European Journal of Risk Regulation (2025), 1–18
doi:10.1017/err.2025.10044

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Deciphering Bug hunters – A Law and Economics Perspective

Michael Faure and Jian Jiang

Faculty of Law, Maastricht University P.O. Box 616 6200 MD Maastricht The Netherlands and Minerva Center for the Rule of Law under Extreme Conditions, University of Haifa, Mt. Carmel, Haifa, Israel
Corresponding author: Michael Faure; Email: michael.faure@maastrichtuniversity.nl

Keywords: artificial intelligence; internet of things; bug hunting; vulnerabilities; cybersecurity

I. Introduction

Recent years have witnessed an extraordinarily swift advancement in the fields of artificial intelligence (AI) and the Internet of Things (IoT). AI applications like ChatGTP are gaining significant influence on various aspects of life and even ordinary households are nowadays highly digitalised, a trend that will only intensify with the growing proliferation of the Internet of Things.

Notwithstanding all the advantages that digitalisation has brought to mankind, the increasing reliance of society on computers also makes it vulnerable to cybersecurity breaches. In fact, software development is so complex, and the development is of such a rapid nature, that it is virtually impossible to create programmes that are completely safe, i.e. that have no security flaws whatsoever, often referred to as vulnerabilities. Given the fact that in even the most sophisticated professional software systems vulnerabilities may emerge, there is a strong activity of so-called bug hunters of various kinds. Their activity basically consists in trying to discover the vulnerability in particular software systems. The question, however, arises of what bug hunters will do after they have discovered a vulnerability. The choices available to them and the elements that influence their decisions are the crucial issue that we will address in this paper. In other words: we address the following research question: how is the market for bug hunting structured and what affects the choices of their decisions? We address this question using the economic analysis of law, also referred to as law and economics. The advantage of that approach is that it has paid a lot of attention to how different legal rules may provide incentives to actors in a market setting towards specific behaviour. Law and economics therefore enables a good insight into the potential incentives of actors, both on the demand and on the supply sides of the vulnerability market. This topic is obviously not only of academic interest. Given the huge societal damage that can be (and is) created by cybersecurity breaches, there are important policy implications in discovering what exactly influences the incentives of bug hunters. We, therefore, in addition to analysing incentives from a theoretical perspective, also pay attention to the policy consequences of the analysis.

The paper is structured as follows: after this introduction, we first sketch the security issue in the realm of both artificial intelligence and the Internet of Things (2). We then sketch the nature of software vulnerabilities which are to an important extent unavoidable (3). Then, we turn to those who can discover the vulnerabilities, who we call “bug hunters” (4). When a vulnerability has been discovered, it can be offered on the market to particular actors who could use the vulnerability (5). Next, we sketch the different choices in a model (6) and then conclude, pointing at the policy implications of our findings (7).

2. Vulnerabilities in AI and IoT

The rapid advancement of Artificial Intelligence (AI) and the Internet of Things (IoT) has transformed the global digital landscapes, catalysing unprecedented levels of interconnectedness and automation. However, this transformative shift is accompanied by an inevitable complication, namely, the problem of software vulnerabilities and the importance of cybersecurity. The intricate web of connected devices and autonomous decision-making systems necessitate that cybersecurity should be at the forefront of discourse and action, as we endeavour to navigate a way across this evolving landscape.

On the one hand, the evolution of AI technologies introduces novel cybersecurity challenges. AI systems, increasingly autonomous, make decisions using complex algorithms and vast amounts of data. However, these systems can be undermined through adversarial attacks, where slight, carefully crafted alterations to input data can cause the AI to malfunction or make incorrect decisions. These potential flaws within AI systems are of particular concern given their increasing integration into critical areas like healthcare, transportation, and defence. Take the example of intelligent vehicles. Although they are increasingly smart, integrating innovative applications that span a multitude of functionalities, the interconnected feature of Electronic Control Units (ECUs) within these vehicles, along with the ECUs' reliance on wireless communication for external interactions, render intelligent vehicles vulnerable to prevalent cyberattacks such as malware injection, which can compromise their overall security.[1]

On the other hand, the proliferation of IoT devices has exponentially increased the number of potential entry points for cyberattacks. Each device, ranging from smart home appliances to intricate industrial sensors, represents a node in a network, and any software vulnerability within these nodes may be exploited to compromise the entire system. Inadequate security measures or unpatched vulnerabilities in these devices can inadvertently create a vast range of possibilities for attack, thus escalating the complexity of securing IoT networks. For instance, the integration of IoT in healthcare has introduced vulnerabilities in medical devices and software.[2]

To sum up, the symbiosis of the IoT and AI creates an interconnected system of smart devices that are autonomously controlled and data driven. Its application is very broad from healthcare to transportation and engenders a myriad of benefits, but it also introduces new complexities within our digital ecosystems. In such a setting, vulnerabilities could enable an attacker to manipulate AI decision-making or gain unauthorised access to sensitive data. The interplay of vulnerabilities in AI systems and IoT devices could lead to a cascade of failures or even catastrophic outcomes. Thus, the preoccupation with software vulnerabilities is not a mere afterthought but rather an integral part of the narrative as we progress in the journey of AI and IoT development.[3]

[1] Abu Elkhail, Refat, Habre, Hafeez, Bacha and Malik (2021) discussed this critical issue of vulnerabilities within intelligent vehicles and the related emerging malware threats.

[2] Mejía-Granda, Fernández-Alemán, Carrillo-de-Gea and García-Berná (2023) focused on software vulnerabilities related to health care system from 2001 to 2022 and examined trends in techniques used by cybercriminals to exploit eHealth systems.

[3] The role of AI in vulnerability discovery adds another layer of complexity. On the one hand advanced machine learning models can potentially identify software vulnerabilities at a scale and speed beyond human capabilities; on the other hand, AI can also be used maliciously to identify these vulnerabilities by cyber attackers.

3. Software vulnerabilities

Software vulnerability refers to "security flaws, glitches, or weaknesses found in software code that can be exploited by an attacker (threat source)."[4] This statement encompasses the following significant dimensions of vulnerabilities in software.

Firstly, vulnerabilities present a potential threat as they can be exploited to cause harm, posing substantial risks to both the integrity of the software and to the security of the data it manages. These vulnerabilities are not merely abstract codes but the concrete "Achilles′ Heel" that could compromise system stability and the confidentiality of data.

Secondly, these vulnerabilities are not homogeneous in nature but can manifest themselves in multiple forms, ranging from buffer overflows to injection attacks. The manifestations of these vulnerabilities can lead to a myriad of adverse effects, including unauthorised data access, system damage, or in extreme cases, complete system control by an attacker. These various forms of vulnerabilities diversify the threat landscape, making the task of cybersecurity even more complex and challenging.

Thirdly, vulnerabilities possess intrinsic value, stemming from their potential to be exploited.[5] This unique feature makes them an indispensable component in the arena of cyber-attacks. The extent to which they can be exploited transforms them from mere system weaknesses into the digital raw materials of cyber weapons[6] in the hands of attackers, underlining their critical role in the dynamics of AI and IoT.[7]

Fourthly, the quality of a vulnerability directly influences the success rate of the cyber-attack exploiting it. In general, the most effective attacks are those that exploit vulnerabilities for which patches have not yet been released, or even those unknown to the related software developers. These particular vulnerabilities are termed "zero-day" vulnerabilities,[8] denoting the fact that the developers have had zero days to fix them before they are exploited. The nature of these vulnerabilities underscores their tremendous attack value, marking them the most prized targets within the cyber threat landscape. These zero-day vulnerabilities represent a significant challenge in the field of cybersecurity due to their inherent unpredictability and potential for causing substantial damage before corrective actions can be implemented.

Finally, it is worth mentioning that vulnerabilities cannot simply be totally avoided for two reasons.

It is human beings who write the source code. Every programmer can make mistakes. Sometimes the mistake is a small logical negligence and sometimes it may be just an input error. According to Steve McConnell, a programming guru, on average people make

[4] https://csrc.nist.gov/glossary/term/software_vulnerability

[5] In simple terms, a vulnerability can be defined as a weakness or flaw in a system or software that can potentially be exploited to compromise its security. See: https://www.google.com/search?q=the+difference+between+vulnerability+and+exploit&rlz=1C1CHBD_zh-CNDE960DE960&oq=the+difference+between+vulnerability+and+ex&gs_lcrp=EgZjaHJvbWUqCAgBEAAYDxgeMgYIABBFGDkyCAgBEAAYDxge0gEJMTc0NTVqMGo3qAIAsAIA&sourceid=chrome&ie=UTF-8.

[6] Cyber weapons are considered as tools that automate the functionality of exploit and link multiple exploits to achieve specific objectives. Simply put, cyber weapons essentially utilise vulnerabilities present in computer software and hardware. See: https://www.google.com/search?q=relationship+between+exploit+and+cyber+weapon&sca_esv=592925482&rlz=1C1CHBD_zh-CNDE960DE960&ei=CqyEZavmNYGQ9u8Pwr-rwAc&ved=0ahUKEwirk6TRuqGDAxUBiP0HHcLfCngQ4dUDCBA&uact=5&oq=relationship+between+exploit+and+cyber+weapon&gs_lp=Egxnd3Mtd2l6LXNlcnAiLXJlbGF0aW9uc2hpcCBiZXR3ZWVuIGV4cGxvaXQgYW5kIGN5YmVyIHdlYXBvbjIFECEYoAFI-LsCUPEMWLa0AnAjeAGQAQSYAXegAb9MqgEFOTEuMjK4AQPIAQD4AQGoAgDCAgoQABhHGNYEGLADwgIGEAAYHhgPwgIFEAAYgATCAgsQLhiABBjHARjRA8ICChAAGIAEGIoFGEPCAgUQLhiABMICFBAuGIAEGJcFGNwEGN4EGOAE2AEBwgIEEAAYHsICBhAAGAgYHsICCBAAGAgYHhgPwgIHEAAYgAQYCsICGhAuGIAEGMcBGNEDGJcFGNwEGN4EGOAE2AEBwgIHEAAYgAQYDMICCBAAGIAEGKIEwgIHEAAYgAQYE8ICBhAAGB4YE8ICCBAAGB4YDxgTwgIIEAAYCBgeGBPCAgcQIRigARgK4gMEGAAgQYgGAZAGCroGBggBEAEYFA&sclient=gws-wiz-serp.

[7] See Section 2 of this paper.

[8] https://www.hpe.com/us/en/what-is/zero-day-vulnerability.html

between 15 to 50 errors in every thousand lines.[9] Careful checking in big software companies can push the number down to nearly 0.5 in every thousand lines.[10] In practice, the possible reduction in the number of vulnerabilities is limited.[11] At the same time, it is very expensive to keep the vulnerability level at an extreme low level. For example, there are no known defects in the Space Shuttle Software of NASA, which costs thousands of dollars for every line of code (Even this does not rule out completely the existence of a vulnerability). No commercial software vendors can afford the same level of testing as NASA.[12]

The source code of most common programs is incredibly long. The following Table 1 gives a rough idea about how many lines compose the programs listed there. The longer the lines of code, the more complicated the problem of the potential vulnerabilities. Not only do the kinds of defects increase with program size, but so also does the number of defects. According to the software construction handbook, when a software product grows twice as large, it is likely to have more than twice as many vulnerabilities.[13]

Moreover, the nature of competition in software development emphasises speed as a crucial factor. Consequently, programs are often released to the market while still containing potential vulnerabilities.[14] Additionally, in recent years, deep learning, a branch of AI, has been used for vulnerability detection. Zeng, Lin, Pan, Tai, Zhang (2020) reviewed twenty-two existing studies in this field and concluded "that the application of deep learning techniques for software vulnerabilities analysis and discovery is not yet mature."[15] Therefore, software vulnerabilities are still an unavoidable risk in cybersecurity.

4. Bug hunting

4.1. Bug hunters

"Hackers" is a term which refers to one of the most pertinent notions that is indubitably associated with software vulnerabilities. The term "hackers," in a broader context, applies to various actors with divergent objectives and methodologies, which can be classified into three primary categories: white hat, black hat and grey hat.

White hat hackers are ethical hackers tasked with enhancing system security. Utilising tactics akin to black hat hackers, they legally conduct penetration tests, identifying vulnerabilities to safeguard a system's integrity. They typically work as security specialists within organisations.

Black hat hackers, conversely, are often associated with cybercrime, and they operate with intentions of financial gain or malicious destruction. Their activities span from bypassing security protocols and penetrating systems in order to steal data and to demand cyber ransom. This group has varied skill levels, ranging from novices employing basic hacking tools to experts proficient in exploiting system vulnerabilities.

Grey hat hackers are spread between the two above-mentioned categories. Their motivations are nuanced; they lack the malicious intent of black hats and the security-driven ethos of white hats. Their activities, although illegal due to unauthorised access,

[9] Industry Average: about 15–50 errors per 1000 lines of delivered code. This is known as the defects per KLOC (1000 lines of code), see: https://labs.sogeti.com/how-many-defects-are-too-many/.

[10] McConnell (2004), p 521; "Microsoft Applications: about 10–20 defects per 1000 lines of code during in-house testing, and 0.5 defect per KLOC in production".

[11] The Economist (2017), Why everything is hackable?

[12] https://labs.sogeti.com/how-many-defects-are-too-many/

[13] McConnell (2004), p 652

[14] Goertzel (2016)

[15] Zeng, Lin, Pan, Tai, Zhang (2020)

Table 1. The length of different Programs´ Code

Program	Number of lines of code
Google (all products)	2 billion
Linux (open source, as of 2015)	20.3 million
Windows	50 million
Android	12 million

Source: Author’s compilation based on data from The Economist (2017).

generally do not involve data theft or destruction. Instead, they identify system vulnerabilities without explicit malicious intent.[16]

We cast our attention onto a collective of actors referred to as “bug hunters,” a group mixed of white hat and grey hat hackers.[17] These individuals distinguish themselves from black hat hackers due to their absence of malicious intentions to exploit the vulnerabilities they discover.

They are not wholly white, despite their engagement in legal penetration tests to discover vulnerabilities. This is because they may not follow through with the corresponding disclosure and reporting procedures. Moreover, they are not entirely grey, given that they employ not only unauthorised access but also authorised access methods to identify vulnerabilities.

These bug hunters are a cohort focusing on vulnerability identification without any explicit moral responsibility or criminal motivation. They are denoted as “bug hunters” purely on account of their involvement in the act of hunting for bugs (vulnerabilities). In most cases, they are technical people who employ proactive approaches to find vulnerabilities before they could be found by others.

4.2. Their impacts on cybersecurity

Vulnerabilities are often uncovered through exploratory testing, analogous to probing whether an unattended door has been left unlocked. Once such vulnerabilities are identified, the subsequent course of action can result in two sharply divergent outcomes: responsible disclosure, which strengthens security, or malicious exploitation, which amplifies risk.

A bug hunter may opt to report the identified vulnerabilities to relevant stakeholders, thereby facilitating timely remediation and contributing to improved cybersecurity. Through the discovery and documentation of such findings, bug hunters offer valuable insights that enable developers to address security flaws effectively. Ultimately, this collaborative process plays a pivotal role in enhancing the robustness and reliability of system security.

Conversely, the bug hunter may choose to profit from the undisclosed vulnerability by selling it to actors with malicious intent. Such actions significantly elevate systemic risk and undermine overall cybersecurity. Once the knowledge of an “unlocked door” becomes accessible to adversaries, the resulting consequences can be severe and unpredictable.

Having comprehended the pivotal role that bug hunters play in cybersecurity, we proceed to analyse the options they have and the markets they face after their discoveries of vulnerabilities in section 5. However, we first provide some statistics on bug hunting.

[16] https://www.avast.com/c-hacker-types

[17] The term “bug hunter” is often specifically used to denote ethical hackers or white hat hackers. Please note that we adopt a more expansive definition in this context.

Table 2. Bug Bounties VS. Median Annual Salary

Developing Countries	Multiplier	Developed Countries	Multiplier
India	16 x	Hong Kong (China)	7.6 x
Argentina	15.6 x	Belgium	2.7 x
Egypt	8.1 x	Australia	2.7 x
Philippines	5.4 x	Canada	2.5 x
Latvia	5.2 x	US	2.4 x
Pakistan	4.3 x	Sweden	2.2 x
Morocco	3.7 x	Germany	1.8 x
China	3.7 x	Italy	1.7 x
Poland	2.6 x	Netherlands	1.7 x
Bangladesh	1.8 x	Israel	1.6 x

4.3. Data on bug hunting

Data can be found in the "Hacker-Powered Security Reports" from HackerOne. HackerOne[18] is a famous global vulnerability bounty and cybersecurity assessment platform, facilitating collaboration between organisations and international security researchers, commonly referred to as "hackers." These registered hackers are authorised to conduct legitimate security testing against suspected entities, and in return, they receive compensation for the vulnerabilities they identify. Annually, HackerOne publishes a report which describes the prominent vulnerability trends from the preceding year, including the amount of money paid out, impacted industries and insights into the backgrounds and expertise of the hackers. From their reports spanning the years 2018 to 2022, the following observations can be drawn.[19]

1) Geographically, bug hunters are distributed not only in developed countries but also in developing countries. The number of bug hunters in developing countries is growing rapidly. Records of activities of local bug hunters are found in countries like India, Pakistan, Egypt, Thailand, Algeria, Morocco, Latvia, Philippines, Romania, Hungary, Chile, Ethiopia and Indonesia. Consider India, for example. Whereas in 2018 bug hunters in India accounted for 23.3% of the total registered amount on the HackerOne platform, in 2019 this number climbed to 27%.[20]
2) According to the survey by HackerOne in September 2022 on 5,738 bug hunters worldwide, 68% of these respondents revealed that their earnings from activities of (ethical) hacking account for less than half of their income. Furthermore, 72% respondents underscored financial motives, the bounties, as "the biggest attraction."[21] As early as 2018, the data[22] has shown that the worldwide average bounty cash inflow to a top bug hunter is 2.7 times the median annual wage of a software engineer in the same home country. In some countries the difference is even wider, especially in developing countries, which we can observe in Table 2. In

[18] https://www.hackerone.com/.

[19] The term "hacker" in the annual reports of HackerOne does not encompass "black hat hackers." It is in line with what is designated as "bug hunter" in this study. Consequently, the surveys on hackers worldwide made by HackerOne serve as a valuable representative sample for understanding the global population of bug hunters.

[20] 2018 Hacker Report & 2019 Hacker Report by HackerOne, https://www.hackerone.com/.

[21] 2022 Hacker-Powered Security Report by HackerOne

[22] 2018 Hacker Report by HackerOne

the following table twenty countries (regions) are listed and the multiplier is found by dividing the upper range of bounty earners in the region by the corresponding regional median annual salary of a software engineer. For those in developing countries, where the average salary level is relatively low, bug hunting activities can improve their financial situation greatly, which is illustrated by the higher multipliers in the table.

3) It was observed that average bounties increased across many industries in 2021 and 2022. Specifically, financial services witnessed a consistent increase in average bounties. The cryptocurrency and blockchain industry experienced the most "dramatic" increase in bounty expenditures: the mean pay-out for a critical vulnerability increased by 315%, ascending from $6,443 in 2021 to $26,728 in 2022. However, such trends are not uniformly observed across all sectors. In fact, the average remuneration for critical vulnerabilities in the retail domain experienced a decline of 15%, while the software sector saw a decrease of 30%.[23]
4) Vulnerabilities remain undetected in the absence of bug hunters.[24] Statistical analysis in 2021 revealed that half of the hackers opted for non-disclosure of identified vulnerabilities. The predominant impediment to disclosure is the absence of a vulnerability disclosure program. This data markedly deviates from the 25% reported in 2018, yet both are predicated on the same rationale.[25]
5) Furthermore, hacking is regarded as a foundational steppingstone in pursuing a career in cybersecurity. A substantial portion of bug hunters aim for recognition, seeking the opportunity to publicly detail their methodology in uncovering vulnerabilities. Survey data from 2022 indicates that 34% secured relevant employment due to this expertise, while 25% achieved promotions as a result.[26] This observation aligns coherently with earlier literature. Algarni & Malaiya (2014) pointed to an intriguing phenomenon they observed after they studied some top bug hunters. Most of them were active and credited with discovering vulnerabilities during the first three years of operation. Then these successful hunters disappeared from the scene for the following years. The authors explained that this was because after they had gained a reputation as successful bug hunters, they started their service for software companies or security service providers on a contract basis, or they initiated their own business as a security expert. From the perspective of economics, reputation itself is also a financial incentive. It is an intangible asset that can bring stable cash flows in the future.

From the aforementioned observations, it is discernible that external actors play a key role in the process of vulnerability identification. The number of bug hunters worldwide is increasing, especially in developing countries. Moreover, monetary incentives act as the primary motivators, while reputation essentially operates as an alternative form of monetary incentive, promising potential future career or job positions. Notwithstanding the bounty offerings by some industries and organisations to incentivise bug hunters to disclose identified vulnerabilities, a considerable segment still opts for non-disclosure. Non-disclosure probably implies that the bug hunter sold the discovered vulnerability on

[23] 2022 Hacker-Powered Security Report by HackerOne

[24] Algarni & Malaiya (2014) pointed out that "a large fraction of the vulnerabilities [. . .] are discovered by outside discoverers. [. . .] Many external discoverers are freelancers either working on their own or on a contract basis". They studied two popular internet browsers, Safari, and Chromium, and found that 80% of the vulnerabilities of Safari and 64% of the vulnerabilities of Chromium were discovered by outsiders, people who were not engaged in discovering vulnerabilities internally in software companies.

[25] In the 2018 Hacker Report, it was observed that approximately 25% of hackers refrained from reporting identified vulnerabilities due to the absence of an established disclosure mechanism.

[26] 2022 Hacker-Powered Security Report by HackerOne

the black market. For some bug hunters, the options provided on the black market are more attractive than the bounties offered for disclosure. So, the way in which bug hunters make that trade-off will exactly depend upon demand and supply on the market for vulnerabilities.

5. The market for vulnerabilities

After having explained the various bug hunters and their activities, we will now turn to the market for vulnerabilities and identify the supply and the demand side; in addition, we will discuss the various markets that may emerge and the specific determinants, as well as the scenarios with which the seller in the market (the bug hunters) may be confronted.

5.1. The supply side

On the supply side of the market for vulnerabilities we find the bug hunter who we have already identified in the previous section. Logically, a bug hunter who discovers a vulnerability will have to decide whether or not to bring his discovery to the market, in other words whether or not to sell it.

Should a bug hunter act rationally, he (she) would typically opt to monetise his (her) discovery rather than do nothing. The rationale underpinning such a decision can be understood from the subsequent two aspects.

Firstly, a bug hunter could monetise the vulnerability due to its intrinsic value. A vulnerability can potentially be exploited to achieve the specific objectives of the bug hunter, such as surveillance or obtaining unauthorised system administration. Any entity with intrinsic value, upon encountering a prospective buyer, can command a corresponding price. Given the presence of related markets and interested buyers, there is no reason for the bug hunter to forego the potential monetary benefits derived from such a transaction.

Secondly, a bug hunter would quickly monetise his (her) findings due to the temporal risk termed as "vulnerability rediscovery," in which two or more hunters independently find the same vulnerability.[27] Should others identify the same vulnerability, and subsequently have it sold, the value of one's own discovery would be diminished. Consequently, a bug hunter will be incentivised to sell the identified vulnerability as soon as possible.

5.2. The demand side

Generally speaking, upon identifying vulnerabilities, a bug hunter is confronted with three distinct categories of buyers who may be interested in purchasing the vulnerability.

The first category comprises software developers or App owners, and their intermediaries. A platform like HackerOne is an example of such an intermediary. Bug

[27] Some scholars have studied this issue and presented different views of this phenomenon.

Herr, Schneier & Morris (2017) state that "15% to 20% of vulnerabilities are discovered independently at least twice within a year. For just Android, 13.9% of vulnerabilities were rediscovered within 60 days, rising to 20% within 90 days, and above 21% within 120 days. For the Chrome browser we found 12.57% rediscovery within 60 days … ." They believe that the rediscovery rates presented in their paper underestimates the true rate of rediscovery. This is because their study is restricted to the high- and critical-severity bugs, but low- and medium-severity vulnerabilities are rediscovered more frequently (Herr, Schneier & Morris (2017), p 1).

Almost at the same time, Ablon & Bogart (2017) focused on zero-day vulnerabilities, the most critical-severity vulnerabilities. They show that for a given stock of zero-day vulnerabilities, the rate of rediscovery within a year is approximately 5.7%. Please refer to: Ablon & Bogart (2017), p xii.

hunters can disclose their findings to these entities in return for monetary incentives termed as "bounties." This type of transaction is referred to as a "white market" trade.

The second category involves governmental entities and their respective agents. This can also involve the payment of a bounty, but that is not necessarily the case. Transactions between bug hunters and these entities are labelled as "grey market" trades.

The third category encompasses buyers outside the aforementioned categories. Transactions where bug hunters sell vulnerabilities to these buyers are illegal, hence, their dealings are termed as "black-market" trades, which predominantly occur online.[28]

5.3. Discussion of the three markets

As previously introduced, when a bug hunter discovers a vulnerability, he (she) is faced with three market choices: the white market, the grey market, and the black market. The table below provides a simple comparison of these three markets.

5.4 Determinants of the market

5.4.1. Legality and the impact on the market transactions.

The distinction between the white market and the black market is clear. The white market is legal, and the increasing practice of responsible disclosure for vulnerabilities serves to mitigate social risks, thereby enhancing the overall cybersecurity. On the contrary, the black market acts as an illicit source of toolkits for cybercrime, exerting a negative impact on cybersecurity. Although the grey market transactions might not explicitly breach legal boundaries, they pose latent threats to cybersecurity, where existing vulnerabilities are not duly addressed and remediated, but left unpatched and socially risky.

5.4.2. The price level

RAND´s experts pointed out that "the grey market is thought to be more lucrative than the black market, and both are distinctly more lucrative than the white market. Many estimates put prices in the grey and black markets at ten times those of the white market."[29]

To recognise the reasons behind, first we notice that the vulnerabilities traded in the grey market and the black market are, to a considerable extent, different. To meet the needs of intelligence or law enforcement, highly risky vulnerabilities, like zero-days, are favoured by government agencies, who are the main buyers in the grey market. In comparison, less risky vulnerabilities are also popular in the black market. The average risk level of these vulnerabilities in the black market is lower than that of those in the grey market.

Second, the buyers in the respective markets are different. The main buyers in the grey market are governments, whereas the main buyers in the black market are criminals or criminal groups. Governments have a higher ability to pay than criminal gangs. They normally have annual budgets allocated for this special purpose, whereas criminals take the deal of vulnerability toolkits as their criminal costs.

For a deeper understanding, let's suppose an autocratic government, who is on the UN blacklist for violations of human rights. If the bad government wants to compete with a democratic government, who can trade on the grey market, for the same zero-day vulnerability, the black market is the only way. In this case, the bad government must pay

[28] Fidler (2015); Libicki, Ablon, & Webb (2015)

[29] Libicki, Ablon & Webb (2015), p 44

a higher price in the black market than in the grey market, to compensate the extra risks to the seller. The extra risk is related to law enforcement and the risk of sanctions.

5.4.3. The agency mechanism

Firms, no matter whether they are platforms, or dealers, or brokers, play a very important role of agent on the vulnerability markets. These intermediaries usually work for (and thus are paid by) the buyers. This agency mechanism has, as well-known, its own disadvantages: asymmetric information. The intermediaries have incentives to deliberately drive the price up, inducing their clients (software vendors, website owners, or governments) to form a long-term expectation of a high price level, in order to increase their own profits. This happens quite often when there exists asymmetric information. Furthermore, when there are no suitable buyers in the legal markets, a profit orientated dealer may turn to opportunities in the illegal market.[30]

5.4.4. The relationship between these markets

The relationship between the white market and the other two markets is competitive. This is because, for any vulnerability, the software or website owner has the incentive to get it repaired. It is not the problem of whether or not to buy the vulnerability, but the problem of at which price to buy it.

The relationship between the grey market and the black market is complementary in a sense, because the buyers in the grey market may also enter the black market when they want to hide their identities completely. As RAND experts mentioned: "sellers who are driven only by money will often bounce between markets chasing the pay-out."[31] When we study Table 3, we can find out that vulnerabilities traded in the grey market and vulnerabilities traded in the black market to a certain extent cannot overlap. Governments need high risky vulnerabilities like zero-day vulnerabilities instead of exploits, which are ready-made tools for mass criminals based on averagely less risky vulnerabilities. Zero-day vulnerabilities are expensive for mass criminals in the black market. However, it was reported in 2022 that zero-day vulnerabilities, the most valuable hacking tools, were no longer the domain of governments. Wealthy cybercriminals are using zero-day-based tools more than ever.[32]

5.5. Scenarios

Based on the aforementioned analysis, we can deduce that once a bug hunter discovers a vulnerability, he (she) will opt to sell it rather than doing nothing. It is important to stress that for the seller the grey market is the most attractive one. The reason is that it offers a higher payoff than the white market, yet, as it is legal, it does not involve the risks of penalties involved with dealing on the black market. As a consequence, the bug hunter will, given the various determinants, encounter two potential scenarios:

Scenario 1: ability to find a grey market buyer

If a grey market buyer can be found, the bug hunter will decide between the white market and the grey market. He (she) may choose the grey market due to monetary incentives or may opt for the white market based on personal ethical standards. In this scenario, black-market transactions are not a preferable choice for the bug hunter. This is

[30] *Id.* p 47

[31] *Id.* p 47

[32] https://www.technologyreview.com/2022/04/21/1050747/cybercriminals-zero-day-hacks/

[33] Based on https://zerodium.com/program.html (retrieved on 24 Aug. 2023); https://www.microsoft.com/en-us/msrc/bounty (retrieved on 24 Aug. 2023); Fidler (2015), p 416; Libicki, Ablon, & Webb (2015), p 48, p 44.

Table 3. A comparison of three markets for vulnerabilities[33]

	White Market	Grey Market	Black Market
Buyers	bug bounty offers	government agents; security firms; dealers	anonymous buyers
Traded Goods	almost any type of vulnerabilities	high-risk vulnerabilities, e.g., zero-day vulnerabilities, with fully functional exploits,	exploitable vulnerabilities
Price Example (from official website)	from up to $15,000 to up to $ 100,000 (Microsoft)	up to $2,500,000 per submission of zero-day vulnerability (Zerodium)	—
Relative Average Price Level to White Market	—	10X	10X
Legality	legal	legal	illegal
Impacts on Cybersecurity	positive	potentially negative	very negative
Transaction Channel	bounty programs; independent bounty platforms	acquisition programs; through dealers; through brokers	online transaction
Relation to White Market	—	competitive	competitive
Relation to Black Market	competitive	complementary in a sense	—

This table clearly indicates the three main markets, which equally indicate the options available to the bug hunter. The choice for a particular market will depend upon specific determinants.

because the black market does not offer more profits than the grey market, yet it presents legal risks.

Scenario 2: inability to find a grey market buyer

In the absence of a grey market buyer, the bug hunter faces a choice between the white market and the black market. Engaging in black-market transactions might yield higher profits than white market rewards. However, this also carries the default risk from the buyer side as well as the risks to bear the legal ramifications from illegal activities.

Additionally, from an economic perspective, the rewards from the white market, coupled with the related good reputation, represent the opportunity cost of the bug hunter when considering black-market transactions. We will delve more deeply into these scenarios, sketching the trade-offs for the bug hunter. Thereby we will use economic analyses in the subsequent section. The most interesting is obviously the scenario where there is no grey market available and the bug hunter is thus left with the choice between the white and the black market. In the next section, we will sketch a model that will allow us to sketch various choices and corresponding pay-offs of the bug hunter under different scenarios.

6. The model

6.1. Construction of the model

Here we develop an economic model to predict how a bug hunter makes decisions when confronted with the option of the black market. Our model is derived from the classical law

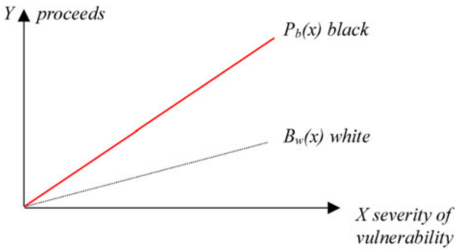


Figure 1. Payoffs from the black and white markets.

& economic model of criminal behaviour developped by Gary Becker (1968) and represented inter alia in Cooter & Ulen (2014).[34]

We assume that bug hunters are rational, seeking to maximise their own economic benefits, in other words their utility. They are also assumed to be amoral, which means that they can freely choose to trade between the legitimate (white) market and the black market, unhindered by any moral constraints.

Vulnerabilities can be ranked by their severity levels. In our coordinate system, the *x*-axis denotes the severity of the vulnerabilities. Similarly, let the *y*-axis denote the proceeds and associated costs for a bug hunter from black-market transactions. Here the associated costs are economic costs, which include the opportunity costs incurred by the bug hunter due to participation in black-market transactions, specifically the monetary bounties from the white market that are foregone, as well as the potential punishments resulting from engaging in illicit transactions. We assume that all the aforementioned proceeds, bounties and punishments can be quantitatively represented by the *y*-axis.

a) Payoffs from two markets

In Figure 1, the solid line $P_b(x)$ represents the payoff (proceeds) from the black market, while the dashed line $B_w(x)$ signifies the payoff (bounties) from the white market. The payoffs in both markets, $P_b(x)$ and $B_w(x)$, are increasing functions of the severity of the vulnerability *x*. In other words, the higher the risk level of the vulnerability, the higher its market price will be. For a specific vulnerability, its black-market price is higher than its white market price, so that the solid line lies above the dashed line. The price level is graphically reflected in the steepness of the (solid or dashed) line. Since the price level in the black market is higher, the solid line is steeper than the dashed line. The ratio of the slopes of the solid line and the dashed line presents the relative price level between the black market and the white market.

b) The expected fine $p(x)f(x)$

In reality, the punishment associated with engaging in black-market transactions is not certain but probabilistic. For simplicity, the punishment is assumed to be a fine. Therefore, the expected punishment function equals the probability *p* times the fine *f*: *pf*. Both *p* and *f* are increasing functions of the vulnerability severity *x*. The logic behind this is clear. The greater the harm of a vulnerability, the more likely it is to attract the attention of law enforcement, thus increasing the probability of apprehension. Similarly, a more harmful vulnerability will result in a corresponding fine. Given that both *p* and *f* increase with *x*, the slope of the curve $p(x)f(x)$ is per se a monotonically increasing function. Consequently, the shape of the curve $p(x)f(x)$ is convex, which we can observe in Figure 2.

[34] To know more about the criminal behaviour model, please refer to: Cooter, Robert; Ulen, Thomas (2014), Law and Economics (6th edition), Chapter 11.

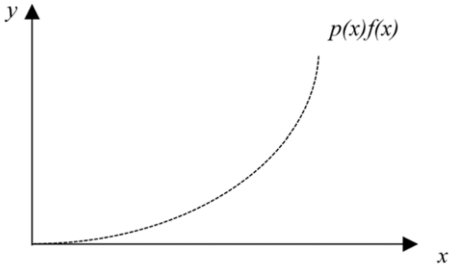


Figure 2. The expected fine p(x)f(x).

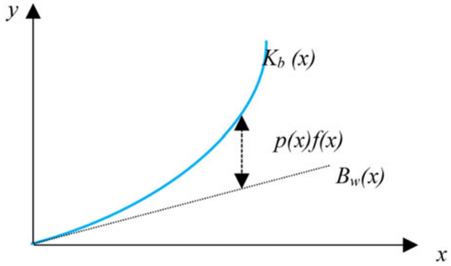


Figure 3. The economic costs K_b(x).

c) The economic costs

The economic costs $K_b(x)$ for a bug hunter's black-market transaction include both the opportunity cost $B_w(x)$ and the expected fine $p(x)f(x)$: $K_b(x)= B_w(x)+ p(x)f(x)$. Graphically, the curve of $K_b(x)$ is the superposition of the line of $B_w(x)$ and the curve of $p(x)f(x)$, which is presented in Figure 3.

d) Payoff vs. costs

Based on the analysis above, in Figure 4, we can observe both the payoff $P_b(x)$ and the costs $K_b(x)$ of the black-market transaction. A bug hunter has an incentive to choose the black market when and only when the payoff $P_b(x)$ is above the costs $K_b(x)$. The logic for the sharp increase in Kb(x) is that when the severity of the vulnerability increases, also the probability of detection will increase (as a result of more investments in law enforcement) as well as the expected punishment.

6.2. The profitable margins

When $P_b(x)$ is above $K_b(x)$, the black market offers profitable margins for the bug hunter. In Figure 5, the enclosed area A formed by the intersection of $P_b(x)$ and $K_b(x)$ represents the profit margins for black-market transactions.

The point x_1 represents the intersection of $P_b(x)$ and $K_b(x)$ and serves as a critical point, where the payoff $P_b(x)$ equals the costs $K_b(x)$. The existence of point x_1 is due to the fact that as the value of x increases, the associated penalties escalate rapidly, thereby leading to a swift compression of the profit margins in the black market, until the costs eventually exceed the proceeds. As long as the severity level of a vulnerability remains below x_1, the anticipated penalties are insufficient to pose a significant deterrent to a bug hunter. Consequently, bug hunters find it profitable to sell these vulnerabilities ($x \leq x_1$) to the black market.

Among all these vulnerabilities with a severity level less than or equal to the critical point x_1, those with the severity level equalling to x^* will yield the maximum profit. This is

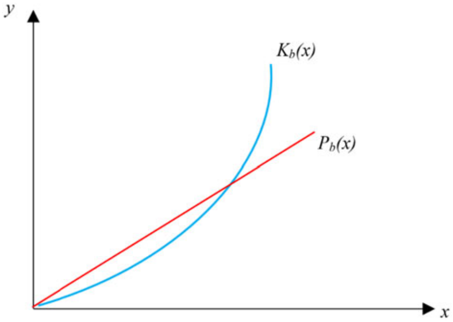


Figure 4. The payoff and economic costs.

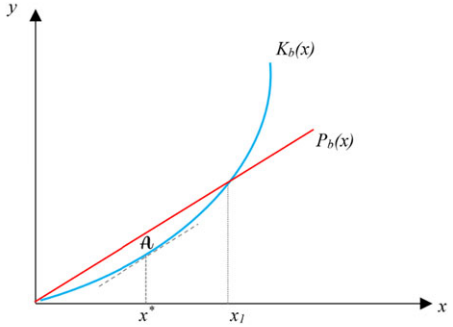


Figure 5. Illustration of x_l and x*

because at this point, the marginal payoff of $P_b(x)$ equals the marginal cost of $K_b(x)$. Graphically observing from Figure 5, the dashed line parallel to $P_b(x)$ is tangent to $K_b(x)$, which implies that at point x^*, the slopes of $P_b(x)$ and $K_b(x)$ are equal.

6.3. Refinements of the model

a) Good reputation

The discussion above of the model has not accounted for the potential benefits that a good reputation can bring to a bug hunter, which should indeed be considered as a kind of opportunity cost and be included into $K_b(x)$.[35] After incorporating the reputation, the intangible opportunity cost, $K_b(x)$ will move upwards overall parallelly, as depicted in Figure 6. The intercept b on the y-axis quantitatively equals to the amount which a good reputation can quantify.

From Figure 6 we observe that the range of vulnerabilities available for purchase in the black market has narrowed. Initially spanning from 0 to x_1, it now ranges between x_2 and x_3. A subset of vulnerabilities with lower levels of severity has, due to b, the capitalised value

[35] As mentioned in Section 3.3, a survey from 2022 indicates that approximately 34% of bug hunters secured an employment due to their ethical hacking activities, and 25% experienced a promotion in their positions. Let's engage in a simple calculation to quantify the reputation, supposing that a good reputation has a 25% probability of bringing an incremental monthly salary of 2,000 € for five years. Without factoring in financial discounting, this reputation can be quantified as 5×12×2,000×25%=30,000 €. If we incorporate this value into the cost function $K_b(x)$, the curve of $K_b(x)$ would move upward. Its intercept b in figure 6 on the vertical axis would equate to 30,000 euro.

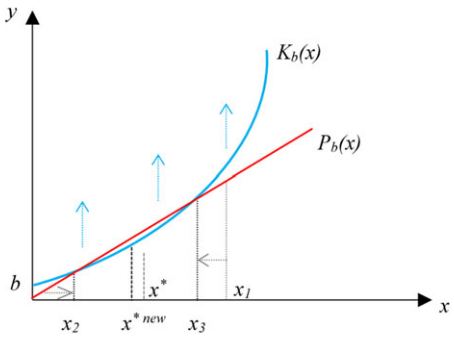


Figure 6. Incorporating the capitalised reputation.

of reputation, become unavailable in the black market. The overall profit area is shrunken, with x^* shifting leftward to x^{*new}. This implies that the severity level of vulnerabilities most likely to be sold by bug hunter to the black market has decreased.

The aforementioned analysis offers significant insights for policymaking. To reduce the number of vulnerabilities entering the black market, widely recognising and valuing the ethical activities of ethical bug hunters emerge as a highly effective approach beyond mere monetary incentives.

b) International cooperation

Another approach entails ways to impose stricter expected punishments,[36] which graphically manifests as a steeper $K_b(x)$ curve. This results in leftwards shift of x_1, leading to a diminished profit margin area for black-market transactions. However, issues of illegal transactions and crimes on the internet also reflect the complexity of internet jurisdiction.[37] The internet has no borders, which addresses challenge calls for extensive and profound international collaboration.[38]

c) Influence from the grey market

The implications arising from the existence of the grey market can theoretically be separated into the following two scenarios. Given that buyers in the grey market seek vulnerabilities with high levels of severity, we posit that the corresponding threshold is denoted as x_{grey}.

Scenario (Figure 7) a: $x_{grey} < x_1$

This implies that vulnerabilities with severity levels ranging between x_{grey} and x_1 will face competition from both grey-market and black-market buyers. This will lead to an increase in the price level within the black market. Graphically, this is represented by a steeper curve of $P_b(x)$, a rightward shift of x_1, and an expansion of the area of profit margins in the black market.

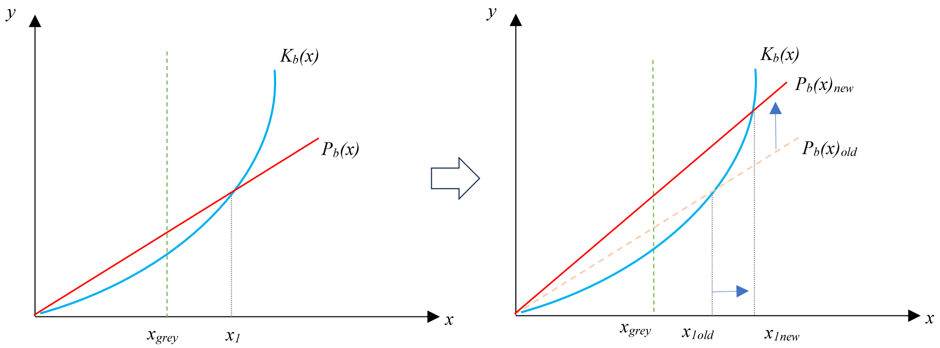
Scenario (Figure 8) b: $x_{grey} > x_1$

If $x_{grey} > x_1$, this suggests that the demands of grey-market and black-market buyers do not overlap. The price level within the black market will not increase due to competition with the grey market, and the $P_b(x)$ graphically will not become steeper. An optimal strategy for a bug hunter would be to sell vulnerabilities with severity levels below x_1 to the black market, those above x_{grey} to the grey market, and vulnerabilities with severity levels between x_1 and x_{grey} to the white market.

[36] This can either be realised by increasing the probability of detection (p) or the sanction (S). The expected punishment is the result of the probability multiplied with the sanction (p.S).

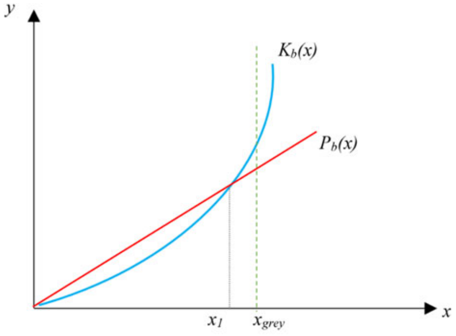
[37] For internet jurisdiction, please refer to Hörnle, Julia (2021).

[38] Johnstone; Sukumar; Trachtman (2023) provides a detailed analysis of cybersecurity norm-making processes and country positions.



Scenario a

Figure 7. Influence from the grey market: Scenario a



Scenario b

Figure 8. Influence from the grey market: Scenario b

However, under the premise of state-sponsored hackers participating in black-market transactions, this scenario will never happen. State-sponsored hackers require a diverse array of vulnerabilities, not just for defence, but predominantly for offence.[39] Under these circumstances, only scenario a is realistically applicable, and furthermore, the price level within the black market would substantially surge.

d) Intermediaries

As discussed in Section 4.2, vulnerability transactions frequently involve intermediaries such as dealers, brokers, and platforms. These agents, driven by strong economic incentives, endeavour to amplify the price difference between the non-white and white markets to maximise their profits. Such activities inevitably culminate in elevated black-

[39] The U.S. National Security Agency (NSA) noted insights into the activities of both national adversaries and cybercriminals in public spaces. It indicates that government agencies are concerned with a broad range of cyber threats, which may include advanced persistent threats (APTs) and state-sponsored hacking, contrasting with the more opportunistic and profit-driven attacks of cybercriminals. Please refer to: 2021 NSA Cybersecurity Year in Review, https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/2921744/nsa-releases-2021-cybersecurity-year-in-review/.

In addition, Li & Liu (2021) reviewed scenarios for government-sponsored cyber warfare, including cyber espionage, attacks aimed at creating unrest or facilitating physical aggression, and attacks complementing physical aggression. These scenarios suggest a strategic and often politically motivated approach to cyber operations, differing from the typically financially motivated attacks of cybercriminals.

market price levels, resulting in steeper $P_b(x)$ and subsequently expanding the critical point x_1 and profit space within the black market. Hence, imposing regulations upon these intermediaries, along with oversight of government practices of procuring vulnerabilities through the market, is both imperative and pressing.

7. Concluding remarks

This paper analysed the important role of so-called bug hunters in promoting cyber security. As a result of the high pressure on these very dynamic markets, vulnerabilities are unfortunately unavoidable in the tens of millions of lines that every programme code contains. Full security (i.e., the complete absence of vulnerabilities) can arguably only be guaranteed in highly specialised systems such as NASA's software – and even then, at a cost that no commercial software vendor could feasibly bear. As vulnerabilities are unavoidable, there is always a risk that malicious individuals would try to discover them and seek to gain benefits from them, e.g., by placing ransomware. It is therefore that bug hunters, who try to discover vulnerabilities, have a socially, highly important function as they contribute potentially to cybersecurity.

This paper provided a detailed economic analysis of the incentives of the bug hunters as a collective group, assuming that they make rational choices between the so-called white, grey, and black markets. Not surprisingly, we found that the choice of the bug hunter to go for a specific market depends on a variety of elements, such as the legality of the market transaction, the price offered for the vulnerability and the role of intermediaries. We showed graphically that at some point in the choice between the black or the white market, the black market becomes less attractive when the bug hunters' costs on the black market sharply increase. That is more particularly the case when the severity of the vulnerability increases, leading to a higher probability of detection as well as of punishment. This leads to a first (pretty obvious) conclusion that society can benefit from increasing the probability of detection and the expected punishment as this makes the black-market transaction less attractive for bug hunters.

But our graphic illustrations also showed that there are other elements that the policymaker can take into account. One is that good reputation can have a profound impact on bug hunters. It may seem like an intangible incentive affecting the decision-making of the bug hunter, but in fact, it has monetary value. Bug hunters who disclose vulnerabilities through legitimate channels are often rewarded later with a promotion or a job offer. Moreover, as we stressed that increasing the expected costs of the black market may provide an important incentive for bug hunters to turn to the white market, there is a strong argument in favour of international cooperation. Again, the argument is straightforward: cybersecurity breaches and internet crimes always take place on a global market whereby cyber criminals benefit from the fact that law enforcement is limited to national borders. Cross-border international cooperation aiming at an increasing of the probability of detection can substantially increase the costs of bug hunters opting for the black market, thus making the white market again more attractive.

And finally, we pointed at the importance of the role of intermediaries. As their payment often depends on the price level of the vulnerability, they may have a (pervert) incentive to prefer the black market (as price is paid on that market for the vulnerability would be higher). That provides an important argument for monitoring and regulating these intermediaries in order to reduce the risk that through their intervention more bug hunters would be lured towards selling their vulnerabilities on the black market.

References

Ablon, Lillian; Bogart, Andy (2017), Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits, RAND Corporation, Santa Monica, CA, p xii., Available: www.rand.org/t/RR1751

Ablon, Lillian; Libicki, Martin; Golay, Andrea (2014), Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar, RAND CORPORATION (Mar. 2014), Available: http://www.rand.org/pubs/research_reports/RR610.html

Abu Elkhail, Abdulrahman; Refat, Rafi Ud Daula; Habre, Ricardo; Hafeez, Azeem; Bacha, Anys; Malik, Hafiz (2021), Vehicle Security: A Survey of Security Issues and Vulnerabilities, Malware Attacks and Defenses, IEEE Access, Vol. 9.2021, 162401–31.

Algarni, Abdullah; Malaiya Yashwant (2014), Software Vulnerability Markets: Discoverers and Buyers, World Academy of Science, Engineering and Technology, International Journal of Computer, Information Science and Engineering, Vol. 8, No. 3, pp 480–90.

Becker, Gary (1968), Crime and Punishment: An Economic Approach, *Journal of Political Economy*, Vol. 76, 169–217.

Cooter, Robert; Ulen, Thomas (2014), Law and Economics (6th edition), Pearson Education Limited.

Fidler, Mailyn (2015): Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis, I/S: A Journal of Law and Policy for the Information Society, Vol. 11.2, 406–83.

Goertzel, Karen (2016), Legal liability for bad software, *CrossTalk,* Sep./Oct. 2016, Vol. 29, No. 5, pp 23-28, Available: https://www.researchgate.net/publication/310674753

Herr, Trey; Schneier, Bruce; Morris, Christopher (2017), Taking Stock: Estimating Vulnerability Rediscovery, Belfer Center for Science and International Affairs (Harvard Kennedy School), Available: https://www.belfercenter.org/publication/taking-stock-estimating-vulnerability-rediscovery

Hörnle, Julia (2021), Internet Jurisdiction Law and Practice, Oxford University Press.

Johnstone, Ian; Sukumar, Arun; Trachtman, Joel (2023), Building an International Cybersecurity Regime, Edward Elgar Publishing.

Li, Yuchong; Liu, Qinghui (2021), A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, EnergyReports 7(2021)8176–86, https://www.sciencedirect.com/science/article/pii/S2352484721007289

Libicki, Martin; Ablon, Lillian; Webb, Tim (2015), The Defender's Dilemma: Charting a Course Toward Cybersecurity, RAND Corporation, Santa Monica.

McConnell, Steve (2004), Code Complete: A practical handbook of software construction, Microsoft Press, Redmond, Washington, Available: https://labs.sogeti.com/how-many-defects-are-too-many/

Mejía-Granda, Carlos M.; Fernández-Alemán, José L.; Carrillo-de-Gea, Juan M.; García-Berná, José A. (2023), Security Vulnerabilities in Healthcare: An Analysis of Medical Devices and Software, *Medical & Biological Engineering & Computing*, Available: http://doi.org/10.1007/s11517-023-02912-0

2022 Hacker-powered Security Report, 2018 Hacker Report, 2019 Hacker Report 2019, HackerOne, Available: https://www.hackerone.com/reports/6th-annual-hacker-powered-security-report

The Economist (2017): Why everything is hackable? The Economist, April 8th, 2017.

Zeng, Peng; Lin, Guanjun; Pan, Lei; Tai, Yongchang; Zhang, Jun (2020), Software Vulnerability Analysis and Discovery Using Deep Learning Techniques: A Survey, IEEE Access, Vol. 8. 2020, 162401–31, 197158–70.

Michael Faure is emeritus professor of comparative and international environmental law at Maastricht University and emeritus professor of comparative private law and economics at Erasmus School of Law Rotterdam. He is adjunct professor at the faculty of law of Universitas Indonesia.

Dr. Jian Jiang is research fellow at University of Haifa (Minerva Center for the Rule of Law under Extreme Conditions), distinguished research fellow at Fudan University (Center for Chinese Business Studies), and guest researcher at Maastricht University (Faculty of Law).

Cite this article: M Faure and J Jiang, "Deciphering Bug hunters – A Law and Economics Perspective". *European Journal of Risk Regulation.* https://doi.org/10.1017/err.2025.10044