36 K. Khetagurovi str., 0102 Tbilisi, Georgia
T: +995 32 2555755 | E: info@geocase.ge

www.geocase.ge

TikTok – a Hidden Threat to State Sovereignty

By Oleg (Bacho) Tortladze, Fellow Researcher at Geocase

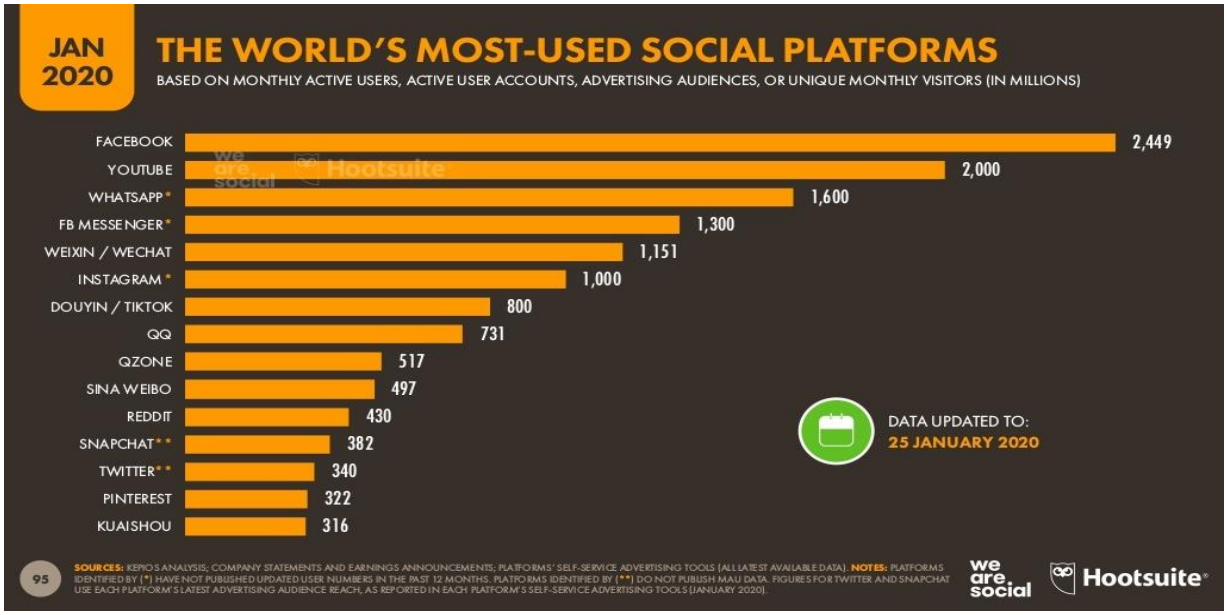
May 14, 2020

Image: PC Mag- www.entrepreneur.com/article/347858

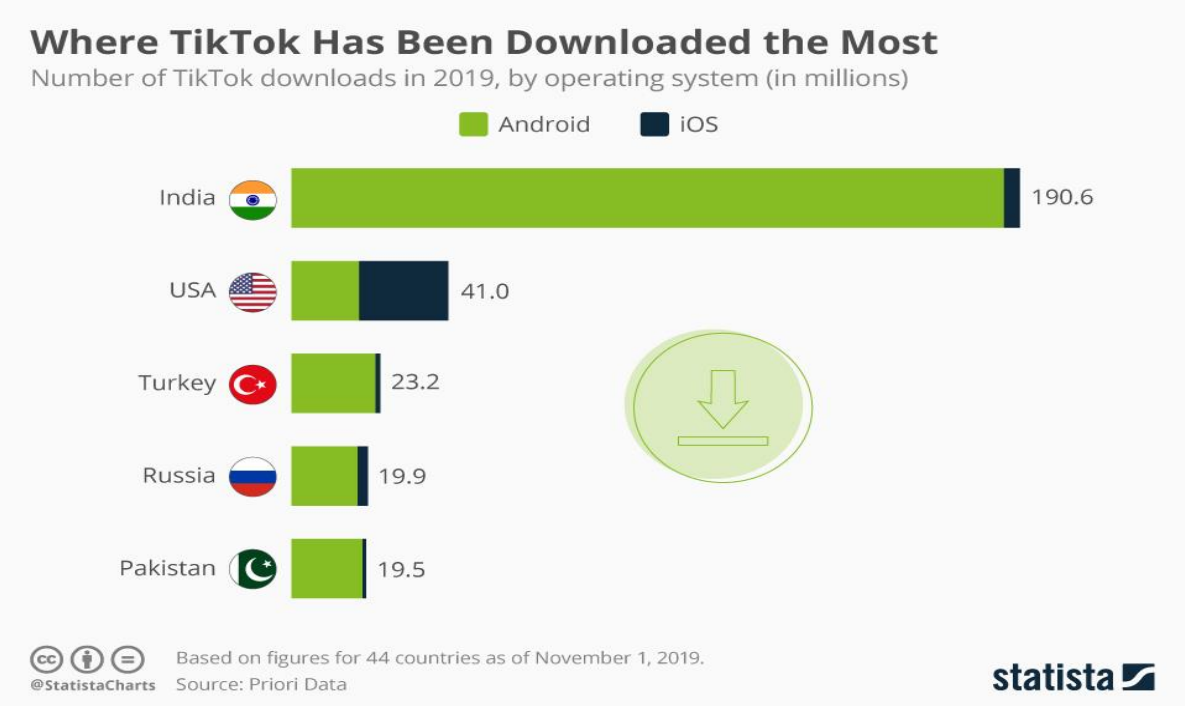
Social networks have become an integral part of everyday life in the 21st century. The development of digital platforms has completely changed the patterns and forms of interpersonal interaction, the behavior of society, the domestic and global politics of states—in short, the entire world. There is no area that has not been touched by technological innovations in general and social networks in particular. When there is a conflict between the benefits and drawbacks of the digital world, the positive aspects will undoubtedly outweigh the negative, however, in the case of certain significant challenges, turning a blind eye to the negative aspects may lead to dramatic consequences. One of the main problems associated with social networking is the protection of the private sphere, including the security of personal data and related issues. This article, in the context of security, is devoted to the evaluation of the newly popular mobile app from Chinese developer ByteDance—TikTok.

TikTok is a video-sharing social network mobile app owned and operated by Chinese internet giant ByteDance. The company created the platform *Douyin* for domestic consumption in 2016, and in 2017 an international version was released—TikTok. The app became especially popular after entering the US and through a merger with California social media startup Musical.ly in 2018, after which the number of accounts on the network increased by 200

million. As of 2020, TikTok has approximately [800 million active users]. In 2019 the application was downloaded 738 million times, and, since its inception—1.5 billion times. TikTok holds an impressive position among the most used social platforms in the world, as seen in the numbers:



Notably, TikTok works in 150 countries and regions and is available in 39 languages. The app covers virtually every continent, with increasing use in countries such as India, the United States and Russia.



As the popularity of the social network grows, more questions about its security arise. The issue was exacerbated when the Federal Trade Commission in the United States fined the social media app Muste.ly, also owned by ByteDance, $5.7 million in 2019 for violating children's privacy. The violations included misuse of the names of children under the age of 13 and the illegal collection of data on their mailing addresses, photos and locations. The organization admitted to the misuse and committed to stopping such data collection practices.

The increase in the popularity and social impact of TikTok in the United States was followed by a backlash from Congress. In 2019 the app began to be studied in the context of national security as a potential threat. A national security inquiry revealed that the social network posed significant risks to cyber security and subsequently both the Department of Defense and the State Department banned the use of TikTok on government-provided cellphones and strongly recommended that the app not be downloaded onto personal devices either.

According to a study published in 2019 by cyber security company Check Point, Tiktok is vulnerable to external intrusion (one of the ways identified are fraudulent short text messages for authorization in the program), thus significantly compromising customer data. In the context of the threat posed to the United States, four major risks have been identified: the collection of data from U.S government employees, the collection of data from ordinary citizens, the dissemination of misinformation, and the censorship of information considered undesirable by the Chinese government. Employees in TikTok's U.S. office have reported on the censoring of culturally and politically sensitive posts. Concerns over censorship have also been raised in the United States Senate, and an initiative has been launched to study it in detail. Speaking at Georgetown University in October 2019, Facebook founder Mark Zuckerberg discussed the Chinese government's censorship policy in relation to TikTok. His remarks highlighted fundamental issues related to freedom of speech in China, which, according to Zuckerberg, has become a major obstacle to Facebook entering the Chinese market. On the flaws of TikTok, Zuckerberg's statements cannot be considered an unbiased source of criticism, as his company has a vested interest in the situation. Not only is TikTok one of Facebook's biggest competitors, but Zuckerberg's active efforts to purchase the application Musical.ly in the past cast doubt on his impartiality. Nevertheless, the blocking of content related to the protests in Hong Kong against the People's Republic of China, Tiananmen Square, and videos related to the independence of Tibet and Taiwan has been confirmed by a number of sources.

Considering China's human rights record and level of democracy, allegations of censorship surrounding TikTok are not revelatory. Intellectual property is not strongly protected in China, confirmed by a simple examination of the external and functional characteristics of certain Chinese products. However, in the context of Tiktok the problem goes beyond the borders of one state and moves into the global security space. In the fierce battle for global internet domination, from the East and the West, China and the United States are on the digital frontlines. The agitation over 5G internet and Huawei proves that neither will the United States give up its existing hegemony nor will China cease fighting for a new hegemony. It is clear that the topic is not only related to technology, but also to the acquisition of strategic geopolitical and geoeconomic advantages. China has begun paying the political and economic price for the COVID-19 outbreak, visible in the apparent breakdown of the Chinese supply chain model. China, of course, cannot stand idle during this crisis but seeks to strengthen its global position, including by utilizing popular social networks. A number of major digital

players have had incidents in which they failed to uphold internet integrity and respect for fundamental human rights, reflected in subsequent financial slaps on the wrist. The risks associated with TikTok are completely unique due to its susceptibility to government pressure.

In the 21st century enemies are not always armed with guns. In the era of hybrid threats, digital platforms characterized by low autonomy and direct connection with the main political thread of a particular country are an important tool for attack. TikTok, as a seemingly harmless social network, is tool of Chinese soft power that can manipulate global public opinion. The app collects the personal data of millions of people, including minors, and there are currently no solid legal or technological guarantees that the social network will not illegally store or use this information. There are many ways to monetize such information that was illegally obtained or unintentionally shared. Consequently, this degree of data insecurity poses a threat to both individuals and the sovereignty of states, as geographic access to other countries' internal affairs has become completely unnecessary in the modern world. Naturally, it is difficult to say whether these threats will become a reality, but the current technical characteristics and information policy of TikTok do not leave much hope for a positive future.

Georgia, as a member of the historic Silk Road and the newer Belt and Road Initiative, is not only part of China's prospective geographic but also its digital sphere of influence. China's political and economic interests in Georgia, which were active in the pre-pandemic world, will increase even more in the post-pandemic period, given the location and political positioning of the country. Against the backdrop of the rapid growth of TikTok use in Georgia, it is important to adequately assess the threats in all dimensions. Considering the risks associated with the application, the promotion of its popularity by a major Georgian ISP in its advertising raises many questions. Before further details about the dangers of the app are revealed, it is important to understand what programs are being used on our electronic devices, how much access we give them, and what personal data we make available. A central characteristic of life online is that nothing posted can ever truly be permanently erased. Consequently, in the case of illegal data processing, it is virtually impossible to talk about a full reparation of any potential harm. At this stage, the best method of preventing harm is to raise public awareness and find ways to redistribute the burden of responsibility to individuals.

May 14, 2020