


# Incorporating the Cyberspace Domain: How Russia and China Exploit Asymmetric Advantages in Great Power Competition

 [mwi.usma.edu/incorporating-the-cyberspace-domain-how-russia-and-china-exploit-asymmetric-advantages-in-great-power-competition/](https://mwi.usma.edu/incorporating-the-cyberspace-domain-how-russia-and-china-exploit-asymmetric-advantages-in-great-power-competition/)

March 15, 2021



*Editor's note: This article is the first in a series, "Full-Spectrum: Capabilities and Authorities in Cyber and the Information Environment." The series endeavors to present expert commentary on diverse issues surrounding US competition with peer and near-peer competitors in the cyber and information spaces. Read all articles in the series [here](#).*

*Special thanks to series editors Capt. Maggie Smith, PhD of the Army Cyber Institute and MWI fellow Dr. Barnett S. Koven.*

When it comes to America's focus on great power competition, China and Russia loom large, making the analysis of these two competitors and their strategies a booming business for analysts and practitioners alike. But while Russia's "Gerasimov doctrine" (which is not really a doctrine) and China's "three warfares" are the focus of many articles, how these two states and their militaries act in cyberspace is less often discussed and less well understood. Information operations play a central role to both the Russian and the Chinese ways of war, and cyber applications are a central mode by which information is applied as a tool of warfare. China conceives of "informationized warfare," with the space and cyber domains

described as becoming the “commanding heights of strategic competition.” Make no mistake: despite claims to the contrary, both China and Russia see themselves currently engaged in information warfare against the United States. This war is playing out principally in the cyber realm. The military application of information as an instrument of war—in isolation and in conjunction with other tools—is a central component of these states’ modern approaches to warfare. As Chief of the Russian General Staff General Valery Gerasimov himself observed, special operations forces leveraging information operations could be effectively employed to “defend and advance [Russia’s] national interests beyond” its borders. China, for its part, has developed and deployed dedicated information operations units skilled in cyberespionage and cyber-enabled information operations. This article serves to highlight some of the differences between how the United States, China, and Russia view cyberspace, and the ways Russia and China are using cyberspace operations to engage the United States asymmetrically.

One way in which both Russia and China view cyberspace operations differently than the United States is through their use of domestic proxies to confront opponents. To the United States, there is a clear bright line separating the employment of the state’s capabilities from those of private US citizens in cyberspace. Both China and Russia have no qualms employing commercial companies, “patriotic hackers,” or cybercriminals on behalf of the state. Of course, both China and Russia leave just enough space between the state and these proxy groups so that they can claim plausible deniability. Another important way in which the United States differs from China and Russia is in how it has organized its military to confront adversaries in cyberspace. In the United States, the government has divided control over cyberspace. While it has created a military command for the cyberspace domain, US Cyber Command (USCYBERCOM), it also rightfully allows information operations to intersect with each of the other commands. This means there is no particular US military command in charge of information operations. Rather, all commands share responsibility over this space. Russia and China view cyberspace very differently.

## **Russian Cyberspace Operations**

For Russia, a core tenet of successful information operations is to be at war with the United States, without Americans even knowing it (and the Kremlin can and does persistently deny it). The Kremlin views cyberspace holistically, to include electronic warfare, psychological operations, and information operations (including information warfare, or informatsionnaya voina). In Russia, the government has taken a much different view of cyberspace than the US government has, particularly the linking of cyberspace operations to special operations. The Russian Main Intelligence Directorate (GRU) of the General Staff has primacy in external cyberspace operations, to include espionage, information warfare, and offensive cyberspace operations. This comprehensive approach creates interesting synergies for the Russian military. In addition to the GRU, the Russian Federal Security Service (FSB) has a domestic operations division with an internal security and counterintelligence (CI) mission. The FSB (the old KGB) also undertakes external cyberspace operations stemming from its

CI responsibilities. As such, its external operations sometimes conflict with the GRU's cyberspace operations due to poor coordination (indeed, poor coordination plagues Russian special operations in general). For example, both the GRU and FSB unknowingly targeted the Democratic National Committee at the same time for a hack-and-dump operation. The final major Russian agency involved in cyberspace operations is the Foreign Intelligence Service (SVR), which conducts espionage on behalf of the Russian state, and has become quite adept at cyberespionage as recently evinced in the SolarWinds hack.

Unlike the United States, Russia is not known to have a definitive cyberspace strategy, policy directive, or doctrine. Therefore, what researchers understand about Russian operations and activities in cyberspace is derived from the writings of Russian military scholars and official documents, and even teaching materials at the nation's various military academies. From these sources, it is apparent that the Russian government views cyberspace primarily in terms of "information confrontation" and the technical infrastructure used to control information. To shape and control information, the Russian military takes a hybrid approach, integrating "special operations forces and non-kinetic political, economic, or informational measures." Therefore, cyber is a central component of the Kremlin's hybrid warfare model, or what Russia refers to as "asymmetric methods."

Russian information operations are among the best in the world and Russia is not afraid to use them. Indeed, Russia believes that the tools of information warfare must be brought to bear early and often. To Russia, there is no distinction between information operations, to include those occurring in cyberspace, during times of war or peace. That said, by employing information operations before the start of a kinetic conflict, Russia may be able to achieve their desired strategic aims without having to resort to kinetic military operations. Even where it is still necessary to use kinetic force, information operations are nevertheless synergistic with the application of military force, by, for example, degrading the resolve of the opposing military force.

Control of information has been critical throughout Russia's authoritarian past, during tsarist times, continuing during the history of the Soviet Union, and now under the current kleptocratic regime. All of these authoritarian governments came to realize that when they control information they can also shape the course of events within the country. Conversely, when they lose control of information, such as during the *glasnost* period, the government cannot control the narrative and may lose legitimacy among the population. Therefore, since Russia understands how susceptible it is to losing control over its own information space, it has also come to realize how vulnerable other countries are in this space, especially those countries that have deep societal cleavages. While Russia has become very proficient at disinformation campaigns to exploit societal cleavages, it is most adept when it can amplify or augment existing homegrown narratives. For example, Russia has long sought to exacerbate racial tensions in the United States. Russia was also implicated in a disinformation campaign to discredit the World Anti-Doping Agency as a "whole-of-society" approach (the operations include actors beyond the government) to highlight Western moral

hypocrisy. More recently, Russian information operations headed by either the GRU or the FSB have targeted left-leaning organizations, like Peace Data, and right-leaning platforms, like Parler, to exacerbate existing tensions in the United States.

Cyberspace has become one area in which Russia has capitalized on the asymmetric power of operations and activities within the information space. As alluded to previously, the United States and Russia understand the domain and how to employ effects in and through cyberspace very differently. As such, the United States and Russia are fundamentally at odds over any sort of cyberspace rules of the road. This has particular significance in three areas: espionage, information warfare, and offensive cyberspace operations.

Russian cyberspace espionage is conducted to gather not only intelligence relating to national security, but also economic intelligence. Most recently, Russia was suspected of attempting to hack into pharmaceutical companies in search of COVID-19 research data. This hacking activity is an unsurprising development. As stated by Gen. Gerasimov, Russia must leverage all elements of national power, and this includes cyberespionage (and cyber-enabled economic warfare) to shape the information space and degrade an adversary's capabilities. One of the more infamous acts of Russian cyberespionage involved a cutout group called the Shadow Brokers, which likely leveraged the work of the Russian cybersecurity firm Kaspersky to locate NSA-developed malware. This malware was possibly found among classified materials that a contractor brought home and operated on his personally owned computer. The EternalBlue exploits employed by Shadow Brokers subsequently wreaked havoc across the world.

When it comes to offensive cyberspace operations, or what the US military describes as deny, degrade, disrupt, destroy, and manipulate (D4M) operations, the GRU is the primary actor. The GRU's dominance makes sense given that the SVR and FSB are more focused on espionage. However, since the GRU is a military organization first and not primarily concerned with stealth, its offensive cyberspace operations are known for being blunt and reckless, as seen in the NotPetya attack, the Saudi petrochemical attack, or the attacks against Ukraine's power grid. These types of aggressive cyber actions that cause real-world effects will allow Russia to be a formidable force when combined with its traditional strengths in information operations and the insights gleaned through cyberespionage.

## **Chinese Cyberspace Operations**

Much like Russia, China also sees information operations as central to its conception of competition in cyberspace. In fact, the Chinese Communist Party (CCP)—and by extension its defender, the People's Liberation Army (PLA)—views information operations via space, cyber, and electronic warfare as the “tip of the spear” in any future conflict to shape the narrative and obtain information superiority, thereby paralyzing a more powerful enemy.

China further expanded upon its comprehension of cyberspace with the creation of the Strategic Support Force (SSF) in 2015. Some analysts view the SSF as an enhanced Chinese counterpart to USCYBERCOM. The SSF not only focuses on the traditional D4M operations of USCYBERCOM, but has also added space, electronic, and psychological warfare. Housing these different but complementary cyber-enabled capabilities within the same command is expected to create synergies that these capabilities cannot achieve on their own. Moreover, having a suite of functions under the same command during peacetime will give the CCP and PLA the ability to seamlessly transition to an integrated campaign during wartime.

While China has not openly published a cyberspace strategy, scholars and practitioners are in widespread agreement as to the CCP's aims. It seeks to control the flow of information to and within China to ensure domestic stability (and halt the efforts of "splittists" who seek the disintegration of the PRC), and preserve economic growth through commercial espionage. By controlling dissent and driving economic growth, the CCP ensures that it is able to maintain power.

China asserts that just as every state is the sovereign within its own borders, each should likewise be the sovereign within its own cyberspace. Cyber sovereignty challenges the US view that information should be allowed to flow freely across borders. China considers the control of information within China to be as vital as "controlling the maritime domain in the eighteenth century or controlling the air domain in the twentieth century." Therefore, to maintain harmony within China and produce disruptive effects beyond its borders, China has increasingly improved its information operations throughout recent years.

In regard to maintaining economic growth, China's operations against economic targets and the commercial sector are viewed by former USCYBERCOM commander General Keith Alexander as "the greatest transfer of wealth in history." While the CCP continues to claim that cyber economic espionage is not the work of the government but rather criminal elements within China, the cybersecurity group FireEye has been able to identify with a high degree of certainty that there are at least ten advanced persistent threats (APTs) operated by the CCP, nine of which focus on industrial espionage.

In addition to these government-supported APTs, China also has a very large patriotic hacker community that it can mobilize when needed. Due to the extensive cyberspace dragnet that the CCP has put in place, the government is aware of the activities of these hackers and can stop them when it so desires. However, the CCP has also employed this hacker network as an extension of the state while at the same time retaining plausible deniability since these patriotic hackers are not formally part of the state apparatus.

The CCP's firm hold on power is a function of both its ability to maintain economic growth and its control over the flow of information in China. This explains why both economic cyberspace espionage and information operations have seen increased investment by the Chinese military in recent years. Moreover, the CCP has leveraged China's commercial

sector to support the state's interests, as seen with the "Made in China 2025" plan that encourages Chinese companies to create dual-use technologies, which can also be employed by the military. This coupling of the state and private enterprise is seen in China's Cyber Security Law and National Intelligence Law, the latter of which necessitates that "any organization and citizen shall, in accordance with the law, support, provide assistance, and cooperate in national intelligence work, and guard the secrecy of any national intelligence work that they are aware of."

The Chinese state does not employ externally focused information operations nearly as effectively as their Russian counterparts. However, the Chinese state is constantly learning, and likely gleaned a lot from Russia's successful 2016 influence operations in the US political space. Traditionally, the Chinese state focused the majority of its information operations internally in order to maintain stability. However, with the rise of Xi Jinping, China has shifted some of their information operations from primarily being for domestic control to influencing the external environment. This is most evident in China's projection of a newfound muscular international image, and in its defensiveness over COVID-19. All that said, Chinese large-scale, external influence operations still need further refinement.

## Looking Ahead

In short, Russia and China view information and cyberspace operations differently than the United States does, and they are designing their operations and cyberinfrastructure to engage the United States asymmetrically. As previously noted and despite persistent claims to the contrary, both states see themselves currently engaged in information warfare against the United States. The military application of information as an instrument of war—in isolation and in conjunction with other tools—is a central component of these states' modern approach to warfare, both today and into the foreseeable future. Recognition of this reality must undergird America's cyberspace and information warfare policies and doctrine.

*Mark Grzegorzewski, PhD, is a professor at the Joint Special Operations University, US Special Operations Command. He has recently published in Special Operations Journal on "Demystifying Artificial Intelligence through DoD Education" and has a chapter in an edited volume titled, "Russian Cyber Operations: The Relationship Between the State and Cyber Criminals." He created JSOU's Quick Look series with forthcoming publications on AI and cryptocurrency.*

*Christopher Marsh, PhD, is the director of research and analysis in the Institute for SOF Strategic Studies at the Joint Special Operations University, US Special Operations Command. He is the author of several books and dozens of articles on Russian and Chinese domestic, foreign, and defense policies, including Unparalleled Reforms: China's Rise, Russia's Fall, and the Interdependence of Transition. He is currently writing a book on great power competition between the United States, Russia, and China.*

*The views expressed are those of the authors and do not reflect the official position of the United States Military Academy, Department of the Army, Department of Defense, US government, or that of any organization with which the authors are affiliated, including US Special Operations Command.*