Information and Knowledge Management (2025)
Clausius Scientific Press, Canada

DOI: 10.23977/infkm.2025.060105
ISSN 2523-5893 Vol. 6 Num. 1

Information Securitisation in China-US Relations: Adjusting the Neoliberal Order

Sijia Liu

Luoyang Normal University, Luoyang, Henan, 471000, China

Keywords: China-US relations, information securitisation, information and communication technology (ICT)

Abstract: This paper focuses on the securitisation of information and explores the impact of information technology on the political, economic, and social dimensions of China-US relations. It begins by reviewing the security challenges posed by the development of information and communication technology (ICT) and examines the differing perspectives of realism, liberalism, and constructivism in international relations theory, highlighting their respective limitations. The study then focuses on the TikTok incident, analysing the divergent stances and policy interactions between China and the United States regarding information governance and securitisation. By integrating theoretical frameworks with case studies, the paper proposes a comprehensive analytical approach to uncover the critical role of information security in the current global political and economic system and its implications for structural transformations in international relations. The findings demonstrate that the securitisation of information technology not only reshapes power distribution among states but also profoundly influences interaction patterns between state and non-state actors.

1. Literature Review.

1.1 The Evolution of ICT and Its Implications for Information Security

Since the 1970s, the rapid advancement of information and communication technology (ICT) has driven profound global transformations across political, economic, and cultural domains[1]. Telecommunication technologies, particularly the Internet, have not only elevated the value of information as a critical asset for political and business decision-making but have also facilitated the generation of vast quantities of data that often escape the regulation and control of sovereign states (Jarvenpaa & Ives: 1993; Strange: 1996, 2015; Boyd & Crawford: 2012; Morelli & Van Weelden: 2013). The decentralised nature of information distribution has further intensified concerns over secure access and storage, making it a particularly sensitive and pressing issue in the modern era[2]. Beyond the realms of politics and national security, information security concerns have permeated global business, cultural exchanges, and personal privacy (Ranstorp: 2007; Lyon: 2014; Bauman et al.: 2014; Janbek & Williams: 2014). As a result, ICTs now occupy a pivotal position at the intersection of contemporary global political, economic, and social relations. This evolution has increasingly securitised the ICT domain, highlighting its critical importance in addressing modern

security challenges.

1.2 Realist Perspectives on Information Security

Meanwhile, mainstream international relations theories present a fragmented and limited understanding of information security, with realists offering a predominantly state-centric interpretation[3-5]. Realist theory, exemplified by Waltz's (2010) state-centric framework, posits that states are the primary unit of analysis and prioritise military power as a key determinant of security (Mearsheimer: 2001). Consequently, realist interpretations of information security often remain confined to state-centric and militarised paradigms. For instance, Lonsdale (1999) conceptualises information technology as a supplementary factor in interstate conflict, focusing on its potential to alter traditional military strategies and geopolitical competition among states. Another strand within realist thought explores the weaponisation of ICTs. Taddeo (2012) examines how ICTs can be utilised as disruptive and cross-dimensional tools of conflict by political and military authorities. While realist theorists acknowledge the security risks posed by the information revolution, their analyses often overlook the role of non-state actors and the broader socio-economic implications of ICTs on global relations (Choucri & Goldsmith: 2012). This narrow focus limits the scope of realist theories in addressing the multifaceted nature of contemporary information security issues, which increasingly transcend traditional state-centric boundaries and encompass complex interactions between state and non-state actors[6].

1.3 Liberalist Perspectives on Information Security

The liberal understanding of information security is primarily rooted in the plurality of actors and the principle of economic interdependence (Keohane & Nye: 1973)[7-9]. Liberalism adopts a more optimistic stance towards the information revolution, emphasising its potential to foster global connectivity and cooperation. In their extended analysis, Keohane and Nye (1998) argue that ICTs enhance the interconnectivity and interdependence among states, thereby reinforcing international cooperation[10-11]. From this perspective, ICTs are perceived by liberalists as tools for economic development and peace rather than sources of risks or conflict. While some scholars, such as Arquilla and Ronfeldt (2001), have attempted to integrate liberal analytical categories—such as globalisation and the role of non-state actors—with information strategies and risks, information security remains largely underexplored within the liberal analytical framework. This omission limits the ability of liberalism to address the complexities of information security in a rapidly evolving digital landscape[12].

1.4 Constructivist Approaches to Securitisation

Constructivist theory offers a broader analytical framework capable of encompassing diverse security issues. A central tenet of constructivism is that international realities—such as interest, power, and anarchy—are not innate but are products of the interactive construction of actors (Wendt: 1992; Adler: 2002). Building on this foundation, the securitisation theory developed by the Copenhagen School analyses the agenda-setting process through which specific policy issues are framed as threats to national security via political speech acts (Eriksson & Giacomello: 2006)[13]. Although the Copenhagen School has provided a dynamic framework to address the evolution of the security agenda, it has not fully incorporated information security into its scope of research. Among the limited number of academics addressing security in the digital age, the primary focus has been on the socio-cultural dynamics that influence the policy agenda (Buzan et al.: 1998; Williams: 2003).

For instance, Everard (2000) highlights how information warfare has disrupted identity boundaries

across multiple dimensions, particularly how the identity and authority of sovereign states are being contested in the global digital era[14-17]. In his research on IT-related threats, Eriksson (2001a, 2001b) examines how security agendas are constructed through speech acts and how risks and responsibilities are distributed across various departments in political discourse[18]. Consequently, constructivism devotes considerable attention to the socio-cultural dimensions of the security agenda, providing valuable insights into how social and cultural factors shape perceptions of security in an increasingly interconnected world[19-20].

1.5 Limitations and Gaps in Current Theoretical Approaches

Although realist, liberalist, and constructivist schools have provided valuable insights into how ICTs influence international relations, their analyses of information security remain constrained by their respective ontological foundations[21]. Realism focuses predominantly on the military dimensions of information security, while liberalism highlights the relationship between ICTs and economic interdependence, often overlooking the associated security risks[22-23]. Constructivism, though offering a broad theoretical framework for understanding securitisation, tends to underexplore information security, confining its analysis to socio-cultural aspects. As a result, these schools of thought engage with different and isolated facets of information security in international relations, failing to capture its multifaceted and interconnected nature[24].

Furthermore, the information revolution has exposed significant gaps in the understanding of the relationship between the global system and the interactions of its actors. The development of ICTs aligns closely with the neoliberal globalisation model, which advocates reduced government regulation, privatisation, and lowered trade barriers. However, this model simultaneously challenges the authority of sovereign states and compels them to reassert control over the digital sphere (Sniegocki: 2008; Rennstich: 2010)[25-27]. While existing theories have explored how ICTs influence the global political economy and actors' interactions, they often neglect the implications of actors' policy responses in reshaping or adjusting the international system[28].

In conclusion, there is a notable absence of a comprehensive and consistent framework for analysing the dynamics of international security in the context of ICTs[29]. Current research in international relations provides only limited understanding of the complex interplay between actors and the global system, leaving significant gaps in the field.

2. Research Questions

2.1 Main Research Question

To address the research gap, this project aims to establish a theoretical framework that comprehensively examines the political, economic, and social dynamics of information security at the actor, interaction, and system levels. Therefore, this research seeks to answer the main question: 'How is information technology framed as a security issue, and how does it influence international relations in today's global political economy?'

2.2 Structural Changes in the Global System

The main research question can be divided into two sub-questions. First, 'How have ICTs changed state and non-state actors' structural position in the global system?' As discussed, sovereign states' identity and authority have been weakened by information and technologies that lie beyond their regulatory reach (Everard: 2000)[30]. Meanwhile, non-state actors, particularly multinational corporations, have amassed significant quantities of information, ranging from market trends to user

personal data. This accumulation of data contributes to their increasing role in shaping the global politico-economic landscape (Strange: 1996; Soussan & Trovati: 2021). Therefore, this question aims to explore how the information revolution redistributes political authority, economic resources, and social influence among state and non-state actors[31-33].

2.3 Securitisation of ICT

Second, 'How is ICT framed as a security issue?' This sub-question examines how the aforementioned changes in the international system contribute to the securitisation of ICTs. Essentially, the information revolution has altered not only the distribution of authority, resources, and power in the international system but also actors' perceptions of interest, risk, and threat. The transformation of, and conflict between, these perceptions and interests are integral to the securitisation of the digital sphere[34]. While securitisation is fundamentally a socio-cultural process, it has profound implications for actors' behavioural patterns, strategies, and policy responses. Furthermore, these interactions may produce structural outcomes, ranging from enhanced regulation to outright conflict (Aronson & Cowhey: 2010). By investigating the process of IT-related securitisation, this question further explores how the information security agenda shapes actors' behaviours and how actor-level interactions influence the broader international system[35-37].

3. Theoretical Framework and Methodology

3.1 Defining Information Security in Securitisation Theory

In terms of the theoretical framework, this project adopts Lundgren and Möller's definition of information security to further integrate political and economic factors into securitisation theory[38]. According to Lundgren and Möller (2017, 428), information security refers to a relationship in which an agent has "just the appropriate access to" specific information relative to the stakeholder. This definition provides significant scope for examining how the plurality of actors shapes the connotation of information security, as Lundgren and Möller (2017, 429) argue that "security is relativized to a particular stakeholder."

3.2 Actor Perception and System Dynamics

Under this definition, the importance and security of information depend on actors' perceptions of their interests, threats, and risks[39]. These perceptions are influenced by actors' subjective experiences, their interactions with other entities, and their structural positions within the international system. In the neoliberal global political economy, the decentralisation of information storage and management reflects a diffusion of sovereign states' authority (Strange: 2015). Consequently, the diminished control over ICTs is perceived as a national threat, prompting state governments to revise existing "free market" norms by enhancing domestic regulations, raising technological and trade barriers, and enacting legislation against foreign enterprises (Sniegocki: 2008).

3.3 Case Study: TikTok Incident in China-US Relations

Regarding research methods, this study adopts a qualitative case study approach to examine the TikTok incident within the context of China-US relations[40]. Although TikTok operates as a separate entity from its Chinese counterpart Douyin, it has been framed as a national security threat and subjected to restrictions in the United States (McMahon: 2024). Focusing on the broader discourse of

information security, the TikTok case illustrates the varying approaches of different nations to information governance, privacy concerns, and regulatory frameworks[41]. This makes the TikTok incident an ideal case for analysing the securitisation of information technology, shifts in actors' interaction patterns, and the impact of China and the US's policy responses on the neoliberal global system.

As this research focuses on both state and non-state actors, data collection will include an in-depth analysis of government policies, corporate reports, congressional hearings, and media coverage. By triangulating these diverse sources, the study aims to provide a comprehensive understanding of how the Chinese and US governments, as well as TikTok, perceive their interests and security concerns. Subsequently, the research will explore the political, economic, and social factors shaping these perceptions and assess whether such perceptions are compatible[42-43]. Finally, it will examine the speech acts and policy responses of the involved actors, which contribute to reframing the information security agenda to their advantage, and analyse how these interactions influence the "free market" norms of the current international system (Sniegocki: 2008). Specifically, the study will investigate how China and the US reorganised their administrative authority and control over the digital sphere through politico-economic regulations and barriers.

4. Timeline

The research process can be divided into four stages. In the first year of the PhD studies, the primary objective involves conducting a comprehensive literature review and critically analysing realist, liberal, and constructivist theories. For the second year, the main goal is to develop the theoretical framework of information technology, actor-level interaction, and the international system, which will result in the production of one paper. The focus of the third year is to carry out an empirical study of the TikTok incident, including data collection and analysis. Research findings at this stage will be synthesised into another paper. Lastly, the fourth year will primarily focus on refining the previous research and completing the PhD thesis.

5. Contribution

The contribution of this project is twofold.

First, it establishes a more comprehensive framework that integrates the realist, liberal, and constructivist perspectives on information security. While these schools conceptualise information security based on their respective ontological foundations, this project highlights that ICTs lie at the intersection of the political, economic, and social dimensions of today's international system. This ontological approach provides a broader and more flexible framework for analysing power dynamics, resource distribution, and socio-cultural factors involved in the securitisation of information technology. Moreover, it addresses the existing research gap concerning the interaction between actors and the international system. By focusing on actors' agency and their efforts to reshape the international structure through domestic regulations and foreign policy, this project seeks to connect the dynamics of information security at both the actor and system levels. This framework may also demonstrate broader applicability in fields such as international trade.

Second, the project provides a systematic analysis of information security in the context of China-US relations. Beyond examining the shifting relative power of the two countries in the realm of information technology, it investigates the structural factors that have influenced their perceptions of ICTs, national interests, and potential threats. The case study of the TikTok incident explores the growing significance of corporate actors in domestic and international politics, information security governance, and the construction of online identities (Everard: 2000). While economic interdependence between China and the US mitigates the likelihood of direct military conflict, their

ongoing disputes over information security highlight how previously neutral fields can quickly become arenas for competition over authority, resources, and discursive power.

6. Conclusions

This study provides a comprehensive analysis of the securitisation of information technology (ICT) in the context of China-US relations, addressing its implications for the global political and economic system. By integrating realist, liberalist, and constructivist perspectives, the paper highlights the multifaceted and interconnected nature of information security, transcending traditional state-centric or socio-economic frameworks.

The findings underscore that the securitisation of ICT not only redefines power dynamics between state and non-state actors but also challenges the existing neoliberal global order. Through the case study of the TikTok case, this research examines how securitisation processes impact perceptions of risks and priorities, adapt international norms, and influence the interactions of stakeholders in the digital sphere. These developments in global governance highlight the need for a comprehensive analysis of political, economic, and socio-cultural dimensions in the context of information security.

Furthermore, the study reveals the growing significance of corporate actors in the securitisation process, as exemplified by TikTok's role in China-US relations. This reflects a broader trend in which multinational corporations increasingly shape international security agendas and influence policy outcomes. The findings suggest that future research should further explore the implications of non-state actors in shaping security dynamics in a digital age.

In conclusion, this research contributes to the existing body of knowledge by proposing a more comprehensive and flexible framework for analysing information securitisation in international relations. By connecting actor-level interactions with systemic transformations, it sheds light on the evolving role of ICT in global security and provides valuable insights for policymakers seeking to navigate the complexities of the digital era.

References

[1] Adler, E. (2002) "Constructivism and International Relations," in Carlsnaes, W., Risse, T., and Simmons, B.A. (eds) Handbook of International Relations. London: Sage.

[2] Aronson, J.D. and Cowhey, P.F. (2010) "The Information and Communication Revolution and International Relations," in Oxford Research Encyclopedia of International Studies. Oxford University Press.

[3] Bauman, Z. et al. (2014) "After Snowden: Rethinking the Impact of Surveillance," International Political Sociology, 8(2), pp. 121–144.

[4] Boyd, D. and Crawford, K. (2012) "Critical Questions for Big Data," Information, Communication & Society, 15(5), pp. 662–679.

[5] Buzan, B., Wæver, O. and de Wilde, J. (1998) Security: A New Framework for Analysis. Lynne Rienner Publishers.

[6] Cha, V.D. (2020) "Allied Decoupling in an Era of US–China Strategic Competition," The Chinese Journal of International Politics, 13(4), pp. 509–536.

[7] Choucri, N. and Goldsmith, D. (2012) "Lost in cyberspace: Harnessing the Internet, international relations, and global security," Bulletin of the Atomic Scientists, 68(2), pp. 70–77.

[8] Clapton, W. (2011) "Risk in International Relations," International Relations, 25(3), pp. 280–295.

[9] Eriksson, J. (2001a) "Cyberplagues, IT, and Security: Threat Politics in the Information Age," Journal of Contingencies and Crisis Management, 9(4), pp. 200–210.

[10] Eriksson, J. (2001b) "Securitizing IT," in Eriksson, J. (ed.) Threat Politics: New Perspectives on Security, Risk and Crisis Management. Aldershot: Ashgate.

[11] Eriksson, J. and Giacomello, G. (2006) "The Information Revolution, Security, and International Relations: (IR) relevant Theory?" International Political Science Review, 27(3), pp. 221–244.

[12] Freund, C. et al. (2023) "Is US Trade Policy Reshaping Global Supply Chains?" Policy Research Working Paper, World Bank Group [Preprint].

[13] Janbek, D. and Williams, V. (2014) "The Role of the Internet Post-9/11 in Terrorism and Counterterrorism," The Brown Journal of World Affairs, 20(2), pp. 297–308.

[14] Jarvenpaa, S.L. and Ives, B. (1993) "Organizing for Global Competition," Decision Sciences, 24(3), pp. 547–580.
[15] Kaska, K., Beckvard, H. and Minarik, T. (2019) Huawei, 5G and China as a Security Threat, NATO Cooperative Cyber Defence Centre of Excellence.
[16] Keohane, R.O. and Nye, J.S. (1998) "Power and Interdependence in the Information Age," Foreign Affairs, 77(5), p. 81.
[17] Keohane, R.O. and Nye, J.S., Jr (1973) "Power and interdependence," Survival, 15(4), pp. 158–165.
[18] Lewis, J.A. (2024) TikTok and National Security, Center for Strategic & International Studies. Available at: https://www.csis.org/analysis/tiktok-and-national-security (Accessed: August 20, 2024).
[19] Lonsdale, D.J. (1999) "Information power: Strategy, geopolitics, and the fifth dimension," Journal of Strategic Studies, 22(2–3), pp. 137–157.
[20] Lundgren, B. and Möller, N. (2017) "Defining Information Security," Science and Engineering Ethics, 25(2), pp. 419–441.
[21] Lyon, D. (2014) "Surveillance, Snowden, and Big Data: Capacities, consequences, critique," Big Data & Society, 1(2), p. 205395171454186.
[22] McMahon, L. (2024) US TikTok ban: When and why could the app be outlawed? BBC News. Available at: https://www.bbc.co.uk/news/technology-53476117 (Accessed: August 20, 2024).
[23] Mearsheimer, J.J. (2001) The Tragedy of Great Power Politics. W. W. Norton & Company.
[24] Morelli, M. and Van Weelden, R. (2013) "Ideology and information in policymaking," Journal of Theoretical Politics, 25(3), pp. 412–439.
[25] Neilson, D. (2021) "Reversing the catastrophe of neoliberal-led global capitalism in the time of coronavirus: Towards a democratic socialist alternative," Capital & Class, 45(2), pp. 191–213.
[26] Nye, J.S. (2009) Soft Power: The Means To Success In World Politics. Hachette UK.
[27] O'Neill, B. (2001) "Risk Aversion in International Relations Theory," International Studies Quarterly, 45(4), pp. 617–640.
[28] Qian, X. (2019) "Cyberspace Security and U.S.-China Relations," in Proceedings of the 2019 International Conference on Artificial Intelligence and Computer Science. New York, NY, USA: ACM. Available at: http://dx.doi.org/10.1145/3349341.3349495 (Accessed: March 26, 2024).
[29] Ranstorp, M. (2007) "The virtual sanctuary of al-Qaeda and terrorism in an age of globalization," in Eriksson, J. and Giacomello, G. (eds) International Relations and Security in the Digital Age. Routledge, pp. 51–76. Available at: http://dx.doi.org/10.4324/9780203964736-10 (Accessed: March 26, 2024).
[30] Rennstich, J.K. (2010) "The World System in the Information Age: Structure, Processes, and Technologies," in Oxford Research Encyclopedia of International Studies. Oxford University Press.
[31] Salganik, M.J. (2019) Bit by Bit: Social Research in the Digital Age. Princeton University Press.
[32] Sniegocki, J. (2008) "Neoliberal Globalization: Critiques and Alternatives," Theological Studies, 69(2), pp. 321–339.
[33] von Solms, R. and van Niekerk, J. (2013) "From information security to cyber security," Computers & Security, 38, pp. 97–102.
[34] Soussan, T. and Trovati, M. (2021) "Social Media Data Misuse," in Lecture Notes in Networks and Systems. Cham: Springer International Publishing, pp. 183–189.
[35] Strange, S. (1996) The Retreat of the State: The Diffusion of Power in the World Economy. Cambridge University Press.
[36] Strange, S. (2015) States and Markets. Bloomsbury Publishing.
[37] Taddeo, M. (2012) "Information Warfare: A Philosophical Perspective," Philosophy & Technology, 25(1), pp. 105–120.
[38] Thrush, G. and Maheshwari, S. (2023) "Justice Dept. Investigating TikTok's Owner Over Possible Spying on Journalists," The New York Times, 17 March. Available at: https://www.nytimes.com/2023/03/17/us/politics/tik-tok-spying-justice-dept.html (Accessed: March 26, 2024).
[39] Tiller, J.S. and Fish, B.D. (2004) "Packet Sniffers and Network Monitors," in Tipton, H.F. and Krause, M. (eds) Information Security Management Handbook. Boca Raton: Auerbach.
[40] Waltz, K.N. (2010) Theory of International Politics. Waveland Press.
[41] Wendt, A. (1992) "Anarchy is what States Make of it: The Social Construction of Power Politics," International Organization, 46(2), pp. 391–425.
[42] Williams, M.C. (2003) "Words, Images, Enemies: Securitization and International Politics," International Studies Quarterly, 47(4), pp. 511–531.
[43] Yan, X. (2019) "Strategic Competition between China and the United States in the Digital Age," World Political Studies, 2.