Available online at www.ijournalse.org

Emerging Science Journal

(ISSN: 2610-9182)

Vol. 8, No. 4, August, 2024

A Digital Service for Citizens: Multi-Parameter Optimization Model for Cost-Benefit Analysis of Cybercrime and Cyberdefense

Constantinos Halkiopoulos [1*], Anastasios Papadopoulos [2], Yannis C. Stamatiou [2, 3], Leonidas Theodorakopoulos [1], Vasileios Vlachos [4]

[1] *Department of Management Science and Technology, University of Patras, 26334 Patras, Greece.*

[2] *Department of Business Administration, University of Patras, 26504 Patras, Greece.*

[3] *Computer Technology Institute and Press "Diophantus", University of Patras Campus, 26504 Patras, Greece.*

[4] *Department of Economics, University of Thessaly, GR-54124 Volos, Greece.*

Abstract

Objectives: This study discusses work performed within the context of the SAINT R&D project concerning the correlation of the prices of cybercrime services with the costs of investing in cyber security technologies. The main goal is to investigate how various financial and business-related cybercrime parameters relate to cybersecurity costs. In this context, the paper also examines the involved stakeholders and how they interact with each other. *Methods/Analysis:* Given the above considerations, from a theoretical standpoint, it is to describe a generic model for pricing illicit cybercrime products and services. This model, namely the Capacity Value Based Pricing (CVBP) model, has been proposed in the context of pricing "normal" products and services. Our study adapts this model suitably to apply the pricing modeling of illicit cybercrime products and services. *Findings:* The findings elucidate the professionalization of cybercrime, the significance of the emerging market for illicit services, and the pressing need for advanced AI methods to process qualitative data into quantitative insights. *Novelty/Improvement:* This paper contributes to establishing theoretical and econometric models vital for stakeholders navigating the financial terrain of the cybercrime economy. Future research should refine the methodologies presented and enhance data reliability for such critical analyses.

Keywords:
Cyber-Crime; Cyber-Defense;
Cost-Benefit Analysis;
CVBP Model; Decision-Makers;
Pricing Modeling;
Stakeholders.

Article History:

Received:	16	November	2023
Revised:	29	June	2024
Accepted:	07	July	2024
Published:	01	August	2024

1- Introduction

In the contemporary era of the 4th industrial revolution, providing digital services to citizens holds the utmost significance in guaranteeing effective governance and the delivery of public services. Moreover, the modern digital economy is based on the notion of secure electronic transactions to facilitate a healthy e-commerce ecosystem. Nevertheless, the escalating incidence of cybercrime presents substantial obstacles to the security and integrity of the digital transformation. Establishing a resilient cybersecurity framework is imperative to protect individuals' digital and physical assets as well as their personal data. This introductory section explores the convergence of digital services for individuals, emphasizing the necessity of a multi-parameter optimization model for cost-benefit analysis in the realm of cybercrime and cyberdefense. The escalation of cybercrime has emerged as a significant societal concern, as evidenced by the daily occurrence of cyberattacks that inflict substantial financial harm on nations, organizations, large enterprises, SMEs, and individuals. The dependence on digital services for various facets of our lives, such as government

* **CONTACT**: halkion@upatras.gr

DOI: http://dx.doi.org/10.28991/ESJ-2024-08-04-06

engagements, financial transactions, and personal communications, has led to an amplified susceptibility to cyberthreats. For various reasons, be they political or financial, cybercriminals find it particularly attractive to target the digital infrastructure of modern societies. Consequently, mitigating cybersecurity risks has become a significant concern, emphasizing the necessity of proactive measures to reduce cyber threats and safeguard digital assets. Building trust among citizens is crucial for the success of smart government services and the digital economy, serving as essential factors in the process of digital transformation. The multifaceted nature of addressing cyberthreats within the context is further emphasized by the impact of cybersecurity knowledge on attack detection and the determination of confiscation of evidence in cyber-crime [1, 2].

In this context, the main goal of this paper is to propose a generic but sufficiently practical model for some financial aspects of cybersecurity, such as how prices of illicit services are determined and how decisions to invest in cybersecurity are taken. The model aims to integrate the interests of all the main stakeholders, the costs and benefits associated with their decisions/actions, and the considerations on how these stakeholders maximize/optimize their revenues. The results we describe are parts of work conducted in the context of the SAINT project related to the correlation of the price of Deep Web digital goods with security methodologies, technologies, and legislation.

To achieve our goals, the approach we follow is based on two anchor points. The first stems from the results of our research efforts. We investigated existing literature concerning theoretical models of cybercrime and its financial aspects for stakeholders (e.g., targeted businesses and attackers). We noticed a lack of fine-grained multiparameter models that encompass, at the same time, all the relevant stakeholders, their decision-making processes, and their financial interactions, as well as parameters that reflect cost/benefit decisions. For instance, to the best of our efforts, we were not able to find literature about illicit service pricing models, which could be used as a vehicle for modeling the pricing decisions of illicit service developers under various constraints stemming from either legislation, persecution by law enforcement agencies, investment decisions, and investment sizes of businesses. These models are critically needed to strengthen businesses' defense strategies against cyberattacks. The second anchor point was that the World Wide Web and the Dark Web contain an immense volume of data and information primarily spread in human-readable formats such as pictures, histograms, and natural language text. However, the Dark Web is much less accessible than the web. As a result, primary data stemming directly from the Dark Web cannot be gathered in quantities that would allow us to derive reliable conclusions. Thus, in this study, we focus, apart from proposing a theoretical model, on developing a more practical model to consider the different financial aspects of cybercrime using statistical techniques rather than optimization formulations. These statistical instruments permit us to analyze the data we collected, mostly from the web, using the tools developed in the SAINT project.

Because of these challenges, our approach in this paper extends along two directions: a theoretical one based on suitable adaptations of a service pricing model (taken from the literature outside the cybercrime domain) and a more practical one based on the information gathered and analyzed by OSINT information sources and tools. Our goal is to demonstrate two key factors. Firstly, there is a clear negative correlation between the amount invested in enhancing cybersecurity and the efforts cybercriminals are willing to exert to attack well-protected entities. In other words, malicious actors act reasonably by targeting well-secured entities only when they anticipate significant gains. Otherwise, they seek soft targets that can be easily exploited, aiming to collect as much 'easy money' as possible." Secondly, the price of illicit services, also known as Cybercrime-as-a-Service (CaaS), serves as an indicator of the quality and strength of existing cybersecurity technologies. Effective cybersecurity technologies are challenging to bypass, leading cybercriminals to be willing to pay significantly more for techniques that can neutralize them, such as 0-day exploits. Even within the white-hat or ethical hacking community, bug bounties or security contests for secure applications are much higher than in the case of poorly maintained and insecure software. Our game-theoretical approach demonstrates that a robust cybersecurity policy can not only withstand massive 'blind' cyberattacks but also serve as a strong deterrent against targeted intrusion attempts by more determined and capable cybercrime groups. The Latin quote "Si vis pacem, para bellum" appears to be effective even in cyberspace.

The paper is organized as follows: Section 2 cites related work focused on cybercrime modeling and its financial impact. Section 3 explains the approach to modeling the financial aspects of cybercrime and how they influence the decisions of defenders and attackers to defend or attack, respectively. Section 4 identifies the main stakeholders involved in the proposed model. Section 5 describes a simple theoretical 2-person game central to the model, which can be used to compute equilibrium points where defenders and attackers make optimal decisions regarding investment in defense measures or attack efforts. Section 6 discusses the *Capacity and Value-Based Pricing* (CVBP) model, proposed for optimally determining digital goods prices based on developers' and buyers' characteristics and capacities, and how it can be applied to model the valuation of illicit goods and services by developers, depending on buyers' needs. Section 7 outlines an approach for cost/benefit analysis for defenders, modeling the decision process of investing or not investing in cybersecurity defense measures. Section 8 presents the approach for cost/benefit analysis for attackers, modeling their decision to invest in or abstain from attacking an organization. Section 9 adapts the game described in Section 5 to account for the cost/benefit analysis of both attackers and defenders, leading to the computation of corresponding equilibria. Finally, Section 10 concludes the paper and suggests directions for future research.

2- Literature Review

The cybercrime landscape is undergoing changes, characterized by the emergence of advanced hacker groups and the prevalence of Advanced Persistent Threats (APTs), which present substantial obstacles to the field of cybersecurity. As highlighted in the current literature [3], most damaging cyberattacks are nowadays conducted by well-organized and focused cybercrimegroups rather than single hackers who seek peer recognition and glory and temporary monetary rewards (i.e., "pocket money"). However, APTs do not follow the mode of operation of cybercriminals in terms of motivation, rewards, and investment in cybercrime. Our research delves into the intricate characteristics of cybercrime, with a specific emphasis on hacker collectives, and the operational dynamics of the cybercrime ecosystem, and, thus, we will not include APTs but other types of illicit cybercrime products and services. For instance, the latest trends indicate an explosion of ransomware attacks, demonstrating that the primary motive for most cybercriminals is financial gain. Organized cybercrimegroups have emerged as a notable element within the realm of cybercrime, exhibiting a scope that surpasses individual exploits and encompasses collaborative and structured criminal endeavors.

All advanced nations are actively working towards improving their ability to defend against cybercrime and are continuously seeking to reform their cybersecurity capabilities [4, 5]. To succeed in this goal, it is crucial to develop a fine-grained multi-parameter optimization model for conducting a cost-benefit analysis to effectively examine the intricate dynamics among cybercrime, and cyberdefense. The proposed model should consider the economic, social, and technical dimensions of cybercrime, incorporating perspectives from diverse fields, including computer science, economics, and public policy. By integrating these various viewpoints, it becomes feasible to construct an analytical framework that guarantees the durability and protection of essential digital services amidst the increasing challenges posed by cyberthreats. For instance, Lagazio et al. (2014) [6] proposed a multi-level approach through a thorough literature review to comprehend the ramifications of cybercrime on the financial sector. This approach highlights the interconnected and distinct factors that influence cybercrime and its economic and social costs. This approach follows the requirement for a model that considers multiple parameters. Furthermore, the significance of employing multi-agent modeling and simulation in cyberdefense was underscored, particularly in evaluating the repercussions of intricate occurrences on vital infrastructure and resources [7]. This statement supports the advancement of a theoretical framework capable of evaluating the cost-benefit analysis of strategies employed in cyberdefense.

Moreover, an extensive investigation has been carried out to examine the financial implications of cybercrime, focusing on the importance of precisely assessing its economic consequences [8]. This research offers significant contributions to understanding cybercrime's economic dimensions, which are essential for conducting an extensive cost-benefit analysis. Additionally, Ospina et al. (2023) [9] made a significant contribution by proposing a quantitative approach to enhance the security of cyber-physical energy systems. This approach considers the physical and cyber network vulnerabilities and employs a multi-criteria decision-making technique. Integrating this method into the optimization model allows for evaluating the cost-effectiveness of cyberdefense strategies within energy systems. Furthermore, Bilen & Özer (2021) [2] conducted a study that centered on predicting cyber-attacks through utilizing machine learning algorithms. The authors emphasized the significance of diverse datasets and parameters associated with cybercrime. The observation mentioned above holds significant value in developing a realistic optimization model that considers a range of cyber-attack scenarios. Furthermore, it highlights the constraints of current cyberdefense frameworks in managing multi-phase attacks characterized by uncertainty and contradictory information [10, 11]. This highlights the necessity of employing a sophisticated optimization model to tackle these challenges effectively. In summary, developing a multi-parameter optimization model for conducting a cost-benefit analysis of cybercrime and cyberdefense necessitates a new approach that considers cybercrime's economic, social, and technical dimensions.

Armin et al. (2020) [12] identified serious research gaps in the quantification and measurement of the spread and severity of cybercrime in our days and its impact as well as its financial effects on markets of different sectors. In addition to the lack of quantification, there is a lack of industry-related best practices, which prevents the development of a more precise and more accurate understanding of the actual "cost of cybercrime", both concerning the pricing of illicit services and the pricing (or cost) of strengthening cybersecurity.

The study conducted by Dupont et al. (2017) [13] examines the social and market dynamics of Darkode, a restricted cybercrime forum, providing insights into the recruitment patterns and transactional characteristics of this infamous hacker community [14]. Moreover, the study offers valuable perspectives on the varied identities and behaviors exhibited by hacker collectives, highlighting the complex and multifarious characteristics of these entities within the realm of cybercrime activities [15]. Concurrently, the rise of Advanced Persistent Threats (APTs) has generated apprehension regarding the persistent and covert cyber risks that specifically target crucial infrastructure and confidential information. On the other hand, most, if not all, APT groups are state-sponsored and, therefore, do not pursue financial rewards; instead, they aim to weaponize the digital infrastructure of enemy nations. Since their objective is not profit maximization but rather the paralysis of other countries, as well as the fact that they receive direct support from foreign governments, they are not well-suited for our model.

The study by Yip et al. (2013) [16] examines the potential risks presented by cybercrimegroups that mostly specialize in ransomware attacks and emphasizes the significance of advanced technologies in the field of cybercrime investigations. Furthermore, the study investigates the trust dynamics within carding forums among cybercriminals, shedding light on the organizational structures that enable organized cybercrime and reduce transaction expenses [17]. Gaining insight into the subcultures and motivations of cybercriminals is imperative to effectively address and mitigate cyberthreats. It specifically draws attention to the interconnectedness between hacking activities and the processes of radicalization, as well as the manifestation of terrorist behaviors [18]. Furthermore, the research presented in this study serves to question the prevailing perception of cybercrime as an activity conducted in anonymity. It provides valuable insights into the concealed aspects of cybercrime, as well as its offline manifestations and local implications [19]. The study of the economic and systemic consequences of cybercrime is a crucial field of research that sheds light on the overall risk posed by cyber threats and the cumulative effects they have. This research highlights the diverse nature and patterns of cyber incidents, as well as the associated financial burdens they impose [20].

Moreover, the study emphasizes the worldwide proliferation of cybercrime enterprises by non-state entities, thereby emphasizing the imperative to tackle cyber threats within the framework of both international development and security. In summary, this study highlights the intricate and varied nature of cybercrime, which encompasses a range of actors such as hackers groups, advanced persistent threats (APTs), subcultural dynamics, and systemic consequences. Through the synthesis of various perspectives, a deep understanding of the emerging cybercrime model can be attained, thereby enabling the development of effective strategies to counter evolving cyber threats.

Additionally, over the recent years, cyberattacks have increasingly been launched by *well-organized*, focused groups operating professionally, mimicking the functioning of real businesses in the ICT domain [12, 21–23]. All successful cybercrimegroups follow a well-organized structure and a group of various people with different skills and expertise, which resemble how regular ICT companies do business. As a result, they can be expected to rely on similar pricing models as legitimate businesses.

Arguably, organized cybercrime [24] appears as the most worrisome of present and future threats to businesses and our societies, given our increasing reliance on digital technologies. Although cybercrime groups are primarily active in ransomware, we take a more relaxed view to include groups offering cybercrime services as regular ICT businesses with legitimate products and services.

The stakeholders populating this ecosystem include other cybercrime groups, businesses, individuals, and law enforcement agencies. Cybercrime groups essentially design and develop illicit services *on demand*, acting much like a professional software solutions development business, upon receiving specific orders from interested parties (possibly even from governmental agencies, as it is discussed in Broadhurst et al. (2014) [21], to whom they sell their illicit services and products. As a professional illicit service developer, a ransomware group employs cybercrime specialists, invests in infrastructure and software tools, and, in general, acts much like a business operating in the services development domain, charging a given price for its services, making a profit, enduring costs, and facing competition from other cybercrime groups. Members of ransomware groups expend considerable effort to combine multiple attack methodologies and toolsets, aiming to penetrate well-protected targets. Ransomware groups operate with a high level of professionalism—methodical, orderly, and focused on achieving their set goals. This requires constant monitoring, feedback, and corrective actions, much like completing a significant software project; therefore, ransomware groups pose a severe threat level because their workforce is very skilled and also very determined. These characteristics render ransomware development a particularly suitable target for our model since it follows, in some sense, a pricing/selling process similar to the process followed by sellers of legal goods and services.

In summary, the picture that emerges is that the cybercrime market is transforming into an ecosystem operated by several loosely coupled hacker groups and professionals that cooperate but also compete against each other, much like in the real economy. This competition tends to drive down the prices of the illicit goods and services they offer. Similar to any business, their strategies are built on cost-benefit analyses to thrive as legitimate players in the black-market economy.

3- Modeling Scope, Assumptions, and Limitations

The cybercrime landscape is highly complex, fast-changing, and includes several stakeholders. Its financial aspects are equally complex, and a complete coverage of them is impossible within a single model, at least within the scope and lifetime of this project. Here, we outline the first necessary steps to model the numerous criminal financial interactions in cyberspace, which call for further refinements once more accurate data and information about the involved stakeholders becomes available. The main objective of the proposed methodology rests on the following assumption: as a general rule, the more secure a technology or application is, the higher the regard for a security researcher or an ethical hacker will be. Similarly, the more protected a target is, the more effort and tools most cybercriminals are willing to invest in order to reap greater gains. These directly contradictory motives between security professionals and cybercriminals are formulating the foundation of our game-theoretic approach.

We gather information for our model from various resources. One such source is information about the cost of damage from organizations that have been cyberattack victims. "Victim organizations" are unwilling to release such information for obvious reasons (e.g., to avoid further tarnishing their image and reputation on the market). Also, pricing information for illicit services and products can probably be found, as demonstrated indirectly by our work with the SAINT tools through legal information sources. In the SAINT project, we explored and analyzed data from ethical hacking platforms such as bug bounties and vulnerability discovery programs. It was more challenging to obtain pricing information directly from the Dark Web. Despite our best efforts, we developed a Deep Web Crawler with limited success, which did not manage to acquire data from various Black Markets. The lesson learned from the partially successful endeavor with the SAINT Deep Web Crawler was that most Black Markets enforce stringent operational security (OPSEC), incorporating strong authentication mechanisms, rigorous monitoring of registered members, and access limited to join-by-invitation only. Nonetheless, we managed to locate dumps of hacked Black Markets, which were made available for research purposes. As a result, we managed to obtain approximate estimates about the prices of illicit digital goods, which we then used to compare to prices that the proposed model derives.

Another significant point is that, although the Internet contains a vast amount of cybersecurity and cyberattack-related information, this information is not easily exploitable by automated means. There is a large volume of publicly available literature related to the financial aspects of cybercrime, but it is often uncategorized and fragmented. This literature forms a secondary information source about the cybercrime ecosystem and its impact on businesses and society. These documents include quantitative and qualitative studies, surveys on the cost of successful cyberattacks on companies (with results typically reported at an aggregate level to protect victims' anonymity), cybercrime field analyses conducted by security companies, specialists, researchers, and state agencies, as well as bug bounties, vulnerability/exploit/attack repositories, white-collar hacker organizations, and even non-technical articles on well-established mass media sites. While most secondary sources are directly and easily accessible, some are scarce, such as those on 0-day vulnerability exploit prices. For example, Zerodium provides such information, which can be used within the SAINT project's development framework for gathering data with a Deep Web crawler. However, Zerodium publishes information only in image format, not text, making it difficult to extract using automated methods, as this requires advanced image processing and OCR (Optical Character Recognition) techniques, which are beyond the scope of this paper. The primary issue with this extensive quantitative and qualitative data is that it is primarily presented in a format understandable by humans and not necessarily suitable for machine-based analyses. Only a few sites offer information in a standard, machine-readable format (e.g., CVE, XLS, HTML, XML, etc.), such as the HackerOne bug bounty site.

One of the main objectives of our work is the promotion of the exploitation of such information sources in modeling the financial aspects of cybercrime. The model we propose in this paper builds on a moderate, pragmatic, and immediately applicable approach, which will pave the way to the above-mentioned approaches. We take a realistic but simplified view of the complex ecosystem of cybersecurity to provide a fully quantitative, machine-workable model for the financial aspects of cybersecurity. Among other simplifications, we limit the number of potential stakeholders that interact in the cybersecurity ecosystem, and we have set aside considerations of certain categories of costs, mostly intangible ones, related to cybercrime to reduce the complexity of the analysis. For instance, we do not consider individuals as a class of stakeholders; we ignore societal costs and disruptions costs that may affect the daily lives of people following the occurrence of a cyberattack directed, for example, at a utility operator.

Our goal in this paper is to start "small" and within a moderate scale to propose a simple, fully quantitative, and algorithmic theoretical model, which we will study concerning its applicability potential and its aptitude to address the financial aspects of cybercrime and cybersecurity. We also propose a more practical model based on the information gathered by the tools developed by SAINT in order to provide a more directly applicable model to complement the theoretical one, whose validation is more demanding and cannot be accomplished within the scope of the project. However, attempts to achieve at least partial validation will be implemented.

In summary, the model we propose targets the following goals:

- To develop a multi-parameter theoretical model that links various parameters that model and reflect financial aspects of cybercrime according to stakeholders' interests and illicit service developers' financial goals.
- To propose a decision support tool for organizations targeted by cybercriminals that will quantify the costs and benefits of investing in cybersecurity and will allow decision-makers to make well-supported (by data and theory) decisions about if, when, and how much to invest in their defense against cybercrime.
- To obtain a better understanding of the financial aspects of cybercrime for all involved stakeholders.
- To obtain a better understanding of the motives for investing in cyber-security from an exposed organization's point of view and the motives of engaging in cyber-criminal activities from an illicit service developer's point of view.
- To show how primary and secondary information sources can be exploited in order to provide values for the parameters of the model.

Below we provide an overview of the flowchart of the proposed methodology:

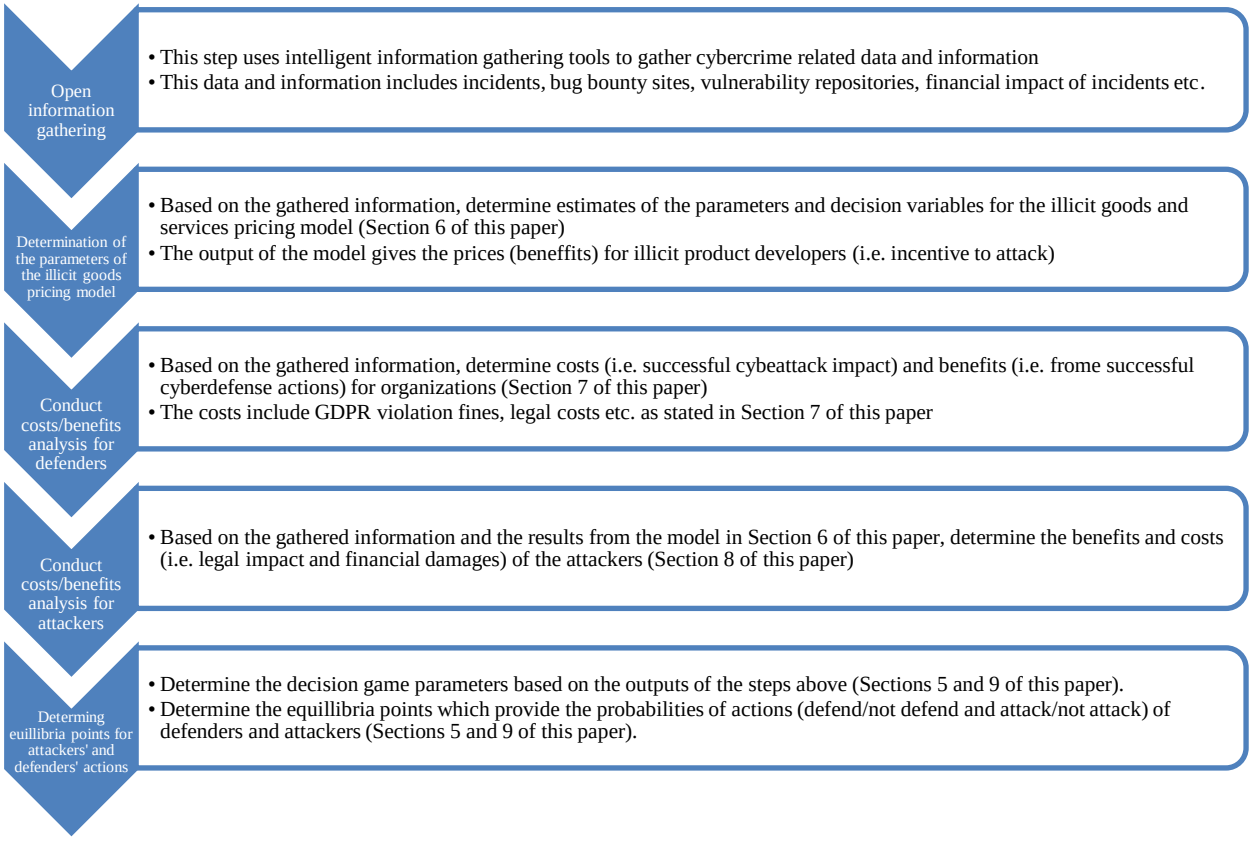

Figure 1. Flowchart of the methodology

4- Principal Stakeholders in the Emerging Cybercrime Economy

This section lists the most relevant types of stakeholders that coexist and interact in the emerging cybercrime economy. These stakeholders will be represented through specific parameters and variables in the model we introduce in the subsequent sections.

4-1- Illicit Service Developers

As explained in the introduction, illicit service developers fall into the cybercrime framework: they are dedicated and focused professional groups that operate like regular service-developing businesses. Therefore, these groups obey the same market rules as any other type of business: they face competition, hire and pay highly skilled personnel, set the price of their services, try to maximize their profit, and minimize their operational costs simultaneously.

Most of the following skills and roles are actively sought among cybercriminals, according to a representative of the US Federal Bureau of Investigation's Cyber Division [22]:

- ***Malware Developers***: The development of new malware strains to infect potential victims typically involves an automated process using a Malware Generator Kit. This kit can continually enhance and mutate malicious code to evade detection from antivirus (AV) engines. Techniques employed for this purpose include polymorphism, metamorphism, and code obfuscation. Groups developing these malware generator tools provide other cybercriminals with the option to order new malware, ensuring it comes with a guarantee of non-detection by AV software. The repetitive purchasing of new malware strains can be cost-prohibitive. In response, cybercrime groups provide their customers with the option to invest in a Malware Generator Kit as a one-time purchase, offering a potentially better Return on Investment (ROI). The provision of malware to interested parties as a commodity is known as MaaS (Malware-as-a-Service). Malware is developed by programmers skilled in both high- and low-level computer languages who devote their efforts to discovering vulnerabilities in targeted systems and designing exploits. They create sophisticated malware, discover software exploits, modify penetration tools to suit their needs, and manipulate any ICT component necessary to fulfill an illicit service development assignment.
- ***Exploit Brokers***: Typically, they are black-hat hackers who develop and sell 0-day exploits to the highest bidder. There are also vendors and brokers who trade knowledge about specific vulnerabilities and exploits, but they operate in a gray area, supposedly selling only to law enforcement agencies of democratic countries. On the other

hand, white-hat hackers and security researchers, when they discover a critical vulnerability, will responsibly disclose it and may claim a bug bounty if the owner has a similar program. In our work, we categorize black-hat hackers as offensive operators and ethical hackers as defensive. Given the complexity of the gray market of vulnerabilities and exploits, we decided not to include them in our model.

- ***Bulletproof Service and Infrastructure Providers***: Companies that operate in a gray area at the boundaries of the law are preferred by criminals to host fraudulent websites, obtain IP addresses, and domain names, as these companies ask no questions whatsoever regarding the nature of their clients' businesses. More importantly, bulletproof service providers take a very long time to comply with law enforcement requests to take down offending services and share information about their clients, as they often fail to keep records, providing a safe harbor for the cybercriminals.
- ***Black Markets***: They offer covert and secure storage facilities for illicit services, stolen information, data for sale, and targeted sites. Additionally, they provide anonymity services via sophisticated botnets and proxy infrastructures using infected systems. Black Markets operate in the Deep Web and function as one-stop shops for various criminal activities, including cybercrime. Many bad actors offer their illicit services in one or more Black Markets.
- ***Spamming and Infection Campaigns***: Fraud specialists design and deploy various social engineering methods, such as phishing, spamming, and domain squatting, to infect as many systems as possible and deliver the malicious payload. Spamming serves as their preferred method of attack.
- Administrators and support technicians: These individuals play a crucial role in supporting developers by creating and maintaining development infrastructures. This includes managing servers, configuring operating systems, enforcing security operations, deleting tracks, and encrypting sensitive information.
- ***Money Laundering Operators***: These individuals, often referred to as 'cashers,' oversee drop accounts—typically addresses for receiving payments in digital currencies such as Bitcoin and Monero. Cashers also frequently supervise individual cash couriers, known in criminal jargon as 'money mules.' Money mules are usually unsuspecting individuals who transfer earnings from illicit services or products to other secure locations or accounts, believing they are engaged in a lawful job. The 'tellers,' who assist in the money laundering of illicit services through digital currency transactions and other fiat currencies, control the money mules. All of them operate under the authority of 'cybercrime bosses' who manage client relations, negotiate deals, recruit skilled personnel, define strategies, and oversee the distribution of earnings.

The proposed model includes the skill parameter and the human resources/costs needed to develop illicit services (the cost parameters), as both influence the decision variables. While obtaining relevant information directly from primary sources (e.g., contacting specific hackers or cybercrime groups) is challenging, one can rely on 'educated guesses' derived from estimates found in leaked private communications between cybercriminals, hacked databases, and forums of black markets.

4-2- Targeted Organizations

The targeted organizations are those most attractive to illicit service developers, i.e., those that offer the highest return on investment (ROI) when attacked. In the proposed model, we categorize the victim organizations through the sector in which they are active since cyberattack costs for a victim organization appear to differ significantly depending on the sector [25]. We have identified some of the main sectors and the typical failures in cybersecurity that characterize them and induce the corresponding damage costs on the victim organizations. These sectors include the following: Healthcare, Utilities (including smart energy grids, innovative metering systems, water supply, electricity production, nuclear factories, etc.), Transportation, Social Networks, Financial Institutions, and the IoT. The proposed model includes the sector parameter since the afflicted cost parameter differs according to the sector where a victim organization is active.

Specifically, the cost parameter for the targeted organizations includes various cost types, all of which are incorporated in the proposed model:

- Proactive costs are those incurred by an organization during regular operations to enhance its security against cyberattacks and reduce vulnerabilities in its systems. Examples of such costs include payments made to security companies for penetration tests, formal security analyses of networks and deployed cybersecurity products, and checks for compliance with legislation (e.g., GDPR compliance and certification). These costs, which are integrated into the proposed model, can be estimated based on service prices set by security companies or by contacting organizations that consistently invest in proactive security measures. This approach ensures that the estimates reflect current security market prices.
- Remedial costs refer to expenses incurred by the victim organization's infrastructure and business operations as a result of a successful cyberattack. The proposed model utilizes the afflicted damage costs model from the Deloitte

research report (2016) [26] to quantify these costs. Our research indicates that this model is both comprehensive and realistic, and the two example applications provided in the cited research report support this assertion.

- Third-Party and Law Enforcement Agencies Liabilities: These are the afflicted costs resulting from lawsuits and penalties imposed by legislation such as the GDPR in Europe. Our model includes these costs as a parameter in determining an organization's cost and benefit balance to provide decision guidance.

4-3- Illicit Service Clients

This stakeholder category comprises the users of illicit services offered by illicit service-developing groups. Most often, these users are other cybercrime groups with limited capabilities in the development of efficient malware and an insufficient understanding of effective delivery methods to their targets. In rare situations, the clients may include governments of rogue countries seeking plausible deniability or corrupted industrial parties aiming to inflict damages on their competitors.

The proposed model includes various service user types in the form of parameters that define their different benefits, the prices they are willing to pay, and the utility each user type assigns to the different services offered on the illicit service market. As a final remark, the proposed model allows the illicit service users to coincide with the illicit service developers, as is usually the case of customary hackers or hacker teams that design, implement, orchestrate, and launch their attacks themselves.

4-4- Security Solutions Developers

This stakeholder group includes companies specializing in cybersecurity solutions and in the security analysis of the ICT infrastructures and company data of other organizations, as agreed by the contract terms. The prices that the security companies charge for these services are included in the proposed model within the cost/benefits factor, which determines whether organizations decide to invest in cybersecurity solutions.

4-5- Law Enforcement Agencies and The Judicial System

The function of this stakeholder group in the model is twofold. First, law enforcement agencies act as a deterrent or, if the crime is committed, as a prosecution instrument for perpetrators. Beyond this function, law enforcement agencies incentivize organizations to invest in security solutions to avoid punishment for non-compliance with security and customer privacy legislation (e.g., GDPR in Europe [27]).

The proposed model incorporates all these aspects of the role of law enforcement agencies and the judicial system, showcasing their efficiency in addressing cybercrime and its impact on targeted organizations. These factors directly influence the financial parameters of the model and play a key role in decisions regarding investments in security solutions for targeted organizations or engaging in cybercrime for illicit service providers.

5- Modeling Main Stakeholders' Decisions: A Simple Attack-Defense Game and its Equilibria

Game Theory is a framework for modeling stakeholder decisions. Among the available game theoretical techniques and decision models, we decided to adopt a simple two-agent, complete information, non-cooperative game for modeling the decisions of the two main stakeholders: the targeted organization and the illicit service developer/user. The two decisions are for each player, respectively, "invest/not invest in defense" and "invest/do not invest in attack".

There have been numerous proposals for games that model security-related situations, but simplicity, fast solvability, and direct applicability to our goals were our main selection criteria within the scope of this paper. The game we describe in the present study is slightly altered in notation to reflect our specific context. Table 1 presents the usual representation of the chosen game (see, also, [28] for more details and a deeper analysis, as well as [29] for an excellent introduction to Game Theory).

Table 1. A simple two-person attack/defense game

	Invest in attack	**Do not invest in attack**
Invest in defense	$(a, -\beta)$	$(-b, 0)$
Do not invest in defense	$(-c, \gamma)$	$(0,0)$

In this setting, one of the two players is displayed in the rows, and the other player is displayed in the columns of the table. This game allows only simultaneous decisions, i.e., the two players decide independently of each other and simultaneously on their actions. This is in contrast with sequential games where one of the two players takes the first decision and then the other one follows. In such games, the ordering of the players is important. However, we believe that in cybersecurity-related game situations it is most appropriate to study *simultaneous* moves of the defender and

attacker since, usually, cybersecurity investments or decisions to attack are not publicly announced. The exception to this is if espionage or information leak takes place, cases which we do not consider here for simplicity. To handle these cases would require the use of the sequential game model or even a mixture of the simultaneous and sequential models, which, however, would complicate our study beyond the scope of our work.

Continuing our discussion on the game's characteristics, the players' *payoff values* (we changed, slightly, the letters used in Alpcan & Basar (2003) [28] to improve readability) are positive real numbers, and the relationship between these parameters defines the outcome of the game (i.e., the game *equilibrium).* The payoff values used here result from the model that is described in the above sections [28, 29].

Based on the information in Table 1, we can interpret the numbers (players' payoffs) as follows:

- Upper-left corner, $(a, -\beta)$: This is the case where both players do invest in either security to strengthen defense (the defender), or in attack (the cyber-criminal). In this case, we assume that the payoff for the defender is positive (the value can be estimated within the context of the model that we propose in this paper), while the payoff for the attacker is negative (which can also be estimated in the context of the proposed model). The latter negative payoff results from the fact that the investment of the attacker is not sufficient to countervail the increase in cyber-security implemented by the defender.
- Lower-left corner, $(-c, \gamma)$: This is the case where the defender has decided not to invest in cybersecurity measures while the attacker has decided to invest in developing and/or implementing an attack. In this case, the damages inflicted on the defender are reflected by the negative payoff value "$-c$" (which can be estimated in the context of the proposed model), while the success of the attacker is reflected by the positive payoff value given by "γ" (which can also be estimated by the proposed model).
- Upper-right corner, $(-b, 0)$: This is the case where the defender is not an attractive or feasible target for the attacker, but he/she still decides to invest in cybersecurity. In that case, the defender's strategy involves unnecessary spending and makes him/her worse off than without investment in cyber-security (as displayed by the negative payoff value "$-b$"). As for the attacker, the payoff is 0 since no attack has been launched.
- Lower-right corner, $(0,0)$: This is the easiest case, where none of the two players takes some action, i.e. the defender does not invest in defense and the attacker does not invest in attack. The payoffs are 0 for both players.

According to the theoretical analysis of this simple (but practical) decision model [29] for the mathematical and algorithmic details), under the rather reasonable condition that $c > 2b$, (i.e. not investing in defense inflicts on the organization theoretically more than double the cost than investing in defense, see the discussion in the model described in Section), there exists a unique *Nash Equilibrium* (*NE)* in *mixed strategies*. This unique NE point is shown in Table 2:

Table 2. The (unique) Nash equilibrium in mixed strategies

	Invest in attack	**Do nothing**
Invest in defense	$\left(\frac{\gamma}{\beta+\gamma}, \frac{b}{a+b+c}\right)$	$\left(\frac{\gamma}{\beta+\gamma}, \frac{a+c}{a+b+c}\right)$
Do nothing	$\left(\frac{\beta}{\beta+\gamma}, \frac{b}{a+b+c}\right)$	$\left(\frac{\beta}{\beta+\gamma}, \frac{a+c}{a+b+c}\right)$

In this table, the values that appear in the parentheses represent *probabilities* of choosing the corresponding strategies. For instance, based on the table we see that the targeted organization decides to "invest in defense" with probability i.e. rate of adoption $\frac{\gamma}{\beta+\gamma}$ and decides to "do nothing" with probability $\frac{\beta}{\beta+\gamma}$. Similarly, the illicit service developer decides to "invest in attack" with probability $\frac{b}{a+b+c}$ and decides to "do nothing" with probability $\frac{a+c}{a+b+c}$.

As pointed out in Alpcan (2003) [28], the mixed strategy choices of the players in the NE makes the opponent players indifferent as to which decision to take as all choices appear equally optimal given the opponents' choices (this is a well-known fact in Game Theory – [29]).

6- Modeling Illicit Service Developers' Service Pricing

6-1- The model's Variables and Parameters

The *Capacity and Value Based Pricing* (CVBP) model was proposed in Wardell et al. (2008) [30], and it is composed of several variables and parameters. The main idea of the model is that the *service developer*, in our case the *illicit* service developer, serves a number of *customers*, in our case illicit service buyers, under a contract whose value depends on several parameters such as customer type (e.g., government, lone hacker, industrial, etc.), delivery time, available resources of the service developer and their cost, the utilities of the services to the customers that order them, etc. The

model defines an *optimization problem* that allows the service provider to maximize profits by suitably selecting prices for the services it offers to customers, considering constraints and parameters defined by the model [31]. This optimization function considers several interplay interactions among the parameters and variables to take into account all stakeholders' interests [32].

In the following, we define the model's variables and parameters, adapting the definitions from Wardell et al. (2008) [30] where necessary. We also explain their role in the proposed, in this paper, model for modeling the financial aspects of cybersecurity and the interests of the involved stakeholders and customer categories.

- N: this is the number of customer segments, i.e. categories of criminals, that have been identified in the cybercrime territory using contracted illicit services. Of course, this parameter can be adjusted to reflect the number of customer types we consider each time we need to use the model. In general, the cybercrime markets for a specific illicit service or product can be segmented with respect to how each customer segment values, assigning specific utility values in the proposed model, a service or product (e.g. malware or a specific exploit kit). Thus, cybercriminal groups can set the prices of their illicit services as a function of specific parameters associated with a particular class of customers. A customer segment can even be a singleton, i.e. a group consisting of a single customer where prices are adjusted to the needs of a specific individual. Frequently, customer segmentation is performed in a straightforward way according to, for instance, whether the customer is a governmental intelligence agency, an individual hacker, an industry player, a political regime etc. The adapted model can handle any segmentation type or size and it outputs a range of illicit service prices tailored to the needs and utilities of each customer type separately.
- M: this parameter denotes the total number of active assignments or contracts. An assignment to the illicit service developer consists of the development of one or more illicit services or products (i.e. a "service bundle") under a contract with a customer coming from one of the customer segments predefined in the model.
- S: this is the number of business sectors in which organizations which are targeted by the illicit service developers and their customers (i.e. illicit service users) are active. To avoid overloading the notation, we can incorporate this parameter into other parameters, e.g. the cost parameters of a data breach.
- T: this parameter denotes the number of time instances (discrete time interval) considered. The model performs illicit service price (i.e. profits) optimization within a predefined time interval consisting of T time instances (e.g. days or months, depending on the desired time granularity). The model allows choosing a time interval as a parameter since illicit service pricing and profits may depend on the time and length of the targeted time period (e.g. prices may fluctuate depending on whether targeted police persecution is active or not, for instance).
- R: this is the number of professional specialties or skills which are required by an illicit service developer in order to meet his/her customers' challenges. The required specialties for such services directly affect prices since they form part of the total operational costs of a developer r.
- d_i^s: is the total demand over all engagements assigned by a customer segment i, at a specific time period s. Estimates of this parameter may be deduced through the history of transactions of the illicit service developer with the various customer segments.
- μ_{ij}: This parameter denotes the average length of a contract assignment in days, for contract type j and for customer segment i. This parameter affects the costs parameter of the illicit service provider for completing a contract assignment.
- ρ_k^t: denotes the daily pay rate for a skill/specialty of type k, when used for the time period t.
- z_k^t: reflects the available "quantity" of a particular skill of specialty type k, at time period t. This is a critical parameter that affects pricing as well as the availability of human resources for future assignments.
- v_{ij}: this parameter is the utility a customer from segment i enjoys from the work performed under a contract assignment of type j, without considering the cost of the contract. In other words, the utility reflects how a customer feels about receiving the illicit service described in the contract assignment.
- ζ_{ij}: is the sensitivity of customers from segment i to the price of the service with contract assignment type j.
- β_{ij}: this parameter reflects the sensitivity of customers belonging in customer segment i to a delay in the start of work for a contract assignment of type j. With this parameter, the model captures how a specific customer segment feels about delays in the start of the execution of the work described in the contract they have with the illicit service developer.

In general, the sets of parameters v, ζ and β are estimated through transaction history information about an illicit service developer's customers choice or may be estimated using surveys on experts' opinions (since it is difficult to obtain information from Dark Web sources).

- Θ: is a parameter of the Logit probability function that indicates the level of uncertainty of customers when making choices (see [30] and [33] for more explanations on discrete choice models and their parameters as well as the use of logit functions).
- $A \in \mathbb{R}^{M \times R}$: this is the daily staffing matrix where matrix element a_{jk} represents the percentage of time that an individual possessing skill of type k is assigned to tasks related to contract assignment of type j.

6-2- The Decision Variables of the Model

The model's primary optimization variables are the prices of the illicit services [34]. Variations of prices affect other model variables, such as customer utility and the probabilities of choosing a particular service, as these two variables are interdependent.

As a result, the main decision variables of the model are the following:

- r_{ij}^{st}: these are the principal optimization variables of the model, i.e. the prices that illicit service developers assign to their illicit goods within a contract. More specifically, this variable denotes the price of a contract for a service of type j for a customer from customer segment i, given that the current time instance is s, and the work on the contract will start at time period t, i.e. the illicit service developer will delay the execution of the contract by a time period t. In what follows, r denotes the price vector r_{ij}^{st} for all possible values of the subscripts and superscripts.
- $U_{ij}^{st}(r)$: this variable denotes the utility of a customer from segment i for an engagement of type j, given that the current time instance is period s and the assignment in the contract starts at instance t. The utilities are functions of the prices of the services.
- $p_{ij}^{st}(r)$: this crucial variable denotes the probability that a customer from segment i will decide to form a contract for a service of type j, given that the current time period is s and the assignment in the contract starts at time t. These probabilities are functions of both the illicit service prices and the customers' expressed utilities from "consuming" these service (see below).
- $g_i^t(r)$: denotes the expected number of active contract assignments for services of type j at time instance t. These are functions of both the prices and probabilities of selecting the available service types.

6-3- The Constrained Price Optimization Problem

The model's primary optimization variables are the prices of the illicit services. Variations of prices affect other model variables, such as customer utility and the probabilities of choosing a particular service, as these two variables are interdependent.

The goal of the chosen model is to define the prices of illicit services that maximize the following *objective function:*

$$max_r \sum_{j=1}^{M} \sum_{t=1}^{T} \left[\sum_{s=1}^{t} \left(\sum_{i=1}^{N} d_i^s \, p_{ij}^{st}(r) r_{ij}^{st} - g_j^t(r) \sum_{k=1}^{R} a_{jk} \, p_k^t \right) \right] \quad (1)$$

Without the maximization operator, i.e. given a specific price vector, the expression above gives the *expected profit* over the specific *time frame* under consideration:

$$PROFIT_{ij}^{st}(r) = d_i^s p_{ij}^{st}(r) r_{ij}^{st} - g_j^t(r) \sum_{k=1}^{R} a_{jk} \, p_k^t \quad (2)$$

More specifically, the equation above gives the net profit gained by the illicit service developer if the developer uses the price vector r for its contracted services of type i, for customers coming from customer segment j and for contracts signed at time instance s that will start at time instance t. The first term, $d_i^s p_{ij}^{st}(r) r_{ij}^{st}$, gives the gross profit while the second term $g_j^t(r) \sum_{k=1}^{R} a_{jk} \, p_k^t$ gives the expenses due to the engagement of skilled personnel (i.e. salary expenses).

The maximization problem is, also, constrained by the following relationship:

$$\sum_{j=1}^{M} a_{jk} g_j^t(r) \leq z_k^t, \forall_t = 1 \dots T, \forall \, k = 1 \dots R \quad (3)$$

This is the capacity constraint that states that the personnel required for fulfilling the obligations imposed by the total number of contracted services during a specific time interval cannot exceed the available personnel for the time period under consideration.

In addition, we have the following quantity in the model:

$$g_j^t(r) = \sum_{i=1}^{N} \sum_{s=1}^{t} \left[\sum_{v=\max(t-\mu_{ij}+1, s)}^{t} d_i^s p_{ij}^{sv}(r) \right] \; \forall \, j = 1 \dots N, \forall \, t = 1 \dots T \quad (4)$$

The function $g_j^t(r)$ gives the expected number of active contracts (i.e. contracts on which work has started) of type j at time instance t. In this function, the outer summation operators sums over the total number of available services that can be contracted by customers, and the second summation operator sums over all possible time instances s, until t, at

which time a contract can be signed. With respect to the inner summation, i.e. $\sum_{v=\max(t-\mu_{ij}+1,s)}^{t} d_i^s p_{ij}^{sv}(r)$, the quantity $d_i^s p_{ij}^{sv}(r)$ is the expected number of services for customer type i that are contracted at time instance s, are of type j, and will actually start at time instance v. Summing over all possible *start* instances v in the inner sum, then, gives the expected number of signed contracts of type j that are active at time instance t. More specifically, at time t there are two types of service contracts on which illicit service provider's personnel is working:

- The contracts signed before time instance t which are scheduled to start exactly at time instance t.
- The contracts that were signed and started before time instance t and have not yet been completed because of the expected length of those contracts, for a specific service type. This implies that these assignments must have started at time instance $t - \mu_{ij} + 1$. The inner summation, however, starts from $\max(t - \mu_{ij} + 1, s)$ to take into account start instances which are smaller than s.

The following constraint states a natural assumption, which is that providing a service at a later time period will cost less than providing it at an earlier time period:

$$r_{ij}^{st} \geq r_{ij}^{s(t+1)} \; \forall \, s, t \geq s = 1 \ldots T, \forall \, i = 1 \ldots N, \forall \, j = 1 \ldots M \tag{5}$$

The following constraint states the fact that prices must be non-negative numbers:

$$r_{ij}^{st} \geq 0 \; \forall s, t = 1 \ldots T, \forall \, i = 1 \ldots N, \forall \, j = 1 \ldots M \tag{6}$$

The following equation defines the utility of a customer from customer class i, for a service of type j, whose contract is signed at time instance s and which will start at time instance t:

$$U\left(r_{ij}^{st}\right) = v_{ij} - \zeta_{ij} * r_{ij}^{st} - \beta_{ij} * (t - s) \; \forall \, s, t = 1 \ldots T, \forall \, i = 1 \ldots N, \forall \, j = 1 \ldots M. \tag{7}$$

Finally, the following critical equation provides the probability model for the choices made by customers with respect to the service types offered by an illicit service provider:

$$p_{ij}^{st}(r) = \frac{e^{\theta \, \cup_{ij}^{st}\left(r_{ij}^{st}\right)}}{e^{\theta U_{i0}^{S}} + \sum_{t'=s}^{T} \sum_{j'=1}^{M} e^{\theta \, \cup_{ij'}^{st'}\left(r_{ij'}^{st'}\right)}} \; \forall \, s, t = 1 \ldots T, \forall \, i = 1 \ldots N, \forall j = 1 \ldots M. \tag{8}$$

These probabilities are modelled according to the well-known *Logit* function, which are commonly used in discrete choice models [33]. The generic form of the Logit discrete choice model is the following [33], where P_{jq} is the probability that individual q makes choice i among N available alternatives [35]:

$$P_{jq} = \frac{e^{V_{jq}}}{\sum_{i=1}^{N} e^{V_{jq}}} \tag{9}$$

This expression pertains to the well-known *multinomial Logit model*. More detailed definitions and properties of this function can be found in Train (2009) [33] and McFadden [35].

In the equation for $p_{ij}^{st}(r)$, a special "service" with subscript 0 appears in the denominator outside from the double sum, in the term $e^{\theta U_{i0}^{S}}$. This "service" corresponds to the competition from other illicit service providers, from which customers derive some utility. Without this "competition term", the price optimization model produces unboundedly large (infinite) prices that, a result of profit maximization in monopolistic and competitive markets, as observed in Wardell et al. (2008) [30].

7- Modeling Target Organizations' Costs/Benefits

Quantifying cost/benefits of cybersecurity attacks/defense respectively entails breaking down the complexity of cost estimates to manageable categories that emphasize different aspects of an organization's nature, size, business objectives and outreach. In Deloitte (2016) [26], a framework with 14 cyberattack impact factors was proposed. Based on our literature survey we concluded that these 14 factors reflect the majority of cost categories in relation to cyberattacks, and which also reflect the benefits of investing in cybersecurity. We rationalize the latter by the fact that, as a reasonable assumption of our model, the severity of inflicted or potential cyberattack related damages is closely related to how much one should invest in corresponding defense measures [36]. However, this may not be always the case.

7-1- Targeted Organization's Costs

7-1-1- Proactive Costs

We consider in detail the costs of implementing proactive security measures for an organization (i.e., in measures implemented prior to the occurrence of a security incident). We assessed several categories of costs which we briefly repeat below, along with specific cost estimates which are of interest to the model we describe in this paper.

- Real-time monitoring of an organization's ICT infrastructure. Real-time monitoring can be implemented either by the organization's specialized IT security personnel and an in-house Security Information and Event Management (SIEM) system or by outsourcing to a managed security service provider.
- Education of all personnel in ICT security and the establishment of a detailed and clear security policy that each member of the personnel should comply with.
- Appointing a DPO (this, along with the corresponding salary plus bonus costs, is obligatory, under specific conditions, by the GDPR in Europe) or a CSO.
- Train technical personnel according to ISO standards and provide incentives for obtaining certification in security protection.
- Obtaining an ICT security related ISO certification. This step usually necessitates thorough penetration testing procedures to assess the level of security of an organisation's infrastructure and guarantee that it complies with the ICT security related standards, such as the ISO/IEC 27001.
- Initiation of an internal or outsourced public bug bounty or vulnerability reward program. For example, as an element of proactive costs, for about 500€ per year, one can start a responsible vulnerability disclosure program at the Vulnerability Lab (https://www.vulnerability-lab.com/) and take advantage of Vulnerability Lab's infrastructure and expertise of its members that participate in vulnerability disclosure programs.
- Employ secure software development and testing methodologies.
- Conduct proactive penetration testing and security drills regularly, utilizing either an internal red team or outsourcing the task to security consultants.

With respect to the last item, which account for a significant fraction of the total proactive costs due to its technical complexity, costs are usually agreed after discussions between the penetration testing provider and the infrastructure owner, but have been reported to usually not be very high, as indicated in the following tables from two different penetration testing service providers:

A) ServerScan (*https://www.serverscan.com/Penetration-Testing*):

Price quotations from the site:

- Base Price: Up to 32 IP Addresses (internal + external) - $6,500
- Additional IP Addresses (per 32) - $1,200
- Internal Penetration Test - Included in Base Price
- First Web Application - $2,200
- Additional Web Applications - $1,200

B) HighBit Security (*https://www.highbitsecurity.com/penetrationtesting-cost.php*):

Price quotations from the site follow in the Table 3:

Table 3. Price quotations

Type	Description	Starting Price, USD
External Network	Base price is for an external penetration test addressing security vulnerabilities at the network layer* and also including host configuration* vulnerabilities, up to 32 IP addresses. A non-credentialed Web Application Test may be substituted if network testing is not needed.	$5,900
Internal Network	Base engagement price is for an internal penetration test (on internal network), addressing security vulnerabilities at the network layer* and also including host configuration* vulnerabilities, up to 32 IP addresses. A non-credentialed Web Application Test may be substituted if network testing is not needed.	$6,900
Web Application	Price is for a single non-credentialed* web application penetration test, in conjunction with an external or internal network penetration test.	$1,900
Wireless	Price is for a wireless penetration test, in conjunction with an internal network penetration test, for one wireless access point and associated client devices.	$4,900
Social Engineering	Price is for a remote social engineering test, including two separate electronic attack vectors with spear phishing email directed at human targets within the organisation, in conjunction with an external network penetration test*.	$4,900

** Network Layer testing includes firewall configuration testing, such as stateful analysis tests and common firewall bypass testing, IPS evasion, DNS attacks including zone transfer testing, switching, and routing issues and other network related testing.*

C) Security check services offered by a research institute to an education institute in Greece as part of the requirements of GDPR compliance:

Further to these cost sources, we cite the following vulnerability analysis project tackled by members of the authors of this paper with extensive expertise in information security auditing among other ICT security sectors. The project was commissioned by a Greek higher education institute and the goal was to analyze [37], security-wise, a web service of the educational institute directed to its students and instructors [38]. This analysis was part of the actions of the educational institute towards GDPR compliance.

The vulnerability analysis work included the following tasks/checks: Information (e.g., log and audit files) collection, O/S (Windows) vulnerability assessment, Attacks on the communication channels, Attacks related to the O/S (Windows), Attacks related to the service's DBMS (e.g., SQL injection attacks), Attacks related DDoS vulnerabilities, robustness against unauthorized transactions with services and applications of the educational institute, robustness against unauthorized access to sensitive data (e.g., students' emails or grades), robustness against efforts to corrupt, modify, or leak information and data [39, 40]. The offer included all the above tests as well as the write-up of a report on the findings and suggestions for remedial actions. The work duration was estimated at 10 days for two security experts, and the price was 1.300 euros + 24% VAT. The offer was accepted by the educational institute, and the vulnerability assessment was successfully conducted.

The above cases, A, B, and C are not expected to cover all possible elements of an extensive penetration and vulnerability testing of an organization that has multiple servers, services, and databases of varying sensitivity and security needs. These cases, nevertheless, may serve as a guide in determining costs related to proactive security measures an organization may take to secure itself against cyberattacks. We also observe that prices are comparable with no significant differences between the different providers. The proactive costs will be denoted by PC_ORG, i.e., *Proactive Costs of the Organization*.

7-1-2- Remedial costs – Third Party and Law Enforcement Agencies Liabilities

Any effort for accurately quantifying costs incurred to organizations from cyberattacks requires a methodological, fine-grained approach since there are numerous contributing factors to these costs with varying weight and importance for different industry and activity sectors as well as organizations annual revenues and sizes. To this end, we have decided to apply a costs model that captures the most important contributing factors as well as the differences in their importance depending on the victim organization's profile and business characteristics. This is the model proposed by Deloitte (2016) [26]. We consider this a most appropriate model for our purposes after reviewing and studying the relevant literature. Below, we review briefly the 14 factors and explain their significance in the proposed model that we describe in this paper. The total cost incurred by these factors will be denoted by RC_ORG, i.e., *Remedial Costs of the Organization*.

- Technical Investigation: this cost factor estimates the technical investigation costs (including forensics analysis), by expert teams, after a breach incident occurs. This cost factor includes digital forensics, vulnerability, and malware analysis, as well as network and data repository scans to identify and assess extend of damages and information leaks.
- Customer Breach Notification: this cost factor refers to the costs involved in informing individuals who are affected by the incident (e.g., customers whose personal data were stolen).
- Post-breach Customer Protection: these are costs for subscribing to premium services that will help reduce the risk of malicious people capitalizing on the stolen information/data.
- Regulatory Compliance: this cost category aggregates fines or compensation fees that the victim organization should pay to the state or its clientele for negligence in complying with data and privacy protection regulations such as the GDPR in Europe.
- Public Relations: these costs refer to the efforts towards handling communications or brand management activities after a security through a massive public relations campaign.
- Attorney Fees and Litigation: these costs include various legal advisory fees and settlement costs, as well as costs incurred through the organization's legal actions to defend its position.
- Cybersecurity Improvements: these costs include the proactive costs, i.e., the costs for strengthening and securing the victim organization's infrastructure before an incident occurs, as well as the costs that resulted from damages inflicted by the attack.

- Insurance Premium Increases: as a result of the incident, insurance companies normally will increase the cost of the insurance coverage, depending on the severity of the incident and the size of compensations paid by the insurance company on behalf of the victim organization.
- Increased Cost to Raise Debt: this cost category refers to the fact that the victim organization will face higher interest rates (as well as a lower credibility rating) for new or older loans it received from financial institutions due to higher stakes involved.
- Impact of operational disruption or destruction: a security breach incidence may cause severe business disruption while investigations last or the victim organization's infrastructure remains non-operable. These costs include repairing equipment and recovering customer data, diverting operations to leased backup infrastructures (e.g., cloud platforms) etc. Assessing these costs is a complex process since they depend on the type of businesses conducted by the victim organization, its size, its revenues as well as its clientele's volume.
- Lost Value of Customer Relationships: this cost type refers to the "customer value" lost for the victim company due to a security breach incident. It is, usually, difficult to estimate this value but, often, economists and marketing specialists work by assigning a "value" to each customer that quantifies, in some sense, the cost and effort invested by the organization to gain and, subsequently, retain the customer.

Value of Lost Contract Revenue: these costs represent lost revenues due to the incident, including loss of opportunities for new contracts or delayed payments of active contracts on which the company stopped working due to the business disruption caused by the incidence. These costs can, usually, be estimated through a *Discounted Cash Flow* (DCF) analysis. As a starting point, one can estimate the *Net Present Valu*e (NPV) of *Cash Flows* (CF) generated over T consecutive years, if the cash was to be invested using interest rate r, based on the following formula:

$$\text{NPV} = \sum_{t=1}^{T} \frac{CF_t}{(1+r)^t} \tag{10}$$

where r is defined to be the *effective annual rate* to match the cash flows. The effective annual rate can be calculated using the following formula:

$$\text{ER} = r = \left[1 + \left(\frac{APR}{n}\right)\right]^n - 1 \tag{11}$$

In this formula, APR is the Annual Percentage Rate defined for n periods per year (usually for a period of $n = 12$ months). APR is often quoted as the period rate multiplied by the number of periods. A detailed description of the DCF methodology can be found, e.g., Algarni & Malaiya (2014) [24]. In simple terms, the delayed (in our case due to a cyberattack incident) payments have "less value", due to money depreciation, than the payments that are delivered on time.

- Devaluation of Trade name: these costs are related to the loss of value of the victim organization's trade name in its business sector. In order to arrive at an estimate of the trade name of a victim organization, Deloitte [26] discusses the relief-from-royalty method which is commonly used to value IP (Intellectual Property) assets such as trade names. This valuation is based on analysing the fees that another organization would have to pay in order to license the organization's trade name i.e., currently known royalty transactions. We can, also, propose the deployment for this cost category another technique which may arrive at more exact estimates of trade name devaluation not from industrial relationships but from a stock market value perspective. We refer to the event-driven analysis based on a technique that investigates the effects (e.g., stock market value fluctuations) of the disclosure of cyberattacks against organizations [28]. This method relies on the following two axes:
  - Observing how an organization's stock market value fluctuates when a vulnerability or attack affecting the organization is publicised.
  - Determining how the disclosure affects the stock market value of the victim organization.
- Loss of Intellectual Property (IP): these costs refer to the leak of industry secrets or copyrighted intellectual property as a result of a cyberattack. This leak may lead to loss of market advantage or, even, to direct financial losses due to competition.

The report of Deloitte (2016) [26] also includes two scenarios for the application of this 14-factor impact model. Scenario A concerns a US health insurance company and Scenario B concerns a US technology manufacturing company. For illustrative purposes, in Figure 2 and 3 we show an example as it is provided and discussed in detail in Deloitte (2016) [26].

About the company:

$60 billion annual revenue;

50,000 employees;

23.5 million members across the US (60% subscribed through employer contracts);

Uses a patient care application which provides medical alerts and allows health practitioners across its provider network to access patient records and insurance coverage information;

Holds open enrollment (the annual period when people can enroll in health insurance plans) November through January;

Regulated by both state and federal authorities;

Plans to raise $1 billion in debt capital to acquire a health system;

Pays $7 million annual premium or a $100 million cyber insurance policy.

Figure 2. An example company profile [26]

Summary of the impact factors

	Impact factor	Term	Cost (in millions)	% Total cost
Above the surface	Post-breach customer protection	3 years	21.00	1.25%
	Cybersecurity improvements	1 year	14.00	0.83%
	Customer breach notification	6 months	10.00	0.60%
	Attorney fees and litigation	5 years	10.00	0.60%
	Regulatory compliance (HIPAA fines)	1 year	2.00	0.12%
	Public relations	1 year	1.00	0.06%
	Technical investigation	6 weeks	1.00	0.06%
Beneath the surface	Value of lost contract revenue (premiums)	5 years	830.00	49.43%
	Lost value of customer relationships (members)	3 years	430.00	25.61%
	Devaluation of trade name	5 years	230.00	13.70%
	Increased cost to raise debt	5 years	60.00	3.57%
	Insurance premium increases	3 years	40.00	2.38%
	Operational disruption	Immediate	30.00	1.79%
	Loss of intellectual property	Not applicable	-	0.00%
	Total		**$1,679.00**	**100.00%**

Figure 3. Estimates of costs for the 14 cost factors of the model due to a cyberattack [26]

We remark here that the required model data, such as the cost values for the 14 factors of the model, may be hard or even impossible to find from individual victim companies. This is caused by the fear of further exposure to bad publicity following a cyberattack, especially if the attack resulted in a privacy breach of customers or stolen customer data. In contrast, data such as the company profile and revenues that appear in Figure are easy to locate for individual companies. With respect to data and information that are related to the 14 factors of the model, one must speculate based on suitable modeling frameworks, such as the one discussed in this paper, based on publicly available information and data gathered by specialized tools, such as the ones being developed within the scope of other research efforts.

With respect to our discussion in the introduction, it is information sources in non-textual, human-friendly formats, such as the information appearing in Figure 1, that can be converted into machine-readable format using advanced AI techniques that go beyond the scope of this paper. Data appearing in such human-readable sources can then provide values for the parameters and variables of the proposed theoretical model.

7-2- Target Organization's Benefits

With respect to the organization benefits from investing in cybersecurity, we take a simple (but reasonable) approach and equate them, as a basis for our estimates, to the costs incurred by a security breach incidents, defined as the aggregate of the separate costs in the 14 categories discussed in Section 7-1-2. In other words, the target organization's benefits from investing in cybersecurity are equal to, at least, the costs that the organization will avoid from becoming a victim of an attack as a result of not investing in cybersecurity proactive measures, i.e. the remedial costs cited in Section 7-1-2, minus the proactive costs invested in strengthening the organization's robustness against cyberattacks, related to the items discussed in Section 7-1-1.

Based on the discussion above, let us denote by PC_ORG the *cybersecurity investment* costs of an organization and by RC_ORG the *damage* costs of a potential cyberattack. Then the *net profit* of the organization that results from investing in cybersecurity, which is denoted by NET_PROFIT_ORG, is given by NET_PROFIT_ORG = RC_ORG – PC_ORG, assuming (which is not unreasonable) that RC_ORG > PC_ORG (it is expected to be many times larger). In other words, the net financial benefit for the organization is given by subtracting the expenses involved in cybersecurity investment from the damages that could be inflicted on the organization due to cyberattack that it may avoid because of the cybersecurity investment.

Observe, that if the organization invests in cybersecurity defense and the attacker does not attack (e.g. in case the organization is not an attractive target) then RC_ORG = 0. However, the organization does not know it since the game model allows only simultaneous decisions of the players. In this case, NET_PROFIT_ORG = 0 – PC_ORG = – PC_ORG, which is negative reflecting the futility of the investment. If, on the other hand, the organization decides to invest and the attacker attacks, then the net profit can be considerable and certainly equal to benefits minus expenses, i.e., NET_PROFIT_ORG = RC_ORG – PC_ORG. This line of thinking is explained in more detail below.

8- Modeling Illicit Service Provider's Costs/Benefits

With respect to modeling the total illicit service provider's costs and benefits, we deploy a simple model that is described in Kshetri (2006) [41], suitably adapted to the purposes of our work.

The model consists in deciding whether an illicit service provider deems beneficial to proceed in committing an illicit act or avoids doing so. To this end, the model leads to a decision to proceed if the following inequality holds true:

$$M_b + P_b > O_{cp} + O_{cm}P_aP_c. \tag{12}$$

The left-hand side of the inequality represents the *benefits*, and the right-hand side represents the *costs*.

Based on this mode, we can consider the net profit value as the difference between the left-hand side and the right-hand side:

$$\text{NET PROFIT} = (M_b + P_b) - \left(O_{cp} + O_{cm}P_aP_c\right) \tag{13}$$

The variables and parameters of the model have the following meanings:

- M_b: represents the monetary benefits of committing a crime or providing an illicit service
- P_b: represents the "psychological" or other immaterial benefits (e.g. fame, spread of achievements etc.) of committing a crime or providing an illicit service
- O_{cp}: represents the "psychological" costs of committing a crime or providing an illicit service
- O_{cm}: represents the monetary opportunity costs of conviction for committing a crime or providing an illicit service
- P_a: represents the probability of arrest as a result of committing a crime or providing an illicit service
- P_c: represents the probability of conviction as a result of committing a crime or providing an illicit service

In the following two subsections we explain in more detail the above parameters.

8-1- Illicit Service Provider's/User's Benefits

In this section we will discuss in more detail the benefits parameters of the model, i.e. the parameters M_b and P_b.

M_b, in the case of an *illicit service developer but not user*, who acts upon a contract engagement, is straightforward to define and estimate since it corresponds to monetary rewards out of illicit service development, use and/or selling. In our proposal, M_b can be estimated (at least on average), through the Capacity and Value Based Pricing (CVBP) model described in Section 7. More specifically, we can assume that:

$$M_b = \sum_{j=1}^{M} \sum_{t=1}^{T} \left[\sum_{s=1}^{t} \left(\sum_{i=1}^{N} d_i^s \, p_{ij}^{st}(r) r_{ij}^{st} - g_j^t(r) \sum_{k=1}^{R} a_{jk} \, p_k^t \right) \right] \quad (14)$$

with the illicit service prices vector r replaced by the vector that maximize the right-hand side of the above equation. This vector is computed, as we discussed in Section 7, by solving the following optimization problem, over the service price vector r:

$$max_r \sum_{j=1}^{M} \sum_{t=1}^{T} \left[\sum_{s=1}^{t} \left(\sum_{i=1}^{N} d_i^s \, p_{ij}^{st}(r) r_{ij}^{st} - g_j^t(r) \sum_{k=1}^{R} a_{jk} \, p_k^t \right) \right] \quad (15)$$

When we have an illicit service user, M_b reflects the monetary benefits from ordering and using an attack. For instance, M_b may be the total amount of money obtained from hacked accounts, hacked credit cards or ransom. In this case, we will denote these profits by M_b', to differentiate it from the value M_b defined by the maximization problem above. In this case, of course, the illicit service user must take into account the contract cost which is reflected in the price asked by the service developer according to the prices vector, for the various service, that results from the optimization problem for the developer, as explained above.

With respect to P_b, this represents the intangible (non-monetary) gains for the illicit service developer and/or user. These gains stem, mainly, from reputation and self-esteem aspects inherent in hacking/illicit service development. Also, as discussed in Kshetri (2006) [41], in this benefits category we also have government-backed cyberwarfare, that is collaboration of governments with illicit service providers or hackers. These benefits are intangible since they are usually related to benefits such as defacing countries, incapacitating a country's ICT infrastructure and gaining political dominance. However, in order to be in position to combine the two benefits, i.e. M_b and P_b, in the sum, $M_b + P_b$ must be represent a monetary value. Thus, P_b must be converted into a monetary value, since M_b already represents such a value. Let us assume a generic monetary conversion function $f(x)$ such that $P_b = f(M_b)$, depending on the case in hand in an effort to quantify the intuitive idea that "good reputation brings revenues". For concreteness, we propose the definition

$$P_b = kM_b + l \quad (16)$$

for two constant values (to be determined when handling a real analysis case) $k, l > 0$, i.e. we propose a simple linear relation between M_b and P_b. The assumption is that, usually, high revenue businesses have also a correspondingly high reputation. Thus, P_b and M_b can be assumed, as a first approximation, to satisfy this linear relationship.

8-2- Illicit Service Provider's Costs

In this section we turn our attention to the costs parameters of the model, i.e. the parameters O_{cp}, O_{cm}, P_a and P_c.

The parameter O_{cp} represents the "psychological" or ethical costs of committing a crime or providing an illicit service. Although it may appear that such costs are zero, constant or even negligible, research results (see [12]) indicate that the feeling of guilt is not equally strong across hackers with different social and cultural backgrounds. Therefore, we include this cost category in the proposed model although one may simply set it to 0 if the situation in hand considers scenarios of highly unethical and ruthless hackers. Again, which cost must be converted into a monetary equivalent in order to be comparable with other quantities in the model.

O_{cm} represents *the monetary opportunity costs* of conviction for committing a crime or providing an illicit service. This cost is, simply, fines or punishment incurred on the hacker if the hacker is caught and judged guilty in court. Also, this cost includes loss of income or revenue as a result of imprisonment.

P_a represents the *probability of arrest* as a result of committing a crime or providing an illicit service. This parameter captures the readiness, alertness and efficiency of the police services of a country or federation of countries (e.g. Europol) in conducting a successful forensics investigation after a cybercrime is committed. This probability of arrest refers, specifically, to the effectiveness of police services of countries and reflects how intensely they prosecute cybercrime and the *rate* at which they resolve cyberattack incidents. This probability can be estimated easily from police files as the fraction of cybersecurity incidents who have been officially reported and has resulted in the arrest of the perpetrators.

Finally, P_c represents the probability of *conviction*, after the arrest, as a result of committing a crime or providing an illicit service. This reflects the readiness of the judicial system and legislation, as well as its capacity, in carrying out all the necessary legal actions in order to prove, beyond doubt, the guilt of arrested cybercriminals. Obviously, the probabilities P_c and P_a need not be correlated. It may well be the case, for instance, that the police are highly efficient in arresting cybercriminals that the judicial system, due to ignorance of deep knowledge of cybercrime and its complexities, let alone the lack of appropriate legislation and expert judges, is unable to prove guilt. Again, the probability P_c can be estimated by the trial records kept by legal institutions of countries.

9- The Complete Model and its Applications

Let us recall, the decision model for the defender and attacker in the form of a strategic game:

Table 4. Price quotations

	Invest in attack	**Do not invest in attack**
Invest in defense	$(a, -\beta)$	$(-b, 0)$
Do not invest in defense	$(-c, \gamma)$	(0,0)

The payoffs related to the defender are while the costs related to the attacker are a, b, c while the payoffs related to the attacker are β, γ.

Based on our discussion in Sections 6 and 8, we can proceed to set the payoffs related to the defender as shown below:

- $a =$ RC_ORG – PC_ORG
- $b =$ PC_ORG
- $c =$ RC_ORG

With respect to the attacker, we differentiate between three classes of attackers: Illicit service developer. Illicit service user, and illicit service developer *and* user. We then work on the payoffs as follows:

Illicit service developer:

- $\beta = O_{cp} + O_{cm}P_aP_c$
- $\gamma = P_b + M_b$

The rationale behind setting $\beta = O_{cp} + O_{cm}P_aP_c$, the "hacker's" total losses according to the model by Armin et al. [12] which we discussed in Section 8-, is that most often the illicit service developer is the one who is found, as the one behind a cyberattack during a forensics investigation, even if the real originator of the cyberattack launch was someone else (e.g. a governmental agency of a country).

The choice $\gamma = P_b + M_b$ reflects the aggregate benefits of the developer which consist of the direct monetary rewards out of developing and selling the illicit service as well as the intangible rewards in recognition, fame and, possibly, attraction of more orders for developing illicit services.

Illicit service user:

- $\beta = 0$
- $\gamma = P_b + M'_b - M_b$, *assuming that* $P_b + M'_b > M_b$

In this category, we have the illicit service users who do not develop the services themselves due to lack of expertise or due to the need to avoid direct exposure as a result of the forensics investigation of a cyberattack.

The rationale behind setting $\beta = 0$ is that an illicit service user is not exposed (or, at least, tries hard to avoid it) so much as the illicit service developer whose tracks can be found using a forensics investigation of a cyberattack incident. For instance, it is known that countries are among the top illicit service users, however rarely a government of a country has been exposed as being behind a cyberattack incident.

The rationale behind $\gamma = P_b + M'_b - M_b$, assuming that $P_b + M'_b > M_b$, is that the illicit service user's net benefits are the intangible benefits, in monetary value, reflected by P_b, plus the monetary benefits as a result of the attack minus the expenses for obtaining the illicit services, as reflected by the parameter $M_b$which is equal to the price demanded by the illicit service developer for the service. The assumption $P_b + M'_b > M_b$ is required so that the net profit for the service user is positive (i.e. ordering the service leads to winnings and not losses).

Illicit service developer *and* user:

- $\beta = O_{cp} + O_{cm}P_aP_c$
- $\gamma = P_b + M'_b - M''_b$, assuming that $P_b + M'_b > M''_b$ *(*see below for an explanation of M''_b)

In this category, we have the illicit service developers who, themselves, develop and launch the attack for their own benefit, not acting upon receiving an order from another party. Setting $\beta = O_{cp} + O_{cm}P_aP_c$, follows the rationale of the case of an illicit service developer (first of the three cases, above). However, with respect to the choice for γ, we have introduced the parameter M''_b beyond M'_b which represents the monetary rewards from using the attack, as in the second case above. The parameter M''_b, however, represents the monetary profits lost *if* the resources deployed by the illicit service provider for developing *and* using the attack were invested for work on external contracts. Thus, we set $\gamma = P_b + M'_b - M''_b$ as the net profit for the illicit service developer *and* user.

Summing up the discussion above, we derive the following three game types (in strategic form) for the three examined cases:

Table 5. Applying the decision model – the case of illicit service developer

	Invest in attack	Do not invest in attack
Invest in defense	(RC_ORG – PC_ORG,$-(O_{cp}+O_{cm}P_aP_c)$)	(–PC_ORG,0)
Do not invest in defense	(– RC_ORG, P_b+M_b)	(0,0)

Table 6. Applying the decision model – the case of illicit service user

	Invest in attack	Do not invest in attack
Invest in defense	(RC_ORG – PC_ORG,$-(O_{cp}+O_{cm}P_aP_c)$)	(–PC_ORG,0)
Do not invest in defense	(– RC_ORG, $P_b+M_b'-M_b''$)	(0,0)

Table 7. Applying the decision model – the case of illicit service developer and user

	Invest in attack	Do not invest in attack
Invest in defense	(RC_ORG – PC_ORG,0)	(–PC_ORG,0)
Do not invest in defense	(– RC_ORG, $P_b+M_b'-M_b$)	(0,0)

Based on these payoff values, one can derive the probability estimates for the decisions that will be taken by the two players, within the context of the NE in mixed strategies (or decisions, in our context, by the defender and the attacker). The corresponding probabilities of the equilibria points are computed based on the expressions provided in Section 5.

10- Concluding Remarks and Future Work

In this paper, we reported on the work performed within the SAINT project related to the correlation of the financial aspects of cybercrime, both the attackers and defenders, as a decision game based on a multiparameter costs/benefits model. Our work focuses on modeling the interplay among various financial and business-related parameters and indicators related to cybercrime and how they affect defense or attack investments and decisions.

To this end, we propose the following two parallel directions in the context of this paper, which we hope will be pursued as future work:

- Utilizing advanced Artificial Intelligence (AI) methods to process human-readable information sources as they currently exist, such as text or multimedia formats, and evolving on the World Wide Web (WWW). In addition, for non-text data, advanced AI methods are currently used in image analysis and for the understanding of histograms and pie charts (including their labels and the numerical data) that appear in picture formats in articles on the Web. For example, the 0-day exploit prices given by Zerodium are provided in picture format, not text. Natural Language Processing (NLP) techniques can be deployed for syntactic and semantic analysis of the text that appears in articles to develop applications that can locate pricing information, cyberattack-related cost figures, etc. However, more advanced techniques, which go beyond the scope of this paper, are required in order for a machine to read important quantitative/qualitative surveys. Several works [23, 26, 42] present methods to transform relevant financial data into standardized text formats. We have deployed such techniques at a primitive level in the SNA and the Clearnet Web Crawler, but they are capable of covering only a very small portion of the available existing resources on the web.

Transformation, first, of human-readable information sources into machine-readable format and structure, much like the Web 3.0 Semantic Web vision and the ambitious ontological frameworks under development for various areas of the discourse of human knowledge. This is a different and maybe more daunting approach as it requires much preparatory work to enable machines to "understand" secondary sources of information, such as the numerous security reports published by leading security consulting companies in their own standardized formats. Another way to achieve the machine readability goal is to develop a standardization body to initiate a discussion with the security consultancy and survey industry concerning defining a standard survey format, including questionnaires and reports, at least for the numerical data of interest to automated processing tools. However, the cost of this transformation effort can be amortized over the resulting benefits that the automated analysis of the transformed data will produce. These costs can be reduced if such transformation efforts are sustained by voluntary contributions through crowdsourcing or following the model of voluntary and massive participation of Wikipedia. Crowdsourcing has gained considerable popularity over the last few years and has been adopted by numerous leading companies, often outside the field of cybersecurity. For instance, we have the following efforts [25, 43] going on based on the Ontology concept [44] and various semantic modeling frameworks (e.g., First Order Logic [44]). Examples include the following:

- Common Sense Semantic Network (ConceptNet) – see *https://www.opasquet.fr/omcsnet/*
- Freebase (entities and mutual relations) – see *https://www.opasquet.fr/omcsnet/*
- Google's Knowledge Graph and Facebook's Entity Graph
- Microsoft's Satori, a semantic knowledge repository to assist Bing's (Microsoft's Internet Search Engine) searchers with more than a billion objects digested over 3.5-year years. Satori is a self-learning system running daily, thus learning more, adding 28,000 DVDs of content daily.
- Yahoo's Knowledge Graph, Spark, a semantic search assistance tool.
- Linked. In's Economic Graph.
- DBpedia, a machine-readable version of Wikipedia. Text information available in Wikipedia in human language is transformed to be structured and semantically annotated to be amenable to automated processing (the ongoing WikiData project).
- Carnegie Mellon University's "Read the Web" project (see *http://rtw.ml.cmu.edu/rtw/*).
- The visionary project of the Gigantic Global Graph (Web of machine-readable, Open Data, see https://en.wikipedia.org/wiki/Giant_Global_Graph). This ambitious project is expected to implement Sir Tim Berners-Lee's vision of the Web as a Gigantic Global Repository (Graph) of Data and Knowledge.

Naturally, emerging AI platforms such as ChatGPT should, also, be considered as information gathering sources from natural language sources. The provided Application Programming Interfaces (APIs) can be deployed to feed natural language based information into structured and more formal information formats suitable for automated analysis.

Monitoring all these data and information sources can provide estimates for our model's parameters and variables based on the impact of security breach incidents on victim organizations, both monetary and non-monetary damages, the prices of illicit services and their determination, illicit service providers' revenues, the cost of cyber defense, and the identification of key factors that lead to the decision to invest in cybersecurity measures or not [45-49].

Modeling these elements, along with their interactions, proved to be a difficult task. The main reason was the lack of primary source information, i.e., information directly from illicit service providers and victim organizations. Having sufficient and accurate information is essential to target the financial aspects of cybercrime and defense. Publicly available information is enormous but scattered, unorganized, and contradictory because it is reported by many entities of varying cybersecurity competence, technical expertise, and knowledge breadth concerning ICT security. In addition, this information is often reported in a format, e.g., picture diagrams and graphs, as well as lengthy text in a natural language (mostly English), that is not easy to process through automated. This is precisely one of the significant *obstacles* and, at the same time, *challenges* for our research goal, i.e., the lack of standardized reporting formats, which considerably hinders empirical research.

The contradictory nature of available secondary information, being voluminous but not directly exploitable, in conjunction with the scarcity of primary information, prompted us to pursue our goals along two parallel but dependent lines of approach. The first approach, presented in the present paper, is mostly theoretical and creates the framework in which the second approach operates. The model that we proposed combines a number of parameters that explain how illicit service providers may price their products in order to maximize profits, taking into account existing constraints and conditions related to their capacity as well as their motivations. We also described a game-theoretical model that, based on the parameter and variable values of the theoretical model, explains when it is cost-beneficial to invest in cybersecurity measures and when it is profit-beneficial to develop and/or launch a cyberattack. To the best of our knowledge, no similar approach has been presented that encompasses, in a fine-grained set of variables and parameters, the main financial aspects of cybercrime along with the characteristics and interests of all principal stakeholders. To this end, the introduced theoretical model can inspire further research into the financial aspects of cybercrime, explaining the observed behavior of stakeholders and identifying the elements that influence their decision.

With respect to the second approach, we complemented our theoretical model with a less fine-grained but directly applicable and practical model. This approach deploys an econometric analysis model based on information that automated tools are able to gather from one of the available indicator sources, such as the HackerOne bug bounty platform. HackerOne was chosen from among all the information sources (considered as cybercrime indicators) we considered because it has the unique feature of linking vulnerability exposition with pricing. The conclusion of this empirical approach is that in bug bounty markets such as HackerOne or (as we conjecture) the Deep Web, illicit service providers appear to have more market power in that they can raise relatively easily their revenues by, simply, raising their prices for bug bounty. In this case, the customers (organizations) appear to still be willing to pay these higher prices without reducing, significantly, their demands for bugs and vulnerabilities that concern them. This is a very attractive feature of these markets that, we conjecture, results in gathering increasing numbers of illicit service providers, which

may, also, be willing to reduce their activities in illegal markets and become active in legal revenue activities such as offering their services, in return of monetary rewards, to legal vulnerability-related services such as bug bounty. This, however, needs further investigation using more bug bounty information stemming not only from HackerOne but other similar markets too, which were not possible to investigate within the scope of this paper and the SAINT project.

In summary, the connection between big data, public information sources/repositories, and cybercrime is. Cybercriminals leverage advanced technologies and analyze large datasets to carry out cyberattacks. On the other hand, big data can assist IT security professionals in detecting anomalies and unauthorized activities, thereby enhancing cybersecurity [50, 51]. Our work aimed precisely at this direction.

Future work should concentrate, we feel, on developing more robust and empirically validated models to better understand the financial dynamics of cybercrime and cybersecurity. This includes acquiring and incorporating actual transactional data from the Dark Web, which necessitates overcoming significant ethical and logistical hurdles. Furthermore, future studies should automate transforming human-readable data on cybersecurity into machine-readable formats to enhance the scope and scale of data analysis using advanced AI techniques. Researchers should also explore the standardization of reporting formats to enable a more unified approach to empirical research in cybersecurity. While the proposed models offer valuable insights, they have limitations. The assumptions and simplifications inherent in the theoretical approach of the CVBP model and the game theory framework may not capture the full complexity and variance of real-world cybercrime economics. Hence, iterative improvements to the model that incorporate real-world behavioral data and feedback loops could enhance its predictive power.

Furthermore, the research is currently hampered by scattered and unorganized secondary data, which could lead to biased or incomplete conclusions. Ensuring ethical considerations, especially when dealing with illegal activities, is also a critical limitation that must be addressed, as is the need for more transparent reporting of potential conflicts of interest. Therefore, future work should advance model sophistication, enhance data collection and analysis methods, resolve ethical and legal challenges, and strive for transparency and replicability in cybersecurity economic research.

Finally, looking ahead to the immediate future, we plan to continue our efforts to explore ways to enhance the applicability of the proposed theoretical model. This involves gaining access to primary information sources and supplementing the practical model with data from additional indicator sources based on data gathered by automated tools.

11- Declarations

11-1-Author Contributions

Conceptualization, A.P., V.V., and Y.C.S.; methodology, A.P. and Y.C.S.; formal analysis, V.V. and L.T.; investigation, V.V. and L.T.; resources, A.P., V.V., and Y.C.S.; data curation, V.V., C.H., and L.T.; writing—original draft preparation, A.P., V.V., and Y.C.S.; writing—review and editing, C.H. and V.V.; visualization, A.P. and L.T.; supervision, C.H., V.V., and Y.C.S.; project administration, C.H. and Y.C.S.; funding acquisition, Y.C.S. All authors have read and agreed to the published version of the manuscript.

11-2-Data Availability Statement

The data presented in this study are available on request from the corresponding author.

11-3-Funding

The publication fees of this manuscript have been financed by the Research Council of the University of Patras, Greece.

11-4-Institutional Review Board Statement

Not applicable.

11-5-Informed Consent Statement

Not applicable.

11-6-Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this manuscript. In addition, the ethical issues, including plagiarism, informed consent, misconduct, data fabrication and/or falsification, double publication and/or submission, and redundancies have been completely observed by the authors.

12- References

[1] Kshetri, N. (2009). Positive externality, increasing returns, and the rise in cybercrimes. Communications of the ACM, 52(12), 141–144. doi:10.1145/1610252.1610288.

[2] Bilen, A., & Özer, A. B. (2021). Cyber-attack method and perpetrator prediction using machine learning algorithms. PeerJ Computer Science, 7, e475. doi:10.7717/PEERJ-CS.475.

[3] Rot, A., & Olszewski, B. (2017). Advanced Persistent Threats Attacks in Cyberspace. Threats, Vulnerabilities, Methods of Protection. Position Papers of the 2017 Federated Conference on Computer Science and Information Systems, 113-117. doi:10.15439/2017f488.

[4] Limba, T., Plėta, T., Agafonov, K., & Damkus, M. (2017). Cyber security management model for critical infrastructure. Entrepreneurship and Sustainability Issues, 4(4), 559–573. doi:10.9770/jesi.2017.4.4(12).

[5] Renaud, K., Flowerday, S., Warkentin, M., Cockshott, P., & Orgeron, C. (2018). Is the responsibilization of the cyber security risk reasonable and judicious? Computers & Security, 78, 198–211. doi:10.1016/j.cose.2018.06.006.

[6] Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber-crime on the financial sector. Computers & Security, 45, 58–74. doi:10.1016/j.cose.2014.05.006.

[7] Bruzzone, A. G., Massei, M., & Poggi, S. (2016). Infrastructures protection based on heterogeneous networks. International Journal of Simulation and Process Modeling, 11(1), 24–35. doi:10.1504/IJSPM.2016.075078.

[8] Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. The Economics of Information Security and Privacy, 265–300. doi:10.1007/978-3-642-39498-0_12.

[9] Ospina, J., Venkataramanan, V., & Konstantinou, C. (2023). CPES-QSM: A Quantitative Method Toward the Secure Operation of Cyber-Physical Energy Systems. IEEE Internet of Things Journal, 10(9), 7577–7590. doi:10.1109/JIOT.2022.3210402.

[10] Alomiri, A., Mishra, S., & AlShehri, M. (2024). Machine learning-based security mechanism to detect and prevent cyber-attack in IoT networks. International Journal of Computing and Digital Systems, 16(1), 645-659. doi:10.12785/ijcds/160148.

[11] Ioannou, G., Louvieris, P., & Clewley, N. (2019). A Markov Multi-Phase Transferable Belief Model for Cyber Situational Awareness. IEEE Access, 7, 39305–39320. doi:10.1109/access.2019.2897923.

[12] Armin, J., Thompson, B., Kijewski, P. (2016). Cybercrime Economic Costs: No Measure No Solution. Combatting Cybercrime and Cyberterrorism. Advanced Sciences and Technologies for Security Applications, Springer, Cham, Switzerland. doi:10.1007/978-3-319-38930-1_8.

[13] Dupont, B., Côté, A. M., Boutin, J. I., & Fernandez, J. (2017). Darkode: Recruitment Patterns and Transactional Features of "the Most Dangerous Cybercrime Forum in the World." American Behavioral Scientist, 61(11), 1219–1243. doi:10.1177/0002764217734263.

[14] Coleman, E. G. (2015). Hacker, hoaxer, whistleblower, spy: the many faces of Anonymous. Choice Reviews Online, 52(08), 52-4477-52–4477. doi:10.5860/choice.188504.

[15] Rani, S., Kataria, A., Sharma, V., Ghosh, S., Karar, V., Lee, K., & Choi, C. (2021). Threats and Corrective Measures for IoT Security with Observance of Cybercrime: A Survey. Wireless Communications and Mobile Computing, 2021. doi:10.1155/2021/5579148.

[16] Yip, M., Webber, C., & Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. Policing and Society, 23(4), 516–539. doi:10.1080/10439463.2013.780227.

[17] Holt, T. J., Freilich, J. D., & Chermak, S. M. (2017). Exploring the Subculture of Ideologically Motivated Cyber-Attackers. Journal of Contemporary Criminal Justice, 33(3), 212–233. doi:10.1177/1043986217699100.

[18] Lusthaus, J., & Varese, F. (2017). Offline and Local: The Hidden Face of Cybercrime. Policing: A Journal of Policy and Practice, 15(1), 4–14. doi:10.1093/police/pax042.

[19] Welburn, J. W., & Strong, A. M. (2021). Systemic Cyber Risk and Aggregate Impacts. Risk Analysis, 42(8), 1606–1622. doi:10.1111/risa.13715.

[20] Kshetri, N. (2016). Cybersecurity and Development. Markets, Globalization & Development Review: The Official Journal of the International Society of Markets and Development, 1(2), 3. doi:10.23860/mgdr-2016-01-02-03.

[21] Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and cybercrime: An analysis of the nature of groups engaged in cybercrime. International Journal of Cyber Criminology, 8(1), 1–20.

[22] FBI. (2010). S.R. Chabinsky, Deputy Assistant Director, Cyber Division, GovSec/FOSE Conference, talk delivered on 23/3/2010. It is, also, available, as a transcript. Available online: https://archives.fbi.gov/archives/news/speeches/the-cyber-threat-whos-doing-what-to-whom (accessed on June 2024).

[23] FireEye Company. (2018). M-TRENDS 2018: Special Report. FireEye Company, Milpitas, United States. Available online: https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html (accessed on June 2024).

[24] Algarni, A. M., & Malaiya, Y. K. (2014). Software vulnerability markets: Discoverers and buyers. International Journal of Computer and Information Engineering, 8(3), 480-490.

[25] Paulheim, H. (2017). Knowledge graph refinement: A survey of approaches and evaluation methods. Semantic Web, 8(3), 489–508. doi:10.3233/SW-160218.

[26] Deloitte. (2016). Beneath the surface of a Cyberattack: a deeper look at business impacts. Deloitte, Baku, Azerbaijan. Available online: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-beneath-the-surface-of-a-cyber-attack.pdf (accessed on May 2024).

[27] EUGDPR. (2017). GDPR Portal: Site Overview. General Data Protection Regulation. Council of the European Union. Available online: https://gdpr.eu/ (accessed on May 2024).

[28] Alpcan, T., & Basar, T. (2003). A game theoretic approach to decision and analysis in network intrusion detection. 42nd IEEE International Conference on Decision and Control (IEEE Cat. No.03CH37475), 3, 2595–2600. doi:10.1109/cdc.2003.1273013.

[29] Fudenberg, D., & Tirole, J. (1991). Game theory. MIT press. Cambridge, United States.

[30] Wardell, C. L., Wynter, L., & Helander, M. (2008). Capacity and value based pricing model for professional services. Journal of Revenue and Pricing Management, 7(4), 326–340. doi:10.1057/rpm.2008.18.

[31] Antonopoulou, I. (2002). A user authentication protocol based on the intractability of the 3-coloring problem. Journal of Discrete Mathematical Sciences and Cryptography, 5(1), 17–21. doi:10.1080/09720529.2002.10697934.

[32] Antonopoulou, S., Stamatiou, Y. C., & Vamvakari, M. (2007). An asymptotic expansion for the q-binomial series using singularity analysis for generating functions. Journal of Discrete Mathematical Sciences and Cryptography, 10(3), 313–328. doi:10.1080/09720529.2007.10698122.

[33] Train, K. E. (2009). Discrete choice methods with simulation. Cambridge university press, Cambridge, United Kingdom.

[34] Greene, W. H. (2003). Econometric Analysis. Prentice Hall, Saddle River, New Jersey.

[35] McFadden, D. (1973) Conditional Logit Analysis of Qualitative Choice Behavior. Frontiers in Econometrics, Academic Press, Cambridge, United States.

[36] Gujarati, D. N., & Porter, D. C. (2009). Basic econometrics. McGraw-hill, New York, United States.

[37] Gkintoni, E., Halkiopoulos, C., & Antonopoulou, H. (2022). Neuroleadership as an Asset in Educational Settings: An Overview. Emerging Science Journal, 6(4), 893–904. doi:10.28991/ESJ-2022-06-04-016.

[38] Antonopoulou, H., Giannoulis, A., Theodorakopoulos, L., & Halkiopoulos, C. (2022). Socio-Cognitive Awareness of Inmates through an Encrypted Innovative Educational Platform. International Journal of Learning, Teaching and Educational Research, 21(9), 52–75. doi:10.26803/ijlter.21.9.4.

[39] Gousteris, S., Stamatiou, Y. C., Halkiopoulos, C., Antonopoulou, H., & Kostopoulos, N. (2023). Secure Distributed Cloud Storage based on the Blockchain Technology and Smart Contracts. Emerging Science Journal, 7(2), 469–479. doi:10.28991/ESJ-2023-07-02-012.

[40] Lin, J., Zhang, H., Adams, B., & Hassan, A. E. (2023). Vulnerability management in linux distributions: An empirical study on debian and fedora. Empirical Software Engineering, 28(2), 47. doi:10.1007/s10664-022-10267-7.

[41] Kshetri, N. (2006). The simple economics of cybercrimes. IEEE Security and Privacy, 4(1), 33–39. doi:10.1109/MSP.2006.27.

[42] Security Intelligence. (2016). Lessons Learned From 11 Years of Cost of Data Breach Research. IBM, United States. Available online: https://securityintelligence.com/cost-of-a-data-breach-2016/ (accessed on May 2024).

[43] Jovanović, J. (2015). Graph-Based Knowledge Models. Available online: http://ai.fon.bg.ac.rs/wp-content/uploads/2015/04/Graph-based-KBs-eng.pdf (accessed on May 2024).

[44] Gómez-Pérez, A., Fernández-López, M., & Corcho, O. (2004). Ontological engineering: with examples from the areas of knowledge management, e-commerce and the Semantic Web, Springer, London, United Kingdom. doi:10.1007/b97353.

[45] Telang, R., & Wattal, S. (2007). An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price. IEEE Transactions on Software Engineering, 33(8), 544–557. doi:10.1109/tse.2007.70712.

[46] Merrick, K., Hardhienata, M., Shafi, K., & Hu, J. (2016). A Survey of Game Theoretic Approaches to Modeling Decision-Making in Information Warfare Scenarios. Future Internet, 8(3), 34. doi:10.3390/fi8030034.

[47] D. Palmer. (2016). Cybercrime Inc: How hacking gangs are modeling themselves on big business. ZDNet, New York, United States. Available online: https://www.zdnet.com/article/cybercrime-inc-how-hacking-gangs-are-modeling-themselves-on-big-business/ (accessed on June 2024).

[48] Armin, J., Foti, P., & Cremonini, M. (2015). 0-Day Vulnerabilities and Cybercrime. 2015 10th International Conference on Availability, Reliability and Security. doi:10.1109/ares.2015.55.

[49] Lund, M. S., Solhaug, B., & Stølen, K. (2011). Model-driven risk analysis: The CORAS approach. Springer, Berlin, Germany. doi:10.1007/978-3-642-12323-8.

[50] Vlachou, E., Karras, A., Karras, C., Theodorakopoulos, L., Halkiopoulos, C., & Sioutas, S. (2023). Distributed Bayesian Inference for Large-Scale IoT Systems. Big Data and Cognitive Computing, 8(1), 1. doi:10.3390/bdcc8010001.

[51] Antonopoulou, H., Theodorakopoulos, L., Halkiopoulos, C., & Mamalougkou, V. (2023). Utilizing Machine Learning to Reassess the Predictability of Bank Stocks. Emerging Science Journal, 7(3), 724–732. doi:10.28991/ESJ-2023-07-03-04.