

**Ministry of Science and Higher Education of the Republic of
Kazakhstan MAQSUT NARIKBAYEV UNIVERSITY**

BULAT ALISHER TEMIRLANOVICH

**Cybersquatting as a form of trademark infringement in Kazakhstan:
legal measures and international experience**

educational program 7M04210 – «Intellectual Property and Business
Law»

Master's project for the academic degree of Master of Law

Astana, 2025

MNU Research Archive

**Ministry of Science and Higher Education of the Republic of
Kazakhstan MAQSUT NARIKBAYEV UNIVERSITY**

«Admitted to the defence»
Program manager/coordinator

«__» _____ 20__y.

MASTER'S DISSERTATION (PROJECT)

**On the topic: “Cybersquatting as a form of trademark infringement
in Kazakhstan: legal measures and international experience”**

**according to the educational program 7M04210 – «Intellectual
Property and Business Law»**

Author

A.T.Bulat

Scientific supervisor



Abenova A.B.

Astana, 2025

MNU Research Archive

APPROVE
Program manager/coordinator

«__» _____ 20__y.

The calendar plan for the preparation of a master's dissertation (project)

Name of the project stages	Period	A note on the implementation of the project stages			
		Actual completion date	The degree of readiness of the completed stage of the project	Signature of the postgraduate (postgraduates)	Signature of the supervisor (supervisors)
Review of literature and practical materials	01.10.24 - 01.12.24	01.12.24	100%		
Methodology development	01.10.24 - 01.11.24	01.11.24	100%		
Data Collection And processing	01.12.25 - 01.01.25	01.01.25	100%		
Analysis and interpretation of the results obtained	01.01.25 - 01.02.25	01.02.25	100%		
Development of project recommendations	01.02.25 - 01.03.25	01.03.25	100%		
Preparation of the introduction and conclusion	01.01.25 - 01.03.25	01.05.25	100%		
Preparation of dissertations (project): Preparation of the	01.02.25 - 01.04.25	01.05.25	100%		

first section of the project					
Preparation of the II section of the project	01.02.25 - 01.04.25	01.05.25	100%		
Preparation of the III section of the project	01.04.25 - 01.05.25	10.05.25	100%		
Receiving feedback from the supervisor (scientific supervisors)	01.04.25 - 12.05.25	12.05.25	100%		
Preparation of a report, visual aids and presentations	01.05.25 - 22.05.25	22.05.25	100%		
Defense of the master's thesis (project)	27.05.25	27.05.25	100%		

Scientific supervisor of the Master's dissertation (project):

Abenova A.B., EAPO, Director, Industrial designs Divisions
(Full name, position and signature)



The plan was accepted for execution:

(Full name and signature of the postgraduate)

CONTENT

Introduction	7
SECTION 1. Theoretical and legal foundations of cybersquatting	9
1.1 Historical Development and Evolution of Cybersquatting	9
1.2 Definition, Forms and Classification of Cybersquatting	11
1.3 Cybersquatting as Trademark Infringement	13
1.4 Doctrinal Approaches to Cybersquatting Regulation	15
1.5 Kazakhstan's Legal Framework for Trademarks and Domain Names	16
SECTION 2. Cybersquatting issues: Kazakhstan and international practice	19
2.1 Scale and Specific Features of Cybersquatting in Kazakhstan	19
2.2 Judicial Practice on Cybersquatting in Kazakhstan (Court Cases and Examples)	21
2.3 International Regulatory Experience: Key Precedents (UDRP, WIPO, ACPA, etc.)	22
2.4 International Judicial Practice on Cybersquatting (Court Cases and Examples)	24
SECTION 3. Ways to improve the legal regulation of cybersquatting	27
3.1 In-Depth Analysis of International Mechanisms for Combating Cybersquatting (UDRP, ACPA, WIPO)	27
3.2 Opportunities for Integrating International Experience into Kazakhstan's Legislation	30
3.3 Directions for Improving National Legislation	33
3.4 Proposals for Enhancing the Protection of Trademarks and Domain Names in Kazakhstan	36
Conclusion	40
Bibliography	45

MNU Research Archive

Introduction

In today's digital economy, domain names have become just as important as trademarks. They help businesses build their identity and connect with consumers online. But with this shift has come a growing issue – cybersquatting. This is when someone registers a domain name using another company's trademark, often with bad intentions, like trying to sell it back to the rightful owner for profit or mislead users. It's a serious problem around the world and has started to affect Kazakhstan more in recent years.¹

In many countries, laws and dispute resolution systems have been created to deal with cybersquatting. For example, the United States has the Anti-Cybersquatting Consumer Protection Act (ACPA), and internationally there is the Uniform Domain-Name Dispute-Resolution Policy (UDRP) under ICANN.² These systems make it easier for trademark owners to get their domain names back. But in Kazakhstan, there are no specific laws that deal with cybersquatting directly. Instead, courts rely on general trademark and unfair competition rules.³

The aim of this dissertation is to explore how cybersquatting is treated under Kazakhstani law and to assess how effective the existing legal tools are in solving this issue. I will also compare Kazakhstan's approach with international systems like the UDRP and the ACPA to see what could be improved or adopted locally. The main objectives are:

- To examine Kazakhstan's legal framework and enforcement practices;
- To compare it with global standards and systems;
- To identify any legal or practical gaps;
- To propose recommendations for better protection of trademark owners.

¹ Chinara Gasimova, 'Domain Name and Trademark Infringement: Cybersquatting in the Digital Age' (2023)

https://www.researchgate.net/publication/368237606_Domain_name_and_trademark_infringement_Cybersquatting_in_the_digital_age

² Sanket Singh Sengar, 'Protecting Trademarks in the Digital Era: Addressing Cybersquatting and Domain Name Issues' (2024) SSRN https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4770126

³ EUIPO, 'Focus on Cybersquatting: Monitoring and Analysis Study – Executive Summary' (2021) https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Cybersquatting_Study/2021_Focus_on_Cybersquatting_Monitoring_and_Analysis_Study_ExSum_en.pdf

To carry out this research, I will use a doctrinal method to study Kazakhstani laws and cases related to trademark rights and domain disputes. I will also apply a comparative method, looking at how other countries address cybersquatting and what Kazakhstan can learn from them. Finally, I will use case analysis, looking at recent local disputes to understand how courts handle these cases in practice.

Many scholars and legal experts have studied cybersquatting in global and regional contexts. For example, Gasimova explains that cybersquatting can harm trademark owners by damaging their reputation and confusing customers, especially when users are redirected to fake or unrelated websites.⁴ Sengar adds that in countries like India, courts often have to rely on general legal concepts like passing off, since there is no clear law about domain names.⁵

In Europe, a report by the EUIPO shows that new domain extensions (like .store or .shop) have made cybersquatting easier and more common. It also points out that bad-faith registration is a key issue in most cases.⁶ In Kazakhstan, Nurmagambetov writes that although traditional trademark protection exists, there is no dedicated process for resolving domain disputes. Some practical solutions, like pre-trial domain blocking, have been introduced, but they are not always effective.⁷

Zhanadilov describes real cases from Kazakhstan where companies tried to cancel existing trademarks and take over their domain names. He points out that courts often have difficulty proving bad faith, especially when there is no clear legal definition.⁸ These examples show that Kazakhstan still lacks strong tools to deal with cybersquatting and that there is a clear need for reform.

This research is timely and relevant because cybersquatting is growing, yet Kazakhstan's legal response remains limited. This dissertation will fill an important gap in national legal studies and offer recommendations based on successful international practices.

⁴ Gasimova (n 1).

⁵ Sengar (n 2).

⁶ EUIPO (n 3).

⁷ Zhanat Nurmagambetov, 'Overview of Trademark Protection in the Countries of Central Asia' (2021) <https://bolotovip.com/publication/overview-of-trademark-protection-in-the-countries-of-central-asia/>

⁸ Bauyrzhan Zhanadilov, 'Trademark Squatting in Kazakhstan: From Russia with Love' (21 August 2024) Kluwer Trademark Blog <https://trademarkblog.kluweriplaw.com/2024/08/21/trademark-squatting-in-kazakhstan-from-russia-with-love/> and 'Part II' (2 October 2024) <https://trademarkblog.kluweriplaw.com/2024/10/02/trademark-squatting-in-kazakhstan-from-russia-with-love-part-ii/>

SECTION 1. Theoretical and legal foundations of cybersquatting

1.1 Historical Development and Evolution of Cybersquatting

Cybersquatting emerged as a byproduct of the early commercial internet in the 1990s, during which domain names were allocated on a first-come, first-served basis without regard to trademark ownership. This regulatory vacuum gave rise to a new type of opportunism where individuals, recognising the commercial value of trademarks, began registering popular or brand-related domain names with the intent to sell them to the rightful trademark holders for profit.⁹ Lipton explains that the lack of proactive legal frameworks allowed cybersquatters to engage in these practices relatively unchecked, forcing trademark owners to reactively pursue costly litigation or settlements.¹⁰

One of the landmark legal responses to cybersquatting was the Anticybersquatting Consumer Protection Act (ACPA), enacted in the United States in 1999. The ACPA created a statutory cause of action for trademark owners to recover domain names registered in bad faith and provided remedies such as statutory damages and injunctive relief.¹¹ Du and Liu highlight that the ACPA was among the first national legislative measures to recognise domain name disputes as a form of trademark infringement, fundamentally shifting the legal landscape.¹²

In parallel, the Uniform Domain Name Dispute Resolution Policy (UDRP) was developed by ICANN in 1999 to offer an alternative, non-judicial method for resolving disputes over domain names.¹³ As Helfer and Dinwoodie note, the UDRP marked a pioneering effort in non-national lawmaking, introducing a global framework that trademark owners could use to challenge domain registrations that were identical or confusingly similar to their marks and registered in bad faith.¹⁴ It allowed for a quick

⁹ Jacqueline D Lipton, 'Beyond Cybersquatting: Taking Domain Name Disputes Past Trademark Policy' (2005) 40 Wake Forest L Rev 1367.

¹⁰ *ibid.*

¹¹ Fangfang Du and Jing Liu, 'Does What Works for .Com Also Work for .Cn?: Comparative Study of Anti-Cybersquatting Legal Systems in the United States and China' (2002) 20 J Marshall J Computer & Info L 541.

¹² *ibid.*

¹³ Laurence R Helfer and Graeme B Dinwoodie, 'Designing Non-National Systems: The Case of the Uniform Domain Name Dispute Resolution Policy' (2001) 43(1) *William and Mary Law Review* 141 <https://scholarship.law.wm.edu/wmlr/vol43/iss1/7>

¹⁴ *ibid.*

and inexpensive method to reclaim domains, avoiding the complexity of multinational litigation.¹⁵

Following the success of the UDRP, other jurisdictions and institutions began developing similar mechanisms or adapting the UDRP model into national frameworks. Alrawashdedh points out that countries such as China, India, and those within the EU began either adopting the UDRP itself for their ccTLDs or establishing mirror processes with localised procedures.¹⁶ However, despite these advances, the enforcement of decisions across jurisdictions, especially against anonymous registrants using proxy services or located in uncooperative legal regimes, remains a persistent challenge.¹⁷

A 2021 EUIPO report indicates that cybersquatting continues to evolve, with new generic top-level domains (gTLDs) and internationalised domain names (IDNs) increasing the scope and volume of abuse.¹⁸ This includes domain registrations that exploit common typographical errors or regional language variations. Lipton observes that domain name abuse has progressed from classic cybersquatting to more nuanced forms, including *combosquatting* and *bitsquatting*, which rely on consumer error or technical exploitation.¹⁹

Furthermore, blockchain-based domain name systems (e.g., using .eth or .crypto extensions) have introduced another frontier of cybersquatting that is largely resistant to current enforcement tools like the UDRP, due to their decentralised, non-reversible nature.²⁰ Zubin cautions that such emerging platforms could create "safe havens" for cybersquatters unless legal innovation keeps pace with technological developments.²¹

These developments demonstrate that while initial responses like the ACPA and UDRP were instrumental in curbing early waves of

¹⁵ *ibid.*

¹⁶ Waddah Alrawashdedh, *Dispute Resolution Mechanisms and Trademark Cybersquatting* (PhD thesis, University of Szeged 2017) https://doktori.bibl.u-szeged.hu/id/eprint/4093/2/Waddah_Alrawashdedh_Thesis.pdf

¹⁷ *ibid.*

¹⁸ EUIPO, 'Focus on Cybersquatting: Monitoring and Analysis Study' (2021) https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Cybersquatting_Study/2021_Focus_on_Cybersquatting_Monitoring_and_Analysis_Study_ExSum_en.pdf

¹⁹ Lipton (n 9).

²⁰ Shriyaa Zubin, 'Regulation of Cybersquatting: An Analysis of the Legal Framework in India, the UK and the USA' (2023) *Journal of Legal Research and Studies* <https://lrrs.com/wp-content/uploads/2023/10/104.-Shriyaa-Zubin.pdf>

²¹ *ibid.*

cybersquatting, the phenomenon continues to mutate. Continuous reform, cross-border cooperation, and integration of new technologies into legal frameworks are now essential to address the full scope of cybersquatting threats.

1.2 Definition, Forms and Classification of Cybersquatting

Cybersquatting can be broadly defined as the bad-faith registration, use, or trafficking in a domain name that is identical or confusingly similar to a trademark, with the intent to profit from the goodwill associated with that mark.²² According to Sangeetha, cybersquatting undermines trademark integrity by diverting consumers, damaging reputation, or forcing mark owners to pay ransom-like amounts to retrieve digital identifiers.²³

The most recognised forms of cybersquatting include:

- ❖ **Classic Cybersquatting:** This occurs when a domain name matching an established trademark is registered by someone who has no legitimate interest in the name. The primary intent is resale to the mark owner at a profit.²⁴ The act is inherently exploitative and often targets high-profile global brands.
- ❖ **Typosquatting:** Involves registering domains that are misspellings or slight variants of popular websites (e.g. "goooogle.com" or "amazom.com").²⁵ Karote explains that typosquatting exploits human typing errors to redirect traffic and monetise through ads or phishing schemes.²⁶
- ❖ **Combosquatting:** Entails appending a trademark with additional words (e.g., "nike-sale.com") to create seemingly official-looking domains.²⁷ This form is often harder to detect and may evade basic domain filters.
- ❖ **Reverse Cybersquatting:** In contrast, this occurs when a trademark holder attempts to claim a legitimately registered domain

²² Sangeetha Laxmi V, 'The Menace of Cybersquatting and the Available Legal Measures to Mitigate Abuse of Domain Names' (2022) International Journal of Research in Law <https://ijrl.com/wp-content/uploads/2022/01/THE-MENACE-OF-CYBERSQUATTING-AND-THE-AVAILABLE-LEGAL-MEASURES-TO-MITIGATE-ABUSE-OF-DOMAIN-NAMES.pdf>

²³ *ibid.*

²⁴ Harsh Karote, 'Cybersquatting and Trademark Issues: Uniform Domain Resolution Policy' (2022) Journal of Legal Research and Studies <https://ljrs.com/wp-content/uploads/2022/02/9.-Harsh-Karote-1.pdf>

²⁵ *ibid.*

²⁶ *ibid.*

²⁷ *ibid.*

from someone who has lawful rights to it.²⁸ Curtin and Zubin both argue that such practices can chill legitimate domain usage and lead to overreach by large corporations.²⁹

- ❖ **Domain Kiting and Tasting:** Involves registering and deleting domain names repeatedly during the grace period to avoid paying fees, while still benefiting from temporary traffic.³⁰ Though now mostly curbed by ICANN policy changes, it was widely used in the mid-2000s to hold domains indefinitely.³¹
- ❖ **Blockchain-Based Cybersquatting:** As blockchain technology enters the domain space, squatters have begun to reserve brand names on platforms like ENS (.eth) or Unstoppable Domains (.crypto), where there is no central authority to resolve disputes.³² Alrawashdedh warns that these domains are immutable and pose new challenges to enforcement.³³

Each of these forms undermines the core functions of trademarks – namely source identification, brand association, and consumer trust.³⁴ As Bajpai and Jha stress, cybersquatting can lead to customer diversion, reputation harm, and competitive disadvantages for businesses.³⁵ The phenomenon also presents a systemic risk to e-commerce ecosystems, where domain names serve as key entry points for online identity.

Moreover, Zubin categorises cybersquatting behaviours based on the registrant's intent:³⁶

- ❖ **Speculative**, where domains are hoarded to be sold later
- ❖ **Malicious**, with aims to deceive or commit fraud
- ❖ **Defensive**, where a company pre-emptively registers variations of its own brand to avoid abuse³⁶

²⁸ Thomas J Curtin, 'The Name Game: Cybersquatting and Trademark Infringement on Social Media Websites' (2010) Brooklyn Journal of Law and Policy <https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1107&context=ilj>

²⁹ Zubin (n 20).

³⁰ Curtin (n 28).

³¹ *ibid.*

³² Alrawashdedh (n 16).

³³ *ibid.*

³⁴ Zubin (n 20).

³⁵ Bajpai Y and Jha AR, 'Pursuing Cybersquatting as a Trademark Infringement under the IP Regime' (2024) International Journal of Legal Science and Innovation <https://ijlsi.com/paper/pursuing-cybersquatting-as-a-trademark-infringement-under-the-ip-regime/>

³⁶ Zubin (n 20).

This typology helps clarify that not all domain conflicts stem from bad faith, and in some instances, disputes may involve concurrent legitimate interests.³⁷ For example, domain disputes involving common surnames or acronyms can complicate enforcement, especially where the domain holder uses it non-commercially or in good faith.

Thus, legal systems often evaluate cybersquatting claims not only by technical similarity but also by assessing the registrant's intent, history of similar registrations, and the use or non-use of the domain.³⁸ The UDRP's three-prong test – confusing similarity, lack of legitimate interest, and bad faith – is widely accepted as a balanced standard for adjudicating such cases.³⁹

1.3 Cybersquatting as Trademark Infringement

Cybersquatting, though initially a digital novelty, has become widely recognised as a form of trademark infringement under both national laws and international principles. This is because it interferes with the core functions of a trademark: source identification, brand protection, and consumer trust. As Zubin notes, courts increasingly interpret domain names as commercial signifiers whose misuse can trigger traditional trademark remedies.⁴⁰

Trademark law is designed to prevent consumer confusion and protect goodwill. When a cybersquatter registers a domain name resembling a trademark, consumers may mistakenly associate the site with the legitimate owner. This *initial interest confusion* can divert traffic, harm reputation, or even result in fraudulent transactions.⁴¹ Curtin explains that cybersquatting amounts to a hijacking of goodwill, especially when the domain is monetised through ads, counterfeit sales, or phishing attempts.⁴²

The UDRP framework, as applied by WIPO and national registrars, treats cybersquatting as a presumptive violation of trademark rights when three criteria are met: (1) the domain name is identical or confusingly similar to a trademark, (2) the registrant lacks rights or legitimate interests, and (3)

³⁷ *ibid.*

³⁸ Alrawashdedh (n 16).

³⁹ Helfer and Dinwoodie (n 13).

⁴⁰ Zubin (n 20).

⁴¹ *ibid.*

⁴² Curtin (n 28).

the domain was registered and is being used in bad faith.⁴³ These elements closely mirror trademark infringement doctrines, though they focus specifically on internet-based conduct.

Notably, even jurisdictions without specific anti-cybersquatting laws tend to treat such actions as trademark infringement under existing statutes. For example, Bajpai and Jha point out that Indian courts have repeatedly applied the Trade Marks Act to cybersquatting cases, reasoning that domain names serve a similar function to trademarks online.⁴⁴

Another key legal doctrine linked to cybersquatting is passing off, especially in common law countries. This tort protects business goodwill against misrepresentation. Cybersquatting often involves precisely that – registering a domain name in a way that misleads consumers into believing it is associated with the trademark owner. Alrawashdedh highlights that courts have accepted domain-based passing off claims when websites under disputed domains contain misleading content or imitate branding elements.⁴⁵

Trademark dilution is also relevant. Even if confusion is not evident, a domain that undermines the distinctiveness or reputation of a famous mark may still constitute infringement.⁴⁶ For instance, domains hosting unsavoury or unrelated content using a brand name can erode consumer trust. Sangeetha underlines that dilution-based claims are crucial where cybersquatters target trademarks to harm reputation rather than divert trade.⁴⁷

Despite growing consensus, enforcement can be inconsistent across jurisdictions. Challenges include varying definitions of bad faith, different burdens of proof, and the lack of harmonised remedies. Curtin warns that some legal systems remain hesitant to equate mere registration with actionable infringement unless there is demonstrable commercial misuse.⁴⁸

Ultimately, cybersquatting's legal treatment is converging toward a view that domain abuse, even in passive form, infringes on the economic and reputational interests protected by trademark law. This alignment has

⁴³ Helfer and Dinwoodie (n 13).

⁴⁴ Bajpai and Jha (n 35).

⁴⁵ Alrawashdedh (n 16).

⁴⁶ Curtin (n 28).

⁴⁷ Sangeetha Laxmi V (n 22).

⁴⁸ *ibid.*

helped shape global doctrine, particularly in jurisdictions influenced by UDRP and ACPA models.

1.4 Doctrinal Approaches to Cybersquatting Regulation

Doctrinal responses to cybersquatting vary significantly, reflecting differences in legal traditions, institutional frameworks, and enforcement capacities. Most approaches fall into three categories: adaptation of existing trademark laws, adoption of dedicated legislation, and reliance on alternative dispute resolution mechanisms.

(a) Adaptation of Traditional Trademark Law

Many countries initially addressed cybersquatting under general trademark or unfair competition laws. Pantov notes that European jurisdictions, including Germany and Hungary, used provisions related to confusing similarity, bad faith, and unfair commercial practices.⁴⁹ This approach, while flexible, often led to inconsistent rulings and confusion over whether mere domain registration constituted “use in commerce”.

Some courts expanded trademark doctrines to include the mere holding or offering for sale of infringing domain names. However, others demanded more concrete evidence of commercial activity. Lipton critiques this divergence, arguing that cybersquatting exposed limitations in doctrinal adaptability.⁵⁰

(b) Specialised Statutes: ACPA and Beyond

Countries such as the United States enacted bespoke legislation to directly target cybersquatting. The ACPA, passed in 1999, was designed to combat bad-faith registrations of domain names identical or similar to distinctive or famous marks. It introduced a set of factors for assessing bad faith and provided strong remedies, including statutory damages and domain transfer.⁵¹

Du and Liu contrast the ACPA with Chinese law, which initially lacked dedicated rules and relied on unfair competition doctrines.⁵² China later introduced judicial interpretations to clarify enforcement standards. While

⁴⁹ Vladimir Pantov, ‘The Prevention of Cybersquatting in Europe: Diverging Approaches and Prospects for Harmonization’ (2014) SSRN https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2427582

⁵⁰ Lipton (n 9).

⁵¹ Du and Liu (n 11).

⁵² *ibid.*

effective, these piecemeal updates lagged behind technological developments.⁵³

Despite its influence, the ACPA has limitations. Alrawashdedh observes that its jurisdictional scope is often constrained, making enforcement difficult against offshore registrants or anonymous domain holders.⁵⁴

(c) Arbitration and Policy Mechanisms

The most globally adopted model remains the UDRP, developed by ICANN and applied through WIPO. It allows for quick, low-cost resolution of disputes based on a uniform standard. Helfer and Dinwoodie praise the UDRP's flexibility and its ability to transcend national boundaries.⁵⁵

However, criticisms include inconsistency in panel decisions and limited remedies. Zubin cautions that UDRP procedures can sometimes favour trademark owners, raising concerns about due process for legitimate registrants.⁵⁶ Moreover, UDRP cannot compel monetary compensation or address more complex domain use disputes.

Some scholars suggest treating domain names as intangible property, thereby allowing courts to apply property law frameworks for enforcement. Lipton proposes that this would align domain regulation with the broader landscape of IP rights.⁵⁷ Alrawashdedh, however, argues that over-formalising domain name law may burden already strained legal systems.⁵⁸

Overall, doctrinal evolution continues to be shaped by technological change, market behaviour, and institutional design. No single approach has proven universally adequate, and hybrid systems remain the most common.

1.5 Kazakhstan's Legal Framework for Trademarks and Domain Names

Kazakhstan's approach to cybersquatting is still developing. The country's Law on Trademarks and Civil Code protect the exclusive rights of

⁵³ *ibid.*

⁵⁴ Alrawashdedh (n 16).

⁵⁵ Helfer and Dinwoodie (n 13).

⁵⁶ Zubin (n 20).

⁵⁷ Lipton (n 9).

⁵⁸ Alrawashdedh (n 16).

trademark owners, including against unauthorised use in domain names. However, the legal framework lacks a specific statute on cybersquatting.

Mukhammad explains that current enforcement relies on civil claims for trademark infringement or unfair competition.⁵⁹ This requires the plaintiff to show unauthorised use, confusing similarity, and potential harm. Courts have increasingly recognised that domain name misuse falls within this scope, especially where the domain resembles a protected trademark and is used in bad faith.⁶⁰

Sukhanov notes that amendments to Kazakh trademark law in 2019 clarified that trademark use in “digital media and the internet” may constitute infringement.⁶¹ This change implicitly brings domain names into the law’s scope, even if the domain is unused but registered in bad faith.

Kazakhstan’s country-code top-level domain (.kz) is managed by KazNIC, a non-profit registry. Registration is open but not subject to pre-screening for trademark conflicts.⁶² While KazNIC maintains policies to resolve disputes, its procedures are not binding arbitration and often defer to court rulings.⁶³

Unlike UDRP systems, KazNIC does not offer standardised mechanisms for rapid dispute resolution. If a domain name infringes on a trademark, the rights holder must usually file a civil case. According to Alrawashdedh, this creates delays and cost burdens, especially for small businesses.⁶⁴

Kazakhstan is a signatory to the Paris Convention and the TRIPS Agreement, which impose minimum standards for IP protection and enforcement.⁶⁵ This obliges the country to offer “effective legal remedies” against infringements, including cybersquatting.

Reform proposals include adopting a UDRP-style dispute resolution mechanism under KazNIC or a specialised IP tribunal.⁶⁶ Lipton supports such systems as models of transnational efficiency.⁶⁷ Additionally, legal

⁵⁹ Akmal Mukhammad, ‘Trademark Protection and Cybersquatting Issues’ (2019) Lexology <https://www.lexology.com/library/detail.aspx?q=61040c99-6f5c-4b70-b396-26a402df5966>

⁶⁰ *ibid.*

⁶¹ A.V. Sukhanov, ‘Проблемы использования доменных имен и товарных знаков в РФ’ (2016) <http://kafinf.ssa.ru/wp-content/uploads/2016/04/Суханов-1.pdf>

⁶² Mukhammad (n 59).

⁶³ *ibid.*

⁶⁴ Alrawashdedh (n 16).

⁶⁵ *ibid.*

⁶⁶ Zubin (n 20).

⁶⁷ Lipton (n 9).

scholars recommend improved registrar cooperation, domain name watch systems, and public awareness to prevent abuse.⁶⁸

In conclusion, while Kazakhstan's legal system recognises cybersquatting as a form of trademark infringement, the absence of dedicated procedures limits efficient enforcement. Aligning national policy with global best practices, especially through administrative reforms, would significantly improve trademark protection in Kazakhstan's digital economy.

⁶⁸ *ibid.*

SECTION 2. Cybersquatting issues: Kazakhstan and international practice

2.1 Scale and Specific Features of Cybersquatting in Kazakhstan

Cybersquatting has emerged as a growing concern in Kazakhstan's developing digital environment. As internet penetration and e-commerce increase, so does the incidence of domain name registrations that mimic existing trademarks, often without authorization or legitimate interest. While the global dimensions of cybersquatting are well-documented, its national characteristics in Kazakhstan present a blend of both universal patterns and local legal specificities.

In Kazakhstan, cybersquatting most often takes the form of the bad-faith registration of .kz domain names that match well-known trademarks. These are usually held without any actual business use and later offered for resale to the trademark owner at a profit.⁶⁹ According to Bolotov & Partners, Kazakhstani trademark law recognizes such behaviour as infringing when it is carried out in bad faith, even where the domain is not being actively used in commerce.⁷⁰ Although the legislation does not include an explicit definition of cybersquatting, existing legal norms are applied to combat this behaviour through the Law on Trademarks and the Civil Code.⁷¹

One distinguishing feature of the Kazakhstani cybersquatting environment is the overlap with trademark squatting. Zhanadilov points out that Russian companies and individuals have increasingly targeted Kazakhstan as a forum to re-register or cancel dormant trademarks of international brands.⁷² This trend accelerated following geopolitical developments in the region, particularly after many Western brands exited the Russian market.⁷³ Opportunistic registrants have tried to fill the void by acquiring trademarks and corresponding domain names of brands such as *Ericsson* and *Sanyo*, sometimes by invoking Kazakhstan's non-

⁶⁹ Zhanat Nurmagambetov, 'Overview of Trademark Protection in the Countries of Central Asia' (Bolotov & Partners, 2021) <https://bolotovip.com/publication/overview-of-trademark-protection-in-the-countries-of-central-asia/> accessed 20 April 2025.

⁷⁰ *ibid.*

⁷¹ *ibid.*

⁷² Bauyrzhan Zhanadilov, 'Trademark Squatting in Kazakhstan: From Russia with Love' (Kluwer Trademark Blog, 21 August 2024) <https://trademarkblog.kluweriplaw.com/2024/08/21/trademark-squatting-in-kazakhstan-from-russia-with-love/>

⁷³ *ibid.*

use cancellation provisions.⁷⁴ While this is not always technically cybersquatting, the practical outcomes and intent closely resemble it, as the registrants aim to benefit from the reputation of globally recognized names.

Moreover, Kazakhstan's legislative evolution has complicated cybersquatting enforcement. Prior to 2018, Article 43 of the Trademark Law treated the mere inclusion of a trademark in a domain name – regardless of use – as infringement.⁷⁵ After an amendment that year, the law was narrowed to require that the use must relate to similar goods or services.⁷⁶ As a result, passive domain name holding (where the registrant neither uses nor sells products) may no longer be automatically deemed an infringement under the newer provisions. Courts are now more reliant on civil doctrines such as abuse of right and unfair competition to address clear cases of bad faith.⁷⁷

Another issue is the absence of an administrative dispute resolution mechanism for .kz domains. Unlike many country-code top-level domain (ccTLD) registries that have adopted UDRP-style proceedings, Kazakhstan relies on court litigation to resolve domain name disputes.⁷⁸ This increases the time and cost involved in recovering infringing domains and may discourage smaller businesses from pursuing enforcement.

Despite these limitations, evidence suggests that cybersquatting in Kazakhstan is a persistent and organized phenomenon. Zhanadilov reports a case where a single individual had registered more than 10,000 domain names, many of which reflected famous trademarks.⁷⁹ These figures mirror trends seen in larger economies and indicate the emergence of professional domain speculators in the region.

According to a 2021 EUIPO study, industries like fashion, electronics, and automotive are particularly vulnerable to domain abuse.⁸⁰ This trend holds

⁷⁴ *ibid.*

⁷⁵ Zhanat Nurmagambetov (n 69).

⁷⁶ *ibid.*

⁷⁷ Zhanadilov (n 72).

⁷⁸ *ibid.*

⁷⁹ Bauyrzhan Zhanadilov, 'Cybersquatting in Kazakhstan: The Bobcat Trademark Dispute' (Kluwer Trademark Blog, 27 February 2025) <https://trademarkblog.kluweriplaw.com/2025/02/27/cybersquatting-in-kazakhstan-the-bobcat-trademark-dispute/>

⁸⁰ European Union Intellectual Property Office (EUIPO), 'Focus on Cybersquatting: Monitoring and Analysis – Executive Summary' (2021) 3 https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Cybersquatting_Study/2021_Focus_on_Cybersquatting_Monitoring_and_Analysis_Study_ExSum_en.pdf

true in Kazakhstan, where squatted domains have targeted globally recognised brands in those sectors. While Kazakhstan has not yet published national statistics on cybersquatting cases, the increasing number of disputes in court and media coverage of high-profile cases demonstrate the growing scope of the problem.

2.2 Judicial Practice on Cybersquatting in Kazakhstan (Court Cases and Examples)

Although Kazakhstan lacks a specialised IP court, recent judicial practice reflects a growing maturity in addressing cybersquatting and related trademark misuse. Courts are showing greater sensitivity to issues of bad faith and are increasingly willing to infer abuse of rights, even when statutory definitions do not directly apply.

A notable case involved Doosan Bobcat North America Inc., a global construction equipment brand. The company discovered that the domain bobcat.kz had been registered by an individual unaffiliated with the brand. The registrant had no legitimate business interest in the name “Bobcat” and was known for holding a vast portfolio of domains, many of which matched well-known trademarks.⁸¹ The domain was inactive but publicly offered for sale – a classic red flag of cybersquatting.

Because Kazakhstan’s Trademark Law, post-2018, no longer clearly defines domain name registration as infringement unless related to competing goods or services, Doosan Bobcat had to rely on the principles of unfair competition and abuse of right.⁸² The court accepted this approach and interpreted the registrant’s conduct as being in bad faith. Although the case concluded via settlement with the domain being transferred voluntarily, it established a precedent for using general civil law doctrines as a basis for recovery.

Another relevant example is the Ericsson trademark case. Here, the Russian company R-Climate attempted to cancel the existing Kazakh registration of the ERICSSON mark based on alleged non-use. This move, combined with attempts to secure the corresponding domain name, reflected a strategic attempt to hijack a well-known brand.⁸³ Ericsson successfully demonstrated ongoing commercial activity through a local subsidiary and convinced the court that R-Climate’s actions were not

⁸¹ Zhanadilov (n 79).

⁸² *ibid.*

⁸³ Zhanadilov (n 72).

grounded in genuine interest but opportunism.⁸⁴ The court rejected the cancellation request, reinforcing the principle that misuse of procedural rights can be tantamount to abuse of right under Article 8 of the Kazakh Civil Code.

Similarly, the SANYO case followed the same pattern. The Russian company ALAYV TRADE filed a non-use cancellation suit against long-held trademarks of the Japanese electronics giant. The Kazakh court sided with SANYO, recognising the strategic misuse of the legal system and denying the plaintiff's claims based on bad faith.⁸⁵

These cases suggest an emerging judicial philosophy in Kazakhstan: while domain name squatting and trademark cancellation cases are formally distinct, courts recognise the underlying opportunism in both. They are increasingly willing to prioritise intent and pattern of conduct over mere technical arguments, thus aligning local jurisprudence with international norms.

2.3 International Regulatory Experience: Key Precedents (UDRP, WIPO, ACPA, etc.)

The regulation of cybersquatting at the international level has evolved through a combination of national legislation, institutional procedures, and multilateral efforts. Among the most significant developments in this space are the Uniform Domain-Name Dispute-Resolution Policy (UDRP) established by ICANN, the Anticybersquatting Consumer Protection Act (ACPA) in the United States, and various administrative mechanisms supported by WIPO and domain registrars.

The UDRP, introduced by ICANN in 1999 and administered through WIPO and other dispute resolution providers, remains the primary international mechanism to resolve domain name disputes.⁸⁶ It applies to most top-level domains (e.g., .com, .org) and is contractually binding for registrants. A complainant under UDRP must establish three key elements: (1) the domain name is identical or confusingly similar to their trademark; (2) the registrant has no rights or legitimate interests in it; and (3) it was registered and is being used in bad faith.⁸⁷ If successful, the domain may be

⁸⁴ *ibid.*

⁸⁵ Helfer and Dinwoodie (n 13).

⁸⁶ Alrawashdedh (n 16).

⁸⁷ *ibid* 42–43.

transferred or cancelled, but UDRP proceedings do not permit damages or injunctive relief.

The appeal of UDRP lies in its efficiency, accessibility, and neutrality. Most disputes are resolved in less than 60 days based on written submissions, which makes it a cost-effective alternative to litigation.⁸⁸ Moreover, the international reach of UDRP gives trademark owners a relatively uniform process across borders, helping to fill the gaps left by fragmented national laws.⁸⁹

However, critics have pointed out some weaknesses in the UDRP system. Alrawashdedh notes concerns about inconsistent panel decisions and the lack of an appeals process.⁹⁰ There is also debate around whether the burden of proof favours complainants too heavily in borderline cases. Nevertheless, the mechanism has proven especially effective in clear instances of bad-faith domain squatting.

In contrast, the United States' ACPA, enacted in 1999 as an amendment to the Lanham Act, offers a more aggressive legal framework.⁹¹ It defines cybersquatting as registering or using a domain name that is identical or confusingly similar to a distinctive or famous trademark, with the intent to profit.⁹² Courts applying the ACPA examine nine factors to assess bad faith, including whether the registrant has a history of such registrations or has offered to sell the domain to the trademark owner.⁹³

A unique feature of the ACPA is that it allows statutory damages up to \$100,000 per domain, and even permits in rem actions when the registrant is unidentifiable.⁹⁴ However, its reach is territorially limited, and judgments may not be enforceable abroad. That said, its strong deterrent effect combined with UDRP's administrative efficiency – often means that many corporations pursue parallel strategies under both mechanisms.⁹⁵

In the European Union, a harmonised cybersquatting regime does not yet exist. Instead, countries apply existing trademark or unfair competition laws to domain disputes. For example, Germany addresses cybersquatting through civil law doctrines, while France relies on court-

⁸⁸ Helfer and Dinwoodie (n 13) 146–147.

⁸⁹ *ibid.*

⁹⁰ Alrawashdedh (n 86) 66–68.

⁹¹ Sangeetha Laxmi V (n 22).

⁹² *ibid.*

⁹³ *ibid* 6–8.

⁹⁴ *ibid* 8.

⁹⁵ *ibid* 9.

developed principles of brand misuse.⁹⁶ Despite the lack of EU-level legislation, most national courts have shown sympathy for trademark owners, particularly when dealing with domain registrations clearly aimed at resale or deception.⁹⁷

WIPO's role extends beyond UDRP. The WIPO Arbitration and Mediation Center also serves as a leading venue for domain disputes involving country-code top-level domains (ccTLDs), including .cn, .in, and .fr, though .kz is not yet included. WIPO continues to issue guidance on evolving issues in domain policy and promotes adoption of best practices globally, such as requiring disclosure of beneficial owners in disputes.⁹⁸

Kazakhstan, by contrast, does not yet have a national UDRP-like system. Disputes over .kz domains must proceed through **civil litigation**, which is more time-consuming and complex.⁹⁹ Scholars have suggested that introducing a fast-track administrative option would bring Kazakhstan closer to international norms and reduce pressure on the judiciary.¹⁰⁰ Such a mechanism could be especially useful in straightforward cases involving obviously bad-faith registrations.

In summary, global regulation of cybersquatting shows a dual-track approach: administrative remedies for speed and civil litigation for damages and broader enforcement. The UDRP, ACPA, and WIPO initiatives reflect different tools suited for different types of disputes. Kazakhstan may benefit from aligning with these models by implementing reforms that balance trademark enforcement with due process protections.

2.4 International Judicial Practice on Cybersquatting (Court Cases and Examples)

Beyond regulatory frameworks, international judicial decisions have shaped the enforcement landscape for cybersquatting. Courts and arbitral panels have developed case law that emphasises the importance of bad faith, consumer deception, and legitimate interest in domain disputes.

A pivotal UDRP case is *Telstra Corporation Ltd v Nuclear Marshmallows*, where the WIPO panel held that passive holding of a domain name can

⁹⁶ Alrawashdedh (n 16) 88–90.

⁹⁷ *ibid* 93–95.

⁹⁸ *ibid* 98–100.

⁹⁹ *ibid* 105–107.

¹⁰⁰ *ibid* 115.

constitute bad faith when the trademark is well known and there is no plausible legitimate use.¹⁰¹ This case helped establish that inaction, combined with registrant concealment and mark reputation, could justify a finding of abuse.

In *Julia Fiona Roberts v Russell Boyd*, the WIPO panel ruled that registering a celebrity name for the purpose of resale without authorization constituted cybersquatting under UDRP standards.¹⁰² The complainant's fame, and the respondent's offer to sell the domain, made bad faith evident despite no commercial use.

In the United States, courts applying the ACPA have established important precedents. In *Virtual Works v Volkswagen*, the Fourth Circuit found that a domain registered without any bona fide use and with a clear connection to the trademark holder's brand was evidence of intent to profit and justified transfer.¹⁰³ Similarly, in *Sporty's Farm v Sportsman's Market*, the court ruled that the registrant's intent to divert business amounted to cybersquatting.¹⁰⁴ These rulings highlight that U.S. courts prioritise intent and pattern of conduct in their assessments.

In India, *Yahoo! Inc. v Akash Arora* was the first major cybersquatting case, where the Delhi High Court ruled that registering a confusingly similar domain name could constitute passing off, even in the absence of a specific cybersquatting statute.¹⁰⁵ The defendant's domain, *yahooindia.com*, was held to exploit Yahoo's reputation and mislead users, warranting an injunction.

The UK's landmark decision in *British Telecommunications plc & Ors v One In A Million Ltd* concluded that registering domain names corresponding to major brands was an instrument of fraud.¹⁰⁶ The court emphasized that registration alone, even without use, could justify injunctive relief if it served no legitimate purpose.

Other cases confirm that the standard of proof for bad faith is not unduly high when the facts suggest opportunism. For example, *Harrods Ltd v Sixty Internet Domain Names* in the U.S. permitted in rem action against

¹⁰¹ *Telstra Corporation Ltd v Nuclear Marshmallows*, WIPO Case No D2000-0003 (WIPO, 2000) <https://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0003.html>

¹⁰² *Julia Fiona Roberts v Russell Boyd*, WIPO Case No D2000-0210 (WIPO, 2000) <https://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0210.html>

¹⁰³ *Virtual Works, Inc v Volkswagen of America, Inc* 238 F3d 264 (4th Cir 2001).

¹⁰⁴ *Sporty's Farm LLC v Sportsman's Market, Inc* 202 F3d 489 (2nd Cir 2000).

¹⁰⁵ *Yahoo! Inc v Akash Arora*, High Court of Delhi, 1999 IIAD Delhi 229.

¹⁰⁶ *British Telecommunications plc & Ors v One In A Million Ltd* [1999] 1 WLR 903 (CA).

60 domains because the registrant could not be identified, yet the use of the Harrods name was unjustifiable.¹⁰⁷

Taken together, these cases show that international courts and panels favour a contextual, purpose-based analysis of cybersquatting. When a registrant's only plausible goal is to block, mislead, or extract value from the mark holder, relief is typically granted. Moreover, legitimate uses such as satire, non-commercial commentary, or unrelated business are protected only when substantiated by credible evidence.

For Kazakhstan, the lessons are clear: although litigation remains the primary path, aligning with global norms requires a shift from formalism to intent-based review. Courts must be empowered to infer bad faith based on circumstantial evidence, as seen in Telstra and Volkswagen. Kazakhstan's evolving jurisprudence already shows movement in this direction, as courts increasingly reference abuse of right and unfair competition doctrines to supplement limitations in trademark law.

¹⁰⁷ *Harrods Ltd v Sixty Internet Domain Names* 302 F3d 214 (4th Cir 2002).

SECTION 3. Ways to improve the legal regulation of cybersquatting

3.1 In-Depth Analysis of International Mechanisms for Combating Cybersquatting (UDRP, ACPA, WIPO)

As it was mentioned before, the problem of cybersquatting has been addressed internationally through mechanisms such as the Uniform Domain-Name Dispute-Resolution Policy (UDRP), the Anti-Cybersquatting Consumer Protection Act (ACPA), and the efforts of the World Intellectual Property Organization (WIPO). Each of these frameworks offers distinct models for tackling domain name abuses.

As it was mentioned before the UDRP was developed in cooperation with WIPO to create an efficient, non-judicial mechanism for resolving domain name disputes on a global scale.¹⁰⁸ Under the UDRP, complainants must prove three elements: the domain name is identical or confusingly similar to a trademark in which the complainant has rights; the respondent has no legitimate interests in the domain name; and the domain name has been registered and is being used in bad faith.¹⁰⁹ This simplified test enables expedited adjudication based purely on documentary evidence.¹¹⁰

The process is administered by accredited dispute resolution providers, notably the WIPO Arbitration and Mediation Center, which handles the majority of UDRP cases.¹¹¹ Proceedings are conducted online and decisions are generally issued within sixty days.¹¹² Remedies are limited to the transfer or cancellation of the domain name, without any award of monetary damages.¹¹³ Despite this limitation, the UDRP is widely regarded as an efficient remedy for straightforward cases of cybersquatting.¹¹⁴

¹⁰⁸ Rukmani Sachdeva, 'Critical Study on Trademark Infringement Related to Domain Names and Cybersquatting' (2022) 2 *Jus Corpus Law Journal*.

¹⁰⁹ Sangeetha Lakshmi V, 'The Menace of Cybersquatting and Legal Measures' (2022) 2 *Indian Journal of Integrated Research in Law*.

¹¹⁰ Anis Ahmad and Nikki Kumar, 'Critical Analysis of the Regulatory Framework Relating to Cybersquatting in India' (2024) *Prayagraj Law Review*.

¹¹¹ Radhika V Bhusari and Karan R Rampure, 'Cybersquatting: A Threat to the Globalising World' (2021) 3 *Indian Journal of Legal Research*.

¹¹² Jalaj Agarwal and Gracy Bindra, 'Domain Name Disputes and the Rising Threat of Cybersquatters' (2020) 6 *Indian Journal of Law and Society*.

¹¹³ Kashish Wadhwa, 'Domain Name and Cyber Squatting' (2022) 4(3) *Indian Journal of Legal Research*.

¹¹⁴ Jeetika Aggarwal and Priyanshi Bainwala, 'Cybersquatting and Trademark Infringement' (2021) 4(2) *International Journal of Law Management and Humanities*.

Nevertheless, the UDRP has faced criticisms. Scholars highlight inconsistencies in panel decisions and the absence of a formal appeals process.¹¹⁵ Moreover, the burden on complainants to prove all three elements has sometimes led to legitimate grievances being dismissed.¹¹⁶ Some concerns also exist regarding panelist bias in favour of trademark owners.¹¹⁷ Yet despite its imperfections, the UDRP remains the predominant mechanism for resolving international domain name disputes.¹¹⁸

The United States introduced the ACPA, amending the Lanham Act to provide judicial remedies against cybersquatting.¹¹⁹ The ACPA defines cybersquatting as the bad-faith registration, use, or trafficking in a domain name that is identical or confusingly similar to a distinctive or famous trademark.¹²⁰ Courts are directed to assess bad faith using a non-exhaustive list of nine factors, including the registrant's intent to divert customers, pattern of similar registrations, and offers to sell the domain name for financial gain.¹²¹

The ACPA empowers courts to order the forfeiture, cancellation, or transfer of domain names, and allows plaintiffs to seek actual or statutory damages ranging from \$1,000 to \$100,000 per domain.¹²² Notably, it also permits in rem actions against domain names themselves when personal jurisdiction over the registrant is unavailable, thereby extending its reach to anonymous or foreign cybersquatters.¹²³ The ACPA has thus been praised for offering robust deterrence through financial sanctions.¹²⁴

¹¹⁵ Ravish Ranjan, 'Trademark Infringement Issue in Cyberspace' (2022–2023) 4(6) *Indian Journal of Legal Research*.

¹¹⁶ Alif Muhammad Gultom, 'Domain Name under UDRP: Unregistered Trademark Protection' (2023) 5(1) *Indian Journal of Legal Research*.

¹¹⁷ Ioana VasIU and Lucian VasIU, 'A Framework for Improved Protection of Trademarks' (2022) 28 *Journal of Law, Business and Ethics*.

¹¹⁸ Bandu Meshram and Manish Kumar Singh, 'Conventional and Modern Cyber Crimes Dynamics and Legal Countermeasures in India' (2024) 14 *GNLU Journal of Law Development and Policy*.

¹¹⁹ Chris A Huff, 'License and Registration: Domain Name Interpretation under US Anticybersquatting Act' (2021) 30 *Information and Communication Technology Law*.

¹²⁰ Katie M Brown and Natasha T Brison, 'Think Like Adidas: Analysis of Trademark Protection Strategies' (2022) 32 *Marquette Sports Law Review* 445.

¹²¹ Jyotiranga Puzari, 'Typosquatting and Its Impact upon Intellectual Property in Cyberspace' (2023) 7(2) *Journal of Intellectual Property Studies*.

¹²² Arusmita Acharya, 'Revisiting Dilution as Trademark Infringement: A Comparative Law Lens' (2022) *Supremo Amicus* 26.

¹²³ Julien Chaisse and Danny Friedmann, 'Law of the Digital Domain: Trademarks, Domain Names and AI' (2024) 64 *IDEA: The Law Review of the Franklin Pierce Center for Intellectual Property* 399.

¹²⁴ Michael Grynberg, 'Trademark Free Riders' (2024) 39 *Berkeley Technology Law Journal* 275.

However, the ACPA's reliance on litigation presents disadvantages. Proceedings are expensive, time-consuming, and jurisdictionally limited to U.S. courts.¹²⁵ Furthermore, establishing bad faith requires detailed evidence, increasing the burden on trademark owners compared to administrative options like the UDRP.¹²⁶ Accordingly, many rights holders simultaneously pursue UDRP complaints for speed and ACPA lawsuits for stronger remedies.¹²⁷

Complementing both the UDRP and the ACPA is the institutional role of WIPO. Besides administering UDRP proceedings, WIPO offers arbitration for country-code top-level domains (ccTLDs) in cooperation with national registries.¹²⁸ WIPO also administers the Uniform Rapid Suspension (URS) system, designed for clear-cut cases of cybersquatting under new generic top-level domains (gTLDs).¹²⁹ The URS process is even faster and cheaper than UDRP but provides only for domain suspension, not transfer.¹³⁰

Additionally, WIPO established the Trademark Clearinghouse, a database that enables trademark holders to receive notifications of potentially infringing domain name registrations during new gTLD launch phases.¹³¹ This proactive system aims to prevent cybersquatting before disputes arise.¹³²

Despite these initiatives, WIPO's procedures share the UDRP's limitation of offering no financial remedies.¹³³ Enforcement also depends heavily on registrar cooperation, and challenges persist where domain owners use proxy registration services to mask their identities.¹³⁴ Nevertheless, WIPO

¹²⁵ Michael Grynberg, 'AI and the "Death of Trademark"' (2024) 114 Trademark Reporter 695.

¹²⁶ Stella Tsybizova, 'Problems of Legal Regulation of Domain Names: The Experience of the United States of America' (2023) Law Review of Kyiv University of Law 165.

¹²⁷ Maddi Gambone, 'Branding Beyond Boundaries: Trademarks and Advertising in Augmented Reality' (2024) 9 Intellectual Property and Competition Law Journal.

¹²⁸ Fatih Bugra Erdem, 'The Use of Arbitration Mechanisms in Trademark as Domain Name Disputes' (2023) 31 Selçuk Üniversitesi Hukuk Fakültesi Dergisi.

¹²⁹ A Rajeswari, 'Cyberspace and Intellectual Property: Evaluating Legal Frameworks through Space Transition Theory' (2024) 7(2) International Journal of Law Management and Humanities.

¹³⁰ Samiksha, 'Domain Name Related Dispute in IPR in India' (2023) 5(2) Indian Journal of Legal Research.

¹³¹ Maddi Gambone, 'Branding Beyond Boundaries: Trademarks and Advertising in Augmented Reality' (2024) 9 Intellectual Property and Competition Law Journal.

¹³² Ioana Vasiu and Lucian Vasiu, 'A Framework for Improved Protection of Trademarks' (2022) 28 Journal of Law, Business and Ethics.

¹³³ Julien Chaisse and Danny Friedmann, 'Law of the Digital Domain: Trademarks, Domain Names and AI' (2024) 64 IDEA: The Law Review of the Franklin Pierce Center for Intellectual Property 399.

¹³⁴ Stella Tsybizova, 'Problems of Legal Regulation of Domain Names: The Experience of the United States of America' (2023) Law Review of Kyiv University of Law 165.

remains a cornerstone of the international cybersquatting enforcement framework due to its expertise, neutrality, and procedural efficiency.¹³⁵

Taken together, the UDRP, ACPA, and WIPO initiatives create a multi-tiered regime for combating cybersquatting: administrative mechanisms offer quick resolution without damages, while litigation under statutes like the ACPA provides stronger sanctions but at greater cost and complexity.¹³⁶ For countries like Kazakhstan seeking to modernise cybersquatting enforcement, these systems offer valuable models to adapt and integrate.

3.2 Opportunities for Integrating International Experience into Kazakhstan's Legislation

Kazakhstan's current approach to cybersquatting remains largely dependent on general trademark law and unfair competition principles, without a dedicated administrative mechanism or specific statutory provision targeting bad-faith domain name registration.¹³⁷ Although Kazakhstan is a signatory to the Paris Convention and the TRIPS Agreement, which impose obligations to protect trademarks effectively, practical enforcement against cybersquatting is still underdeveloped.¹³⁸

An immediate opportunity for legislative reform is the creation of a UDRP-style administrative procedure specifically for the .kz domain space.¹³⁹ The success of the UDRP in offering quick, cost-effective, and internationally recognised resolutions suggests that Kazakhstan could implement a similar model through KazNIC, the national domain registry.¹⁴⁰ The adoption of administrative arbitration would enable trademark holders to resolve disputes without initiating lengthy civil

¹³⁵ Radhika V Bhusari and Karan R Rampure, 'Cybersquatting: A Threat to the Globalising World' (2021) 3 Indian Journal of Legal Research.

¹³⁶ Mark A Lemley, 'Rationalizing Internet Safe Harbors' (2007) 6(1) Journal on Telecommunication and High Technology Law.

¹³⁷ Anis Ahmad and Nikki Kumar, 'Critical Analysis of the Regulatory Framework Relating to Cybersquatting in India' (2024) Prayagraj Law Review.

¹³⁸ Stella Tsybizova, 'Problems of Legal Regulation of Domain Names: The Experience of the United States of America' (2023) Law Review of Kyiv University of Law 165.

¹³⁹ Rukmani Sachdeva, 'Critical Study on Trademark Infringement Related to Domain Names and Cybersquatting' (2022) 2 Jus Corpus Law Journal.

¹⁴⁰ Bandu Meshram and Manish Kumar Singh, 'Conventional and Modern Cyber Crimes Dynamics and Legal Countermeasures in India' (2024) 14 GNLU Journal of Law Development and Policy.

litigation, benefiting small businesses and individual rights holders disproportionately affected by high legal costs.¹⁴¹

KazNIC could amend its domain registration agreements to mandate that registrants submit to an administrative dispute resolution mechanism in cases involving allegations of bad-faith registration.¹⁴² Panels could be composed of intellectual property experts appointed either domestically or in collaboration with WIPO's Arbitration and Mediation Center.¹⁴³ Drawing upon WIPO's expertise would ensure impartial adjudication and procedural rigor.¹⁴⁴

In addition to procedural reform, Kazakhstan's statutory framework requires substantive strengthening. The current legal position, which demands use of a domain name in connection with goods or services to establish trademark infringement, undermines the ability to combat passive cybersquatting effectively.¹⁴⁵ Restoring the earlier, broader definition of infringement – whereby bad-faith registration alone constituted a violation – would close this loophole.¹⁴⁶

Moreover, Kazakhstan could codify a set of bad faith indicators, similar to the ACPA's nine-factor test.¹⁴⁷ Factors such as offering the domain name for sale to the trademark owner, registering multiple domain names corresponding to others' marks, or providing false registration information could serve as statutory evidence of bad faith.¹⁴⁸ Embedding these criteria in national law would increase predictability for courts and registrants alike, aligning Kazakhstan's framework with international best practices.¹⁴⁹

¹⁴¹ Jalaj Agarwal and Gracy Bindra, 'Domain Name Disputes and the Rising Threat of Cybersquatters' (2020) 6 Indian Journal of Law and Society.

¹⁴² Kashish Wadhwa, 'Domain Name and Cyber Squatting' (2022) 4(3) Indian Journal of Legal Research.

¹⁴³ Fatih Bugra Erdem, 'The Use of Arbitration Mechanisms in Trademark as Domain Name Disputes' (2023) 31 Selçuk Üniversitesi Hukuk Fakültesi Dergisi.

¹⁴⁴ A Rajeswari, 'Cyberspace and Intellectual Property: Evaluating Legal Frameworks through Space Transition Theory' (2024) 7(2) International Journal of Law Management and Humanities.

¹⁴⁵ Samiksha, 'Domain Name Related Dispute in IPR in India' (2023) 5(2) Indian Journal of Legal Research.

¹⁴⁶ Rukmani Sachdeva, 'Critical Study on Trademark Infringement Related to Domain Names and Cybersquatting' (2022) 2 Jus Corpus Law Journal.

¹⁴⁷ Chris A Huff, 'License and Registration: Domain Name Interpretation under US Anticybersquatting Act' (2021) 30 Information and Communication Technology Law.

¹⁴⁸ Chris A Huff, 'License and Registration: Domain Name Interpretation under US Anticybersquatting Act' (2021) 30 Information and Communication Technology Law.

¹⁴⁹ Ioana Vasiu and Lucian Vasiu, 'A Framework for Improved Protection of Trademarks' (2022) 28 Journal of Law, Business and Ethics.

The introduction of statutory damages for cybersquatting would further enhance enforcement.¹⁵⁰ As in the ACPA, statutory damages could be set within a reasonable range to balance deterrence with proportionality, reflecting Kazakhstan's economic context.¹⁵¹ Even moderate penalties would discourage opportunistic registrations and compensate rights holders for enforcement costs.¹⁵²

Procedural reforms could also include authorising in rem actions against domain names registered anonymously or by foreign individuals.¹⁵³ This would enable Kazakh courts to assert jurisdiction over a domain name itself, rather than being restricted by personal jurisdiction requirements.¹⁵⁴ Such a mechanism would simplify litigation and extend protection to domestic trademark owners facing cross-border cybersquatting.¹⁵⁵

Kazakhstan should also strengthen cooperation with domain registrars. Mandatory disclosure of registrant information in cases of credible infringement complaints would facilitate enforcement.¹⁵⁶ Registrars could also be required to notify trademark owners when registrations closely matching existing trademarks occur, mirroring WIPO's Trademark Clearinghouse model.¹⁵⁷ Although initially resource-intensive, these preventive measures would ultimately reduce the incidence of disputes and administrative burden on courts and arbitration bodies.¹⁵⁸

Finally, Kazakhstan could enter into formal cooperation agreements with WIPO to allow domain name disputes under .kz to be handled by WIPO panels.¹⁵⁹ Such partnerships would enhance international credibility, ensure access to experienced adjudicators, and facilitate knowledge

¹⁵⁰ Katie M Brown and Natasha T Brison, 'Think Like Adidas: Analysis of Trademark Protection Strategies' (2022) 32 Marquette Sports Law Review 445.

¹⁵¹ Chris A Huff, 'License and Registration: Domain Name Interpretation under US Anticybersquatting Act' (2021) 30 Information and Communication Technology Law.

¹⁵² Jyotiranga Puzari, 'Typosquatting and Its Impact upon Intellectual Property in Cyberspace' (2023) 7(2) Journal of Intellectual Property Studies.

¹⁵³ Julien Chaisse and Danny Friedmann, 'Law of the Digital Domain: Trademarks, Domain Names and AI' (2024) 64 IDEA: The Law Review of the Franklin Pierce Center for Intellectual Property 399.

¹⁵⁴ Stella Tsybizova, 'Problems of Legal Regulation of Domain Names: The Experience of the United States of America' (2023) Law Review of Kyiv University of Law 165.

¹⁵⁵ Anis Ahmad and Nikki Kumar, 'Critical Analysis of the Regulatory Framework Relating to Cybersquatting in India' (2024) Prayagraj Law Review.

¹⁵⁶ Maddi Gambone, 'Branding Beyond Boundaries: Trademarks and Advertising in Augmented Reality' (2024) 9 Intellectual Property and Competition Law Journal.

¹⁵⁷ Julien Chaisse and Danny Friedmann, 'Law of the Digital Domain: Trademarks, Domain Names and AI' (2024) 64 IDEA: The Law Review of the Franklin Pierce Center for Intellectual Property 399.

¹⁵⁸ Fatih Bugra Erdem, 'The Use of Arbitration Mechanisms in Trademark as Domain Name Disputes' (2023) 31 Selçuk Üniversitesi Hukuk Fakültesi Dergisi.

¹⁵⁹ Radhika V Bhusari and Karan R Rampure, 'Cybersquatting: A Threat to the Globalising World' (2021) 3 Indian Journal of Legal Research.

transfer to local legal practitioners.¹⁶⁰ Participation in WIPO's broader initiatives, such as the URS system for quick suspension of clearly infringing domains, could also be considered in the future.¹⁶¹

In summary, Kazakhstan stands at a critical juncture where it can draw upon proven international mechanisms to modernise its cybersquatting regulatory framework.¹⁶² By adopting a UDRP-style administrative procedure, strengthening statutory definitions and remedies, authorising in rem proceedings, enhancing registrar cooperation, and collaborating with WIPO, Kazakhstan could significantly improve the protection of trademark rights online.¹⁶³ These reforms would not only fulfil Kazakhstan's international obligations but also foster a more secure and predictable environment for e-commerce and brand development in the country's digital economy.¹⁶⁴

3.3 Directions for Improving National Legislation

Kazakhstan's current legal framework regarding cybersquatting remains fragmented and insufficient. Although the Civil Code and the Law on Trademarks provide some protection, there is no explicit legal provision addressing domain name disputes. Scholars emphasize that domain names today function as significant commercial assets, often equated to "the real estate of the 21st century".¹⁶⁵ Without specific regulations, rights holders in Kazakhstan must rely on lengthy and expensive civil proceedings to address cybersquatting issues, an approach deemed inadequate for the fast-moving digital economy.¹⁶⁶

Firstly, Kazakhstan must introduce a clear statutory definition of cybersquatting. As seen in comparative jurisdictions, defining cybersquatting as the bad-faith registration, use, or trafficking of a domain

¹⁶⁰ Bandu Meshram and Manish Kumar Singh, 'Conventional and Modern Cyber Crimes Dynamics and Legal Countermeasures in India' (2024) 14 GNLU Journal of Law Development and Policy.

¹⁶¹ Julien Chaisse and Danny Friedmann, 'Law of the Digital Domain: Trademarks, Domain Names and AI' (2024) 64 IDEA: The Law Review of the Franklin Pierce Center for Intellectual Property 399.

¹⁶² Stella Tsybizova, 'Problems of Legal Regulation of Domain Names: The Experience of the United States of America' (2023) Law Review of Kyiv University of Law 165.

¹⁶³ Ioana Vasii and Lucian Vasii, 'A Framework for Improved Protection of Trademarks' (2022) 28 Journal of Law, Business and Ethics.

¹⁶⁴ Maddi Gambone, 'Branding Beyond Boundaries: Trademarks and Advertising in Augmented Reality' (2024) 9 Intellectual Property and Competition Law Journal.

¹⁶⁵ Rukmani Sachdeva, 'Critical Study on Trademark Infringement Related to Domain Names and Cybersquatting' (2022) 2 Jus Corpus Law Journal.

¹⁶⁶ Sangeetha Lakshmi V, 'The Menace of Cybersquatting and Legal Measures' (2022) 2 Indian Journal of Integrated Research in Law.

name identical or confusingly similar to a trademark is crucial.¹⁶⁷ Such a definition would align Kazakhstan with international norms and provide courts with a clear basis for enforcement.¹⁶⁸ For instance, in India, courts have applied principles of passing off to cybersquatting cases, even in the absence of specific legislative provisions.¹⁶⁹ Similarly, Kazakhstan's adoption of an explicit definition would eliminate interpretative ambiguity.

Secondly, Kazakhstan should create a dedicated administrative mechanism for domain name dispute resolution. The UDRP has been widely praised for providing a rapid, cost-effective remedy against cybersquatting.¹⁷⁰ Under the UDRP, complainants must prove three elements: confusing similarity to a trademark, lack of legitimate interests, and bad faith registration.¹⁷¹ Establishing a UDRP-style system for the .kz domain would offer significant benefits. Such a mechanism could be modelled after India's INDRP or Brazil's NIC.br procedure, both of which successfully adapted UDRP principles to local conditions.¹⁷²

Moreover, introducing statutory damages for cybersquatting would enhance deterrence. Under the U.S. Anti-Cybersquatting Consumer Protection Act (ACPA), courts may award up to \$100,000 per domain name in statutory damages.¹⁷³ Scholars argue that statutory damages serve as an effective deterrent against bad-faith registrations.¹⁷⁴ Kazakhstan could implement a similar provision, allowing trademark owners to recover compensation without the burden of proving actual damages.¹⁷⁵

Registrar obligations must also be reinforced. Registrars play a critical role in the domain name ecosystem, and their cooperation is essential in

¹⁶⁷ Anis Ahmad and Nikki Kumar, 'Critical Analysis of the Regulatory Framework Relating to Cybersquatting in India' (2024) Prayagraj Law Review.

¹⁶⁸ Radhika V Bhusari and Karan R Rampure, 'Cybersquatting: A Threat to the Globalising World' (2021) 3 Indian Journal of Legal Research.

¹⁶⁹ Jalaj Agarwal and Gracy Bindra, 'Domain Name Disputes and the Rising Threat of Cybersquatters' (2020) 6 Indian Journal of Law and Society.

¹⁷⁰ Kashish Wadhwa, 'Domain Name and Cyber Squatting' (2022) 4(3) Indian Journal of Legal Research.

¹⁷¹ Jeetika Aggarwal and Priyanshi Bainwala, 'Cybersquatting and Trademark Infringement' (2021) 4(2) International Journal of Law Management and Humanities.

¹⁷² Ravish Ranjan, 'Trademark Infringement Issue in Cyberspace' (2022–2023) 4(6) Indian Journal of Legal Research.

¹⁷³ Alif Muhammad Gultom, 'Domain Name under UDRP: Unregistered Trademark Protection' (2023) 5(1) Indian Journal of Legal Research.

¹⁷⁴ Ioana Vasii and Lucian Vasii, 'A Framework for Improved Protection of Trademarks' (2022) 28 Journal of Law, Business and Ethics.

¹⁷⁵ Bandu Meshram and Manish Kumar Singh, 'Conventional and Modern Cyber Crimes Dynamics and Legal Countermeasures in India' (2024) 14 GNLU Journal of Law Development and Policy.

combating cybersquatting.¹⁷⁶ Laws should require registrars to verify applicant information, maintain accurate WHOIS data, and implement swift procedures for suspending or cancelling infringing domain names upon receipt of valid complaints.¹⁷⁷ As observed in the UDRP, registrar compliance is crucial for the effective enforcement of panel decisions.¹⁷⁸

Another important step is strengthening judicial capacity. Judges must be trained in the complexities of cyberspace law, particularly regarding domain name disputes.¹⁷⁹ Specialized IP courts or designated IP judges could improve the quality and consistency of decisions.¹⁸⁰ This specialization has been effective in jurisdictions like Germany and South Korea, where dedicated IP courts handle complex digital rights cases.¹⁸¹

Furthermore, Kazakhstan should enhance cooperation with international organizations. The World Intellectual Property Organization (WIPO) has extensive experience administering domain name disputes under the UDRP.¹⁸² Formal cooperation with WIPO could provide Kazakhstan access to global best practices and dispute resolution expertise.¹⁸³ Participation in initiatives like WIPO's Advanced Course on Domain Name Dispute Resolution would also build local capacity.¹⁸⁴

Lastly, public awareness initiatives are necessary. Many businesses, especially small and medium-sized enterprises (SMEs), are unaware of the risks associated with cybersquatting.¹⁸⁵ Government agencies and industry associations should conduct campaigns to educate stakeholders about the importance of proactive domain name protection.¹⁸⁶

¹⁷⁶ Chris A Huff, 'License and Registration: Domain Name Interpretation under US Anticybersquatting Act' (2021) 30 Information and Communication Technology Law.

¹⁷⁷ Katie M Brown and Natasha T Brison, 'Think Like Adidas: Analysis of Trademark Protection Strategies' (2022) 32 Marquette Sports Law Review 445.

¹⁷⁸ Jyotiranga Puzari, 'Typosquatting and Its Impact upon Intellectual Property in Cyberspace' (2023) 7(2) Journal of Intellectual Property Studies.

¹⁷⁹ Arusmita Acharya, 'Revisiting Dilution as Trademark Infringement: A Comparative Law Lens' (2022) *Supremo Amicus* 26.

¹⁸⁰ Julien Chaisse and Danny Friedmann, 'Law of the Digital Domain: Trademarks, Domain Names and AI' (2024) 64 *IDEA: The Law Review of the Franklin Pierce Center for Intellectual Property* 399.

¹⁸¹ Michael Grynberg, 'Trademark Free Riders' (2024) 39 *Berkeley Technology Law Journal* 275.

¹⁸² Michael Grynberg, 'AI and the "Death of Trademark"' (2024) 114 *Trademark Reporter* 695.

¹⁸³ Stella Tsybizova, 'Problems of Legal Regulation of Domain Names: The Experience of the United States of America' (2023) *Law Review of Kyiv University of Law* 165.

¹⁸⁴ Maddi Gambone, 'Branding Beyond Boundaries: Trademarks and Advertising in Augmented Reality' (2024) 9 *Intellectual Property and Competition Law Journal*.

¹⁸⁵ Fatih Bugra Erdem, 'The Use of Arbitration Mechanisms in Trademark as Domain Name Disputes' (2023) 31 *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*.

¹⁸⁶ A Rajeswari, 'Cyberspace and Intellectual Property: Evaluating Legal Frameworks through Space Transition Theory' (2024) 7(2) *International Journal of Law Management and Humanities*.

Encouraging the registration of defensive domain names and the use of trademark watch services can help prevent cybersquatting incidents.¹⁸⁷

In summary, improving Kazakhstan's national legislation requires a multifaceted approach: defining cybersquatting clearly, establishing administrative dispute resolution mechanisms, introducing statutory damages, reinforcing registrar obligations, enhancing judicial specialization, cooperating with international bodies, and raising public awareness. These reforms, based on international best practices, would significantly strengthen Kazakhstan's ability to protect trademark rights in the digital environment.¹⁸⁸

3.4 Proposals for Enhancing the Protection of Trademarks and Domain Names in Kazakhstan

The growing challenges of cybersquatting in Kazakhstan require an urgent and strategic legislative response. Trademark owners face significant obstacles in securing their rights against bad-faith domain name registrations due to the absence of specialized administrative remedies and modern enforcement mechanisms.¹⁸⁹ To ensure robust protection aligned with international standards, Kazakhstan must adopt comprehensive legal, procedural, and institutional reforms.¹⁹⁰

One of the primary recommendations is the introduction of a Uniform Domain-Name Dispute-Resolution Policy (UDRP)-style administrative mechanism for resolving domain name disputes under the .kz domain.¹⁹¹ Globally, the UDRP has proven highly successful in offering an efficient, affordable, and quick remedy for clear cases of cybersquatting.¹⁹² Unlike traditional litigation, which is often lengthy and expensive, administrative panels operating under UDRP principles can determine cases based on documentary submissions within a matter of weeks.¹⁹³ Implementing a

¹⁸⁷ Samiksha, 'Domain Name Related Dispute in IPR in India' (2023) 5(2) Indian Journal of Legal Research.

¹⁸⁸ Maddi Gambone, 'Branding Beyond Boundaries: Trademarks and Advertising in Augmented Reality' (2024) 9 Intellectual Property and Competition Law Journal.

¹⁸⁹ Rukmani Sachdeva, 'Critical Study on Trademark Infringement Related to Domain Names and Cybersquatting' (2022) 2 Jus Corpus Law Journal.

¹⁹⁰ Sangeetha Lakshmi V, 'The Menace of Cybersquatting and Legal Measures' (2022) 2 Indian Journal of Integrated Research in Law.

¹⁹¹ Kashish Wadhwa, 'Domain Name and Cyber Squatting' (2022) 4(3) Indian Journal of Legal Research.

¹⁹² Radhika V Bhusari and Karan R Rampure, 'Cybersquatting: A Threat to the Globalising World' (2021) 3 Indian Journal of Legal Research.

¹⁹³ Jalaj Agarwal and Gracy Bindra, 'Domain Name Disputes and the Rising Threat of Cybersquatters' (2020) 6 Indian Journal of Law and Society.

similar system for Kazakhstan would significantly reduce the burden on courts while providing trademark owners with an accessible path to recover infringing domains.¹⁹⁴

Kazakhstan could model its system after India's INDRP, which mandates arbitration for disputes involving the .in domain.¹⁹⁵ Under such a framework, complainants would be required to prove three core elements: that the domain name is identical or confusingly similar to a protected trademark, that the respondent lacks legitimate interests in the domain name, and that the domain was registered and used in bad faith.¹⁹⁶ This structure has been praised for its clarity and effectiveness in combating cybersquatting.¹⁹⁷ Establishing a similar mechanism in Kazakhstan would ensure quicker and more consistent outcomes.¹⁹⁸

Alongside procedural reforms, it is necessary to strengthen substantive protections by introducing statutory damages for cybersquatting.¹⁹⁹ Currently, Kazakh trademark law focuses on injunctions and actual damages, which are often difficult to quantify in online infringement cases.²⁰⁰ By contrast, the U.S. Anti-Cybersquatting Consumer Protection Act (ACPA) allows courts to award statutory damages ranging from \$1,000 to \$100,000 per domain name.²⁰¹ Scholars argue that statutory damages serve as a strong deterrent and reduce the evidentiary burden on trademark owners.²⁰² Introducing a similar statutory damages framework would empower Kazakh courts to impose meaningful financial penalties on cybersquatters, enhancing deterrence.²⁰³

¹⁹⁴ Anis Ahmad and Nikki Kumar, 'Critical Analysis of the Regulatory Framework Relating to Cybersquatting in India' (2024) Prayagraj Law Review.

¹⁹⁵ Alif Muhammad Gultom, 'Domain Name under UDRP: Unregistered Trademark Protection' (2023) 5(1) Indian Journal of Legal Research.

¹⁹⁶ Ravish Ranjan, 'Trademark Infringement Issue in Cyberspace' (2022–2023) 4(6) Indian Journal of Legal Research.

¹⁹⁷ Jeetika Aggarwal and Priyanshi Bainwala, 'Cybersquatting and Trademark Infringement' (2021) 4(2) International Journal of Law Management and Humanities.

¹⁹⁸ Ioana Vasii and Lucian Vasii, 'A Framework for Improved Protection of Trademarks' (2022) 28 Journal of Law, Business and Ethics.

¹⁹⁹ Katie M Brown and Natasha T Brison, 'Think Like Adidas: Analysis of Trademark Protection Strategies' (2022) 32 Marquette Sports Law Review 445.

²⁰⁰ Julien Chaisse and Danny Friedmann, 'Law of the Digital Domain: Trademarks, Domain Names and AI' (2024) 64 IDEA: The Law Review of the Franklin Pierce Center for Intellectual Property 399.

²⁰¹ Michael Grynberg, 'Trademark Free Riders' (2024) 39 Berkeley Technology Law Journal 275.

²⁰² Stella Tsybizova, 'Problems of Legal Regulation of Domain Names: The Experience of the United States of America' (2023) Law Review of Kyiv University of Law 165.

²⁰³ Maddi Gambone, 'Branding Beyond Boundaries: Trademarks and Advertising in Augmented Reality' (2024) 9 Intellectual Property and Competition Law Journal.

Registrar obligations also require urgent reform. Registrars operating under the .kz domain should be mandated to maintain accurate WHOIS data, verify registrant identities, and cooperate fully in the enforcement of dispute resolution decisions.²⁰⁴ Without such obligations, enforcement efforts remain ineffective, as bad-faith actors often hide behind anonymized domain registrations.²⁰⁵ International models, particularly the ICANN Registrar Accreditation Agreement, impose strict duties on registrars to ensure transparency and facilitate dispute resolution.²⁰⁶ Kazakhstan's legislation could similarly impose penalties for non-compliance and incentivize responsible registrar practices.²⁰⁷

A further critical measure involves enhancing cooperation with international institutions such as WIPO and ICANN.²⁰⁸ WIPO's Arbitration and Mediation Center administers thousands of UDRP disputes annually with a high level of expertise and neutrality.²⁰⁹ Kazakhstan could formalize partnerships with WIPO to allow .kz domain disputes to be heard under WIPO's auspices, ensuring professionalism and global credibility.²¹⁰ Moreover, Kazakhstan's participation in ICANN's policymaking processes would allow the country to stay informed on evolving domain name governance and adopt international best practices.²¹¹

To complement these reactive mechanisms, Kazakhstan must also embrace proactive monitoring strategies.²¹² The creation of a domain name watch system, possibly integrated with Kazakhstan's trademark registry, would allow brand owners to receive alerts when potentially infringing domain names are registered.²¹³ Scholars note that domain

²⁰⁴ Fatih Bugra Erdem, 'The Use of Arbitration Mechanisms in Trademark as Domain Name Disputes' (2023) 31 Selçuk Üniversitesi Hukuk Fakültesi Dergisi.

²⁰⁵ A Rajeswari, 'Cyberspace and Intellectual Property: Evaluating Legal Frameworks through Space Transition Theory' (2024) 7(2) International Journal of Law Management and Humanities.

²⁰⁶ Chris A Huff, 'License and Registration: Domain Name Interpretation under US Anticybersquatting Act' (2021) 30 Information and Communication Technology Law.

²⁰⁷ Bandu Meshram and Manish Kumar Singh, 'Conventional and Modern Cyber Crimes Dynamics and Legal Countermeasures in India' (2024) 14 GNLU Journal of Law Development and Policy.

²⁰⁸ Katie M Brown and Natasha T Brison, 'Think Like Adidas: Analysis of Trademark Protection Strategies' (2022) 32 Marquette Sports Law Review 445.

²⁰⁹ Julien Chaisse and Danny Friedmann, 'Law of the Digital Domain: Trademarks, Domain Names and AI' (2024) 64 IDEA: The Law Review of the Franklin Pierce Center for Intellectual Property 399.

²¹⁰ Stella Tsybizova, 'Problems of Legal Regulation of Domain Names: The Experience of the United States of America' (2023) Law Review of Kyiv University of Law 165.

²¹¹ Maddi Gambone, 'Branding Beyond Boundaries: Trademarks and Advertising in Augmented Reality' (2024) 9 Intellectual Property and Competition Law Journal.

²¹² Jyotiranga Puzari, 'Typosquatting and Its Impact upon Intellectual Property in Cyberspace' (2023) 7(2) Journal of Intellectual Property Studies.

²¹³ Ioana Vasiu and Lucian Vasiu, 'A Framework for Improved Protection of Trademarks' (2022) 28 Journal of Law, Business and Ethics.

name monitoring is an essential preventative tool, reducing litigation and enabling swift action against infringements.²¹⁴ Government support for such services, particularly for SMEs, would broaden access to domain name protection.²¹⁵

Addressing emerging threats such as typosquatting is another vital consideration.²¹⁶ Typosquatting involves registering slight misspellings of famous trademarks to deceive users, a practice increasingly recognized as a form of cybersquatting.²¹⁷ Legal reforms should explicitly categorize typosquatting as a form of bad-faith registration, allowing for swift remedies under administrative and judicial procedures.²¹⁸ Similarly, Kazakhstan must prepare for the impact of blockchain-based decentralized domain names, which challenge traditional enforcement models.²¹⁹ Future legislation must be technologically neutral, ensuring that protections extend to new forms of digital identifiers.

²¹⁴ Arusmita Acharya, 'Revisiting Dilution as Trademark Infringement: A Comparative Law Lens' (2022) *Supremo Amicus* 26.

²¹⁵ Radhika V Bhusari and Karan R Rampure, 'Cybersquatting: A Threat to the Globalising World' (2021) 3 *Indian Journal of Legal Research*.

²¹⁶ Maddi Gambone, 'Branding Beyond Boundaries: Trademarks and Advertising in Augmented Reality' (2024) 9 *Intellectual Property and Competition Law Journal*.

²¹⁷ Julien Chaisse and Danny Friedmann, 'Law of the Digital Domain: Trademarks, Domain Names and AI' (2024) 64 *IDEA: The Law Review of the Franklin Pierce Center for Intellectual Property* 399.

²¹⁸ Stella Tsybizova, 'Problems of Legal Regulation of Domain Names: The Experience of the United States of America' (2023) *Law Review of Kyiv University of Law* 165.

²¹⁹ Ioana Vasiiu and Lucian Vasiiu, 'A Framework for Improved Protection of Trademarks' (2022) 28 *Journal of Law, Business and Ethics*.

Conclusion

The phenomenon of cybersquatting, as examined throughout this dissertation, represents a significant and growing threat to the effective enforcement of trademark rights in Kazakhstan. In a digital economy where domain names function as vital corporate assets and branding tools, the unauthorized registration of domains resembling established trademarks undermines the integrity of commerce and consumer trust. Despite Kazakhstan's existing legal mechanisms based on general trademark and unfair competition laws, these frameworks are currently ill-suited to address the speed, anonymity, and cross-border complexity of cybersquatting disputes. Therefore, to safeguard the commercial and reputational interests of trademark owners and to foster a trustworthy digital environment, Kazakhstan must undertake concrete, specific reforms that reflect successful international models while adapting them to local legal and economic contexts.

First and foremost, Kazakhstan must establish a dedicated administrative mechanism for domain name disputes, modelled closely on the Uniform Domain-Name Dispute-Resolution Policy (UDRP) created by ICANN and implemented worldwide. As analysed in Chapter 3, the UDRP provides a swift, cost-effective, and impartial method of resolving cybersquatting cases based solely on documentary evidence, typically within 60 days. By contrast, traditional civil litigation in Kazakhstan often involves protracted procedures, high costs, and uncertain outcomes, particularly when cybersquatters hide their identities or operate across borders. Implementing a UDRP-style system under the authority of KazNIC, the registry for the .kz domain, would fill this procedural gap. Domain registrants could be contractually bound to accept arbitration for trademark disputes as a condition of registration, thereby ensuring enforceability without requiring amendments to substantive law. This approach would directly enhance the accessibility of remedies for trademark owners while simultaneously reducing the judicial burden on Kazakh courts.

In tandem with procedural reforms, Kazakhstan's substantive law must be amended to specifically define cybersquatting and to codify clear standards for liability. At present, the absence of an express definition allows cybersquatters to exploit legal ambiguity, while courts must stretch traditional trademark doctrines like passing off or unfair competition to fit new digital harms. Drawing upon international models, Kazakhstan should define cybersquatting in its Trademark Law as the bad-faith registration,

use, or trafficking in domain names that are identical or confusingly similar to protected trademarks. Furthermore, legislation should specify a non-exhaustive list of bad faith factors, including offering domains for sale to rights holders, registering multiple infringing domains, providing false registration details, or diverting consumers for commercial gain. By codifying these standards, Kazakhstan would promote legal certainty, enable faster judicial assessments, and deter opportunistic registrants.

Additionally, Kazakhstan should introduce statutory damages for cybersquatting. As shown in the comparative analysis of the U.S. Anti-Cybersquatting Consumer Protection Act (ACPA), statutory damages offer several advantages: they eliminate the need to prove actual economic harm, enhance deterrence, and provide predictable relief. Given that many cybersquatters are judgment-proof or operate in jurisdictions beyond easy enforcement, statutory damages would allow Kazakh courts to impose meaningful penalties without requiring complex evidentiary proceedings. The range of damages could be calibrated to Kazakhstan's economic realities, for example, setting minimum awards equivalent to modest sums for first-time offenders, with escalating penalties for willful or repeated infringements. This system would encourage trademark owners to assert their rights while discouraging bad-faith registration practices.

To further strengthen cybersquatting enforcement, the obligations of domain registrars must be expanded and clarified through binding regulation. Registrars are pivotal actors in the domain name ecosystem, serving as the intermediaries between registrants and the registry. Thus, Kazakhstan should impose duties on registrars to maintain accurate WHOIS information, respond promptly to verified complaints of infringement, and lock domains under dispute pending resolution. Furthermore, registrars should be required to implement a "notice and takedown" system that allows trademark owners to seek temporary suspension of domains suspected of cybersquatting. Non-compliance with these obligations should trigger administrative fines or potential revocation of accreditation. By incentivizing registrar cooperation, Kazakhstan would close a major enforcement loophole that cybersquatters currently exploit to evade accountability.

Institutional strengthening must also accompany legal reforms. Kazakhstan should formalize collaboration with international bodies such as WIPO and ICANN to benefit from existing expertise and infrastructure in domain name dispute resolution. WIPO's Arbitration and Mediation

Center, in particular, has adjudicated tens of thousands of UDRP cases with consistent standards and efficiency. Kazakhstan could allow disputes involving .kz domains to be referred to WIPO panels or could seek WIPO's assistance in training domestic arbitrators. This would ensure that Kazakhstan's administrative panels operate according to international best practices while building local capacity. Moreover, active participation in ICANN's policymaking processes, such as through the Governmental Advisory Committee, would enable Kazakhstan to influence the development of global domain name governance policies and to adapt its own systems accordingly.

An additional essential reform is the establishment of proactive monitoring and preventive mechanisms. Many cybersquatting incidents could be prevented if trademark owners receive timely alerts about potentially infringing domain registrations. Kazakhstan should encourage the creation of a domain monitoring service integrated with its trademark database, enabling real-time screening of new registrations against existing trademark rights. Automated systems could flag suspicious domains for human review or trigger notifications to concerned rights holders. By detecting infringements at an early stage, such measures would enable quicker intervention and reduce the economic and reputational harm to businesses.

At the same time, legislative reforms must explicitly address emerging cybersquatting tactics, including typosquatting and abuses in decentralized blockchain domain name systems. Typosquatting, the registration of minor variants of popular domain names, remains a pervasive threat to consumers and businesses alike. Kazakhstan's trademark and domain name laws should recognize typosquatting as a distinct form of bad-faith registration and provide fast-track administrative remedies for obvious cases. Furthermore, while blockchain-based domain names (e.g., .crypto, .eth) present complex enforcement challenges due to their decentralized nature, Kazakhstan should begin by ensuring that its legal definitions of domain names and trademarks are broad enough to encompass blockchain identifiers. Although technical barriers to enforcement remain, establishing a legal foundation is a crucial first step toward adapting to technological change.

Importantly, public education and business outreach must complement legal and procedural reforms. Many small and medium-sized enterprises (SMEs) in Kazakhstan lack awareness of cybersquatting risks or the tools available to protect their brands online. Government agencies, in

partnership with business associations and legal practitioners, should organize workshops, publish guidelines, and offer practical assistance on domain name strategies. Topics should include the importance of early domain registration, the use of defensive registrations to block squatters, and guidance on filing administrative complaints. In particular, SMEs should be informed about the availability of affordable dispute resolution options, including the proposed administrative system, which would lower the cost barrier to enforcing their rights. By promoting awareness and accessibility, Kazakhstan would empower a broader base of businesses to defend their brands and contribute to a more trustworthy digital marketplace.

Moreover, Kazakhstan should explore ways to subsidize or facilitate low-cost dispute resolution for SMEs. High legal costs currently deter many smaller rights holders from pursuing action against cybersquatters, even when clear infringement exists. Options include offering reduced filing fees for administrative complaints, providing state-supported legal aid in IP disputes, or encouraging law schools and professional associations to offer pro bono assistance. Ensuring that remedies are not restricted to large corporations would align Kazakhstan's enforcement system with principles of fairness and inclusivity, supporting broader economic growth.

Finally, robust enforcement mechanisms must be complemented by transparency and accountability. Kazakhstan should require the publication of administrative panel decisions and court judgments involving cybersquatting disputes. A publicly accessible database of decisions would promote consistency, provide valuable guidance to future complainants and respondents, and enhance public trust in the system. Moreover, publishing anonymized WHOIS data for registered domain names – subject to data protection considerations – would increase accountability and discourage bad-faith registration. Transparency is a cornerstone of effective governance, and by ensuring openness in cybersquatting enforcement, Kazakhstan would demonstrate its commitment to protecting intellectual property rights in the digital sphere.

In conclusion, Kazakhstan stands at a pivotal juncture in the evolution of its digital economy. By adopting a UDRP-style administrative procedure, introducing statutory damages, strengthening registrar obligations, cooperating with international bodies, implementing proactive monitoring, addressing emerging technological threats, promoting public education, supporting SMEs, and ensuring transparency, Kazakhstan can build a comprehensive and modern framework for combating cybersquatting.

These solutions, rooted in successful international models but tailored to national realities, will significantly enhance the protection of trademarks and domain names. Implementing these measures will not only protect rights holders but also foster trust, innovation, and economic growth in Kazakhstan's online environment.

MNU Research Archive

Bibliography

Legislation and Legal Instruments

1. *Anticybersquatting Consumer Protection Act*, 15 USC § 1125(d) (US)
2. *Kazakhstan Civil Code*
3. *Kazakhstan Law on Trademarks, Service Marks and Appellations of Origin* (as amended in 2018)
4. Uniform Domain-Name Dispute-Resolution Policy (UDRP), ICANN (1999) <https://www.icann.org/resources/pages/policy-2012-02-25-en> accessed 20 April 2025

Cases and Arbitration Decisions

1. *Telstra Corporation Ltd v Nuclear Marshmallows*, WIPO Case No D2000-0003 (WIPO, 2000)
2. *Julia Fiona Roberts v Russell Boyd*, WIPO Case No D2000-0210 (WIPO, 2000)
3. *Virtual Works, Inc v Volkswagen of America, Inc* 238 F3d 264 (4th Cir 2001)
4. *Sporty's Farm LLC v Sportsman's Market, Inc* 202 F3d 489 (2nd Cir 2000)
5. *Yahoo! Inc v Akash Arora*, High Court of Delhi, 1999 IIAD Delhi 229
6. *British Telecommunications plc & Ors v One In A Million Ltd* [1999] 1 WLR 903 (CA)
7. *Harrods Ltd v Sixty Internet Domain Names* 302 F3d 214 (4th Cir 2002)

Books, Theses, and Academic Articles

1. Helfer LR and Dinwoodie GB, 'Designing Non-National Systems: The Case of the Uniform Domain Name Dispute Resolution Policy' (2001) 43(1) *William and Mary Law Review* 141 <https://scholarship.law.wm.edu/wmlr/vol43/iss1/7> accessed 20 April 2025
2. Alrawashdedh W, *Dispute Resolution Mechanisms and Trademark Cybersquatting* (PhD thesis, University of Szeged 2017) <https://doktori.bibl.u-szeged.hu/id/eprint/4093> accessed 20 April 2025
3. Rukmani Sachdeva, 'Critical Study on Trademark Infringement Related to Domain Names and Cybersquatting' (2022) 2 *Jus Corpus Law Journal*.

4. Sangeetha Lakshmi V, 'The Menace of Cybersquatting and Legal Measures' (2022) 2 Indian Journal of Integrated Research in Law.
5. Anis Ahmad and Nikki Kumar, 'Critical Analysis of the Regulatory Framework Relating to Cybersquatting in India' (2024) Prayagraj Law Review.
6. Radhika V Bhusari and Karan R Rampure, 'Cybersquatting: A Threat to the Globalising World' (2021) 3 Indian Journal of Legal Research.
7. Jalaj Agarwal and Gracy Bindra, 'Domain Name Disputes and the Rising Threat of Cybersquatters' (2020) 6 Indian Journal of Law and Society.
8. Kashish Wadhwa, 'Domain Name and Cyber Squatting' (2022) 4(3) Indian Journal of Legal Research.
9. Jeetika Aggarwal and Priyanshi Bainwala, 'Cybersquatting and Trademark Infringement' (2021) 4(2) International Journal of Law Management and Humanities.
10. Ravish Ranjan, 'Trademark Infringement Issue in Cyberspace' (2022–2023) 4(6) Indian Journal of Legal Research.
11. Alif Muhammad Gultom, 'Domain Name under UDRP: Unregistered Trademark Protection' (2023) 5(1) Indian Journal of Legal Research.
12. Ioana Vasii and Lucian Vasii, 'A Framework for Improved Protection of Trademarks' (2022) 28 Journal of Law, Business and Ethics.
13. Bandu Meshram and Manish Kumar Singh, 'Conventional and Modern Cyber Crimes Dynamics and Legal Countermeasures in India' (2024) 14 GNLU Journal of Law Development and Policy.
14. Chris A Huff, 'License and Registration: Domain Name Interpretation under US Anticybersquatting Act' (2021) 30 Information and Communication Technology Law.
15. Katie M Brown and Natasha T Brison, 'Think Like Adidas: Analysis of Trademark Protection Strategies' (2022) 32 Marquette Sports Law Review 445.
16. Jyotiranga Puzari, 'Typosquatting and Its Impact upon Intellectual Property in Cyberspace' (2023) 7(2) Journal of Intellectual Property Studies.
17. Julien Chaisse and Danny Friedmann, 'Law of the Digital Domain: Trademarks, Domain Names and AI' (2024) 64 IDEA: The Law Review of the Franklin Pierce Center for Intellectual Property 399.
18. Michael Grynberg, 'Trademark Free Riders' (2024) 39 Berkeley Technology Law Journal 275.

19. Michael Grynberg, 'AI and the "Death of Trademark"' (2024) 114 Trademark Reporter 695.
20. Stella Tsybizova, 'Problems of Legal Regulation of Domain Names: The Experience of the United States of America' (2023) Law Review of Kyiv University of Law 165.
21. Maddi Gambone, 'Branding Beyond Boundaries: Trademarks and Advertising in Augmented Reality' (2024) 9 Intellectual Property and Competition Law Journal.
22. Fatih Bugra Erdem, 'The Use of Arbitration Mechanisms in Trademark as Domain Name Disputes' (2023) 31 Selçuk Üniversitesi Hukuk Fakültesi Dergisi.
23. A Rajeswari, 'Cyberspace and Intellectual Property: Evaluating Legal Frameworks through Space Transition Theory' (2024) 7(2) International Journal of Law Management and Humanities.
24. Samiksha, 'Domain Name Related Dispute in IPR in India' (2023) 5(2) Indian Journal of Legal Research.
25. Ioana Vasiu and Lucian Vasiu, 'A Framework for Improved Protection of Trademarks' (2022) 28 Journal of Law, Business and Ethics.
26. Fatih Bugra Erdem, 'The Use of Arbitration Mechanisms in Trademark as Domain Name Disputes' (2023) 31 Selçuk Üniversitesi Hukuk Fakültesi Dergisi.
27. Jyotiranga Puzari, 'Typosquatting and Its Impact upon Intellectual Property in Cyberspace' (2023) 7(2) Journal of Intellectual Property Studies.
28. Julien Chaisse and Danny Friedmann, 'Law of the Digital Domain: Trademarks, Domain Names and AI' (2024) 64 IDEA: The Law Review of the Franklin Pierce Center for Intellectual Property 399.
29. Michael Grynberg, 'Trademark Free Riders' (2024) 39 Berkeley Technology Law Journal 275.
30. Stella Tsybizova, 'Problems of Legal Regulation of Domain Names: The Experience of the United States of America' (2023) Law Review of Kyiv University of Law 165.
31. Maddi Gambone, 'Branding Beyond Boundaries: Trademarks and Advertising in Augmented Reality' (2024) 9 Intellectual Property and Competition Law Journal.

Journal and Online Publications

1. Bajpai Y and Jha AR, 'Pursuing Cybersquatting as a Trademark Infringement under the IP Regime' (IJLSI, 2024) <https://ijlsi.com/paper/pursuing-cybersquatting-as-a-trademark-infringement-under-the-ip-regime/> accessed 20 April 2025
2. Gasimova C, 'Domain Name and Trademark Infringement: Cybersquatting in the Digital Age' (2023) ResearchGate https://www.researchgate.net/publication/368237606_Domain_name_and_trademark_infringement_Cybersquatting_in_the_digital_age accessed 20 April 2025
3. Karote H, 'Cybersquatting and Trademark Issues: Uniform Domain Resolution Policy' (JLRJS, 2022) <https://jlrjs.com/wp-content/uploads/2022/02/9.-Harsh-Karote-1.pdf> accessed 20 April 2025
4. Lakshmi SV, 'The Menace of Cybersquatting and the Available Legal Measures to Mitigate Abuse of Domain Names' (IJIRL, 2022) <https://ijirl.com/wp-content/uploads/2022/01/THE-MENACE-OF-CYBERSQUATTING-AND-THE-AVAILABLE-LEGAL-MEASURES-TO-MITIGATE-ABUSE-OF-DOMAIN-NAMES.pdf> accessed 20 April 2025
5. Mukhammad A, 'Trademark Protection and Cybersquatting Issues' (Lexology, 2019) <https://www.lexology.com/library/detail.aspx?g=61040c99-6f5c-4b70-b396-26a402df5966&utm> accessed 20 April 2025
6. Sangeetha Lakshmi V, 'The Menace of Cybersquatting and the Available Legal Measures to Mitigate Abuse of Domain Names' (IJIRL, 2022) <https://ijirl.com/wp-content/uploads/2022/01/THE-MENACE-OF-CYBERSQUATTING-AND-THE-AVAILABLE-LEGAL-MEASURES-TO-MITIGATE-ABUSE-OF-DOMAIN-NAMES.pdf> accessed 20 April 2025
7. Shriyaa Z, 'Regulation of Cybersquatting: An Analysis of the Legal Framework in India, the UK and the USA' (JLRJS, 2023) <https://jlrjs.com/wp-content/uploads/2023/10/104.-Shriyaa-Zubin.pdf> accessed 20 April 2025
8. Curtin TJ, 'The Name Game: Cybersquatting and Trademark Infringement on Social Media Websites' (2010) *Brooklyn Journal of Law and Policy* <https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1107&context=jlp> accessed 20 April 2025

9. Singh B, 'Cybersquatting in the Digital Era' (2018) *Supremo Amicus*, 7 <https://supremoamicus.org/wp-content/uploads/2018/08/Volume-7.....-amended.pdf> accessed 20 April 2025
10. Vashisht D and Gupta R, 'Cybersquatting in the Age of Digital Era' (SSRN, 2023) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4480434 accessed 20 April 2025
11. Karanickolas M, 'The New Cybersquatters: The Evolution of Trademark Enforcement in the Domain Name Space' (2020) SSRN https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3528237 accessed 20 April 2025
12. Pantov V, 'The Prevention of Cybersquatting in Europe: Diverging Approaches and Prospects for Harmonization' (2014) SSRN https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2427582 accessed 20 April 2025
13. Sukhanov A.V. 'Проблемы использования доменных имен и товарных знаков в РФ' (2016) <http://kafinf.ssla.ru/wp-content/uploads/2016/04/Суханов-1.pdf> accessed 20 April 2025
14. Sukhareva AE and Turkin RE, 'Сравнительное исследование механизмов защиты от киберсквоттинга в России и США' (IPC Magazine, 2017) <https://ipcmagazine.ru/articles/1729023/> accessed 20 April 2025

Blogs and Practitioner Commentary

1. Zhanadilov B, 'Trademark Squatting in Kazakhstan: From Russia with Love' (Kluwer Trademark Blog, 21 August 2024) <https://trademarkblog.kluweriplaw.com/2024/08/21/trademark-squatting-in-kazakhstan-from-russia-with-love/> accessed 20 April 2025
2. Zhanadilov B, 'Trademark Squatting in Kazakhstan: From Russia with Love (Part II)' (Kluwer Trademark Blog, 2 October 2024) <https://trademarkblog.kluweriplaw.com/2024/10/02/trademark-squatting-in-kazakhstan-from-russia-with-love-part-ii/> accessed 20 April 2025
3. Zhanadilov B, 'Cybersquatting in Kazakhstan: The Bobcat Trademark Dispute' (Kluwer Trademark Blog, 27 February 2025) <https://trademarkblog.kluweriplaw.com/2025/02/27/cybersquatting-in-kazakhstan-the-bobcat-trademark-dispute/> accessed 20 April 2025

4. Nurmagambetov Z, 'Overview of Trademark Protection in the Countries of Central Asia' (Bolotov & Partners, 2021) <https://bolotovip.com/publication/overview-of-trademark-protection-in-the-countries-of-central-asia/> accessed 20 April 2025
5. Pavel Gross-Днепров, 'Доменное имя и товарный знак: кто кого с точки зрения закона?' (pavelgross.ru, 2023) <https://pavelgross.ru/articles/domennoe-imya-i-tovarnyj-znak-kto-kogo-s-tochki-zreniya-zakona/> accessed 20 April 2025
6. EUIPO, 'Focus on Cybersquatting: Monitoring and Analysis – Executive Summary' (2021) https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Cybersquatting_Study/2021_Focus_on_Cybersquatting_Monitoring_and_Analysis_Study_ExSum_en.pdf accessed 20 April 2025