Governance of Dark Web Crimes from the Perspective of a Holistic Approach to National Security

Shanshan Jiang, Guangxuan Chen*and Tao Wang

Zhejiang Police College, Hangzhou, 310053 China

*chenguangxuan@zjjcxy.cn

Abstract. As a relatively covert form of cybercrime, dark web crime is spreading and proliferating in China. Traditional forms of crime have gradually shifted from offline activities to the surface web and further to the dark web, giving rise to a wide range of illegal activities based on the dark web, including terrorism, drug trafficking, arms trading, child pornography, forged documents, hacking services, and the sale of personal information. This paper analyzes dark web crime and its impact on national political security, social security, economic security, and information security. It further explores the difficulties and challenges in the governance of dark web crime. Drawing on domestic and international experiences in dark web crime governance, and from the perspective of a holistic approach to national security, this paper proposes a diversified governance approach to combat dark web crime.

Keywords: Dark Web Crime; A Holistic Approach to National Security; Cybersecurity; Crime Governance.

1 Introduction

The Dark Web is a part of the internet, distinct from the surface web that we access daily, because its content cannot be indexed by conventional search engines like Google, Yahoo, Bing, Baidu, etc. The Dark Web uses a distributed, multi-node data access method and multiple layers of data encryption. Each data packet is designed to communicate with an encrypted IP address, making it difficult to trace users' identities [1]. At the same time, the technical characteristics of the Dark Web make monitoring and tracking activities on it extremely challenging. This provides convenience for illegal activities, particularly the various black markets on the Dark Web, where a large number of illicit activities take place, such as terrorism, drugs, weapons, pornography, fake documents, hacker services, and the trafficking of personal information.

In general, the Dark Web is a highly anonymous and difficult-to-monitor space. It includes both illegal activities and legitimate privacy protection services. Due to its secrecy, the Dark Web poses significant challenges to network security and legal regulation, and it presents enormous difficulties for law enforcement agencies investigating illegal activities on the Dark Web.

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_158

2 Dark Web Crime and its Real Threat to National Security

The internet can be divided into the surface web, deep web, and dark web. The surface web refers to websites and data that can be easily found using standard search engines, typically carrying domain markers such as ".com" and ".org." In contrast, the deep web cannot be searched through standard search engines, meaning it is an unindexable layer of the internet. If we visualize the entire internet as an iceberg floating in the water, the deep web would be the submerged part of the iceberg, which is much larger than the surface web. The deep web is hidden beneath the surface web, protecting users' privacy, such as financial accounts, email, private business databases, and social communication accounts. The dark web is a more hidden subset of the deep web, requiring specialized browsers or techniques to access. This gives it a high degree of anonymity.

Due to its anonymity and difficulty in tracking, the Dark Web has become a platform for illegal transactions and criminal activities. Dark web crime refers to unlawful activities carried out in the anonymous online space of the Dark Web. Criminal behavior that uses the Dark Web as a tool for crime or as a space for criminal activities can all be considered Dark Web crime. While some individuals use the Dark Web for privacy protection and other purposes, its characteristics make it a breeding ground for various crimes, such as drug trafficking, smuggling, pornography, money laundering, counterfeit goods, and terrorism. Currently, organized crime activities within the Dark Web are becoming increasingly rampant, with the number of Dark Web tools and services growing. Ransomware and Dark Web markets are continuously expanding. These trends indicate that Dark Web actors are adapting to the cybersecurity measures and governance implemented by governments and organizations, while also posing a serious challenge to the existing cybersecurity systems with the support of technologies such as big data, cloud computing, and artificial intelligence. As a new form of cybercrime, Dark Web crime has gradually spread from Europe and the United States to China, posing significant challenges to law enforcement in the country.

2.1 Political Security Threats

The concealment and connectivity characteristics of the Dark Web make it an important battleground and an indispensable tool for hostile Western forces to challenge China's political security. In recent years, the unprecedented global changes have presented significant challenges and transformations for countries worldwide in the areas of politics, economics, society, technology, and the environment. Western countries, adhering to Cold War thinking, continue to view the collapse and division of the socialist camp as a core strategy, successfully creating events like the changes in Eastern Europe and the disintegration of the Soviet Union, achieving their political goal of global dominance. Meanwhile, China is undergoing a social transformation, with various conflicts and contradictions being unavoidable. Political attitudes and private demands collide and interact on the Dark Web, continuously impacting exist-

ing value systems and political identities, and affecting social stability and public security. As China's efforts to govern the surface web continue to strengthen, the scope of anti-China activities by foreign and domestic forces on the internet has been limited, prompting them to turn to the Dark Web to engage in political division. Foreign governments, intelligence agencies, hackers, separatist groups, terrorist organizations, and cults combine methods such as stealing state secrets, spreading extremist ideologies, infiltrating values, distorting historical events, sensationalizing social issues, and exacerbating social conflicts with Dark Web technology, undermining societal values and moral standards, severely disrupting the mainstream national ideology, and threatening China's political security.

The notorious terrorist organization ISIS's shift to the Dark Web is a typical example of the combination of terrorist activities and Dark Web technology. In November 2015, ISIS planned and carried out the Paris terrorist attacks, which included six shootings, three explosions, and one hostage situation, resulting in at least 132 deaths. After the attack, ISIS's websites were subjected to large-scale cyberattacks, but this did not cause catastrophic damage. Instead, ISIS quickly moved its websites to the Dark Web, continuing activities such as fund transfers, internal communications, recruitment, self-promotion, and terrorist coordination[2]. The negative impact of the Dark Web space and its technology on political security and public safety is evident. Furthermore, in terms of ideological infiltration and online coordination, Dark Web technology has become an indispensable communication tool[3].

2.2 Social Security Threats

With the intensified crackdown by law enforcement agencies in various countries, the space for traditional criminal activities has been continuously squeezed.Existing serious criminal activities, such as the illegal trade of drugs and controlled substances, human trafficking, firearms and ammunition smuggling, child sexual exploitation and pornography services, and the sale of hacking tools, have begun to shift toward the more concealed Dark Web in order to evade legal sanctions. This trend has increased the difficulty for law enforcement agencies to track and combat criminal activities, posing a severe challenge to social security and, by extension, overall national security.

For example, many analyses suggest that a large portion of illegal activities on the Dark Web is related to child pornography. In recent years, ongoing monitoring of Dark Web sites and markets has shown that the Dark Web is flooded with a large amount of child pornography and related illegal activities. In October 2019, the U.S. Department of Justice announced that with the help of an international law enforcement coalition, they had taken down the largest known child pornography site on the Dark Web, "Welcome to Video." The site operated from June 2015 until March 2018, hosting over 250,000 videos of child and infant pornography. This site was also the first on the Dark Web to use Bitcoin to sell child pornography videos. By analyzing the seized servers, law enforcement officials discovered over 1 million wallet addresses used to receive payments. During the three years the site was operational, at least 7,300 transactions occurred, and the site received at least 420 bitcoins. This operation successfully arrested the 23-year-old South Korean site administrator and 337

individuals suspected of using the illegal website, and rescued 23 children living in the U.S., Spain, and the U.K., who were being abused[4].

In today's world, where telecom network fraud is rampant, black and gray market activities related to telecom fraud have also emerged on the Dark Web. Non-bank payment accounts, online payment interfaces, online banking digital certificates, SIM cards, IoT cards, instant messaging internet accounts, and hardware devices such as "cat pools," GOIP devices, and multi-card boxes used for criminal activities, all related to financial flow black markets, communication flow black markets, and technology flow black markets, can be easily accessed on the Dark Web. The formation of these industrial chains is purely driven by crime. Not only do they profit from illegal transactions, but they also further fuel criminal activities such as telecom fraud, creating a severe threat to social security.

2.3 Information Security Threats

With the alternating development of internet technology and society, the focus of Dark Web crime has also shifted, from drug trafficking to human trafficking and pornography services, and then to data trading. Illegal data transactions on the Dark Web are primarily concentrated around crimes that violate citizens' personal information. Criminals obtain large amounts of personal information and data through hacking, illegal purchases, and other methods, and then sell them for profit. In the internet era, crimes that infringe on citizens' personal information are known as the "source of a hundred crimes," further giving rise to various illegal activities such as telecom fraud, internet fraud, blackmail, kidnapping, credit card fraud, and illegal debt collection. These crimes have a severe social impact, and the public has strongly reacted.

The cybercrime forum BreachForums, launched in June 2022, has undergone multiple legal crackdowns and resurgences, becoming one of the major threats in the global cybersecurity landscape. As an important data breach and trading market on the Dark Web, the forum quickly attracted a large number of users to buy or sell stolen data (such as personal information, bank accounts, corporate databases, etc.), hacking tools, access credentials, and other illegal items. In November 2022, a large-scale data breach occurred on the forum, resulting in the exposure of personal information of over 1 billion users, including data from Shanghai's "Suishin Code." According to incomplete statistics, China ranks third in terms of countries affected by data breaches, following the United States and Russia[5]. In March 2023, U.S. law enforcement arrested Pompompurin, the main administrator of BreachForums, and the forum was subsequently shut down. However, the forum did not disappear entirely and was taken over by other hacker organizations and relaunched. In 2024, the FBI once again seized multiple domains and Telegram pages of BreachForums, but the forum quickly reappeared with new domains, demonstrating its strong resilience and adaptability.

In addition, hackers and foreign intelligence agencies can launch large-scale, deep, and sustained cyberattacks on government agencies, classified organizations, critical infrastructure, and other key enterprise network systems, thereby stealing data related to national security strategies, military deployments, intelligence materials, and more.

The Dark Web provides a covert trading space for such data. For example, according to Portuguese media Diario de Noticias, in 2022, the Portuguese Armed Forces General Staff was subjected to an unprecedented hacker attack, leading to hundreds of NATO confidential documents being put up for sale on the Dark Web[6]. According to sources, the leaked documents were "extremely serious," and their dissemination could lead to a crisis in the country's credibility within the military alliance. Once this information is leaked, national security will be severely threatened.

2.4 Economic Security Threats

Dark Web transactions mainly rely on Dark Web marketplaces, such as the notorious AlphaBay, Silk Road, and Hansa. These platforms are often involved in illegal activities, including the sale of illicit goods and services, smuggling, and money laundering. These unregulated illegal transactions not only violate existing laws but also damage the stability and credibility of financial markets, directly threatening national economic security and the property interests of the public. The impact is far-reaching and cannot be ignored. In recent years, scholars have also identified Chinese-language Dark Web trading platforms. For example, in 2021, the Sichuan Provincial Public Security Department reported the "Luzhou Wang's Case of Infringing on Citizens' Personal Information." In this case, Wang and other suspects, including Guo, accessed a "Chinese Dark Web Trading Forum" multiple times starting in March 2018, purchasing citizens' personal information and then using several chat software platforms to contact buyers for resale, illegally profiting more than 230,000 yuan. Through further investigation into their buyers, law enforcement discovered that suspects such as He Hong used the purchased personal information to carry out online fraud through loan issuance, severely infringing on citizens' property security[7]. The emergence of Chinese-language Dark Web markets also indicates that Dark Web crime is not far from us.

Furthermore, current financial market infrastructures, such as payment platforms, securities settlement systems, cloud service providers, and central banks, are all heavily dependent on network operations. If hackers attack these financial systems and network information systems, it could lead to the collapse or slowdown of trading systems, causing significant legal risks and economic losses for the involved enterprises and individuals, directly threatening national economic security and the property interests of the public. It is worth noting that the anonymity of the Dark Web also increases the risks of transactions, leading to numerous instances of "black-on-black" situations. The "Besa Mafia" website is a typical example. This website was presented as a marketplace for mafia activities, but it was ultimately exposed as a scam. The operators accepted various tasks through the site and charged commissions, but never carried out any assassination operations. A similar situation occurred in illegal arms trading, where most weapon transactions were initiated by scammers and undercover police officers, leading to the complete cessation of gun sales on the famous Dark Web market "Agora"[8].

3 Governance Dilemmas and Challenges of Dark Web Crime

The Dark Web and its technologies are fundamentally changing the way crimes are carried out. Dark Web crimes often use relay point proxies, anonymous redirections, and various encryption technologies to hide the identities of users, Dark Web transaction orders, payment records, and other data, effectively evading law enforcement tracking and legal sanctions. Although we categorize Dark Web crime as a new type of crime, it not only poses a serious and real threat to emerging non-traditional security fields but also combines with crimes in traditional security areas, further impacting national security. Therefore, Dark Web crime not only exacerbates old legal challenges but also brings new governance dilemmas.

3.1 Technical Countermeasures

Understanding and learning how to use the Dark Web is not a difficult task, but tracking back, securing evidence, and bringing criminals to justice require advanced technology to support these efforts. Given the anonymity features of Dark Web crime, mastering stable de-anonymization technologies is an essential factor in Dark Web crime governance. Currently, the development of de-anonymization technologies for Dark Web crimes is slow and often lags behind the development of criminal methods. In past cases, researchers have implemented various de-anonymization techniques by exploiting direct vulnerabilities in anonymous networks or utilizing indirect flaws. For example, in 2014, Carnegie Mellon University's Software Engineering Institute attacked the technical flaws in the TOR network and, through IP tracing, identified Brian Farrell, a staff member of the infamous Dark Web marketplace Silk Road 2.0, thus initiating the crackdown on Silk Road 2.0[9]. Additionally, attacks on the vulnerabilities of the TOR protocol or browsers running TOR may also achieve de-anonymization. However, once these de-anonymization attacks succeed, the TOR project developers immediately work to debug and upgrade the system to fix technical flaws and vulnerabilities. In other words, these de-anonymization methods are not replicable.

Based on the current practical work situation, de-anonymization has actually been achieved through non-technical means. Silk Road, a Dark Web marketplace primarily focused on drug trafficking, was seized in 2013 by a joint operation involving the FBI, the Department of Homeland Security, and other agencies. Its founder, Ross Ulbricht, revealed his identity while running the Dark Web market. In early January 2011, he used the alias "altoid" to promote his market online, and in a post seeking programming help, he left his email address: rossulbricht@gmail.com. Although this information was deleted, it was retained in the responses to the post, and law enforcement was able to track Ulbricht down through this clue and successfully arrest him. Similarly, Blake Benthall, when setting up and operating "Silk Road 2.0," was caught by law enforcement after using his personal email address to register the server for running the anonymous website. These cases demonstrate that effectively using open-source intelligence is also crucial in Dark Web crime investigations. However, like

de-anonymization methods that exploit vulnerabilities, these non-technical de-anonymization operations also have unpredictability, and they are not a systematic or stable form of de-anonymization.

Due to the anonymity and decentralization features of the Dark Web, securing and extracting evidence of criminal activities poses significant challenges. The scope of electronic forensics in Dark Web crimes includes but is not limited to specialized virtual network forensics, electronic device memory forensics, TOR browser forensics, mirror website forensics, network traffic forensics, and cryptocurrency forensics. Unlike ordinary electronic investigations, Dark Web crime forensics primarily focuses on investigating the anonymous software used in the Dark Web space. Through electronic forensics, investigators can restore the criminal's access trajectory on the Dark Web, thereby corroborating their criminal activities and forming a legally valid logical connection. However, Dark Web sites are often unstable and encrypted to a significant degree, and any improper handling during the forensic process may result in the destruction or loss of important evidence. Furthermore, existing technologies struggle to crack the encryption algorithms of cryptocurrencies, making it difficult to directly identify the transaction participants' information from extracted wallet data, logs, IP addresses, and so on, hindering the acquisition of critical evidence. At the same time, cryptocurrency transactions are defined as illegal financial activities in China, so there is a lack of practical guidance regarding the seizure, freezing, and disposal of cryptocurrency encountered in case investigations.

3.2 Regulatory Systems

Currently, the governance of Dark Web crime is mainly implemented through criminal law regulation. This post-fact passive law enforcement model shows an over-reliance on criminal law regulation and exposes flaws such as delayed response phases, a single regulatory body, insufficient regulatory measures, and weak post-event remedies. However, no matter how criminal law evaluates criminal behavior retrospectively, it cannot eliminate the negative impact of Dark Web crime, and it is difficult to purify the ecosystem of Dark Web crime. At the same time, addressing the entire industrial chain of Dark Web crime requires not only focusing on the criminal activities at the backend but also paying attention to the precursor behaviors and criminal assisting actions at the front end. For example, when novice Dark Web users browse criminal information related to hacking, internet fraud, illegal transactions, or create images, videos, or fake accounts that could be used for Dark Web crimes, such behaviors are clearly difficult to regulate through criminal law. The lack of supervision over these front-end behaviors results in a lack of systematic and forward-looking governance of Dark Web crime, further nurturing the environment for Dark Web crime, thus becoming a breeding ground for various illegal activities.

From the perspective of the illegal crime costs of Dark Web crime, the convenience of accessing the Dark Web, its anonymity, and the aggregation of criminal activities make the Dark Web a breeding ground for crime. Even if an individual accesses the Dark Web and engages in illegal activities, the lack of regulatory oversight greatly reduces the likelihood of facing legal risks, which undoubtedly fuels the arrogance of

Dark Web crime. From the perspective of criminal economics, if the output of criminal behavior remains unchanged, it will be difficult to prevent crime unless the cost of engaging in Dark Web crime is increased.

3.3 Rule of Law Construction

The challenges in the governance of Dark Web crime in terms of rule of law construction mainly consist of two aspects. On one hand, there is insufficient legislative regulation of Dark Web crime itself. As traditional criminal activities gradually move into the Dark Web space, crimes committed with the help of the Dark Web or in the Dark Web environment are still regulated by traditional criminal legislation. According to a search on the China Judgments Online website, the crimes related to Dark Web activities in China involve violations of citizens' personal rights, the disruption of the socialist market economy order, endangering public safety, obstructing social management order, and other charges. However, Dark Web crime, with its networked nature, presents essential differences from traditional crime in terms of location, actions, and targets. Traditional criminal legislation is clearly unable to adapt to this area[10].

On the other hand, there is significant controversy regarding the principle of proportionality in Dark Web crime investigations. While the Dark Web is rife with crime, encryption is not synonymous with criminal activity, and security and law enforcement needs should not be used as a pretext for violating privacy. The excessive use of search warrants and entrapment techniques in Dark Web investigations has already drawn some societal attention. For example, the FBI developed a tool called "NIT" (Network Investigative Technique). By implanting NIT software into a website, it collects related request data from users and then conducts "entrapment" to identify the real information of these users. Some network experts have pointed out that NIT is essentially a Trojan horse or malicious software. During the investigation of the child pornography site "Playpen," the FBI continued to operate the site for 13 days after seizing it, during which NIT was used to attack over 8,000 personal devices in more than 120 countries[11].This "entrapment" has sparked widespread attention and debate in the United States. U.S. federal government officials have also acknowledged the risks associated with the FBI's actions.

3.4 International Cooperation

Dark Web crime often has significant cross-border and global characteristics, and addressing this international crime requires seeking the help of international law enforcement organizations. However, the capacity of INTERPOL is derived from its membership; it is not a legislative body and does not have law enforcement authority. Its main function is to facilitate international coordination. As a longstanding issue, there is still a lack of an international body to take the lead in Dark Web crime-related work. Currently, the enforcement against Dark Web crime is still carried out by individual countries or specific regional agencies, with no formal international mechanism to ensure law enforcement activities targeting Dark Web crime.

From past law enforcement activities, it can be seen that national law enforcement agencies have been working to overcome cultural and legal differences, striving for cooperation. However, for cybercrime, especially Dark Web crime, which are new types of crimes, certain difficulties still exist. For example, in international cooperation, complex legal procedures, missing information or insufficient reporting, legal inconsistencies, and differing national priorities often result in delays in the legal assistance process. Although there has been subjective intent to coordinate internationally, countries often approach matters from their own national perspectives. Different legal systems, political stances, and cultural viewpoints lead to disagreements in methods and opinions, which make it difficult to resolve cross-border cooperation challenges.

4 Governance Countermeasures for Dark Web Crime under the Perspective of a Holistic Approach to National Security

Dark Web crime poses a serious threat to national security. By analyzing Dark Web crime and its governance challenges, this paper attempts to propose countermeasures for the governance of dark web crime.

4.1 Promoting the Innovation and Development of Technological Means

As the technology behind cybercrime, particularly Dark Web crime, continues to evolve and upgrade, corresponding countermeasure technologies must also keep pace with the times, continuously innovate, and ensure effective responses to curb the further spread of Dark Web crime. On the Dark Web, criminals constantly share information with each other, so mainstream Dark Web forums and markets are likely to contain data that helps uncover crime-related intelligence. In order to identify the latest trends in Dark Web crime and important leads, technologies and products capable of thoroughly and rapidly searching and analyzing Dark Web data and intelligence must be developed. In 2014, the U.S. Department of Defense's Defense Advanced Research Projects Agency (DARPA) launched the "Memex" search engine research project to effectively uncover hidden information on the Dark Web and expose illegal activities. The engine has been proven to provide substantial assistance to law enforcement in tracking down human traffickers, drug dealers, and terrorists. In academia, many researchers have conducted in-depth studies on Dark Web intelligence monitoring technologies, attempting to develop monitoring models from various perspectives such as Dark Web forums, markets, websites, malicious software, and malicious traffic. For example, Yang Yingna and others developed a visual analysis platform for Dark Web forums, which quickly identifies detailed information on relevant posts in visual form, aiming to process large amounts of forum data to help law enforcement analyze Dark Web crime leads more thoroughly[12]. Many scholars have also conducted academic research on de-anonymization technologies for the TOR anonymous communication network. Currently, mainstream de-anonymization technologies can mainly be divided into website fingerprint analysis and traffic correlation analysis. Li Yanlin combined

genetic algorithms to optimize convolutional neural networks for TOR website fingerprint recognition and a cross-temporal TOR website fingerprint recognition model based on multi-head attention mechanisms, designing and implementing a TOR network website identification system[13].is system can provide strong support for enhancing Dark Web regulation efforts. However, these research projects are often limited to theoretical and academic studies and have not yet been effectively applied in the practical fight against Dark Web crime.

In the field of Dark Web electronic forensics, Zheng Rongzhe and others introduced the forensic approach, step design, and detailed process of a case in which a criminal suspect was selling citizens' personal information on the Dark Web[14]is demonstrates that combining theoretical research with practical case studies can effectively enhance the operational ability and success rate of Dark Web crime forensics. However, after searching through papers on Dark Web electronic forensics technologies, it was found that research results in this area are relatively scarce, indicating that there is still a vast space for exploration and development potential in this field.

4.2 Improving a Systematic, Diverse, and Proactive Regulatory System

Although law enforcement actions are a key measure to curb Dark Web crime, purely post facto punitive measures are not sufficient to eliminate the root causes of Dark Web crime. Based on past experiences in cracking down on Dark Web markets, shutting down a specific Dark Web marketplace does not significantly reduce the overall level of Dark Web crime. When a market is shut down by law enforcement or paralyzed due to a cyber attack, new markets often emerge to maintain the overall stability of the Dark Web market. Therefore, a multi-faceted regulatory system led by the government and involving the collaborative participation of various sectors of society is particularly important.

In order to break through the current governance model of Dark Web crime, which mainly focuses on criminal enforcement, internet governance should gradually shift towards a multi-stakeholder governance model, with a focus on prevention rather than post-event punishment, and the establishment of systems that continuously adapt to technological advancements. The multi-stakeholder governance model refers to the increasing importance of network platforms in assuming primary responsibility for proactively preventing crimes as the scope of cybercrime continues to expand. This involves strengthening the implementation of crime prevention obligations and broadening the stakeholders involved in Dark Web counter-governance. Furthermore, continuous improvement of governance systems is necessary to enhance Dark Web monitoring, analysis, and early-warning technologies, fostering positive interaction between systems and technologies, and driving continuous improvement in Dark Web crime governance capabilities and effectiveness.

In the process of governing Dark Web crime, the government should use systems, legislative measures, and media publicity to help the public establish an objective understanding of the Dark Web. It is worth mentioning that young people, due to their proficiency with internet technology and strong curiosity, have become a high-risk

group that is likely to come into contact with and possibly engage in Dark Web crime. Therefore, special attention must be given to this group, and through positive educational guidance, they should be helped to establish correct online usage concepts and foster a sense of social responsibility, ultimately reducing the potential number of participants in Dark Web crime.

4.3 Establishing and Improving the Legal Regulation of the Dark Web

With the close integration of the internet and various fields of societal activity, Dark Web crime has developed into a more industrialized and ecological model, seriously endangering network security and national security. For this new form of crime, the criminal legislative response is somewhat lagging. Academic research on the rule of law in Dark Web crime often focuses on criminal legal regulation, neglecting the necessity of administrative regulation, which results in the legal regulation of Dark Web crime lacking certain overall coherence and systematization. Criminal and administrative regulations differ in their purposes, methods, scope of application, and processing procedures. A thorough study and optimization of Dark Web legal regulation from both criminal and administrative perspectives not only lays a solid legal foundation for the legitimacy of Dark Web governance but also fully utilizes the special and general preventive functions, applying effective legal deterrence to individuals who have committed or are potentially involved in Dark Web crimes. Additionally, this approach can curb the emergence and spread of Dark Web tools and services at the source, thereby ensuring a clean and secure online environment.

4.4 Strengthening International Cooperation to form a Global Joint Effort in Combating Dark Web Crime

In the governance of Dark Web crime, due to its typically transnational nature, involving multiple countries and regions, international cooperation is particularly important. However, differences in policies, laws, systems, and technologies across different countries and regions pose significant challenges to combating Dark Web crime. In the successful operation that dismantled the notorious Dark Web marketplace "AlphaBay," the U.S. Federal Bureau of Investigation (FBI), U.S. Drug Enforcement Administration (DEA), and the European Police Organization (Europol) worked together with government regulatory agencies from multiple countries, including the U.S., Canada, the U.K., the Netherlands, France, and Thailand. This highlights the critical role of international cooperation in combating Dark Web crime.

In order to effectively respond to this global threat, countries must strengthen cooperation and jointly build a more closely-knit international cooperation framework. For example, in 2015, the UK government announced the establishment of a specialized "Joint Law Enforcement Agency" to combat Dark Web crime. The main responsibilities of this agency include early warning and crackdown on serious crimes such as child exploitation, drug trafficking, illegal goods trading, document forgery, and financial data theft. In 2016, seven European countries—Germany, Lithuania, Russia, the Netherlands, France, Switzerland, and others—launched a joint special operation

targeting the Dark Web. The operation primarily focused on arresting Dark Web forum operators and users involved in trafficking drugs, fake documents, investigative data, and illegal labor services. According to reports from Deutsche Presse-Agentur (DPA), the raid resulted in the arrest of nine criminal suspects. However, to date, no global organization specifically dedicated to combating Dark Web crime has been established.

In terms of global conventions in relevant fields, it has been difficult to reach consensus for a long time due to the differing definitions of Dark Web crime across countries. Currently, there are only a few regional multilateral treaties in the international community concerning cybercrime, such as the *Budapest Convention, the Shanghai Cooperation Organization Member States Agreement on Intergovernmental Cooperation to Ensure International Information Security*, and the *Arab League Convention on Combating Information Technology Crimes*. However, these treaties often focus on different aspects based on the needs of the contracting parties, and the number of contracting countries is limited. In November 2019, China, Russia, Belarus, Cambodia, Iran, Myanmar, Nicaragua, Syria, and Venezuela proposed an international convention to combat cybercrime and passed the resolution in December of the same year. The draft convention is set for final revision in 2024 and will be submitted to the United Nations General Assembly for a vote. However, the drafting stage of the convention has sparked widespread controversy. Countries have actively sought provisions that align with their own national interests. One major point of contention is cybercrime jurisdiction, which still needs to be determined through equal consultations while respecting cyber sovereignty. Additionally, while the draft convention aims to address cybercrime, there are concerns that it might expand government surveillance powers, potentially leading to violations of human rights. Furthermore, some provisions in the draft do not distinguish between the intent behind cyberattacks, potentially misclassifying legitimate activities by white-hat hackers or researchers as criminal acts[15].

International cooperation in combating Dark Web crime should not be limited to legal aspects; it must also involve the exchange and cooperation of technology and expertise. Countries should actively share new technologies and emerging trends in Dark Web crime, collaboratively discuss strategies and methods for Dark Web governance, and form a unified joint effort to combat Dark Web crime.

5 Conclusion

As a new type of cybercrime, Dark Web crime has quietly spread in China. Due to its relatively unbreakable anonymity and strong instability, monitoring the Dark Web poses significant challenges in terms of technology, systems, and legal regulation. The negative impact it has on national security far exceeds what is described in this paper. Although considerable achievements have been made in combating Dark Web crime both domestically and internationally over the years, the continuous upgrade and development of internet information technologies such as big data, artificial intelligence, and deepfake technologies are making the challenges of Dark Web crime governance increasingly severe.

This paper examines Dark Web crime through a systematic and comprehensive approach. It briefly analyzes the harm that Dark Web crime poses to national security, the challenges in its governance, and attempts to propose governance strategies. Specifically, the governance of Dark Web crime should emphasize a comprehensive and integrated systemic security approach. By building a solid and robust national security governance system, the challenges posed by Dark Web crime can be addressed. This strategic thinking integrates traditional national security elements such as political stability, military security, and economic stability with non-traditional security fields such as cybersecurity and social stability, forming a positive ecological cycle for Dark Web crime governance and ensuring long-term peace and stability for the nation.

Acknowledgements

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

References

1. Luo, J. Z., Yang, M., et al. A survey on anonymous communication and the dark web. *Journal of Computer Research and Development*, 1(2019).
2. Xiao, Y. The Dark Web offensive of the Islamic State and its countermeasures. *Journal of Jiangnan Social University*, 1(2017).
3. Zhao, Z. Y., Zhang, X., Luo, Z., et al. A study on the application of the Dark Web and regulatory methods. *Knowledge Management Forum*, 1(2016).
4. Feds shut down largest Dark Web child abuse site; South Korean admin arrested. The Hacker News. https://thehackernews.com/2019/10/dark-web-child-abuse.html.(2019).
5. 6 billion personal information sets traded on the Dark Web; Prosecutors take action to safeguard cybersecurity. China Youth Online.http://m.cyol.com/gb/articles/2021-12/03/content_6nRGmfjpB.html.(2021).
6. Dark Web analysis report Part 3: BreachForums — A dying but unyielding giant. Anquan419. http://www.anquan419.com/news/21/2227.html.(2023).
7. NATO confidential military documents leaked on the Dark Web.Security Reference Network. https://www.secrss.com/articles/46745. (2022).
8. Stay alert! Sichuan police release top 10 typical cases from the "Net Clean 2020" special operation.CCTV News. https://m.news.cctv.com/2021/01/05/ARTIZFCFgI46XYSKWlcLhpbr210105.shtml .(2021).
9. Koch, R., et al.Hidden in the Shadow:The Dark Web-A Growing Risk for MilitaryOperations?2019 11th International Conference on Cyber Conflict.(2019).
10. Su, Z. T., Zhang, Y. Y., & Huang, Z. W. Research on Dark Web forensics. *Information Security and Communication Confidentiality*, 3(2021)
11. Pi, Y., & Zhang, M. C. Criminal legal regulation of cybercrime in China from the perspective of the overall national security concept. *Journal of Suzhou University (Philosophy and Social Sciences Edition)*, 1(2023).
12. FBI launches largest cyber operation in history, infiltrating 120 countries. Sohu E-Security. https://www.sohu.com/a/119818937_257305.(2016).

13. Li, Y. L. Research on Tor network website fingerprinting technology (Master's thesis). China People's Public Security University(2022).
14. Jiao, K. W. Research on China's response to Dark Web crime from the perspective of the overall national security concept. *Crime Research*, 6(2017).
15. The United Nations' draft convention on cybercrime is nearly completed.Security Reference Network. https://www.secrss.com/articles/62570 (2024).