https://doi.org/10.53656/str2024-1s-3-enh

Research Results
Резултати от научни изследвания

ENHANCING ECONOMIC SECURITY THROUGH INTELLECTUAL PROPERTY

Dr. Dimiter Gantchev, Assist. Prof.
University for National and World Economy

Abstract. Intellectual property has a key role in ensuring national economic security. It is being constantly challenged and multiple risks affect its adequate application. Intellectual property threats need to be addressed on government, company and individual level to tackle serious security risks and prevent damages. The article reviews relevant policies and strategies, which need to be put in place, in view of the adoption of disruptive technologies such as artificial intelligence. It also discusses the elements of a robust and systemic economic model, which would enable monitoring and assessing the risks and multiple dimensions of IP threats in their interaction with the digital environment and infrastructure. Such a model could form and objective basis for evidence-based policy making to enhance national security through intellectual property.

Keywords: intellectual property; economic security; competitiveness
JEL: O34, L82

Introduction

The concept of economic security has a narrow and broad interpretation. In the narrow sense it usually refers to the degree, to which individuals are vulnerable to hardship-causing economic losses (OECD, 2018). Much research has been done in this field. The broad concept of economic security today presents a multifaceted approach to ensuring a secure environment for the development of nations. It encompasses a broad set of interconnected issues and elements, such as investment screening, anti-coercion instruments, research integrity, and supply chain resilience (Chattam House 2023). The economic prosperity of nations motivates policy actions, it dominates the public debate and influences decisions in all areas. Among the central components of economic security today feature such values as competitiveness, efficiency, leadership in new technologies, investment in future related developments, among others. One common feature of these elements is that they are all intangible and indicate a level of superior knowledge in different domains.

Overwhelming evidence suggests that the in the current environment knowledge is the most valuable asset of nations. Increasingly countries are adopting models of

growth which are based on knowledge and innovation. As the body of knowledge expands it is becoming a crucial necessity to protect this knowledge from misuse and misappropriation in view of its central role to the competitiveness of nations. The most efficient way of safeguarding knowledge is by way of intellectual property (IP) protection. Through its main forms – patents, trademarks, copyright, design and trade secrets, intellectual property defines the mechanisms for monetization of creative and innovative expressions. Creativity becomes the new currency, and it travels across boundaries and formats. In the creative economy IP protection is the major method through which creators and innovators can monetize the expression of their innovative ideas.

Intellectual property as intangible property is, by definition, perfectly adapted for digital transactions in the online environment. It can be monetized, securitized, and serve as mechanism to secure funding for economic undertakings. IP protection mechanisms define the market framework for transactions with creative and innovative products. During its economic exploitation there are various risks which can undermine the efficiency of the IP framework. Today intellectual property is becoming a strategic asset and as such it needs to be protected insofar as it may jeopardize strategic national development objectives (Gantchev 2022). The efficient management of intellectual property is a key factor for the functioning of Industry 5.0 (Stoyanova 2022) and a well structured policy on intellectual property protection stimulates economic growth (Stijlev 2019).

The purpose of this article is to review relevant concepts to the role of intellectual property in economic security. It focuses on three questions:

– How do we deal with the major security risks to intellectual property as part of the economic security?

– How are IP security risks treated in national IP strategies?

– How can we better assess the level of security risk posed by intellectual property-related challenges?

Background

In order for IP protection to function it needs to be widely adopted, respected and enforced. Protecting intellectual property is not without problems and requires proper assessment of the risks and challenges involved.

The first challenge is of policy nature. Is the government committed to ensuring respect for IP? The obvious response would be positive, because many governments have signed up to the international conventions establishing the IP multilateral framework for protection. 180 countries are members of the Paris Union Convention on industrial property rights and 181 of the Berne Convention Assembly, governing the protection on literary and artistic works (WIPO, 2024). This means that most countries have taken upon obligations to respect international IP norms. However, in a number of cases governments turn a blind eye to systematic infringement of IP because it gives a competitive edge to their companies, allowing them to circumvent

international norms, gaining in speed, volume and scope of economic operations which are de facto based on non-respect of IP protection. Some countries even form alliances to revise international IP norms, prevent IP protection for extending to new areas or challenge the strict implementation of existing rules and norms.

The second group of challenges to IP are of technology nature. Technological security is threatened by the following developments:

– Evolving Cyber Threat Landscape: Cybercriminals continually adapt their tactics, techniques, and procedures to breach security defenses and exploit vulnerabilities in IP protection strategies.

– Advanced Persistent Threats: these are often sponsored by nation-states and engage in long-term, covert operations to steal intellectual property for economic, political, or military gain.

– Insider Threats: Employees or trusted insiders with access to sensitive information can abuse their privileges or leak IP, posing a significant risk to organizations.

– Lack of Awareness and Training: Insufficient cybersecurity awareness among employees, infrastructure changes during mergers and acquisitions, and a reluctance to change working practices, can lead to sharing of sensitive IP or being prone to social engineering attacks.

While the digital transformation has brought about numerous benefits, it has also made countries susceptible to cyber threats, including IP theft. Safeguarding digital assets from cyber threats is a global pressing concern. The number of breached data records in 2023 was almost 6 billion 5,951,612,884 (IT Governance, 2023). One should bear in mind that not all security incidents are publicly disclosed, so this number is an underestimation. A recent report published by the UK's National Cyber Security Centre found that nearly 75% of the UK's top-100 law firms have been affected by cyberattacks (National Cyber Security Center, 2023). Phishing and cyber-attacks are becoming more sophisticated because attackers are using personal information pulled from the Dark Web (stolen financial information, social security numbers, addresses, etc.), LinkedIn and other internet sources to create targeted personal profiles that are highly detailed and convincing. They also use trusted services such as Outlook.com or Gmail for greater credibility and legitimacy. Ai is increasingly used to generate these attacks. Today's cybersecurity realities are recognized by professionals at technology, cultural and law firms: highly sensitive data, a continuously evolving threat landscape and an ever-increasing attack surface in corporate environments.

Intellectual property theft refers to unauthorized access, use, or exploitation of someone else's creative work, inventions, or proprietary information. In the digital realm, intellectual property theft concerns all branches of intellectual property and involves hacking, data breaches, trade secret theft, file sharing and unauthorized distribution or replication of copyrighted material (Halbert 2016).

What are the major consequences of these threats?

The consequences of IP theft can result in serious damages of different nature to nation states, companies and organizations:

– Economic Impact: Lost revenue due to IP theft, which can result in impact on market share as well as the loss in value of stolen assets, limited resources for further innovation due to the cost of investigations and legal proceedings.

– Damage to Reputation: Intellectual property theft can impact on the organization's reputation, jeopardize customer trust, and result in a loss of business opportunities. Investors always check the level of IP respect and infringement before making strategic decisions on new investment in companies or countries.

– Competitive Disadvantage: Unauthorized use or disclosure of IP can enable competitors to replicate or undermine the organization's unique products, services, or technologies, eroding market share.

– Innovation Stifling: Fear of IP theft can deter businesses and individuals from investing in research and development, hindering technological advancement. A lower level of inventive, patent, licensing and innovation activity usually is accompanied by increased level of counterfeiting and piracy.

– Job Losses: In sectors like software development and creative industries, IP theft can lead to job losses if businesses struggle to compete.

– Legal and Regulatory Consequences: Organizations may face lawsuits, penalties, and other legal repercussions if they fail to protect their intellectual property adequately. Even if they win in the litigation process, they will have suffered losses in terms of time, preventing the use of the IP during the proceedings and occasionally loss of the innovative edge of the IP.

Dealing with IP challenges as security threats

Security threats to IP can be addressed on several levels. Policy challenges which are dealt on the level of the state can be tacked through international cooperation and multilateral negotiations. IP protection is a recurrent theme for high level talks between government officials representing countries which have a strong IP profile. Moreover, we see that IP protection becomes a norm for new Free Trade Agreements, indicating that IP is becoming an important part of economic policy. Examples of these are to be found in recent US, EU, ASEAN and NAFTA trade agreements. Collaboration with international and regional organizations is required to effectively combat cross-border IP theft effectively. Public Awareness is key to educating consumers about the importance of IP protection and the consequences of IP theft and is given high priority as a policy dimension of the work on IP respect.

On the legal side measures usually include strengthening of the legal frameworks through enhancing IP laws and regulations to adapt to the digital age, ensuring that they provide adequate protection for digital assets and ensuring secure transactions with IP. This trend is observed in multiple territories. Recent example is Croatia

which is undertaking steps to significant changes in order to achieve clarity and to develop a streamlined version of secured credit involving IP (Matanovac, Ernst & Gliha 2020).

Economic measures include the encouragement of innovation and research by providing incentives and support to businesses and individuals, thus reducing incentives for IP theft. The World Bank notes that "The stronger the capabilities of a nation's enterprises to develop distinctive products and new technologies, the greater the preferences of consumers for quality guarantees among similar products; the wider the markets in which artists wish to sell their music and literature, and the easier it is to misappropriate the returns to invention through imitation, the more pronounced will be interests in protection"(World Bank 2002).

On the organizational policy level IP challenges require companies to have a strict IP policy providing clear guidelines on the levels of intolerance to IP leakage and on the resulting actions and measures. These may include:

– Implementing Robust Access Controls: Role-based access control can restrict access to sensitive information. The zero-trust approach assumes that no user or device should be automatically trusted, regardless of their location within or outside the network perimeter. By implementing zero trust principles, organizations enforce granular access controls, authentication, and continuous monitoring, ensuring that only authorized entities can access resources. This approach also minimizes the potential for lateral movement within the network, reduces the attack surface, and mitigates the risk of insider threats. Zero trust provides a proactive and adaptive security framework that aligns with the evolving threat landscape and safeguards critical assets effectively. Strong authentication mechanisms, such as multi-factor authentication, to prevent unauthorized access can be used, as well as encryption of sensitive data to protect against unauthorized interception.

– Insider Threat Mitigation: Implementing strict user access monitoring and auditing is a modern-day necessity and industry best practice. This may involve background checks on employees with access to critical IP and implementing other data loss prevention solutions to detect and prevent unauthorized data exfiltration.

– Continuous Vulnerability Management: Regular vulnerability assessments and penetration testing can identify and address potential security weaknesses. This gives organizations tactical advantage in adopting intellectual property security. A comprehensive approach to cybersecurity includes an ability to scale detection and response capabilities.

– Employee Education and Awareness: Providing comprehensive cybersecurity training to employees, focusing on the importance of IP protection, social engineering threats, and best practices for data handling, is becoming a proactive industry standard. Conducting regular awareness campaigns to reinforce security protocols and encourage reporting of suspicious activities is a common approach adopted by businesses of all sizes.

Adopting IP strategies

The World Intellectual Property Organization (WIPO) defines a national IP strategy as 'a set of policy measures formulated and implemented by a government to improve its IP and innovation ecosystem in line with social, cultural and economic development goals. It is cross-cutting by nature: it links IP with a wide range of public policy areas to enhance coherence and coordination in government law and policy-making (WIPO, 2020).

The WIPO guidelines on developing national IP strategies do not contain any direct reference to national security, nor the methodology for this particular risk assessment. However, addressing security can be considered as part of the broader category of respect for IP, which features prominently in the Guidelines and in almost all strategies and especially the most recent ones (Saudi Authority for Intellectual Property, 2022). A recent document analyzing the Canadian strategy states "The scope and contents of IP strategies are often superficially similar even if the more detailed measures they propose differ, for example, because of differences in levels of economic development. Typically, they include awareness-increasing measures for SMEs; (mandatory) IP teaching in engineering, natural sciences, business, and arts schools; technology transfer support; specific changes in national legislation; and improved inter-agency coordination. They normally target organisations in the R&D and innovation system but also the creative industries via the copyright theme, such as collecting societies; eventually, also enforcement agencies (judges, customs, police) (Technopolis group, 2020).

Economic security is linked to securing the competitive edge of the nation. In this regard IP strategies are much more clear and speak often of the role of IP for competitiveness, science technology and innovation.

"For Canadian businesses to grow and succeed in the innovation economy, they need to commercialize their ideas and compete in the global marketplace. Businesses need to protect their intellectual property, just as they would protect physical assets such as buildings and equipment. Patents, copyrights, trademarks, registered industrial designs, plant breeders' rights, geographical indications or trade secrets can give entrepreneurs an important advantage over their competitors" (Intellectual Property Strategy, Government of Canada, 2023).

The strategy /vision of Finland stresses also "the importance of the strategy to boost the competitiveness of the economy" (National Intellectual Property Strategy of Finland, 2022).

United States researcher, professor James Morrison at the University of Cincinnati College of Law declared that "The acknowledgment that intellectual property is integral to U.S. national security is necessary for the U.S. to continue to thrive." (Morrison 2021).

Two former heads of the United States Patent and Trademark Office USPTO – David Kappos and Andrei Iancou published a critical analysis of the current US IP

strategy. In their report they stated that national security advantages will come to the country who gains the lead in critical research on AI and who gains the lead on research and advancement in these technologies (Iancou, Kapps 2021) AI. They identified as the most significant threat to US leadership in AI technology the lack of comprehensive intellectual property policies to incentivize investments" and a strong push from China through domestic and geopolitical strategies to fill the void of U.S. intellectual property global leadership (National Security Commission, 2021).

In order to compete globally and produce a strong economy, the management and regulation of intellectual property rights are essential. Specifically, the creation of strong policies and regulations in the field of patent law and trade secrets have been considered as an integral to the growth of a country's economy and thereby the promotion of national security. According to Rob Farley, senior lecturer at Patterson School at the University of Kentucky and visiting professor at the U.S. Army War College, the two main areas of intellectual property that deal with national security are patent law and trade secrets (Farley 2019).

On the one hand, patent law and trade secrets are critical to develop or encourage the development of inventions, techniques, or other applicable material that correlates directly with national security use, i.e. in the military field. On the other hand, patents or trade secrets can advance the economy and ensure leadership and competitive edge as they can incentivize and protect the huge investments required to make important discoveries.

This understanding is clearly adopted by China as well. The Chinese President Xi Jinping has recognized on multiple occasions the critical role of IP in innovation and national security. Chinese innovations have come in the form of increased patenting, providing injunctions for infringement of patented inventions, and creating special intellectual property courts. China became the leading country in the world in terms of the number of patents filed in domestic offices. In 2022, China's IP office received around 1.62 million patent applications (WIPO, 2023). Of course, one should differentiate between measures which simply incentivize mass generation of patent applications and policies that incentivize actual innovation.

According to the Commission on the Theft of American Intellectual Property, the effect of IP theft on the U.S.'s economy is disastrous and directly related to national security (Morrison 2021).

The debate on the IP related to national security takes a different dynamics in light of Artificial Intelligence, machine learning and associated technologies. AI and its applications are transforming existing threats, creating new classes of threats, and enabling adversaries to exploit the vulnerabilities of democratic societies. The National Security Commission on Artificial Intelligence ("NCSAI) stated that the way that AI systems extend the "range and reach of adversaries" into the U.S. is comparable to ways that the missile age and terrorism brought threats "closer to home" (NCSAI, 2021).

The NSCAI summarized five core AI related threats.

The first one is "AI-Enabled Operations." AI and associated technologies increase the magnitude, precision, and persistence of adversarial information operations, mostly through the production of malign information based off individual's online profiles and the providing this information into online platforms. The interjection of malign software and information into the general data stream and social media creates can create chaos and a multitude of false realities, which is a threat to national security.

The second AI-related threat identified in the report is "Data Harvesting and Targeting of Individuals." AI allows for a systematic harvest of data on U.S. companies and personal data. While this data incursion is a clear national security threat, it also lends credence to intellectual property theft issues, as theft of personal data could logically be done alongside any theft or make it easier to gain access to intellectual property.

The third AI-related threat is "Accelerated Cyber Attacks." AI-enhanced malware will make "cyber attacks more precise and tailored" through a compilation of new and old "algorithmic means to automate, optimize, and inform attacks." While the defensive applications of AI can improve national cyber defenses, it cannot defend "an inherently vulnerable digital infrastructure."

The fourth AI-related threat is "Adversarial AI." New artificial systems represent a unique target for attack, with a number of documented attacks involving "evasion, data poisoning, model replication, and exploiting traditional software flaws to deceive, manipulate, compromise, and render AI systems ineffective." Only "three of 28 organizations" with AI capabilities have the ability to make their systems secure from outside theft or hacking (Intellectual Property and Computer law Journal, 2021).

The fifth AI-related threat from the NSCAI's Final Report is "AI-Enabled Biotechnology." The assumption is that biology "is now programmable," referencing technology like the gene editing tool and the ability to make massive innovations in biotechnology. According to the report U.S. competitors such as China and Russia are comparatively likely to take more "risk-tolerant actions and conform less rigidly to bioethical norms and standards" (NSCAI report, 2021).

The sixth factor the NSCAI addresses is that the U.S.'s "lack of explicit legal protections for data or express policies on data ownership" may actually lead to the hindering of innovation and collaboration as technologies evolve. The argument behind this is that the absence of any explicit data protection de-incentivizes companies or similar parties form making investments to develop data sets that are critical for the U.S.'s development in areas such as "machine learning and AI systems." The overall risk of an emerging market, coupled with limited amounts of protection for input, makes companies less likely to engage within this new market.

Addressing these threats requires significant development in the national intellectual property policy. The Commission recommended that the U.S. President issue an Executive order to recognize intellectual property as a national priority and require the development of a comprehensive plan to reform and create new intellectual policies designed to address the threat of AI and similar technologies and the U.S.'s current inept policies.

The first comment that can be made is that these extensive discussions in the USA are probably of relevance to every nation state which is serious about addressing IP related security risks. Digital developments are global and equally affect all countries. Secondly, it can be noted that the broad IP protection against misuse of AI extends not only to patents and trade secrets, which used to be the primary area of concerns for IP infringement. Much of the software is nowadays protected through copyright and related rights which should broaden the focus of attention to various forms of IP protection. Thirdly, the issues of data protection have come to the forefront of discussions on adequate forms of IP protection. While data protection is more advanced in the EU many regions are considering improvements in this field. It can be noted that data protection becomes relevant in particular regarding the training data sets for AI, which can be controlled much easier than the Machine learning process itself.

Assessing the level of security risk posed by intellectual property-related challenges

Existing research on the role of intellectual potential in the system of economic security of the state indicates that the quality development and rational use of the intellectual potential determines its impact on the level of economic security of the state. Yet, even though there are clear threats to IP security which result into national security challenges there is no single model which allows for a proper assessment of the risk level.

To the extent to which IP challenges and threats are systemic, a proper risk assessment model needs to be built on a systemic and coherent approach. It suggests considering the IP and economic security environment, infrastructure, operational modalities, regulatory issues and practice. The category "intellectual potential" here is used to describe the role of intellectual inputs as main drivers of productivity. Of particular interest is the role of this intellectual potential in the economic security of the state. The category "intellectual security" is used to describe the level of security of the IP system *vis a vis* various threats and challenges.

The analysis of intellectual security within the concept of economic development is present in the work of certain scholars (Vinogradova, Sizikova, Rybakova 2019). In this body of literature, the intellectual capital is narrowly interpreted to comprise of human capital in relation to innovation, but it leaves

out the role of intellectual property as a market framework and driver for technological progress. These approaches are also country specific and overemphasize the relevance of selected factors (as cyber security, brain drain, etc.).

A second group of approaches focus on the level of intellectual security and its relationship to life satisfaction (Almahaireh , Alzaben , Aladwan & Aljahani 2021). They are built on correlation analysis and ultimately underestimate the role of the IP system for incentivizing intellectual and technological development and strengthening the economic security.

A much more developed approach to defining a risk assessment model is contained in the work of the Ukrainian scientists Bryhinets, Shapoval and Bakhaieva (2021). In their research they suggest four levels of risk analysis:

The first level analyses the level of innovation of the country and its regions, the technology underpinning the economic structure, the importance of science-intensive products in GDP, the competitiveness of the economy; the intellectual potential of the nation – number of people employed in knowledge-intensive areas of economy, trends of migration of the intellectual capital. Effectively, this level analyzes the IP environment and the global economic context.

The second level focuses on the intellectual property market itself, the major players and intellectual outputs, incl. their legal security.

The third level focuses on the management environment of the intellectual property market, in particular the participation of the state in the protection and promotion of intellectual activity.

The fourth level analyzes the commercialization of intellectual property items and the impact of this process on the level of innovation development of the country.

These four levels of analysis provide the basis for calculating an integrated index of the intellectual security of the country, focused on factor analysis. The analysed risks are diverse in nature, sources and forms of manifestation – they cover regulatory, institutional, organizational and managerial, economic, subjective, social and global factors which have a stimulating or destabilizing effect on the state of intellectual security of the state. The objective of this model is to support a more efficient use of the intellectual potential taking into account the intellectual security threats in the economic security of the state.

The proposed intellectual security index builds on a wide range of international indices, including the Global Innovation Index, the Global Competitiveness Index, the Global Index of Intellectual Property Protection and others which allows determining the level of innovation development of a country on a global scale. The index offers the results of an empirical study considering positive and negative factors and identifying potential threats. Calculations are based on eight main indicators that determine the integrated intellectual security index of of Ukraine. They are presented in the following table:

Table 1. Ukraine in the Global Index of Intellectual Property Protection ranking

No.	Intellectual security objects	Indicators of intellectual security of Ukraine	Character of influence on security level
1.	Intellectual goods (services)	Volume of output (production) of goods and services in professional, scientific, technical activities and education, % of GDP	Stimulant
2.	Intellectual investments	Share of investments in intangible assets in total capital investments, %	Stimulant
3.	Intelligence bearer	Number of highly qualified specialists per 100 thousand people	Stimulant
4.		Number of highly qualified specialists who left for permanent residence abroad per 100 thousand people	Disincentive
5.	Intellectual institutes	Number of higher education institutions and research organizations per 100 thousand people	Stimulant
6.	Intellectual property items	Coefficient of patent activity (number of issued protection documents: patents for inventions, utility models, industrial designs, certificates for marks of goods and services in the name of national applicants per 10 thousand people)	Stimulant
7.		Number of crimes committed in the field of intellectual property per 100 thousand people	Disincentive
8.	Intellectual potential	Integrated intellectual potential index	Stimulant

Source: Bryhinets, Shapoval and Bakhaieva, 2021, p. 478

The influence of each indicator is determined through its direct (stimulant) or inverse (disincentive) influence on the value of the integrated index. The calculated weighing coefficient and values of the integrated intellectual security index provide the overall index results.

The work of the Ukrainian scientists is quite interesting. Through the 4 levels of analysis they capture various trends which provide the basis of policy recommendations for addressing the major threats and improving the index of the intellectual security of the country. It has to be noted that the recommendations are mainly targeting state institutions and the legal system, but their operational value for practical improvements in the market-based operations are not fully developed. The index strongly relies on data from other sources (international governmental and mostly non-governmental organizations) for which no verification can be obtained. Finally, the proposed index carries a strong imprint of the national context with the specific tasks of a transition economy and society. Nonetheless, it is a serious step into operationalizing the concept of IP security and its role for national economic security.

Conclusion

Intellectual property is of key relevance for ensuring he economic security of nations. It protects their most valuable assets and secures a competitive edge in the global competition. Protecting digital assets is paramount for individuals, organizations, and governments. Intellectual property theft is a pressing concern in the digital landscape, with far-reaching consequences for businesses, innovation, and

economic growth. To safeguard digital assets effectively, a multi-faceted approach is necessary, including robust cyber security measures, legal frameworks that adapt to the digital age, public awareness campaigns, and international cooperation. By taking these steps, countries can protect its valuable intellectual property and foster a climate of innovation and creativity in the digital era.

There is growing evidence that governments increasingly understand the strategic importance of IP and its protection and are taking active measures to put in place adequate mechanisms for minimizing the risk of IP theft. Various policies and practices are being developed in this regard.

The search for more comprehensive solutions to IP security requires a new approach to AI as a mechanism for protection, but also as a potential threat. Data volumes continue to grow at what will eventually be an unmanageable rate. Because of this, AI and ML will increasingly be used to identify real-time trends, automate compliance processes, and predict risks. Continuous, automated monitoring of compliance posture using AI can drastically reduce manual efforts and errors. More granular, sophisticated risk assessments will be available via ML algorithms, which can process vast amounts of data to identify subtle risk patterns, offering a more predictive approach to reducing risk and financial losses.

There is a need to develop a robust and dynamic model for proper assessment of the level of IP related risk. A systemic index has many advantages and woul require international cooperation. The value of such work will be of utmost importance to each country which is serious about protecting IP to improve national economic security.

REFERENCES

ALMAHAIREH, A.; ALZABEN, M.; ALADWAN, F. & ALJAHANI, M., 2021. The Level of Intellectual Security and its Relationship with Life Satisfaction among Mutah University Students. *Journal of Social Studies Education Research*, vol. 12, no. 3, pp. 28 – 46. https://files.eric.ed.gov/fulltext/EJ1318811.pdf.

BRYHINETS, O.; SHAPOVAL, R.; BAKHAIEVA, A., 2021. Problems of intellectual property in the national security system of the country, *Entrepreneurship and Sustainability Issues*, Vol. 8, no. 3, pp. 471 – 486. DOI: 10.9770/jesi.2021.8.3(30).

FARLEY, R.; WAR, R., 2019. Intellectual Property Rights & National Security, U.S. Army War College (Feb. 5th), https://perma.cc/KMH2-K94R.

GANTCHEV, D., 2022. Intellectual property and competitiveness – a macroeconomic analysis perspective. *Intellectual Property and Business*, no. 2, p. 82 – 106. ISSN: 2815-3464, Institute of Intellectual Property and Technology Transfer, „Publishing house ZIP“ Ltd.

HALBERT, D., 2016. Intellectual property theft and national security: Agendas and assumptions, *The Information Society*, vol. 32, no. 4, pp. 256 – 268. DOI:10.1080/01972243.2016.1177762.

IANCU A. & KAPPOS D., 2021. U.S. Intellectual Property is Critical to National Security (July 12). https://perma.cc/DG4H-S48L.

MATANOVAC VUČKOVIĆ, R.; ERNST, H.; GLIHA, I., 2020. Security Rights in Intellectual Property in Croatia. In: KIENINGER, E. (Ed.) *Security Rights in Intellectual Property. Ius Comparatum – Global Studies in Comparative Law*, vol 45. Springer, Cham. https://doi.org/10.1007/978-3-030-44191-3_8.

MORRISON, J., 2021. Intellectual Property & National Security, 6 U. Cin. Intell. Prop. & Computer L.J., p.3. Available at: https://scholarship.law.uc.edu/ipclj/vol6/iss1/8 .

NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE. 2021. Final report [1] [207] 4 H.R. 5515, 115th Cong. §1051(b)(1).

STOYANOVA, P., 2022. Digitization, Digital Transformation and Intellectual Property. *Fourth National Scientific Forum The Business in 21st Century on the topic: "Recovery and sustainability after the crisis". Conference proceedings* URL: https://www.ceeol.com/search/chapter-detail?id=1109942.

STRIZHLEV, H., 2019. New business models for radio industry product distribution through digital technologies. *Journal of Economic and Social Alternatives*, vol. 1, pp. 32 – 39, ISSN 1314 – 6556.

VINOGRADOVA, M.; SIZIKOVA, V.; RIBAKOVA, A., 2019. Intellectual Security as the Leading Factor of Economic Development in Advances in Social Science. *Education and Humanities Research*, vol. 386, 5th International Conference on Social, Economic, and Academic Leadership (ICSEALV 2019) https://www.researchgate.net/publication/338849206_Intellectual_Security_as_the_Leading_Factor_of_Economic_Development/fulltext/5e2f8484a6fdcc309695a36e/Intellectual-Security-as-the-Leading-Factor-of-Economic-Development.pdf.

OECD, For Good Measure**,** *Advancing Research on Well-being Metrics Beyond GDP, https://doi.org/10.1787/9789264307278-en.*

WORLD INTELLECTUAL PROPERTY ORGANIZATION (WIPO), Global IP filing activity 2022 at https://www.wipo.int/en/ipfactsandfigures/patents.

WORLD INTELLECTUAL PROPERTY ORGANIZATION (WIPO), 2020. Guidelines on Developing National IP Strategies, 2020. https://www.wipo.int/ipstrategies/en/.

WORLD BANK, 2002. Global Economic Prospects. https://documents1.worldbank.org/curated/en/285571468337817024/310436360_20050012013328/additional/Global-economic-prospects-and-the-developing-countries-2002-making-trade-work-for-the-worlds-poor.pdf.

Websites

Economic security: A need for a renewed global effort, Chattamnhouse
https://www.chathamhouse.org/2022/03/economic-security-need-renewed-global-effort
https://www.wipo.int/wipolex/en/treaties/
IT governance, https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023#top-data-breach-stats
The National Cyber Security Centre, UK Government, https://www.ncsc.gov.uk/
https://ecipe.org/publications/iprs-in-eu-ftas/
https://www.everycrsreport.com/reports/RL33205.html
Saudi Arabia Intellectual Property office, https://www.saip.gov.sa/en/national-strategy/
Technopolis group https://www.technopolis-group.com/the-current-wave-of-national-ip-strategies/
https://ised-isde.canada.ca/site/intellectual-property-strategy/en
https://projects.research-and-innovation.ec.europa.eu/en/research-area/industrial-research-and-innovation/eu-valorisation-policy/knowledge-valorisation-platform/repository/national-intellectual-property-rights-strategy-finland

✉ **Dr. Dimiter Gantchev, Assist. Prof.**
Intellectual Property and Technological Transfer Department
Business Faculty
University of National and World Economy
Studentski district
19, December 8th St.
1700 Sofia, Bulgaria
E-mail: dimitar.ganchev@unwe.bg