Cyber Conflict and Geopolitics

Richard B. Andres

In today's world, a prominent question raised by several U.S. presidents is whether or not new cyber technology is contributing to the rise of Russia and China's prevalence in cyberspace. Russia is known to have used social media outlets to conduct cyber-psychological operations to cause uncertainty in both the United States and Europe. China has carried out economic espionage and other information-retrieving methods. Even with this information, leading to the U.S. sanctions of both China and Russia in 2017, there is little evidence as to what exactly the countries are doing. It is believed that the countries will attempt to facilitate the creation of a new global system that allows Russia or China to have a larger impact geopolitically.

Technological influence of nations dates back as far as ancient Greek times, highlighting how Egypt used technology to become the predominant power of the ancient world. Theorists, such as Alfred Mahan and Halford Mackinder, attempted to predict the patterns of technological impact in global geopolitics. Mackinder argued the primacy of Britain depended on maritime technology, which could be challenged by continental European powers, such as Germany and Russia, developing railroad technology. He also predicted Russia and Germany's economic power would eventually eclipse Britain's power, leaving Britain poorly equipped to compete.

The information age has also led to a shift in military and economic power. Emergence of cyber piracy, informational theft, and network sabotage are all too common in today's world. Cyber technology also has a hand in the geopolitical sphere. The United States was the first nation to take advantage of technology for geopolitical gain, using cyberspace to conduct espionage activities as early as the 1990s. While the use of cyber was in no way "revolutionary," the United States further defined itself as the predominant power, even in the cyber front.

Russia began its use of cyber in the wake of the Cold War. With little resources, cyber seemed like the only viable option, utilizing it in economics as well as in espionage operations. Between the period of 2011 and 2018, Russia seemed to have perfected its use of cyber influence through information operations, perhaps peaking in the accusation of influence in the 2016 U.S. presidential election. Russia has shown its capabilities, highlighting the vulnerability of the U.S.'s cyber infrastructure. However, with a GDP that is one-fifteenth the size of the United States, it is unlikely that Russia would be able to drastically improve its geopolitical status.

China's interest in the cyber-geopolitical realm began as early as 2004. Major General Li Bingyan argued for the adoption of a cyber policy based on deception and control, eventually leading to China implementing this approach. China executed cyber operations pioneered by the United States with a focus on economic espionage. In 2013, U.S. company Verizon reported that 96 percent of cyber espionage attempts originated in China. China's GDP can compete with the United States, predictively surpassing it in the coming decades. The likelihood of China surpassing the United States in the geopolitical sphere due to cyber operations seems more likely, as well.

The first two rounds of the international contest for cyber dominance have unfolded. In the first, the United States developed the exact cyber methods that China and Russia use in round two. China's use of cyberspace is based on the incentive of rewards each state receives for attacking rival computer networks, especially the United States. Russia is incentivized to foster nationalism and infiltrate Western critical infrastructure. With no foreseeable end to this "game," each country is battling for supremacy in a particularly heated cyber climate. It is not a question of "will" cyber technology will lead to geopolitical change, but rather "when." For the last two decades on the cyber front, it seems that the United States is yielding its ground.