Truly Understanding the Adversary:
Describing the Threat in the Information Space

Colonel Christina A. Bembenek

Introduction

Imagine sending the 82nd Airborne Division on a no-notice deployment to Europe as Russian troops make an initial incursion into the Suwalki gap. The division lands in darkness at the staging airfield, but the host-nation government, a close ally, refuses to allow the Soldiers to disembark. Local media has reported credible information that American forces are preparing to arrest government leaders so that those forces can use the entire country as a staging area for a wider conflict. Social media, news stations, and radio broadcasts are all carrying the same narrative.

How could rational leaders in an allied nation believe the U.S. military was there to stage a coup? Unfortunately, this is not an imaginary scenario, and it has already happened in the United States—in 2015, Russian intelligence services engineered a conspiracy around the United States military exercise Jade Helm, which caused the governor of Texas to send the Texas State Guard to observe the exercise just in case the story was true.[1] According to Michael Hayden, retired Air Force general and former director of the Central Intelligence Agency and National Security Agency (NSA), Russia used Jade Helm, to test its ability to influence the cognitive information space by co-opting a narrative found in the fringes of American media and using bots, social media influencers, and fake personas to amplify the story.[2]

In order to prevail in conflict, the military must train to compete in the cognitive information space now, which requires a more nuanced understanding of how the two greatest challengers, Russia and China, operate in this space.

Manipulating the Information

Russia has provided both clear doctrine and several real-world test cases exemplifying its proficiency in information operations. In his March 2017 speech at the Russian Academy of Military Sciences, Chief of the General Staff Valery Gerasimov outlined an operational concept that emphasized the "extensive employment of political, economic, diplomatic, information, and other nonmilitary measures" in confronting the threat from the United States and the North Atlantic Treaty Organization (NATO).[3] Understanding the underpinnings of this operational concept and how it merges Russia's military capabilities with gray zone operations, particularly in the information space, is critical for the United States to compete in this space.

President Vladimir Putin believes Russia is in an ongoing conflict with the West, and his ultimate goal is to restore Russia's position as a great power and world civilization.[4] This includes—

- Returning to a multipolar world.
- Ensuring Russian primacy in the post-Soviet spaces.
- Opposing NATO and all transatlantic institutions.
- Forming a closer partnership with China.[5]

As a former KGB officer, Putin views information as a key component of his strategy, and an element of risk management, to be employed in concert with military operations or when hard power applications are not suitable. According to Fiona Hill, former senior director for European and Russian affairs on the National Security Council, Putin focuses most of his efforts on manipulating information to shape a particular perception of himself and Russia. One of the reasons he granted asylum to Edward Snowden, the NSA contractor who provided reams of sensitive intelligence to WikiLeaks, was because it allowed him to present himself as a protector of free speech and information transparency.[6]

The Example of Crimea and Disinformation

Russia's 2014 annexation of Crimea, an autonomous republic within Ukraine, offers a rich example of its effective use of information operations in concert with military operations. Following the overthrow of the Ukrainian government amidst widespread protests, Russian operatives introduced further uncertainty and confusion into the local populace by flooding the media with false narratives and conspiracy theories about the interim Ukrainian government and its military forces. Putin capitalized on this environment of mistrust to move Russian troops into Crimea to "protect" its citizens. The Russian government crafted a narrative claiming Crimea was Russian territory in every respect—historically, linguistically, and culturally—and used media, theatrics, and military troops to bring the story to life. When the occupation was complete, Putin hosted a televised extravaganza in the Crimea that re-created the events leading up to the annexation and mixed in masonic symbols, swastikas, and dollar signs to denigrate the West while also featuring old Soviet symbols and patriotic songs to hearken back to the historic greatness of the Soviet Union. To the international community, Putin transmitted the message that Crimea is part of the *Russkiy mir* (Russian world) by assembling the Russian Duma in Yalta, the site of the 1945 great power conference that divided up Europe following World War II, and attesting that Russian society would consolidate and return to "hard work for Russia and in the name of Russia."[7]

Russia has been dominating the information space every day since Crimea and honing the tactics that it will undoubtedly use against the United States in any future conflict. According to a report by the Global Engagement Center, Russia has created an ecosystem of disinformation and propaganda that magnifies the effectiveness of its "information confrontation" strategy.[8] The Russian government issues key themes that are echoed across state-funded media like RT and Sputnik, "verified" in Russian-aligned think tanks like Global Research, and amplified across social media by networks of bots and false personas. More perniciously, the Russians have become adept at co-opting and spreading misinformation and false narratives generated by domestic actors in a country, thus making it appear that the disinformation is genuine and coming from inside the state. As they exploit partisan divides, the Russians are not concerned with creating one consistent version of the "truth" but rather seek to amplify all sides of an issue and create what the RAND Corporation labeled a "firehose of falsehood" that spreads confusion, overwhelms the information space, and further divides society.[9]

Information Confrontation

"Information Confrontation" is the term used in Russian strategic and military circles to describe their approach to the use of information in both peacetime and conflict. There is also a rich public record of the use of "Active Measures" to describe long-standing Russian political warfare methods that utilize disinformation and propaganda as a core tool.[10]

The Chinese Strategy

The Chinese are equally engaged in the information space, and though President Xi Jinping shares the same nationalist goal as President Putin—to return China to its rightful place at the center of the world—Xi has a different strategy. Rather than create confusion and disunity in the information space, the Confucius-based Chinese state seeks to build a unified, favorable opinion of China. Although China has not as explicitly paired information operations with military action, as Russia did in Crimea, information plays a key critical role in its military doctrine. The 2019 Chinese National Defense white paper states, "war is evolving in form towards informationized warfare, and intelligent warfare is on the horizon."[11] China's Ministry of National Defense aims to increase transparency with the Chinese population through monthly press conferences on military matters and its Information Office's Weibo and WeChat accounts, which have more than 6 million followers. The Defense Intelligence Agency labels "information warfare" as a core People's Liberation Army (PLA) strength, and PLA doctrine identifies "information dominance" as a prerequisite for victory in modern war.[12] Any future Chinese military operation will feature a robust information campaign conducted across multiple platforms.

Chinese influence in the cognitive information space is a sleeping giant. The Chinese Communist Party (CCP) runs a sophisticated propaganda model. It has created a diverse, sprawling information infrastructure to manipulate information and disseminate its preferred narratives both at home and abroad. China's Central Propaganda Department, established in 1924, penetrates every channel of mass communication in China, including the arts, social media, and print publications.[13] Xinhua, one of the largest news agencies in the world, regularly pays to insert *China Daily* articles into international newspapers; Chinese language publications in diasporas also echo and amplify CCP narratives. The CCP operates on both domestic and international social media networks, posting messages tailored to an international audience on YouTube, Twitter, and Facebook and a domestic message on Weibo and WeChat. The CCP also

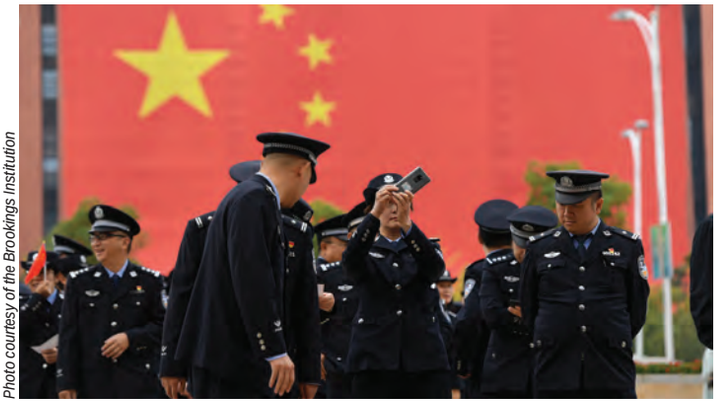

Photo courtesy of the Brookings Institution

Chinese officials are taking to Twitter and other social media platforms to respond to criticism of China or the ruling Communist Party.

leverages in-person networks, including business and academic groups, to amplify its narratives that orchestrate local influence campaigns across the globe. China has also conducted covert influence operations online, targeting Western audiences with fake social media personas and using high-volume bot accounts to amplify controversial content.[14] Considering that there are more than 1.3 billion Chinese native speakers compared to 379 million native English speakers,[15] the potential for China to spread authentic-sounding messaging to Chinese speakers across the globe is enormous. With a ready network of Chinese-speaking humans, constructed personas, media outlets, and bots, China is a formidable competitor in the information space.

Conclusion

The *U.S. Army in Multi-Domain Operations 2028* describes Russia and China as information-based states and highlights their sophisticated information warfare capabilities, but it only scratches the surface of the complexity of their information ecosystem. Intelligence doctrine does not yet exist to support modern operations in the cognitive information space, but this is where the competition will take shape. In order to accurately describe the information ecosystem, as well as its effect on both domestic and international audiences, and to recommend operational counters, military intelligence agencies will need to expand their normal partnerships, work to expand their authorities, and get comfortable operating and communicating at the unclassified level. The Active Measures Working Group, an effective Cold War interagency team, offers one possible model for how military intelligence can contribute in both competition and conflict in the information space. Regardless of the strategy the military pursues, it is critical that we start competing now because when competition turns to conflict, there is no time to build credibility, communications channels, or trusted partnerships.

Endnotes

1. Molly McKew, "Current Information Operation Topics: US Intelligence Is Finally Figuring Out How To Communicate With The American Public On Threats In Our Information Domain, And We Should All Pay Attention," *Stand Up Republic* (blog), July 30, 2020, https://standuprepublic.com/current-information-operation-topics-us-intelligence-is-finally-figuring-out-how-to-communicate-with-the-american-public-on-threats-in-our-information-domain-and-we-should-all-pay-attention/.

2. Cassandra Pollock and Alex Samuels, "Hysteria over Jade Helm exercise in Texas was fueled by Russians, former CIA director says," *Texas Tribune,* May 3, 2018, https://www.texastribune.org/2018/05/03/hysteria-over-jade-helm-exercise-texas-was-fueled-russians-former-cia-/.

3. Harold Orenstein, trans., "Contemporary Warfare and Current Issues for the Defense of the Country," *Military Review* 97, no. 6 (November–December 2017): 23, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/November-December-2017/.

4. Fiona Hill and Clifford G. Gaddy, *Mr. Putin: Operative in the Kremlin* (Washington, DC: Brookings Institution, 2013), 324.

5. Eugene Rumer, "The Continuation of Politics," *The Primakov (Not Gerasimov) Doctrine in Action* (Washington, DC: Carnegie Endowment for International Peace, 2019), https://www.jstor.org/stable/resrep20980.5.

6. Hill and Gaddy, *Operative in the Kremlin,* 422.

7. Ibid., 458.

8. Global Engagement Center, *Pillars of Russia's Disinformation and Propaganda Ecosystem* (U.S. State Department, August 2020).

9. Christopher Paul and Miriam Matthews, "The Russian 'Firehose of Falsehood' Propaganda Model: Why It Might Work and Options to Counter It," RAND Corporation, 2016, https://doi.org/10.7249/PE198.

10. Global Engagement Center, *Pillars of Russia's Disinformation,* 5.

11. The State Council Information Office of the People's Republic of China, *China's National Defense in the New Era* (Beijing: Foreign Languages Press, July 2019), 6, http://www.xinhuanet.com/english/download/whitepaperonnationaldefenseinnewera.doc.

12. Defense Intelligence Agency, *China Military Power: Modernizing a Force to Fight and Win* (November 2018), 17.

13. Renée DiResta, Carly Miller, Vanessa Molter, John Pomfret, and Glenn Tiffert, *Telling China's Story: The Chinese Communist Party's Campaign to Shape Global Narratives* (Stanford Cyber Policy Center, July 21, 2020), 9.

14. Ibid., 27.

15. James Lane, "The 10 Most Spoken Languages In The World," Babbel, September 6, 2019, https://www.babbel.com/en/magazine/the-10-most-spoken-languages-in-the-world.

COL Christina Bembenek is the Commandant for the U.S. Army Intelligence School at Fort Huachuca, AZ. She previously has served as the 82nd Airborne Division G-2 and in multiple intelligence positions at the tactical, operational, and strategic levels. She recently completed an Army War College fellowship at Columbia University where her research focused on the impacts of disinformation on the military and society.