Central Asian Bureau for Analytical Reporting

The Hidden Side of the Internet: How Governments Track Populations

На русском

The authorities of Kazakhstan are using communication technologies to secretly monitor the population. Baurzhan Rakhmetov, Assistant Professor of the University of KazGUU named after M.S. Narikbayeva, a member of the CABAR.asia school of analytics, believes that civil society needs to understand the scale of the problem and learn how to resist digital spyware.

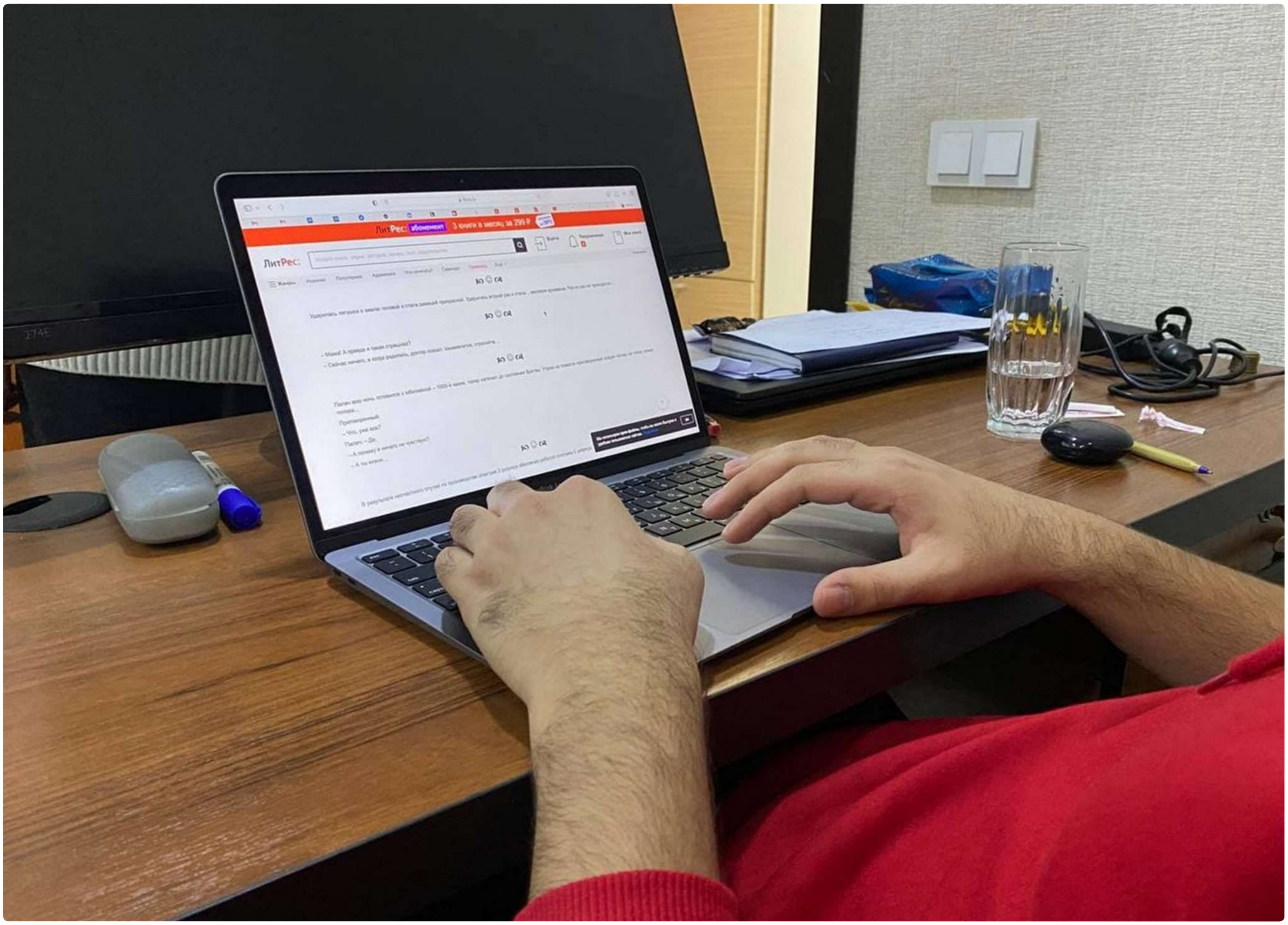


Photo: CABAR.asia

Many countries have learned to use digital technologies to conduct massive, uncontrolled surveillance of the population, which implies the secret collection, monitoring and analysis of metadata (who communicated with whom and when). The undisputed leader among countries sinning hidden online surveillance is the **United States**, but **Kazakhstan** did not stand aside either.

At the same time, the resources of the special services are often used not for the security of the country, but for pinpoint surveillance of citizens, including representatives of the political elite.

Big Brother in the American manner

In June 2013, the world’s leading media announced the disclosure of a secret global online surveillance system conducted by the US National Security Agency (NSA).

It became clear from the investigations of the journalists that the US government has launched a large-scale program of uncontrolled monitoring of millions of people around the world, carried out via the Internet and under the veil of absolute secrecy.

The NSA did not limit itself to spying only on the American population: other countries , including those friendly to the United States, were taken at gunpoint . For example, massive data collection was also carried out on citizens, including high-level politicians in Brazil and Germany.

In 2014, **Reporters without borders**, an international press freedom NGO, ranked the American NSA as an enemy of the Internet for its uncontrolled spying on the public. Together with the United States, the list of enemies also includes the departments of Turkmenistan, Cuba, Sudan, Uzbekistan, Saudi Arabia, Iran, Russia, and China.

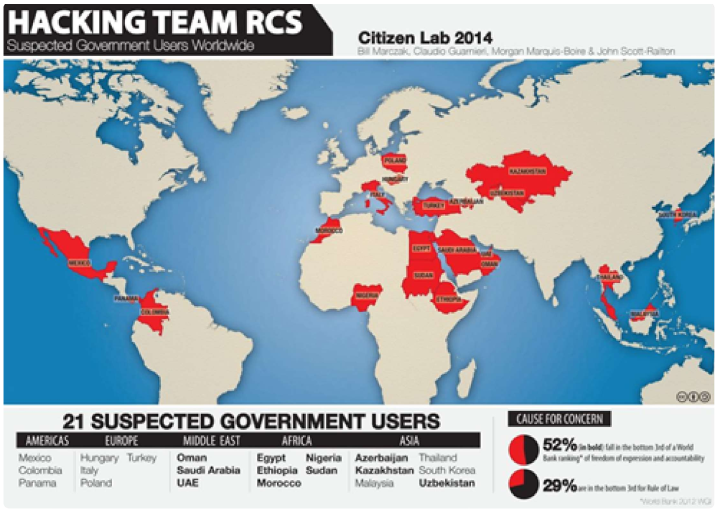
Subsequent litigation and waves of protest from officials, human rights defenders and civil society led to greater protection of anonymity and privacy at the legislative level only in a number of countries and organizations (Brazil, European Union). In most cases, the new laws only strengthened the capabilities of the intelligence services of individual countries to conduct digital surveillance (Canada, France, Germany, Russia, China). **Kazakhstan** did not remain in the shadows **either**.

Online surveillance in Kazakhstan

Kazakhstani intelligence services also use communication technologies, including the Internet, to secretly monitor the population. The actual extent of online surveillance and personal data collection is unknown, but in recent years, several cases of possible use of spyware by government agencies have become known to the public.

So in 2014, **The Citizen Lab**, an interdisciplinary laboratory at the University of Toronto that studies digital espionage and Internet censorship, published a report on the **Remote Control System** (RCS) spyware. RCS was only sold to government departments and advertised as an impossible-to-track data interception program. The spyware made it possible to copy files from your computer’s hard drive, record video calls, emails, messages, and passwords, and connect to your computer’s webcam and microphone. However, experts at **The Citizen Lab** managed to identify twenty-one countries using RCS, where Kazakhstan was among them as well.

Countries Suspected of Buying RCS Spyware



Source: The Citizen Lab

In 2016, **Freedom House**, a nongovernmental organization that studies the level of democracy and Internet freedom in the world, reported with reference to *Wikileaks* that the government of Kazakhstan may have acquired RCS software in order to monitor and intercept Internet traffic (information passing through the Internet) and to carry out targeted attacks against users and digital devices.

In July 2021, **Forbidden Stories**, a consortium of investigative journalists, and **Amnesty International** published a joint investigation into the use of **Pegasus** spyware by governments. According to the publication, Pegasus allows full access to the contents of a mobile phone, including reading messages, tracking calls, saving passwords, determining locations, collecting data from applications used, and remote access to the phone’s camera and microphone.

It became known that online surveillance by government agencies in various countries, from India to Mexico, was carried out in relation to thousands of targets. Kazakhstan is among the numerous clients of Pegasus spyware. It turned out that about two thousand phone numbers from the database of the Israeli company **NSO Group**, which fell into the hands of **Forbidden Stories** journalists, are associated with Kazakhstan. These two thousand include the numbers of many representatives of the political, and far from opposition, elite of Kazakhstan. In other words, according to the investigation, the Kazakh special services spied on local politicians.

The exact number of digital devices infected with the aforementioned spyware is not yet known, but these cases characterize the growing capabilities of the Kazakhstani special services, allowing them to spy on anyone within the country. Moreover, in addition to probable purchase of foreign software, the powers of Kazakhstan's security agencies are also expanding through **legislative acts**.

So, according to the Law "On Communications" and the Rules for the Collection and Storage of Service Information, telecom operators must collect and store personal data of users for two years. At the same time, they are obliged to provide the agencies carrying out operational-search, counterintelligence activities (for example, the police or the National Security Committee (KNB)) with access to subscriber data, including information about subscriber numbers, billing information, the location of the subscriber device, addresses in the data transmission network, addresses of access to Internet resources, identifiers of the Internet resource and protocols of the data transmission network. Also, telecom operators are required to install and maintain equipment for conducting law enforcement intelligence-gathering activities at their own expense.

In addition to Internet providers, laws are also aimed at limiting the anonymity of Kazakhstanis. For example, in accordance with the amendments to the Law "On Communications", starting from 2019, all owners of mobile phones are required to register their devices along with the number, IIN and IMEI in the database of telecom operators. And since 2017, anonymous commenting on Kazakhstani websites has been prohibited. Users must first provide personal data to the owner of the website in order to be able to leave a comment. At the same time, following the global trend, personal data of users should be stored in databases located in Kazakhstan.

In addition, under the Law on Communications, the State Technical Service (STS) has a monopoly in Internet governance. Thus, the STS is responsible for the management of telecommunications networks and Internet exchange points (IXPs) within the country. Internet exchange points are the physical infrastructure to which ISPs connect to exchange traffic (peering), which can increase connection speed and reduce costs.

In 2016, the STS was transferred from the jurisdiction of the Ministry of Information and Communications to the KNB. In 2020, the STS was transformed into a Joint Stock Company, but with 100% state participation; The KNB remained the sole shareholder of the STS.

However, the purchase of foreign spy software and legislation are not all the resources available in the arsenal of the state. The Kazakh government is also trying to implement a domestic program that could greatly facilitate online surveillance of the population. We are talking about the **National Security Certificate** (Qaznet Trust Network).

Back in December 2015, the introduction of the National Certificate was announced, which must be installed on digital devices for supposedly safe Internet use. Despite assurances from the authorities and the media that the certificate is safe and necessary for the fight against terrorism and child pornography, there was a flurry of criticism against the certificate. Many experts feared that installing a certificate under the pretext of ensuring national security would only strengthen the already strong resources of Kazakhstan's special services to control the Internet and online surveillance.

However, due to public criticism, as well as due to the fact that browsers did not include the Kazakh certificate in the list of trusted ones, its implementation within the country was suspended. Only three and a half years later, in July 2019, the government of Kazakhstan resumed its attempt to persuade the population (manually) to install a national certificate (which was introduced as part of the state cybersecurity concept "Cyber Shield of Kazakhstan") in order to cancel it again in August of the same year.

After the cancellation, the popular *Mozilla* browser completely blocked the use of the Kazakh certificate, even in the case of manual installation. The reason is simple: the threat of the certificate to the security of users and the browser itself due to the vulnerability of data to interception. *Chrome* and *Apple* followed *Mozilla's* lead. In other words, Internet companies have banned the Kazakh certificate in order to protect the privacy of their users' personal data.

As it turned out, the suspension of the implementation of the certificate was temporary. In December 2020, the Ministry of Digital Development, Innovation and Aerospace Industry, together with the National Security Committee (KNB), announced a cyber exercise in Nur-Sultan, recommending the installation of a national certificate in order to avoid difficulties in connecting to foreign sites. As a result, many social networks and websites became inaccessible to those who did not install the certificate.

There are the most serious reasons for mistrust of the certificate, also from a technical point of view. This is because Internet connections – for example, visiting https://cabar.asia through the *Chrome browser* – often use secure HTTPS encryption, which encrypts the connection (that is, ISPs and governments cannot intercept traffic).

A secure connection to a website is based on digital certificates, which are authenticated by CAs and trusted by browsers (Chrome, *Mozilla*, *Safari*, *Opera,* and others). Thus, if a website provides a digital certificate issued by a Certification Authority when connected to the Internet, it means that the website is genuine; accordingly, the connection to this site is secure.

The problem is that the Kazakhstani certificate is not universally recognized on a par with those issued by Certification Authorities, and, accordingly, is not trusted by browsers and websites. As a result, the installation of the national certificate on devices connected to the Internet (mobile phones, tablets, laptops) must be done manually. Note that in this case, some browsers (for example, Mozilla) do not recognize the certificate and its installation on these resources is impossible.

Most importantly, once the certificate is installed, there is a risk of a cyberattack called Man-in-the-Middle, which allows the interception and, most importantly, decryption of Internet traffic.

This means that the state, which owns the national certificate, can get access to personal data of Internet users, even using a secure HTTPS connection. At the same time, there is a risk that attackers, having cracked the national certificate, will gain access to all information of users who installed the certificate; moreover, in practice, such hacks have already happened.

Given the ongoing efforts, the government of Kazakhstan has not yet abandoned the use of the national certificate. In the near future, we should expect further attempts to convince the population about the need to install the made in Kazakhstan certificate. At the moment, government agencies are limited to foreign software, laws, and control of the Internet infrastructure.

Balancing national security and the right to privacy

Uncontrolled covert surveillance of citizens (who and what everyone does, reads, visits, who communicates with whom, befriends, enmities) in the realities of authoritarian states is one of the tools of the fight against opposition-minded citizens. For example, the authorities use illegal video filming of the intimate life of objectionable citizens to discredit or blackmail them. The last sensational case of pressure on an unwanted deputy took place in Uzbekistan. Also in Kazakhstan, there is a known case of using a spyware program against oppositionists, activists and journalists in order to collect potential compromising material, as well as track their actions.

At the same time, it is meaningless to deny that government agencies conducting online surveillance ensure national security and help protect citizens from crime, including terrorism.

However, in the absence of an independent oversight body capable of ensuring the transparency of the actions taken by government bodies monitoring the population via the Internet, it is difficult to determine the line between truly ensuring security and violating human rights to privacy.

Many Internet users do not know or do not think about the fact that their every step is recorded, and personal data can be collected and analyzed uncontrollably.

However, the use of electronic technologies to discredit the unwanted is already a reality.

An invisible threat is always difficult to take seriously. However, ignorance or refusal to take seriously the extent of government-sponsored online surveillance of its citizens does not alleviate the consequences.

Civil society needs to understand the scale of government-led Internet surveillance. With each new law, with each new spyware, the security services expand their powers and capabilities to control information flows by intercepting, collecting, storing, and analyzing metadata.

In Kazakhstan, the state is already taking measures to increase the "digital literacy" of the population. However, in the courses that are held within the framework of state programs, they are unlikely to talk about the threats associated with the same National Certificate or the possible digital surveillance of unwanted ones.

Thus, civil society needs to adopt massive programs to improve the information security of citizens.

Second, citizens need to individually work to improve their digital literacy.

Ignoring questionable sites, links and applications and buying an antivirus program are basic steps for using the Internet safely will help minimize the risk of malware or spyware infecting digital devices, both by hackers and government agencies.

Digital security is also served by the following actions: regular software updates; using a "guest" (non-administrator) account on the computer (due to the limit for installing programs); careful use of public Wi-Fi.