IJLAI Transactions on Science and Engineering (ISSN: 3006-3418) 2024, vol. 2, no. 4, pp: 9–17

A Chinese View on Social Media and Its Implications on Cyber Security

Xiaoxu He[1]

Shenyang City University
110000 Shenyang, China
563118744@qq.com
Received Oct. 28, 2024; Revised and Accepted Nov. 16, 2024

Abstract. Social media development creates new challenges to the sphere of cyberspace security and privacy. WeChat and Weibo have also been targeted by phishers. This analysis places particular emphasis on how social networks influence information systems protection in China, including the aspects of strategic insights on enterprises, social governance, information security, and national security. It addresses both, major depth of reach, such as AI-based adversary reconnaissance, as well as the weaknesses-such as the use of social networks for global intelligence capture. It also discusses China's separation and individuals with the encompassing methods of containment including legal, as well as modern methods, to counter the unique threats posed by an uncontrollable landscape of social networks.

Keywords: Social media cybersecurity, China digital ecosystem, Data privacy, Phishing attacks, Cybersecurity threats, Artificial intelligence in cybersecurity.

1. Introduction

The Cybersecurity Law, which emphasizes cyberspace sovereignty, is essential to preserving national security. To reduce threats like phishing and data breaches, it requires social media companies to put strict data localization controls and strict monitoring mechanisms in place [1,2]. Millions of people in China now rely heavily on social media sites like WeChat, Weibo, and Douyin (TikTok), which are versatile instruments for information sharing, communication, and business. China has one of the world's fastest rates of social media usage as approximately a billion people go online. Out of this, WeChat has over 1.2 billion active accounts, peace several accounts. Such fora also foster increasing security risks in cyberspaces. Social media has increasingly been utilized by cybercriminals to spread disinformation impersonation-related thefts, and intrusions of private data. Of these, phishing is a rather serious issue hoisted upon society [3,4]. For example, a report from 2023 by the Tencent Security Lab tells us that more than 60% of phishing attacks conducted in China were carried out over social media networks. As a result, these strikes depended heavily on personal and corporate information. Many of these attacks result in data breaches, thefts of identity, and financial crime: hence the need exists for effective security reforms. The enormous complexity of China's digital environment brings cybersecurity challenges since it is the largest internet market in the world. This has however made the links between social media and cybersecurity important to the public and private sectors within China, The popularity of social media has led the government to impose strict regulations on these platforms to protect the sovereignty of the country. Initiatives such as the 2021 Data Security Law and the Cybersecurity Law adopted by the government have assisted in the construction of a legal framework aimed at protecting business information, personal privacy, and national security [5,6]. Under such legal provisions, social media and other internet-based firms have undergone severe limitations including censorship, local storage of data and compliance with stringent data security measures. The laws have raised debates about how one can enjoy privacy while a heavy-handed state goes about its other primary objectives like extenuating cyber threats.

In terms of cybersecurity, Chinese firmsłparticularly technology giants like Tencent, Alibaba, and ByteDance-are irreplaceable. Under this aspect, many firms including Company a acquired technology-artificial intelligence (AI) and machine learning (ML) as a way of upping their rivalry. For example, Tencent applies complex artificial intelligence-based algorithms on the WeChat ecosystem to track the actions of specific users highlighting such illegitimate activities as unauthorized access attempts as well as phishing. In the case of social media platforms, we were able to handle massive amounts of data generated through AI and ML and also notify anyone of any threat in real time [7-9]. They also block or censor out material that is not suitable for the consumer which can belong to a scam artist or contains unsuitable content. However, with the advent of artificial intelligence (AI), the picture changed because the attackers read more reliant on AI to carry out rampantly elaborate tricks like deep fake scams and AI-based phishing schemes. Likewise, cybersecurity has complemented the state's general plan of 'informational sovereignty' and the management of data exchange and digital infrastructure within the state's territory. Major social media companies are governed by Chinese legislation regulating Internet information services,

requiring Internet content service providers-so-called ICPs-to police and remove unlawful content that might endanger state security. Big data and artificial intelligence can help the government monitor the conversation on the internet, potential threats to cyber security and even control public opinion. While it has achieved aims of cutting cyber threats and controlling misinformation the extensive surveillance authority has made people concerned over state surveillance and declining privacy liberties and human rights. Other than cybersecurity regulation, some of the issues they have presented about their regulatory system exemplify fears about international cooperation and cross-border data transfer [10,11]. The Data Security Law of 2021 strengthened the control over data exports and narrowed down some previously allowed categories of data exports as sensitive or critical data. These rules are based on the apprehensions regarding the access that companies from other countries have to the data of users present in China, and have raised doubts about whether the social media organisations functioning in China, now or via their local offices and branches (TikTok for example), adhere to these rules while dealing with user data [12]. Even though these regulations serve the purpose of protecting the nation's security, these have again raised the horn sensationally about the role of China in the digital economy with tensions between data sovereignty and global digital connectivity and commerce.

In the same manner, cybersecurity has become part of the general program of "cyber sovranism," which established state control over information flows and digital structure within the state territory. Many social media organizations are governed by China's legal statutes concerning Internet information centres require Internet content providers to eliminate unlawful content that is potentially detrimental to national security. Big data analytics and artificial intelligence when applied to internet conversations help the government plan cybersecurity approaches and manage the public sentiments. While it has achieved near success concerning threats and managing misinformation, the sophisticated surveillance system has raised alarm with officials and eroded individual freedoms and the right to privacy. Besides, consisting of seven rules, the Regulation also showcases China's position towards cybersecurity and its domestic regulatory system, exploring the apprehension of international cooperation and cross-border data transfer. The Data Security Law of 2021 strengthened the regulation of cross-border transfer especially on sensitive or critical data. These restrictions come after issues about foreign firms' access to Chinese users' data- issues which have prompted questions as to how Chinese social media firms-including social media giants like TikTok that operate globallyCrespect the above-mentioned restrictions concerning users' data [13,14]. These regulations are aimed at securing the nation's security; however, they have contributed to rekindling controversies on the role of China in the contaminated and global digital economy focusing on the conflict on data ownership and global digital commerce and integration. Besides this; other social sites are used as instruments to disseminate knowledge concerning cyber security. The government and private companies have carried out campaigns to create awareness among the people on the dangers of using social media [15,16]. One more social campaign in WeChat and Douyin is about cyber security and unveils tips like avoiding phishing, using stronger passwords, and two-factor authentication. It is also thus the syncing point where cybersecurity experts exchange weaknesses, learn of new threats and offer solutions in real-time. Credible threat identification is a vital application of crowdsourced threat intelligence within China's social media platforms as it boosts the general resilience of cybersecurity as well as reciprocally boosts the capacity to address novel threats.

Twitter alone allegedly terminated over 70 million such profiles per month starting January to June 2018- the reality with open systems- and Chinese social media has gone through a much more drastic transformation after the incorporation of artificial intelligence learning into cyberspace security. Cognitive systems or AI systems are capable of ingesting large volumes of data to look for patterns and feature the kind that could be a forerunner to a cyber-attack [17]. These technologies have greatly minimized the cases of phishing attacks, data break-ins and other cyber-criminal incidences based on the fact that such social platforms can easily detect intruders and other unlawful individuals [18,19]. For example, a lot of the WeChat security system comes from AI algorithms that can analyze interactions between users, determine if there is any potential suspicious activity, and prevent unauthorized entrance into accounts. Inspired by these developments, however, AI systems have to evolve all the time to stay one step in front of ever more advanced cyber threats, so it is clear that there is still some way to go. Deepfakes represent a growing cybersecurity threat, as the use of AI-generated audio and video recordings is increasingly used for identity theft and fraud [20]. In China, social media cybersecurity rule-making is closely tied to a national cybersecurity objective of controlling cyberspace within states that call for "cyber sovereignty." The nation has one of the world's toughest regulatory systems, with laws mandating data localization as well as strict control of online content and a broad regulatory regime for social media companies. This, in turn, has led to debates over privacy and the role of government spying, however, and some of them within the scope of this regulatory apparatus as well. While these regulations are effective in protecting national security and preventing cybercrime, critics argue that they also provide the government with wide-ranging powers to monitor and control internet activity, raising issues related to personal privacy and freedom of speech. The role of social media in China's complex cyber environment bears a variety of relevant functions. While also performing the role of a communications platform for illegal (along with legal) activity, the dark web offers powerful slippery tools to aid

in identifying threats, understanding cybersecurity and preparing for crisis management [21]. The way by which China has regulated social media and cybersecurity reflects China's political and social realities, as it seeks to find a balance between fostering innovation and economic development, and its national security imperatives. Indeed, embracing state-of-the-art technology such as artificial intelligence (AI) and machine learning in security plans has enhanced the ability of social media companies to detect and disable threats, but it has also reflected some unique challenges. Maintaining a secure digital landscape as the role of social media and the general purpose web on which it runs continues to change the prospects of Chinese national security-shaping will depend heavily on the Chinese ability to amend not only its technology but its legal landscape.

2. The Digital Landscape in China

China enjoys an unusually high degree of connectivity in its digital ecosystem, thanks to the broad, fast adoption of mobile technologies as well as vigorous government efforts to bolster the country's internet architecture. This alone has made the country a front-runner in the digital field with some of the largest and most relevant social media networks in the world. Given its more than one billion active users, this provides a relevant example of WeChat, which is an essential tool for daily communications, business, and several other digital services [22].

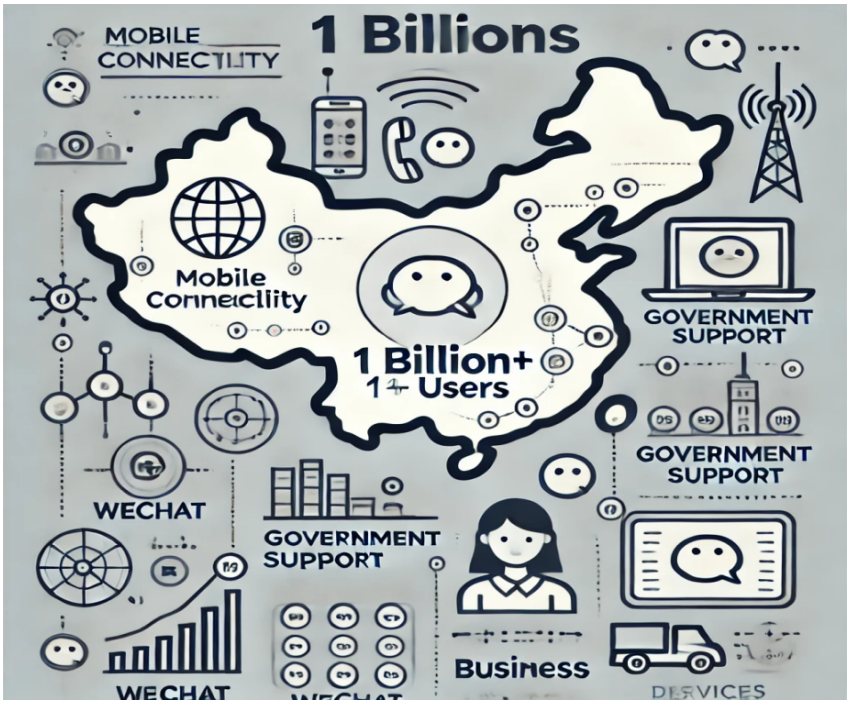

Fig. 1. The Digital Landscape in China

In addition, China's digital space is backed by a global-level e-commerce system, digital payment systems, and advanced technologies such as big data and artificial intelligence (AI). The fact is that it goes far beyond simple over-the-network socializing, though. Combined with these technologies has trimmed and transformed retail trading, healthcare and education businesses among others, thus placing China at the helm of the global digital economy.

It is anticipated that organisations all around the world are on the fast track to embrace digital strategies, there are real issues attached and one of the major issues is the cyber security issue. Due to the country's massive population surfing the internet and consequent high daily production of information, china is highly vulnerable to cyber threats. The hackers now get deeper, inside networks and the databases forming the framework of Chinese cyberspace; making it a threat not just to corporations but to national security too [23]. This constantly expanding digital environment is incredibly large and constantly becoming more challenging to safeguard, which has led to new and more than ever before security policies and frameworks to defend public and private organizations from these altering cyber threats. China has an unparalleled opportunity to tap into digitization as a source of competitive economic advantage and innovation, but it extends a unique perspective toward the threat of cyber threats one that casts an increasingly connected digital world continuing to expand by the hour.

2.1. Governmental Control and Regulation

The Cybersecurity Law of China permits the Chinese government a fair amount of data access generated in China while requiring that essential data be stored within the country. However, to achieve cyber sovereignty it also raises issues on freedom of speech as well as privacy. Article 37 of the law also requires data localization for any crucial infrastructure based on unrelated personal data, such as the data shared on social networks, including WeChat. The regulatory environment of the Digital ecosystem in China is unique because the state owns the information dissemination and data privacy systems. Apart from guaranteeing technological advancement, the social media & cybersecurity model of the country fulfil the bellowing national interest & derives the official controls. This legal structure is primarily formed by the Cybersecurity Law of 2017 and the Data Security Law of 2021, as both laws establish rules strictly for data and digital platforms companies in China. The Cybersecurity Law of 2017 is among the key acts aimed at improving the protection of the digital assets of the country [24,25]. This exposes network operators for example social networking companies and services to strict compliance requirements charge of handling potentially sensitive data as well as personal information. One of the most obvious elements of this law is that it states that many kinds of data must stay within China while exporting other types of data that can harm national security is prohibited. The law also mandates security audits and government assessments of state-controlled network hardware, to be carried out periodically as a tool for maintaining 'real control' over computerized networks in the state.

The Data Security Law of 2021 extends these rules by distinguishing data by its significance for economic stability and national security. It has tough legal requirements on data disclosure as well as on the international transfer of data, especially on sensitive or critical data. It also enforces severe punishment for noncompliance, showing how serious the state is about maintaining the tight reign of its digital platforms [26]. These regulations impose extensive security measures to protect data and comply with governmental demands that must be adhered to by companies and social media sites. They enhance the state's ability to observe social media and sanction violators of the regulations though the administration is likely to justify them as measures meant to protect the state from cyber threats. Critics argue that new rules bolster state control, whereby, for example, the government gets powers to monitor the usage of the internet and blockage of tempting or politically uncomfortable material. Postings related to human rights, protest or political change are often banned or erased on sites that are under scrutiny, particularly those of the social networking type. It raises questions as to how these rules encroach on the right of free speech and whether such excessive government surveillance of its citizens is feasible. Moreover, this legislation also has serious problems with privacy. While the difference between spying on people and securing computers is quite clear-cut, the state has extensive powers to monitor what people are doing online and to collect user data or spy on people's interactions. The level of state regulation raises concerns over the decline of civil liberties and human rights while the stated focus of the authorities is on the protection of the susceptible Infowarfare Cyberspace of the country. As the laws provide the state with this virtually exclusive control over what information is disseminated, who gains access to it or how residents conduct themselves on the Internet, residents may voluntarily abstain for fear of reprisal [27].

This regulatory structure is an example that we evidenced earlier in Chinese strategy as following a pattern of strict governmental control with advanced digital technologies. While it has provided China with a very effective base and security for a digital economy it has also placed the totality of the internet service directly under the discretion as well as control of the government, including the ability to control, monitor and erase content. These rules have long-term impacts that are not even restricted to cyberspace because they determine the way China's digital communication, business and civil liberties will evolve. Whether progressive legislation on social media or strengthened security measures in cyberspace, China's legislative model represents the ability to foster social innovation together with the creation of robust authority control [28]. One of the main components of this process is the Cybersecurity Law and Data Security Law, which imply the structure of digital security and at the same time allow for increasing the degree of governmental regulation. While all these regulations sought to protect national interests, these come with questions regarding freedom of speech, personal privacy and extent of the state scrutiny in China's evolving digital sphere.

2.2. Corporate Strategies

China Cybersecurity law compels home-grown social media giants in China such as Tencent, Alibaba, and ByteDance to safeguard the data of their users, regulate themselves on the monitoring guidelines set by the China government and enhance the cybersecurity of their platforms. Further, these businesses are applying AI to prevent hacking and phishing attempts like those recently increasing on social media.

Due to the influence of Chinese companies especially pioneer technological firms cybersecurity in the nation has been defined. Hyper Tet Protect has developed and implemented robust measures in place by giants like Tencent, Alibaba and Bytedance from internal and external threats. Pursuing ever higher technologies in their

industries, including AI and machine learning to detect and mitigate cyber risks, these entities provide full cooperation within government frameworks to strictly follow national security standards [29].

3. Social Media as a Double-Edged Sword in Cybersecurity

Due to the amount of Personal/financial information that goes through such sites as WeChat and Weibo, such sites are most susceptible to such attacks as phishing. However, these venues are focused by the Government for public campaigns dedicated to safe Internet use; therefore, they contribute to increasing awareness of the issue of cybersecurity. Social media platforms in China are double-sided in the realm of protecting cybersecurity: enabler and guardian. Since WeChat, Weibo, and Douyin have already become ubiquitous tools in our daily lives, malicious actors utilize immense amounts of users' data for malware distribution, phishing, and identity theft. On these networks, social engineering processes ł when the users themselves compromise the security ł are used rather widely. Also, the ever-increasing amount of information shared by social media users has attracted both domestic and foreign cyber spying thus posing a great security threat to the nation. People who work online should therefore ensure they exercise ethical and legal acceptable compliant use of the social media and also cultivate responsible digital citizenship [30,31].

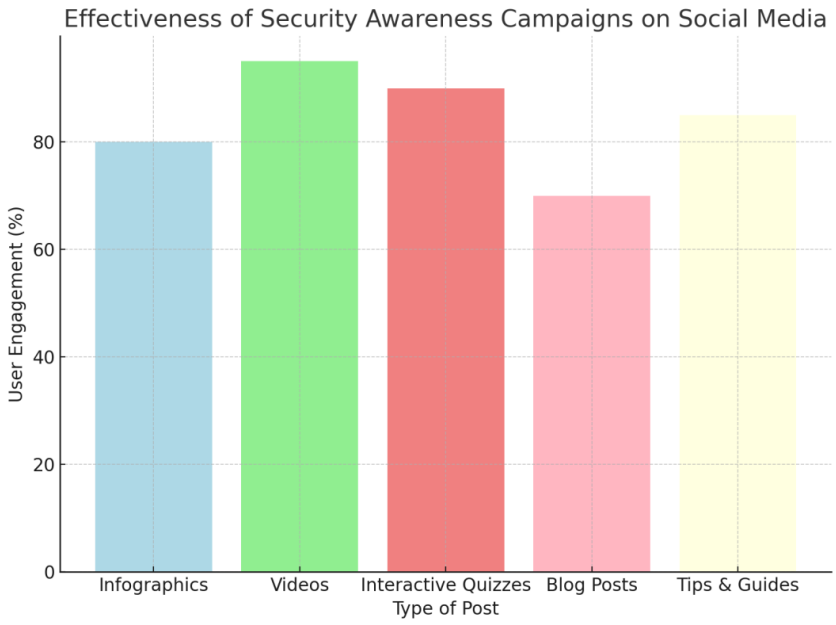

Fig. 2. Effectiveness of Security Compaigns on Social Media

But at the same time, social media is an important part of protecting against cyber threats as well. These platforms are employed by the Chinese government and companies to disseminate information on different types of cyber threats, enhance awareness, and teach people correct behaviour on the internet. To present, firms respond to criminality or threats to homogeneity through algorithms and machine learning that detect crime; and legislation such as the Data Security Law of 2021 and Cybersecurity Law of 2017 demand high-security systems. These rules that are a part of China's greater scheme of managing its online sphere require platforms to protect user's data and help in the government's surveillance efforts [32].

That is why it is necessary to not underestimate The strengths of social networking sites in promoting ethical behaviour among people in cyberspace, and in coordinating the collective efforts to provide Internet security despite the risks are obvious'. This way, reflecting the fact that cybersecurity in China is challenging to regulate further demonstrates that China is both an attack target and a defence instrument. The challenge is therefore in how it is possible to utilise those platforms for defence and at the same time manage the threats that come with connectivity.

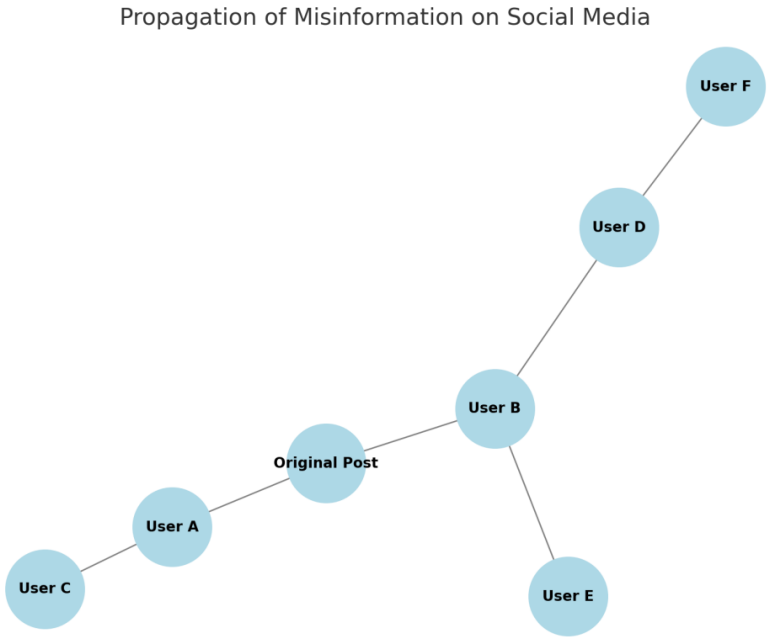

Fig. 3. Propagation of Misinformation on Social Media

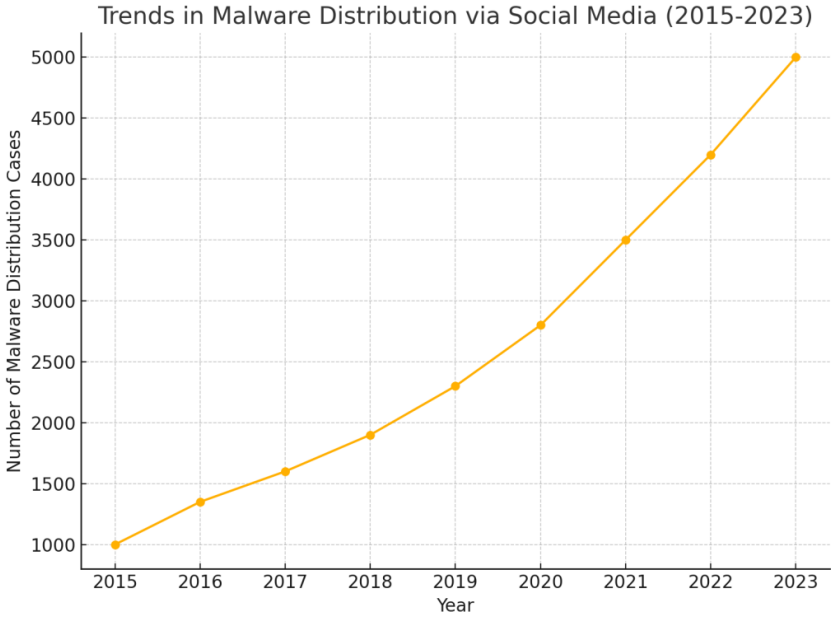

Fig. 4. Trends in Malware Distribution via Social Media (2015-2023)

4. The Role of Artificial Intelligence in Social Media and Cybersecurity

It is established that both AI and ML are becoming progressively significant in dictating cybersecurity on Chinese social media because they open up new avenues for cyberattacks, while also offering sturdier protection mechanisms than traditional security solutions. Due to the magnitude of these platforms-WeChat and Weibo, advanced artificial intelligent-driven security procedures are required to detect anomalies, monitor suspicious behaviour, and initiate self-healing mechanisms [33]. While machine learning helps cybersecurity systems improve their ability to detect threats by teaching them from prior attacks, AI can help detect phishing, malware, and fraud in real time [34]. AI is also useful in moderating content and also in eradicating all the prohibited information in other supporting legislations that promote order in society. The state thus has increased hold over social media through automated recommendation algorithms which are crucial in flagging political material and fake news.

However, artificial intelligence is also dangerous in the hands of hackers. Others are more advanced forms of attacks for example adaptive phishing and the deepfake-realistic fake content that can be applied to deceive users or spread fake information are made possible by some AI technologies [35]. Moreover, security algorithms can be controlled by adversarial machine learning that allows threats to be misclassified, and hence go unnoticed. In this context, AI and ML are two-folded sword in China's social media context. While modernising greatly enhances security, it also improves the capabilities for much harder, less easily distinguished intrusions. For this reason, China's perpetual endeavour is to evolve in military technologies to be aware of these novel perils [37-40].

5. Conclusion

China's plan for managing the digital space, particularly for social media management, is anchored on the Cybersecurity Law. It has given rise to problems with privacy, international collaboration, and the new generation of dangers from AI-supported cyberattacks while strengthening cybersecurity and developing data sovereignty. There are three major aspects of social media involvement in cybersecurity: The first is the penetrate-and-secure model, in which social media is an important tool for detection as well as a serious security threat given the nature of the digital environment in China. These present very real cybersecurity issues including misinformation, and data breaches but are also very useful tools for threat notification, awareness and management. An effective combination of using IT and maintaining cybersecurity, as well as creating the legal framework for Chinese international relations will be critical for the future development of China's IT. Methodologically, this paper provides a Chinese analysis of the intertwined phenomena of social media with an emphasis on cybersecurity. He highlighted that decision-makers, firms and cybersecurity professionals, can benefit a lot from the studies of the specific challenges and strategies adopted by China in facing the complexities in a world where digitalization is becoming the New Normal. To gain a clearer perspective on how to build successful cybersecurity measures in a world setting it will be imperative to consider China's strategy.

6. Conflict of Interest

The authors declare that there are no conflict of interests, we do not have any possible conflicts of interest.

Acknowledgments. None.

References

1. Wang A. Cyber Sovereignty at Its Boldest: A Chinese Perspective[J]. Ohio St. Tech. LJ, 2020, 16: 395.
2. Soomro T R, Hussain M. Social media-related cybercrimes and techniques for their prevention[J]. Applied Computer Systems, 2019, 24(1): 9-17.
3. Fan Y, Li H, Sun B. Cycle GAN-MF: A Cycle-consistent Generative Adversarial Network Based on Multifeature Fusion for Pedestrian Re-recognition[J]. IJLAI Transactions on Science and Engineering, 2024, 2(1): 37-44.
4. Yu J, Lu Z, Yin S, et al. News recommendation model based on encoder graph neural network and bat optimization in online social multimedia art education[J]. Computer Science and Information Systems, 2024, 21(3): 989-1012.
5. Parasol M. The impact of China's 2016 Cyber Security Law on foreign technology firms, and on China's big data and Smart City dreams[J]. Computer law & security review, 2018, 34(1): 67-98.
6. Liu J, Zhang J, Yin S. Hybrid chaotic system-oriented artificial fish swarm neural network for image encryption[J]. Evolutionary Intelligence, 2023, 16(1): 77-87.
7. Calzada I. Citizens data privacy in china: The state of the art of the personal information protection law (pipl)[J]. Smart Cities, 2022, 5(3): 1129-1150.
8. Zhou L, Wang T. Social media: A new vehicle for city marketing in China[J]. Cities, 2014, 37: 27-32.

9. Yin S, Li H, Teng L, et al. Attribute-based multiparty searchable encryption model for privacy protection of text data[J]. Multimedia Tools and Applications, 2024, 83(15): 45881-45902.
10. Ibrar M, Yin S, Li H, et al. Comprehensive review of emerging cybersecurity trends and developments[J]. International Journal of Electronic Security and Digital Forensics, 2024, 16(5): 633-647.
11. Mubarak R, Alsboui T, Alshaikh O, et al. A survey on the detection and impacts of deepfakes in visual, audio, and textual formats[J]. IEEE Access, 2023, 11: 144497-144529.
12. Yin S, Li H, Sun Y, et al. Data Visualization Analysis Based on Explainable Artificial Intelligence: A Survey[J]. IJLAI Transactions on Science and Engineering, 2024, 2(2): 13-20.
13. The internet, social media, and a changing China[M]. University of Pennsylvania Press, 2016.
14. Wan W S, Dastane D O, Mohd Satar N S, et al. What WeChat can learn from WhatsApp? Customer value proposition development for mobile social networking (MSN) apps: A case study approach[J]. Journal of Theoretical and Applied Information Technology, 2019.
15. Jarmon J A. The new era in US national security: an introduction to emerging threats and challenges[M]. Rowman & Littlefield, 2014.
16. Bui N S, Lee J A. Comparative Cybersecurity Law in Socialist Asia[J]. Vand. J. Transnat'l L., 2022, 55: 631.
17. Yin S, Li H, Laghari A A, et al. An anomaly detection model based on deep auto-encoder and capsule graph convolution via sparrow search algorithm in 6G internet-of-everything[J]. IEEE Internet of Things Journal, 2024, 11(18): 29402-29411.
18. Wang L, Shoulin Y, Alyami H, et al. A novel deep learning-based single shot multibox detector model for object detection in optical remote sensing images[J]. Geoscience Data Journal, 2024, 11(3): 237-251.
19. Jisi A, Yin S. A new feature fusion network for student behavior recognition in education[J]. Journal of Applied Science and Engineering, 2021, 24(2): 133-140.
20. Cai P, Chen L. Demystifying data law in China: a unified regime of tomorrow[J]. International Data Privacy Law, 2022, 12(2): 75-92.
21. Khan N F, Ikram N, Murtaza H, et al. Social media users and cybersecurity awareness: predicting self-disclosure using a hybrid artificial intelligence approach[J]. Kybernetes, 2023, 52(1): 401-421.
22. Kumar S, Gupta U, Singh A K, et al. Artificial intelligence: revolutionizing cyber security in the digital era[J]. Journal of Computers, Mechanical and Management, 2023, 2(3): 31-42.
23. Farid G, Warraich N F, Iftikhar S. Digital information security management policy in academic libraries: A systematic review (2010C2022)[J]. Journal of Information Science, 2023: 01655515231160026.
24. Yang J, Chen Y L, Por L Y, et al. A systematic literature review of information security in chatbots[J]. Applied Sciences, 2023, 13(11): 6355.
25. Yas N, Elyat M N I, Saeed M, et al. The Impact of Intellectual Property Rights and the Work Environment on Information Security in the United Arab Emirates[J]. Kurdish Studies, 2024, 12(1): 3931-3948.
26. Gowda V D, Kawale S R, Prasad K, et al. Technologies for Comprehensive Information Security in the IoT[C]//2023 International Conference for Advancement in Technology (ICONAT). IEEE, 2023: 1-5.
27. Alshurideh M, Alquqa E, Alzoubi H, et al. The effect of information security on e-supply chain in the UAE logistics and distribution industry[J]. Uncertain Supply Chain Management, 2023, 11(1): 145-152.
28. Pizam A, Ozturk A B, Hacikara A, et al. The role of perceived risk and information security on customers' acceptance of service robots in the hotel industry[J]. International Journal of Hospitality Management, 2024, 117: 103641.
29. Shaikh F A, Siponen M. Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity[J]. Computers & Security, 2023, 124: 102974.
30. Saeed S. Education, Online Presence and Cybersecurity Implications: A Study of Information Security Practices of Computing Students in Saudi Arabia[J]. Sustainability, 2023, 15(12): 9426.
31. Yu J, Zhao L. A novel deep CNN method based on aesthetic rule for user preferential images recommendation[J]. Journal of Applied Science and Engineering, 2021, 24(1): 49-55.
32. Yin S, Li H, Liu D, et al. Active contour modal based on density-oriented BIRCH clustering method for medical image segmentation[J]. Multimedia Tools and Applications, 2020, 79(41): 31049-31068.
33. Riemenschneider C K, Burney L L, Bina S. The influence of organizational values on employee attitude and information security behavior: the mediating role of psychological capital[J]. Information & Computer Security, 2023, 31(2): 172-198.
34. Zhu J, Feng G, Liang H, et al. How do paternalistic leaders motivate employees information security compliance? Building a climate and applying sanctions[J]. Journal of the Association for Information Systems, 2023, 24(3): 782-817.
35. Chua H N, Khor V V, Wong S F. Examining the effect of different knowledge aspects on information security awareness[J]. Information & Computer Security, 2023, 31(4): 427-448.
36. Yin S, Liu J, Teng L. A Sequential Cipher Algorithm Based on Feedback Discrete Hopfield Neural Network and Logistic Chaotic Sequence[J]. International Journal of Network Security, 2020, 22(5): 869-873.
37. Guaña-Moya J, Borja-López Y, Gutiérrez-Constante G, et al. Information Security Vulnerabilities Using Steganography as the Art of Hiding Information[C]//International Conference on Information Technology & Systems. Cham: Springer Nature Switzerland, 2024: 107-116.
38. Lysenko S, Marukhovskyi O, Krap A, et al. The Analysis of World Information Warfare and Information Security in the Context of the Russian-Ukrainian War[J]. Studies in Media and Communication, 2023, 11(7): 150.
39. Shaheen H, Singh M P. Multiclass skin cancer classification using particle swarm optimization and convolutional neural network with information security[J]. Journal of Electronic Imaging, 2023, 32(4): 042102-042102.
40. Alenazy S M, Alenazy R M, Ishaque M. Governance of information security and its role in reducing the risk of electronic accounting information system[C]//2023 1st International Conference on Advanced Innovations in Smart Cities (ICAISC). IEEE, 2023: 1-5.

Biography

Xiaoxu He is with the Shenyang City University. Research direction is computer application and AI.