P-ISSN: 2709-6254	Journal of Development and Social Sciences	Oct-Dec 2022, Vol. 3, No. 4
O-ISSN:2709-6262	http://dx.doi.org/10.47205/jdss.2022(3-IV)03	[19-30]

Journal of Development and Social Sciences
www.jdss.org.pk

RESEARCH PAPER

Cybersquatting: Violation of Trade Marks, Intellectual Property Laws in Pakistan

Naheeda Ali

Assistant Professor, Department of Law, University of the Punjab, Gujranwala Campus, Punjab, Pakistan

***Corresponding Author:** naheeda.ali@pugc.edu.pk

ABSTRACT

Internet has substantially expanded, and it has become a widespread platform for commerce and trading. In the case of a company, goodwill refers to the intangible asset. A company's ability to differentiate its goods and services from those offered by other companies in the same industry and to convey any existing goodwill in the market is facilitated by using a trademark. In recent years, many companies have begun to reach out to their clients using online marketplaces such as social media and websites. The domain name of an internet website plays an important function in assisting clients in recognizing a certain company when interacting in cyberspace. The process operates on a "first-come, first-serve basis," any person or company may try to acquire the domain names of already-established enterprises. A practice known as "Cybersquatting", occurs when individuals register domain names with the fraudulent object of selling to already established companies and operating a company in their name by misinterpreting their domain name. This research examines the notion of cybersquatting in Pakistan, and its effects in globalized society, and how World Intellectual Property Organization (WIPO) has been playing a significant role in preventing the act of cybersquatting.

KEYWORDS Arbitration, Cybersquatting, Domain Name, Passing Off, Trademarks

Introduction

When it was first conceived in the 1960s, the Internet was supposed to function as part of a project known as ARPANET. During that time, it was referred to as a computer network, and it enabled the countries and their military departments to communicate with one another in the event of a disaster. Soon after the end of the cold war, the computer network project known as ARPANET became known as the Internet. Many civilian users who were not affiliated with the military began utilizing the network. Due to its high cost, the Internet had a relatively limited user base, with most of its users affiliated with educational institutions and government-run organizations. The price of having internet access and a computer has gradually become more affordable (Deo & Deo, 2019). The number of people who use the Internet has been steadily growing over the last several years. Only lately have many corporations and enterprises begun to see its potential as a tool for doing business and reaching customers and clients in several counties. The registration of a domain name is necessary for commercial enterprises in order for them to have a presence on the Internet, which offers a unique virtual area for communication and is quite expansive. On the Internet, a domain name serves the same purpose as an address by allowing anybody to get to a certain website. For obvious reasons, companies and trade businesses want to use their current trade names and trademarks as domain names to be recognized. This is done for digital marketing, allowing these companies to reach their target audience for business with greater visibility (King, 1999).

Few people take competitive advantage by registering the domain names of reputed trademarks or names similar to those of such trademarks with the malicious intention of creating confusion in the mind of any reasonable customers, misleading them, and

conducting business with the goodwill of the reputed trademark owners. The registrars do domain name registration on a first-come, first-serve basis. Suppose these individuals are not engaged in commercial activity. In that case, they may have the mala fide intention of vending the registered domain name to their rival or proprietor himself at an expense. The act that these individuals are engaging in is known as cybersquatting. The Internet has introduced a whole new dimension to the process of digitization. In today's increasingly digitalized world, it is more challenging for intellectual property owners to safeguard their assets and prevent unauthorized use. The Internet gives its users much power, but with that power comes much responsibility. Because of this, it is the user's responsibility to protect himself and his property and take preventative measures against illegal acts. However, suppose a user fails to fulfil this responsibility. In that case, it is the responsibility of the state and governing bodies to have a framework in the form of rules and regulations to prevent other users from violating it. Nevertheless, what happens if the actions occur outside the states' limits? After conducting in-depth research, the researchers have arrived at the following conclusions to address this issue and others like it (Sood & Nakta, 2022).

Material and Methods

Qualitative Research Methodology has been used to gain a deeper comprehension of the subject matter under investigation in this study. For this research, data such as legislation and judicial decisions of courts from countries such as Pakistan, the United States of America (USA), the United Kingdom (UK), and Australia were studied. Additionally, legal data from the World Intellectual Property Organization (WIPO), The Internet Corporation for Assigned Names and Numbers (ICANN), and the Uniform Domain-Name Dispute Resolution Policy (UNDRP) were taken into consideration. In order to acquire in-depth information, properly evaluate the data, and accomplish the goals of the research project, secondary data in the form of a variety of research publications, journals, and reference books were also consulted.

Intellectual Property Rights: Trademarks

The term "intellectual property" refers to an intangible property resulting from the creations of the human mind. This property type may be employed in commercial settings and includes literary, musical, and creative works, designs, pictures, symbols, inventions, and so on. When these intellectual assets are safeguarded by legal protections, a system known as intellectual property rights has been established (IPR). The person who created or invented the work has exclusive ownership of these rights. It makes it easier for people to get recognition and financial reward for the time, effort, money, and expertise that went into creating such a property. It is an exclusive right since it restricts others from utilizing or replicating the product or innovation in question for a certain amount of time. This strikes a balance between the interests of creators and the general community and encourages creators to further develop their particular works or innovations by conferring legal protection on them. Copyright, patents, trademarks, industrial designs, geographical indication, and other intellectual property rights are some of the many categories of intellectual property rights (Sachdeva, 2021).

A sign or symbol that can distinguish the products and amenities of one entity from other entities is referred to as a trademark. Whether or not a company has a good reputation, doing business in cyberspace on the internet presents several possibilities and dangers, particularly for fortifying intellectual property rights such as trademarks. For consumers to recognize and get in touch with a company in cyberspace, that company must have a domain name, which is most likely to be recognized as the same thing as the company's trademark. This is because many companies and consumers who use the internet are excited about the prospect of engaging in commerce or trade. Therefore, in order to make it possible for the current consumers and customers of the established business, some of whom may not be able to have a direct physical relationship with the company but may still choose to engage in commerce or trade with them, to do so online (De Silva et al., 2021).

Domain Names

All internet means, whether websites or information files, hold their address. This address is referred to as the Uniform Resource Locator (URL), and its unique to that resource (URL). The domain names are a component of the addresses mentioned above, and they are allotted to one of the computers to facilitate the provision of a service in cyberspace. When opposed to the actual Internet Protocol (IP) address of a specific website, which is comprised of numbers, domain names are the form of internet addresses that are easier to remember. Domain names are also known as the form of internet addresses that can be recognized (Yatsyk & Shkelebei, 2018). Because these numbers are difficult to remember, it is connected with any domain name that the person who registers it desires to register in the name of. Domain names, often known as human-friendly forms of internet addresses, are what the World Intellectual Property Organization (WIPO) considers to be how users detect websites on the internet (Ranjan, 2022). The Domain Term System (DNS) is the name given to the worldwide addressing system that is used to assign and convert domain names into Internet Protocol (IP) addresses and vice versa (DNS). In recent years, domain names have increasingly become connected with trademarks to make it easier for people to recognize a company's brand when it appears on the internet. For instance, the sequence of letters and numbers "www.abcd.com" would be recognized as the domain name, while the sequence of numbers "1.2.3.4.5" would be recognized as the IP address. In this case, the letters "abcd" would be helpful for others in identifying it as a firm or any trademark linked with a company whose name is similar to the one being discussed (Maravela, 2021).

Types of Domain Names

Domain names might be broken down into three categories, each based on a different level in the hierarchical structure. These categories are as follows:

Top Level

One may determine which part of a domain name is the top level by looking at the part that comes at the very end, after the last dot. It is the section that comes after the domain names and is the very last one. Use this website as an example: www.intellectualpropertylawers.com/.net/.eu/.in. There are two categories of names that may be used for websites' top-level domains (TLDs): generic top-level domains (gTLD) and country-code top-level domains (ccTLD). The generic top-level domain (gTLD) denotes the sector in which the domain name owner's activities are focused; for example, ".com" can be used for any purpose, ".edu" is used for educational institutions, and ".biz" is used for commercial enterprises. The country code top-level domain (ccTLD) denotes the territory or country in which the domain name owner operates; for example, "pk" is for Pakistan, and ".uk" is for the United Kingdom (Cheng, Chai, Zhang, Lu, & Du, 2021).

Second Level

One may easily identify the second level of a domain name as the one that comes before the last dot, which is to say, right before the level considered to be the highest level of the domain name. The second domain name level is subject to the vast majority of the disagreements around domain names. For instance, if the URL were "www. intellectualpropertylawers.com," the intellectual property lawyers, portion of the address would be understood to refer to the second domain name level (Zeng, Chen, Zang, & Tsang, 2021).

Third Level

It is possible to identify the 3rd level of a domain name as the one situated to the left of the second level domain. This level is also referred to by its other term, which is the subdomain. It is often used to represent a distinct segment of the website, particularly when the domain name's owner has multiple departments in its organisation; nevertheless, it is not always present since it is not always present to indicate the different sections of the website. For instance, in the domain name www.help.intellectualpropertylawers..com, "help" would stand for the third level in the domain name hierarchy (Chiba et al., 2018).

In 2011, ICANN introduced the "New gTLD Program." This initiative aimed to assist individuals and businesses in registering their domain names with the new gTLD, which introduced new extensions that did not have any particular meaning in relation to a particular geographical location. For example, a book in addition to trademarks that were written in a script other than English, such as Chinese.

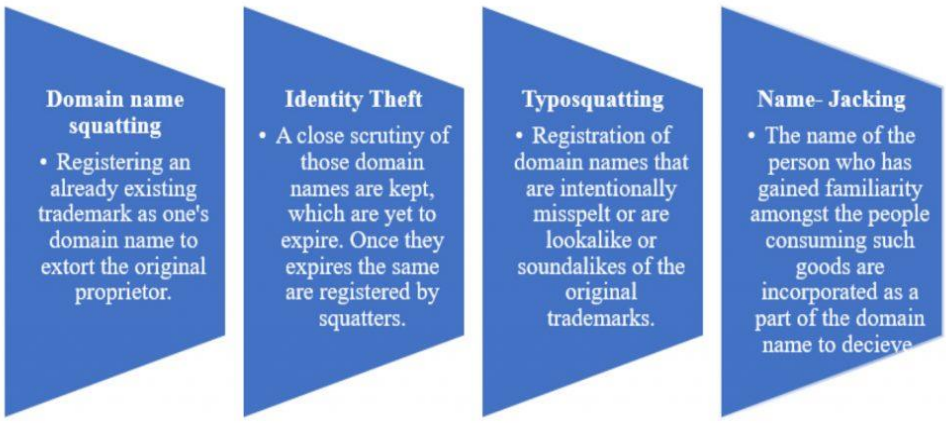
Cybersquatting

The practice of registering a trademark of a business or any other company, as a domain name on the internet by any third party other than the trademark owner, with a motive to vend a domain name to such a rightful proprietor of such trademark to get profit; or registering such domain name not in good faith, with mala fide intention to trade and conduct business in the trade name and goodwill of such business or such organisation owned by rightful trademark owner is identified as cybersquatting. The act of cybersquatting was first implemented and is widely acknowledged to have begun at the same time as the World Wide Web (www.). The vast majority of companies were completely unprepared to take advantage of the commercial prospects that might be found on the internet and lacked any expertise necessary to do business in this manner. Before many businesses and well-known companies recognised the need for domain names, individuals and entities had already registered them with the intent of vending them back to rightful proprietors of trademarks. This occurred before many businesses, and well-known companies even used the internet. Cybersquatters targeted well-known businesses such as Panasonic, Avon, and Hertz, among others (Oguama, 2021).

Because trademark holders place a high priority on registering their domain names, the likelihood of cybersquatters attempting to make a profit off the sale of domain names is currently quite low. This is because registering a domain name is one of the most important steps in protecting a trademark. Cybersquatters' major goal these days is to unjustly do business on the internet at the expense of the goodwill and trade name of the legitimate owners of the trademarks. Many methods of cybersquatting are being implemented (Wahdani, 2021).

Types of Cybersquatting

The following is a list of the four most common forms of cybersquatting that are seen in the online environment at the moment (Chandra & Bhatnagar, 2019):



Typo Squatting

Making a deliberate typographical mistake in a domain name that is about to be registered is an example of "typosquatting," which refers to registering domain names that are close to but not the same as prominent or well-known trademarks. These mistakes are general, and there is a possibility that a significant number of visitors would input wrongly, leading them to be sent to the website owned by cybersquatters. For this kind of cybersquatting, the squatters would have to place bets on the general public's typos when typing in a certain domain name (Vranken & Alizadeh, 2022).

Identity Theft

The cybersquatters monitor the expiration of the domain names owned by famous or well-known trademark owners with the help of various means such as online applications. Until ownership of the domain name expires, which is in the name of the rightful trademark owner, the cybersquatters register it in their name to deceive the visitors of the website into believing that the website is being managed by the same original trademark owner, who had the domain name registered in the first place (Yang et al., 2021).

Name Jacking

The most impacted folks by this form of cybersquatting are celebrities and other such \ public personalities. Cybersquatters register domain names using the names of well-known public figures to target the people who are expected to visit the website that serves as the famous person's official cyberspace handle. This is done in order to capitalize on the traffic that is expected to visit that website. They are often utilized to enhance traffic on the website of the cyber squatter, which may or may not have any connection to the material that the famous person has posted on their site(Majmudar, 2021).

Inversion of the Cybersquatting Process

In this kind of cybersquatting, the cybersquatters would threaten the legitimate owner of the trademark, who had obtained the domain name lawfully after registering it. They would pressure the legitimate proprietor to transfer the domain name into the name of the cybersquatters. If they are not properly aware of it and look forward to not wasting their money and time if any form of domain name dispute process arises, many genuine domain name owners will fall victim to these types of cybersquatting. When they engage in criminal activities, such as cybersquatting, those who do these acts intend harm. The following is a list of the methods of monetization used by these cyber squatters (Sood & Nakta, 2022):

Domain Parking

In order to create online traffic on the website of the cyber squatters from the website of the legitimate domain name owner, the person who has such a purpose will adopt ways that will redirect the traffic to his website, which contains adverts.

Holding Domain Names

For ransom, the cyber squatters would distribute ransomware to limit access to the data on the website of the legitimate owner, and they would then demand that the legitimate owner pay some ransom.

Affiliate Marketing

This would affect the website of the rightful owner in such a way that the traffic on his website would be redirected to the web pages or website with products on the sales from which the cyber squatters would be benefitted. This would hurt the website of the rightful owner.

Hit Stealing

This technique often involves stealing the traffic that is visiting the website of the legitimate owner, which has been cyber squatted and redirecting that traffic to the rival's website. This has the effect of negatively impacting the business of the trademark owner.

Scams

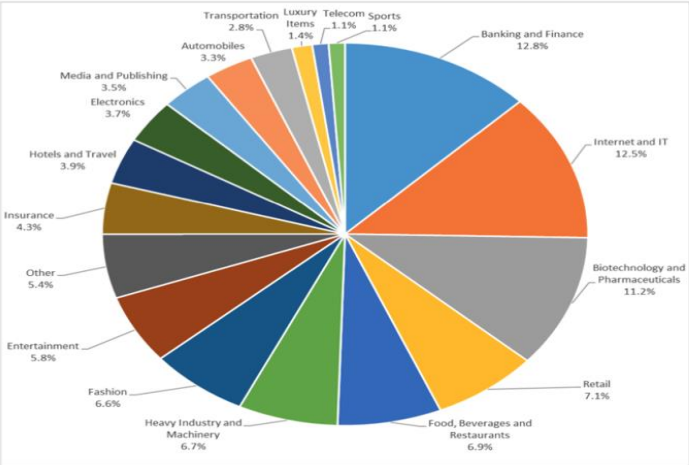
This is one of the most common, but it is still an effective illicit activity, and it involves frauds committed using credit cards or online banking. They could email the people they are trying to reach bogus notices that they have won a lottery, and they might gather people's personal information in a manner that would eventually result in identity theft in the digital domain (Dhawan, 2020).

Literature Review:

Uniform Domain Name Dispute Resolution Policy (UDRP)

The Internet Corporation for Assigned Names and Numbers (ICANN) established the Uniform Name Dispute Resolution Policy (UDRP) in 1999. (ICANN). The aim of creating it was to settle disputes about the ownership of domain names, which was the motivation for its creation. Disputes may be settled in a manner that is both extremely economical and highly successful, thanks to this approach. The threshold of 50,000 cybersquatting cases has just been passed. These cases were submitted to the Arbitration and Mediation Centre of the World Intellectual Property Organization (WIPO) per the rules. These cases originated from more than 180 nations (Lee, 2020).

Annex 11: Areas of WIPO Domain Name Complainant Activity (2021)



The Uniform Domain Name Dispute Resolution Policy (UDRP) is responsible for resolving disputes brought before it by trademark holders against the registrants of domain names. These registrants have registered a domain name identical to the trade name or the trademark of the rightful owner without having any rights or legitimate interests in doing so and have done so in bad faith. There is the potential for disagreements to arise in situations in which both parties are the owner of the trademark. If this occurs, the disagreement must be settled using fair and objective criteria to determine who obtained ownership of the trademark first or whether there was a valid reason to register the trademark in question (Lee, 2020).

World Intellectual Property Organization (WIPO): Since 1999, trademark owners have been addressing WIPO's Arbitration and Mediation Centre with complaints that their domain names are registered by cybersquatters mala fide to attack their trade name or trademark. WIPO has seen a growth in the number of incidents of cybersquatting, particularly after the pandemic, Covid-19, since a significant number of businesses have moved their operations online and working from home has been the norm for everyone. WIPO just achieved the milestone of 50,000 UDRP-based cybersquatting cases during this pandemic. This provides us with an indication of how rapidly this problem is growing (De Silva et al., 2021).

What measures is Pakistan taken to combat cybersquatting?

There is currently no formal domain name protection law in Pakistan that addresses the issue of cybersquatting. In situations involving cyber-squatting, Pakistan's courts enforced the Trademarks laws. A trademark has legal protection under the statutes of Pakistan in which it is registered or under any other laws in which it may be registered. On the other hand, given that the Internet does not impose any geographical restrictions on its users, customers may register a domain name regardless of where they are physically located. Because of the possibility for worldwide networking, a domain name must be exclusive over the whole planet. However, the laws of a single country may not be enough to properly resolve a dispute involving a domain name and provide a solution for the problem. This is the remedy for trademark infringement; in order for a trademark owner to make use of this remedy, the owner of the trademark must first get it registered. If a trade mark is not registered, the remedy of passing off can be used (Maravela, 2021).

The IN Domain Dispute Resolution Policy

Pakistan's domain dispute policy. Pakistan's TLD is "pk." PK Registry has released PK-Dispute Resolution Policy to resolve issues (INDRP). Therefore, INDRP and its Rules of

Procedure are resolved.in domain issues. The Uniform Domain Name Dispute Resolution Policy (UDRP) is not applicable in Pakistan, although the Pakistan Domain Name Dispute Resolution Policy (INDRP) was created using UDRP ideas.

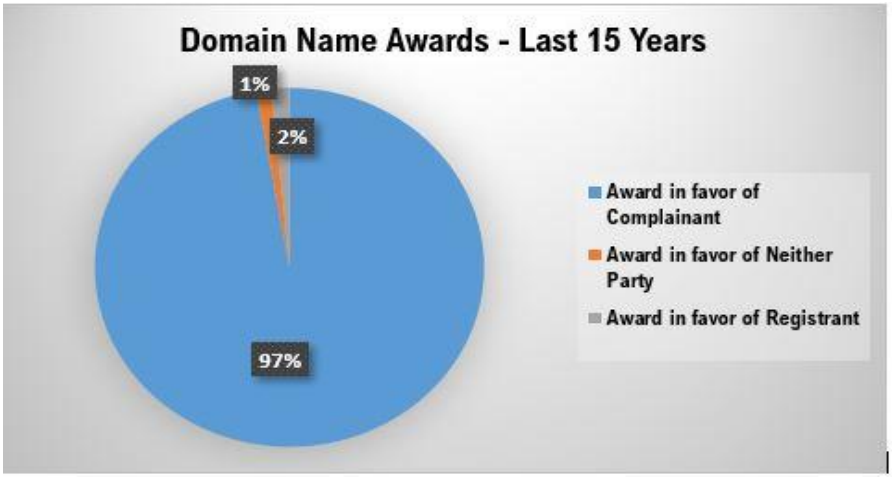
According to INDRP regulations, a complaint can be filed with the Registry if the domain name in conflict is identical or confusingly similar to the Complainant's trademark or service mark, the Registrant has no rights or legitimate interests in the domain name, and the domain name is registered and used in bad faith.

The Internet Domain Name Disagreement Resolution Policy (INDRP) specifies handling a domain name dispute. After the Registry has been provided with the complaint, it will choose an Arbitrator from a list of candidates it has kept. When an arbitrator has been chosen, the PK Registry will inform the parties by communicating with them. As soon as the Arbitrator has the complaint in their possession, they have only three days to notify the Respondent.

An arbitrator will be chosen to preside over the proceedings, and they will be run by the Arbitration and Conciliation Act, the INDRP, and the INDRP norms of Procedure. The complaint, the Respondent, and the.PK Registry shall get a copy of the Arbitrator's ruling. After proceedings have been initiated, the decision of the Arbitration must be rendered within sixty days. This time limit may be pushed back to thirty days, but the Arbitrator must produce a written explanation for the extension (Aggarwal & Bainwala, 2021).

All papers, responses, applications, rejoinders, and orders must be filed.PK Registry to preserve records and ensure transparency. No in-person hearings will be held unless the Arbitrator finds, in his sole discretion, that they are needed to resolve the complaint. If the arbitrator orders in-person hearings, these will be held. According to the Policy, in-person hearings will not occur unless the Arbitrator demonstrates that one is essential in his or her sole discretion and great authority (Pratama & Rafii, 2021).

Before an arbitrator is appointed and arbitration procedures begin, the Complainant's remedies are restricted to cancelling or transferring the Registrant's domain names. Even if the Complainant wins in Arbitration, this happens. The Arbitrator may award costs. It is against policy for a Registrar to transfer a "disputed domain name registration" to another owner for 15 business days after the proceeding or during the dispute until the party to whom the domain name registration has been transferred agrees, in writing, that such a transfer will not be prohibited under this policy. This phase starts after or during the Procedure (Oguama, 2021).



Internet Corporation of Assigned Names and Numbers (ICANN) Procedure

In 1999, the Internet Corporation for Assigned Names and Numbers (ICANN) established and implemented the Uniform Domain Name Dispute Resolution Policy to resolve the debate surrounding domain names. Arbitration of a disagreement, as opposed to court action, is the likely conclusion of this hypothetical situation. The following are some grounds that can be used to file a lawsuit for cybersquatting. A domain name that matches a complainant's trademark or service mark. The domain owner has no valid rights or interests. Bad faith registration and usage of the domain. For the complaint to be effective, it is necessary to provide evidence that all of the elements stated above are accurate. If the complaint successfully demonstrates any of the grounds indicated above, the domain name in issue will either be transferred to the person who filed the complaint or terminated. On the other hand, by the U.D.R.P., the plaintiff is not eligible for any monetary or financial remedy (King, 1999).

Initiating action under the ACPA

Allow trademark owners to file a lawsuit in high Court against individuals accused of cybersquatting. If the trademark owner wins the lawsuit, the Court must then order the return of the trademark to the trademark owner. In some situations, the cyber squatter may be held financially responsible for the harm caused by their actions. To prohibit cybersquatting, a trademark owner must prove: The registrant wanted to benefit from the trademark. The domain name was identical or confusingly similar to the brand when it was initially registered. The domain name is likely to create customer confusion and is. The trademark qualifies for high court protection since it is distinctive, and the owner was the first to use it commercially (Bhusari & Rampure, 2022).

Analysis & Recommendation

The act of cybersquatting is related to the infringement of the trademark or trade name of a company that is already registered and has goodwill that was acquired through hard work. The crime is committed against the business that has already been registered. Cybersquatters have taken advantage of this crisis to take part in illegal activities by not just selling the domain names to the trademark owners but by initiating business in their name and deceiving users with various types of frauds. The press release of the WIPO evidenced this, and we can deduce that it is a crime that has gradually increased in number. However, during the pandemic, as more activities were performed by various companies and businesses online, the cybersquatters took advantage of this (Ali & Khan, 2021).

As more and more businesses move their activities online, there has been an uptick in the practice of cybersquatting. We want more stringent laws to call to account those involved in this heinous crime. In order to assist in preventing activities that are against the law, Pakistan's laws need to include a specific section on cybersquatting. For the legislature to effectively deal with the growing number of cybersquatting cases, different legislation will need to be introduced. In addition, the plaintiff ought to be allowed the potential to recover statutory damages due to the huge loss caused by such unlawful activities (Wang, Bai, Grzeslo, Peng, & Jayakar, 2021).

There is a need for the I.N.D.R.P. to be redesigned; the I.N.D.R.P. should be transformed into law rather than just remaining as a policy that must be adhered to. One of the drawbacks of a policy is that it does not require obedience; as a result, the regime is lax in its application of the policy. When combating this threat, the United States of America has consistently been one step ahead of other nations. It has created distinct regulations in order to manage the situations that are appropriately linked to cybersquatting. There is a need for a specific law that is enforced in a manner that is more stringent than what is currently being done in other nations, such as Australia and the United Kingdom, to regulate the instances (Ranjan, 2022).

Conclusion

As a result of what has been discussed, we have concluded that cybersquatting poses a significant risk to all types of organizations, regardless of their size, whether they are big, medium, or tiny start-ups. These companies have suffered monetary setbacks and damage to their reputation in the marketplace. Cyber squatters are registering even more domain names to take advantage of legal company owners as a direct consequence of the ease with which they may access the Internet. Since its inception, the Uniform Domain Name Dispute Resolution Policy (U.D.R.P.) has been used by WIPO to resolve more than 50,000 domain name disputes and 91,000 domain names. The number of new cases filed in 2020 was 4,204, representing a 16 per cent rise over the previous year's total. It has been hypothesized by the World Intellectual Property Organization (WIPO) that the outbreak of covid-19 is mostly responsible for the increase in online trademark infringements such as phishing and sales of counterfeit products. The proliferation of computer technology and the ease with which users may connect to the Internet have had a significant influence on commerce all over the globe, leading to the development of new markets and other opportunities. However, it has also "allowed" other people to violate intellectual property laws by using their work without permission.

As a result, there are several adjustments that may be made to the laws and regulations that are currently in place, or a new legislation should be developed specifically to deal with the offence of cybersquatting in Pakistan. Electronic Transaction Ordinance (ETO) 2002, Electronic / Cyber Crime Bill 2007, Prevention of Electronic Crimes Act (PECA) 2016, Electronic Transaction Ordinance (ETO) 2002, Pakistan signed a Service Level Agreement, (SLA) with World Intellectual Property Organization (WIPO) on 7th March 2022 are the laws at question here. In order to adequately address the ever-increasing number of instances of cybersquatting that have been reported in Pakistan, separate legislation similar to that which has been enacted in the United States of America is urgently required.

References:

Agarwal, A. (2022). Information Technology vis-a-vis Human Rights: An Analytical and Legal Approach. *Issue 2 Int'l JL Mgmt. & Human., 5*, 106. Aggarwal, J., & Bainwala, P. (2021). Cybersquatting and Trademark Infringement. *Issue 2 Int'l JL Mgmt. & Human., 4*, 1220.

Ali, N., & Khan, K. I. (2021). Legal framework for compulsory licensing: a solution to the conflict of intellectual property rights and intellectual monopoly. *International Journal of Public Law and Policy, 7*(2), 122-133.

Bhusari, R. V., & Rampure, K. R. (2022). Cybersquatting: A Threat To The Globalising World. *Indian Journal of Law and Legal Research, 3*(2), 2283-2304.

Castro, C. F. d. P., Silva, D. A. A., Souto, G. A., & Albrecht, N. F. (2022). Domain Names And Intellectual Property: Law And Economics Reflections On Dispute Settlement. *Revista Direito GV, 18*.

Chandra, R., & Bhatnagar, V. (2019). Cyber-squatting: a cyber crime more than an unethical act. *International Journal of Social Computing and Cyber-Physical Systems, 2*(2), 146-150.

Cheng, Y., Chai, T., Zhang, Z., Lu, K., & Du, Y. (2021). Detecting malicious domain names with abnormal whois records using feature-based rules. *The Computer Journal*. 65(9), 2262–2275, https://doi.org/10.1093/comjnl/bxab062

Chiba, D., Akiyama, M., Yagi, T., Hato, K., Mori, T., & Goto, S. (2018). DomainChroma: Building actionable threat intelligence from malicious domain names. *computers & security, 77*, 138-161.

Christie, A. F., Gloster, J., & Goddard, S. (2019). An Empirical Analysis of 15 Years of Australian Domain Name Disputes. *Australian Intellectual Property Journal, 30*(1), 4-25.

De Silva, R., Nabeel, M., Elvitigala, C., Khalil, I., Yu, T., & Keppitiyagama, C. (2021). *Compromised or {Attacker-Owned}: A Large Scale Classification and Study of Hosting Domains of Malicious {URLs}.* Paper presented at the 30th USENIX security symposium (USENIX security 21).

Deo, S., & Deo, S. (2019). Cybersquatting: Threat to domain name. *International Journal of Innovative Technology and Exploring Engineering, 8*(6).

Dhawan, V. (2020). Cyber Squatting: Need for Comprehensive and Standalone Legislation. *Issue 4 Int'l JL Mgmt. & Human., 3*, 1114.

Huff, C. A. (2021). License and registration: how both property and contract legal frameworks fall short on interpreting domain name registration under the US Anticybersquatting Act. *Information & Communications Technology Law, 30*(3), 363-379.

King, S. H. (1999). The Law That It Deems Applicable: ICANN, Dispute Resolution, and the Problem of Cybersquatting. *Hastings Comm. & Ent. LJ, 22*, 453.

Lee, I. (2020). The Uniform Domain Name Dispute Resolution Policy (UDRP): not quite arbitration, but satisfying? *Research handbook on intellectual property and digital technologies*: Edward Elgar Publishing.

Majmudar, S. (2021). Evocative Analysis of Intellectual Property Rights. *Jus Corpus LJ, 2*, 205.

Maravela, M. (2021). Applicable Law in Domain Name Arbitrations. *Rom. Arb. J., 15*, 91.

Oguama, L. (2021). Domain Name Theft–Cybersquatting: What It Means for Trade Marks. *Available at SSRN 3837629*.

Pratama, B., & Rafii, M. (2021). *Implementing trademark law in domain name cases.* Paper presented at the IOP Conference Series: Earth and Environmental Science.

Ranjan, R. (2022). Cyber Squatting–The Digital Version of Passing Off. *Journal of Legal Studies & Research, 8*(2), 1-12.

Roy, A., & Marsoof, A. (2015). 'Bad Faith'and'Rights or Legitimate Interests' Under Domain Name Law—Emerging Themes from the UDRP and auDRP.

Roy, A., & Marsoof, A. (2016). A critical and comparative review of auDRP and UDRP domain name decisions. *The Journal of World Intellectual Property, 19*(5-6), 203-237.

Sachdeva, R. (2021). Critical Study on Trademark Infringement related to Domain Names and Cybersquatting. *Jus Corpus LJ, 2*, 427.

Sood, E., & Nakta, V. (2022). Cybersquatting: Need for Protection of Domain Names in the Realm of Cyberspace *Handbook of Research on Cyber Law, Data Protection, and Privacy* (pp. 120-136): IGI Global.

Vinayakumar, R., Soman, K., & Poornachandran, P. (2018). Detecting malicious domain names using deep learning approaches at scale. *Journal of Intelligent & Fuzzy Systems, 34*(3), 1355-1367.

Vranken, H., & Alizadeh, H. (2022). Detection of DGA-Generated Domain Names with TF-IDF. *Electronics, 11*(3), 414.

Wahdani, F. (2021). The Legal Character Of Domain Names'cybersquatting. *Law, Society & Organisations*, 10 (VI). 23-41.

Wang, R. Y., Bai, Y., Grzeslo, J., Peng, R. X., & Jayakar, K. (2021). *The diffusion of National Domain Name Dispute Resolution Policies: A Network Approach*. *SSRN 3898264*.

Yang, L., Liu, G., Liu, W., Bai, H., Zhai, J., & Dai, Y. (2021). Detecting Multielement Algorithmically Generated Domain Names Based on Adaptive Embedding Model. *Security and Communication Networks, 2021*.

Yatsyk, T., & Shkelebei, V. (2018). Investigation of new forms of cyber crime (phishing and cybersquatting). *Серія ПРАВО*. Випуск 53. Том 2, 121-123

Zeng, Y., Chen, X., Zang, T., & Tsang, H. (2021). *Winding path: Characterizing the malicious redirection in squatting domain names.* Paper presented at the International Conference on Passive and Active Network Measurement.