Xinxin X. (2025) COPYRIGHT PROTECTION STRATEGIES FOR BROADCASTING SPORTS EVENTS: A COMPREHENSIVE ANALYSIS. Revista Internacional de Medicina y Ciencias de la Actividad Física y el Deporte vol. 25 (99) pp. 200-214.
DOI: https://doi.org/10.15366/rimcafd2025.99.014

ORIGINAL

COPYRIGHT PROTECTION STRATEGIES FOR BROADCASTING SPORTS EVENTS: A COMPREHENSIVE ANALYSIS

Xie Xinxin

School of Journalism and Communication, Shaanxi Normal University, Xi'an, Shaanxi, 710119, China
E-mail: sylvia930105@163.com

Recibido 07 de Marzo de 2024 **Received** March 07, 2024
Aceptado 10 de Octubre de 2024 **Accepted** October 10, 2024

ABSTRACT

In today's digital and globalized context, the live broadcast of sports events has become the focus of public attention, but it also raises many copyright-related issues. The broadcast of sports events not only involves the event itself, but also covers the broadcast, comment, recording and use of related content. This study provides an in-depth analysis of the cybersecurity challenges faced by sports meeting broadcasting and live streaming platforms. It examines the applicability and limitations of the existing legal framework in protecting these platforms from cyber threats. Through case studies, the research identifies common forms of illegal live streaming and online broadcasting infringement and assesses the effectiveness of relevant legal regulations. Finally, the paper offers recommendations for improving the legal framework and enhancing international cooperation to address the growing complexity of cybersecurity threats, ensuring the fairness of sports meetings and the operational security of broadcasting platforms.

KEYWORDS: Sports Meeting Broadcasting, Cybersecurity, Live Streaming Platforms, Legal Research, Online Broadcasting Infringement.

1. INTRODUCTION

With the development of technology, especially the rise of the Internet and new media, the traditional copyright law is facing many challenges. Live broadcasts of sports events often need to be broadcast on multiple platforms, which complicates the ownership and use of copyright. The digital transformation of large-scale sports meetings has dramatically reshaped the

way these events are broadcasted and consumed. With advancements in information and communication technologies, sports broadcasting platforms have evolved into complex systems that not only deliver live event coverage but also provide an interactive experience for global audiences (Petrović et al., 2015). This transformation has brought significant benefits to the sports industry, enhancing the viewer experience and expanding the reach of sports meetings. However, it has also introduced new challenges, particularly in the realm of network security and legal protections. Sports meeting broadcasting platforms are characterized by rapid development cycles, high system density, and short lifecycles, which are driven by the unique demands of large-scale events (Yang et al., 2012). These platforms must deliver high-quality, uninterrupted service within tight timeframes, often involving the integration of numerous systems across various domains. The operational complexity is further compounded by the involvement of multiple stakeholders, including domestic and international suppliers, each with their own responsibilities and requirements. Moreover, the platforms are primarily cloud-based, with centralized protection mechanisms; however, the decentralized nature of maintenance and management responsibilities adds to the overall security challenge. The network assets, spread across numerous venues, each with its own specific conditions, must also meet stringent compliance requirements both domestically and internationally (Gadinis, 2015). Figure 1 shows the live broadcasting control room at the Olympics.

Figure 1: Olympics Live Broadcasting Control Room in Action

Since the Sydney 2000 Olympic Games, the threat landscape for international sports meetings has become increasingly severe. Network security incidents during these events have highlighted the vulnerability of sports broadcasting platforms to cyber-attacks. These attacks have evolved in sophistication, becoming more targeted, employing polymorphic malware, and increasing in scale. The attacks have also become more industrialized, with organized groups systematically targeting specific components of the broadcasting infrastructure. For example, during the Beijing 2008 Olympics,

over 600,000 network attacks were recorded, including 10,000 worm virus incidents, 3,000 DDoS attacks, over 100 database intrusion attempts, and more than a dozen Trojan backdoor installations. Similarly, the London 2012 Olympics faced nearly 250 million cyber-attacks, with critical systems like the timing and scoring systems being compromised. The Rio 2016 Olympics experienced over 500 million attacks (Szabolcs et al., 2022), and the PyeongChang 2018 Winter Olympics saw its official website and ticketing system crippled by large-scale attacks (Li, 2021), including phishing emails that led to database breaches. These incidents underscore the escalating nature of cyber threats facing international sports meetings. The motivations behind these attacks are varied and complex, ranging from political agendas and economic incentives to the desire to disrupt and manipulate public opinion. Malicious entities often exploit the high visibility of sports meetings to advance their objectives, whether by stealing sensitive information, such as athlete and official data, or by compromising financial systems to gain illicit profits (Grow & Shackelford, 2020). In some cases, cyber-attacks have even been used to influence the outcome of events, such as by tampering with timing systems or arbitrating video feeds, thus undermining the integrity of the competition and fueling public mistrust. The network security challenges faced by international sports meetings are distinct from those encountered in other sectors due to the unique characteristics of these events (Horne & Manzenreiter, 2006). Firstly, the client base for these events is exceptionally diverse and concentrated. Major international sports meetings, particularly those on the scale of the Olympics or World Cup, attract a wide array of participants, including athletes, team officials, VIPs, technical officials, media representatives, broadcasters, spectators, and event staff. This diverse group brings with it a variety of network usage patterns and security needs, creating numerous potential entry points for cyber-attacks (Al-Mohannadi et al., 2016). The challenge is further exacerbated by the fact that these users often come from different countries, each with its own network standards and security protocols, making it difficult to establish a cohesive defense strategy. Secondly, the IT infrastructure of international sports meetings is inherently complex. The architecture typically spans several layers, from the network layer, which includes dedicated networks for management, competition, security, and broadcasting, to the application layer, which supports essential functions such as event management, timing and scoring, results publication, and media services. These systems are highly interdependent, with tight coupling between different components, meaning that a security breach in one system can quickly cascade to others. For example, an attack on the media service platform could potentially affect the timing and scoring systems, leading to inaccurate results being published (Yao et al., 2017), which could, in turn, trigger widespread public dissatisfaction and damage the event's credibility. Moreover, the rapid adoption of new technologies such as cloud computing, 5G, the Internet of Things (IoT), and blockchain has further complicated the network security landscape for sports meetings (Omolara et al., 2022). While these

technologies offer significant benefits, such as enhanced connectivity, real-time data processing, and secure transactions, they also introduce new vulnerabilities. The integration of IoT devices, for instance, extends the attack surface by adding numerous interconnected devices that are often difficult to secure adequately. Similarly, the use of cloud-based services centralizes data storage and processing, making it a prime target for large-scale attacks. The widespread use of social media and digital payment systems during these events also introduces additional risks, as these platforms can be exploited for phishing, fraud, and other malicious activities. The economic stakes associated with sports broadcasting have also grown significantly in recent years, as evidenced by the multi-billion-dollar deals for broadcasting rights (Bell, 2005). This economic value has made sports broadcasting a lucrative target for cybercriminals, who seek to exploit the digital distribution of event coverage. Unauthorized streaming, in particular, has become a pervasive issue, with individuals and websites illegally broadcasting live sports meetings without the proper licenses. These illegal streams not only undermine the financial viability of legitimate broadcasters but also pose significant security risks. Websites that aggregate and distribute unauthorized streams often expose users to malware and other threats, compounding the security challenges faced by broadcasting platforms. Despite the rapid evolution of sports broadcasting technology, legal protections have struggled to keep pace. In many jurisdictions, including China, the legal framework for sports broadcasting rights remains underdeveloped. There is often a lack of clear legal definitions and protections for sports broadcasting, leaving broadcasters and event organizers without adequate recourse in the face of infringement. This legal gap is particularly problematic in the digital age, where the lines between live broadcasting, streaming, and recording have blurred. The absence of robust legal protections makes it difficult to enforce broadcasting rights, leading to a proliferation of unauthorized streams and other forms of infringement. This paper seeks to explore the intersection of network security and legal protections in the context of sports meeting broadcasting platforms. By examining the current state of network security for these platforms, the legal challenges associated with broadcasting rights, and the evolving threat landscape, this research aims to provide a comprehensive analysis of the issues at hand. Furthermore, the paper will offer recommendations for strengthening the legal and regulatory framework to better protect sports broadcasting platforms in an increasingly digital and interconnected world. Through a detailed examination of case studies, legal frameworks, and technological advancements, this research will contribute to the ongoing discourse on how to safeguard the integrity and security of sports broadcasting in the face of emerging cyber threats.

2. Current State of Cybersecurity in Sports Meeting Broadcasting Platforms

In recent years, major sports meetings have increasingly become prime

targets for cyberattacks, reflecting the growing sophistication and frequency of these threats. Table 1 provides an overview of notable cyberattacks on various global sports meetings, highlighting the scale and impact of these incidents.

Table 1: Overview of Cyberattacks on Major Sports meetings

MAJOR SPORTS MEETING	INTENSITY OF CYBERATTACKS	CYBERATTACK INCIDENTS
2022 BEIJING WINTER OLYMPICS	Over 2.4 billion types of cyberattacks detected	According to reports, 5,782 security vulnerabilities were discovered and fixed, and 54 types of malicious samples were found.
2022 FIFA WORLD CUP IN QATAR	6,346,000 login attempts were detected by Microsoft	Numerous phishing emails sent in an attempt to steal personal data.
2021 TOKYO OLYMPICS	4.5 billion cyberattacks detected	The official website was attacked 1.4 billion times, with DDoS attacks, malware, and multiple phishing attempts.
2018 PYEONGCHANG WINTER OLYMPICS	Opening ceremony directly attacked	Key systems, including IPTV, official website, and other major systems were affected. Attackers used a fake domain to launch attacks.
2016 RIO DE JANEIRO OLYMPICS	Over 5 billion cyberattacks detected	The official website was hit by DDoS attacks reaching speeds of 500 Gbps.
2014 FIFA WORLD CUP IN BRAZIL	Associated websites hit by DDoS attacks, leading to service disruptions	High-profile individuals targeted, affecting their ability to access the internet.
2012 LONDON OLYMPICS	2.5 billion cyberattacks detected	Power and other critical systems targeted by DDoS attacks, causing operational disruptions.
2008 BEIJING OLYMPICS	2 billion cyberattacks detected	An average of 11 million cyberattacks occurred daily.

2.1 Analysis of the Cyberattack Trends

The data from recent years indicates a sharp rise in both the frequency and intensity of cyberattacks targeting major international sports meetings. This trend underscores the need for enhanced cybersecurity measures to protect the integrity of these events. Notably: Increased Volume of Attacks: The number of cyberattacks detected during these events has escalated to billions, reflecting the scale at which attackers are now operating. For example, the 2022 Beijing Winter Olympics saw over 2.4 billion cyberattacks, while the 2021 Tokyo Olympics experienced 4.5 billion attacks. This increase is likely driven by the greater use of digital platforms and the heightened global visibility of these

events. Diverse Attack Vectors: The nature of the attacks has diversified, including Distributed Denial of Service (DDoS) attacks, phishing attempts, and malware distribution. These attack vectors target not just the public-facing components of the events, such as websites, but also critical infrastructure, including power systems and IPTV services. The 2016 Rio Olympics, for example, experienced DDoS attacks that reached speeds of 500 Gbps, highlighting the scale of the threat. Targeting of Key Systems: Cyberattacks have increasingly focused on disrupting key systems integral to the operation of these events. The 2018 PyeongChang Winter Olympics is a case in point, where the opening ceremony and essential systems like IPTV and the official website were directly targeted. The attackers used sophisticated methods, including creating fake domains, to deceive users and exploit vulnerabilities. Persistent Security Vulnerabilities: The repeated discovery of security vulnerabilities across different events, such as the 5,782 vulnerabilities found during the 2022 Beijing Winter Olympics, emphasizes the ongoing challenge of securing these events. Despite efforts to patch these vulnerabilities, the sheer number and variety of attacks make it difficult to protect against every possible threat. Global Impact and Response: The global nature of these events means that cyberattacks can have far-reaching consequences, affecting not only the host country but also international stakeholders, including broadcasters, sponsors, and participants. The response to these threats requires coordinated efforts across multiple jurisdictions and sectors to ensure comprehensive protection. The trend towards increasingly sophisticated and large-scale cyberattacks on major sports meetings highlights the critical importance of robust cybersecurity measures. As these events continue to rely heavily on digital technologies, the need for proactive and adaptive security strategies becomes ever more pressing. Stakeholders must collaborate to strengthen defenses, identify and mitigate vulnerabilities, and ensure the safe and successful execution of these globally significant events.

2.2 Legal Security Challenges

In the context of escalating technological risks, the cybersecurity challenges faced by sports meeting broadcasting platforms are also accompanied by significant legal hurdles. Existing cybersecurity laws and regulations often struggle to keep pace with the rapid evolution of technology, leading to insufficient legal protections and even legal voids in some areas. Cross-Border Data Compliance: International sports meetings typically involve multiple countries and regions, making cross-border data transmission unavoidable. However, the data protection laws and cybersecurity standards vary widely between countries, imposing significant compliance pressures on sports meeting broadcasting platforms. These platforms must not only comply with their home country's laws but also adhere to regulations from other countries, such as the European General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) in the United States. This

complex legal environment increases the operational costs and legal risks for the platforms. Lagging Legal Frameworks: In many countries, the legal protection of sports broadcasting rights is still relatively underdeveloped. Existing laws often lack clear definitions, protection scopes, and criteria for identifying infringements related to sports broadcasting rights, rendering them ineffective in addressing new forms of infringement in the digital age. For example, activities such as unauthorized live streaming and unlicensed content sharing are not yet explicitly regulated in the legal systems of some countries, making it difficult for broadcasting organizations to seek legal recourse. Challenges in Defining Liability: Sports meeting broadcasting platforms involve multiple stakeholders, including event organizers, broadcasters, technology providers, and audiences. When a cybersecurity incident occurs, determining the legal liability of each party often becomes a contentious issue. Due to the complexity and opacity of cyberattacks, identifying the source of the attack and the responsible party typically requires considerable time and resources, which not only prolongs the resolution of disputes but also may prevent the affected parties from receiving timely compensation.

2.3 Current State of Platform Security Management

In the face of increasingly complex cybersecurity threats, sports meeting broadcasting platforms generally face significant challenges in security management. Although most platforms have established basic cybersecurity measures, they often fall short when it comes to defending against high-level cyberattacks. Inadequate Security Measures: While some large platforms have deployed traditional security measures such as firewalls, Intrusion Detection Systems (IDS), and data encryption, these measures are often insufficient against the growing complexity of cyberattacks. For instance, the scale and sophistication of DDoS attacks have continuously increased, rendering traditional firewalls and load balancers ineffective in defending against such threats. Lack of Incident Response Capabilities: Quick incident response is crucial to minimizing damage and restoring services during a cybersecurity event. However, many platforms lack well-developed incident response plans, event detection mechanisms, and response protocols, making it difficult to react effectively in the aftermath of a cyberattack, thereby exacerbating the impact of the incident. Weak Cybersecurity Awareness: The weak cybersecurity awareness among internal personnel is another widespread issue. Cybersecurity is not solely the responsibility of the IT department but requires the participation of all staff. Due to the lack of effective security training, some employees may inadvertently become targets for attackers, such as through phishing emails that lead to the disclosure of sensitive information. Therefore, enhancing cybersecurity awareness across the entire organization is crucial. Insufficient Collaboration with Legal Departments: Effective collaboration with legal departments is essential in addressing complex cybersecurity threats. However, many platforms fall short in their cooperation with legal departments

on issues of legal compliance and incident handling, placing them at a disadvantage when dealing with cyberattacks and legal disputes. Establishing a close collaborative relationship with legal departments can help platforms better address cybersecurity challenges and reduce legal risks. In conclusion, sports meeting broadcasting platforms are currently facing severe challenges in terms of cybersecurity. The complexities at the technical, legal, and management levels put these platforms at a disadvantage when confronting cyberattacks. To ensure the smooth operation of sports meetings and the secure operation of broadcasting platforms, comprehensive measures must be taken across technical, legal, and managerial domains to address the increasingly sophisticated cybersecurity threats.

3. Analysis of the Existing Cybersecurity Legal Framework

The cybersecurity landscape is rapidly evolving, particularly in the context of sports meeting broadcasting platforms, which face unique challenges due to the high-profile nature of their operations and the complexity of their technical infrastructure. To mitigate the risks posed by cyber threats, it is crucial to understand and analyze the existing legal frameworks governing cybersecurity. This section provides an in-depth analysis of the current cybersecurity legal framework, focusing on its applicability to sports meeting broadcasting platforms, its strengths, and its limitations.

3.1 International Cybersecurity Legal Frameworks

International sports meetings often involve cross-border data transfers and operations, necessitating compliance with multiple legal frameworks. Several key international regulations have significant implications for sports meeting broadcasting platforms: General Data Protection Regulation (GDPR): The GDPR, implemented by the European Union in 2018, is one of the most comprehensive data protection regulations globally. It applies to any organization that processes the personal data of individuals within the EU, regardless of where the organization is based. For sports meeting broadcasting platforms, the GDPR imposes stringent requirements on data protection, including the necessity of obtaining explicit consent from users for data processing, ensuring data portability, and implementing robust data security measures. The regulation's extraterritorial reach means that any platform broadcasting sports meetings to EU citizens must comply with its provisions, which can involve significant operational changes and compliance costs. California Consumer Privacy Act (CCPA): The CCPA, effective since January 2020, is a key piece of legislation in the United States that enhances privacy rights for California residents. Similar to the GDPR, the CCPA grants individuals the right to know what personal data is being collected about them, to whom it is being sold or disclosed, and the right to access and delete their data. For sports meeting broadcasting platforms that collect data from viewers in

California, compliance with the CCPA is mandatory. This includes providing transparent information about data practices, enabling opt-out options for data sales, and ensuring that data protection measures are in place to prevent unauthorized access. Budapest Convention on Cybercrime: The Budapest Convention, adopted by the Council of Europe in 2001, is the first international treaty aimed at addressing internet and computer crime. It provides a comprehensive framework for national legislation on cybercrime and fosters international cooperation in the investigation and prosecution of such crimes. While not all countries are signatories, the convention influences global standards on cybersecurity. For sports meeting broadcasting platforms, the convention's focus on criminalizing unauthorized access, data interference, and system attacks is particularly relevant, as it offers a legal basis for addressing cyberattacks on their systems (Stern et al., 2023).

3.2 Domestic Cybersecurity Laws and Regulations

Sports meeting broadcasting platforms must also comply with domestic cybersecurity laws, which vary significantly from country to country. These laws often impose specific requirements that must be integrated into the platform’s operations to ensure legal compliance: China’s Cybersecurity Law: Enacted in 2017, China's Cybersecurity Law represents one of the most stringent national frameworks for internet security. The law emphasizes the protection of critical information infrastructure, which includes systems that support major public services and key industries such as telecommunications and finance. Sports meeting broadcasting platforms operating in China must adhere to strict data localization requirements, which mandate that data collected within China must be stored domestically. Additionally, the law requires platforms to undergo regular security assessments and to cooperate with government authorities during cybersecurity investigations. The law’s emphasis on data sovereignty and national security reflects China’s broader approach to cybersecurity, which prioritizes control over data and the protection of national interests. United States Cybersecurity Information Sharing Act (CISA): CISA, passed in 2015, encourages the voluntary sharing of cyber threat information between the private sector and the federal government. The law aims to improve the collective cybersecurity posture by facilitating timely and actionable intelligence sharing. For sports meeting broadcasting platforms in the United States, participating in information sharing can help enhance their threat detection capabilities. However, the voluntary nature of the law means that platforms must balance the potential benefits of sharing information with the risks of exposing sensitive operational details. India’s Information Technology Act (ITA): The ITA, initially enacted in 2000 and amended several times since, serves as the primary legal framework for cybersecurity in India. It addresses various aspects of cybercrime, including unauthorized access, data breaches, and identity theft. For sports meeting broadcasting platforms operating in India, compliance with the ITA involves ensuring that robust security measures are in

place to protect against data breaches and cyberattacks. Additionally, the ITA includes provisions on data protection and privacy, which require platforms to implement appropriate safeguards when handling user data.

3.3 Limitations and Challenges in the Existing Legal Framework

While the existing cybersecurity legal frameworks provide a foundation for protecting sports meeting broadcasting platforms, they also present several limitations and challenges: Fragmentation and Inconsistency: The global nature of sports meeting broadcasting means that platforms must navigate a patchwork of legal requirements across different jurisdictions. The lack of harmonization between international and domestic laws can lead to significant compliance burdens, as platforms must adapt their operations to meet the varying standards and regulations. This fragmentation not only increases operational costs but also creates legal uncertainties, particularly when conflicting requirements arise. Lagging Legal Protections for Sports Broadcasting Rights: Many legal frameworks have not kept pace with the rapid technological advancements in sports broadcasting. For example, laws governing broadcasting rights often lack clear provisions for addressing new forms of infringement, such as unauthorized live streaming or illegal content distribution on digital platforms. This gap in legal protections leaves broadcasting platforms vulnerable to piracy and other forms of intellectual property theft, with limited recourse available through existing legal channels. Challenges in Enforcement: Even when robust legal frameworks are in place, enforcement can be a significant challenge, particularly in cases of cross-border cybercrime. The decentralized and anonymous nature of many cyberattacks makes it difficult to identify perpetrators and bring them to justice. Additionally, differences in legal systems, investigative capacities, and law enforcement priorities between countries can hinder international cooperation, complicating efforts to prosecute cybercriminals and recover damages. Evolving Threat Landscape: The rapid evolution of cyber threats often outpaces the development of legal frameworks, leading to gaps in protection. For instance, the rise of sophisticated ransomware attacks, state-sponsored cyber espionage, and the use of AI-driven attacks present new challenges that existing laws may not adequately address. This dynamic threat environment requires continuous updates to legal frameworks, as well as adaptive strategies by sports meeting broadcasting platforms to stay ahead of emerging risks.

4. Case Analysis

With the rapid development of internet technology and the rise of the online live streaming industry, the methods of broadcasting sports meetings have undergone significant changes. However, this trend has also brought about various forms of infringement and cybersecurity issues, particularly during major international sports meetings such as the Olympics. This section

analyzes specific cases of online live streaming infringement and online broadcasting infringement, highlighting the legal and cybersecurity challenges currently faced by sports meeting broadcasting.

4.1 Case Analysis of Online Live Streaming Infringement and Cybersecurity

The emergence of the online live streaming industry has provided unprecedented opportunities for unauthorized broadcasters, while also introducing new cybersecurity risks. The 2008 Beijing Olympics marked the advent of the "Portal Olympics Era," where viewers first accessed the Olympics through the internet, with online media playing a significant role. By the time of the 2016 Rio Olympics, the online live streaming industry had flourished, and the Olympics became a focal point for live streaming. However, this surge in popularity also led to an increase in online live streaming infringements and associated security risks. During the Rio Olympics, many live streaming platforms, without authorization from the International Olympic Committee (IOC), sent teams of streamers to cover the event. Although these platforms did not have broadcasting rights, streamers attracted viewers by showcasing their experiences in Rio and informally streaming from event venues. This behavior constituted a new form of infringement: live streaming events from venues using mobile devices.

These devices, being small and discreet, allowed streamers to broadcast from the audience without being easily detected. This not only violated broadcasting rights but also posted significant cybersecurity threats. For instance, unauthorized live streams might be transmitted over insecure networks, increasing the risk of data breaches and the spread of malware. Cybersecurity issues are particularly acute in such cases of infringement. When unauthorized devices connect to public or unsecured networks, they are highly vulnerable to cyberattacks. Attackers can exploit vulnerabilities in these devices to implant malware or even hijack the live stream, which could lead to broader cyberattacks. Such attacks may not only degrade the quality of the event's live coverage but also cause serious security consequences for the streaming platform and its users. Typically, online live streaming infringements are managed by the online service providers (i.e., the live streaming platforms). When a platform detects that a streamer is engaging in behavior that infringes on broadcasting rights, it usually takes measures to stop the infringement. However, due to the limited regulatory capacity of the platforms, and the covert and decentralized nature of these infringements, they often go undetected or unaddressed in a timely manner. This issue highlights the limitations of current laws in addressing emerging forms of infringement, especially in the realm of cybersecurity, where effective regulation and protection of broadcasting rights are pressing concerns.

4.2 Case Analysis of Online Broadcasting Infringement and Cybersecurity

Online broadcasting infringement is a more traditional form of infringement, but with the advancement of internet technology, particularly the widespread use of P2P technology, these practices have become more complex and prevalent. Unauthorized broadcasters intercept legitimate broadcasting signals or footage and stream them online without authorization, directly infringing on the rights of the broadcasting rights holders and introducing significant cybersecurity risks. A typical case occurred during the 2008 Beijing Olympics when Century Dragon Company illegally streamed a live broadcast of the Germany vs. Brazil women's soccer match from CCTV's Olympic Channel on its website without authorization. CCTV filed a lawsuit, and the court ultimately ordered Century Dragon to pay RMB 200,000 in damages. This case not only illustrates the legal consequences of illegal online broadcasting but also reveals related cybersecurity issues. The act of intercepting broadcast signals often involves invasive technologies, which themselves constitute a form of cyberattack, potentially compromising the security of the legitimate media's systems and threatening the security of the entire network infrastructure. Another notable case involves the Canadian website iCraveTV, which provided users with online access to sports meetings broadcast by U.S. television networks. Due to the unauthorized nature of these broadcasts, a coalition of U.S. media companies sued iCraveTV. The court ruled in favor of the plaintiffs, ordering iCraveTV to pay damages and temporarily banning it from streaming any of the plaintiffs' content. This case highlights the complexity of cross-border online broadcasting infringements and the cybersecurity challenges they present. Unauthorized broadcasting activities often spread through unmonitored channels, increasing the risks of malware distribution, data breaches, and other cyber threats. The widespread use of P2P technology has further exacerbated these cybersecurity issues. Unauthorized broadcasters use distributed networks to intercept and disseminate broadcast signals, making traditional regulatory and legal enforcement methods less effective. Additionally, P2P networks themselves are vulnerable to exploitation by hackers to distribute malicious content or launch denial-of-service (DDoS) attacks, which can compromise the operational security of legitimate broadcasting platforms.

4.3 Implications of the Case Analysis

The analysis of these cases demonstrates that online live streaming and broadcasting infringements are not only legal issues but also pose significant cybersecurity risks. These cases expose the inadequacies of current legal frameworks in addressing emerging technologies and infringement practices, and they underscore the importance of strengthening both legal protections and cybersecurity measures. First, as the online live streaming industry continues to grow, laws need to be more clearly defined and enhanced to protect the

broadcasting rights of sports meetings. This includes stricter legal regulations and enforcement mechanisms specifically targeting unauthorized live streaming using portable devices. Additionally, platforms must enhance their cybersecurity measures to ensure that live stream content is not tampered with or hijacked. Second, in response to the widespread use of P2P technology, regulatory bodies need to improve their cybersecurity monitoring capabilities, combining technological and legal approaches to effectively curb unauthorized broadcasting activities. Furthermore, the complexity of cross-border infringement cases necessitates stronger international cooperation in both legal and cybersecurity domains to jointly combat and prevent online broadcasting infringements. In conclusion, the issues of online live streaming and broadcasting infringements are becoming increasingly severe and are accompanied by significant cybersecurity risks. This calls for concerted efforts from lawmakers, enforcement agencies, and industry participants to create a more effective protection framework that safeguards the legal broadcasting rights of sports meetings and the integrity of the market, while also addressing the growing complexities of cybersecurity threats. Different countries and regions have different laws and regulations on the copyright of live sports events, and international cooperation and conflicts have gradually emerged. A study of national legislation and practice in this field will help to find a more effective protection path. Emerging technologies, such as blockchain and artificial intelligence, offer new possibilities for copyright protection. The application of these technologies can improve the efficiency of copyright management and reduce the occurrence of infringement.

5. Recommendations for Enhancing Legal Protections

To address these limitations and challenges, several steps can be taken to enhance the cybersecurity legal framework for sports meeting broadcasting platforms:

International Harmonization of Cybersecurity Laws: Efforts should be made to harmonize cybersecurity regulations across different jurisdictions, particularly in areas such as data protection, incident reporting, and cross-border data transfers. This would reduce the compliance burden on global platforms and create a more predictable legal environment.

Updating Legal Protections for Digital Broadcasting: Legal frameworks need to be updated to address the unique challenges posed by digital broadcasting, including the protection of intellectual property rights in the context of live streaming and online content distribution. Clearer definitions and stronger enforcement mechanisms are necessary to safeguard broadcasting rights in the digital age.

Strengthening International Cooperation: Enhancing international

cooperation in the investigation and prosecution of cybercrimes is essential. This could involve the creation of more robust legal agreements between countries to facilitate information sharing, joint investigations, and the extradition of cybercriminals.

Adaptive Legal Frameworks: Given the rapidly evolving nature of cyber threats, legal frameworks should be designed to be adaptive and responsive to new developments. This might include the establishment of regulatory bodies tasked with monitoring emerging threats and proposing timely updates to cybersecurity laws. In conclusion, while the existing cybersecurity legal frameworks provide a valuable foundation for protecting sports meeting broadcasting platforms, there is a clear need for further development and adaptation. By addressing the limitations and challenges identified above, these frameworks can be strengthened to better protect against the growing array of cyber threats facing this critical sector.

Acknowledgement

Project supported by the Foundation for Key Philosophy and Social Science Program of Ministry of Education, China (Grant No.21JZD010).

REFERENCES

Al-Mohannadi, H., Mirza, Q., Namanya, A., Awan, I., Cullen, A., & Disso, J. (2016). Cyber-attack modeling analysis techniques: An overview. 2016 IEEE 4th international conference on future internet of things and cloud workshops (FiCloudW),

Bell, T. (2005). Qualitative Analysis of Revenue Sharing in Professional Sports Broadcasting Using Network Theory.

Gadinis, S. (2015). Three pathways to global standards: Private, regulator, and ministry networks. *American Journal of International Law*, *109*(1), 1-57.

Grow, N., & Shackelford, S. J. (2020). The sport of cybersecurity: How professional sports leagues can better protect the competitive integrity of their games. *BCL Rev.*, *61*, 473.

Horne, J., & Manzenreiter, W. (2006). An introduction to the sociology of sports mega-events. *The sociological review*, *54*(2_suppl), 1-24.

Li, M. X. (2021). *The Preparation for the Winter Olympic Games: The Soft Power of China's Citizens Created China's Global Promotion* Regent University].

Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., & Arshad, H. (2022). The internet of things security: A survey encompassing unexplored areas and new insights. *Computers & Security*, *112*, 102494.

Petrović, L. T., Milovanović, D., & Desbordes, M. (2015). Emerging technologies and sports events: Innovative information and communication solutions.

Sport, Business and Management: An International Journal, *5*(2), 175-190.

Stern, G., Psycharakis, S. G., & Phillips, S. M. (2023). Effect of high-intensity interval training on functional movement in older adults: a systematic review and meta-analysis. *Sports Medicine-Open*, *9*(1), 5.

Szabolcs, M., Nagy-Tóth, N. Á., Dávid, L. D., Gogo, A. F. C., & Bujdosó, Z. (2022). The role of sports policing and tourism safety at the summer Olympics. *Sustainability*, *14*(10), 5928.

Yang, L., Su, G., & Yuan, H. (2012). Design principles of integrated information platform for emergency responses: the case of 2008 Beijing Olympic Games. *Information Systems Research*, *23*(3-part-1), 761-786.

Yao, Y., Viswanath, B., Cryan, J., Zheng, H., & Zhao, B. Y. (2017). Automated crowdturfing attacks and defenses in online review systems. In *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security* (pp. 1143-1158).