Journal of Computational Social Science (2025) 8:24
https://doi.org/10.1007/s42001-024-00346-8

RESEARCH ARTICLE

Exploring China's cyber sovereignty concept and artificial intelligence governance model: a machine learning approach

Ho Ting Hung[1]

Received: 14 August 2024 / Accepted: 24 November 2024

Abstract

The current global cyber governance model is dominated by Western liberal norms and multi-stakeholder values. Dissatisfied with the status quo, some developing countries like China embrace another governance concept called cyber sovereignty, which advocates more state control. Meanwhile, AI development further enlarges cyberspace's national security threats, but an international governance framework is absent in the AI realm and China is eager to take the lead in building one. This gives rise to the question: what explains China's approach to cyber and AI governance? Current studies on cyber sovereignty and China's AI governance model are mostly qualitative and/or have a small sampling frame, while the meaning of cyber sovereignty is debatable. Therefore, this article applies topic modelling to official/semi-official texts about cyber and AI governance to understand the cyber sovereignty concept and how it shapes China's approach to AI governance. This article finds that cyber sovereignty is an extension of China's state-centric view of international order. Not being a passive recipient of norms, China hopes to shape alternative cyber norms to defend national security. Now, since the global community has not reached a consensus over global AI governance, China is exploiting this gap to promote its own set of cyber visions.

Keywords China · Cyber sovereignty · AI governance · Cyber governance · Machine learning · Computational IR

✉ Ho Ting Hung
bosco.hung@politics.ox.ac.uk
https://www.politics.ox.ac.uk/

[1] University of Oxford, Manor Rd, Oxford OX1 3UQ, England

Published online: 04 January 2025

Introduction

Currently, the West is dominating resources, technological standards, norms, and the discourse power of the cyber realm [14]. This shapes a Western-centric global cyber governance model promoting the participation and collaboration of technical communities, civil society, and the private sector [26, 78]; fundamental rights like human rights, transparency, and democracy [90]. Therefore, it is often seen as serving to realize the Western vision of an integrated, liberal, and democratic world [55]. While Western countries have espoused a free and open view of the Internet, non-Western countries like China, Russia, Brazil, and South Africa have challenged this status quo and some defended another approach: cyber sovereignty [24, 39, 52].

China was among the earliest countries to advocate a closed cyber system tightly controlled by state authority. It consistently iterates that cyberspace falls under national sovereignty where the government is the most important rule executor and maker [99, 111]. During the 2000s, China already criticized the current multi-stakeholder cyber governance models for marginalizing government authority and granting other stakeholders excessive interventional power. In 2010, it published the *White Paper on the Internet in China* which first mentioned cyber sovereignty (State Council Information [96]). Since then, the notion has been consistently asserted in various official documents, laws, and declarations [13].

Considering China's rising international status and cyber capacity, its quest for cyber sovereignty particularly deserves attention. Its gigantic online population and active developing ICT sector made China increasingly considered an ideal partner of non-Western states seeking to challenge the US hegemony [39]. Therefore, it has the capacity, support, and potential to challenge the Western cyber governance leadership. Despite the significance of China's revision of the current cyber governance model, scholars have surprisingly not yet reached a consensus over China's direction, which makes a re-examination of it necessary.

Meanwhile, the rise of artificial intelligence (AI) indicates an ever-faster evolvement of technological capabilities for processing data, manipulating information, and expanding online information operations [4, 34, 48, 64], further raising cyberspace's strategic importance. Meanwhile, unlike most technologies like the internet, telecommunications and space technology, norms and institutions are yet to be created in the AI governance field. China has accordingly enthusiastically expressed its eagerness to lead AI governance to regulate its development and deployment [61]. This gives rise to the importance of understanding China's AI governance visions and the underpinning values, which could (re)shape international norms sooner or later.

To examine what norms govern the emergence of AI, one place to seek the answer would be China's existing approach to cyber governance. This article will show how China's cyber norms are structuring China's approach to a new technological area: the AI realm, with the scope lying in the political and international governance aspects. Military technology applications, economic development, domestic issues (e.g. defamation, scamming) and other

non-political/governance aspects are not covered since they deal with specific and technical issues and/or do not articulate governance norms. I address the following questions by applying topic modelling to official/semi-official textual materials: What norms underpin China's approach to cyber and AI governance? What explains the evolution of norms in the AI realm?

This article makes three main contributions. First, it fills the literature gap about the relationship between China's development of cyber sovereignty and AI governance, thus facilitating the study of the evolvement of China's role in emerging realms. This contribution is timely as China is actively advocating alternative cyber and AI models, while often linking discussions of the two realms together. Second, it introduces the first quantitative machine learning study on China's cyber sovereignty and AI governance, covering both official and state-affiliated textual materials. By addressing the existing literature's shortcoming of covering a relatively small sampling frame, this article adjudicates a contested conceptual interpretation of China's governance visions. Third, while current analyses of norm theory are dominated by qualitative approaches, this article puts forward a quantitative methodological framework [77], which will benefit future scholarly examination of textual data which observes a growing complexity and volume, yet helpful for informing norm emergence.

This article proceeds as follows. First, I review existing literature on China's cyber sovereignty and AI governance approach. Second, I explain the theoretical framework and hypotheses. I then lay out its methodology. Subsequently, I present the analysis results. Finally, I offer some discussions and outline the broader implications.

Literature review

Chinese cyber governance approach

China's approach to cyberspace is largely affected by its emphasis on sovereignty, which provides this study with the context of why China is enthusiastic about managing the virtual sphere. Studies have established that while sovereignty was a concept imported to China, China actively defends and seeks sovereignty, especially Westphalian sovereignty [22, 32, 100].[1] Westphalian sovereignty is primarily about the idea of final and absolute political authority within a state. Its key principles include political independence, territorial integrity, equality in law, and non-intervention [43]. As China considers a state's political status unquestionable, it has made use of (Westphalian) sovereignty as a shield against outside interference and an instrument for achieving its territorial ambitions [16, 22, 32, 58, 72, 100]. This shield is also applied to resisting the spread of Western norms. Insisting that

[1] As this article's focus is not on unfolding China's general conception of sovereignty, this sub-section will not explain all its historical evolution, variants, and debates thoroughly, such as the debate about China's imperialist/hierarchical conceptions of sovereignty and the so-called *tianxia* idea [15, 100, 74, 75].

a country's development progress, culture, and values should be considered when advancing liberal claims, China disregards democracy and human rights as having universality. It considers the Western implementation of relevant international laws subjugation attempts disrespecting its political authority and infringing its sovereignty [22, 42, 71]. However, the spread of such norms is especially facilitated by the Internet's transnational nature and its rise, which increase the ease of creating, finding, and spreading anti-state information, including Western liberal ideas. This threatened China's one-party state rule and centralized information control model, bringing a need to govern cyberspace to protect sovereignty [90, 99, 109].

The *cornerstone* of China's vision for global cyber governance is cyber sovereignty [17], which is characterized by the following dimensions reflecting China's active defence of state authority and Westphalian sovereignty: (1) Information or discourse control for protecting the state from unfavourable narratives spread online [13, 17, 49, 69, 73, 90, 99, 109], (2) data regulations for strengthening state control over corporate data (e.g. data localization, legal jurisdiction rights of virtual data) [21, 23, 44, 90], (3) Security enhancement of technological industry and structure for reducing vulnerability to foreign influence and asserting the state predominance in cyber technology development (e.g. expanding domestic technological capacity, promoting national security checks of supply chain components, setting international cybersecurity standards) [23, 44, 90].

Although cyber sovereignty remains a concept upholding state authority, it remains contested to what extent cyber sovereignty is a state-centric concept and this study mediates this debate. There are three competing accounts about how absolute state control is under the concept and why it is the case: (i) China advocates state leadership in cyber governance and rejects multistakeholderism [24, 65], (ii) Considering non-state actors important collaborators on cyber issues, China advocates a multilateral model which promotes state leadership but accepts their participation [13, 14, 21, 99]; (iii) there is no consensus within China on what cyber sovereignty is and how it can be exercised, so we cannot determine the concept's exact position [98, 109]. As further examination of the concept's position remains necessary to settle the debate, this study revisits relevant government discourse and applies a quantitative approach to evaluate what cyber norms China is hoping to promote.

This study also adds to the literature exploring the reasons behind China's promotion of a new international cyber governance model. Many scholars interpret this move as a promotion of a new norm for promoting state control, thus contesting against Western liberal and multi-stakeholder norms and shaping the global internet governance order in its favour [17, 65, 109, 70, 109, 17] further suggest that China hopes to encourage other states, especially authoritarian ones, to adopt a more state-centric approach, thereby legitimizing and regaining state control of the online sphere. Nonetheless, these scholars have ignored China's developing country status, which Cai [14] deemed important. He stresses that the developed West writes international cyber norms to reflect its interests, so the participation between developed countries and China in establishing cyber governance is unequal. This re-orients us to acknowledge China's developing country status is important in explaining why China opposes the current Western monopolization

of cyber governance. Incorporating historical power hierarchies into the analysis of alternative norm promotion can help better understand China's behaviour and the corresponding intention. Built upon this insight, this paper can more effectively assess how state-centric China's approach is because its fear of sovereignty erosion could influence its degree of acceptance of non-state stakeholders' participation in cyber governance.

Moreover, this study hopes to address the existing methodological gap resulting from the dominance of qualitative studies on cyber sovereignty and governance, which are primarily built on qualitative discourse, content, and/or historical analysis [6, 44, 65, 94, 98, 109]. Others remain conceptual papers or commentaries drawing from official documents and key academic writings [13, 47, 68]. The above qualitative analyses tend to have a small sampling frame confined to a specific language/audience group, with most of them focusing exclusively onChinese-language publications (e.g. academic articles, newspapers, commentaries, policy documents, and elite discourse) which generally targets domestic audiences [6, 44, 98, 109]. Admittedly, qualitative analyses allow in-depth examinations of *specific* conceptual nuances and how the concept is communicated in a *specific* setting. However, collecting materials from more occasions and official/semi-official channels will benefit our understanding of it in a *general* manner and thus address the academic disagreement over the concept's meaning—and this will require a quantitative approach given human's limited processing power in addressing a larger frame of documents.

There is an existing scarce attempt involving quantitative components, but its sampling frame remains relatively small: Brehm [12] applies qualitative close reading on a set of internet-related articles to explore China's strategic narratives, and then uses quantitative analysis to identify discourse shifts to test replicability. Acknowledging that previous studies mainly focus on materials directed at domestic audiences, he uses an English-language state-affiliated media *Global Times* as a source to analyse the concept, but the sampling frame remains relatively small as he restricts the study to a single media source. There remains a gap for this study to apply quantitative analysis to a larger frame of relevant discussions to adjudicate the contestation about the meaning of the cyber sovereignty concept.

Chinese global AI approach

Here I turn to review literature on China's global AI governance approach. Note that related scholarly literature is limited. This could be explained by first, the relatively new nature of AI development. China's first *Global AI Governance Initiative* was released on 18/10/2023 [67], second, scholars' tendency to analyse specific application areas of AI (e.g. healthcare and education) instead of general AI governance [51, 97]. Nonetheless, Sheehan [92] suggests China's national AI governance model could be a reference for writing global rules and norms. Similarly, [20] suggest China can extrapolate its system to shape global AI standards. Therefore, discussions of national AI governance can still help us understand

China's vision of global AI governance. This offers us the advantage of having a wider source for examining a single issue, while maintaining relevance without ignoring related affairs.

Existing literature characterizes China's global AI approach, as covering the following dimensions: (i) information control and stability maintenance for mitigating information manipulation and spread of anti-state narrative [84, 92, 93], (ii) strengthening national control of data and downplaying individual privacy [10, 61], (iii) standards-setting of safety procedures and ethical norms [4, 28, 37, 61, 90, 107, 108]. They, again, reflect China's eagerness to strengthen control to defend its sovereignty. This aligns with my former literature review that China is fear of the erosion of state authority.

While the aforementioned discussions suggest China's AI governance model is state-centric, some Chinese scholars argue that philosophical and cultural practices can shape China into embracing a more open approach, and this study adds to the literature by joining the debate between these two views. Cheng [19] considers Chinese AI governance principles highlighting the importance of harmony and cooperation among individuals, society, and AI. This should imply China will acknowledge the merits of multistakeholderism and the significance of non-state actors. Besides, Song [95] argues that traditional Chinese philosophies (Confucianism, Buddhism, Taoism) share a non-anthropocentric moral root which implies AI and humans can co-exist harmoniously, so the Chinese community is less suspicious and fearful of AI. In this sense, China's AI discourse should be less security-focused and more external-looking. Nonetheless, Roberts et al. [84] criticize that it is unclear from China's government documentation what roles such cultural values should play in AI governance. The emphasis on harmony can be politicized to justify state suppression of individual rights and reassert state authority in AI governance instead. This points us to the need to examine the actual content of relevant government discourse to understand whether and how such cultural elements are translated into practice, which would have an implication on the question of whether China sees AI as a significant threat to its government authority and whether it allows non-state actors to participate in its governance.

When answering what drives China to establish global AI governance norms, studies indicate that the absence of governance norms and institutions gives China the strategic room to realize its leadership ambitions [20, 27, 108]. Ding et al. [28] further link China's eagerness to establish *global AI governance* to its inferior status in establishing *cyber governance*. China hopes to avoid exclusion from the rule-setting process again, so it actively discusses building new governance norms. This implies that cyber sovereignty can be an underpinning value of AI governance and examining China's developing country status is crucial to understanding its norm promotion. It also informs this study that China's promotion of alternative global governance norms should not be read as simply conflicts of interests or values. Western ignorance of its interests is important in explaining China's eagerness to establish new norms. Considering China's historical status in global governance can thus establish a useful starting point for understanding its behaviours and genuine intentions.

Another implication is that cyber and AI governance is largely different from other governance issues, which provides this study with the justification to examine the two fields together. Literature has maintained that no universal approach defines China's approach to global governance and China could adopt different approaches to different issues within the same governance regime, so its approach to a single domain may not help us understand its approach to another domain. For instance, China applied multilateralism in the context of space station operation, but bilateralism in the case of lunar governance [36, 54]. In this sense, examining cyber and AI governance using the lens or together might lack relevance. However, Ding et al.'s [28] account indicates specifically, China's approach to the cyber domain can be extended to the AI domain. This can also be confirmed by the previous literature review which suggests that discussions on the characteristics of China's AI governance share similar patterns with those on cyber sovereignty and governance, i.e. information control, data control, and standard-setting. Examining cyber and AI governance visions together is thus particularly relevant and plausible, instead of being overly reductionist, in this specific case.

Methodologically speaking, current studies on China's AI governance vision mainly explore academic and scientific writings [10, 38] or national-level strategy and policy documents [84, 85, 92, 107]. They ignored press releases, state-affiliated media articles, and government commentaries which also inform official stances and/or directly communicate with the international audience. Others remain conceptual articles or analyses [20]. In this sense, the same methodological gap in the discussions about cyber governance applies to the AI realm, in which most analyses cover a limited source of data. To capture the whole picture of China's global AI governance vision, we need a wider sampling source, which can be analysed effectively using quantitative methods.

Such research gaps lead to my overarching design: applying an automated text analysis on official and state-affiliated textual materials about China's discussion of cyber sovereignty and AI governance. This article provides an empirical test about how China's subsidiary status explains its desire to rewrite norms about cyber and AI governance, while adjudicating the academic debate about how state-centric China's approach is.

Theoretical framework and hypothesis

As the literature review suggests the need to consider China's developing country status, this article applies the norm subsidiarity theory to explain what drives China's approach to cyber and AI governance. Norms are commonly known as 'a standard of appropriate behavior for an actor with a given identity' [35], p. 891). They provide a *logic of appropriateness* which defines acceptable justification for an actor's behaviour [62]. While early norm literature treats norms as stable objects which diffuse linearly [31, 106], norms are subject to contestation even if the recognition that a norm exists will structure actors' behaviour [76, 103, 105].

Existing norm contestation literature tends to analyse how powerful actors exploit their power to challenge new norms [50, 89] or treat new norms as a function of

existing or fundamental norms under socialization [3, 104]. However, fundamental norms tend to be established by current powers, so such accounts confine norm contestation to the structural limits set by the existing rules primarily built by strong actors. This downplays the possibility that weak actors can reject fundamental norms and promote their own set of norms, which is what this article is studying.

In contrast, Acharya [1] develops a bottom-up approach addressing the role of weaker actors to study norm evolution: norm subsidiary. Norm subsidiarity is defined as 'a process whereby local actors create rules with a view to preserve their autonomy from dominance, neglect, violation, or abuse by more powerful central actor' [1], p. 97). As the post-war international system has been largely dominated by Western states who Marginalized weaker states (or in general, non-Western states) from the global norm-making process. Accordingly, the rules the West sets do not always reflect the ideas, interests, and identities of weaker states. Norm subsidiarity is therefore a response to the tyranny of the stronger states, implying that states are not necessarily passive recipients of established norms [1, 2].

The norm subsidiarity theory is especially applicable to this article because norm contestation among developed and developing countries is common in the cyber governance realm. As mentioned, developing and middle-income states including China have discursively criticized the current West-dominated status quo. As the literature review shows, being a late-comer to internet technology, China is in a disadvantaged position in the norm-making process. In contrast to its economic size and material achievements, China has often downplayed its status to legitimize its defense of national interests and consolidate its relationship with developing countries and gain support [80]. It has then clung to its developing country identity when challenging the existing global governance model (even though China is known for being characterized by multiple identities contradicting each other).[2] This reflects a challenge to existing norms made by weaker actors in the international community.

Below I explain how this article applies that framework and develops the hypotheses. Historically, the CCP regime has faced insecurity due to inter-party division, socioeconomic inequality, corruption, people's distrust, and China's history of bullying by foreign powers. This motivated China to long consider survival its primary aim, prioritizing the preservation of non-interference, domestic stability, political system, and one-party leadership [9, 63]. However, cyberspace worsens survival concerns as illustrated. Meanwhile, as discussed, China holds a state-centric view of the international order and believes state authority can never be challenged, therefore downplaying other actors. To successfully guarantee state control of cyberspace, it advocates a sovereigntist approach to the cyberspace realm [90].

Nonetheless, the Western multi-stakeholder model promotes the free flow of information and recognizes the importance of non-state stakeholders, which clashes with China's governance vision [109]. In China's eyes, the West's promotion of a

[2] Given China's emphasis on its developing country identity, this article does not delve into the nuances of China's multiple identities when exploring its governance approach.

free Internet was a subjugation attempt which disturbs China's state authority and interests. Under the logic of norm subsidiarity, instead of importing and accepting Western liberal norms, China hopes to revise the Western-led cyber governance model. Accordingly, the development of cyber sovereignty is an extension of its sovereigntist view of international order and the digital sphere, while its discussions on cyber governance should stress promoting national security and state control. This leads to a hypothesis testing whether China is a norm follower or a reviser, thus assessing whether China's cyber vision is liberal:

H1 Due to its state-centric approach to sovereignty, China has also applied a state-centric official discourse on global cyber governance.

China's eagerness to alter the global cyber governance model is reinforced by its inferior past. Although arguably, China is now a great power even stronger than many European states, it remained a developing country when cyber governance was established. Therefore, the current model fails to fully reflect China's interests, breeding resentment against Western domination in cyber governance. This motivates China to demand allowing developing countries' participation and criticize developed countries' dominance through promoting cyber sovereignty. This leads to a hypothesis testing whether China's new cyber norms are characterized by the desire to revise Western dominance and whether this drives China to challenge current norms:

H2 Due to its residual identity as a developing country and non-Western power, China stresses developing countries' participation in cyber governance.

Despite the resentment toward the current multistakeholder model, China lacks the capability to revise it since it has emerged as a longstanding norm. Meanwhile, AI development deepened China's concern about sovereignty and national security erosion. While China fears being excluded from AI governance like what it faced in cyber governance, the West has not created a governance model for AI [28, 59]. This provides opportunities for China to exploit to reshape governance norms, thereby reinforcing state authority and justifying its control of cyberspace. By extending and promoting its cyber norms to the AI realm, China can counteract the West's advocate of online openness and liberal values, while advocating equal rights of participation between developed and developing countries in governing AI. This leads to a hypothesis testing what characterizes China's AI governance norms and drives their evolution:

H3 China is extrapolating its sovereigntist view of cyber governance to the AI governance realm.

Meanwhile, there remains a possibility that China's official discourse on cyber and AI governance does not divert from the Western view. This brings an alternative hypothesis, which I also draw from norm literature about socialization. Socialization

is the process of inducing actors into endorsing a given society's norms, rules, and expected behaviour [18, 46]. Emerging powers, including China, often integrate with existing norms to seek acceptance and avoid confrontation, especially when they may not have the capability to revise the longstanding norms [79]. As a weaker actor excluded from the norm-making process of cyber governance, China is pressured to endorse the long-standing Western norms. Although a governance norm is not yet established for the AI realm, China is obliged to follow Western liberal norms to avoid suspicion. This leads to an alternative hypothesis suggesting China is a norm taker instead:

H4 Due to socialization effects, China's official discourse reflects the Western model of liberal cyber and AI governance.

Methodology

To test the hypotheses, I apply topic modelling to study texts discussing cyber sovereignty and AI governance. Topic modelling is an unsupervised machine learning method for automated content analysis. It considers a document formed by groups of topics, and a topic formed by groups of words/phrases. By scanning through documents to analyse how different groups of words or phrases co-occur, topic models unfold the emergence and evolution of themes across a large number of documents automatically, while not requiring any coding sheets [7]. This way, topic modelling provides preliminary insights into the broad patterns of the collection of texts. This tool can be especially helpful in the case of analyzing a collection of hundreds or thousands of (long) government texts since humans have limited processing power for performing manual analysis to identify the key patterns.

Topic model's extractions of themes from discussions about cyber and AI governance allow us to infer what is valued and actively promoted by China effectively. We can then identify whether China's official narratives are filled with resentful claims related to sovereignty or its subsidiary status, or whether its narratives actually support current practices. By examining the similarities and differences in the broad patterns of discussions about cyber and AI governance, we can further test whether China is extrapolating its view on cyber governance to the realm of AI governance.

However, topic modelling is not a panacea for addressing text analysis problems. As I will demonstrate below in more detail, this study acknowledges the past topic model applications' limitations in navigating noises in the text corpus, irrelevant topics, and arbitrary labelling of topics. I will put forward a framework that incorporates additional fine-grained analyses and contextual examination of documents to ensure the validity of the results.

Model Choice

This article employs the Correlated Topic Model (CTM) instead of the most common topic model Latent Dirichlet Allocation (LDA). Unlike LDA, CTM allows topics to be correlated and has proved to provide a closer approximation to the true document structure, thus generating more coherent topics [11]. This will especially benefit our study as topics like security, sovereignty, and data can be correlated.

Data collection

Existing literature discussing cyber sovereignty often relies on the Chinese National Knowledge Infrastructure to collect official/semi-official/expert texts [6, 65, 109]. However, since March 2023, access to it for universities and research institutions outside of China has been terminated. Therefore, I scrapped government websites instead to collect data using the *RVest* [102] and *Selenium* packages (Selenium, n.d.) on R and Python respectively.

I constructed the keywords based on those used by existing literature researching the topic and different translations/expressions of the same term (e.g. digital/cyber/Internet sovereignty) [44, 56, 65, 109]. Table 1 summarizes such keywords.

I collected the texts from numerous relevant government websites covering up to 21/11/2023. While government speeches, documents and press releases reflect official discourse, their discussion on cyber sovereignty could be vague [98]. Given the Chinese regime's authoritarian nature, state-affiliated media could represent views largely if not completely resembling the government's stance. To enrich the analysis, I collect state-affiliated media texts shared by Chinese government websites, which reflect state endorsement of their opinions.

Moreover, I take US discussions as baseline data to validate whether Chinese discussions are particularly sovereigntist. The US considers cyberspace domains

Table 1 Keywords used in searches

Category	Sub-category	English keywords	Chinese keywords
Cyber	Cyber sovereignty	Cyber sovereignty	赛博主权
		Network sovereignty	网路主权
		Internet sovereignty	网络主权
		Information sovereignty	信息主权
		Digital sovereignty	
	Cyber governance	Cyber governance	网络治理
		Internet governance	
		Information governance	
AI	/	AI governance	人工智能治理
		Artificial intelligence governance	人工智慧治理

Table 2 Sources used by this article

Category	China	US
State government	State Council State Council Information Office	White House
Legislature	National People's Congress	Congress[$]
Diplomacy	Ministry of Foreign Affairs	Department of State
Defence	Ministry of Defence	Department of Defense
Cyber/AI-related departments	Ministry of Industry and Information Technology[*] Cyberspace Administration of China[*]	Bureau of Cyberspace and Digital Policy[^] Office of Science and Technology Policy[&]
Examples of official/state-affiliated media (Collected from government websites)	Xinhua People.com.cn People's Daily China Daily Chinese Communist Party News Dazhong Daily	N/A

[*]English website not available

[^]Under the Department of State

[&]Under White House

[$]Only committee reports, committee publications, and legislations/bills that have become law are collected. Meeting notes, drafts and communications are ignored.

Texts by some other media like PLA Daily and provincial media like Nanfang Daily werealso collected, but after the screening process, they were found to be irrelevant.

Table 3 Number of texts covered by the subset

	China (Chinese)	China (English)	US
Cyber governance and cyber sovereignty	284	91	153
Cyber sovereignty	72	28	54

'global commons', which no single state controls and sovereignty should not apply [21]. Its AI approach is regarded as liberal or even laissez-faire [64]. Considering this stark contrast, China's textual discussions on global cyber and AI governance should be less liberal compared to its US counterparts. Therefore, I search through the websites of US government agencies using the same set of keywords. To ensure comparability, I examine sources with the same function as

their Chinese counterparts (e.g. Ministry of Foreign Affairs vs US Department of State). Table 2 summarizes the sources used.

While Voice of America is a state-owned news network, it receives less interference from the state government compared to its Chinese counterparts like Xinhua, so its reporting is inherently less consistent with the government's stance [30]. Thus, texts by Voice of America were not collected Table 3.

Since the US adopts a laissez-faire approach to AI governance [64], I expect fewer official texts collected from the US side.

Data screening

Government websites often utilize fuzzy searches, so irrelevant texts may be returned. Therefore, I run another round of data screening by checking whether the collected text actually contains the keyword.

Moreover, duplicated materials will likely be downloaded as several keywords can be all mentioned in a single text. I remove duplicates to avoid overstating the frequency of topic occurrence.

All the processes (summarized in Fig. 1) resulted in a total of 689 articles included.

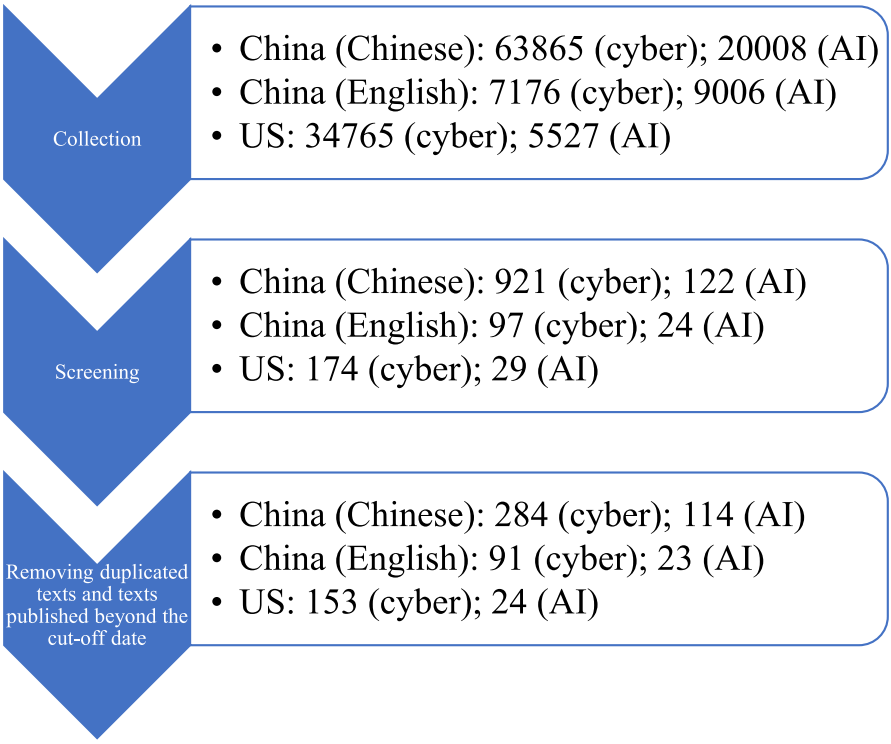

Fig. 1 Identification of items and screening process

*Excluding broken links, non-text files, or absent texts.

Pre-processing

When applying automated text analysis, pre-processing is needed to ensure the text is machine-readable. Although statistical methods for text analysis tend to be language agnostic, pre-processing tools are not [60]. Different packages are needed to pre-process Chinese and English texts to maximize accuracy.

First, unlike English words which are separated by spacing, Chinese characters have no obvious delimiters. I use the *JiebaR* package to segment the Chinese-language texts, i.e. dividing them into individual words [81]. Second, I convert all words to lowercase and remove all punctuation, whitespaces, email addresses, and URLs. Third, I use the *tmcn* [53] and *tm* [33] packages to remove common stop words which are usually non-informative [7]. Fourth, since tense and number are usually not indicative of the text topics, I perform lemmatization in English texts using the *textstem* package to reduce the input dimension [83]. Chinese words do not require lemmatization since they are not conjugated or pluralized by adding an ending. Fifth, I drop words appearing in less than 5% of the documents, thereby preventing interpretation from becoming skewed by loosely connected words [101]. Figure 2 summarizes the pre-processing steps.

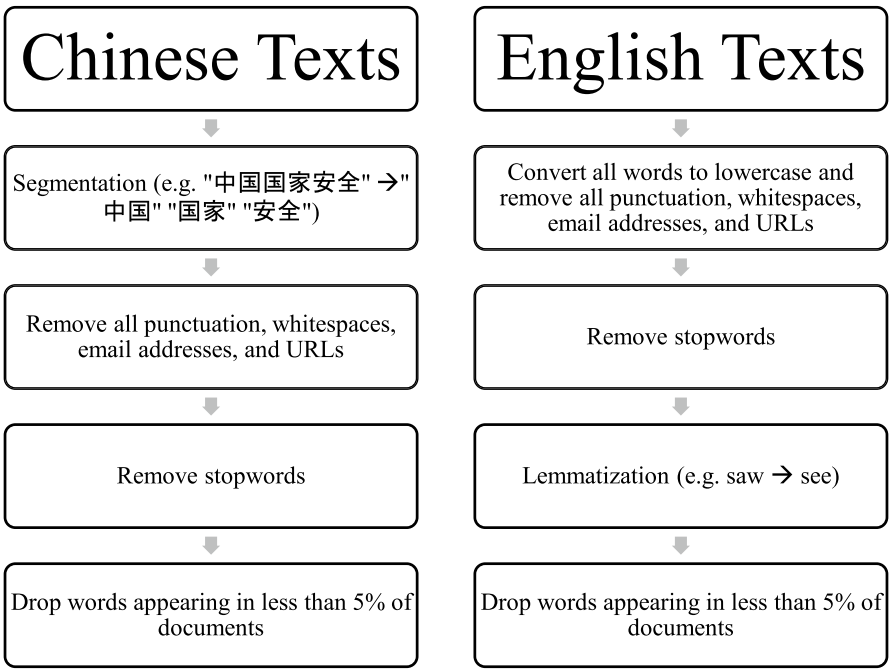

Fig. 2 Pre-processing steps

Model optimization

When conducting topic modelling, one should not blindly pursue the maximum number of topics (k). Having too many or too few topics can cause difficulties in interpreting their meaning and distinguishing different topics [41, 57]. Meanwhile, the k value used by existing literature can span from 8 [29] to 100 [8].

I use the *searchK* function under the *stm* package to test the relative goodness of fit for each k. I pick the k giving a relatively high held-out likelihood, a lower bound of the marginal log-likelihood, and topic coherence, and also relatively low residuals [66, 86, 88]. This helps achieve internal consistency and topic quality [87]. See the online Appendix for model fit comparisons.

It is expected that the number and the category of topics generated by models analysing Chinese and English texts respectively are vastly different. This can be because a particular text may not appear in another language. Accordingly, the number of documents, the types of themes in the corpus and their statistical associations will also vary, and so will the optimal k and the actual topic categories interpreted.

Additional sub-set analysis and validation

Textual datasets inevitably contain certain degrees of noise, so irrelevant topics can be generated [45]. This can be problematic because most data I examine are long texts and the subject matters tend to be less internally homogeneous, i.e. the topic inter-relationships are less readily interpretable [40].

Therefore, I apply Altaweel et al.'s [5] approach to ensure result validity. I keep sentences containing the keywords, and also the sentences before and after for analysis. This creates a 'short corpus'. I then repeat the previous steps of k optimization to create a different set of topic model outputs, thereby determining whether a more focused search will yield more relevant topics.

Moreover, I will perform additional analysis on a subset of documents by removing texts discussing cyber governance only but not cyber sovereignty. Such texts can give irrelevant results such as pornography and e-scams, which are not relevant to sovereignty and this article. Note that the US does not have the concept of 'cyber sovereignty' [52], so the discussion and the number of relevant topics are expected to be limited.

Eventually, a total of 18 models will be created.

Topic interpretation

Although topic models generate sets of statistically associated topics and words, only human analysts can examine their conceptual meanings, while the topic number given by the *stm* package gives no additional contextual information. Nonetheless, there is no established, systematic procedure for mapping labels to each topic generated [40].

Mainstream approaches of simply examining the commonalities of words listed by each topic could overlook the context of the texts, thus giving biased results. Moreover, topic modelling is ultimately an automated method for identifying the statistical correlation between words, so not all topics are interpretable or useful for answering a particular research question [45, 101], especially when government texts are long and cover many matters.

Therefore, besides applying contextual acknowledge to interpret the topics, I also take Gillings and Hardie's [40] validation approach: close reading of the top 10 documents which the model reports as having the highest proportion of that topic. This approach encourages an additional human examination for identifying how the listed words are expressed across texts *in context*, thus avoiding arbitrary and ad-hoc labelling.

Results

The results below are generated using a separate model with an individual value of k given by the procedures above (See Table 4). For each model, I provide a table showing the names of all topics. See the online Appendix for the tables showing the top 10 common words within each topic and the word clouds.

Expectedly, all 18 models produced some irrelevant topics, as is common in such exercises as discussed. Topics are discarded if the topics and associated documents (1) are clearly irrelevant and overly broad (e.g. bilateral cooperation, anti-terrorism, national defense, community welfare disputes); (2) describe a specific event/meeting/committee/law/publication about cyber/AI governance, but the 10 most common words contain no substance (e.g. World Internet Conference); (3) are meaningless (e.g. Stopwords); (4) are related to cyberspace/AI, but are not directly related to the political/international governance aspect (e.g. E-commerce development, anti-pornography). For example, the topic 'e-commerce development' will be removed if the associated documents only discuss how to stimulate the domestic economy by promoting e-commerce or China's achievement in e-commerce development, but it will be retained if they discuss how the international community or the national

Table 4 Optimal k values

			China (Chinese)	China (English)	US
Cyber	Cyber governance and cyber sovereignty	All	25	8	29
		Short	13	13	14
	Cyber sovereignty only	All	18	13	16
		Short	9	8	20
AI	All	All	20	9	9
		Short	29	8	8

Table 5 Illustrations of topic removal criteria

Reasons	Example of topics	Example of words
Irrelevant and overly broad	Model of China (Chinese) (All documents) (Cyber): Topic 4 (bilateral cooperation)	成员国, 重申, 联合国, 恐怖主义, 呼吁, 认为, 强调, 组织, 国际法, 印度 (member states, reaffirm, United Nations, terrorism, appeal, view, emphasize, organization, international law, India)
Describe a specific event/meeting/committee/law/publication about cyber/AI governance, but contain no meaning	Model of China (English) (All documents) (Cyber): topic 4 (World Internet Conference)	wuzhen, zhejiang, cpc, committee, conference, provincial, achievement, mr, speech, law-based *(For context, the World Internet Conference is held in Wuzhen, Zhejiang.)*
Meaningless	Model of US (All documents) (Cyber): Topic 23 (Stopwords)	's, 've, go, know, 'll, say, something, think, sure, want
Related to cyberspace/AI, but are not directly related to the political/international governance aspect and/or not associated with paragraphs/documents related to these aspects	Model of China (Chinese) (All documents) (Cyber): topic 2 (E-commerce development)	知识产权, 电子商务, 简要, 一带, 一路, 互联互通, 侵权, 东盟, 提到, 表示 (intellectual property, e-commerce, brief, one belt, one road, interconnection, infringement, ASEAN, mention, representation)

governments should regulate e-commerce and business data, i.e. related to politics/governance. See Table 5 for illustrations.

In contrast, meaningful topics directly related to cyber/AI governance will be included. Examples include 'Multilateralism' (the type of governance framework), 'common destiny' (the rationale behind international cooperation), and 'mutual respect of sovereignty' (characteristics of the governance model).

Given the large total number of models and topics, I will directly discuss the relevant topics. The tables indicating the list of topics can be found in the online Appendix.

Cyber

All documents

For China (Chinese) documents, they reflect China's cyberspace vision of how countries' interests are associated and that national sovereignty should be mutually respected (Topic 15). They also discuss the need to regulate cyberspace using legal means (Topic 1).

For China (English) documents, the only topics related to cyberspace are Topics 1 and 6. Topic 1 reflects the digital evolvement of the global economy, but it discusses nothing about the political/governance side. Words associated with topic 6 (e.g. cyberspace, cyber, ict, white, rule, governance) contain no substance about the white paper's content. Thus, I consider all topics irrelevant.

For US texts, Topic 22 reflects the US rejection of China's human rights suppression, surveillance, and other digital authoritarian acts. The associated documents describe China's development of new governance models as 'digital authoritarianism' and 'deeply troubling'.

Short corpus

For China (Chinese) texts, the relevant topics focus on four main themes: First, security and sovereignty are interlinked and should be ensured (Topics 3, 6). The associated documents involve quotes specifically linking security and sovereignty together: 'Cyber sovereignty is the expansion of national sovereignty in cyberspace', 'the primary purpose of maintaining cyber sovereignty is to ensure national security'; second, China hopes to cooperate with other countries in building a multilateral model (Topic 13). Specifically, document 7 states that 'International cyber governance should adhere to multilateral participation and multi-party participation, and give full play to the role of various entities like governments, international organizations, Internet companies, technical communities, non-governmental organizations, and individual citizens'; Third, regarding the governance participation, every country should have equal sovereign rights to protect its information security (Topic 10); Fourth, specifically, state/party leadership should be the foundation for the development of enterprises. For example, pairing and jointly establishing party branches will 'make the party's grassroots organizations a red engine for the healthy development of Internet companies' (Topic 2).

For China (English) texts, the texts share a main theme of indicating China's firm defense of its own cyber sovereignty (Topic 1). They also discuss that all countries share common interests in cyberspace (Topics 5, 9) and that countries should collaborate to promote responsible state behaviour in cyberspace (Topics 6, 11). Particularly, China values openness in cyber governance and cooperation (Topic 7). Topic 13 points to the specific desire to reform the current cyber governance framework to promote equal participation of all countries in internet development.

For US texts, the relevant topics mainly criticize China's proposal to establish an alternative cyber governance model characterized by government control (Topic 2) and defend the current multistakeholder cyber governance framework (Topics 4, 9, 14). Topic 8 further elaborates on the current multi-stakeholder model's nature: encouraging the free flow of data.

Cyber sovereignty

All texts

For China (Chinese) texts, topic 1 is the only relevant topic. It discusses the idea that all humans have the same shared destiny in cyberspace and that countries should collaborate to govern it.

For China (English) texts, Topic 4 discusses China's worldview that all countries share common interests in cyberspace and should promote openness in cyber governance. Topic 8 precisely illustrates China's support for openness by criticizing the unbalanced digital development and calling for equal participation involving developing countries in its cooperation.

For US texts, as expected, topics are either irrelevant or criticizing China's approach. The only relevant topic (Topic 4) criticizes China's new cyber governance model, which it describes as being 'worrying'.

Short corpus

China (Chinese) texts have a prevailing theme of reflecting China's view that countries' destiny in cyberspace is shared (Topic 7). The texts also stress the need to protect sovereignty in cyberspace and ensure every state has equal rights in protecting its national interests (Topics 1, 6). Topic 2 extends the discussion of equality to call for guaranteeing equal participation in cyber governance and regulating information technology. Topic 9 further reflects China's proactiveness in participating in rule-setting and infrastructure-building to foster cyber governance. Meanwhile, Topic 5 criticizes US hegemony in cyberspace and suppression of other countries' cyber sovereignty.

For China (English) texts, they call for recognising national sovereignty in cyberspace issues (Topics 1, 2) and countries' autonomy in considering their domestic circumstance in establishing cyber governance and improving access to digital resources (Topic 8). Common interests in cyberspace is another important

topic in these texts (Topics 3, 7). Meanwhile, relevant texts also criticize the US for expanding offensive capabilities and stressing the need to build a peaceful cyberspace (Topic 6).

For US texts, all the relevant topics are either criticizing China's proposal of a new cyber governance framework or defending the current multi-stakeholder model. Some target Russia's international sovereignty law, which is outside our study's scope.

AI

All documents

For China (Chinese) texts, the relevant topics cover two main themes: China's eagerness to research AI ethics and establish effective ethical governance mechanisms (Topics 2, 14) and China's view that developing generative AI is equally important as regulating it (Topic 11).

For China (English) texts, they stress the need to ensure the security and trustworthiness of AI content and data (Topic 2). Specifically, China is concerned about the ethical dimension of AI risks. It requests improving ethical norms and regulations of AI to allow all countries to share benefits from its development (Topic 7). While calling for more regulations, China stresses that all countries should have equal representation and participation in AI governance and accessing resources (Topic 8).

For US texts, the only relevant topic is about calling for addressing algorithmic bias and discrimination caused by the use of automated systems (Topic 2).

Short corpus

For China (Chinese) documents, they cover five main themes: First, China encourages AI development, while stressing the need to ensure safety to maximize AI benefits (Topics 26, 29); Second, all human has a shared destiny and China has a responsibility to help mankind grasp the opportunity provided by AI (Topic 21); Third, China encourages cooperation in building AI governance and addressing AI risks (Topic 10); Fourth, regarding the risks, the documents have a specific emphasis on ethics (Topics 6, 16), the black-box nature of generative AI regulations (Topics 7, 19), and data security issues (Topic 15); Fifth, regarding participation in risk management, the relevant texts request equal and fairer participation in AI governance (Topics 2, 12, 23).

For China (English) texts, the relevant topics express concerns about AI risks (Topic 8) and suggest using clear rules and laws to govern AI development (Topic 1). However, Topic 4 suggests that cooperation among national governments is necessary for managing AI risks, while Topic 5 stresses that participation in AI governance and rule-making should be broad and involve developing countries.

For US texts, Topic 1 calls for mitigating AI risks and recommends reducing barriers to the responsible use of AI by reducing barriers like cybersecurity processes. The associated texts also give examples like 'information technology infrastructure'

and 'data, workforce, budgetary restrictions' as barriers. Topic 3 further discusses promoting international cooperation and multistakeholder engagement to improve the technical standard and trustworthiness of AI, thereby mitigating the corresponding risks.

Discussion

The findings broadly support H1 (Due to its state-centric approach to sovereignty, China has also applied a state-centric official discourse on global cyber governance). Both the US and China have expressed their eagerness to participate in global cyber and AI governance. This is expected because the search keywords used for data collection surround the word 'governance' and major powers are usually interested in leading discussions on an important global issue. Specifically, China has consistently described the international community as a 'community of common destiny', which is a catchphrase commonly appearing in China's strategic narratives. This seems to imply that China hopes to promote international efforts in addressing cyber and AI development which are issues of all countries' common interests to promote common prosperity. However, scholars have noted that this concept's meaning is unclear yet politicized [82, 110]. China could be using the catchphrase to request other countries to adapt their approaches to China's national interests because they are living in a common community and China's interests should be considered [25]. Thus, interpreting China's frequent mention of 'community' requires special caution.

The results show that sovereignty and security prevail in China's discussion of cyber governance in both languages, which resonates with past studies that it is a cornerstone in China's cyber vision [13, 17]. Specifically, Chinese texts have discussed party control of enterprises as the driver of their healthy development. On the contrary, US texts have not linked sovereignty to cyber governance. Instead, it prioritizes discussions on democratic values, such as rejecting censorship and promoting the free flow of data. This reflects China's more sovereigntist attitude in its cyber approach. It has adopted a Westphalian narrative of non-interference and political independence to protect its authority and regime security, while exerting tight control over domestic entities to ensure stability.

(Admittedly, China has also defended liberal values like democracy, transparency, and openness. However, the topics related to the values are associated with texts discussing shared interests and developing countries' fair participation in governance frameworks, rather than promoting civil liberty and rejecting authoritarianism. The notion of democracy is thus used to confront Western hegemony instead as China's common practice [79].

Although sovereignty does not form a topic in China's discussions of AI governance, China has expressed a need for national security and state control in both discussions. Its specific emphasis on generative AI echoes Sheehan [93] that Generative AI's impact on the creation and dissemination of online content is arousing China's concerns. Moreover, China expresses a strong interest in ethical norm regulations. This agrees with the former literature review that China is

pursuing information control and ethical norm standard-setting in AI governance. While the US texts have also discussed AI risk mitigation, the topics have a greater emphasis on civil aspects like algorithmic discrimination and bias. The topic about cybersecurity is about reducing barriers to the use of AI, rather than safeguarding national security. In this sense, China's discussions are more security-oriented.

Moreover, both powers have been actively encouraging international cooperation in cyber and AI governance to address the ethical and security challenges. This may seem to suggest that China's key objective is to promote shared interests in cyberspace and address all countries' functional need for governance frameworks through coordination. However, their approaches have been different, which ultimately reflect China's sovereigntist attitude towards cyberspace. For China, most topics and associated texts point to cooperation among *national governments*, which confirms that China considers the state holding supreme authority in cyber and AI issues. In contrast, US texts have been promoting the multistakeholder approach and collaboration with stakeholders other than national governments.

Unexpectedly, the results found that in *one* of the top associated texts with the topic multilateralism, China advocates a multi-party (e.g. international organization, internet enterprises, individual citizens) approach. This seems to support Cheng [19] that China upholds the principle of harmony and cooperation, thus acknowledging multistakeholderism's merits. Nonetheless, the US texts criticize China for revising the current multistakeholder model and promoting a state-centric multilateral model. Such a contrasting narrative makes it unclear whether China really sincerely embraces multistakeholderism or whether the US is defaming China. The topics and associated texts have been more consistent in demonstrating support for multilateral cooperation with national governments instead, so the surprising result is probably an outlier.

A possible reason for such acknowledgement is that China ultimately cannot avoid collaborating with other stakeholders in addressing some technical issues, so it will accept their participation yet continue to advocate giving states a more important position [13, 14, 21, 99]. However, there lies a possibility that China will reject such participation if possible and only accept it when it is inevitable. This will lead to the conclusion that China rejects multistakeholderism instead [24, 65]. Regardless, if China genuinely hopes to facilitate coordination to address common cyber and AI problems more effectively, it should provide more room for non-state entities which are important stakeholders in these issues to participate in the process, and thus, advocate a multiparty approach more consistently. Future research can further explore to what extent China rejects the participation of non-state stakeholders and how China presents its stance differently on different occasions.

The findings support H2 (Due to its residual identity as a developing country and non-Western power, China stresses developing countries' participation in cyber governance). China has indicated its firm support for promoting fair participation in both cyber and AI governance. Specifically, it demands governance frameworks to consider developing countries' needs. It has consistently rejected unequal treatment of countries' national interests and security needs. This agrees with Cai [14] that the unequal participation between developed countries and developing countries in cyber governance drives China's opposition to the current framework. Moreover,

China demands state independence in promulgating regulations according to their development and security requirements. This reinforces Coleman and Maogoto's argument (2013) that China rejects the coercive Western implementation of liberal values in international frameworks. It also adds to former qualitative literature that China hopes to make use of cyber sovereignty to legitimize its tight control over cyberspace and encourage other developing countries to adopt similar measures, who follow a different development path and disagree with Western democratic values [17, 109]. The promotion of mutual respect for the right to independently choose their approach to governance exhibits a promotion of sovereign equality across developed and developing countries, which ensures all countries can focus on their individual security needs [6]. The findings thus reiterate the need to consider China's subsidiary status as a developing country in understanding its cyber and AI governance approaches.

The findings' support for H2 implies that scholars should not simply interpret the promotion of alternative governance models as a pursuit of power. While this does provide analytical relevance at a time of great power competition, such claims cannot fully explain why China picked this particular normative framework of stressing developing countries' participation, instead of using its economic power and rapid development to justify more representation in the governance frameworks. Although this normative framework allows China to show solidarity and also gain a greater influence, China has to share its decision-making power with other weaker actors if it succeeds in promoting this norm. In contrast, if China justifies more representation with its material power instead, it can gain exclusively and thus maximize its power without dilution. Thus, future research should not ignore China's developing country status as a factor when examining China's motivation to establish an alternative model.

Overall, the results support H3 (China is extrapolating its sovereigntist view of cyber governance to the AI governance realm). The findings show that China's discussions about AI governance resemble similar patterns to discussions about cyber governance. While both countries share concerns about the development of cyberspace and AI, China has been more active in stressing state authority and sovereignty in its discussions compared to the US. Although sovereignty is not explicitly listed as a theme in discussions of AI governance, China has been continually stressing the need to protect national security, promote sovereign equality, and ensure non-interference. This shapes security-oriented discussions for both cyber and AI governance, thus reflecting conceptual elements of cyber sovereignty.

Meanwhile, while both countries have encouraged international cooperation to address the challenges, China has been vocal in requesting fair participation and equal consideration of interests in international governance frameworks. China's desire for shaping an alternative norm where developing countries have more say in the frameworks has thus been manifested in the AI realm as well. This reflects China's active efforts to avoid the marginalization of developing countries in the global norm-making process of both cyber and AI fields.

Ultimately, the three primary hypotheses stand, implying H4's rejection (Due to socialization effects, China's official discourse reflects the Western model of liberal

cyber and AI governance). The official discourses of the US and China do share some similarities, such as supporting international cooperation. Nonetheless, as summarized, China's approach is more security-oriented and state-centric, while its discourse is less concerned about democratic values. Thus, China is not bound by socialization to promote liberal values.

Meanwhile, although this article does not examine China's actual efforts in promoting its cyber and AI governance visions, its findings suggest that we should not dismiss China's norm revision intention. The above discussions have shown that China has been promoting a sovereigntist narrative, as well as stressing fair participation and state authority. Its narrative is similar to what developing countries like Brazil and South Africa have been using [24, 39, 52], so it could help China gain appeal from them. As China self-positions itself as a natural leader of developing countries, it will face a great reputation cost if it has been so vocal in promoting alternative norms but strategically avoiding any actual implementation effort. This will hinder its agenda of strengthening its connections with non-Western countries [79]. Additionally, if China prioritizes the maintenance of a harmonious relationship with the West over its national interests, it should not even promote the alternative concept which can arouse suspicion about its ambition. Therefore, we should not assume that China has no intention to revise cyber or AI governance norms.

Conclusion

This article seeks to understand China's cyber and AI governance approaches by performing a topic model analysis and comparing relevant Chinese discussions with their US counterparts. Building on existing literature about norm subsidiarity and the enquiry topic, it addresses the literature gap about the relationship between cyber sovereignty and AI governance. By applying a quantitative method and examining a larger sampling frame, this article provides additional depth to the current literature which has been dominated by qualitative analysis and often confined to a limited source of textual data. This way, this article helps adjudicate a contested debate in the political science discipline about how state-centric China's model is, where the contestation could be partly attributed to the limited data past studies examine.

This article confirms that sovereignty protection and state control characterize China's approach to governing cyberspace and AI development, which reflects an extrapolation of Chinese cyber norms to an emerging field. China's subsidiary position in cyberspace development and its value clashes with the West have ignited its desire to introduce alternative norms to cyber governance and also the AI sphere, under which developing countries' development and security needs should be catered. This rejects the '(relatively) liberal strand' of the past literature's argument that China is more than happy to forgo parts of its sovereign control over cyberspace and lend it to non-state stakeholders. Additionally, this article further highlights that China is not a passive norm recipient, despite its necessity to integrate into the international society to seek acceptance. It is instead active in defending its national interests and seeking compensation for its historical inferiority.

This article's findings have a wider implication that historical context and the corresponding power asymmetries matter in norm revisions. Future research on China's alternative cyber and AI norm revision, or the broader norm revision issues, should systematically consider the importance of a country's past position on the international stage. As this article identifies the Chinese government's emphasis on its inferior status in its textual discussion of cyber sovereignty and AI governance, it reflects the norm subsidiarity theory's applicability to explaining China's position in emerging technology governance and its promotion of alternative norms. To further test the theory's plausibility and the feasibility of China realistically realizing its visions, future research can examine how norms are diffused, accepted, criticized, challenged, and implemented. Scholars may analyse China's diplomatic discourse and interactions in international organizations or negotiations, developing countries' perception of China's alternative cyber and AI governance model, or the US reaction to China's vision. Another area of interest could be how the general features of China's cyber and AI governance approach identified by this article change over time. As cyber threats and AI technology are constantly evolving, future research can compare similarities and differences in the discussions to understand how China's approach and diplomatic discourse have evolved over time.

Moreover, this article explores how China communicates its cyber and AI governance vision in its official texts broadly, thus examining their conceptual meanings. Future research can analyze more precisely how the topics will change if the texts are from different sources and serve different audiences (e.g. Chinese-language and English-language texts, or texts serving domestic and international audiences) as China may communicate strategically to different audiences in different languages. This will allow scholars to understand whether China is strategically presenting a subsidiary narrative to legitimize its pursuit of power in the cyber and AI realms.

This article also makes a methodological contribution by showing how topic modelling can be helpful for examining government opinions and international affairs. Although researchers still bear the burden of result interpretation, topic model allows the extraction of the overview of a large text collection and the identification of broad patterns of themes [45]. Specifically, in the context of cyber and AI governance norm revision, the large amount of diplomatic discourse and texts (in different languages) implies that automated text analysis can facilitate norm examination. It could complement qualitative study which captures contextual nuances more effectively yet inevitably covering a smaller sampling frame, which limits such studies' comprehensiveness.

Furthermore, this article develops a methodological framework that can effectively analyse long government texts, which political scientists often rely on for data sources. As the findings demonstrate, some irrelevant topics like veteran affairs and investor relations are clearly out of scope and can be quickly discarded, while some like network provider responsibility require closer examination. Such limitations reflect the need for close reading and subsetting texts when applying topic modelling to government texts. The former allows researchers to identify associated texts and validate whether the topic words are actually relevant, while the latter allows a more refined result. This article, therefore, lays a groundwork for the wider

discipline to apply computational methods to address complex textual data to study norms. Advancing research on such methods will allow future political scientists and also researchers of other fields to navigate complicated research questions and the vast volume of useful yet unstructured information more effectively.

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1007/s42001-024-00346-8.

Acknowledgements I am grateful for Dr Rohan Muherjee's guidance and encouragement for this study.

Funding No funding is received for this study.

Data availability The primary code files and markdown files of the topic model that analyses the data can be found in the supplementary materials submitted to the journal. The data that support the findings of this study is collected from publicly available sources, but the scrapping code and textual data used cannot be directly provided here due to copyright restrictions.

Declarations

Conflict of interest The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Ethical approval and informed consent statements No ethical approval is needed for this study.

References

1. Acharya, A. (2011). Norm subsidiarity and regional orders: sovereignty, regionalism, and rule-making in the third world. *International Studies Quarterly, 55*(1), 95–123.
2. Acharya, A. (2013). The R2P and norm diffusion: towards a framework of norm circulation. *Global Responsibility to Protect, 5*(4), 466–479. https://doi.org/10.1163/1875984X-00504006
3. Alderson, K. (2001). Making sense of state socialization. *Review of International Studies, 27*(3), 415–433.
4. Allen, G. C. (2019). *Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security*. Center for a New American Security.
5. Altaweel, M., Bone, C., & Abrams, J. (2019). Documents as data: a content analysis and topic modeling approach for analyzing responses to ecological disturbances. *Ecological Informatics, 51*, 82–95. https://doi.org/10.1016/j.ecoinf.2019.02.014
6. Arsène, S. (2016). Global internet governance in Chinese academic literature. *China Perspectives, 2016*(2), 25–35. https://doi.org/10.4000/chinaperspectives.6973
7. Asmussen, C. B., & Møller, C. (2019). Smart literature review: a practical topic modelling approach to exploratory literature review. *Journal of Big Data*. https://doi.org/10.1186/s40537-019-0255-7
8. Barberá, P., Casas, A., Nagler, J., Egan, P. J., Bonneau, R., Jost, J. T., & Tucker, J. A. (2019). Who leads? Who follows? Measuring issue attention and agenda setting by legislators and the mass

public using social media data. *The American political science review, 113*(4), 883–901. https://doi.org/10.1017/S0003055419000352
9. Bell, D. A., & Wang, P. (2021). It's Just Hierarchy Between States—On the Need for Reciprocity. In H. Wang, & A. Michie (Eds.), *Consensus or Conflict?. China and Globalization* (pp. 9–30). Springer.
10. Bisson, C., Giron, A., & Verin, G. (2023). A comparative analysis with machine learning of public data governance and AI policies in the European Union, United States, and China. *Journal of Intelligence Studies in Business, 13*(2), 61–74. https://doi.org/10.37380/jisib.v13i2.1084
11. Blei, D. M., & Lafferty, J. D. (2007). A correlated topic model of Science. *Annals of Applied Statistics, 1*(1), 17–35. https://doi.org/10.48550/arXiv.0708.3601
12. Brehm, S. (2021). Whose vision is it anyway? The "free internet" in Chinese state media. *Journal of Current Chinese Affairs, 50*(1), 12–38. https://doi.org/10.1177/1868102621998084
13. Cai, C. (2018). China and global cyber governance: main principles and debates. *Asian Perspective, 42*(4), 647–662. https://doi.org/10.1353/apr.2018.0029
14. Cai, C. (2018). Global cyber governance: china's contribution and approach. *China Quarterly of International Strategic Studies, 4*(1), 55–76. https://doi.org/10.1142/S2377740018500069
15. Callahan, W. A. (2008). Chinese visions of world order: post-hegemonic or a new hegemony? *International Studies Review, 10*(4), 749–761.
16. Carrai, M. (2019). *Sovereignty in China: A Genealogy of a Concept since 1840*. Cambridge University Press.
17. Cary, D. (2023). *Community watch: China's vision for the future of the internet* Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/community-watch-chinas-vision-for-the-future-of-the-internet/
18. Checkel, J. T. (2005). International institutions and socialization in europe: introduction and framework. *International Organization, 59*(4), 801–826.
19. Cheng, J. (2023). Contextualizing China's AI Governance. *Global Policy*. 2023. https://www.globalpolicyjournal.com/blog/01/06/2023/contextualizing-chinas-ai-governance.
20. Cheng, J., & Zeng, J. (2023). Shaping AI's future? China in global AI governance. *Journal of Contemporary China, 32*(143), 794–810. https://doi.org/10.1080/10670564.2022.2107391
21. Chin, Y. C., & Li, K. (2021). A Comparative analysis of Cyber Sovereignty Policies in China and the EU. *TPRC49: The 49th Research Conference on Communication, Information and Internet Policy* https://doi.org/10.2139/ssrn.3900752
22. Coleman, A., & Maogoto, J. (2013). "westphalian" meets "eastphalian" sovereignty: China in globalized world. *Asian Journal of International Law, 3*(2), 237–270. https://doi.org/10.1017/S2044251313000179
23. Creemers, R. J. E. H. (2020a). *China's Approach to Cyber Sovereignty*. Konrad-Adenauer-Stiftung. https://www.kas.de/documents/252038/7995358/China%E2%80%99s+Approach+to+Cyber+Sovereignty.pdf/2c6916a6-164c-fb0c-4e29-f933f472ac3f?version=1.0&t=1606143361537
24. Creemers, R. J. E. H. (2020b). China's conception of cyber sovereignty: rhetoric and realization." In D. Broeders & B. van den Berg (Eds.), *Governing Cyberspace: Behavior, Power, and Diplomacy* (pp. 107–142). Rowman & Littlefield. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3532421
25. Davies, G. (2015). Destiny's Mixed Metaphors. In G. R. Barmé, L. Jaivin, & J. Goldkorn (Eds.), *Shared Destiny* (pp. 146–169). ANU Press. http://www.jstor.org/stable/j.ctt19893k8.21
26. DeNardis, L. (2014). *The Global War for Internet Governance*. Yale University Press.
27. Ding, J. (2018). *Deciphering China's AI Dream: The context, components, capabilities, and consequences of China's strategy to lead the world in AI.* Centre for the Governance of AI.
28. Ding, J., Triolo, P., & Sacks, S. (2018). Chinese Interests Take a Big Seat at the AI Governance Table. *New America*. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinese-interests-take-big-seat-ai-governance-table/
29. Edelmann, A., Moody, J., & Light, R. (2017). Disparate foundations of scientists' policy positions on contentious biomedical research. *Proceedings of the National Academy of Sciences, USA, 114*(24), 6262–6267. https://doi.org/10.1073/pnas.1613580114
30. El Damanhoury, K., & Garud-Paktar, N. (2022). Soft power journalism: a visual framing analysis of COVID-19 on Xinhua and VOA's Instagram pages. *Digital Journalism, 10*(9), 1546–1568. https://doi.org/10.1080/21670811.2021.1957969
31. Epstein, C. (2012). Stop telling us how to behave: socialization or infantilization? *International Studies Perspectives, 13*(2), 135–145.

32. Etzioni, A. (2011). Point of order: is China more westphalian than the west? *Foreign Affairs, 90*(6), 172–176.
33. Feinerer, I., & Hornik, K. (2023). *tm: Text Mining Package*. R package version 0.7–11. https://cran.r-project.org/package=tm
34. Feldstein, S. (2023). The consequences of generative AI for democracy. *Governance and War. Survival, 65*(5), 117–142. https://doi.org/10.1080/00396338.2023.2261260
35. Finnemore, M., & Sikkink, K. (1998). International norm dynamics and political change. *International Organization, 52*(4), 887–917.
36. Freeman, C. P. (2020). An uncommon approach to the global commons: interpreting China's divergent positions on maritime andouter space governance. *The China Quarterly, 241*, 1–21. https://doi.org/10.1017/S0305741019000730/
37. Gamito, M. C. (2023). The influence of China in AI governance through standardization. *Telecommunications Policy, 47*(10), 102673. https://doi.org/10.1016/j.telpol.2023.102673
38. Gao, J., Huang, X., & Zhang, L. (2019). Comparative analysis between international research hotspots and national-level policy keywords on artificial intelligence in China from 2009 to 2018. *Sustainability, 11*(23), 6574. https://doi.org/10.3390/su11236574
39. Gao, X. (2022). An attractive alternative? China's approach to cyber governance and its implications for the western model. *The International Spectator, 57*(3), 15–30. https://doi.org/10.1080/03932729.2022.2074710
40. Gillings, M., & Hardie, A. (2023). The interpretation of topic models for scholarly analysis: an evaluation and critique of current practice. *Digital Scholarship in the Humanities, 38*(2), 530–543. https://doi.org/10.1093/llc/fqac075
41. Greene, D., O'Callaghan, D., & Cunningham, P. (2014). How many topics? Stability analysis for topic models. In T. Calders, F. Esposito, E. Hüllermeier, & R. Meo (Eds.), *Machine Learning and Knowledge Discovery in Databases* (pp. 498–513). Springer.
42. Hellström, J. (2021). Sovereignty. *China Media Project*. https://chinamediaproject.org/the_ccp_dictionary/sovereignty/
43. Hinsley, F. H. (1986). *Sovereignty*. Cambridge University Press.
44. Hong, Y., & Goodnight, G. T. (2020). How to think about cyber sovereignty: The case of China. *Chinese Journal of Communication, 13*(1), 8–26. https://doi.org/10.1080/17544750.2019.1687536
45. Jacobi, C., van Atteveldt, W., & Welbers, K. (2016). Quantitative analysis of large amounts of journalistic texts using topic modelling. *Digital Journalism, 4*(1), 89–106. https://doi.org/10.1080/21670811.2015.1093271
46. Johnston, A. I. (2001). Treating international institutions as social environments. *International Studies Quarterly, 45*(4), 487–515.
47. Jiang, M. (2010). Authoritarian informationalism: china's approach to internet sovereignty. *SAIS Review of International Affairs, 30*(2), 71–89. https://doi.org/10.1353/sais.2010.0006
48. Katagiri, N. (2023). Artificial intelligence and cross-domain warfare: balance of power and unintended escalation. *Global Society*. https://doi.org/10.1080/13600826.2023.2248179
49. Kettemann, M. C. (2020). *The Normative Order of the Internet: A Theory of Rule and Regulation Online*. Oxford University Press.
50. Klossek, L. (2020). India's 'Silent Contestation' of the EU's Perspective on Local Ownership. In E. Johansson-Nogués, M. Vlaskamp, & E. Barbé (Eds.), *European Union Contested. Norm Research in International Relations* (pp. 75–93). Springer. https://doi.org/10.1007/978-3-030-33238-9_5
51. Knox, J. (2020). Artificial intelligence and education in China. *Learning, Media and Technology, 45*(3), 298–311. https://doi.org/10.1080/17439884.2020.1754236
52. Kolton, M. (2017). Interpreting China's pursuit of cyber sovereignty and its views on cyber deterrence. *The Cyber Defense Review, 2*(1), 119–154.
53. Li, J. (2019). *tmcn: A Text Mining Toolkit for Chinese*. R package version 0.2–13. https://cran.r-project.org/web/packages/tmcn/index.html
54. Li, K., & Mayer, M. (2023). China's bifurcated space diplomacy and institutional density. *The Hague Journal of Diplomacy, 18*(2–3), 253–281. https://doi.org/10.1163/1871191x-bja10155
55. Lindsay, J. R. (2015). The impact of China on cybersecurity: fiction and friction. *International Security, 39*(3), 7–47. https://doi.org/10.1162/ISEC_a_00189
56. Liu, H. (2021). The role and logic of nontraditional security in China's engagement in global governance mechanisms under Xi Jinping's regime. *Journal of Chinese political science, 26*(3), 505–523. https://doi.org/10.1007/s11366-020-09704-5

57. Liu, Q., Liang, Y., Wang, S., Huang, Z., Wang, Q., Jia, M., Li, Z., & Ming, W. K. (2022). Health communication through Chinese media on E-cigarette: a topic modeling approach. *International journal of environmental research and public health, 19*(13), 7591. https://doi.org/10.3390/ijerph19137591
58. Lo, C. (2010). Values to be added to an "Eastphalia Order" by the emerging China. *Indiana Journal of Global Legal Studies, 17*(1), 13–25. https://doi.org/10.2979/gls.2010.17.1.13
59. Lovelace, R. (2024). China's interest in global AI rules is fueled by fear of falling behind U.S., experts say. *Washington Times*. https://www.washingtontimes.com/news/2024/apr/2/chinas-interest-global-ai-rules-fueled-fear-fallin/
60. Lucas, C., Nielsen, R. A., Roberts, M. E., Stewart, B. M., Storer, A., & Tingley, D. (2015). Computer-assisted text analysis forcomparative politics. *Political Analysis, 23*(2), 254–277. http://www.jstor.org/stable/24572972
61. Lucero, K. (2019). Artificial intelligence regulation and china's future. *Columbia Journal of Asian Law, 33*(1), 94–171. https://doi.org/10.7916/cjal.v33i1.5454
62. March, J. G., & Olsen, J. P. (1998). The institutional dynamics of international political orders. *International Organization, 52*(4), 943–969. https://doi.org/10.1162/002081898550699
63. Maurer, T. (2020). A dose of realism: the contestation and politics of cyber norms. *Hague Journal on the Rule of Law, 12*, 283–305. https://doi.org/10.1007/s40803-019-00129-8
64. Mazzucato, M., Schaake, M., Krier, S., & Entsminger, J. (2022). *Governing artificial intelligence in the public interest.* UCL Institute for Innovation and Public Purpose. https://www.ucl.ac.uk/bartlett/public-purpose/wp2022-12
65. McKune, S., & Ahmed, S. (2018). Authoritarian practices in the digital age: the contestation and shaping of cyber norms through China's internet sovereignty agenda. *International Journal of Communication, 12*, 21.
66. Mimno, D., Wallach, H. M., Talley, E., Leenders, M., & McCallum, A. (2011). Optimizing Semantic Coherence in Topic Models. In *Proceedings of the Conference on Empirical Methods in Natural Language Processing* (pp. 262–272). Association for Computational Linguistics. http://dl.acm.org/citation.cfm?id=2145432.2145462
67. Ministry of Foreign Affairs. (2023). *Global AI Governance Initiative*. https://www.mfa.gov.cn/eng/wjdt_665385/2649_665393/202310/t20231020_11164834.html
68. Mirza, M. N., Ali, L. A., & Qaisrani, I. H. (2021). conceptualising cyber sovereignty and information security: China's image of a global cyber order. *Webology, 18*(5), 598–610.
69. Moore, G. J. (2023). Huawei, cyber-sovereignty and liberal norms: china's challenge to the west/democracies. *Journal of Chinese Political Science, 28*, 151–167. https://doi.org/10.1007/s11366-022-09814-2
70. Mueller, M. (2017). *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace*. Polity.
71. Odgaard, L. (2022). Home versus abroad: China's differing sovereignty concepts in the South China Sea and the Arctic. *Cambridge Review of International Affairs*. https://doi.org/10.1080/09557571.2022.2078278
72. Pan, C. (2020). Westphalia and the Taiwan conundrum: a case against the exclusionist construction of sovereignty and identity. *Journal of Chinese Political Science, 15*, 371–389. https://doi.org/10.1007/s11366-010-9117-z
73. Parasol, M. (2021). AI development and the 'fuzzy logic' of Chinese cyber security and data laws. *Cambridge University Press*. https://doi.org/10.1017/9781009064804
74. Paris, R. (2020). The right to dominate: how old ideas about sovereignty pose new challenges for world order. *International Organization, 74*(3), 453–489. https://doi.org/10.1017/S0020818320000077
75. Pathak, S. (2021). China's Concept of Sovereignty and Military Aggression. *Indo-Pacific Perspectives*, 15–19. https://www.airuniversity.af.edu/Portals/10/JIPA/IndoPacificPerspectives/June%202021/04%20Pathak.pdf.
76. Payne, R. A. (2001). Persuasion, frames, and norm construction. *European Journal of International Relations, 7*(1), 37–61. https://doi.org/10.1177/1354066101007001002
77. Peez, A. (2022). Contributions and blind spots of constructivist norms research in international relations, 1980–2018: a systematic evidence and gap analysis. *International Studies Review, 24*(1), via055. https://doi.org/10.1093/isr/viab055
78. Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*. https://doi.org/10.14763/2020.4.1532
79. Pu, X. (2012). Socialisation as a two-way process: emerging powers and the diffusion of international norms. *The Chinese Journal of International Politics, 5*(4), 341–367.

80. Pu, X. (2019). *Rebranding China: contested status signaling in the changing global order*. Stanford University Press.
81. Qin, W., & Wu, Y. (2019). *jiebaR: Chinese Text Segmentation.* R package version 0.11. http://cran.nexr.com/web/packages/jiebaR/index.html
82. Rigby, R., & Taylor, B. (2015). Whose Shared Destiny? In G. R. Barmé, L. Jaivin, & J. Goldkorn (Eds.), *Shared Destiny* (pp. 56–73). ANU Press. http://www.jstor.org/stable/j.ctt19893k8.11
83. Rinker, T. (2022). *Package 'textstem'*. R package version 0.1.4. https://cran.r-project.org/web/packages/textstem/textstem.pdf
84. Roberts, H., Cowls, J., Hine, E., Morley, J., Wang, V., Taddeo, M., & Floridi, L. (2023). Governing artificial intelligence in China and the European Union: comparing aims and promoting ethical outcomes. *The Information Society, 39*(2), 79–97. https://doi.org/10.1080/01972243.2022.2124565
85. Roberts, H., Cowls, J., Morley, J., Taddeo, M., Wang, V., & Floridi, L. (2021). The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation. *AI & Society, 36*, 59–77. https://doi.org/10.1007/s00146-020-00992-2
86. Roberts, M. E., Stewart, B. M., & Tingley, D. (2019). stm: An R package for structural topic models. *Journal of Statistical Software, 91*(2), 1–40. https://doi.org/10.18637/jss.v091.i02
87. Roberts, M. E., Stewart, B. M., Tingley, D., Lucas, C., Leder-Luis, J., Gadarian, S. K., Albertson, B., & Rand, D. G. (2014). Structural topic models for open-ended survey responses. *American Journal of Political Science, 58*(4), 1064–1082.
88. Rodriguez, M. Y., & Storer, H. (2020). A computational social science perspective on qualitative data exploration: using topic models for the descriptive analysis of social media data. *Journal of Technology in Human Services, 38*(1), 54–86. https://doi.org/10.1080/15228835.2019.1616350
89. Sandholtz, W. (2008). Dynamics of international norm change: rules against wartime plunder. *European Journal of International Relations, 14*(1), 101–131. https://doi.org/10.1177/1354066107087766
90. Segal, A. (2020). China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace. In N. Rolland (Ed.), *An Emerging China-Centric Order: China's Vision for a New World Order in Practice* (pp. 85–100). The National Bureau of Asian Research. https://www.nbr.org/wp-content/uploads/pdfs/publications/sr87_aug2020.pdf
91. Selenium. (n.d.) *Selenium*. Retrieved November 17, 2023, from https://github.com/SeleniumHQ/selenium
92. Sheehan, M. (2023). *China's AI Regulations and How They Get Made*. Carnegie Endowment for International Peace. https://carnegieendowment.org/files/202307-Sheehan_Chinese%20AI%20gov.pdf.
93. Sheehan, M. (2024). *Tracing the Roots of China's AI Regulations.* Carnegie Endowment for International Peace. https://carnegieendowment.org/2024/02/27/tracing-roots-of-china-s-ai-regulations-pub-91815
94. Shen, H. (2016). China and global internet governance: toward an alternative analytical framework. *Chinese Journal of Communication, 9*(3), 304–324. https://doi.org/10.1080/17544750.2016.1206028
95. Song, B. (2021). Introduction: How Chinese Philosophers Think About Artificial Intelligence? In B. Song (Ed.), *Intelligence and Wisdom* (pp. 1–14). Springer. https://doi.org/10.1007/978-981-16-2309-7_1
96. State Council Information Office. (2010). *White Paper on the Internet in China*. The Information Office of the State Council. http://www.chinadaily.com.cn/china/2010-06/08/content_9950198.htm.
97. Sun, T. Q., & Medaglia, R. (2019). Mapping the challenges of Artificial Intelligence in the public sector: Evidence from public healthcare. *Government Information Quarterly, 36*(2), 368–383. https://doi.org/10.1016/j.giq.2018.09.008
98. Tai, K., & Zhu, Y. Y. (2022). A historical explanation of Chinese cybersovereignty. *International Relations of the Asia-Pacific, 22*(3), 469–499. https://doi.org/10.1093/irap/lcab009
99. Wang, A. (2020). Cyber sovereignty at its boldest: a chinese perspective. *The Ohio State Technology Law Journal, 16*(2), 395–466.
100. Wang, F. L. (2015). From *Tianxia* to Westphalia: The Evolving Chinese Conception of Sovereignty and World Order. In G. J. Ikenberry, W. Jisi, Z. Feng (Eds.), *America, China, and the Struggle for World Order* (pp. 43–68). Palgrave Macmillan. https://doi.org/10.1057/9781137508317_3
101. Weston, S. J., Shryock, I., Light, R., & Fisher, P. A. (2023). Selecting the number and labels of topics in topic modeling: a tutorial. *Advances in Methods and Practices in Psychological Science, 6*(2), 1–13. https://doi.org/10.1177/25152459231160105
102. Wickham, H. (2023). *rvest: Easily Harvest (Scrape) Web Pages*. https://rvest.tidyverse.org/
103. Wiener, A. (2008). *The Invisible Constitution of Politics*. Cambridge University Press.
104. Wiener, A. (2014). *A Theory of Contestation*. Springer.
105. Winston, C. (2018). Norm structure, diffusion, and evolution: A conceptual approach. *European Journal of International Relations, 24*(3), 638–661. https://doi.org/10.1177/1354066117720794

106. Wunderlich, C. (2013). Theoretical approaches in norm dynamics. In H. Müller & C. Wunderlich (Eds.), *Norm dynamics in multilateral arms control* (pp. 20–47). University of Georgia Press.
107. Yang, C., & Huang, C. (2022). Quantitative mapping of the evolution of AI policy distribution, targets and focuses over three decades in China. *Technological Forecasting and Social Change, 174*, 121188. https://doi.org/10.1016/j.techfore.2021.121188
108. Zeng, J. (2022). *Artificial Intelligence with Chinese Characteristics National Strategy*. Palgrave MacMillan.
109. Zeng, J., Stevens, T., & Chen, Y. (2017). China's solution to global cyber governance: Unpacking the domestic discourse of "internet sovereignty." *Politics & Policy, 45*(3), 432–464. https://doi.org/10.1111/polp.12202
110. Zhang, D. (2018). The Concept of 'Community of Common Destiny' in China's Diplomacy: Meaning, Motives and Implications. *Asia and the Pacific Policy Studies, 5*(2), 196–207. https://doi.org/10.1002/app5.231
111. Zheng, F., & Di, G. (2022). Global Cyber Governance in China: Towards Building a Community of Shared Future in Cyberspace. *Science, Technology and Society, 27*(3), 456–475. https://doi.org/10.1177/09717218221075958