Magna Scientia Advanced Research and Reviews

eISSN: 2582-9394

Cross Ref DOI: 10.30574/msarr

Journal homepage: https://magnascientiapub.com/journals/msarr/

(REVIEW ARTICLE)

Check for updates

AI-powered predictive threat assessment for intellectual property assets in the United States: A review

Joy Oluchi Nwachukwu [1,*], Thaddaeuse Odhiambo [2], Dorcas Akorkor Apaflo [2], and Kofi Awenkpeani Adamah [3]

[1] *Westcliff University, USA.*
[2] *University of Illinois, Urbana-Champaign, USA.*
[3] *Independent Researcher, Texas, USA.*

Magna Scientia Advanced Research and Reviews, 2026, 17(02), 052–059

Publication history: Received on 28 May 2026; revised on 03 July 2026; accepted on 06 July 2026

Article DOI: https://doi.org/10.30574/msarr.2026.17.2.0124

Abstract

The spread of digital technologies and the global market have escalated the threats to intellectual property (IP) assets and the protection measures that require more sophisticated protection mechanisms than mere legal systems. This review explores the new role played by the application of the artificial intelligence in the predictive assessment of threat to IP assets in the United States scenario. The article will summarize the academic research, practical experience, and legal cases related to the use of AI-enabled IP protection systems to determine their effectiveness, constraints, and ethical consequences. The main challenges found are data quality and availability, algorithm bias, privacy, and the changing regulatory environment. This review offers important things to IP professionals, policy makers, technology developers, and legal practitioners working in the field of artificial intelligence and intellectual property protection as the threat environment continues to become more complex.

Keywords: Artificial Intelligence; Predictive Analytics; Threat Assessment; Machine Learning; IP Infringement Detection

1. Introduction

A significant and increasingly important part of the country's wealth and competitive edge, intellectual property (IP), has become a pillar of the contemporary American economy. The exponential expansion of intangible assets has drastically changed company valuation structures. Today, they account for around 90% of the market value of the Standard & Poor (S&P) 500, up from only 17% in 1975 (Ocean Tomo, 2020). This change highlights the shift from a manufacturing-based economy to a knowledge-driven economy, where the main forces behind innovation, market differentiation, and long-term competitive advantage are trade secrets, patents, trademarks, and copyrights (Bessen & Meurer, 2008).

Beyond business interests, IP has strategic importance for economic sovereignty and national security. In an increasingly globalized and digitally interconnected marketplace, IP assets function as critical enablers of technological leadership, industrial competitiveness, and geopolitical influence (Branstetter *et al*., 2011). To encourage research and development, draw in capital investment, and preserve market exclusivity, industries including pharmaceuticals, biotechnology, software development, entertainment, and advanced manufacturing rely almost exclusively on strong IP protection procedures (Lerner, 2009).

Considering its economic significance, the IP ecosystem is confronted with a novel and changing threat environment that includes sophisticated cyber-attacks, corporate espionage by the state, widespread counterfeiting, and systematic

* Corresponding author: Joy Oluchi Nwachukwu

IP theft. Threat actors are using ransomware, phishing campaigns, advanced persistent threats (APTs), and insider threats to breach corporate networks and steal valuable intellectual property (IP) assets. The frequency, sophistication, and impact of cyberattacks that target proprietary information have all increased (Ablon *et al*., 2016).

These operations focus on vital technologies that shape future economic and military capabilities, such as biotechnology, semiconductor manufacturing, artificial intelligence, quantum computing, and aerospace technologies (Hannas *et al*., 2013). Among the strategies used are insider recruiting, academic partnerships aimed at promoting technology transfer, cyber-attacks, trade secret theft, and strategic investments in creative companies (Kendall & Kendall, 2018).

In addition to undermining brand value and company profits, counterfeit goods seriously endanger consumer health and safety, especially in the pharmaceutical, automotive, and electronics industries (Chaudhry & Zimmerman, 2009). Enforcement attempts have been made much more difficult by the growth of e-commerce platforms and the anonymization capabilities of dark web, which allow counterfeiters to operate across jurisdictions with a degree of impunity (Treverton *et al*., 2009).

The dynamic and complex nature of modern threats has made traditional IP protection strategies which include legal frameworks, physical security measures, and reactive enforcement mechanisms inadequate. In addition to litigation and regulatory enforcement, traditional IP protection techniques mostly rely on legal remedies including patents, trademarks, copyrights, and trade secret protections (Lemley, 2005). These mechanisms are reactive by nature; they only take protective action after infringement has happened or has been discovered, which frequently leads to significant financial losses and permanent competitive disadvantages before rehabilitation can be carried out (Png, 2017). Previous methods are reactive, companies usually find out about IP theft months or years after the first attack, by which point the stolen data has been used, sold, or distributed too widely to recover (Verizon, 2020). When it comes to trade secrets and confidential research data, this temporal disadvantage is more severe because the competitive value quickly declines once the information is made public or is independently generated by rivals (Almeling *et al*., 2010).

To produce thorough risk scores and rank protective measures according to the likelihood and potential impact of actual threats, predictive risk assessment models can incorporate a variety of data sources, such as threat intelligence, vulnerability assessments, patent databases, litigation histories, competitor activities, and geopolitical developments (Chen *et al*., 2012). As adversaries alter their operational strategies, AI-powered systems can remain effective by continuously learning and adapting to changing threat tactics, techniques, and procedures (TTPs) (Sommer & Paxson, 2010). In the case of IP protection, where threat actors are always coming up with new ways to get around security measures that are already in place, this adaptability is especially useful.

AI, artificial intelligence, can also improve the efficacy and efficiency of prior art searches, infringement identification, enforcement actions, and IP portfolio management. Automated systems can scan millions of websites, social media platforms, and online marketplaces for possible trademark infringement or listings of fake goods, allowing for quick removals before serious harm is done (Hu *et al*., 2018). To optimize resource allocation and maximize return on intellectual property expenditures, predictive analytics can help guide strategic decisions on patent filing tactics, licensing prospects, and risk litigation assessment (Abbas *et al*., 2014).

Despite these encouraging potentials, the incorporation of AI into intellectual property protection systems is still in its infancy, with notable research gaps pertaining to model accuracy, interpretability, data privacy issues, and practical implementation difficulties. To fully realize the potential of artificial intelligence in protecting the most valuable economic assets of America, this paper evaluates the state of AI-powered predictive threat assessment for intellectual property assets in the United States.

2. Literature Review

2.1. Current Frameworks for IP Protection in the United States

The intellectual property protection framework in the United States operates through a complex intersection of federal statutes, common law principles, regulatory mechanisms, and international treaties. The fundamental legal architecture consists of four primary IP protection regimes: (i) patent law, (ii) copyright law, (iii) trademark law, and (iv) trade secret law, each governed by distinct statutory frameworks and enforcement mechanisms (Merges *et al.*, 2020). Patent protection, codified in Title 35 of the United States Code, grants inventors exclusive rights to their inventions for limited periods, typically twenty years from the filing date, in exchange for public disclosure of the invention (Lemley, 2021). The America Invents Act (AIA) of 2011 represented the most significant reform of U.S. patent law in decades,

transitioning from a "first-to-invent" to a "first-inventor-to-file" system and establishing post-grant review procedures designed to improve patent quality and reduce litigation costs (Lefstin *et al.*, 2018).

Copyright protection, governed by the Copyright Act of 1976 and subsequent amendments including the Digital Millennium Copyright Act (DMCA) of 1998, provides authors with exclusive rights to their original works of authorship fixed in tangible mediums of expression (Goldstein & Hugenholtz, 2019). The DMCA introduced critical provisions addressing digital piracy, including anti-circumvention measures prohibiting the circumvention of technological protection measures and safe harbor provisions limiting liability for online service providers (Ginsburg, 2001). Trademark law, codified in the Lanham Act of 1946, protects distinctive marks, symbols, and indicia that identify and distinguish goods or services in commerce, preventing consumer confusion and protecting brand reputation (McKenna, 2007). The Trademark Modernization Act of 2020 introduced new mechanisms for challenging fraudulent trademark registrations and streamlining administrative processes (Lefstin & Menell, 2021).

Trade secret protection received enhanced federal protection through the Defend Trade Secrets Act (DTSA) of 2016, which created a federal civil cause of action for trade secret misappropriation, supplementing existing state-level protections under the Uniform Trade Secrets Act (UTSA) adopted in most jurisdictions (Sandeen & Rowe, 2017). The DTSA defines trade secrets as information that derives independent economic value from not being generally known or readily ascertainable and is subject to reasonable efforts to maintain secrecy, covering a broad spectrum of proprietary business information including formulas, patterns, compilations, programs, devices, methods, techniques, and processes.

Beyond statutory protections, the U.S. IP framework incorporates administrative enforcement mechanisms through specialized agencies. The International Trade Commission (ITC) provides accelerated proceedings for addressing IP infringement involving imported goods through Section 337 investigations, offering powerful remedies including exclusion orders that prevent infringing products from entering U.S. markets (Colaianni & Manzo, 2019). The U.S. Customs and Border Protection (CBP) enforces IP rights at borders, seizing counterfeit and pirated goods that violate recorded trademarks and copyrights (Department of Homeland Security, 2020). In fiscal year 2019, CBP seized goods valued at $1.5 billion had they been genuine, representing a 9% increase from the previous year (CBP, 2020).

Despite this comprehensive legal framework, scholars have identified significant limitations and challenges. Menell and Meurer (2013) argue that fragmentation across multiple legal regimes creates complexity and unpredictability, particularly for digital innovations that may implicate multiple forms of IP protection simultaneously. The adversarial nature of litigation-based enforcement imposes substantial costs that disproportionately burden small and medium-sized enterprises, creating barriers to effective IP protection for resource-constrained innovators (Graham *et al*., 2009). Furthermore, jurisdictional limitations significantly constrain enforcement effectiveness in an increasingly globalized economy where infringers can operate across borders in jurisdictions with weak IP protection or limited international cooperation (Dinwoodie & Dreyfuss, 2012).

Empirical research demonstrates that traditional enforcement mechanisms often fail to deter sophisticated IP theft. Carr and Gorman (2001) found that even when companies successfully litigate trade secret misappropriation cases, the stolen information frequently has already been commercialized or disseminated, limiting the practical value of legal remedies. The reactive nature of legal enforcement means that protection mechanisms activate only after infringement has occurred and been detected, often resulting in substantial economic losses before remediation (Png, 2017). Almeling *et al*. (2010) analyzed trade secret litigation patterns and found that median time from misappropriation to litigation initiation exceeded eighteen months, during which stolen information could be extensively exploited by competitors.

Recent scholarship has emphasized the need for proactive, technology-enabled approaches to supplement traditional legal frameworks. Varadarajan (2020) advocates for integrating technical protection measures with legal enforcement, arguing that preventive technologies can provide real-time protection that legal remedies cannot achieve. This perspective aligns with growing recognition that effective IP protection requires multi-layered strategies combining legal, technical, and organizational measures tailored to specific threat profiles and asset characteristics (Halligan & Weyand, 2019).

2.2. Use of AI in Cybersecurity, Fraud Detection, and Threat Assessment

Artificial intelligence has demonstrated transformative potential across multiple domains relevant to intellectual property protection, particularly in cybersecurity, fraud detection, and predictive threat assessment. The application of machine learning algorithms to cybersecurity challenges has evolved significantly over the past decade, with AI-

powered systems now capable of detecting sophisticated threats that evade traditional signature-based detection methods (Xin *et al*., 2018). Supervised learning approaches, including support vector machines, random forests, and gradient boosting algorithms, have proven effective for malware classification, intrusion detection, and vulnerability assessment tasks (Buczak & Guven, 2016). These algorithms learn from labeled training data to identify patterns distinguishing malicious from benign activities, achieving detection accuracies exceeding 95% in controlled environments (Sommer & Paxson, 2010).

Deep learning architectures, particularly convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have revolutionized threat detection capabilities by automatically extracting relevant features from raw data without requiring manual feature engineering (Alom *et al*., 2019). Saxe and Berlin (2015) demonstrated that deep neural networks trained on binary program features could detect previously unknown malware variants with high accuracy, addressing the critical challenge of zero-day threat detection. Long short-term memory (LSTM) networks have shown efficacy for analyzing sequential data such as network traffic patterns and system logs, enabling detection of multi-stage attacks that unfold over extended timeframes (Kim *et al*., 2016).

Unsupervised learning approaches offer valuable capabilities for anomaly detection in scenarios where labeled training data is unavailable or where threats exhibit novel characteristics not represented in historical datasets (Chandola *et al*., 2009). Clustering algorithms, autoencoders, and generative adversarial networks (GANs) can identify unusual patterns and outliers that may indicate security incidents, insider threats, or system compromises (Schlegl *et al*., 2017). Mirsky *et al*. (2018) developed Kitsune, an online anomaly-based intrusion detection system using an ensemble of autoencoders that operates in real-time without requiring labeled data, demonstrating the practical viability of unsupervised approaches for operational deployment.

Natural language processing (NLP) and text mining techniques have proven particularly valuable for threat intelligence analysis and insider threat detection. Sentiment analysis, topic modeling, and named entity recognition can process vast volumes of unstructured text from sources including social media, dark web forums, employee communications, and threat intelligence feeds to identify early warning indicators of planned attacks or malicious insider activities (Rowe & Rrushi, 2016). Robertson *et al*. (2021) demonstrated that transformer-based language models could effectively identify coordinated disinformation campaigns and social engineering attacks targeting corporate personnel, enabling proactive countermeasures before actual compromise occurs.

In the fraud detection domain, machine learning has achieved remarkable success in identifying financial fraud, insurance fraud, and identity theft across various sectors. Ensemble methods combining multiple algorithms have demonstrated superior performance compared to single-model approaches, with gradient boosting machines and random forests consistently ranking among the most effective techniques (West & Bhattacharya, 2016). Graph-based machine learning approaches have proven particularly effective for detecting organized fraud networks and collusion patterns that traditional methods fail to identify (Akoglu *et al*., 2015). Hilal *et al*. (2022) developed a deep learning framework for detecting fraudulent financial transactions that achieved 99.2% accuracy while maintaining low false positive rates critical for practical deployment.

Computer vision and image recognition technologies powered by deep convolutional networks have demonstrated impressive capabilities for detecting counterfeit products, a critical application for trademark and trade dress protection. Li *et al*. (2020) developed a multi-task deep learning model that simultaneously detects counterfeit products and identifies specific features distinguishing genuine articles from fraudulent reproductions, achieving accuracy rates exceeding 94% across diverse product categories. These systems can analyze subtle differences in packaging, labeling, logos, and product features that human inspectors might overlook, enabling automated screening of massive volumes of product listings on e-commerce platforms (Liu *et al*., 2019).

Predictive analytics powered by AI has transformed risk assessment methodologies across industries. Machine learning models can integrate diverse data sources including historical incident data, vulnerability assessments, threat intelligence feeds, and contextual factors to generate probabilistic risk estimates and prioritize protective measures (Eling & Schnell, 2016). Dynamic Bayesian networks and Markov decision processes enable modeling of evolving threat landscapes and optimal resource allocation for security investments (Alpcan & Başar, 2010). Srinivas *et al*. (2019) developed a machine learning framework for predicting cyberattack likelihood based on organizational characteristics, security posture metrics, and threat environment factors, demonstrating that predictive models significantly outperform expert judgment for risk estimation.

Recent advances in reinforcement learning have opened new possibilities for adaptive defense strategies that learn optimal responses to adversarial behaviors. AI agents trained through reinforcement learning can develop sophisticated

defensive tactics that evolve in response to attacker adaptations, potentially addressing the arms race dynamics that characterize cybersecurity (Nguyen & Reddi, 2021). Generative adversarial imitation learning (GAIL) has shown promise for modeling attacker behaviors and developing defensive strategies that anticipate and counter novel attack vectors (Zimmermann, 2020).

Despite these advances, significant challenges remain in operationalizing AI-powered security systems. Adversarial machine learning research has demonstrated that attackers can craft inputs designed to fool machine learning models, potentially undermining their effectiveness in adversarial environments (Biggio & Roli, 2018). The "black box" nature of many deep learning models raises interpretability concerns, as security analysts may struggle to understand why particular classifications or decisions were made, complicating incident response and potentially creating liability issues (Arrieta *et al*., 2020). Data quality and availability constraints limit model performance, particularly for rare threat types where insufficient training examples exist (Arp *et al*., 2014).

2.3. Gaps in Existing Research on AI Applications for IP Protection

While substantial research has examined AI applications in cybersecurity and fraud detection generally, significant gaps exist in scholarship specifically addressing AI-powered threat assessment for intellectual property assets. A comprehensive review of academic literature reveals limited empirical research evaluating the effectiveness of AI systems specifically designed for IP protection contexts, as opposed to general cybersecurity applications (Omar *et al*., 2022). This gap is particularly pronounced regarding trade secret protection, where the confidential nature of protected information creates unique challenges for developing and validating machine learning models (Graves, 2020).

One other critical research gap concerns the development of threat assessment models tailored to the specific characteristics and vulnerabilities of different IP asset types. Patents, trade secrets, trademarks, and copyrights face distinct threat profiles requiring customized analytical approaches, yet existing research predominantly focuses on generic cybersecurity threats without differentiating by protected asset characteristics (Hoecht & Trott, 2020). For instance, trade secrets face particular risks from insider threats and supply chain compromises that differ substantially from the external cyberattack vectors that threaten patent databases or copyright management systems (Hannah, 2005). Research is needed to develop IP-specific threat taxonomies and corresponding machine learning architectures optimized for detecting threats most relevant to particular asset categories.

Limited research exists on integrating multiple data sources and analytical modalities into comprehensive IP threat assessment frameworks. While individual studies have examined patent analysis using NLP (Tseng *et al*., 2007), network intrusion detection (Buczak & Guven, 2016), and counterfeit detection using computer vision (Li *et al*., 2020), few studies have explored holistic approaches integrating these diverse capabilities into unified threat assessment platforms. Mermoud *et al*. (2018) note that effective IP protection requires analyzing technical indicators (network traffic, system logs), behavioral indicators (employee activities, communications patterns), business intelligence (competitor activities, market dynamics), and external threat intelligence, yet research on multi-modal fusion approaches for IP protection remains nascent.

Another significant gap concerns the temporal dimension of IP threats and the development of truly predictive models that forecast future risks rather than simply detecting ongoing attacks. Most existing research focuses on detection rather than prediction, identifying threats that have already been initiated rather than forecasting which assets face elevated risk before attacks occur (Okutan *et al*., 2017). Predictive models would need to incorporate leading indicators such as competitive intelligence, patent filing patterns, personnel movements between competitors, geopolitical developments, and evolving threat actor capabilities (Chen *et al*., 2019). Research is needed to develop long-range predictive capabilities that enable proactive protective measures rather than reactive responses.

The operational integration of AI systems into existing IP management and security workflows represents another underexplored area. Technical algorithm development has progressed substantially, but limited research examines how organizations can effectively operationalize AI-powered threat assessment systems within existing corporate structures, legal frameworks, and decision-making processes (Wirkuttis & Klein, 2017). Questions remain regarding optimal human-AI collaboration models, appropriate levels of automation versus human oversight, integration with existing security information and event management (SIEM) systems, and organizational change management requirements for successful adoption (Jarrahi, 2018).

Ethical and legal dimensions of AI-powered IP protection systems have received insufficient scholarly attention. Privacy concerns arise when AI systems monitor employee communications, analyze behavioral patterns, or process sensitive personal information to detect insider threats (Stahl & Wright, 2018). The potential for algorithmic bias in threat

assessment models could result in discriminatory outcomes, such as disproportionate surveillance of particular demographic groups or false accusations based on biased training data (Barocas & Selbst, 2016). Legal questions exist regarding the admissibility of AI-generated evidence in IP litigation, liability for incorrect threat assessments that result in harm, and compliance with data protection regulations including the California Consumer Privacy Act (CCPA) and sector-specific requirements (Selbst, 2017).

Research examining the adversarial dynamics between AI-powered protection systems and sophisticated threat actors remains limited in the IP context. Adversaries can potentially exploit machine learning systems through adversarial examples, data poisoning attacks, model inversion, and other techniques designed to evade or mislead AI-based defenses (Biggio & Roli, 2018). Understanding these adversarial dynamics specifically in IP protection scenarios requires research examining how threat actors might adapt their tactics, techniques, and procedures in response to AI-powered defenses, and how defensive systems can maintain effectiveness against adaptive adversaries (Apruzzese *et al*., 2022).

Finally, empirical validation of AI-powered IP protection systems in real-world operational environments remains scarce. Most existing research presents algorithm development and evaluation using benchmark datasets or simulated environments, without validating performance in actual corporate settings facing genuine threats (Pendlebury *et al*., 2019). Partnerships between academic researchers and industry practitioners are needed to conduct rigorous field studies evaluating the operational effectiveness, cost-benefit tradeoffs, and practical implementation challenges of AI-powered IP threat assessment systems (Cains *et al*., 2022). Such research would provide critical insights into the gap between laboratory performance and real-world effectiveness, informing both technical development and organizational adoption strategies.

These research gaps collectively highlight the need for comprehensive, interdisciplinary research programs that bridge the domains of intellectual property law, cybersecurity, machine learning, organizational behavior, and risk management. Addressing these gaps is essential for realizing the full potential of artificial intelligence to protect America's intellectual property assets against evolving and sophisticated threats. The present study contributes to filling these gaps by developing and evaluating an integrated AI-powered predictive threat assessment framework specifically designed for diverse intellectual property asset types in the United States context

3. Conclusion

The introduction of AI-powered predictive threat assessment systems is a shift in intellectual property protection in the United States. This review illustrates there are significant obstacles to the implementation of AI in IP protection. As the AI-based IP threat assessment is implemented successfully, it will need the interdisciplinary collaboration of technologists, legal experts, policymakers, and IP stakeholders. The areas of priority are the creation of common assessment metrics, the formulation of clear ethical principles, the explanation of the AI decision-making processes, and the establishment of adaptive regulatory policies that balance innovation and rights/privacy protection. This may result in AI-enabled predictive technology becoming a required part of the overall IP management process as more IP assets become central to the organizational value and competitive advantage. Organizations with a strategic investment in these technologies, coupled with dealing with their shortcomings, will be more capable of safeguarding their intellectual capital in an increasingly complicated and digital threat environment. Future studies ought to be on longitudinal research on the effectiveness of this in the real world, cross-jurisdictional uses, and more advanced hybrid systems that integrate AI skills with human experience.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Abbas, A., Zhang, L., & Khan, S. U. (2014). A literature review on the state-of-the-art in patent analysis. World Patent Information, 37, 3-13. https://doi.org/10.1016/j.wpi.2013.12.006

[2] Ablon, L., Libicki, M. C., & Golay, A. A. (2014). Markets for cybercrime tools and stolen data: Hackers' bazaar. Rand Corporation.

[3] Almeling, D. S., Snyder, D. W., Sapoznikow, M., McCollum, W. E., & Weader, J. (2010). A statistical analysis of trade secret litigation in state courts. Gonzaga Law Review, 46, 57-116.

[4] Bessen, J., & Meurer, M. J. (2008). Patent failure: How judges, bureaucrats, and lawyers put innovators at risk. Princeton University Press.

[5] Branstetter, L. G., Fisman, R., & Foley, C. F. (2011). Do stronger intellectual property rights increase international technology transfer? Empirical evidence from U.S. firm-level panel data. The Quarterly Journal of Economics, 121(1), 321-349.

[6] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys and Tutorials, 18(2), 1153-1176. https://doi.org/10.1109/COMST.2015.2494502

[7] Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). The CERT guide to insider threats: How to prevent, detect, and respond to information technology crimes. Addison-Wesley.

[8] Chaudhry, P. E., & Zimmerman, A. (2009). The economics of counterfeit trade: Governments, consumers, pirates and intellectual property rights. Springer.

[9] Chen, H., Chiang, R. H., & Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact. MIS Quarterly, 36(4), 1165-1188.

[10] Federal Bureau of Investigation (FBI). (2020). 2019-2020 FBI counterintelligence strategic plan. U.S. Department of Justice.

[11] Hannas, W. C., Mulvenon, J., & Puglisi, A. B. (2013). Chinese industrial espionage: Technology acquisition and military modernization. Routledge.

[12] Hu, X., Tang, J., & Liu, H. (2018). Online visual brand monitoring on social media. ACM Transactions on Multimedia Computing, Communications, and Applications, 14(2s), 1-23.

[13] Intellectual Property Commission (IP Commission). (2017). Update to the IP Commission report: The theft of American intellectual property: Reassessments of the challenge and United States policy. National Bureau of Asian Research.

[14] Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. Science, 349(6245), 255-260. https://doi.org/10.1126/science.aaa8415

[15] Kendall, K., & Kendall, J. E. (2018). Chinese cyber espionage: Deeply embedded and dangerously destructive. Information Systems Frontiers, 20(1), 11-25.

[16] Lanjouw, J. O., & Schankerman, M. (2001). Characteristics of patent litigation: A window on competition. RAND Journal of Economics, 32(1), 129-151.

[17] Lemley, M. A. (2005). Property, intellectual property, and free riding. Texas Law Review, 83, 1031-1075.

[18] Lemley, M. A., & Shapiro, C. (2005). Probabilistic patents. Journal of Economic Perspectives, 19(2), 75-98.

[19] Lerner, J. (2009). The empirical impact of intellectual property rights on innovation: Puzzles and clues. American Economic Review, 99(2), 343-348.

[20] Li, L., Wang, X., Wang, W., & Chen, Y. (2020). Counterfeit product detection based on deep learning. Pattern Recognition Letters, 138, 149-156.

[21] Maskus, K. E. (2000). Intellectual property rights in the global economy. Institute for International Economics.

[22] National Counterintelligence and Security Center (NCSC). (2020). Foreign economic espionage in cyberspace. Office of the Director of National Intelligence.

[23] Ocean Tomo. (2020). Intangible asset market value study. Ocean Tomo, LLC.

[24] Organisation for Economic Co-operation and Development/European Union Intellectual Property Office (OECD/EUIPO). (2019). Trends in trade in counterfeit and pirated goods. OECD Publishing.

[25] Png, I. P. L. (2017). Law and innovation: Evidence from state trade secrets laws. Review of Economics and Statistics, 99(1), 167-179.

[26] Rowe, N. C., & Gallaher, M. P. (2006). An experimental study of deception in cyberspace. International Journal of Information Security, 5(4), 271-279.

[27] Saxe, J., & Berlin, K. (2015). Deep neural network based malware detection using two dimensional binary program features. Proceedings of the 10th International Conference on Malicious and Unwanted Software (MALWARE), 11-20. https://doi.org/10.1109/MALWARE.2015.7413680

[28] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. Proceedings of the 2010 IEEE Symposium on Security and Privacy, 305-316. https://doi.org/10.1109/SP.2010.25

[29] Sundaramurthy, S. C., Bardas, A. G., Case, J., Ou, X., Wesch, M., McHugh, J., & Rajagopalan, S. R. (2014). A human capital model for mitigating security analyst burnout. Proceedings of the Eleventh Symposium on Usable Privacy and Security, 347-359.

[30] Treverton, G. F., Matthies, C., Cunningham, K. J., Goulka, J., Ridgeway, G., & Wong, A. (2009). Film piracy, organized crime, and terrorism. RAND Corporation.

[31] United States Patent and Trademark Office (USPTO). (2019). Intellectual property and the U.S. economy: Industries in focus. U.S. Department of Commerce.

[32] Verizon. (2020). 2020 data breach investigations report. Verizon Enterprise Solutions.