The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

On the Cyber Battlefield, China, Not Russia, Is the Biggest Threat to the U.S.

Russia is a genuine short-term problem, but China is the greater long-term challenge for the U.S.

By Tinatin Japaridze & Lincoln Mitchell

February 25, 2019



Tomas Roggero / Flickr (CC BY 2.0)

Amid rampant discussions of the Kremlin's interference in American elections and its cyber espionage targeting the United States, Russia and the U.S. may be embarking on what some refer to as a New Cold War.

However, the larger threat to the U.S., and to a free internet globally, will likely turn out to be China. The U.S. failure to recognize this would be an enormous mistake.

Some in the American government understand this. For example, during a hearing of the

Senate Committee on Homeland Security and Government Affairs, FBI Director Christopher Wray noted that it is China, not Russia, that poses the broadest and most complicated counterintelligence threat to the U.S. — and that cyberspace will likely continue as its battlefield of choice.

"Russia is in many ways fighting to stay relevant after the fall of the Soviet Union. They're fighting today's fight," Wray said. "China is fighting tomorrow's fight."

Despite observations like Wray's, the American people, particularly those on the center and left who are seeking answers regarding Russia's role in the 2016 election, have lost sight of the reality that China is much bigger technological threat to the U.S. than Russia.

In 2015, a milestone bilateral pact was signed by former U.S. President Obama and Chinese President Xi Jinping. China has, however, since surpassed Russia as the most prolific state-sponsored cyber adversary against Western firms, government departments, think tanks, NGOs and universities in its pursuit of commercial secrets and intellectual property.

This is exacerbated by increased dialogue around cyber issues between Russia and China. The first-ever Sino-Russian cyber agreement, also signed in 2015, marked the beginning of bilateral cooperation in the cyber arena. The pact highlighted two key features: mutual assurance of nonaggression in cyberspace and clear language advocating for each country's respective cyber sovereignty.

According to the agreement, each state has the right to shield its cyberspace from foreign interference. Moreover, each party has the right to manage and, if need be, even censor its domestic internet content — all of the above falling under the umbrella of cyber sovereignty.

Aside from Chinese leadership's use of cyber sovereignty as a means of securing its online borders from American and Western interference, China is simultaneously looking to establishing itself as the "primary power" of the digital era.

In the midst of its economic rise, Beijing is demonstrating an absolute and unwavering determination to become an undisputed leader of the ongoing digital revolution.

Related article: Russia Flirts With Internet Sovereignty

Today, Russia is moving closer to the Chinese model of internet policing through hybrid tactics aimed at minimizing — if not eliminating — undesirable online content. This strategy combats what the Kremlin perceives as sensitive material with the potential to destabilize the Putin regime.

Earlier this month, Russia passed new legislation that Western critics and human rights activists have likened to an "online Iron Curtain." Andrei Klishas, a senator and one of the draft bill's authors, which was approved in its first reading in the State Duma two weeks earlier, noted that the Russian government had already designated 20 billion rubles

(approximately $300,000) to cover the costs of protecting its cybersecurity and critical infrastructure in the event of foreign interference and cyber aggression.

Related article: Russia Must Build Own Internet in Case of Foreign Disruption, Putin Says

Critics of the Kremlin and this latest bill more specifically describe this recent move as Russia's adoption of the Chinese internet governance model. In 2017, President Putin openly supported Chinese cyber censorship, noting that the internet cannot be a place of "excessive 'quasi-freedom.'"

Yet, by the same token, he suggested that instead of following in China's footsteps, Russia will pursue its "own path," further adding that "regulations in general should correspond to the level of development of a society." The Russian leader concluded, "We have limitations and they are known, [but] in my view, these limitations are enough at the moment."

For many Americans today, it is almost impossible to think about cyber crimes, hacking, bots and other nefarious internet behaviors without thinking about Russia. There are good reasons for that. But thinking only about Russia and ignoring a larger, more powerful, more sophisticated — and possibly more nefarious — power would be a very big mistake.

The views expressed in opinion pieces do not necessarily reflect the position of The Moscow Times.

Original url:
https://www.themoscowtimes.com/2019/02/25/in-the-cyber-battlefield-china-not-russia-is-the-biggest-threat-to-the-us-a64612