COUNCIL on FOREIGN RELATIONS

The Consequences of Internet Shutdowns in Kazakhstan

Despite high costs, both economically and socially, internet shutdowns will remain a tool for authoritarian leaders. Kazakhstan has led the way in manipulating the internet to stifle dissent.

Baurzhan Rakhmetov and Brandon Valeriano
February 24, 2022

Internet disruptions or shutdowns during periods of mass protest are now a common feature of the cyber security landscape. While many focus on a brewing "cyber war" between Russia and the United States over Ukraine, the reality is that the most frequent form of cyber conflict is exhibited by states seeking to maintain control over digital communications during periods of turmoil. January 2022 in Kazakhstan was no different, with potentially devastating economic and social impacts on society.

In the beginning of January 2022, nationwide anti-government protests began in Kazakhstan. Soon the protests turned to unrest and violence. Military assistance from the Collective Security Treaty Organization (CSTO)–a Russia-led prototype of NATO–resulted in the deployment of Russian troops while the internet was intentionally shut down in the country. For more than five days, except for short breaks of a few hours, people could not access websites, applications, or messenger apps. The week-long, nationwide internet blackout cost the economy more than $400 million.

Establishing the means of internet control is a key state strategy in reaction to a series of protest movements. For Kazakhstan, a post-Soviet country where almost 90 percent of the population has access to the internet, digital disruptions are now common during political unrest. Starting more than a decade ago, the practice of switching off communications during a (perceived) political crisis has become routine. Localized internet shutdowns or disruptions by the government took place amid the street protests in Zhanaozen in December 2011, currency devaluation in February 2014, ethnic conflict in the South Kazakhstan region in February 2015, protests against land reforms in May 2016, a terrorist attack in Aktobe in June 2016, ethnic clashes in the Korday district in February 2020, anti-

government protests in Almaty and Nur-Sultan in February 2021, and a rally in Almaty in April 2021.

The latest elections, the presidential in June 2019 and the parliamentary in January 2021, were both accompanied by the disruption of internet connectivity. To enable digital control over particular regions or even the whole country, the government has acquired command over crucial internet infrastructure. The only internet exchange point (IXP) in Kazakhstan is managed by the State Technical Service, whose single shareholder is the National Security Committee, while the main internet service provider (ISP) Kazakhtelecom is state-owned. According to the 2004 communication law, ISPs must give investigative and counterintelligence agencies access to their communication networks whenever requested.

In addition, legislation has been adopted allowing state agencies to "legitimately" and freely terminate communications, including the internet, across the country. According to the 2012 law on national security, the government is allowed to disrupt communication channels during anti-terrorist operations and containment of riots. This was an early attempt to align the means of political communication with increasingly restrictive national legislations.

In April 2014, amendments to a 2004 communication law were made that enabled the Prosecutor General's Office to shut down the internet without a court decision. Communications can be turned off if, for example, the information distributed on the internet breaks laws on elections, contains calls for riots, terrorist and extremist activity, or appeals to participate in mass public events carried out in violation of the established legal procedures for gatherings. Given that anti-government and opposition protests are routinely prohibited in Kazakhstan, internet access can be systematically restricted at any sign of unrest.

December 2016 amendments to the communication law expanded the number of actors able to terminate communications. Now the National Security Committee can also restrict the internet connectivity and block access to websites without a court order– the National Security Committee only needs to notify the Prosecutor General's Office and the Ministry of Information twenty four hours after the shutdown. As the National Security Committee controls the IXP, termination of the internet in the country has become an easy task for the state, though not without significant economic costs.

Finally, in October 2018, according to the decree of the government, four state agencies–the Prosecutor General's Office, the National Security Committee, the Ministry of Internal Affairs, and the Defense Ministry, are now able to terminate communications in case of a "social emergency", although the government has yet to define what constitutes a social emergency. Kazakh authorities have thus finalized the process of control over political

communication in the country and are able to restrict the spread of information and reduce the potential for collective action by citizens.

Despite the high cost of digital outages, there is no indication the practice of internet shutdowns will be abandoned soon. Fear of popular unrest and change has pushed the Kazakh government to its current position, with few options to change course short of massive political upheaval. With the means of communication under state control, protest and activism can be easily stifled, insulating the government from criticism, and hindering the economic and social growth of Kazakhstan.

Brandon Valeriano is a senior fellow at the Cato Institute and a Distinguished Senior Fellow at the Marine Corps University.