Advances in Social Behavior Research Vol.16 Issue 10 EWA Publishing
Available Online: 17 November 2025 DOI: 10.54254/2753-7102/2025.29747

Research on the prevention and control of high-tech crime

Junyi Wang

School of Law, Guilin University of Electronic Technology, Guilin, China

125118067@qq.com

Abstract. Science and technology are the primary driving forces behind social progress. With the rapid advancement of technology, human society has witnessed vigorous economic growth, continuous evolution of civilization, and flourishing cultural development. People's material lives and spiritual well-being have been greatly enriched. However, high technology, like a double-edged sword, while bringing a better life, has also created fertile ground for the emergence and spread of new forms of crime—thus giving rise to high-tech crime. As a new type of criminal activity, high-tech crime is characterized by its concealed methods, far-reaching harm, and difficulties in prevention and control. The proportion of such crimes among all criminal activities has become significant and continues to increase. Therefore, conducting in-depth analysis and research on high-tech crime is particularly important. By exploring its concepts, typical features, and strategies for prevention and control, we can more effectively prevent and combat this emerging form of crime, thereby ensuring social harmony, stability, and the well-being of the people. The rise of high-tech crime reminds us that technological development not only brings benefits but also poses potential risks. To effectively address high-tech crime, it is necessary to strengthen the supervision and management of science and technology, enhance public awareness of technological security, and improve the formulation and enforcement of relevant laws and regulations. Moreover, it is crucial to establish a comprehensive system for the prevention and suppression of high-tech crime. Only through these measures can we effectively respond to the challenges posed by high-tech crime and safeguard social harmony, stability, and the interests and safety of the people.

Keywords: high and new technology, high-tech crime, characteristics of crime, crime prevention and control

1. Introduction

Technology, like a double-edged sword, brings both convenience and hidden dangers. Precisely because of this dual nature, while we marvel at the rapid advancement of science and technology, we must also remain vigilant about the risks and challenges it entails. We should fully recognize that alongside the countless benefits brought by technological progress, there also exist unforeseen dangers. In this era of both opportunities and challenges—an era where technological progress advances hand in hand with the evolution of crime—it has become a pressing issue for all nations to explore how to effectively mitigate the negative impacts of technology. The motivation and purpose of this paper are to examine the evolution of high-tech crime under the premise of constant technological innovation, and to employ the theoretical tools of criminology, criminal law, sociology, and other interdisciplinary approaches to accurately define the concept of high-tech crime in the new era. It also aims to analyze in detail its connotations and extensions, features, and underlying causes. On the basis of scientific and rigorous analysis, this paper further proposes feasible prevention and control strategies to address the increasingly complex challenges posed by high-tech crime, thereby enabling a calm and well-informed response.

Although Chinese scholars have made considerable achievements in studying high-tech crime, there remain certain deficiencies in practical application. In fact, research on high-tech crime in China has often started from specific crime types. For example, A Comparative Study of Computer Crime by Professor Zhao Bingzhi and others, and A Study on Crimes Involving Letters of Credit and Credit Cards by Professor Hou Fang. However, in today's world—where science and technology are deeply intertwined with criminal activity—focusing solely on specific types of crime can no longer meet practical needs. What is more important now is a conceptual and theoretical analysis of high-tech crime to identify its general characteristics and underlying patterns, so as to prevent and regulate such crimes before they occur. In more recent studies, Professor Gao Mingxuan analyzed the criminal risks of high-tech crime from the perspectives of "Internet Plus" and artificial intelligence. Gao Sinong examined high-tech crime from a technological perspective in his master's thesis, while Li Shaozheng analyzed its causes and control mechanisms from the perspective of crime prevention.

From a theoretical standpoint, existing principles and systematic knowledge related to high-tech crime have become somewhat outdated, making them ill-suited to the accelerating pace and increasing complexity of modern high-tech crime. This theoretical lag means that judicial practice often struggles to clearly define the latest forms of high-tech crime, predict their trends, or understand the motivations behind them—thus making it difficult to implement effective prevention and control measures. Therefore, given the diversity and complexity of contemporary high-tech crime, it is essential to scientifically define its concept in light of China's historical background and specific national conditions. On this basis, we should make accurate predictions about its future evolution, analyze its root causes and operational mechanisms in depth, and ultimately formulate practical prevention and control strategies that can provide a solid theoretical foundation for countering high-tech crime in the new era.

From a practical perspective, criminology is an empirical discipline that serves social practice and subjects theoretical achievements to real-world testing. In contemporary society, as high technology increasingly influences human activity, the accompanying rise of high-tech crime has also had a profound and lasting impact on social practice. In the context of the information age, the evolution of high-tech crime is not merely a reflection of technological progress—it is also a touchstone of human civilization. As modern high-tech crimes become more intelligent, complex, and severe, they cast an invisible shadow over human advancement. Therefore, we must closely align our efforts with the realities of the times and practical needs, applying systematic and scientific theoretical guidance to the prevention and suppression of high-tech crime, and confronting this formidable challenge head-on.

This paper consists of six parts. Part One is the introduction, which explains the purpose of the study and its theoretical and practical significance. Part Two provides an overview of high-tech crime in the new era. It elaborates on the connotations and extensions of high technology and high-tech crime, distinguishes them according to the technological means employed, and discusses how technological development both influences and is influenced by criminal activity. Part Three analyzes the internal and external characteristics of high-tech crime in the new era, examining offenders' traits, evolving criminal motivations, innovations in criminal methods, and the severe harm caused by such crimes to uncover their deeper underlying causes. Part Four explores the causes and elements contributing to high-tech crime from multiple perspectives, including technology, law, and ethics, in order to reveal the essence behind the phenomenon and provide theoretical support for subsequent prevention strategies. Part Five proposes strategies for the prevention and control of high-tech crime in the new era, suggesting targeted measures from various dimensions such as technological countermeasures, legal sanctions, institutional development, and moral education to effectively address high-tech crime and maintain social harmony and stability. Part Six presents the conclusion, summarizing the study and emphasizing that while practical strategies have been proposed, high-tech crime remains a complex social issue requiring concerted efforts across multiple sectors to achieve long-term peace and stability.

2. Overview of high-tech crime in the new era

2.1. Related concepts of high-tech crime

2.1.1. Definition of high technology

High and new technology, commonly referred to as high technology or high-tech, refers to the collection of cutting-edge theories and applied technologies that stand at the forefront of scientific advancement. These technologies, grounded in modern scientific foundations, exert a profound influence on social transformation, scientific progress, and economic development, while driving industrial innovation and structural change. High technology encompasses both "science" and "technology," each demonstrating characteristics of high intelligence, high technical sophistication, and rapid development [1]. The term "high" is relative to traditional or conventional technologies of the past, indicating that the concept of high technology is dynamic and evolves alongside historical and technological progress. What is considered high-tech today may well become routine or conventional tomorrow. High technology is not a single technology but rather a composite entity composed of a cluster of emerging technologies at the frontiers of science, technology, and engineering. The various components of this cluster interact, complement, and promote one another. Moreover, high technology is closely linked to high-tech industries, forming an integrated system that combines science, technology, and production. Under the impetus of market forces, this system continues to grow and evolve, playing a pivotal role in shaping the modern economy and social development.

2.1.2. Definition of high-tech crime

In its broadest sense, high-tech crime refers to all criminal behaviors related to or involving high and new technologies. This encompasses not only traditional crimes committed through or dependent upon high-tech means but also those directed against high-tech facilities, institutions, and their normal operations. As a new form of criminal activity, high-tech crime is intrinsically linked to the advancement of science, technology, and the economy. It arises from the birth and development of high technology

itself and relies on technological tools for its execution. The main categories of high-tech crime include computer and cybercrime, biochemical crime, crimes involving the forgery of various cards and certificates using modern technologies, and crimes carried out through the integration of multiple advanced technological means [2].

2.2. The interaction between high technology and high-tech crime

From a functional perspective, the effects of high technology on high-tech crime can be viewed from both positive and negative dimensions. On the positive side, the development of high technology has significantly enhanced the capability of relevant authorities to combat high-tech crime. As the saying goes, "When the devil advances one foot, the righteous advance ten," meaning that while high technology enriches the methods and forms of high-tech crime, it simultaneously provides more advanced and effective tools to fight such crimes. However, it is equally important to recognize the negative effects of high technology, which can facilitate the commission of high-tech crimes. Therefore, while enjoying the convenience brought by high-tech innovations, society must remain acutely aware of the risks associated with high-tech crime and adopt effective measures to counter these emerging threats [3].

At the same time, high-tech crime also exerts a reactive influence on the development of technology itself. The creation and evolution of technology are often driven by real-world needs, and the problem of high-tech crime plays a crucial role in this process. As the adverse impacts of high-tech crime intensify, national governments have paid increasing attention to the issue and have sought effective technological and policy-based methods to combat it. This growing demand has accelerated improvements in crime-fighting technologies. To keep pace with the evolving sophistication of high-tech crime, outdated technologies must be upgraded or replaced, and new technological tools must be developed. This ongoing cycle of technological renewal has undoubtedly accelerated the pace of technological change, fostering continuous innovation and progress in high technology. Thus, while high-tech crime presents a serious challenge, it also paradoxically serves as a driving force for the further advancement of high technology itself.

2.3. Classification of high-tech crime

High-tech crime refers to criminal activities committed through the use of advanced technologies. In the 21st century, information and biotechnology—at the core of the new wave of scientific and technological revolution—have not only accelerated social development but have also become the primary arenas for high-tech criminal behavior.

2.3.1. Information technology crime

Information science and technology occupy the forefront of modern high-tech fields, with key applications in information retrieval, communication, and data processing. Over time, this field has developed rapidly, centered on microelectronics, and has expanded into diverse domains such as communication technology, automation, and artificial intelligence. Information technology crime refers to criminal activities committed through the use of information technologies. Among these, crimes conducted via computers and the Internet have become the predominant form. The emergence of frontier technologies such as virtual reality and quantum computing has posed new challenges to information security and law enforcement. In this rapidly evolving landscape, information technology crime is no longer confined to traditional computer or network offenses. With the continuous advancement of emerging technologies such as artificial intelligence and blockchain, offenders are constantly probing for new security vulnerabilities and criminal opportunities. Consequently, the challenges to information security have grown exponentially. Facing these looming threats, it is imperative to establish stricter legal frameworks and develop more advanced technical safeguards to ensure information security and maintain social stability [4].

2.3.2. Biotechnology crime

Biotechnology crime refers to illegal or criminal acts committed through the application of biological knowledge and technological means. Emerging alongside the rise of modern biotechnology, it represents a new and more complex manifestation of high-tech crime. While biotechnology, as a new productive force, has generated tremendous material benefits for humanity, it has also introduced a range of serious risks and ethical dilemmas. Since the latter half of the 20th century, biotechnology has gained prominence and, after the 1980s, achieved significant breakthroughs. The integration of biotechnology with information technology has made biotech crime particularly covert and dangerous. Current developments in biotechnology encompass genetic engineering, cloning, biochips, hepatocyte research, and tissue engineering. With ongoing scientific progress, new technologies such as gene editing, stem cell therapy, protein recombination, and genetic modification of pharmaceuticals have become realities. Modern biotechnology—especially genetic engineering and cloning—differs radically from traditional human conceptions of life and morality, and its development inherently carries substantial risks. Therefore, when studying and applying

these technologies, it is essential to consider the potential ethical, moral, and legal implications. If such technologies are used in ways that violate social norms, the resulting consequences could be immeasurable and profoundly harmful to humanity.

2.3.3. Chemical technology crime

Chemical technology–related crime, as a form of traditional crime, has existed since the dawn of humanity. Its primary manifestation involves the use of chemical substances or other related methods to commit offenses against society or individuals. The advancement of chemical technology has provided criminals with more means to conceal their identities, making their offenses increasingly difficult to detect and prevent. As chemical technology continues to evolve, the potential harm arising from its misuse has become progressively more severe. Consequently, the need for societal prevention of chemical technology–related crime has become urgent. In recent years, such crimes have emerged as some of the most difficult forms of high-tech crime to anticipate and control. From the perspective of targeted victims, chemical technology–related crimes can be classified into three main categories: crimes against individual targets, crimes against specific groups, and crimes against humanity as a whole. Crimes against individual targets are typically motivated by personal grievances, revenge, or similar purposes. The victims are usually single individuals or a small number of specific persons. This type of crime tends to cause relatively minor social harm, with effects generally limited to the targeted individuals, and it seldom produces mass casualties or widespread public panic. Crimes against specific groups are more severe. They are usually organized and planned, involving chemical attacks on certain populations, such as through toxic gas assaults or water contamination. Chemical technology–related crimes targeting specific groups are often a form of modern terrorism, with consequences that are relatively severe. Compared with other crimes involving chemical technology, these acts have a more significant social impact. Crimes specifically aimed at humanity as a whole primarily manifest as modern terrorist attacks using chemical substances. Perpetrators are often driven by extreme psychological motivations, including hatred toward society or the world and resentment of social injustices. Under such motivations, criminals may synthesize lethal toxins or release hazardous chemicals to generate widespread panic and chaos. This type of chemical terrorism represents an extreme form of criminal behavior. Its objective is not limited to a particular individual or group but threatens the survival and continuity of humanity itself. Chemical terrorist acts often involve deep ideological or belief-based factors. In addition to being influenced by common external factors such as politics and economics, they may also be associated with religious or cultural motives. The harm caused by chemical terrorism extends beyond immediate loss of life, as it can inflict long-term negative impacts on social stability and public psychology. The threats posed by these crimes and their broader societal consequences are considerable. Therefore, it is essential to maintain high vigilance and adopt timely, effective measures to prevent and combat such offenses.

3. Characteristics of high-tech crime in the new era

3.1. High intelligence and younger demographics of offenders

Compared with traditional criminals, the perpetrators of modern high-tech crimes generally possess distinctive personal attributes. They tend to have higher levels of education, often with professional training or even advanced academic degrees. Many of them have strong technical expertise and outstanding capabilities in operating new technologies. Some hold key positions in government agencies, scientific research institutions, or enterprises, where they are responsible for technological support or administrative management. Leveraging their knowledge, skills, and occupational advantages, they carefully plan and execute various illegal activities.

Statistics indicate that globally, 70% to 80% of computer-related crimes are committed by computer specialists. In China, individuals involved in such crimes often have formal training in computer science or network technology. In the field of drug-related offenses, the tightening of international control over cross-border drug trafficking and precursor chemicals has made it increasingly difficult to obtain traditional drug materials. As a result, some offenders have turned to high-tech methods to synthesize new types of narcotics, such as methamphetamine.

It is also noteworthy that perpetrators of high-tech crimes tend to be significantly younger than those involved in traditional crimes. In the United States, the average age of high-tech criminals is about 25. In China, as educational levels rise and young people become increasingly proficient in technology, the number of high-tech crimes committed by younger individuals has also grown. According to recent domestic case statistics, most offenders involved in high-tech crimes are under the age of 35, with an average age of around 25 [5].

3.2. Concealment of criminal behavior

With the widespread application of advanced technologies—such as smart vehicles, modern communication devices, and computer networks—high-tech crimes have become more sophisticated and concealed than traditional offenses. Victims often

fail to recognize that they have been targeted, resulting in a low detection and conviction rate. Computer crime, as a representative form of high-tech crime, illustrates this problem vividly. It is difficult to distinguish between normal computer operations and criminal activities conducted through computers. Such crimes are often completed within milliseconds or microseconds, leaving almost no trace.

The detection of crimes during the programming or operational process is therefore highly challenging. International data show that only 5% to 10% of computer crimes are ever discovered, and in some cases, the figure may be as low as 1%. Among the reported cases, fewer than 10% are successfully resolved. According to relevant experts, in China, confirmed computer crimes account for only about 5% of the actual total. Moreover, many of these cases come to light only due to accidental circumstances—such as system malfunctions, whistleblowing among accomplices, or the offenders' self-exposure through boasting. Consequently, cybercrimes are characterized by extreme concealment and a high rate of unreported or undiscovered cases, posing significant challenges for law enforcement agencies in prevention and investigation.

3.3. The severe harm of high-tech crime

High-tech crimes pose extremely serious threats to society. In terms of their scope, such crimes may not only inflict severe damage on specific sectors or regions but also endanger public safety and citizens' lives and property on a broad societal scale. From an economic perspective, high-tech crimes often employ sophisticated and modern technological means, resulting in large-scale operations that can cause economic losses amounting to tens or even hundreds of billions of yuan—losses that are often difficult, if not impossible, to recover.

The gravity of high-tech crimes also lies in their intelligent design, concealment, and deceptive execution, which make them much more difficult to investigate and solve than conventional crimes. Consequently, offenders are less likely to be promptly detected and punished, enabling them to evade legal sanctions more easily. This leniency fosters both a sense of impunity and a tendency toward recidivism among criminals. The result is a destabilization of social governance, an increase in the complexity of maintaining public security, and a decline in public confidence in law enforcement institutions. A survey conducted in the United Kingdom revealed that among over two thousand corporate executives, computer crime had risen from tenth place to third among the top ten risks most concerning to British companies within just two years. This demonstrates that the social harm of high-tech crime is intensifying and that urgent, effective measures are required for its prevention and control.

3.4. The concentration and expanding spread of high-tech crime

With the growth of the economy and the advancement of technology, high-tech crimes have become increasingly frequent, particularly in economically and technologically developed regions. In China, such crimes are most common in technologically advanced cities and sectors and are spreading from foreign countries to domestic regions, and from coastal to inland areas. These criminal activities tend to cluster in major cities with prosperous economies, high levels of science, education, and culture, as well as in government departments equipped with advanced technological facilities. Specifically, cities such as Shenzhen, Guangzhou, Beijing, Harbin, Hohhot, Chengdu, Shanghai, Nanjing, and Hangzhou have become primary hotspots for high-tech criminal activity.

As computers and the Internet become more deeply integrated into various aspects of life and governance, increasing amounts of sensitive information—ranging from state and military secrets to corporate trade data and personal privacy—are being stored digitally. This has led to a sharp rise in cybercrime. At present, most cybercrimes are concentrated in the financial and security sectors. However, as law enforcement efforts intensify in the financial, military, and judicial systems, offenders are expected to shift their focus toward emerging fields, further expanding the reach and complexity of high-tech crime.

4. Analysis of the causes of high-tech crime

4.1. Technological iteration facilitates high-tech crime

Technology is a double-edged sword: while it streamlines everyday work and life, it is also frequently exploited by criminals. The methods used in high-tech offenses are continually evolving, and today even ordinary citizens can become victims. Thanks to technological progress, high-tech crime typically has lower operating costs and is easier to carry out, yet its potential social harm grows exponentially. As technology advances, the information society both brings convenience and breeds new forms of crime. In QR code fraud, for example, offenders need only affix a fake QR code to a shared bicycle, a shop checkout, or the window of a illegally parked car; an unsuspecting victim who scans that code with a smartphone can be defrauded with a single tap. The tools used to carry out QR-code scams are becoming increasingly sophisticated and continue to develop, with a variety of QR-code generators tailored to different scenarios. In terms of cost, perpetrators need little planning or strategic investment: by using a QR-code generator to "cast a wide net" and relying on victims' inattention, they can reap rewards with minimal effort.

This simple trick is alarming: the more QR codes are tampered with, the more victims there will be and the greater the cumulative loss. In the digital age, technological progress provides offenders with more opportunities while simultaneously increasing the difficulty for law-enforcement agencies to secure convictions. In short, technology makes committing crimes easier but convicting offenders harder [6].

4.2. Low cost, high return

From an economic perspective, risk and return are generally positively correlated: higher risk usually brings higher return. High-tech crime, however, is on the rise precisely because it often delivers high returns at relatively low risk. Compared with traditional crimes, high-tech offenses can yield greater profits while exposing perpetrators to lower detection risk. Their concealment and technical sophistication make them harder to trace, and their targets and methods tend to be less visible. In some types of high-tech crime, an offender can commit the entire offense from home—merely having an Internet-connected computer suffices to complete the criminal process. As scientific and technological capabilities advance, the methods of high-tech crime become ever more modernized. Because these crimes offer low risk and high profit, an increasing number of offenders are abandoning traditional criminal methods in favor of high-tech approaches [7].

Technical offenses account for the vast majority of high-tech crime, and the use of technology is the principal modus operandi in such cases. Consider the theft case involving Mou Luo (name anonymized), a security management engineer at a well-known P2P car-rental company. After discovering timing discrepancies in the company's financial reconciliations, he first registered a user account and then used his account privileges to alter the user's financial data. Repeating these manipulations over four months, he illicitly obtained more than RMB 6 million. Mou Luo became engrossed in the digital world; every keystroke was a step through his virtual maze. With an annual salary below RMB 500,000 and faced with enormous temptation, he needed no capital outlay—only simple keystrokes or modest code changes—to earn sums reaching into the millions. This low-cost, high-reward criminal strategy drove him to take the risk and commit the offense.

4.3. Lack of victims' self-protection awareness

Although technology has profoundly transformed our daily lives, the public still feels uncertain about how to properly handle the potential risks and problems brought by technological development. Therefore, cybersecurity education must emphasize the importance of password management and urgently enhance public awareness of online safety. Cybersecurity education is not merely about setting or updating passwords—it is fundamentally about cultivating individuals' awareness of privacy protection. From one perspective, many victims have not developed proper cybersecurity habits. They fail to understand that passwords should not be overly simple, that different accounts should use distinct passwords, or that passwords should be updated regularly. In today's digital age, people face unprecedented threats to their personal privacy. Once personal information is leaked, many individuals unknowingly fall into traps set by fraudsters. Their weak awareness of privacy protection has created ample opportunities for telecommunications and online fraud. Meanwhile, the lack of systematic cybersecurity education remains a major hidden danger. From another perspective, when personal data is leaked, most individuals remain almost completely unaware of it—this lack of vigilance further fuels various forms of online deception. Consequently, the absence of strong self-protection awareness and cybersecurity education has become one of the key factors behind the frequent occurrence of telecom and Internet fraud.

4.4. Lag in legislation on high-tech crime

Compared with the rapid growth of high-tech crime, the development of China's criminal legislation appears relatively slow. Therefore, it is urgent to accelerate the legislative process related to high-tech crime in line with scientific and technological advancements, so as to effectively address the challenges posed by emerging forms of crime. The rate at which high-tech crime is expanding in contemporary society is astonishing—each new scientific breakthrough potentially gives rise to new criminal behaviors. Thus, a flexible legislative mechanism is needed to ensure that the law can promptly adapt to technological progress and respond to the challenges of new types of high-tech crime. However, relative to the swift evolution of such crimes, legislation in this field has clearly lagged behind—a delay that has now become almost normalized. This legislative lag manifests itself in several key ways. First, when enacting laws concerning high-tech crime, legislators are inevitably constrained by objective conditions and their own cognitive limitations. As a result, it is difficult for legal provisions to fully cover every aspect of high-tech crime. Even the most capable and forward-looking lawmakers cannot foresee all possible scenarios. Consequently, in the realm of high-tech crime, reactive legislation has become the norm. In most cases, the only means of narrowing this legislative gap lies in subsequent legal interpretation and amendment.

5. Countermeasures for the prevention and control of high-tech crime

5.1. Legal prevention and control

In the field of legislation for preventing and controlling high-tech crime, China should not only learn from successful international legislative experiences and introduce new legal provisions to enhance legal precision but also provide domestic legal support for global cooperation against high-tech crime. The newly established legal provisions must closely align with the realities of technological development and emphasize the protection of specific individuals and sectors. For new types of crimes committed through high-tech means that are not yet explicitly defined in the Criminal Law—but which target particular entities and disrupt the normal order of high-tech industries—relevant laws should clearly stipulate their legal liabilities. New criminal categories should be defined, with clear punitive measures and boundaries of illegality. To ensure a well-developed legal framework for high-tech fields, legislators should thoroughly study domestic and international cases, learn from precedent, revise existing laws in a timely manner, and close potential legal loopholes to improve the precision of judicial interpretation [8]. In particular, serious crimes resulting from human error in high-tech industries must be clearly defined in relevant laws, regulations, and judicial interpretations. While refining legal provisions, law enforcement agencies should strengthen technical training and update investigative equipment to adapt to the evolving complexity of high-tech crime. From another perspective, when it is unnecessary to enact entirely new laws, efforts should be made to refine existing provisions and expand the scope of their application to cover more high-tech crimes. In this rapidly developing technological era, the legal system must evolve with the times. China's legislative efforts in preventing and controlling high-tech crime should adhere to the principle of introducing new criminal offenses when necessary, while also broadening the applicability of existing ones. In addition, administrative laws should specify clear authorities and penalties for unlawful activities that do not constitute criminal acts. Only through timely legislative adaptation can the legal system effectively respond to the dynamic and complex nature of high-tech crime.

5.2. Technological prevention and control

To effectively prevent and curb high-tech crime, collective effort and participation from the entire society are essential. Strengthening the scientific and technological training of law enforcement personnel is a crucial step toward improving their ability to handle complex, technology-driven crimes. Science and technology are the primary forces of production, and in policing, this principle manifests through "technology-driven policing"—deploying manpower based on technological tools, enhancing officers' investigative capacities through scientific education, and employing advanced technologies in the detection of high-tech crimes.

Many countries around the world now regard the development and application of high technology as a powerful weapon in combating crime. In China's pursuit of a harmonious socialist society, greater use of advanced technologies is vital to strengthening law enforcement capabilities. Public security agencies must integrate high-tech applications into all aspects of policing to meet modern demands, effectively suppress criminal activities, and better serve social stability. Investment in scientific and technological equipment for law enforcement agencies should be significantly increased. Efforts must be made to enhance the technological literacy of judicial and police personnel, thereby improving their capacity to combat high-tech crimes. At the same time, focused technological training should be provided for leadership-level officials to improve their professional competence and strengthen their resistance to corruption and external pressures. Law enforcement institutions should also promote the widespread study of science and law, ensuring that mastery of technological knowledge becomes a fundamental qualification for police and judicial officers. Police officers should be encouraged to consciously apply advanced technologies in investigations and evidence collection, allowing agencies to obtain reliable and timely data to support crime prevention and prosecution. Since high-tech crimes often rely on advanced technology in determining criminal patterns, executing offenses, and using counter-investigation methods, they differ significantly from traditional crimes. Consequently, law enforcement must adopt a "science-and-education-strengthening policing" strategy. Officers should skillfully use technology to collect and analyze criminal intelligence, enhance the technological capabilities of both police and community organizations, and rapidly establish technology-based systems for social governance, crime data management, and criminal investigation. Such measures will help ensure that law enforcement remains capable of meeting the ongoing challenges posed by high-tech crime.

5.3. Moral prevention and control

To effectively prevent and control high-tech crime from a moral perspective, education should be emphasized, aiming to raise societal awareness of the severe consequences of such crimes and to cultivate a sense of shame regarding unethical behavior. In this era of rapid technological advancement, moral education is particularly critical. Beyond imparting scientific knowledge, schools must emphasize the ethical responsibilities associated with using technology, ensuring that students understand that technology should serve the advancement of human peace, progress, culture, and well-being, rather than cause societal harm.

This moral training helps cultivate future leaders in the technology sector who can positively influence society and use ethical judgment to prevent high-tech crimes from emerging. Strengthening moral education is also vital for employees at all levels. Ordinary employees, technical personnel, and corporate managers should receive continuous moral guidance to correct any indifference or misunderstanding regarding high-tech crime. Prevention requires active participation from all sectors. Leaders in technology companies should be involved in moral governance to enhance corporate cohesion and alignment. Managers must monitor employees' thought processes and take proactive measures to eliminate negative attitudes, preventing the misuse of technology for criminal purposes [9]. By consistently reinforcing moral education, society can foster a strong sense of responsibility and mission in its members, establishing correct notions of right and wrong, honor and shame. This ethical foundation increases individuals' self-regulation, strengthens their resistance to temptation, and ensures adherence to moral standards. Ultimately, a morally aware society promotes a positive social environment and plays a critical role in preventing and resisting criminal behavior. Moral values—including the distinctions between good and evil, honor and shame, and the cultivation of a sense of guilt—are essential for building a healthy, orderly society and mitigating high-tech crime.

5.4. Institutional prevention and control

Although many countries are gradually establishing specialized institutions to prevent and combat high-tech crime, organizational structures still require optimization in several key areas. First, dedicated organizations should be established to prevent various types of high-tech crime, supported by relevant legislation to ensure their effective operation. Given the characteristics of cybercrime—high concealment, rapid spread, significant destructive potential, and cross-regional impact—it is imperative to adopt specialized investigative methods. Establishing dedicated departments to prevent and combat cybercrime is therefore essential. High-tech crime is increasingly complex, with new forms emerging continuously. Rather than waiting for crimes to occur before forming specialized institutions, it is more effective to proactively create such organizations to investigate and prevent these crimes. Strengthening legal protections is also crucial in this effort, as it serves as an important measure to prevent the occurrence and development of high-tech crime. Combating these crimes is not the responsibility of investigative agencies alone; it requires active societal participation. High-tech crimes can target any entity, especially multinational corporations, financial institutions, and other organizations that often serve as prime targets. These crimes are increasingly cunning, complex, and organized, requiring professional knowledge and specialized personnel for effective countermeasures. Companies and institutions typically establish dedicated departments to prevent high-tech crimes, reducing economic losses while also providing crucial intelligence for law enforcement [10]. Public security agencies should strengthen collaboration with relevant departments, leveraging technology to detect early signs of high-tech criminal activity. This coordinated approach ensures comprehensive societal prevention and control, leaving high-tech criminals with fewer opportunities to succeed or escape detection.

6. Conclusion

The beauty of technology and the malevolence of crime may seem like opposing forces, yet in the process of social development, they have intertwined in a peculiar way, giving rise to numerous new forms of high-tech crime. High-tech crime is not inherently frightening; by studying and analyzing its characteristics and development trends, such crimes can gradually be transformed into conventional criminal patterns, allowing relevant authorities to detect and investigate them in a timely manner. In doing so, high-tech crimes can be curtailed at their early stages, preventing them from escalating. When this occurs, society need no longer fear that technological progress will give rise to criminal activity, and technology can instead serve as a powerful driver for human development and social advancement.

As a novel and rapidly evolving type of crime, high-tech crime warrants systematic analysis of its current status, characteristics, causes, and preventive strategies. Conducting such research can help reduce the incidence of these crimes, alleviate public anxiety regarding high technology, and diminish fear of high-tech crime. Ultimately, this contributes to the effective maintenance of social stability, while enhancing citizens' well-being and quality of life.

References

[1] Bird, A. (2008). Philosophy of science (J. Y. Jia & R. X. Xue, Trans., pp. 10–12). Beijing: Renmin University of China Press.
[2] Zhao, G. Z. (2002). Prevention and countermeasures of modern high-tech crimes (pp. 4–5). Beijing: China Science and Technology Press.
[3] Ma, J. B., & Yuan, G. L. (2008). Research on high-tech crime (pp. 307–308). Beijing: People's Public Security University Press.
[4] Gao, M. X., & Wang, H. (2018). Criminal risks and typology analysis in the era of Internet plus artificial intelligence. *Journal of Jinan University*, (6), 78–80.
[5] Randy. (2015). Research on high-tech crime prevention mechanisms. *Journal of Jiangxi Police Institute*, (1), 99–102.
[6] Wang, C. Z., & Mao, J. R. (2012). Technology ethics: Balancing and adhering to utilitarianism and morality. *Studies in Philosophy of Science and Technology*, (12), 73–76.

[7] Xiong, B. (2019). The lack of technical legislative methods in technology criminal law and technical planning. *Journal of Criminal Law Theory*, (2), 88–91.
[8] Liu, C. Q. (2019). Accurately positioning criminal law in response to life science and technology activities. *China Health Law Review*, (3), 74–75.
[9] Chawki, M., & Darwish, A. (2015). Cybercrime: Digital forensics and jurisdiction (pp. 116–119). Cham, Switzerland: Springer International Publishing.
[10] H., E. (1947). Principles of criminology (pp. 15–17). Philadelphia, PA: J. B. Lippincott Co.