Great Powers in Cyberspace: The Strategic Drivers Behind US, Chinese and Russian Competition

Matthew Bey

Earlier this year the Pentagon released its first National Defense Strategy in a decade. The document put the long-term great power competition between the United States and what it calls two revisionist powers, China and Russia, at the forefront. Russia's global influence on the global stage has been steadily resurging over the past ten years, culminating with its intervention in Ukraine in 2014, and China, likewise, has regained its historical status as a global power after its so-called century of humiliation. Though the United States' attention has been elsewhere – namely on the Middle East and the Global War on Terrorism – for much of this time, it is now renewing its focus on its near peers in a return to the status quo.

Cyberspace will be a critical battleground for the United States, China, and Russia as they jockey for global influence. The domain is, of course, a relatively new environment where the governing norms and treaties are still only in their infancy and not universally accepted. And because the United States, China, and Russia are by far the three greatest cyber powers worldwide, the rivalry between them will define the treaties and norms that develop. The process will take time, and it could get messy.

The three parties involved diverge significantly in their views of issues such as how to apply international law to cyberspace, the extent of national sovereignty over cyberspace, and the nature of human rights within it. As the global competition increases, we can expect these topics to become only more polarizing. The U.N. Group of Governmental Experts failed miserably last year in trying to gain consensus on these points of contention. After all, the difference in US, Russian and Chinese viewpoints on cyberspace are rooted in the three countries' very different geopolitical imperatives and constraints.

Matthew Bey is a senior global analyst at Stratfor, an Austin, Texas-based geopolitical intelligence firm, where he leads the company's analysis on international trade, economics, energy, emerging technologies, and related trends with an emphasis on China, the Middle East and Africa. Mr. Bey holds a master's degree in mathematics from The University of Texas at Austin and a bachelor's degree from Texas Lutheran University.

CHINA'S MULTIFACETED STRATEGY

China's overall strategy toward cyberspace consists of several layers. First, the country's view of the global system and its relationship to the great power competition shapes how aggressive Beijing will be in promoting its viewpoint. China today is seeking to revise the US-led international system to have greater prominence, having spent much of the twentieth century in the periphery and largely excluded from developing global norms. Much as Beijing views the dollar-backed international financial system as evidence of the United States' entrenched power, it considers the application of US law to other countries and the Western interpretation of international law on Internet freedom as a way for Washington and its allies in the West to assert their influence worldwide. The size of its market gives China the power to dictate the terms of doing business there, making the discussion over cyberspace standards one of the first where Beijing has a seat at the table to legitimately argue that it is a peer competitor of the US and, as such, an important voice in the debate.

That does not mean, however, that China wants to break the current system. Quite the contrary. The country's economic and social stability depends on the continuation of the status quo. Global trade flow, information flow, and interconnectivity underpin China's economy as much as they do the US economy. For that reason, China views the ad hoc bilateral deals it has struck over its cyber policies – such as the 2015 agreement with the United States to halt cyberattacks used for industrial espionage – as necessary to defuse tensions with other countries while avoiding disruptions. These types of agreements will also become increasingly important to China as it develops technology that it seeks to protect from industrial espionage, regardless of whether it abides by these deals. China’s priority is to ensure that international cyber norms don’t evolve in such a way that its domestic policies become a liability.

Second, China’s strategy over cyberspace is closely tied to its national security. It’s no secret that the Chinese government has tried to control the flow of information for decades to maintain rigid governance of its expansive territory and large population. To update that campaign for the twenty-first century, Beijing has developed a sophisticated cyber strategy. External threats – whether from an outside power such as the US or a domestic opposition group – have long been a catalyst for unrest (consider the 1989 Tiananmen Square uprising, for example, or the more recent protests in Ukraine, Central Asia, and the Arab world.) In the information age, China worries that hostile forces could use the internet to undermine the Communist Party's authority and destabilize the country with a cyberattack or merely the dissemination of information. President Xi Jinping’s administration has taken steps to mitigate that risk, tightening censorship to enhance ideological conformity and to suppress political dissidents during the difficult socio-economic transition underway in his country.

As China gears its strategic environment toward the growing competition with the United States, Beijing will further strengthen its grasp on domestic cyberspace through measures such as data localization laws. At the same time, Beijing will likely intensify its online intelligence gathering. Its intrusions this year into US maritime companies’ data and various political groups in the run-up to Cambodia's elections have showcased its expanded collection efforts.

Third, China’s cyber strategy corresponds to its industrial policy. Though China’s capabilities in cyber operations and emerging technologies such as artificial intelligence are becoming more sophisticated, the country still depends largely on Western technology. Beijing is hoping to break that dependency through the Made in China 2025 plan. Just as the United States worries that products from Chinese tech companies Huawei and ZTE may include backdoors that Beijing can exploit, China has reason to believe that Western technologies will give foreign intelligence agencies a way into the country. The US, in response, is working to pressure Beijing into abandoning its techno-nationalist ambitions; a recent example is its proposal to expand the jurisdiction of the Committee on Foreign Investment in the United States to include export controls on industrially significant emerging technologies.

These attempts, however, will only push the Chinese government to redouble its efforts to develop its own tech giants, including conducting industrial espionage as needed, despite the 2015 deal with Washington. Given the increasing convergence between the tech and defense sectors, the Chinese military will take on a larger role in supporting China's tech pursuits. Its involvement will give China a competitive advantage over the US, where a gulf remains between the military and Silicon Valley.

RUSSIA: THE NOT-SO-NEAR PEER

Like China, Russia bases its cyber strategy in large part on its need to resist external influence. Both countries encompass large territories and disparate populations that over time have defied centralized government. To manage that challenge, Moscow, like Beijing, has historically restricted the flow of information to its public as a means of controlling the population; it is similarly concerned about rivals using information against it, even more so since the color revolutions across the former Soviet Union during the previous decade. Russia, therefore, shares China's belief in national sovereignty over cyberspace, though it is perhaps more focused on information warfare than the threat of tactical attacks and physical disruptions.

In other respects, Russia’s cyber strategy differs from that of China. For one thing, it is an interventionist strategy, in line with Russia's interventionist foreign policy. Russia and China alike use cyber operations for general intelligence gathering, but Moscow has also used them to conduct large-scale disinformation campaigns overseas, most notably ahead of elections in countries such as the US and France. For another, Russia is not the near-peer economic competitor to the US like China. A growing number of obstacles stand in the way of its achieving that status. Along with the economic stagnation caused by the 2014 crash in oil prices, the country is in the throes of a demographic crisis that will reduce its population by 2.4 percent by 2030.

Russia is a leader in certain cyber capabilities, and it does have a few well-established technology companies on the software side of things. Nonetheless, it simply does not have the commercial industry that China and the US have to support tech development. The Russian Google or Huawei does not exist, and it probably never will. Consequently, the Kremlin will have to rely on the levers it already has at its disposal to achieve its goals regarding China and the US, namely cyberattacks and disinformation campaigns. These relatively low-cost tactics will remain a key feature of Russia’s cyberspace policy going forward, even though the West will continue to develop more sophisticated response mechanisms to counteract them.

THE DEBATES TO COME

The return of near-peer competition will not result in the bipolar international system of the Cold War; the economies of China, Russia, and the US are too deeply intertwined to enable that outcome. Although the intensifying rivalry among the US, China, and Russia stymied the U.N. Group of Governmental Experts, it does not necessarily preclude the establishment of international norms on cyberspace. Instead, it will merely limit their scope.

Despite international concerns over state-sponsored cyberattacks, the use of intrusive tactics such as hacking, for political or military gain, has become more or less an accepted fact of life in the internet age. Industrial espionage, likewise, is emerging as a red line in the cyberspace discussion because of China's pragmatic stance on the issue. Norms around operations that either physically disrupt business operations or cause physical damage will be hard to hammer out. The US, China, and Russia have all been deliberately vague about where they would draw the line on unacceptable practices, an approach that is not exactly conducive to establishing clear global standards. Nevertheless, norms will eventually materialize, even if they are hazy and largely implied since few treaties or enforceable agreements are likely to come about to implement them. The West's push for a rules-based system or a central body, like the World Trade Organization, to govern cyberspace and adjudicate on complaints will probably be a non-starter for China. Furthermore, Beijing and Moscow would have more to lose than to gain from joining such an institution and relinquishing control over their domestic cyberspace.

In short, the rules of cyberspace probably will remain ad hoc and muddled as the geopolitical competition heats up. It is unlikely that China would support the creation of well-defined cyber norms in the context of the Western-led international system. Both China and Russia, meanwhile, will continue to try to exploit the gaps in cyberspace governance to further their objectives. These countries will, for example, keep using mercenaries and cyber proxies to carry out cyber operations on their behalf so they can circumvent existing norms in cyberspace while maintaining plausible deniability.

Under these uncertain conditions, the Balkanization of cyberspace and of the technology sector, which have manifested so far in the push for data localization, will likely continue. The absence of a global rules-based system governing cyberspace means that the differences in laws, regulations, and litigation practices from state to state will only grow as countries try to exert greater control over the internet.

The escalating great power competition between Russia, China, and the US will shape the evolution of cyberspace and of the conventions surrounding it. Though Moscow will have its role to play in the process, Beijing and Washington will largely determine its outcome as they embark on what is likely to be a lengthy period of economic, military, technological and political rivalry without precedent since the Cold War.