Governance of Illicit and Gray Industries on the Internet in the Context of Common Prosperity

Tao Wang, Guangxuan Chen* and Shanshan Jiang

Zhejiang Police College, Hangzhou, 310053, China

*1223208809@qq.com

Abstract. In the current information age, the Internet has become a vital driver of socio-economic development. However, it has also given rise to a series of black and grey market activities online, posing new challenges to social governance and public security. With China's full-scale advancement of common prosperity, the focus of governance has shifted toward building a fair, just, stable, and orderly society. According to a report by the Internet Society of China on the scale of the black and grey market, there are currently over two million[1] practitioners in this field in China, with an average age of 23, and a market scale exceeding 110 billion yuan. Therefore, in-depth research on how to govern the Illicit and Gray Industries on the Internet under the common prosperity framework is of great significance for promoting the modernization of public security work and meeting practical needs. This study focuses on the governance of black and grey internet industries, aligning with cutting-edge developments in public security technologies and responding to practical policing demands. By analyzing typical cybercrime cases from the Ministry of Public Security, the paper explores patterns of technological iteration and governance challenges. Through systematic research on the characteristics and spread of black and grey industries, this study advocates for dynamic legislation, the decentralization of smart policing technologies, and interdepartmental data sharing to construct a governance system aligned with the goals of common prosperity. It also proposes effective governance models and technological strategies to contribute to the establishment of a safe, stable, and prosperous social environment.

Keywords: Common Prosperity; Illicit and Gray Industries on the Internet; Governance Challenges; Countermeasures.

1 Introduction

The rapid development of the Internet has profoundly transformed economic growth, social interaction, and governance models. While the digital economy injects new vitality into achieving common prosperity, it also brings challenges such as cybercrime, data breaches, and the rise of illicit and gray industries. These hidden and evolving threats undermine cybersecurity, social fairness, and sustainable development, posing serious obstacles to the realization of a fair and orderly digital society.

© The Author(s) 2025
B. Majoul et al. (eds.), *Proceedings of the 2025 11th International Conference on Humanities and Social Science Research (ICHSSR 2025)*, Advances in Social Science, Education and Humanities Research 945,
https://doi.org/10.2991/978-2-38476-440-2_157

In the context of promoting common prosperity, the governance of black and grey internet industries has become a critical frontier of public security modernization. This paper systematically examines the governance dilemmas faced today, including technological abuse, internationalization of cybercrime, public awareness gaps, and talent shortages. It further analyzes China's innovative practices in law, technology, value guidance, and public-private cooperation. By proposing a governance framework that integrates security, fairness, and inclusiveness, this study aims to contribute to building a safer and more equitable cyberspace, thus supporting the long-term goal of common prosperity.

2 Synergizing Internet Development and Common Prosperity: A Public Security Perspective

In the digital age of the 21st century, the Internet has emerged as a crucial force driving global economic and social development. Particularly in China, rapid internet expansion has significantly contributed to the modernization of the economy and provided new momentum and possibilities for achieving the goal of common prosperity. Since China's initial connection to the global Internet in the late 1990s, the number of Chinese netizens has surged dramatically. According to the China Internet Network Information Center (CNNIC), by the end of 2022, the number of internet users in China had exceeded one billion, with an internet penetration rate of 73.0%. Among these users, more than 99% access the internet via mobile devices[2]. This massive user base has given rise to emerging industries such as e-commerce, online education, and digital payment systems, profoundly transforming lifestyles and modes of social interaction.

The rapid advancement of the Internet has also fueled the exponential growth of information technology and related services, establishing China as one of the world's largest digital economies. In 2022, the total output of China's digital economy reached 45.5 trillion RMB, accounting for 39.8% of the national GDP. The digital economy has not only facilitated the transformation and upgrading of traditional industries but also demonstrated remarkable resilience and potential during the COVID-19 pandemic, playing a vital role in stabilizing employment and boosting consumption.

However, the widespread adoption of the Internet has also introduced new social and security challenges. The openness and anonymity of cyberspace have turned it into a breeding ground for cyberattacks and the dissemination of misinformation. In recent years, cyber fraud and personal information leaks have become increasingly common. Moreover, the digital divide remains a pressing issue. Uneven internet development across regions and income groups may further exacerbate existing disparities and hinder the realization of common prosperity. To address these challenges, the Chinese government has strengthened network infrastructure construction, especially in rural and remote areas. Additionally, laws and regulations such as the Cybersecurity Law have been implemented to enhance cyberspace governance, improve cybersecurity, safeguard users' information, and crack down on cybercrime.

In the context of common prosperity, the Internet not only injects new vitality into China's economic and social development but also brings with it new risks and challenges. While further advancing internet development, it is essential to reinforce the security and governance of cyberspace to ensure that the benefits of digital progress are equitably shared among all people. This is a fundamental prerequisite for achieving the overarching goal of common prosperity.

3 Governance Challenges of Black and Grey Internet Industries

With the vigorous growth of the digital economy, black and grey internet industries have emerged and proliferated rapidly, becoming major threats to cybersecurity and social stability. These industries encompass various illegal online activities, including but not limited to data theft, online fraud, illicit transactions, and cyberattacks. Due to their rapid technological evolution, strong concealment, and transregional operations, traditional governance methods have proven insufficient. This section analyzes current governance dilemmas from four perspectives: technological confrontation, international cooperation, public awareness, and talent shortages—drawing on public security practices and typical case studies.

3.1 Technological Abuse and Legal Lag

In the context of China's common prosperity strategy, building a fair, stable, and sustainable digital ecosystem has become a key objective of modern governance. However, the abuse of technology within black and grey industries poses significant challenges to this vision, with a widening gap between rapidly evolving criminal techniques and lagging legal frameworks. This contradiction has created regulatory blind spots in the dynamic struggle between crime and enforcement, representing a fundamental pain point in the current governance system.

On one hand, as new technologies continue to emerge, black and grey market actors have adopted increasingly sophisticated and covert methods[3]. In recent years, criminal groups have made widespread use of cutting-edge technologies such as artificial intelligence, blockchain, and deep synthesis to upgrade their criminal toolkits, forming integrated crime ecosystems involving "technology + platforms + capital." For example, in a 2023 case reported by the Ministry of Public Security, a gang used deepfake technology to produce realistic videos impersonating acquaintances of victims, defrauding them of large sums under the pretense of "emergency loans," with single case losses exceeding 5 million RMB.

On the other hand, legal frameworks remain outdated in both technological applicability and enforcement standards. Although police were able to quickly identify suspects, the prosecution process was hampered by gaps in the legal system—existing laws such as the Cybersecurity Law and Criminal Law do not yet contain clear provisions addressing acts such as deepfakes. This legal vacuum hinders the judicial system's ability to attribute responsibility and solidify evidence.

The foremost challenge in black and grey internet governance today lies in the structural mismatch between intelligent, systematized cybercrime and incomplete legal adaptation. Overcoming this dilemma requires a multi-pronged approach: enhancing technological assessment capabilities, improving legislative responsiveness, and unifying law enforcement standards. Ultimately, a new triadic governance model—integrating "technology, law, and public security"—must be established to provide institutional guarantees for the realization of common prosperity.

3.2 Concealment and Internationalization of Black and Grey Industries

The black and grey internet industries are marked by a high degree of concealment and internationalization, which significantly complicates efforts at social governance. These networks often operate across borders, exploiting legal disparities among different countries and regions to carve out a broad and resilient space for illicit activities.

First, concealment is fundamental to the survival of these industries. Criminals frequently use advanced encryption and anonymization technologies to evade detection and surveillance. Such technical measures not only increase the difficulty of law enforcement investigations but also enable these criminal ecosystems to expand rapidly and covertly.

Second, the internationalized nature of black and grey industries poses unprecedented challenges to governance. Divergences in legal systems and enforcement standards between countries hinder effective international cooperation. In some Southeast Asian countries, for instance, local protectionism has allowed black and grey networks to flourish with limited interference. These networks often operate across social platforms, e-commerce sites, and financial systems, forming interconnected and self-sustaining criminal chains[4].

In current law enforcement practice, collaboration barriers between platforms and data fragmentation remain serious issues, resulting in the dispersal of governance resources and delayed response times. This fragmented approach—where individual criminal nodes are targeted without dismantling the full chain—undermines overall governance effectiveness[5].

Addressing this dilemma requires enhanced international cooperation to jointly combat the global spread of cybercrime. Countries must improve intelligence sharing and data interoperability to increase the precision and efficiency of enforcement. In parallel, efforts should be made to promote harmonization in international legal standards and enforcement mechanisms to close existing loopholes and dismantle safe havens for cybercriminals.

3.3 Inadequate Public Awareness of Cybersecurity

In the increasingly complex digital environment, black and grey industry actors have evolved from exploiting technical vulnerabilities to manipulating cognitive gaps in users. The general public's insufficient awareness of cybersecurity has become a key vulnerability exploited by these groups in targeted fraud and manipulation schemes.

Particularly across differences in age, geography, and education levels, a digital literacy gap persists and is systematically exploited. For example, elderly users are often key targets. According to data from the National Anti-Fraud Center, in 2023, individuals aged 60 and above accounted for 45% of victims in "retirement investment fraud" schemes. These scams often use enticing phrases such as "high returns, low risk" and take advantage of the elderly's isolation and limited access to timely communication with family[6].

In one 2024 case, a criminal syndicate launched a hybrid scam campaign combining offline "health seminars" and online "rebate investments" to promote fraudulent "digital retirement products." Victims were promised 120% returns on investments made over 100 days, leading many elderly participants to repeatedly invest over a six-month period. The total amount defrauded exceeded 38 million RMB before authorities were alerted.

To counter this, it is urgent to strengthen public cybersecurity education and awareness campaigns. Citizens need to be informed on how to identify scams, protect personal data, and set secure passwords. Both government and private enterprises must take active responsibility in raising awareness through lectures, guidelines, and accessible consultations. Only through comprehensive public engagement can the systemic human vulnerabilities exploited by black and grey markets be effectively mitigated.

3.4 Shortage of Skilled Cybersecurity Professionals

Technical professionals are the core force in monitoring and countering black and grey internet activities. However, a severe shortage of skilled cybersecurity talent poses a critical bottleneck in effective governance. As cybercrime becomes more technologically advanced and diversified, the demand for highly skilled professionals continues to grow.

Unfortunately, talent cultivation cannot be achieved overnight. Current shortcomings in China's cybersecurity education system—such as outdated curricula and limited hands-on training—have hindered the steady supply of qualified professionals. Additionally, the nature of cybersecurity work requires a rare blend of technical proficiency, analytical thinking, and strong communication skills[7].

To address this issue, several strategies must be pursued: strengthening cybersecurity education at universities and vocational schools, increasing financial incentives to attract and retain top talent, and enhancing international exchange programs to learn from global best practices. Only by closing the talent gap can China's governance capacity match the sophistication of modern cyber threats.

4 Theoretical and Practical Innovations under the Framework of Common Prosperity

In today's globalized context, internet governance has evolved into a multi-dimensional and complex issue, particularly when aligned with the social development goal of achieving common prosperity. Traditional governance models often emphasize legal

and technical mechanisms, but tend to overlook the critical roles of economic equity and social justice[8]. In the context of common prosperity, it is imperative to rethink and redesign internet governance theories and practices to ensure that governance is not only effective but also equitable and inclusive.

4.1 Innovation in Theoretical Frameworks

Theoretical innovation forms the foundation for developing comprehensive governance strategies. Within the common prosperity framework, internet governance theory must incorporate perspectives from the social sciences, with a strong emphasis on economic equality and social justice. For example, internet access has become a necessity in modern life, yet significant disparities still exist both globally and regionally.

To bridge the digital divide, it is essential to ensure that all regions not only have access to the internet, but also benefit equally from the growth of the digital economy. This requires the formulation of holistic policy measures to support internet infrastructure development and digital skills training in remote and impoverished areas. The government could establish dedicated funds to subsidize rural connectivity, offer low-cost internet services, and provide free digital literacy programs. These initiatives would enhance both the economic development potential and the information access capabilities of underdeveloped regions, thereby promoting more equitable economic growth on a national scale.

4.2 Innovation in Practical Strategies

On a practical level, governance strategies must be adapted to the rapidly evolving digital environment and the diverse needs of society. Governments should implement dynamically adjustable policies through the establishment of multi-stakeholder regulatory bodies that include public institutions, private enterprises, and civil society organizations. These bodies would jointly formulate and enforce internet governance rules.

Such a diversified governance model can significantly enhance policy adaptability and efficiency, while also improving transparency and public trust. For instance, mechanisms for regular public consultation and feedback would ensure that all stakeholders—from large technology corporations to ordinary users—have a voice in the policy-making process. This inclusive approach fosters wider acceptance of governance decisions and helps ensure that they are both fair and effective.

4.3 Innovation in Technological Applications

Technological innovation plays a pivotal role in advancing both economic and social justice. While technologies like big data analytics can be used to monitor and prevent cybercrime, it is essential to strike a balance to avoid infringing on individual privacy. Technology developers and policymakers must work together to ensure that technological advancement serves societal development rather than becoming a tool for excessive surveillance or exploitation.

For example, machine learning algorithms can be deployed to detect and prevent online fraud and other cybercrimes, while advanced encryption techniques can be used to protect user data. Such innovations, when implemented responsibly, can enhance cybersecurity and build social trust without compromising personal privacy. Ultimately, they help create a safer and more equitable digital environment for all.

By advancing both theoretical and practical innovations in governance, it is possible to construct a more just and inclusive digital society—one that not only drives comprehensive economic growth but also ensures that the benefits of technological development are shared equitably. This is critical to the successful realization of China's vision for common prosperity, and to fostering long-term social harmony and stability.

5 China's Distinctive Approaches to the Governance of Black and Grey Internet Industries

In addressing the challenges posed by black and grey internet markets, China has adopted a series of governance strategies that reflect both innovation and the incorporation of socialist core values. Rather than focusing solely on short-term crackdowns, these efforts emphasize long-term, systemic improvements through education, institutional reforms, and coordinated social participation. This chapter outlines China's multi-faceted governance model, highlighting its legal, technological, cultural, and cooperative innovations.

5.1 Constructing a Comprehensive Governance System: China's Strategic Innovations

In response to the severe threats posed by black and grey internet industries, China has pursued a multidimensional and comprehensive strategy aimed at addressing the root causes of such criminal activity. At the governmental level, the legal framework has been continuously strengthened to provide a robust foundation for combating cybercrime. Recent years have witnessed the enactment of laws such as the Cybersecurity Law and the Personal Information Protection Law, which clearly define conduct in cyberspace, increase the cost of violations, and represent unprecedented regulatory strength against black-market operations.

Concurrently, China has leveraged its technological advantages by promoting the integration of big data and artificial intelligence in law enforcement and regulatory mechanisms[9]. Advanced data analytics allow authorities to identify traces of illicit activity more efficiently, while AI technologies enhance analytical capabilities and improve the precision of interventions. This comprehensive approach not only demonstrates China's commitment to cyber governance but also showcases its strength in legal and technological innovation. Together, these efforts are steadily building a safer and more stable digital environment, reinforcing the public's information security and supporting broader socio-economic development.

5.2 Integrating Socialist Core Values: A Culturally Rooted Governance Path

China's governance strategy is also characterized by its deliberate integration of socialist core values into internet regulation. Recognizing the importance of cultural and ethical guidance, the government has promoted online civility through nationwide educational campaigns and value-based media initiatives. These efforts aim to cultivate responsible online behavior, legal awareness, and a collective sense of duty among citizens—particularly youth.

Schools, media outlets, and social organizations have all contributed to embedding values such as integrity, lawfulness, and social responsibility into online engagement[10]. Educational programs are delivered through classrooms, extracurricular activities, and digital platforms to instill positive cyber habits from an early age.

Furthermore, China has launched nationwide campaigns to promote "cyber civility," with the "Clean and Bright" (Qinglang) initiative serving as a key example. These campaigns target online rumors, explicit content, and violent materials, significantly improving the quality of digital discourse. The incorporation of socialist values into internet governance represents China's unique strategy—strengthening social cohesion while enhancing network resilience. This model fosters civic responsibility and encourages widespread participation in the safeguarding of cyberspace.

5.3 Innovating Multi-Stakeholder Cooperation: A New Chapter in Public-Private Collaboration

One of the most notable features of China's governance model is its innovative public-private partnership mechanism. This approach breaks away from traditional government-dominated models and instead fosters deep collaboration between authorities and major internet companies. Through joint development of anti-fraud technologies, risk control systems, and governance platforms, enterprises contribute technological expertise and operational insight to national efforts.

These companies also participate in the policymaking process by offering feedback and helping to shape governance strategies, thereby ensuring that policies are both scientifically grounded and practically implementable. This collaboration strengthens communication, clarifies responsibilities, and enhances the overall efficiency of governance[11].

Additionally, the flexibility and sustainability of this model are key advantages. Partnerships between the public and private sectors can be dynamically adjusted to meet changing conditions, while long-term cooperation fosters mutual trust and strategic alignment. In recent years, cities like Hangzhou have pioneered models such as "government-platform collaboration," where early-warning systems are embedded into apps to facilitate user reports, real-time detection, and seamless law enforcement intervention.

For instance, in 2023, Hangzhou police partnered with a local payment service provider to establish a real-time monitoring mechanism for abnormal fund transfers. The

system's algorithm flagged suspicious activity and notified authorities immediately, helping to intercept and freeze illicit funds totaling nearly 100 million RMB.

Moreover, some regions have launched "joint police-enterprise labs" and "collaborative innovation hubs" to align law enforcement needs with R&D strategies, enabling targeted technological solutions and adaptive governance models. Enterprises also fulfill social responsibilities through content moderation, identity verification, and transaction risk control, contributing to a more transparent and orderly online ecosystem.

Through these integrated measures, China is steadily building a digital governance system that is secure, equitable, and sustainable. These efforts not only curb the spread of black and grey industries but also lay the foundation for achieving common prosperity[12]. As technological and social conditions evolve, these strategies will continue to be refined to meet new challenges in the digital age and ensure long-term cybersecurity and public trust.

6 The Construction and Development of Modernized Public Security Work

In the journey toward common prosperity, the modernization of China's public security system plays a pivotal role in maintaining cybersecurity and combating black and grey internet markets. This modernization is not merely a technological upgrade but a critical component of improving the country's governance capacity. By integrating advanced technologies with legal and institutional reforms, public security modernization contributes to a fairer, more orderly society and supports the equitable distribution of social resources.

6.1 Enhancing Regulatory Technology and Information Sharing

Given the complexity and cross-border nature of black and grey internet activities, public security departments have adopted cutting-edge information technologies and big data analytics to improve detection and response capabilities[13]. For example, the establishment of a national cybercrime information database and the promotion of cross-regional and inter-agency information sharing have significantly enhanced the ability of law enforcement to quickly identify and respond to criminal behavior.

These technological applications not only improve enforcement efficiency but also optimize resource allocation—achieving a balance between justice and operational performance. Furthermore, the implementation of real-time monitoring and early-warning systems enables proactive intervention before crimes occur, moving public security strategy from reactive to preventive.

6.2 Strengthening Legal Frameworks and Ethical Education

As technology continues to evolve, the need for continually updated legal frameworks becomes increasingly urgent to ensure adequate protection of citizens' rights. In addition to advancing legal reforms, public security departments have prioritized public education on cyber ethics and legal responsibilities.

Through public lectures, online training, and community outreach, authorities have raised awareness of cybercrime and self-protection strategies. These educational initiatives reduce crime at its roots while fostering a more informed and harmonious digital society.

6.3 Application of Smart Policing Technologies in Black and Grey Market Governance

Technological empowerment has become a crucial pillar in the modernization of public security, particularly in addressing the increasingly complex, systematized, and intelligent nature of black and grey market operations. Traditional governance models—heavily reliant on manual judgment and passive response—are no longer sufficient to meet the practical demands of cybercrime enforcement.

The smart policing model provides a new, efficient, and precise technological path forward. Relying on integrated information systems and comprehensive operations platforms, local public security bureaus are now able to rapidly detect, assess, and address online criminal activities. These systems facilitate the aggregation of case data, enabling faster suspect profiling and risk analysis[14]. This not only improves holistic understanding of criminal networks but also prevents fragmented or short-sighted governance approaches.

Smart policing also significantly enhances interdepartmental coordination. Many black and grey market investigations require collaboration across jurisdictions, agencies, and even platforms. Standardized and streamlined technical mechanisms have enabled the seamless integration of information flows, command structures, and police resources—boosting the efficiency of multi-level responses.

Additionally, smart policing has transformed the working methods of public security agencies. There is now a greater emphasis on data-driven decision-making, predictive analysis, and resource optimization. This transition from “technology-supported work” to “technology-driven transformation” represents a strategic leap in the modernization of law enforcement.

6.4 Innovating Public-Private Cooperation Models

To effectively combat the evolving challenges posed by black and grey internet industries, collaboration between public security departments and the private sector has deepened. Partnerships with internet companies—such as joint development of anti-fraud technologies and monitoring systems—have bolstered law enforcement’s capabilities while encouraging technological and resource sharing.

These collaborative models integrate social resources, enhancing the overall effectiveness of governance. For instance, in Zhejiang and Guangdong provinces, local authorities have launched "government + platform" initiatives. Platforms now include built-in fraud risk alerts, enabling users to report suspicious activity, while systems automatically identify risks and provide law enforcement with real-time access.

A notable example is Hangzhou's partnership with a local payment firm to establish a "transaction anomaly monitoring mechanism." During a 2023 campaign against illegal fund laundering schemes, this system flagged suspicious transfers, helping to freeze nearly 100 million RMB in illicit funds. The platform's algorithmic alerts provided valuable preliminary screening support to police investigations.

Moreover, through joint innovation labs and co-governance platforms, public security agencies and enterprises are aligning enforcement needs with R&D roadmaps. This problem-oriented collaboration fosters targeted technological development and agile response strategies. As platforms increasingly assume governance responsibilities, they now play active roles in real-name account verification, content monitoring, and transaction risk management, forming a collaborative defense line against cybercrime.

6.5 Advancing National Governance Modernization

Modernized public security work is a core pillar of national security and social stability, and an essential element of national governance modernization. The measures outlined above have enabled law enforcement to make substantial progress in combating cybercrime and supporting the goal of common prosperity. These reforms ensure fair allocation of resources and equal protection of citizens' rights, enhancing both governance capacity and public trust.

As technology and society continue to evolve, public security modernization must keep pace. Ongoing innovation in technology, legislation, education, and public-private cooperation is critical to maintaining an adaptive, effective, and just governance system. This will ensure that public security agencies continue to serve society with greater precision and accountability, laying the foundation for a secure, orderly, and equitable social environment.

7 Conclusion

This paper has examined the profound impact of cybersecurity on national security, economic development, and social justice within the framework of common prosperity. As a fundamental infrastructure of modern society, cyberspace security directly influences political stability, economic prosperity, and the well-being of citizens. With the rapid advancement of the Internet, we now face a multitude of security threats—ranging from data breaches and online fraud to information warfare. These challenges not only endanger political and economic security but may also obstruct the achievement of common prosperity.

To counter these threats, a multidimensional strategy is essential—one that integrates legal reform, technological advancement, public education, and international cooperation. Strengthening cybersecurity protections, securing critical national infrastructure, and safeguarding ideological integrity in cyberspace must all become strategic priorities. In parallel, China should actively participate in global internet governance initiatives, fostering mutual trust and cooperative frameworks with the international community to build a safer, more open, and more equitable global digital environment.

Achieving the goals of common prosperity also requires widespread public engagement in cybersecurity efforts. Encouraging active participation across all sectors of society is crucial for creating a more just and equitable digital future. This collective endeavor is not only a response to the challenges of our time, but also a historic opportunity to ensure that all members of society can equitably share the dividends of the digital age.

Acknowledgements

this work was supported by the National Social Science Foundation of China under Grant No.21BSH051.

References

1. Du, Y.: Research on the Industrial Chain of Internet Black and Grey Industries. Master's thesis, Zhejiang University (2018).
2. Tang, J.: Research on the Problems, Causes and Countermeasures of College Students' Safety Education. Master's thesis, Central China Normal University (2006).
3. Wu, S.Y.: Research on Money Laundering through Point-Running Platforms and Countermeasures for Governing Internet Black Industry. Cyberspace Security 13(04), 12–17 (2022).
4. Chen, J., Zheng, H.: Governance of Internet Black and Grey Industries: A Model Transformation from Back-End Response to Front-End Prevention. Public Governance Studies 35(5), 69–79 (2023).
5. Ming, L.: Research on the Trends and Countermeasures of Cybercrime in the Black Industry. Journal of Shandong Police College 31(4), 90–100 (2019).
6. Zhao, J., Zhang, J.: Multi-Pronged Measures Needed for Cybercrime Governance. China Information Security (12), 73–74 (2017).
7. Yang, G., Miao, L.: Current Situation and Countermeasures of New "Living Payment-Type" Benchmarking Crimes. Journal of Jiangsu Police Institute 38(3), 109–115 (2023).
8. Policy Suggestions for Building "Youth Communities" in Tongxiang under the Background of Common Prosperity. Zhejiang Economy (11), 52–53 (2023).
9. Xu, Z., Chen, Z.: Research on Strategies for Integrating Culture and Tourism to Empower Rural Revitalization under the Common Prosperity Background: A Case Study of Huzhou, "China's No.1 City for Rural Tourism". Journal of Tonghua Normal University 44(05), 78–82 (2023).
10. Liu, P., Qian, T., Huang, X., et al.: The Connotation, Realization Path and Measurement Methods of Common Prosperity. Management World 37(8), 117–129 (2021).

11. Zhou, L.: Opportunities and Challenges of Internet Finance Development under the Policy Background of Common Prosperity. International Business Finance & Accounting (6), 51–53, 87 (2022).
12. Kakwani, N., Wang, X., Xue, N., et al.: Growth and Common Prosperity in China. China & World Economy 30(1), 28–57 (2022).
13. Zhou, X.: A Brief Analysis of Internet Black and Grey Industries and Their Investigation and Prevention Countermeasures. Cybersecurity Technology and Application (3), 122–124 (2023).
14. Yu, Y., Zheng, J.: Research on Governance Countermeasures of Key Links in Cybercrime: A Case Study of City T. Journal of Shandong Police College 34(3), 124–135 (2022).

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.