Conceptualizing the reverse great firewall: cybersecurity and the logics of government geo-blocking in China

Brussee, V.W.D.

Journal of Cybersecurity, 2026, **12**(1), 1–15
https://doi.org/10.1093/cybsec/tyag005
Research paper

Conceptualizing the reverse great firewall: cybersecurity and the logics of government geo-blocking in China

Vincent Brussee *

Leiden Institute for Area Studies, Leiden University, Witte Singel 27A, 2321BG Leiden, Zuid Holland, The Netherlands
*Corresponding author. Leiden Institute for Area Studies, Leiden University, Witte Singel 27A, 2321BG Leiden, Zuid Holland, The Netherlands. E-mail: v.w.d.brussee@hum.leidenuniv.nl

Abstract

China's Great Firewall originally focused on restricting domestic access to resources on the global web. Today, however, efforts in China and beyond concentrate on restricting global access to information on the domestic internet. This article conceptualizes an emerging "Reverse Great Firewall": a set of practices through which Chinese government organs restrict foreign access to domestically hosted information. Geo-blocking is core in this development. It argues that geo-blocking emerges from decentralized responses to top-down cybersecurity pressures, shaped by cadre evaluation systems and local discretion. These cybersecurity concerns in China's context do not just target traditional risks like DDoS-attacks but especially foreign data aggregation, open-source intelligence, and politically sensitive information. Using HTTP/1.1 requests from residential proxies in 14 countries across the world, this study tests the availability of all 13 508 official government websites from China. The results show that >50% of government websites are inaccessible from abroad, with roughly 10% of websites exhibiting explicit and indiscriminate geo-blocking, primarily through either server-side or DNS blocking. The remaining 40% largely reflect network bottlenecks and fragmented infrastructure rather than coordinated policy. Bureaucratically, geo-blocking patterns resemble the fragmented nature of government websites in China, being concentrated in small batches of province and prefecture-level jurisdictions. While the Reverse Great Firewall remains uneven and opaque, it signals a shift in how states may leverage cybersecurity logics to reshape the digital information ecosystem.

Keywords geo-blocking, Reverse Great Firewall, China, censorship, cybersecurity

Introduction

Until recently, internet filtering practices around the world primarily focused on restricting domestic access to resources on the global web. China's Great Firewall has been the paradigm of this type of internet censorship ever since its establishment [1], restricting access to at least 311 000 worldwide domains for over a billion Chinese internet users [2]. In recent years, however, efforts in several countries equally concentrate on keeping *domestic information* out of *foreign* hands. In China, initial reports have emerged of government websites that have started blocking access to foreign observers [3]. The USA have started blocking access to a range of government and military websites for internet users in mainland China and Hong Kong [4]. Since Russia formally invaded Ukraine in 2022, its authorities have started blocking international access to many government websites, too [5].

This article focuses on the emergence of this new type of internet filtering: geo-blocking. Geo-blocking refers to mechanisms restricting access to online content based on the IP address of the user who attempts to access it, which serves as a proxy for the user's geographic location [6]. Superficially, geo-blocking is by no means a new development. Between 2% and 5% of the world's most popular websites geo-block at least one region [7] for reasons ranging from intellectual property to local regulatory compliance [6]. However, what is novel is that some authorities now use geo-blocking to prevent the outside world from accessing information about matters within their country. This resembles a kind of *Reverse Great Firewall*. It adopts the same logics as the 'original' Great Firewall but inverses subject and object. Instead of restricting domestic access to global information, it restricts international access to domestic information. Moreover, this article argues that this type of geo-blocking is surrounded by a discourse of a particular kind of cybersecurity.

In conceptualizing the Reverse Great Firewall, this article takes China as a case study. China's authorities pioneer geo-blocking in the same way as they pioneered the 'original' Great Firewall. They this as a way to guarantee cybersecurity, which in the Chinese context does not just refer to preventing hacking, sabotage, and cyberespionage. Specifically, authorities also take it to mean preventing open-source intelligence and data mining of resources on the public web. Moreover, China has a track-record of inspiring internet filtering practices worldwide: Russia, Uganda, and Myanmar are but a few of the countries that observers claim to have benefited from China's experiences—and sometimes even technical support—in internet filtering [8,9]. Thus, China's practices may not remain confined to its case.

Received: 5 April 2025. **Revised:** 26 November 2025. **Accepted:** 6 January 2026

The emergence of geo-blocking from China will inevitably contribute to the fragmentation of the online information ecosystem. It is problematic for worldwide researchers and stakeholders because it further adds to the already-growing range of access restrictions to offline and online sources from China [see e.g. 10–12]. For businesses, it will make it more difficult to obtain information on, for example, regulatory norms and enforcement. Geo-blocking is also a headache for both Chinese citizens abroad and international citizens with a stake in China, as they may experience increasing challenges obtaining relevant government information. To illustrate, as of March 2025, one of Google's top suggested completions for a Chinese-language search starting with 'government website' is 'cannot enter government website' (政府网站进不去). Using China's Baidu search engine, the fourth suggested completion is 'cannot open government website' (政府网站打不开). Moreover, as a frontrunner in the digital domain, China's experiences are likely to become a model for other actors with similar intentions.

Although geo-blocking has been investigated at length in the computer science [7,13] and intellectual property law [6] communities, these studies have generated few insights into these new cybersecurity-related dimensions. Hence, the aim of this article is threefold. First is to theorize the driving forces behind this type of geo-blocking. Second is to measure the scope and patterns of access restrictions from abroad. Third is to provide insight into the functional logic of geo-blocking from both a technical and governance or political point of view. Given that most known instances of geo-blocking appear on government websites, the article takes these websites as its main object of analysis.

The article proceeds as follows. The next section argues that cybersecurity (in its official Chinese understanding) is a powerful motive for the adoption of geo-blocking, though not a coherent strategy. In China's administrative system, geo-blocking is a localized response to central-level pressures and incentives. Subsequently, the article tests worldwide availability of all extant 13 508 government websites using HTTP/1.1 requests routed through proxies in 14 countries across the world. The results are split in two parts: the first detailing the overall patterns and technical implementation behind geo-blocking, and the second detailing the government's logics. The article concludes by further conceptualizing the Reverse Great Firewall and reflecting on broader implications for China and the world. Together, it demonstrates that >50% of government websites are inaccessible from multiple countries. However, it also shows that both technical and government logics are fragmented and that not all access issues occur due to overt geo-blocking.

Cybersecurity is a powerful potential motive for geo-blocking

This study defines geo-blocking as a range of techniques where service operators deny users from specific geographic regions from accessing their online resources (like websites). Geo-blocking is a rapidly emerging trend. In 2013, lawmakers in Australia exposed price discrimination of online services powered by geo-blocking [14]. In 2018, a variety of news media from the USA blocked access to users from the European Union (EU) over compliance with its new privacy legislation, the General Data Protection Regulation [15]. Current estimates suggest that 13.7% of US media outlets continue to geo-block today [16]. Following the start of Russia's war against Ukraine starting in 2022, service providers deployed geo-blocking techniques against Russia to comply with international sanctions. Meanwhile, Russian government websites adopted geo-blocking to combat extensive distributed denial-of-service (DDoS)-attacks on their infrastructure [5].

This non-exhaustive overview of geo-blocking practices shows its increasing importance for understanding the global internet. Unsurprisingly, therefore, geo-blocking is a rapidly emerging topic in scholarly discussions. Notably, however, most of these discussions take place in the legal domain. An extensive range of articles discusses phenomena such as the European Union's regulations on geo-blocking [6,17,18]. An equally wide range of studies focus on questions surrounding the prohibition of (parts of) geo-blocking [19,20]. Outside the legal domain, a smaller but emerging body of literature from the field of computer science focuses on *measuring* geo-blocking. For example, a leading research team found that 4.4% geo-block at least one country, further nothing that their estimates are likely to have been conservative [7].

Few of these studies explicitly addresses China and only two relevant starting points exist in the current literature. The first found surprisingly poor transnational internet performance in mainland China, which the authors referred to as the 'Great Bottleneck of China'. They suggested that poor network infrastructure was a principal driver, but were not able to identify precisely why. They also did not discuss whether it may have a relationship with geo-blocking [21]. The second, a think tank report, tested a small and unsystematic subset of government websites and found that ˜26% of these websites were unavailable from foreign IP addresses, a substantial part of which appeared to occur due to such internet bottlenecks [3]. However, the investigation provided little further detail beyond this. This has left the geo-blocking in the context of China poorly understood.

Theorizing the interaction of geo-blocking and cybersecurity

Cybersecurity is commonly defined as securing information systems from malicious actors and digital attacks. Many popular definitions connect it to the integrity of computer systems and digital infrastructure [22]. Conceptually, however, definitions of cybersecurity remain uncertain and contested [23]. In practice, its meaning depends on the political and institutional context in which it is invoked: 'it is a terrain on which multiple discourses and (in)securities compete' [24]. Most 'Western' discussions of the cybersecurity concept refer to hacking, disruptions of critical cyber infrastructure, and cyberespionage by 'bad actors' like Russia and China [25]. Meanwhile, Chinese authorities frame cybersecurity as 'the prevention of any risk to the integrity of the Party-led regime' in the digital domain [26].

Because China's authorities adopt a much broader understanding of cybersecurity, it encapsulates not just the aforementioned issues of hacking and cyberespionage, but also 'information security' and 'cultural and ideological security' [25]. This entails issues of online content management (censorship), such as controlling 'rumours'—a catch-all phrase for information that violates the authorities' hegemony on online information. It also includes questions of data exports and cross-border information flows, or

of negative public opinion that can arise from online information. For instance, a local government document from 2022 describes issues like 'errors in wording' in government documents as showcasing 'inadequate cybersecurity defences' [27]. These become cybersecurity issues because, in the Chinese context, such content in the cyber domain could lead to public opinion crises that challenge the security of the political system. Yet, the exact priorities associated with cybersecurity in China evolve as political pressures mould the use of the relatively broad concept [compare e.g. 28,29]. The article takes this understanding of cybersecurity as the foundation of the subsequent analysis.

Although publicly-available sources by China's authorities make few explicit references to geo-blocking, several articles indicate that cybersecurity could be an important potential motive. In 2018, an analysis posted on the website of China's National Administration of State Secrets Protection argued that 'the era of big data blurs the boundaries between confidential and non-confidential data'. This report made extensive references to open-source intelligence conducted by foreign intelligence, military organizations, and even companies like Bellingcat. It noted that these had established significant data mining capacities. Citing a speech by Xi Jinping, it explicitly linked this to the issue of cybersecurity [30]. Similar articles discuss how even 'garbage data' can become a risk in the era of big data [31]. Referring more specifically to government information, another state-affiliated researcher in China suggested that 'some' foreign governments might use government information to 'create divisions among the Chinese people' [32]. Thus, open-source information such as those found on government websites becomes a cybersecurity risk as it could domestically lead to crises in public opinion, and internationally to foreign entities obtaining information on matters that China's authorities would rather keep secret. This risk is not hypothetical. For instance, a 2022 report by the United Nations High Commissioner for Human Rights drew extensively (albeit not exclusively) from open-source information on Chinese government websites to warn about serious indications of crimes against humanity in the Xinjiang region [33]. Subsequently, authorities pulled several sources from the internet, only to re-upload them later with omission of the sensitive bits.

Such concerns in quasi-official circles rapidly made their way into policy and legislation. In 2022, a policy document by the State Council—China's cabinet—explicitly called to 'prevent the risk of leakage [of state secrets] caused by data aggregation' in the context of government information published online [34]. In 2024, these concerns were enshrined in regulations jointly issued by the Cyberspace Administration of China (CAC), Central Organisation Department, Ministry of Industry and Information Technology, and Ministry of Public Security [35]. Note, here, that in China's legal context, state secrets do not need to be explicitly labelled as such as long as the information could be related to China's national security [36].

Another cybersecurity-related risk that geo-blocking can help mitigate are DDoS-attacks and other attacks on the front-end of websites. As noted, Russian websites started geo-blocking to combat extensive DDoS-attacks on their infrastructure [5]. Certain geo-blocking techniques can reduce or entirely eliminate the load of attacks coming from abroad on servers, such as by ensuring that a request never makes it to the server altogether. In this context, China's cyberspace authorities announced as early as 2019 that they were increasing efforts to crack down on malicious use of domestic cloud platforms, that were in that period responsible for >50% of DDoS attacks [37]. Even then, that meant that slightly under half of DDoS-attacks came from abroad, for which geo-blocking can then present a solution. As the article reveals later, at least one website explicitly states such risks as its motive for geo-blocking.

Government concerns coincide with cybersecurity-driven access restrictions on private platforms

These political developments coincide with explicitly cybersecurity-motivated access restrictions on privately operated platforms. In 2022 and 2023, foreign access was cut to several platforms including the important company database Qichacha, the academic database China National Knowledge Infrastructure (CNKI) [38], and financial service provider Wind [3]. This followed regulatory action by the Cyberspace Administration of China (CAC). The CAC is a remarkably opaque organization and usually remains tight-lipped about the precise drivers of its actions [39]. However, in the case of CNKI, it explicitly cited *cybersecurity* reviews as the reason for the restrictions. Aiqicha, another company database, explicitly notes on its website that 'according to relevant laws and regulations, we temporarily do not support access to this website from regions outside of mainland China' (https://web.archive.org/web/20251113025408/https://aiqicha.baidu.com/acount/accessrestriction). These developments follow the increasing deletion of government data, a declining transparency of the Chinese government [11,40] and heightened emphasis in Chinese law and policy on issues of data localization [41] and controls on data exports [42]. Altogether, these instances reveal a concern of information on the Chinese internet falling in foreign hands and a drive to implement foreign access restrictions in response.

Nevertheless, these instances did not involve geo-blocking. Instead, they involve means such as real-name registration. Real-name registration refers to requiring users to register for online services using a phone number with a Chinese country code (+86). This is because Chinese phone numbers are linked to the user's real identity card information [43]. Hence, such phone numbers are difficult to obtain. Other platforms have simply revoked licenses for foreign entities. However, such measures are often off-limits to government organs. One potential reason for this is that government information must be available to all Chinese citizens, especially also for users with lower digital mobility. Tools like real-name registration, licensing requirements, or even captchas would inhibit accessibility, as not everyone is digitally literate or has access to a phone number. This leaves geo-blocking as the main remaining tool in the toolbox for government organs.

Thus, cybersecurity—in the interpretation of China's authorities—is a powerful potential motive for the adoption of geo-blocking. Official sources express concerns with how foreign institutions or companies can mine information from the Chinese internet in an era where the value of data only becomes apparent *after* it is aggregated and combined with other sources [30]. The notion that the value of data cannot always be determined in advance limits the policy options at authorities' disposal. It means that tweaks to mechanisms for the review of information disclosure—measures discussed in the early 2010s

[44]—would be insufficient. Furthermore, fully restricting disclosure of *all* government information to the public would harm other government priorities: transparency is a core means to resolve principal-agent dilemmas in policy implementation [45], fight corruption [46,47] inform citizens and businesses about the norms they need to comply with, and improve trust in the government [46] Even China's president Xi Jinping has been explicit about considering at least partial transparency as crucial to the country's development [48].

Management of government websites in China fosters fragmented responses to centrally directed cybersecurity concerns and pressures

A closer look at the management practices for government websites in China helps elucidate how these concerns can lead to foreign access controls like geo-blocking. The management of official websites in China is decentralized yet strictly supervised. The General Office of the State Council is end responsible for guiding and supervising government websites [49]. Subsequently, the general office of each province or ministry is responsible for the websites under their jurisdiction. For example, the General Office of China's National Development and Reform Commission (NDRC) is responsible for all websites operated by the NRDC and its subordinate agencies. At a provincial level, the general office of that province is responsible for the websites of all government organs (provincial departments, prefectures, and counties) in that region.

The General Office of the State Council has prescribed a range of functions and design standards for official websites. These include standards for domain names, the use of visual elements like logos, the types of information that should be made public, services to be offered, and so on. The standards for such visuals, content, and services are relatively clear and strict [50]. For security and technical implementation, however, details are comparatively vague. Design guidelines only indicate that websites must 'take necessary measures to prevent attacks, intrusions, damage to government websites, and unexpected incidents affecting the normal operation of government websites' [49]. Other than specific measures to prevent access to back-end systems, local authorities are left to develop measures on their own accord. This is by design and reflects a long-standing practice in Chinese policy, where top-level guidance is left open-ended for local authorities to implement according to their discretion [51].

Instead of prescribing specific security measures, central authorities evaluate local authorities on the *outcomes* of their approaches. Starting in 2019, the General Office of the State Council has organized annual inspections of government websites [52]. On top of that, it has required the general offices of ministries and localities to conduct quarterly inspections of websites. These evaluations feed into the annual cadre evaluation mechanisms for government officials, meaning that performance on such assessments can contribute to one's promotion and demotion. Furthermore, they contain 'veto criteria': conditions that will automatically cause the government website and the responsible department to fail the assessment, irrespective of performance in other domains. Such criteria include security breaches and leaks, which these criteria define as (amongst others) 'serious negative opinion arising from website management' and 'leaks of state secrets'. These criteria echo many of the aforementioned cybersecurity concerns related to data aggregation and leaks of open government information. They also reinforce the intrinsic connection between Beijing's conception of cybersecurity and information controls. Meanwhile, a notable omission from the evaluation criteria is international access. The evaluation criteria do require websites to load within 15 s. Failure to do so for at least 5% of requests throughout a week of testing will lead to a veto. However, these do not require testing from abroad [52].

The pressures associated with such website evaluations appear serious. One city demands that cadres must submit a rectification report within *one* working day of receiving the inspection results [53]. In assessing these results, local authorities indicate the need to establish a 'bottom-line mentality' for cybersecurity [29]. To do so, cadres responsible for the management of websites must 'firmly guard against political, legal, policy, confidentiality, and textual issues' [54].

The strict supervision imposed on website administrators means that little is left to chance. Outcome-based evaluation often leads lead to over-implementation, where lower-level cadres attempt to score good results by any means possible [e.g. 55,56]. Prioritizing outcomes over processes also creates the foundations of fragmented implementation, where every department implements whatever measures they deem subjectively necessary to ensure the right outcomes. In lieu of specific guidelines on international access, local authorities have little interests to foster connectivity yet have incentives to expand their cybersecurity toolbox. Thus, it is impossible to speak of a centralized strategy or a coherent practice. Instead, the resulting actions of local authorities are individual responses to centrally-directed cybersecurity concerns and pressures. This is consistent with the development of China's 'original' *Great Firewall*, where some local authorities have added extra layers of internet filtering on top of the national mechanisms [57].

Granted, this discussion connecting geo-blocking in China with authorities' conception of cybersecurity remains circumstantial. It showcases a clear correlation between cybersecurity concerns, the management practices for government websites, and the emerging patterns of geo-blocking. However, it cannot establish causal relationships. After all, even if geo-blocking would be a national strategy, it is unlikely that authorities would broadcast this to the world. This discussion should, therefore, also not be read as establishing hard causal evidence. Instead, these factors are potential drivers that emerge from the governing logics of China's authorities and their discursive understanding of the concept of cybersecurity.

Methods

The remainder of this article empirically measures government geo-blocking in China and studies the technical and functional logic. It obtained information on all extant government websites through China's official *National Database of Basic Information on Government Websites* (全国政府网站基本信息数据库) [58] (Full dataset available via: https://doi.org/10.5281/zenodo.18172144. Specific testing results will be shared upon reasonable request to the corresponding author.). This database comprehensively covers all government websites in existence today. Information it

provides includes the link to the page, the name of the government organ, its administrative level, and the status of the website. In total, this yielded 13 508 links, of which the official database indicates that 13 497 (all but eleven) should be operating as usual. Table 1 shows their composition. The distribution of websites reflects China's Leninist bureaucratic system, which reproduces the structure of the national government across its localities. This creates a pyramid-like structure. The national-level government has over 60 different departments. This then multiplies itself across all 32 provinces, 335 prefectures, and counties (over 3000). However, not all local departments have their own website, especially at the county level. Instead, many have in recent years migrated their content to the websites of higher-level government units [59]. Hence, the pyramid tapers again towards the lowest levels of government.

Testing took place in November 2025 using standard HTTP/1.1 requests (I manually investigated a small sample of around 20 government websites, including the most authoritative https://www.gov.cn, and none supported other protocols. Hence, the article did not test HTTP/2.0 or QUIC.), routed through a network of proxies provided by a third-party provider. These proxies exclusively include residential proxies (A residential proxy is a device connected to a home network, in contrast to a large datacentre.) to mimic real-life users and prevent the websites from seeing these requests as spam from large data centres. Testing used random browser headers (A browser header provides metadata about the request to a server, describing the details of the browser submitting the quest.) for each request from a collection of one thousand common browser headers. Each website was given three different attempts with a fixed time-out duration of 15 s per request, each attempt rotating to a different residential proxy within the specified location and using a different browser header. Although testing through proxies might be inferior to testing directly from a local server, the author also compared results with results obtained from a third-party website speed tester. Appendix 2 provides a brief overview of these robustness checks.

Testing relied on proxies from a balanced mix of 14 countries across the world, with diverse levels of diplomatic relations with China and at varying geographic proximity to China (Unfortunately, the provider used for this study no longer supported Russian proxies at the time of testing, potentially in relation to Russia's ongoing war against Ukraine.). For especially large countries or countries with a potentially mixed quality of internet infrastructure, the proxies routed from a specific city. Proxies in Shanghai, China provided a baseline to assess results against, allowing to differentiate blocked websites from broken websites or those detecting the testing methods as suspicious web traffic. See Table 2 for the full overview.

To detect geo-blocking, researchers typically identify geo-blocking through the status code that a client uses to respond to a HTTP request. In this way, the author classified 403-status codes ('Forbidden') as forms of geo-blocking [7,13]. Status codes are three-digit responses that a server uses to respond to a request. They indicate how the request was handled by the client. A 403-status code indicates server-side blocking. That means that the server denied access to the online resource based on certain parameters of the request, such as its geographic origin. A comparison with results from the Shanghai-based proxies as well as manual spot checks confirmed that virtually all 403-status codes indeed indicated geo-blocking.

Upon investigating the initial results, the author stumbled upon other types of failed requests. Sometimes, a request was unable to reach the server in its entirety. In such cases, the request does not reach the client and fails to return a status code. Instead, the browser returns an error message. Hence, the author followed an iterative process to develop a custom classification scheme. This is based on a combination of HTTP status codes and any other errors throughout the process. Table 3 describes these classifications. In all cases, the author combined this analysis with alternative sources like the Wayback Machine, third-party speed testers, and domain name system (DNS)-checkers for more information. Appendix 1 provides more detail on the classification scheme.

The tester encountered miscellaneous errors in a tiny percentage of cases (4.4% from the Shanghai testing location). Some of these included websites blocking automated requests, often represented as 412 HTTP status codes (Precondition Failed). In other cases from this group, the websites returned 502 HTTP status codes (Bad Gateway) for all requests coming from requests routed through proxies. However, there were also instances where such errors were still indicative of geo-blocking, discussed in more detail later.

The multifaceted technical logics of geo-blocking

Overall, the worldwide availability of Chinese government websites is limited yet not absolutely restricted. Figure 1 illustrates this by aggregating the results by testing location. Using the Shanghai-based proxies, 91.3% of websites were accessible normally. This decreases to 66.4 and 64.9% for the Hong Kong and Taiwan-based proxies, respectively. These were the best-performing locations outside mainland China. Beyond this, successful response rates dropped to below 50%, ranging from 49.7% for South Africa to 46.7% for the Netherlands. Geo-blocking practices amount for up to 10% of failed requests, while time-outs account for 38–40% of requests from proxies outside mainland China. This section breaks down the multifaceted technical logics of these access constraints.

Explicit server-side blocking

Server-side blocking is the most common form of overt geo-blocking, although it currently still affects a relatively small proportion of websites (between 5.5 and 7%). Server-side blocking means that the server hosting a website inspects the details of a request to the server (i.e. to load a webpage), and denies it based on the details of the request. Technically, this can happen for a variety of reasons but in this case, manual verification confirmed that the server denies the request based on the origin location of the request.

Although the overall percentage of server-side blocking is relatively small, the websites that implement it are significant. The provincial government of Anhui Province—one of China's largest provinces with a population of >60 million—was the first to consistently geo-block foreign IP addresses. At least 51 sub-domains under the provincial government currently use server-side means to block foreign access. Together with it came most departments and localities under its administrative area. According to records of the Wayback Machine, Anhui has done so consistently since October of 2022, although earlier snapshots indicate it intermittently

Table 1 Overview of websites tested.

Administrative level	Total number of websites analysed
National and ministerial organs (部委门户网站)	63
Sub-ministerial departments (国务院部门所属网站)	534
Provincial-level governments and their departments (省级政府/组成部门网站)	1596
Prefecture-level governments and their departments (地级政府/组成部门网站)	8220
County/district-level governments	3095

Table 2 Overview of locations tested.

Region (abbreviation)	City *(if applicable)*
China (cn)	Shanghai
The Netherlands (nl)	
United States (us)	Los Angeles
Australia (au)	Sydney
Singapore (sg)	
Taiwan (tw)	Taipei
Japan (jp)	Tokyo
Hong Kong (hk)	
South Africa (za)	Johannesburg
Thailand (th)	Bangkok
Nigeria (ng)	Lagos
Brazil (br)	Rio de Janeiro
Germany (de)	
Italy (it)	

Table 3 Classification of results and interpretation.

Classification	Identification	Interpretation
Available	HTTP status codes starting with 2xx	The request to the website succeeded and the website is accessible.
Blocked (Server-side)	403 status codes	The server blocks the testing client from accessing this webpage, a typical response in geo-blocking.
Blocked (DNS)	DNS resolution errors when attempting to reach the server	The browser is not able to find the location of the server in the Domain Name System (DNS). A manual investigation, discussed in detail later, confirmed that these issues exclusively occurred for non-China-based DNS servers.
Time-out	The request times out before reaching the server	The request is unable to reach the requested server within the allocated time.
Other errors	Any other miscellaneous non-successful requests	Residual category for a variety of errors. These errors include client errors (4xx-range HTTP status codes) and server errors (5xx-range) that may have been caused by servers detecting the testing methods as suspicious activity. There were also instances of defunct websites during testing.

used this prior to this period, too (See: https://web.archive.org/web/20220515000000*/http://ah.gov.cn/.). Other prominent regions include Henan (41 domains) and Hainan (16 domains). At a national level, the Supreme People's Court (SPC) has geo-blocked all non-mainland-China IPs on the Chinese-language version of its website since September 2023. It, too, had briefly geo-blocked its webpages during November 2022 but has now implemented it consistently.

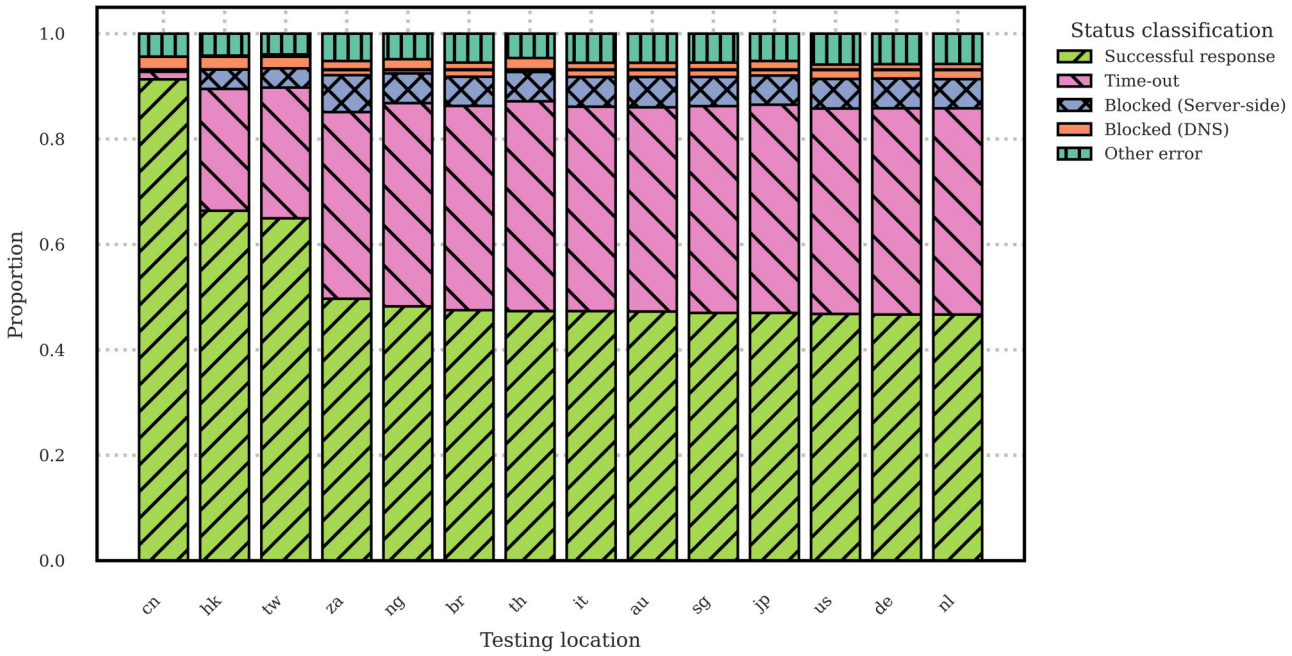

Figure 1 Website availability by location of proxy server.

DNS-based blocking

Failures to DNS-resolve accounted for 2.8% of all requests. In the dozens of cases that I manually investigated, all DNS resolution errors turned out forms of geo-blocking. DNS-based blocking involves using the DNS, which translates human-readable domain names into IP addresses that a computer can use to locate others on the internet. It is, in effect, the phonebook of the internet. Website administrators configure their servers to only allow resolution by specific DNS servers, such as those within China. In such case, non-China based DNS servers will not be able to resolve the domain name into an IP address. In this way, a browser request will be unable to reach the website. DNS resolution errors *can* occur due to technical errors, yet they are also easy to identify and resolve. This makes it rather unlikely that errors occur for large government websites and that these errors affect only those outside of mainland China, especially for extended time periods. This is also consistent with how government and military domains in the USA deploy DNS-blocking against China and Hong Kong [4].

As the data illustrates, DNS-based blocking is relatively less common than server-side blocking. At a provincial level, units under the Tibet Provincial Government are DNS-blocking the most, but the practice also extends to (departments of) the provincial governments of Inner Mongolia, Beijing, Liaoning, Tianjin, and Xinjiang. At the prefectural level, localities that use DNS-blocking include Changsha (the capital of Hunan Province), Shenyang (capital of Liaoning Province), and Hefei (capital of Anhui Province). In total, at least 41 unique prefecture-level cities use DNS blocking on at least one (sub-)domain.

Opaque geo-access filtering at the content delivery network-level

In the majority of cases I manually investigated, errors classified as 'other' were related to broken websites or, more commonly, websites blocking the testing methods. However, there were scattered cases where these errors appeared indicative of geo-blocking, too. In total, 4% of requests from Shanghai-based proxies failed due to miscellaneous reasons, while 5.5% failed from other parts of the world. This difference indicates that there is a small percentage of websites that uses more opaque forms of geo-blocking.

One particularly opaque case that I manually investigated is that of Shaoyang, a prefecture-level city in Hunan. All websites of the city, including its municipal departments, returned 502 HTTP errors while testing. First, using an international speed-checking tool with local servers, I confirmed that these websites were accessible from within mainland China, as well as from Hong Kong. As it turned out, the municipal government domain czj.shaoyang.gov.cn exhibited opaque Content Delivery Network (CDN)-mediated access geo-filtering. In this case, the Chinese government site is fronted by a CDN that splits traffic by geography. This sends domestic Chinese users to the working server while foreign users are sent to an edge closer to their physical location (usually France or the Netherlands, in this case). However, this upstream edge fails to serve the content, yielding the 502 Bad Gateway response. To test whether this was an issue of misconfigured local nodes or intentional tampering, I attempted to force direct access to the origin using *curl—resolve* commands to direct traffic to domestic nodes of the CDN. When prompted from abroad, the request reached the server, yet immediately returned a 502 Bad Gateway error too. The error message briefly mentioned 'wswaf', which appears to refer to the Web Application Firewall (WAF) by Chinese cybersecurity company Wangsu (https://en.wangsu.com/product/52). Domestic Chinese vantage points, by contrast, resolved to Chinese Telecom/Unicom nodes and received normal HTTP 200 responses. The pattern indicates a policy-driven geographical access restriction implemented through CDN/WAF routing rather than a fault or transient misconfiguration.

Internet bottlenecks and time-outs

As reflected in Figure 1, requests timing out before reaching the server make up, by far, the largest group of unavailable websites throughout the testing. There are certain indications that this is not a conscious strategy. While research has identified timeouts can occur as a result of interference by elements of the Great Firewall [60], there still remain more plausible explanations. A request to a provincial department in Shaanxi Province that relatively consistently times out requests is a representative example. After checking that DNS resolution proceeded normally and that the server was accessible through proxies in China, the author traced the path followed by the request using route tracing tools. That is to say, web requests are routed through a network of routers and servers ('hops') on the way to their destination server. Route tracing tools follow this path, allowing diagnosis of bottlenecks or technical issues. Table 4 displays the route from the author's client in the Netherlands to this webpage. Even using a longer time-out delay of 30 s per hop, this request eventually fails and times out.

As the Table reveals, the request is pinged back and forth within China, failing to find a route to the server. The request to the website makes it into China relatively quickly, albeit with one time-out in Europe. After arriving in China, however, the request ends up being pinged back and forth between different locations attempting to find a path. This ultimately fails. Meanwhile, the routing speed has slowed down tremendously, taking over one second per hop. All evidence points towards this being a technical bottleneck on cross-border traffic into China. Previous research has demonstrated the presence of the 'Great Bottleneck of China' [21]. Moreover, it highlighted that, in most cases, the bottleneck is located deeper into China [21]. The results from this article are consistent with this finding. Figure 2 groups the results by the administrative location of each website. It illustrates that availability is worse for websites of local government organs than it is for national organs. Websites of provincial governments perform relatively better than those of smaller prefecture or county-level governments, too. In effect, the websites that time out are concentrated in more rural regions, where the internet capacity may be more limited. This equally explains why the patterns of time-outs have not been found in previous research on internet infrastructure in China, as most websites tested in such studies are commercial websites that have a wider geographic range of servers at their disposal.

Furthermore, websites timing out, indeed, are more concentrated in areas further from China's main internet gateways in Beijing, Shanghai, and Guangzhou. These three regions, in fact, are among the lowest time-out rates. Figure 3 displays the percentage of websites timing-out by the prefecture-level division of the website. It shows two things. One is that that especially websites in regions deeper into China time-out regularly. If there *were* a conscious decision to control access to government websites, one would, to the contrary, expect this to be concentrated in regions with more cyber-related resources rather than fewer. One might also expect it to follow a more top-down pattern, rather than being arbitrarily scattered across smaller divisions of government, or to be concentrated in China's more contentious western regions. Both are not the case here. Still, not all more remote regions exhibit extensive time-outs—such as Xinjiang, Ningxia, and Tibet—indicating that the problem is inconsistent and may depend on local context. Second is that the time-outs are concentrated at the prefecture level. While the majority of regions witness little to no time-outs, where time-outs do occur, they affect all or nearly all websites in the region.

It remains plausible that political and administrative priorities indirectly shape some of the observed timeout patterns, even in the absence of explicit geo-blocking decisions. As noted, government websites are exclusively evaluated on cybersecurity risks and domestic availability, not on international availability. Under such conditions, extensive time-outs for cross-border requests reflect the absence of incentives for local authorities to invest in robust external connectivity. Moreover, researchers investigating internet bottlenecks have hypothesized that data inspection by the Great Firewall may contribute to slow cross-border traffic, although their research did not establish evidence to prove this [21]. Unfortunately, transnational networks are a black box, and it may remain impossible to reach a definitive conclusion without insider knowledge [21].

The government logics of geo-blocking

Because there are no explicit references to geo-blocking in Chinese policy or surrounding discussions, there is little conclusive evidence of what triggers authorities to adopt the practice and how authorities have arranged it organizationally. As noted, Anhui appears to have been the first region to geo-block at a large scale in 2022, followed by the SPC in 2023. The timing appears to correlate with a policy directive by China's State Council from spring 2022 that, for the first time, acknowledged the potential risks of the aggregation of government information [11,34]. Nevertheless, there is not enough evidence to establish causality. Instead, this section discusses what the *data* reveals about the government logic in play.

Fragmented geo-blocking practices are concentrated at the provincial and prefecture levels

That geo-blocking is not applied universally and that the exact means of implementation differ illustrate that geo-blocking is not dictated in clear terms by the central government. Instead, geo-blocking becomes a localized *interpretation of and response to* central-level cybersecurity pressures. Figure 4 shows the proportion of websites that conduct geo-blocking by geographic region. At a provincial level, Anhui and Henan are the only ones to geo-block at a substantial scale, although there are scattered instances in other provinces as well. At a prefecture-level, many cities under these provinces also geo-block, such as Hefei, Anqing, Nanyang, Xinyang, and so on. In this way, when the provincial government's website geo-blocks, many websites under its authority follow.

Although this data indicate that the provincial government directs many instances of geo-blocking under their jurisdiction, this is not the case all the time. As Anhui and Henan geo-block a variety of websites under their jurisdiction, not all prefectures follow suit. Regrettably, there is not enough evidence to speculate whether this indicates a difference of opinion, a lack of resources, or simply an implementation lag. Inversely, however, there are fewer cases where geo-blocking practices are initiated by governments below

Table 4 Route tracing of a request to servers timing out.

Hop	Target router of hop	Time to reach router (ms.)	Time at router (ms.)	Time back to device (ms.)
1	Client router	6	6	6
2	Local routing server of client's internet service provider	8	8	8
3	Datacentre, the Netherlands	39	*	*
4	*Request time-out*	*	*	*
5	Datacentre, Germany	17	19	16
6	China Telecom Europe datacentre, Germany	46	44	41
7	*Request time-out*	*	*	*
8	ChinaNet backbone datacentre Huizhou (Guangdong Province)	266	*	264
9	ChinaNet backbone datacentre, Beijing	267	279	284
10	ChinaNet backbone datacentre, Huizhou (Guangdong Province)	*	*	283
11	ChinaNet datacentre, Taiyuan (Shanxi Province)	*	*	291
12	ChinaNet datacentre, Taiyuan (Shanxi Province)	289	281	291
13	*Request time-out*	*	*	*
14	ChinaNet datacentre, Taiyuan (Shanxi Province)	287	452	424
15	Shaanxi Province Economy Info Centre, Xi'an	274	267	*
16	*Request time-out*	*	*	*

Asterisks (*) indicate no response. All requests after hop #16 timed out (for a total of 30 attempted hops). For readers less familiar with Chinese geography, note that Shanxi and Shaanxi are two different but neighbouring provinces.

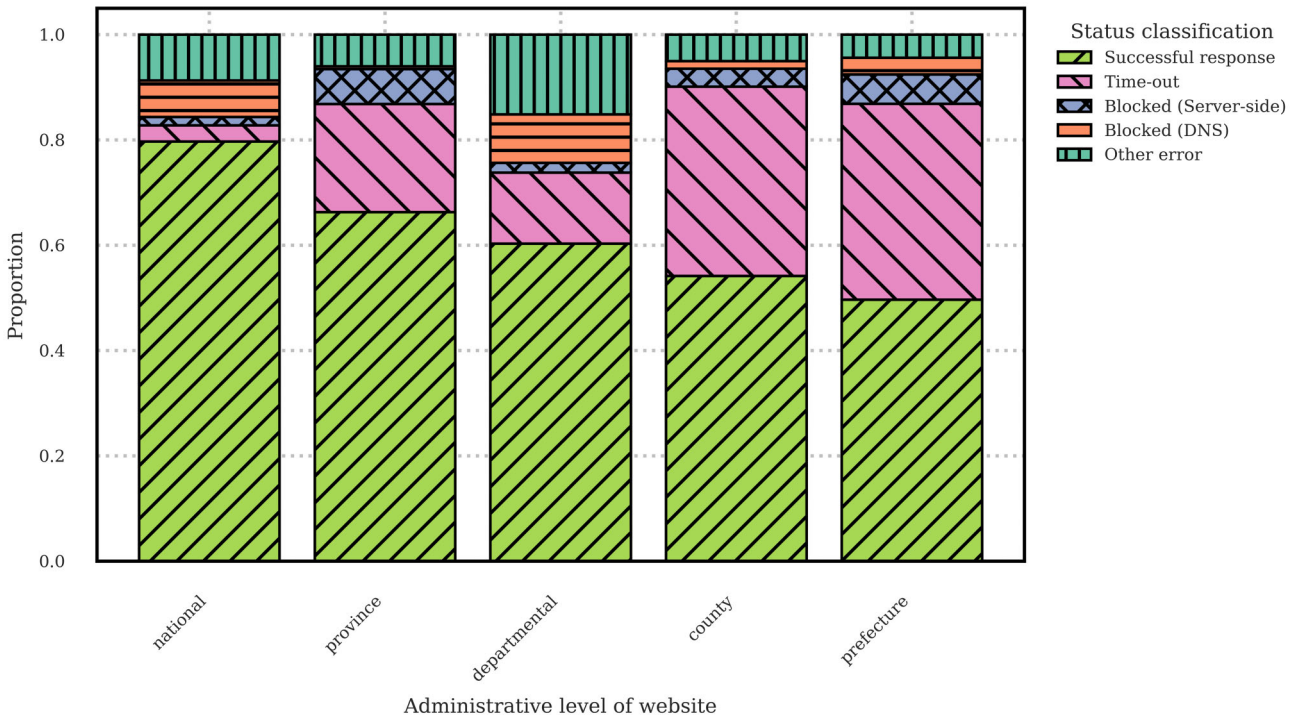

Figure 2 Website availability by administrative level, aggregate of all proxy locations.

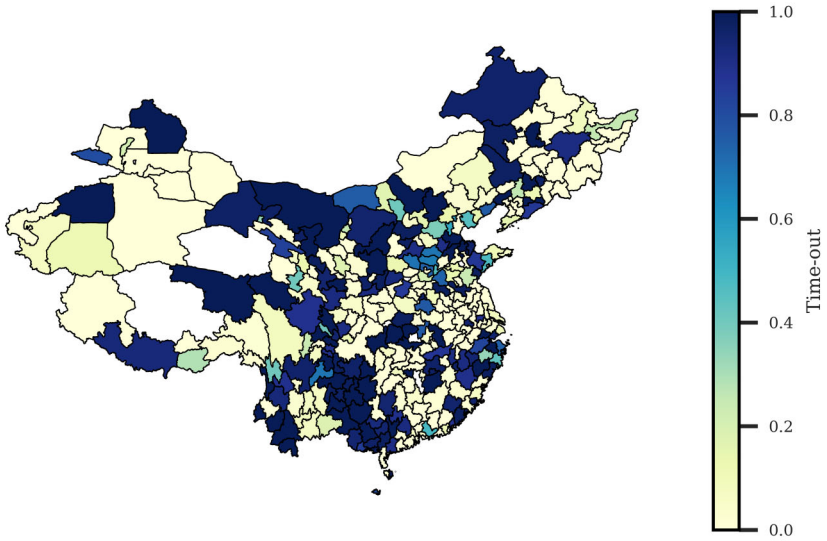

Figure 3 Proportion of websites that time-out relative to total number of tested websites, categorized by their corresponding prefecture-level division. Testing location: USA, Los Angeles.

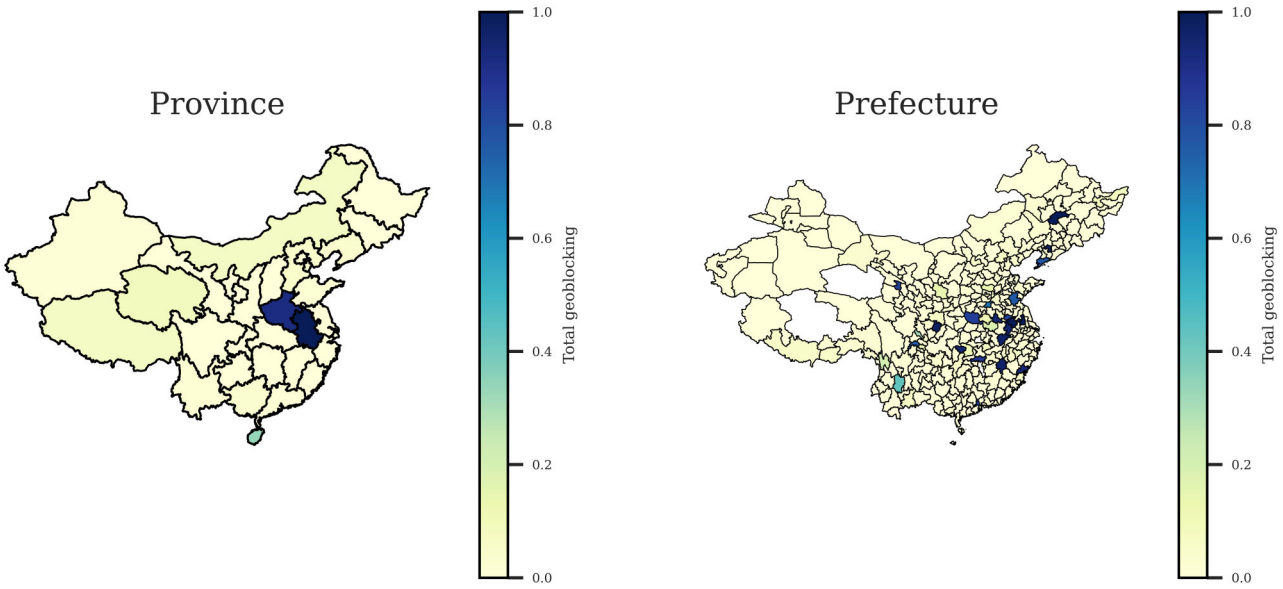

Figure 4 Proportion of websites conducting DNS-based and server-side blocking, by corresponding provincial and prefecture-level administrative division. Testing location: USA, Los Angeles.

the provincial level. Thus, geo-blocking is neither a fully top-down nor bottom-up initiative. It falls somewhere in the middle, where there is a degree of direction from provincial and prefecture-level authorities but also a degree of flexibility.

Instead, the deployment of these practices overlaps with the management structures of government websites. According to the State Council's guidelines for government websites, the General Office of each ministry and provincial government is responsible for websites under its jurisdiction. In effect, this means that they are responsible for setting up the technical infrastructure used to host relevant websites, which all subservient departments must use. Prefecture-level cities can apply for the approval of independent infrastructures. Some of them indeed have independent website infrastructures, while others continue to use the provincial infrastructure. This explains why many, but not all local websites follow the example of the provincial government. County-level governments must rely on the infrastructure of their superior governments (the prefecture and/or provincial government), which explains why there is no significant difference between county-level and prefecture-level results [49]. Thus, geo-blocking is neither truly bottom-up or top-down. Instead, its adoption reflects the fragmented ecosystem of government websites.

Some websites are explicit about the cybersecurity-related motives for this geo-blocking. One local website in Zhejiang returns a non-standard 420 HTTP status code to all responses from abroad, excluding Hong Kong. It directs users to a 'blacklist page' that

indicates that the IP address in question 'was blocked due to a suspected attack'. It, however, even does so for requests from previously unseen IP addresses, such requests by the research team from authentic networks that had never been used to request the website before. Thus, instead of using targeted scanning for potential risks, website administrators simply banket-banned all foreign IP addresses from visiting the website.

Geo-blocking is indiscriminate, with the exception of Hong Kong and Taiwan

Authorities make little difference between countries or regions in overt geo-blocking. Figure 5 isolates and zooms in on the overt forms of geo-blocking from Fig. 1. The results show that, for the most part, geo-blocking rates are consistent across the world. For most regions, around 5.5% of websites conduct server-side blocking while 2.8% of websites use DNS blocking. The exact percentage fluctuates a little per region, but this difference is generally negligible. However, the results also show a split regarding Hong Kong and Taiwan. Only two-thirds of the websites that geo-block countries in the rest of the world also geo-block these areas, at a total of 3.7 and 3.6%, respectively. This is a further indication of fragmentation. It also hints that cybersecurity risks from these regions are not assessed consistently, or that they compete with political motivations that signal unity between China and these regions.

Preliminary evidence indicates institutional learning is taking place

There appears to be a process of institutional learning. Notable is that both Anhui and the SPC have had periods of intermittent geo-blocking before they switched to a more permanent mode of operations that has been stable for over a year. Anhui and the SPC also display the exact same distinctive error message when geo-blocking clients, hinting at the use of similar service providers. Some organs might still be in an explorative phase. The National People's Congress—China's legislature—geo-blocked all clients outside of mainland China, Hong Kong, Macao, and Taiwan between 21 and 23 May 2024 (it, too, displaying the same distinctive message). It, however, switched back to permitting full access, leaving only speculation about its motivations. Meanwhile, there are also cases where authorities initially geo-blocked and halted this later. For example, Jiangxi Province blocked all provincial-level websites under its jurisdiction in early 2025, but rolled this back at the time of testing. Still, as of this study, five prefecture-level cities in the province continue to geo-block. The fact that such patterns of partial or intermittent geo-blocking have appeared for virtually all websites points towards authorities testing the waters before deciding whether to implement it more broadly. Alternatively, they may see geo-blocking as an interim solution while implementing more robust alternative measures.

Discussion: conceptualizing the reverse great firewall

The emergence of government geo-blocking in China resembles a *Reverse Great Firewall*. This refers to a range of techniques that authorities can deploy to restrict foreign access to websites within China, specifically to obscure important information from prying eyes. Although geo-blocking itself is far from novel, the Reverse Great Firewall is unique because of its overtly geopolitical and information control-driven nature. Its emergence follows concerns surrounding the 'leaks' of important government data to foreign observers, especially through data aggregation and open-source intelligence. In this way, it is intrinsically connected to China's cybersecurity agenda.

The Reverse Great Firewall is fragmented and involves different techniques. Like its namesake, the Reverse Great Firewall is not one comprehensive system but rather a collection of various mechanisms. Research on the original Great Firewall has revealed regional and technical fragmentation [60]. Technologies it relies on include Domain Name Service (DNS)-blocking, DNS poisoning, and the blacklisting of specific IP addresses [60,61]. Equally like its counterpart, there is no established legal framework governing the Reverse Great Firewall. Not a single (public) legal or policy document refers explicitly to geo-blocking. Still, institutional learning appears to be taking place, with local governments testing and sometimes expanding, sometimes rolling-back geo-blocking practices.

Like the 'original' Great Firewall, which was a term coined by analysts, the concept of the Reverse Great Firewall is principally an analytic concept. Both the 'original' and its reversed form do not resemble a fully comprehensive system. Neither do these concepts resemble a direct translation of a concept or practice with a Chinese origin. Thus, there must remain some caution in drawing too many parallels between the two. The Great Firewall, for example, relies extensively on DNS poisoning [60]. This is ineffective for blocking access to resources on China's internet, as its authorities cannot manipulate DNS servers that are not based within their geographic jurisdiction. Still, the concepts are useful 'twins' that describe similar information control logics: where the 'original' restricts access to resources on the global web for Chinese internet users, its newer sibling restricts access on the Chinese web for global internet users.

Moreover, the concept only partially covers the empirical patterns witnessed in this study. Table 5 below summarizes the four main layers of access restrictions highlighted in this article. Cross-border time-outs, for which it is difficult to conclusively establish cause and motive, make up the vast majority of cases (39% for the US-based proxies). Explicit instances of geo-blocking that one may ascribe to the Reverse Great Firewall make up 8.3% of results from US proxies, or 1 125 websites. The actual percentage may be higher, as websites that are not available due to time-outs may actually implement server-side blocking as well—the test requests simply were not able to reach this stage. Extrapolating from the finding that 5.6% of websites implement server-side blocking of US proxies, the total number of geo-blocking websites would reach up to 1420 or 10.5% of the total. Moreover, 'other errors' during testing were 1.2% more frequent for non-China-based proxies, which may indicate that more instances of geo-blocking remain.

More than just a new conceptual development, government geo-blocking is a challenge that researchers, businesses, and policymakers will have to manage when analysing developments in China. It is not that simple to circumvent given that China's internet watchdogs have embarked on a quest to purge the use of unlicensed proxies and virtual private networks (VPNs). Although this measure was implemented to restrict opportunities to circumvent the original Great Firewall, a side effect is that most established

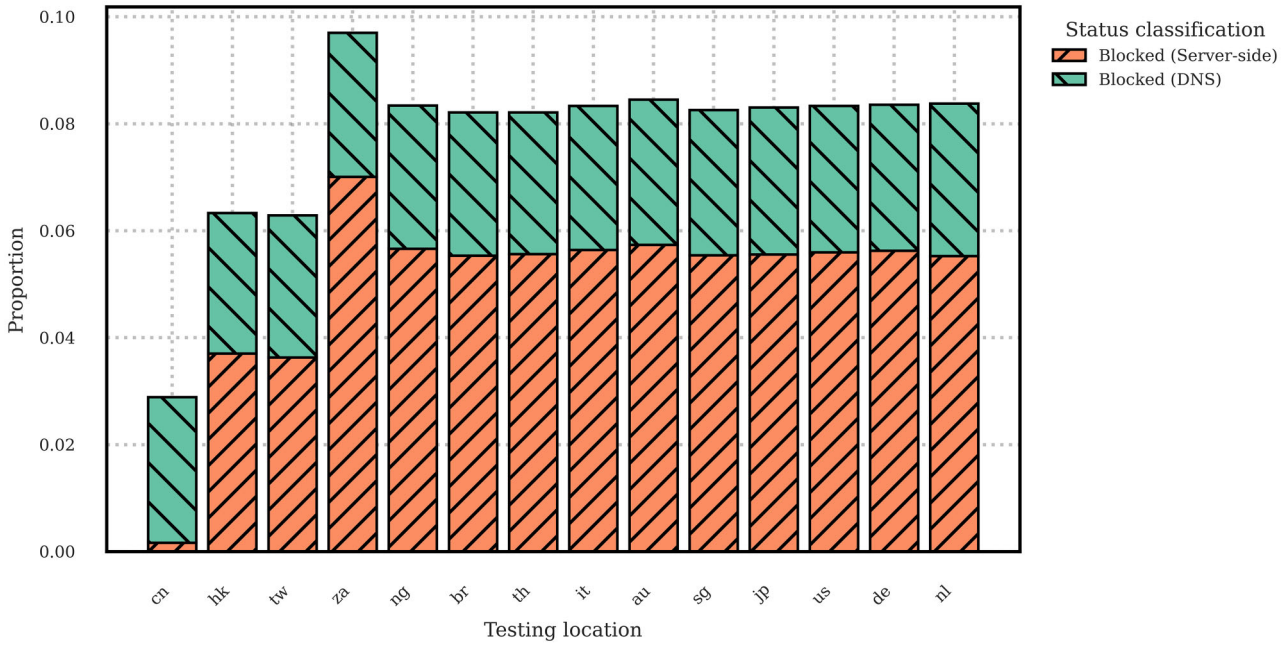

Figure 5 Server-side and DNS blocking by proxy location. DNS blocking also appears for the proxy in Shanghai, as the testing tools still use a non-China-based DNS server. The very small percentage of server-side blocking in Shanghai indicates potential testing errors, such as proxies being detected as suspicious behaviour.

Table 5 Taxonomy of access restrictions under the Reverse Great Firewall.

	Category	Position in request path	Technical layer	Opaqueness	Share of websites	Explanation
1	DNS-Based Blocking	Earliest point of failure	DNS infrastructure	Medium	2–3%	Domains resolve only via China-based DNS; foreign resolvers fail.
2	CDN/WAF Geo-Filtering	Intercepts after DNS resolution	CDN edge/firewall	High	<1%	CDN routes foreign traffic to nodes that deny service or trigger WAF rules.
3	Cross-Border Time-Outs	Routing stage inside China	Network transport/routing	High	38–40%	Requests fail in deep-China routing; reflects bottlenecks rather than explicit blocking.
4	Server-Side Geo-Blocking (403)	Final point of failure	Application/server	Low	5–7%	Explicit refusal of foreign IPs; clearly intentional and administratively controlled.

service providers only offer servers located outside of China. Still, there are VPNs available that were developed to help Chinese nationals access intellectual property-restricted content like movies and series when residing abroad, although their security and reliability are more uncertain.

In this context, the current levels of fragmentation are both a curse and a blessing. It is a curse because it means that researchers will need the skill and flexibility to work around moving targets. Instead of being presented with one challenge that has one solution, they may need to develop dozens of solutions for an even more diverse range of challenges. Still, it may also be a blessing by leaving some sources entirely unaffected, as is the case at the time of writing. Simultaneously, geo-blocking may not just harm research that the Chinese authorities deem to be undesired, it will also harm people-to-people exchanges and complicate foreign businesses doing business with China. At the same time, any informed (policy) response must acknowledge that authorities in the USA also conduct geo-blocking against China, as noted in the introduction.

There remain limitations to what this study can conclusively establish about the Reverse Great Firewall. Specifically, the absence of longitudinal datasets means that it is difficult to draw conclusions about the evolution of geo-blocking over-time. This article preliminary investigation using the Wayback Machine of websites that are known to conduct geo-blocking suggests that the prac-

tice is recent. Earliest indications of geo-blocking only appear in the first years of the 2020s. Still, without any visible policy discussions in China, there must be a certain degree of caution especially when speculating about motivations and future trajectories. Thus, this article's findings should be seen as explorations to uncover these logics through data, but not as conclusive evidence. Future research may develop different approaches to study government geo-blocking and provide further insights. Further research may also apply this concept to understand geo-blocking practices in different regions, like in Russia and even the USA.

Although geo-blocking is primarily visible on government websites, this does not mean that the Reverse Great Firewall does not expand beyond government sources. As noted, the emergence of geo-blocking coincides with a variety of access restrictions on global access to online third-party services from China. Although these are not new developments, discussions of these remain relatively ad-hoc. Further empirical and conceptual work might help grasp the full range of implications for global discussions of cybersecurity and the internet more broadly.

Finally, there may still be positive news ahead for global information availability. In July 2024, authorities announced plans for six new internet gateways, to be located in the provinces of Guangxi, Shandong, Yunnan, and Hainan [62]. While it remains uncertain when these will be completed and whether they will have the capacity to significantly improve access, they remain highly welcome steps in principle to resolve internet bottlenecks and improve access to resources on the Chinese web.

Acknowledgements

The author is grateful to Rogier Creemers for his feedback on earlier versions of this manuscript and to Xin Tong for helping conduct background research, as well as to the Bright Initiative by Bright Data for providing the proxies for used for testing.

Author contributions

Vincent Brussee (Conceptualization [lead], Data curation [lead], Formal Analysis [lead], Funding acquisition [lead], Investigation [lead], Methodology [lead], Project administration [lead], Resources [lead], Software [lead], Supervision [lead], Validation [lead], Visualization [lead], Writing – original draft [lead], Writing – review & editing [lead])

Supplementary material

Supplementary material is available at *Journal of Cybersecurity* online.

Conflicts of interest

None declared.

Funding

This work was supported by the Netherlands Organization for Scientific Research (NWO) [grant number 406.22.CTW.013].

References

1. Deibert R, Rohozinski R. Beyond Denial: introducing Next-Generation Information Access Controls. In: R Deibert, J Palfrey, R Rohozinski *et al.* (eds.). *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge, Massachusetts: The MIT Press, 2010. https://doi.org/10.7551/mitpress/8551.001.0001
2. Hoang NP, Niaki AA, Dalek J *et al.* How Great is the Great Firewall? Measuring China's DNS Censorship. *Proc 30th USENIX Secur Symp* 2021.
3. Brussee V, Von Carnap K. *The Increasing Challenge of Obtaining Information from Xi's China*. Berlin: MERICS, 2024.
4. Ramesh R, Raman RS, Ensafi R. *US Government and Military Websites Are Geoblocked from Hong Kong and China*. Ann Harbor, MI: Censored Planet at University of Michigan, 2020.
5. Moss S. Russia seems to geofence government sites after DDoS attacks, partially blocks Facebook and Twitter. https://www.datacenterdynamics.com/en/news/russia-seems-to-geofence-government-sites-after-ddos-attacks-partially-blocks-facebook/. Published 2022, (22 January 2025, date last accessed).
6. Trimble M. *The EU Geo-Blocking Regulation*. Cheltenham: Edward Elgar, 2024, https://doi.org/10.4337/9781803923871
7. McDonald A, Bernhard M, Valenta L *et al.* 403 Forbidden: a Global View of Geoblocking. *Proc ACM SIGCOMM Internet Meas Conf*. 2018. https://doi.org/10.1145/3278532.3278552
8. Griffiths J. *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet*. London: Zed Books, 2021, https://doi.org/10.5040/9781350257948
9. Beech H, Mozur P. *A Digital Firewall in Myanmar, Built With Guns and Wire Cutters*. New York: The New York Times, 2021, Published February 23, https://www.nytimes.com/2021/02/23/world/asia/myanmar-coup-firewall-internet-china.html.
10. Shambaugh D. The evolution of American contemporary China studies: coming Full Circle? *J Contemp China* 2024;**33**:314–331.
11. Brussee V. Mitigating missingness in analysing Chinese policy and implications for the fragility of our knowledge base. *China Quarter* 2025;**261**:234–48. https://doi.org/10.1017/S0305741024000948
12. Tiffert GD. Peering down the memory hole: censorship, digitization, and the fragility of our knowledge base. *Am Hist Rev* 2019;**124**:550–68. https://doi.org/10.1093/ahr/rhz286
13. Afroz S, Tschantz MC, Sajid S *et al.* Exploring server-side blocking of regions. 2018.
14. Australian House Standing Committee on Infrastructure and Communications. At what cost? IT pricing and the Australia tax. 2013.
15. Satariano AUS. *News Outlets Block European Readers Over New Privacy Rules*. New York: The New York Times. 2018, Published May 25, https://web.archive.org/web/20180525124657/https://www.nytimes.com/2018/05/25/business/media/europe-privacy-gdpr-us.html.
16. Maynier E. Analyzing US Media Blocking of EU Visitors. 2021.
17. Trimble M. The role of geoblocking in the Internet legal landscape. *12th International Conference on Internet, Law and Politics: Building a European Digital Space*. Barcelona, 2016.
18. Synodinou TE. Geoblocking in EU Copyright Law: challenges and Perspectives. *GRUR Int* 2020;**69**:136–50. https://doi.org/10.1093/grurint/ikaa001

19. Podobnik K. Geo-blocking Regulation: antitrust or Consumer Protection? *BYIO* 2020;**18**:194–207. https://doi.org/10.1163/22115897_01801_011
20. Yu PK. A Hater's Guide to Geoblocking. *BU J Sci Tech L* 2019;**25**:503–29.
21. Zhu P, Man K, Qian Z *et al.* Characterizing Transnational Internet Performance and the Great Bottleneck of China. *Proc ACM Meas Anal Comput Syst* 2020;**4**:1–23. https://doi.org/10.1145/3379479
22. Schiliro F. Towards a Contemporary Definition of Cybersecurity. 2023.
23. Lewallen J. Emerging technologies and problem definition uncertainty: the case of cybersecurity. *Regul Govern* 2021;**15**:1035–52. https://doi.org/10.1111/rego.12341
24. Hansen L, Nissenbaum H. Digital Disaster, Cyber Security, and the Copenhagen School. *Int Stud Q* 2009;**53**:1155–75. https://doi.org/10.1111/j.1468-2478.2009.00572.x
25. Creemers R. The Chinese conception of cybersecurity: a conceptual, institutional, and regulatory genealogy. *J Contemp China* 2024;**33**:173–88. https://doi.org/10.1080/10670564.2023.2196508
26. Creemers R. Cybersecurity Law and Regulation in China: securing the smart state. *China Law Soc Rev* 2021;**6**:111–45. https://doi.org/10.1163/25427466-06020001
27. General Office of the Anhui Provincial People's Government. Cable Regarding the Inspection Results of Provincial Government Websites and Official New Media Platforms during the Third Quarter of 2022. 2022. https://www.ah.gov.cn/public/1681/554172191.html (20 November 2025, date last accessed).
28. General Office of the Fujian Provincial People's Government. Cable Regarding the Inspection Results of Provincial Government Websites and Official New Media Platforms during 2022. 2023. https://www.fujian.gov.cn/zwgk/zxwj/szfbgtwj/202303/t20230302_6124135.htm (20 November 2025, date last accessed).
29. General Office of the Fujian Provincial People's Government. Cable Regarding the Inspection Results of Provincial Government Websites and Official New Media Platforms during 2023. 2024. https://www.fujian.gov.cn/zwgk/zxwj/szfbgtwj/202403/t20240306_6410314.htm (20 November 2025, date last accessed).
30. National Administration of State Secrets Protection. Confidentiality, leakage and prevention in the context of big data. 2018. https://web.archive.org/web/20250325103612/https://www.gjbmj.gov.cn/n1/2018/1218/c411145-30474549.html/ (27 March 2025, date last accessed).
31. National Administration of State Secrets Protection. How do to a good job at the work for protecting state secrets in the era of big data. 2019. https://web.archive.org/web/20250327133816/https://www.gjbmj.gov.cn/n1/2019/1030/c411145-31428595.html (27 March 2025, date last accessed).
32. South China Morning Post. New work rules for China's State Council put the party firmly in charge. 2023. Published March 28, https://archive.ph/3aALE (26 September 2023, date last accessed).
33. United Nations Human Rights Office of the High Commissioner. *OHCHR Assessment of Human Rights Concerns in the Xinjiang Uyghur Autonomous Region, People's Republic of China*. Geneva: United Nations, 2022.
34. General Office of the State Council. 2022 Work Priorities for Open Government Work. 2022. https://web.archive.org/web/20230630090021/https://www.gov.cn/gongbao/content/2022/content_5688781.htm (30 June 2023, date last accessed).
35. Cyberspace Administration of China, Office of the Central Organization Department, Ministry of Industry and Information Technology. Provisions on the Security Management of Online Government Affairs Applications. 2024. https://web.archive.org/web/20240613002208/https://www.gov.cn/lianbo/bumen/202405/content_6952956.htm (13 July 2024, date last accessed).
36. Supreme People's Court. Interpretation of Several Issues Concerning the Specific Application of the Law in Case Trials Involving Stealing, spying, buying, and providing state secrets and intelligence for foreign countries. 2001. https://web.archive.org/web/20210816024523/http://www.gd.gov.cn/zwgk/wjk/zcfgk/content/post_2950463.html (16 August 2021, date last accessed).
37. Xinhua. National Cyber Emergency Centre: cloud Platform Security Risks are Prominent. 2019. https://www.cac.gov.cn/2019-07/18/c_1124769181.htm (25 November 2025, date last accessed).
38. University World News. Database shuts out foreign researchers in 'security' move. 2023.Published March 30, https://web.archive.org/web/20230330102813/https://www.universityworldnews.com/post.php?story=20230329194656185 (30 March 2023, date last accessed).
39. Horsley JP, Creemers R. The Cyberspace Administration of China: a Portrait. In: R Creemers, S Papagianneas, A Knight (eds.). *The Emergence of China's Smart State*. Lanham: Rowman & Littlefield, 2023, 9–34. https://doi.org/10.5040/9798881817602
40. Liebman B, Stern R, Wu X *et al.* Rolling Back Transparency in China's Courts. *Columbia Law Rev* 2023;**123**:2407–82.
41. Liu J. China's data localization. *Chinese Journal of Communication* 2020;**13**:84–103. https://doi.org/10.1080/17544750.2019.1649289
42. Creemers R. China's emerging data protection framework. *J Cybersecurity* 2022;**8**:1–12. https://doi.org/10.1093/cybsec/tyac011
43. Lee J-A, Liu C-Y. Real-name registration rules and the fading digital anonymity in China. *Wash Int Law J* 2016;**25**:1–34.
44. Central Leading Group for Cybersecurity and Informatization. Circular on Strengthening the Security Management of Websites of Party Organs. 2014. https://web.archive.org/web/20241114131712/https://www.cac.gov.cn/2014-05/10/c_1112142115.htm/ (14 Novemeber 2024, date last accessed).
45. Chen L, Liu Z, Tang Y. Judicial Transparency as Judicial Centralization: mass Publicity of Court Decisions in China. *Journal of Contemporary China* 2022;**31**:726–39. https://doi.org/10.1080/10670564.2021.2010871
46. Horsley JP. Toward a More Open China?In: A Florini (ed.). *The Right to Know: Transparency for an Open World*. New York: Columbia University Press, 2007:54–91. https://doi.org/10.7312/flor14158
47. Stromseth J, Malesky E, Gueorguiev D. *China's Governance Puzzle: Enabling Transparency and Participation in a Single-*

Party State. Cambridge: Cambridge University Press, 2017, https://doi.org/10.1017/9781316388501
48. Xi J. Important speech delivered at the Second Plenum of the 18th Central Commission for Disciplinary Inspection. 2013. https://web.archive.org/web/20230526090751/http://jhsjk.people.cn/article/20289660 (26 May 2023, date last accessed).
49. General Office of the State Council. Guidelines for the Development of Government Websites. 2017. https://web.archive.org/web/20240718053652/https://www.gov.cn/zhengce/content/2017-06/08/content_5200760.htm (18 July 2024, date last accessed).
50. China Centre for the Operation of Government Websites. Reference Plan for the Design of Government Information Disclosure Sections. 2019. https://web.archive.org/web/20250901081329/https://www.gov.cn/zhengce/content/2019-12/03/5457588/files/f78997ecef234e928a16bd438552846e.pdf (1 September 2025, date last accessed).
51. Heilmann S, Perry EJ. Mao's invisible hand : the political foundations of adaptive governance in China. *Mao's Invisible Hand*. Cambridge, Massachusetts: Harvard University Asia Center, 2011,
52. General Office of the State Council. Indicators for the Inspection of Government Websites and Media on Government Affairs. 2019. https://web.archive.org/web/20250902044857/https://www.gov.cn/zhengce/content/2019-04/18/content_5384134.htm (2 September 2025, date last accessed).
53. General Office of the Wuxi Municipal People's Government. Cable Regarding the Inspection Results of Government Websites and Official New Media Platforms during the Third Quarter of 2024. 2024. https://www.wuxi.gov.cn/doc/2024/08/20/4376895.shtml./ (14 November 2025, date last accessed).
54. General Office of the Zhongshan Municipal People's Government. Cable Regarding the Inspection Results of Municipal Government Websites and Official New Media Platforms during the Fourth Quarter of 2023. 2024. http://www.zs.gov.cn/zwgk/gzdt/tzgg/content/post_2442175.html/ (14 November 2025, date last accessed).
55. Deng Y, O'Brien K, Chen J. Enthusiastic Policy Implementation and its Aftermath: the Sudden Expansion and Contraction of China's Microfinance for Women Programme. *China Quarter* 2018;**234**:506–26. https://doi.org/10.1017/S0305741018000425
56. Shao J. Implementation gap of China's environmental policies: logic behind the over-implementation of the coal to gas transition. *J Environ Plann Policy Manage* 2023;**25**:611–24. https://doi.org/10.1080/1523908X.2023.2232313
57. Wu M, Zohaib A, Durumeric Z *et al. A Wall Behind A Wall: Emerging Regional Censorship in China*. San Fransisco: IEEE Symposium on Security and Privacy, 2025.
58. Database of Basic Information on National Government Websites. 2025.
59. General Office of the State Council. 2020. Cable Regarding the Inspection Results of Government Websites and Official New Media Platforms during 2020. https://web.archive.org/web/20250902044854/https://www.gov.cn/zhengce/content/2020-12/16/content_5569781.htm (2 September 2025, date last accessed).
60. Wright J. Regional variation in Chinese internet filtering. *Inform Commun Soc* 2014;**17**:121–41. https://doi.org/10.1080/1369118X.2013.853818
61. Ensafi R, Winter P, Mueen A *et al.* Analyzing the Great Firewall of China Over Space and Time. *Proc Priv Enhancing Technol* 2015;**2015**:61–76. https://doi.org/10.1515/popets-2015-0005
62. CCTV. A first after 30 years: china Establishes 6 New International Telecommunication Gateways. 2024. Published July 10, https://web.archive.org/web/20240806021649/https://news.cctv.com/2024/07/10/ARTIPGV0NjIZoAQu7ptQAz8T240710.shtml (1 June 2025, datelast accessed).

Received: 5 April 2025. **Revised:** 26 November 2025. **Accepted:** 6 January 2026