# Intellectual Property Valuation in the Cyber Security Sector

Marta E. Wachowicz
Technology Transfer Unit
NASK - National Research Institute
Warsaw, Poland
marta.wachowicz@nask.pl

## ABSTRACT / POVZETEK

This paper explores the applicability of intellectual property rights (IPR) valuation methods in cyber security by using the criteria of the Artificial Intelligence development phase model. After analysis of the interconnections and interdependency in cyber security products, an approach to data quality is proposed. It is worth emphasizing that the process of valuating IPRs is highly contextual and requires professional judgment based on the experience of the appraiser, now also in terms of data management. This issue has not been discussed in the literature, an article is a contribution to the discussion on the importance of valuation in the cyber sector, given the specific characteristics of cyber start-ups using AI and machine learning solutions. Despite all these difficulties, IPR valuation will become increasingly necessary and induce further questions regarding the valuation of a given intellectual property (IP). Firstly, how to value a patent with Artificial Intelligence (AI), secondly how to assess the level of sophistication of model training, and thirdly how to rate and value data quality, or more broadly data sets. The findings can help practitioners, especially from Technology Transfer Offices, to develop roadmaps for IP valuation in the cyber security industry.

KEYWORDS / KLJUČNE BESEDE

IPR valuation, IP in cyber security, data quality in AI model

## 1. CYBER SECURITY SPECIFICITY VERSUS IPR VALUATION

### 1.1 Introduction

The growth in importance of IPR is unquestionable, in every sector of the economy, and in those key to the digital transformation an undisputed. The IPR valuation is gaining in importance and reliable valuation is relevant in the cyber security sector. The valuation approach dedicated to the cyber market is not described in the literature and represents an unexplored research question. In IPR valuation, whatever the method, the essential characteristics of an intellectual asset should be taken into account. There is a fundamental complication arising from the difficulty of determining the essential characteristics of IP, the scope of protection, and the need to consider source data related to potential cyber exploitation on an unprecedented scale. IP assets can be independently identified, are transferrable, protected and that protection can be enforced. In the case of cyber, they have an economic lifespan, defined by their characteristics. Depending on the nature of intangible assets, there are different legal instruments by which protection is possible and ultimately benefit from using them. It is important to understand the economic value of cyber IP assets by carrying out an IP valuation. The article addresses a topic specific and relevant to the digital economy, the literature abounds with methodologies for different approaches to valuing IPR [9], [1], but there is no guidance on how to consider the importance of data, learning models, and all aspects of AI in new inventions. The challenges faced by the cyber security sector are defensive AI and machine learning technology, sophisticated cyber attacks, reinforcement learning-based cyber attacks, AI-enabled malware, the vulnerability of IoT technology, cloud security issues, and the involvement of cryptography. However, future directions, in cyber security, such as quantum-secure encryption, biometric authentication, advanced artificial intelligence, and machine learning, may be able to address these issues.

### 1.2 Cyber security products

According to the American Authorities, precisely Cyber Security and Infrastructure Security Agency, cyber security is “the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information” [2]. The current cyber security situation is characterized by the regular emergence of new cyber threats. The most common types of cyber threats include malware, phishing attacks, ransomware, threats against data or availability, disinformation, supply chain targeting, and distributed denial of service (DDoS) attacks. The level of digital resilience varies from different industries and countries, however, effective cyber security remedies use security technologies and techniques such as intrusion detection and prevention systems, firewalls, antivirus software, and encryption [8]. Cyber attackers are constantly evolving their approach to penetrate the computer systems of enterprises which means that organizations must continuously monitor their networks against potential attack vectors, using a broad array of cybersecurity solutions to protect the entire ecosystem, including clouds and several applications [8].

Typical products are software for stopping the biggest, bandwidth-busting DDoS attacks, software that proactively reduces attack surfaces, Edge DNS, authentication services, clouds for protecting customers and providing data security, which reduce friction during registration, authentication, and sign-ins while making it easy for customers to control their accounts from any device. Products are, on the one hand, closely related to IT or ICT. On the other hand, they use the latest developments in biometrics, behaviorism, psychology, and the sociology of human behavior. They use, as in criminology, knowledge about human behavior, but the implementation of knowledge is strictly technical, in a digital world.

# 2. MULTIDIMENSIONAL IP PROTECTION

## 2.1 Impact of cyber product features on IP protection

The development of new solutions to combat or prevent cybercrime requires the proactive action and the creation of new inventions combating the criminal incidents. Since AI is widely used in cyberspace, AI-based products are also tools for mitigating attacks. Ransomware and phishing attacks encrypt critical data, demand high ransoms, and disrupt a wide range of operations. The growing use of Internet of Things devices is introducing new security vulnerabilities, while cyber attacks targeting the software supply chain are exploiting third-party vulnerabilities to gain access to sensitive information. Artificial intelligence technologies enable cybercriminals to launch sophisticated attacks. These AI-based threats are often not subject to traditional security measures, making them difficult to detect and mitigate. The World Intellectual Property Organization (WIPO), the United Nations agency that serves the world’s innovators, is following the trend of consumer interest in AI in various economic, social, and cultural sectors, having published some very interesting and important reports on AI over the past few years. [6], [10]. WIPO Technology Trends 2019 – Artificial Intelligence reveals trends in patenting of artificial intelligence innovations [10]. AI-related patents disclose AI techniques and applications and refer to an application field or industry. WIPO analysis shows that many sectors and industries are exploring the commercial exploitation of AI, telecommunications (mentioned in 15 % of all identified patent documents), transportation (15 %), life and medical sciences (12 %), and personal devices, computing and human-computer interaction (11 %), the rest - other sectors including banking and security. In the WIPO patent landscape report on Generative AI, there are the latest patent trends for GenAI with a comprehensive and up-to-date understanding of the GenAI patent landscape, alongside insights into its future applications and potential impact. The report explores patents relating to the different modes, models, and industrial application areas of GenAI. Deep neural networks can be adapted to be either discriminative or generative tasks, which has led to the development of various types of GenAI models, which can support different types of input and output data. This opens up a new perspective on the protection of inventions and products.

There is a need to answer the threshold question of whether such AI-related inventions qualify for patent protection. The United States Patent and Trademark Office (USPTO) has issued guidelines to clarify the requirements for patenting AI-assisted inventions. For an invention to be patentable, there must be significant human input into its conception. Human inventors must make a significant contribution to the invention that goes beyond the mere use of AI tools. Otherwise, the invention is not eligible for patent protection. In addition, the USPTO has created five principles for evaluating AI-assisted inventions, the fifth is worth mentioning here - namely, merely owning or supervising an AI system does not qualify a person as an inventor without a significant contribution to the concept of the invention [7]. This principle ensures that human ingenuity remains at the heart of patentable inventions while recognizing the supporting role of AI in the inventive process. In the cyber industry, solutions can be protected by patents and then there is a need to value IPR in the form of a patent on an AI-related property. The number of cyber security patent applications per year shows that the amount of investment going into finding new ways to help prevent cyber attacks is huge. However, it is usually a bundle of different IPs that is valued. Apart from the fact that AI-related IP problems appear numerous, including AI inventorship, patent eligibility, and AI-related copyright issues, particularly important are data issues.

## 2.2. FLDX system – an example of IPR protection

An example of a cyber security product is the FLDX system, patent protected by NASK, a Polish National Research Institute, whose mission is to develop and implement solutions that facilitate the development of information and communication networks in Poland, in addition to improving their effectiveness and security. Patent – PL241005-*Method and system for adaptive creation of network traffic filtering rules on a network device spontaneously detecting anomalies and automatically suppressing volumetric attacks (DDoS)* protects digital services and network devices from DDoS attacks and a sudden and unpredictable increase in user activity. Sudden and unexpected bursts of Internet traffic can saturate network links or overloading application servers. Therefore, protecting networks and digital services from intentional attacks must go along with fair distribution of network resources. The FLDX system is a fast and extremely effective way to protect the availability of services on the network - whether the source of the threat is a volumetric DDoS attack or a sudden increase in user activity. Maintaining a fair distribution of network bandwidth is the primary goal of the FLDX system, achieved in a time of up to 10 seconds. Unlike the solutions currently offered in the anti-DDoS market, the FLDX system is not based on a database of signatures and static rules. It dynamically self-adjusts filters to the current situation. This approach allows us to react extremely quickly to the observed changes in network load, as well as forecast them. The FLDX system is therefore not only a protection tool - it is also a network knowledge discovery tool. The object of the invention is a method for adaptively creating network traffic filtering rules on a network device spontaneously detecting anomalies and automatically suppressing volumetric attacks (DDoS).

That FLDX example may illustrate the challenges of protecting IPR in this area. The speed and precision of the FLDX system are the result of years of scientific research in the fields of control theory and adaptive signal processing, the IP behind the solution is not only a patent, but also a copyright protecting the software and the user's system, trade secret, the implicit knowledge of the implementation as well as the knowledge contained in the technical documentation. Solutions are sporadically planned to be patent-protected, due to non-compliance with requirements for implementations of mathematical theorems or new applications of functional analysis. However, even an obtained exclusive right is not sufficient protection in the market. It is necessary, as with other software-based products, to supplement protection not only with copyright protection due to the nature of the solution but also to keep in secret any know-how resulting from the implementation and to circumvent technical problems arising from software development and installation in the cloud or at the customer's site.

# 3. IPR VALUATION ISSUES

## 3.1 Valuation approach selection

Valuation of IPR regardless of the subject of valuation strictly depends on the potential area of application of the protected technology. In the cyber sector, the issue of the valuation of IP goods is becoming increasingly challenging, for several reasons. First, this is due to the obvious development of the cyber market and the growing demand for all kinds of services and products protecting digital assets. Secondly, AI technologies are finding applications in this sector, which makes the valuation problem more complicated, and thirdly, a complex method of product IPR protection is common. The issue of IPR valuation in high-growth sectors, for new technologies, and cutting-edge technologies, has been addressed in the literature for years. Major researchers (such as Damodaran) describe the challenges of estimating value for technology [1], [9]. However, the growing cyber market introduces a significant level of complexity to the subject, due to the dynamics of development, key development trends, market estimation, and the scalability and adaptability of solutions in this market.

Depending on the nature of intangible assets, various legal instruments are offered to protect and ultimately profit from them. IP management is a key element of the business strategy of entities developing cyber services. The linkage of copyright protection, patent, trade secret, and confidential know-how protection makes IP valuation difficult. Trade secrets may be preferable to patents in several circumstances, such as when the patentability requirements may not be satisfied; the cost of pursuing patent protection outweighs the benefits; and/or the need for IPR protection extends beyond the available patent term [9].

Regardless of the method used, the valuation process requires gathering a lot of information about intellectual property assets, as well as an in-depth understanding of the economy, industry, and specific businesses that directly affect their value. It is well known that there are three basic categories of valuation methods for evaluating intellectual property and intellectual property rights: income-based, market-based, and cost-based. The choice of the appropriate method for valuing intellectual property depends on the type of intellectual property, the stage of development, the purpose of the valuation, and the available data. The cost method establishes the value of an IP asset by calculating the cost of a similar (or exact) IP asset. The cost method is particularly useful when the IP asset can be easily reproduced and when the economic benefits of the asset cannot be accurately quantified. This method does not account for wasted costs, nor does it consider any unique or novel characteristics of the asset. Although a cost-based method is used for software value estimation, the combination of various elements of protection makes one think about the wisdom of choosing a revenue-based method [9]. The income method values the IP asset based on the amount of economic income that it is expected to generate, adjusted to its present-day value. This method is easiest to use for IP assets with positive cash flows, for those whose cash flows can be estimated with some degree of reliability for future periods, and where a proxy for risk can be used to obtain discount rates. The market method is based on a comparison with the actual price paid for the transfer of rights to a similar IP asset under comparable circumstances. This method has the advantage of being simple and based on market information, so it is often used to establish approximate values for use in determining royalty rates and inputs for the income method. For cyber industry this type of approach can be highly problematic, since products in the cyber crime market are evolving very quickly and there is considerable difficulty in comparing them. Often, it is only possible to make inferences on the level of effects offered, i.e. expected rather than concrete results, due to the widespread confidentiality of information. Companies do not necessarily boast about the ineffectiveness of protecting their computers, resources, or access to the cloud.

While one approach may seem particularly well-suited, the final value estimation should merge the value indications obtained under different approaches [1], [9]. Irrespective of the choice of valuation approach, in the situation of innovation, patent, or AI-related know-how, there is an issue directly related to the understanding of the operation and use of AI models [4].

## 3.2. Data in Artificial Intelligence model

During training, the artificial intelligence model is exposed to a prepared dataset and tries to learn the patterns and relationships present in the data. This process involves adjusting the internal parameters of the model based on the input data and the desired outcome. In a situation where AI is used, another problem arises. When is the product in question completed? AI models need to be taught. What does AI model training include?

AI model training includes three main aspects:

a) data collection

There are ready-to-use open-source data sets. Data collection and other resources are also collected and used. Internal data collection provides access to proprietary information and control over data quality. Web scraping is the process of extracting data from websites using various tools. Automation eliminates the need for manual data collection, which in itself is impractical when it comes to training AI models. Regardless of the data collection technique, the data should be relevant, accurate, consistent, presentable, and complete. Such data increases the accuracy of the AI model, reduces bias, and increases user confidence and trust in the AI model.

b) data processing

Having a rich data set, it is necessary to validate the data. Data validation involves preparing the data to match the requirements of the specific learning mechanism used by the artificial intelligence model. Each learning technique requires the data to be presented in a specific way. An artificial intelligence model incorporating algorithms that learn through supervised learning aims to predict or classify new data points. So, to select data for an artificial intelligence model equipped with supervised learning algorithms, label your data. Then divide the selected data into training, validation, and test sets. Using the training set is needed to teach the artificial intelligence model, the validation set to evaluate performance, and the test set to evaluate the final model. For unsupervised learning, the artificial intelligence model aims to reveal underlying structures, group similar data, and discover patterns without the help of labels. The model needs to understand the data by finding commonalities and understanding the features that define a particular dataset. In this case, feature-based clustering of the data is required. This makes it easier for the AI model to navigate and learn from unlabelled data. The situation becomes a little more complicated taking into account reinforcement learning (learning through interaction) [5]. Artificial intelligence models involving reinforcement learning learn by exploring the specifics of a task in a particular environment and performing functions by trial and error. In reinforcement learning, an environment must be simulated for the AI model to interact with. However, another level of complication relates to deep learning (neural networks and beyond) , it is an advanced learning mechanism that drives the AI model and enables it to handle complex actions. AI models with deep learning algorithms require large-scale data collection based on what the model is supposed to do. As deep learning algorithms use multiple layers of learning, the goal is to have different versions of large data sets.

c) providing selected data to the AI model and iterative refinement

Once the data has been structured based on the AI model's learning technique, the data is fed into the AI model. The model learns from the algorithms on which it is built. During the learning stage, the capabilities of the model should be explored for refinement. Without iteration, the model cannot adapt to changing data and cannot improve its performance when exposed to other data sets.

This raises further questions regarding the valuation of a given IP. Firstly, how to value a patent with AI, secondly how to assess the level of sophistication of model training, and thirdly how to assess and value the quality of training and validation data, or more broadly data sets. In addition, in the cyber area, matters are further complicated by the use of sensitive or confidential data, such as tools for detecting illegal, offensive or harmful content based on data from law enforcement agencies. An additional legal complication arises.

## 4. RECOMMENDATIONS AND CHALLENGES OF VALUATION IN CYBER SECURITY SECTOR

### 4.1 Exploring difficulties

Nowadays, cyber security plays a crucial role in the global economy. The risk of cyber threats becomes more prevalent and cyber attacks can have devastating consequences leading to financial losses, reputational damage, and national security breaches. Therefore, it is imperative that governments prioritize cyber security measures to safeguard their interests. In addition to economic implications, cyber attacks also pose significant risks to national security. Governments around the world are increasingly concerned about hacking activities that aim to steal sensitive information or disrupt critical infrastructure systems.

Cyber attacks usually modify, access, or destroy sensitive information, extort users' money, or disrupt normal business processes. In 2024, the cyber security industry is expecting a paradigm shift in a more coherent and business-involved approach that reflects a better understanding and management of cyber threats [8]. This shift concerns the latest technology adoption and revolution, associated liability, maturity, integration, regulatory, quantification, communication, and behavioral shifts. As the market grows, there will undoubtedly be an increased demand for intellectual solutions to support the fight against cyber crime. Hence, the growth in importance of IPR will be indisputable, which in turn will result in a significant increase in the valuation of IP and its need in the market [3]. Therefore, IP valuation is an important issue, and reliable valuation is important for multinational corporations involved in IP transactions. IP valuation guidelines and regulations are also changing around the world due to different statutory provisions in each country. Valuing intellectual property involves assigning a monetary value to the intangible assets of a business entity. However, the intangible nature of intellectual property means that it is often difficult to value and define, making it challenging to set a fair price.

### 4.2 Recommendations

The most challenging tasks are determining the scale of the valuation portfolio, determining the role of AI in an invention, patent, or confidential know-how, determining the strength of a patent using AI and comparing it to other similar solutions, and determining the extent of model validation and database quality. Of course, issues related to the market, comparison of coverage, the scale of adaptation, etc. are also in force. However, completely new problems are gaining importance, the valuation of IPR in the cyber sector will be a further stage of complication and will require knowledge of a great level of AI invention protection and data management. A large part of everyday life is based on technology; personal, sensitive, and business data are stored on computers, smartphones, and tablets, so an extensive range of concepts are covered by cyber security - from communication to transport, and shopping to healthcare. It is crucial to consider the interrelationships and relationships between the different types of IP. Depending on the business needs, an appropriate valuation method should be chosen, taking into account whether the IP relates to AI. When analyzing an AI-related patent, the relationship to the data, the individual datasets, and the way the models are taught should be explored. Particular care should be taken to analyze the quality of the data and to understand the principles of data management (from collection, description, sharing, archiving, etc., including the FAIR principle – it is an acronym for Findable, Accessible, Interoperable, and Reusable). In addition, the origin of the data in the cyber sector should be taken into consideration. Moreover, in the cyber area, further complications are caused by using sensitive or confidential data, such as tools for detecting illegal, offensive, or harmful content based on data from law enforcement agencies.

Without high data quality, even the most advanced artificial intelligence models will fail. Data quality in the new era of AI highlights the key role of data quality in shaping effective data strategies. The task of the IPR evaluator in cyber products or solutions is to evaluate the AI model, and assess how each dataset is used, how the evaluation process works, which IPRs use it, and to what extent, and what parameters influence the business aspect of the entire evaluation process. The process of valuing IPRs is highly contextual and requires professional judgment based on the experience of the appraiser, now also in terms of data management and understanding of AI development and application phase.

### REFERENCES

[1] Damodaran, A., Investment Valuation, John Wiley & Sons, New York, 1994

[2] https://www.cisa.gov

[3] Marius Schneider, Intellectual property rights, the new currency, Journal of Intellectual Property Law & Practice, Vol 14, Iss.11, 2019, p.825–826, https://doi.org/10.1093/jiplp/jpz106

[4] Kathi Vidal, The Applicability of Existing Regulations as to Party and Practitioner Misconduct Related to the Use of Artificial Intelligence, 2024

[5] Lee J. Tiedrich, Gregory S. Discher, Fredericka Argent, and Daniel Rios 10 Best Practices for Artificial Intelligence Related Intellectual Property Intellectual Property Technology Law Journal,.vol.32, nr.7, 2020.

[6] Patent Landscape Report - Generative Artificial Intelligence (GenAI), World Intellectual Property Organization Geneva, Switzerland, 2024, https://doi.org/10.34667/tind.49740

[7] https://www.uspto.gov

[8] Wasyihun Sema Admass, Yirga Yayeh Munaye, Abebe Abeshu Diro, Cyber security: State of the art, challenges and future directions, Cyber Security and Applications Vol.2, 2024, 100031. https://doi.org/10.1016/j.csa.2023.100031

[9] William J. Murphy, John L. Orcutt, Paul C. Remus, Patent Valuation: Improving Decision Making through Analysis, Wiley, 2012

[10] WIPO Technology Trends 2019 – Artificial Intelligence, Geneva, Switzerland: World Intellectual Property Organization, 2019, https://doi.org/10.34667/tind.29084