce coerced and exploited by powerful companies. I conclude by highlighting four aspects of the emergence of a market that binds together hackers and companies, that take us beyond this simplistic narrative before sketching a more general perspective on security work (exemplified here by vulnerability disclosure) as always deeply embedded in a complex sociohistorical, economical and political situation that value security issues differently through time.

First, the disciplinarization of hacking has not been the project of one discrete actor or even one type of actor (i.e., the digital industry). In fact, it hasn't even been a unified project. Rather, it is the result of competing organizations and hackers themselves through countless interactions, tweaks, and fixes pertaining to vulnerability disclosure processes over several decades. Obviously, the same can be said about the emergence of a defensive market in the form of bug bounties. The emergence of the bug bounty regime in 2010 marked a novel step in the integration of hackers in the digital tech industry. To argue that hacking have simply been progressively channeled and regimented into bug bounty programs would misrepresent the hackers' agency and success in 'stitching' hacking to business operations.[57]

Second, bug bounties have established a gig economy for the practice of hacking. There is no doubt that, amid capitalist dynamics and powerful corporate actors, bug hunters have begun to suffer from a degree of exploitation (Ellis & Stevens, 2022). However, this does not simply mean that all hackers have become gig workers reporting vulnerabilities for monetary compensation. Indeed, the bug bounty market for vulnerabilities operates alongside other regimes of disclosure in which power relationships are unfolding differently.

Third, the complex transformation of vulnerability disclosure models and practices that I recounted in this article exist within the larger context of the flexibilization of

work (Boltanski & Chiapello, 1999), platform economy (Srnicek, 2017), the externalization of company costs onto workers (Neff, 2012), and the rising magnitude of free labor in the digital economy (Terranova, 2000). The shape taken by the bug bounty regime is *in part* the result of these global economic trends and their intersections with pre-existing hacker practice and historically changing institutions of vulnerability disclosure.

Finally, the analysis of ethical hacking provides insights about the complex structuration and social embeddedness of security work. As a dynamic series of co-existing sociotechnical regimes, ethical hacking points at various and changing values and norms that are not tied up to hackers but are loosely shared among various classes of actors involved in a disclosure regime. The values and norms constituting moral projects are indeed primarily embedded in what a regime devises and enacts.

The norms and values embedded in disclosure regimes far exceed the realm of procedural rules as they include broader ideals and societal projects of various scopes and scales. In this perspective, a disclosure regime is the result of a particular economic and political situation and the solidification of a solution to a problem perceived in a specific way. Thus, for instance, a defensive market for vulnerabilities results from the circumstances of the vulnerability disclosure landscape, an attempt to control hackers' research and to train a much needed workforce in a global context of platformization and flexibilization of work.

The emergence of a new regime of disclosure doesn't entail a complete change from existing regimes. I have indeed highlighted the existence of several continuities across regimes' change. What *signals* the emergence of a new regime is primarily a change of moral project that rearranges disclosure norms, values, principles, practices and expectations to fit new goals such as inducing corporate responsibility, collaboration and standardization or workforce management. Such projects redefine also, in part and at least temporarily, the moral stance of actors, their practices, their agency and their influence in a particular regime.

Notes

1. For instance, https://www.nytimes.com/2015/06/08/technology/hackerone-connects-hackers-with-companies-and-hopes-for-a-win-win.html
2. I copied every source to build my own archive. It comprises 179 documents available online at https://cva.unifr.ch/content/history-vulnerability-disclosure-0 and is displayed on a timeline thanks to Elise Vuitton, a student assistant. This web-archive is built on the PECE framework (Platform for Experimental, Collaborative Ethnography) developed by a group of anthropologists led by Kim Fortun and Mike Fortun at RPI and UC Irvine.
3. https://g.foolcdn.com/EETimes/1997/EETimes970418.htm
4. The reasons are detailed in Bozzini (2023).
5. One of the first full disclosure documented dates from 1984 when the Chaos Computer Club hacked the BTX system in Germany. More details in Bozzini (2023).
6. Computer Emergency Response Team – Coordination Center was founded in 1988 in the US. Today, national CERTs and computer security incident response teams (CSIRTs) are present in many countries.
7. See Shepherd (2003) and https://www.schneier.com/crypto-gram/archives/2001/1115.html
8. https://seclists.org/bugtraq/Other lists include notably the Cypherpunks mailing list partially available at the following link: https://cryptoanarchy.wiki/getting-started/what-is-the-cypherpunks-mailing-list and Zardoz, https://github.com/matthewgream/www-securitydigest-org/blob/master/tcp-ip/index.htm

9. https://seifried.org/security/articles/20011015-elias-levy-interview.html
10. https://seifried.org/security/articles/20011015-elias-levy-interview.html
11. http://fish2.com/security/admin-guide-to-cracking.html
12. Security Administrator Tool for Analyzing Networks
13. https://www.usenix.org/publications/login/november-1999-special-issue
14. In the US, notably the Computer Fraud and Abuse Act from 1986 and Operation Sundevil in 1990.
15. This perspective on full disclosure differs thus from a culturalist view arguing that a pre-existing moral and cultural stance of hacking as a practice unmotivated by financial gain (for instance, Levy, 1984) shaped the practice of full disclosure.
16. One good example of this glorification is the Back Orifice 2000 hacking tool's presentation at DEFCON 1999: https://www.youtube.com/watch?v=oHxNEvklKqE
17. https://www.youtube.com/watch?v=VVJldn_MmMY
18. Securitization refers to the processes shaping an issue into a threat to national security (regarding cyber-threats see Dunn Cavelty, 2008). Vulnerabilities in digital system were securitized for the first time in the 1960s (Ware, 1967) and hackers contributed to put them back on the political agenda in the late 1990s.
19. This includes the Melissa virus (1999), the I LOVE YOU worm (2000), and the Anna Kournikova virus alongside the Ramen, Lion, Sadmind, Code Red, and Nimda worms (2001).
20. https://www.youtube.com/watch?v=g93ofG4OYJU
21. Interestingly, hackers in defense of non-disclosure surfaced shortly after Ranum's speech, collectively presenting themselves as the 'anti-sec' movement. They argued against full disclosure, highlighting the marketization of hacking and advocating for a greater focus on the underground hacking scene: http://web.archive.org/web/20010402024501/http://anti.security.is/
22. It is partly documented in the online archive at https://cva.unifr.ch/content/history-vulnerability-disclosure-0
23. https://www.ranum.com/security/computer_security/archives/script-kiddiez-suck.pdf
24. Economization is a process '[…] through which behaviours, organizations, institutions and, more generally, objects are constituted as being "economic".' (Çalışkan & Callon, 2010, p. 2)
25. https://www.youtube.com/watch?v=EtZxpoxXr7I
26. Nomad Mobile Research Centre is a hacker group based in the US and active since 1998. https://www.nmrc.org/pub/advise/policy.txt
27. Hacker Rainforest Puppy https://web.archive.org/web/20010930194040/http://pcworld.com/news/article/0,aid,63944,00.asp
28. http://www.kb.cert.org/vuls/html/disclosure
29. https://web.archive.org/web/20080725172731/http://news.zdnet.co.uk/security/0,1000000189,2081837,00.htm
30. This argument was strongly underlined by Ranum in his keynote speech to rally both parties under a common interest.
31. https://web.archive.org/web/20011109045330if_/http://www.microsoft.com:80/technet/treeview/default.asp?url=/technet/columns/security/noarch.asp
32. Microsoft Security Response Center
33. The IETF (Internet Engineering Task Force) is an organization that defines and publishes technical standards for the Internet. https://datatracker.ietf.org/doc/draft-christey-wysopal-vuln-disclosure/.
34. For instance, the DHS: https://www.dhs.gov/xlibrary/assets/vdwgreport.pdf
35. Common Vulnerabilities and Exposures (CVE) was established in 1999 to create a comprehensive database of known vulnerabilities. The Open Web Application Security Project (OWASP) was founded in 2001 to bridge security knowledge with online application development. CERTs began to spring up in various countries, and CVSS – a standard with which one can determine the severity of vulnerabilities – was developed by the National Infrastructure Advisory Council (NIAC) in 2004.
36. https://www.itnews.com.au/news/iso-vulnerability-disclosure-standard-now-free-418253

37. https://security.googleblog.com/2010/07/rebooting-responsible-disclosure-focus.html
38. https://msrc-blog.microsoft.com/2010/07/22/announcing-coordinated-vulnerability-disclosure/
39. e.g. https://seclists.org/bugtraq/1994/Nov/143
40. https://msrc-blog.microsoft.com/2008/08/07/threats-in-a-blender-and-other-raisons-dtre/
41. '[…] a team of security researchers at Google who study zero-day vulnerabilities in the hardware and software systems […]' https://googleprojectzero.blogspot.com/p/about-project-zero.html
42. https://www.nytimes.com/1995/10/16/business/the-new-watchdogs-of-digital-commerce.html
43. https://blog.mozilla.org/press/2004/08/mozilla-foundation-announces-security-bug-bounty-program/
44. https://www.helpnetsecurity.com/2003/04/01/interview-with-sunil-james-manager-of-idefenses-vulnerability-contributor-program/
45. https://web.archive.org/web/20020812035333/ and http://www.idefense.com/contributor.html
46. https://www.helpnetsecurity.com/2003/04/01/interview-with-sunil-james-manager-of-idefenses-vulnerability-contributor-program/
47. David Endler worked at iDefense before joining TippingPoint in 2004 to found ZDI (Perlroth, 2021, p. 583).
48. https://www.zerodayinitiative.com/blog/2020/8/19/15-years-of-the-zero-day-initiative
49. https://econinfosec.org/archive/weis2007/papers/29.pdf
50. https://duo.com/decipher/lawyers-bugs-and-money-when-bug-bounties-went-boom
51. https://googleblog.blogspot.com/2010/01/new-approach-to-china.html
52. For instance, https://www.bugcrowd.com/resources/guide/the-ultimate-guide-to-managed-bug-bounty/
53. Disciplinary normalization as defined by Foucault didn't occur in full disclosure. Indeed, we cannot identify the emergence of an analytical grid rearranging the elements of disclosure and a form of control enforcing the norms of the model.
54. Refering to a voluntary and temporary employment, gig work is not necessary tied to platforms.
55. The values of kindness, patience, and diligence are the most heavily promoted in this discourse. See for instance https://www.youtube.com/watch?v=CU9Iafc-I and https://www.youtube.com/watch?v=gul-DFzibaE&list=PLxhvVyxYRviYrJ7S2WhJB6P5cwSIjbL4w&index=6
56. https://www.youtube.com/watch?v=E9Qk7MZNTX8
57. For example, a recent Twitter thread discusses how hackers hired by Microsoft instigated themselves into new technology projects, including the Microsoft bug bounty program: https://twitter.com/mattt_cyber/status/1526729401068445696?s=21

Acknowledgements

I would like to thank Matt Spencer for his numerous insightful comments and suggestions. I also benefitted from discussion with Roberto Carrion and comments from Sylvain Besençon on earlier versions of this article and the two anonymous reviewers. All remaining errors are mine.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by The SNSF Digital lives Grant 183223 and the Swiss Post – University of Fribourg 2024 fund.

Notes on contributor

David Bozzini is an associate Professor of Anthropology at the University of Fribourg in Switzerland. After conducting research on surveillance and security in Africa for more than a decade, he has been developing a new research agenda exploring security hacking, vulnerability disclosure and bug bounties for the last few years [email: david.bozzini@unifr.ch].

References

Anderson, R., & Moore, T. (2006). The economics of information security. *Science*, *314*(5799), 610–613. https://doi.org/10.1126/science.1130992

Birch, K. (2013). The political economy of technoscience: An emerging research agenda. *Spontaneous Generations: A Journal for the History and Philosophy of Science*, *7*(1), 49–61. https://doi.org/10.4245/sponge.v7i1.19556

Böhme, R. (2006). A comparison of market approaches to software vulnerability disclosure. In G. Müller (Ed.), *Proceedings of the 2006 international conference on emerging trends in information and communication security* (pp. 298–311). Springer.

Boltanski, L., & Chiapello, È. (1999). *Le nouvel esprit du capitalisme*. Gallimard.

Bozzini, D. (2023). *How vulnerabilities became commodities. The political economy of ethical hacking (1990-2020)*. https://hal.science/hal-04068476/

Brügger, N. (2018). *The archived web: Doing history in the digital age*. The MIT Press.

Çalışkan, K., & Callon, M. (2010). Economization, part 2: A research programme for the study of markets. *Economy and Society*, *39*(1), 1–32. https://doi.org/10.1080/03085140903424519

Coleman, G., & Golub, A. (2008). Hacker practice: Moral genres and the cultural articulation of liberalism. *Anthropological Theory*, *8*(3), 255–277. https://doi.org/10.1177/1463499608093814

Delfanti, A., & Söderberg, J. (2018). Repurposing the hacker. Three cycles of recuperation in the evolution of hacking and capitalism. *Ephemera. Theory & Politics in Organization*, *18*(3), 457–476.

Dunn Cavelty, M. (2008). *Cyber-Security and threat politics. US efforts to secure the information age*. Routledge.

Dwyer, A. C., Stevens, C., Muller, L. P., Cavelty, M. D., Coles-Kemp, L., & Thornton, P. (2022). What can a critical cybersecurity Do? *International Political Sociology*, *16*(3), 1–26. https://doi.org/10.1093/ips/olac013

Elazari, A. (2019). Private ordering shaping cybersecurity policy: The case of Bug bounties. In R. Ellis, & V. Mohan (Eds.), *Rewired: Cybersecurity governance* (pp. 231–246). Wiley.

Ellis, R., Huang, K., Siegel, M., Moussouris, K., & Houghton, J. (2017). Fixing a hole: The labor market for bugs. In H. Shrobe, D. L. Shrier, & A. Pentland (Eds.), *New solutions for cybersecurity* (pp. 129–159). MIT Press.

Ellis, R., & Stevens, Y. (2022). *Bounty everything: Hackers and the making of the global Bug marketplace*. Data & Society.

Foucault, M. (2008). *Security, territory, population. Lectures at the college de France 1977-78*. Palgrave Macmillan.

Fourcade, M., & Healy, K. (2007). Moral views of market society. *Annual Review of Sociology*, *33*(1), 285–311. https://doi.org/10.1146/annurev.soc.33.040406.131642

Fuenfschilling, L., & Binz, C. (2018). Global socio-technical regimes. *Research Policy*, *47*(4), 735–749. https://doi.org/10.1016/j.respol.2018.02.003

Geels, F. W. (2002). Technological transitions as evolutionary reconfiguration processes: A multi-level perspective and a case-study. *Research Policy*, *31*(8-9), 1257–1274. https://doi.org/10.1016/S0048-7333(02)00062-8

Goerzen, M., & Coleman, G. (2022). *Wearing many hats. The rise of the professional security hacker*. Data & Society.

Granick, J. S. (Spring 2005). The price of restricting vulnerability publications. *International Journal of Communications Law & Policy*, *9*. https://ssrn.com/abstract=874846

Halbert, D. (1997). Discourses of danger and the computer hacker. *The Information Society*, *13*(4), 361–374. https://doi.org/10.1080/019722497129061
Harvey, D. (2005). *A brief history of neoliberalism*. Oxford University Press.
Hellegren, Z. I. (2017). A history of crypto-discourse: Encryption as a site of struggles to define internet freedom. *Internet Histories*, *1*(4), 285–311. https://doi.org/10.1080/24701475.2017.1387466
Hunt, E. (2012). Us government computer penetration programs and the implications for cyberwar. *IEEE Annals of the History of Computing*, *34*(3), 4–21. https://doi.org/10.1109/MAHC.2011.82
Latzko-Toth, G., Bonneau, C., & Millette, M. (2016). Small data, thick data: Thickening strategies for trace-based social media research. In L. Sloan & A. Quan-Haase (Eds.), *The SAGE handbook of social media research methods* (pp. 199–214). SAGE Publications.
Levy, S. (1984). *Hackers: Heroes of the computer revolution*. Anchor Press/Doubleday.
Neff, G. (2012). *Venture labor. Work and the burden of risk in innovative industries*. MIT Press.
Perlroth, N. (2021). *This is how they tell Me the world ends*. Bloomsbury.
Shepherd, S. A. (2003). *How do we define responsible disclosure?* SANS Whitepapers.
Söderberg, J., & Maxigas (2022). *Resistance to the current. The dialectics of hacking*. MIT Press.
Srnicek, N. (2017). *Platform capitalism*. John Wiley & Sons.
Steinmetz, K. (2016). *Hacked. A radical approach to hacker culture and crime*. NYU Press.
Terranova, T. (2000). Free labor: Producing culture for the digital economy. *Social Text*, *18*(2), 35–58. https://doi.org/10.1215/01642472-18-2_63-33
Venturini, T. (2009). Diving in magma: How to explore controversies with actor-network theory. *Public Understanding of Science*, *19*(3), 258–273. https://doi.org/10.1177/0963662509102694
Ware, W. H. (1967). Security and privacy in computer systems. *Proceedings of the April 18-20, 1967, Spring Joint Computer Conference, Atlantic City, New Jersey*.