Online People - Watching: Censorship, Surveillance, and The National Internet Gateway in Cambodia

Key Takeaways

► The implementation of the National Internet Gateway (NIG) can enable large-scale censorship and surveillance on online communications in Cambodia.

► Social media platforms are unlikely to be blocked, but the pressure to comply with the government may become more intense.

► By allowing the government to have control over network traffic, the NIG may enable the state to develop more sophisticated censorship and surveillance methods, especially if it follows the Great Firewall of China as a model.

► Self-censorship of websites operating in Cambodia is likely to become more intense.

► Communities at risk in Cambodia, such as civil society organizations, the independent media, and activists, will need to prepare and adapt to the possibility of a worsening situation.

► There is a need to closely monitor the situation to track how censorship and surveillance may intensify after the NIG is implemented.

► Using privacy-enhancing technology, such as well-configured VPNs and end-to-end encryption applications, can help improve online privacy and digital security.
On February 16, 2021, the Royal Government of Cambodia issued Sub-Decree No.23 on the Establishment of National Internet Gateway, which consists of 11 chapters and 20 articles. According to Article 1 of the law, the National Internet Gateway (NIG) is established for the purpose of “facilitating and managing Internet connections in order to strengthen the effectiveness and efficiency of the national revenue collection, protection of national security, and preservation of social order, culture, and national tradition.” Cambodia’s adoption of the NIG has drawn concerns given the country’s human rights records; it has been perceived as a similar practice to the Chinese government’s censorship and surveillance effort, which is widely known as the Great Firewall of China and considered the most sophisticated internet censorship system in the world.

The adoption of the NIG Sub-Decree may facilitate the Cambodian government’s efforts to increase its control over the digital space and online communications in the country. According to the law, the government would exercise its power through “NIG operators,” although the term has yet to be defined. Covering both domestic and cross-border data traffic, the law stipulates that all data traffic will pass through internet exchanges operated by the NIG operators.

The government requires those interested in the position of NIG operators to apply and obtain a license from the Telecommunication Regulator of Cambodia (TRC) within 12 months after the adoption of the Sub-decree. The adoption of the Sub-decree cancels all approvals and permits that were secured prior to the adoption of the law. NIG Operators are required to monitor network traffic and submit traffic data reports to the Ministry of Post and Telecommunications (MPTC) and TRC on a regular basis. The law further permits the Cambodian authorities, through the NIG operators, to block or disconnect any network connection that is considered as a threat to “national revenue, safety, social order, dignity, culture, traditions, and customs”.

The Great Firewall is a complex system of internet censorship and surveillance in China that was created in 1996 as part of the Golden Shield Project, or National Public Security Work Information Project of the Chinese Government. It is considered the most extensive and most advanced regime in the world. The intention of the Great Firewall is to filter and censor politically sensitive information, dubbed as “wrong information”, from outside of China, in order to curtail the influence of this information on Chinese society. The system consists of tactics and legislation that are combined to achieve this goal; it is considered an immensely sophisticated system and therefore is difficult to describe its extent and reach.

---

Inside China, foreign websites such as Facebook, Google, and Twitter, are blocked. Other platforms of these major tech companies, such as YouTube, Instagram, and WhatsApp, are also blocked. While TikTok has its own Chinese version known as Douyin, this app is not quite the same as TikTok, as some content that can be found on TikTok is not available on Douyin and vice versa. Foreign news sites, including The New York Times, The Guardian, and The Washington Post, are also blocked in the country. Chinese Netizens cannot access Wikipedia. It has been estimated that as many as 10,000 websites are blocked in China, with the list of blocked websites and applications expected to increase as the Great Firewall continues to evolve.

To be able to legally operate in China, websites are required to register for a license, known as the Internet Content Provider (ICP) license; without ICP numbers, websites can be blocked by the Internet Service Providers (ISPs). To access blocked sites, Chinese citizens are required to use network relays such as Virtual Private Network (VPN), Tor, and proxy. However, in 2017, the Chinese government issued a notice that all VPNs in China would require authorization from telecoms regulators. The method has been implemented to support the government in its increased surveillance on Chinese netizens. In 2020, the Great Firewall began to block new developments in encrypted HTTPS that hide domain names, such as TLS 1.3 and ESNI (Encrypted Server Name Indication); as a result, site operators and users were forced to remain on older versions. When new protocols encrypt the domain name, authorities are unable to discern which websites users are connecting to, resulting in less information for the Chinese government to inspect. The Chinese government has also employed tactics such as Domain Name System (DNS) poisoning, deep packet inspection, and keyword and URL filtering to censor content for political purposes.

Apart from censorship and surveillance, authorities in China have also used content manipulation to spread pro-government propaganda to shape the narratives in order for the government to maintain political power. The Chinese government allegedly uses fake social media accounts and posts to influence online dialogue, and steer discussion away from politically sensitive topics on a regular basis. The government is alleged to

---


fabricate at least one in every six online comments on social media. Paid commentators have also been instructed to bombard social media with pro-government messages⁶. These paid commentators are sometimes called the “50-cent party,” as they are said to be paid fifty Chinese cents for each comment made in favor of the Chinese government⁷.

Chinese tech giants such as Tencent, Baidu, Alibaba, and ByteDance have also been alleged to assist the government on surveillance and censorship with their products and services. The blocking of Western social media platforms has allowed Chinese homegrown platforms to thrive. Tech platforms widely used in China, such as Sina Weibo, Baidu, and WeChat, are required to follow the government’s rules to monitor content, prohibit discussions of political sensitive topics, and log users’ behavior when using the platforms. These tech giant companies are required to report regularly to the Chinese government, and the data acquired from these reports have been allegedly used by the Chinese government to conduct mass surveillance in China⁸.

Legislations have also been passed to support the government and its technological system. In fact, the use of legislation in China has become a model for many governments in Southeast Asia, including Cambodia. A series of laws support the lawfulness of the Great Firewall, and these laws have also been amended over time as the Great Firewall is continually upgraded. The most important legislation is the Cybersecurity Law, which came into effect in 2017 and authorizes the government to have more control over online information as well as people’s personal data⁹. Apart from requiring data to be stored within China, it requires network operators to cooperate with the Chinese authorities to allow full access to data and unspecified “technical support” when requested. In 2018, additional provisions, known as the Regulations on Internet Security Supervision and Inspection by Public Security Organs, were passed, which allow the government to inspect computer networks onsite and remotely¹⁰.

---

China has also exported its surveillance and censorship technology, and has provided its know-how to other countries through efforts that have been widely covered by the media. In 2013, the Belt and Road Initiative (BRI) was launched by the Chinese government to provide support on infrastructure to other countries\(^1\). After the BRI was launched, the Chinese government later introduced the world to the ‘Digital Silk Road’ initiative in 2015\(^2\). As the project aims to boost development of the digital service sector and accelerate technological progress, it allows Chinese-owned technology companies to promote their products and services to the global market. This move includes the members of the Association of Southeast Asian Nations (ASEAN)\(^3\), and in November 2020, China announced a plan to deepen cooperation and promote the Digital Silk Road with ASEAN.

**WHAT CAN POSSIBLY HAPPEN AFTER THE NIG IS IMPLEMENTED?**

The implementation of the NIG marks an important step for Cambodia to tighten its censorship and surveillance efforts. As a country known for having a close relationship with China\(^4\) and with its own poor records on human rights, there is a potential that the government will learn from China’s approach on internet control and adapt it to the Cambodian context. However, the scale of censorship and surveillance of the Great Firewall of China would require a longer time for Cambodia to achieve in comparison, while not all methods used by China can be applied to the Cambodian context. The Cambodian government would be required to initiate a few test runs to see which approaches would work best. As the NIG is being implemented, censorship and surveillance methods are likely to happen stepwise than all at once. As the internet and circumvention techniques continue to evolve, these methods of censorship and surveillance are likely to adapt accordingly as government authorities seek to maintain the online space under their control.

---


1. Pressure on Social Media Platforms

The implementation of the NIG reveals the government’s efforts to establish greater control over the digital space and online communications; this leaves many to wonder what would happen to social media platforms due to the critical role they play in people’s lives. Unlike China, Western social media platforms are dominant in Cambodia, making the blocking of Facebook, Twitter, and Google, as in the case of China, more difficult to achieve in Cambodia. The government itself also uses social media, particularly Facebook, as a channel to communicate with the public. Hun Sen, Prime Minister of Cambodia himself uses Facebook on a regular basis. Although he has been previously accused of buying his social media engagement figures, his page has millions of followers. The country’s mainstream media, which is usually linked to the government, also use social media platforms, particularly Facebook, as one of their main platforms to engage with their audiences.

Social media platforms can be used to criticize the government; however, the government cannot selectively block pages, groups, and accounts on these platforms even after the NIG is implemented. The NIG enables the government authorities to intercept the traffic only. In order to block pages, groups, or accounts on social media platforms or applications, the government would still require cooperation from social media companies. Therefore, it is more likely that the government would put pressure on the companies to shut down pages, groups, accounts, as well as take down or label posts that are considered to be critical of the government. The government could use a number of laws and legislations to force social media companies to comply.

Another issue of concern is the government’s link to pro-government propaganda campaign on social media. According to several reports, evidence reveals that state-sponsored cyber troops have been used to spread propaganda to attack political opposition and dissidents. In 2020, Luon Sovath, an activist Buddhist monk who has been critical of the government, was forced to flee the country after information to discredit him was made and went viral on social media; this spread of incident was reported to be

---


a part of a smear campaign created by the government. The situation in Cambodia is similar to that in China, where the government attempts to eliminate information that is considered to be critical of the regime, while creating and promoting pro-regime narratives that may be false, fake, or misleading. While the government has been able to manipulate and gain political advantages from the popularity of social media platforms in Cambodia, this popularity also makes it difficult for the government to block social media platforms completely.

2. More Sophisticated Censorship Methods

In general, the blocking of websites and applications will be easier to achieve when the NIG is implemented. In fact, the NIG can enable a larger scale of blocking websites and applications as the government controls the data traffic. Previously, websites have been shut down in Cambodia for political reasons. In 2018, a number of independent media websites, such as Voice of America, Radio Free Asia (RFA), Voice of Democracy, and The Phnom Penh Post, were blocked for 48 hours before the 2018 General Election. Monoroom.info, an online independent Khmer language news website, was blocked in Cambodia after its coverage on the COVID-19 pandemic.

The government’s control over the network traffic also enables the censorship methods to become more sophisticated, especially through the lessons learned from China’s Great Firewall. The Great Firewall uses a wide array of techniques, including IP blocking, DNS poisoning, deep packet inspection, URL filtering, and active probing. While these methods have also been employed outside of China, China is distinct in using these techniques altogether at a large and sophisticated scale. The Great Firewall also continues to evolve over time to overcome circumvention techniques and cybersecurity methods that would otherwise reduce the power of the Great Firewall.

Understanding these different methods is beneficial, especially for human rights activists, NGO workers, independent media, political opposition, and others who are considered as vulnerable groups and often targeted by the government.

---

A. IP Blocking

All communications over the Internet use the Internet Protocol (IP). The IP refers to the rules that direct how packets of data travel across networks and arrive at the correct destination, and each packet carries a source and destination address. Every device that is connected to the Internet is called a host and has its own IP address. The government can censor particular websites and services by matching the destination address and IP address of the websites and services that it wants to block. This method is called IP blocking.

In China, the Chinese government is able to block websites and services at a large scale by using null routing, which is a highly efficient technique of IP blocking. However, while the government is able to block the websites and services at a large scale through this method, a drawback is that the blockings may be excessive such that some websites that are not targeted may also be blocked. This blocking occurs because the non-targeted websites may share the same IP address with the targeted website if they share a hosting. Websites that share a hosting may not have related or similar content to each other. They may be completely different from each other; for instance, one website may be that of a non-profit organization, while the other can be an e-commerce website of a completely unrelated company.

B. DNS Poisoning

The Domain Name System (DNS) functions as a phone book of domain names. It is a database where internet domain names like “digitalreach.asia” can be searched and translated into IP addresses. Internet users can view the website on their browsers after they input the domain name (i.e. the name of the website). The DNS then translates the domain name to the IP address, after which the website is shown on the user’s browser. DNS poisoning occurs when a malicious actor intervenes in that process and intentionally provides the wrong information. The method can be carried out by man-in-the-middle attack or man-on-the-side attack\(^\text{20}\). The malicious actor would trick the user, divert traffic, and feed fake websites to the browser instead. As a result, the browser would display a fake website or a generic error.

\(^{20}\)A man-in-the-middle attack is when an attacker is secretly in a position between two parties and has a complete control over a communication. A man-on-the-side attack is when an attacker has a regular access to a communication between two parties but does not have a complete control.
Facebook, Google, and Twitter have been censored in China through the use of this technique. When visiting websites, internet users would receive a timeout message or an error message which stated these websites were unavailable; this “error message” occurs as most of the rerouted IP addresses do not exist. However, as more internet users have learned how to thwart the DNS poisoning by using circumvention tools, the Great Firewall has also changed the way it conducts DNS poisoning by injecting random routable IP addresses instead\textsuperscript{21}. The tactic has made circumvention more challenging due to the fact the IPs are random, with no discernable patterns.

C. Deep Packet Inspection (DPI)

Deep Packet Inspection (DPI) is an advanced method to examine and manage data packets\textsuperscript{22}. It is a method of first screening the content before the censorship method is used. DPI is able to evaluate the actual content of the packet; in comparison, a conventional packet filtering can only examine the headers of the packet, which usually contains information that tells where the data is from and where it is going to. As an analogy, a conventional packet filtering is similar to when those who are in control of the delivery can read the addresses printed on the outside of an


\textsuperscript{22} A data packet is a unit of data that is made into a package and travels along a given network path. Data packets are used in Internet Protocol (IP)-based systems for communication over the Web.
envelope. In contrast, deep packet inspection is akin to the delivery person opening an envelope and reading its content. Those who are in control of the network are able to make real-time decisions about whether these data packets should be allowed to pass through the checkpoint.

DPI is time-consuming and can slow down legitimate traffic. To manage this, China's Great Firewall first allows the traffic to pass while simultaneously, a copy of the traffic is sent to a separate system for deep analysis. Once the system detects that the connection is undesirable, it will interrupt and terminate any established connections. This process is similar to when a person makes a phone call and is able to connect to the person or place they want to reach, while at the same time, a separate system monitors all phone calls and detects this particular call, and then terminates the call. It then stores a record of this terminated call, so it can stop this particular call from being made again.

**D. Analyzing and Filtering URLs**

URL filtering is another form of screening method that is used before the censorship occurs. In general, URL filtering restricts the sites that internet users can access by blocking certain URLs from loading. URL filtering can be used for positive aims, such as cybersecurity through mitigating malware and phishing attacks by blocking malicious webpages. URL filtering typically involves the use of a list of prohibited websites, otherwise known as a “blocklist”. When a user attempts to access a website that is on the blocklist, the request is blocked and the website does not load on the user’s device.
In China, the method of URL filtering has been used for political purposes, and have targeted websites that have the potential to contain politically sensitive information. The Chinese government also has a long list of blacklisted keywords, including the words “democracy”, “Radio Free Asia”, “demonstration”, and “Chinese democracy movement”\(^{23}\). The Great Firewall can scan URLs and block connections if they contain these keywords.

If the blacklisted keywords are included in the domain name, it is easier to block the website than in cases where the keyword is featured in the website’s content. For example, if the word “democracy” is blacklisted in Cambodia, a domain name such as “democracyforcambodia.org” can easily be blocked compared to a website whose domain name does not contain any blacklisted keyword, includes the word in the site’s content. This method of filtering is more challenging when it is performed on a site that uses HTTPS and contains blacklisted keywords in the content; this challenge is due to the encryption in the HTTPS. URL filtering works best on sites that use HTTP as there is no encryption. With the new protocols of the HTTPS, such as TLS 1.3 and ESNI, in place, the domain name of a site is also hidden, which makes the URL filtering unable to do a match on the domain name. Because the encryption prevents the screening and hinders censorship, China has chosen to block the HTTPS that use the new protocols entirely.

**E. Active Probing to Detect Network Proxy**

Internet users usually circumvent censorship by using proxies or relays, such as VPN or Tor, to disguise the traffic of these relays. The censorship and circumvention can be a cat-and-mouse game where new relays are set up to circumvent the censorship, and authorities try to identify them to block them. To address this circumvention technique, the Great Firewall uses active probing as one of its innovations.

In active probing, deep packet inspection (DPI) is first used to identify potential circumvention traffic by analyzing traffic patterns. In the next step, scanners probe the suspected IP address by posing as a user. If the server responds to the request of the scanners, the IP address would be blacklisted by the authorities.

\(^{23}\) University of New Mexico and Citizen Lab. *China Chats*, china-chats.net/keywords.
In China, active probing was used to identify and block usage of the Tor protocol. Tor is a known software that can enable anonymous communication, therefore concealing the location and usage of an internet user from those who are conducting network surveillance or traffic analysis. As a result, Tor has long been a target of the Chinese authorities. As Tor develops its techniques, the Great Firewall has also evolved.

3. Enabling Mass Surveillance

By implementing the NIG, the Cambodian government would have complete control over the network traffic, which will enable mass surveillance over online communications in the country. Surveillance over people's internet behaviors, including political opposition members, independent media, and activists, will also become more effective through the combination of censorship and surveillance technologies. Moreover, according to Article 6 of the Sub-Decree, NIG operators have an obligation of reporting to the Cambodian government on a regular basis. Information, such as the websites and applications that internet users visit, the content that they viewed on the sites, and the duration they stayed on the websites, can be revealed to the NIG operators from the log data.

---

4. More Intense Self-censorship

The NIG has a potential to exacerbate an already hostile environment towards online information that is deemed politically sensitive. The implementation of the NIG is likely to lead to more self-censorship of websites that operate in Cambodia. Article 6 of the Sub-decree prescribes that the NIG operators are required to collaborate with the Cambodian authorities to take action in “blocking and disconnecting all network connections that adversely affect national revenue, safety, social order, dignity, culture, traditions, and customs.” The broad scope of the legislation means that NIG operations are able to block any content that the government interprets and considers as falling under the prescribed categories.

Article 16 of the Sub-decree also prescribes that NIG operators who fail to comply with the law can have their licenses restricted, suspended, and revoked. Their accounts can be frozen by the authorities, and they can be fined for not complying with the law. The Sub-decree can enable the situation of self-censorship to be more intense among websites operators in Cambodia, particularly domestic ones, in their efforts to avoid being censored by the NIG operators.

CONCLUSION AND RECOMMENDATIONS

The move towards implementing the NIG in Cambodia runs counter to the international human rights principles, namely that internet should be open for all, and users should not be prevented by their governments from openly using the internet or having their privacy being threatened while being online. According to the non-binding resolution adopted by the United Nations Human Rights Council on July 17, 2018, it states that “privacy online is important for the realization of the right to free of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association.” In the same Resolution, the United Nations also recognizes that “for the Internet to remain global, open and interoperable, it is imperative that States address security concerns in accordance with their international human rights obligations, in particular with regard to freedom of expression, freedom of association and privacy.”

As Cambodia became a party member of the International Covenant on Civil and Political Rights (ICCPR) on May 26, 1992, the government of Cambodia should protect and promote internet freedom instead of creating an environment of fear among netizens in Cambodia.

---

The implementation of the NIG can enable mass censorship and surveillance. Techniques on censorship and surveillance can be done without the implementation of the NIG. However, its implementation allows the censorship and surveillances efforts to be much more effective and coordinated, because the NIG operators will have to meet certain requirements stated in the law in order to be able to maintain their business in Cambodia. However, these sophisticated censorship and surveillance methods will take time to be implemented, especially if Cambodia aims for a system similar to the Great Firewall of China, as it would take time to test run the techniques within the Cambodian context. Mass censorship also comes with a great cost, as the censorship may also inadvertently include those websites and applications that are not targeted by the government.

The NIG will likely contribute to an environment of fear among users. However, there are a number of workarounds and solutions that individual users can use to protect their privacy and circumvent censorship, especially as the NIG cannot break encryption.

**Recommendations to consider in response to the implementation of the NIG are as follows:**

1. Monitoring the situation is a significant step to see how the situation has changed from before and after the NIG is implemented. Censorship on websites and applications can happen without notice. It is important to monitor which websites and applications are blocked, how they are blocked, and which category of websites are blocked. Being able to compile a list of websites that are censored can provide information about which categories of these websites are specifically targeted. Knowing which of these websites and applications are blocked can also assist in identifying the best method of circumvention in response to the type of censorship used. The Open Observatory of Network Interference (OONI) offers OONI Probe, a tool that can be used by local organizations and individuals to effectively monitor internet censorship. It is recommended that civil society organizations partner with OONI to document the situation in the country.

2. Individuals at risk, such as political dissidents and opponents, need to protect themselves by learning how to use privacy protection technology, such as well-configured VPNs, encrypted messaging platforms, and encrypted meeting conference platforms. The NIG will not be able to break the encryption as a result of this privacy protection technology. The use of a VPN will not reveal the user’s internet activities when the user is connected to the VPN, but it will still show the IP address of users. Therefore, Tor can be a good option for those who seek anonymity while connecting to the Internet. It is also better to use an encrypted email provider. However, security over emails is still a matter of concern, as communication may be less secured when an email is sent from an encrypted email provider’s server to an unencrypted server of an email provider.
Civil society organizations that operate in Cambodia face the possibility that their websites will be banned or blocked by the government. Therefore, it is important for civil society organizations to prepare and protect their organization's digital security. It is recommended for organizations at risk to consult with those providing support on digital security and internet freedom, such as equalit.ie, Qurium, or Cloudflare’s Project Galileo. This briefing paper can be used as a reference during the IT consultations and as part of the organization’s preparation. One method for organizations to consider is to host their sites on multiple web servers, while having copies of their websites outside of Cambodia and working with trusted web-hosts who are aware of the situation and can respond when their websites are banned. By having multiple web servers with copies of the website, users may continue to access information in cases when the site is banned. Other options include creating the websites on free website-building sites, such as Wordpress.com27, or using different website-building platforms. In preparation for the worst-case scenario, organizations should also make a plan of where the content of their sites should be moved to, in case Facebook and other social media channels are banned. While the banning of social media is unlikely to happen, it remains a possibility.

Local organizations and individuals who are at risk often lack the necessary resources on capacity and finance; therefore, it is important to provide support on digital security to assist these organizations and individuals. Those who provide support on digital security should also be aware, and adapt their techniques to the changes following the implementation of the NIG and the threats to internet freedom.

Due to sites like Wordpress.com being a popular website hosting platform, the collateral damage is high if the government considers blocking it. It means that every website that is hosted on Wordpress.com, including commercial websites or websites of educational institutions, will not be accessible in Cambodia.

---

**About DigitalReach**

DigitalReach was founded in 2019 with the objective of assessing the impact of technology on human rights in Southeast Asia. The organization's mission is to safeguard digital rights and internet freedoms in the region. Our work revolves around research and monitoring, advocacy, and community building and empowerment.

For further assistance and support, please contact digitalreach@digitalreach.asia