Threat Approaches to Cognitive Warfare

smallwarsjournal.com/2026/03/18/narrative-as-a-weapon

by John Wirges

March 18, 2026

The Social Design Agency (SDA), a Kremlin-linked agent, executed a significant influence operation known as Operation Doppelgänger from 2022 to 2024. Through Doppelgänger, the SDA disseminated pro-Russian narratives by fabricating legitimate news websites, and amplified the content through fake social media personas and bots. Doppelgänger's significance, however, emanated from its secondary effects. While Western governments effectively responded to the crisis and contained the disinformation, the operation remained in the new cycle as news people ruminated and politicians securitized the issue. Russia's success was found in this amplification; Russia framed and controlled the narrative and normalized Russian penetration of the cognitive environment.

Adversarial states such as Russia, Iran, and China seek to modify the balance of power internationally and recognize cognitive warfare's role in achieving state interests in a subversive era. Russia, Iran, and China employ cognitive warfare to pursue power and influence at Western expense. These regimes use weaponized narratives domestically to suppress domestic dissent, and abroad to advance state interests by shaping and changing human behavior. Given recent developments in the Middle East, understanding cognitive warfare's role in conflict and statecraft is vital. This article seeks to provide a priming analysis of the similarities and differences between Russian, China, and Iranian cognitive warfare and clarify the central role that narrative plays in manipulating human behavior. This article explores how Russia and Iran produce well-built influence campaigns targeting Western societies, while China uses disinformation and influence activities successfully to promote pro-Chinese Communist Party (CCP) narratives. Additionally, this essay explores how each regime controls domestic information, Russian and Iranian covert media influence, and China's global network of media and security services. Finally, this article identifies several key areas Iran has exploited in the information environment during the ongoing conflict.

Defining Cognitive Warfare

Western literature defines operations in the information environment through a multitude of terms, including hybrid warfare, subversion, information operations, and cognitive warfare. NATO states that cognitive warfare seeks to "exploit facets of cognition to disrupt, undermine, influence, or modify human decision-making by altering human behavior and cognition through any means and technological advances." Chinese theorists Tzu-Chieh

Hung and Tzu-Wei Hung define cognitive warfare as “controlling others’ mental states and behaviors by manipulating environmental stimuli.” Russia sees cognitive warfare as more related to western Cold War thinking on *political* warfare. Andreas Krieg provides a useful definition of Russia’s approach to cognitive warfare more as subversion, or “the strategic exploitation of sociopsychological, infrastructural, and physical vulnerabilities in the information environment by an external adversary to erode a sociopolitical consensus or status quo.” Krieg’s definition of subversion and Hung and Hung’s definition of cognitive warfare recognize the communal political effect of distorted perception, whereas NATO’s definition focuses on individual cognition as a precursor to decision making. Even though these countries and actors define cognitive warfare differently, the above definitions all highlight the use of weaponized narratives to achieve military or political goals and focus on the exploitation of the information environment to modify human behavior. This article uses the term “cognitive warfare” to standardize terminology and address the state-centric nature of narrative-based conflict. This article will utilize Krieg’s narrative and subversive-oriented definition to explore how Russia, Iran, and China weaponize and employ narrative across all domains.

Russia

Cognitive warfare is a vital aspect of Russian, Chinese, and Iranian statecraft; however, each state approaches cognitive warfare’s application differently. Russia has long believed that Western governments actively seek to disrupt its regime. Cognitive warfare is seen within the Russian strategic culture as defensive in nature. Russian cognitive warfare campaigns include attempted interference in U.S. Presidential elections in 2016, 2020, and 2024, interference in the 2024 Romanian Presidential elections, and cyber-based attacks including 2025’s Jaguar Land Rover attack in the UK, which cost the UK roughly £1.3 billion. Russia is uniquely capable in comparison to Iran and China due to government’s centralized approach to cognitive warfare.

Modern Russian cognitive warfare has roots in the USSR’s “Active Measures,” which were subversive campaigns designed to alienate allies and attack social cohesion. For example, between 1959 and 1960 the USSR executed an active measure known as “the *red swastika*” to alienate the West German Government from its NATO allies, particularly France, the UK, and U.S. The target audience was latent antisemites in Western Germany. Soviets understood that individuals in Germany continued to harbor sympathy for the Nazi regime and held antisemitic beliefs. The Soviets assessed that they could mobilize latent anti-Jewish feelings in society; furthermore, the Soviets assessed that by painting West Germany as largely antisemitic, the West German Government could be implicated. With KGB support, this cognitive warfare operation mobilized widespread organic antisemitic activity in Germany, additionally antisemitic activity spread to other European countries and the U.S. Today, Russian state media, proxies, and government actors are well-organized and create reinforcing narratives, making truth difficult to distinguish or discern.

Russian media sources all operate with either formal or clear indirect links to the regime. While the Russian information space may be less controlled than Iranian or Chinese internet, the Russian cognitive warfare ecosystem is a trusted source of information for domestic audiences. Russian media such as RT and Rossiya produce content that benefits the regime and, at times, act as state agents. Almost immediately after the attempted assassination of Sergei and Yulia Skripal in Salisbury, UK in 2018, Russian linked media sources, Twitter accounts, and official statements—including the Russian Embassy's social media account in London—began disseminating dozens of conspiracy theories or conflicting narratives. RT and Rossiya produced dozens of false and misleading narratives to confuse European audiences and investigation efforts. Through the use of bots and trolls to create competing narratives, Russia proxies such as the Internet Research Agency (IRA), demonstrated their capability as social media-based cognitive warfare practitioners. In total, Russian-linked sources put our forty-six different stories. These activities were designed to make truth harder to discern and complicate attribution of the crime to the Russian regime. This penetration of the environment leveraged narratives to confuse, misdirect, and slow western policy responses.

Iran

Iran appears to have successfully adopted Russian-style approaches to cognitive warfare. Iran's 'Storm-2035' campaign leveraged news and social media sites to deliver poignant and well-crafted narratives in an attempt to influence the U.S. election. Iran, like Russia, seeks to utilize cognitive warfare to weaken Western political institutions and erode social cohesion. Iran demonstrated advanced cognitive warfare capabilities in its attempts to interfere with the 2020, 2022, and 2024 U.S. Presidential and midterm elections; these included establishing multiple fake news sites with artificial intelligence to create discord and portray certain candidates in a negative light. For example, Iran's 'Storm-2035' campaign developed well-crafted disinformation websites to disseminate well-crafted narratives targeting both liberal and conservative political groups. Iran created web sites such as Even Politics (evenpolitics.com), Nio Thinker (niothinker.com), and Savannah Time (savannahtime.com) to disseminate disinformation and subversive content to hyper-mobilize domestic partisanship and erode social cohesion in the United States.

Since the U.S., Israel, and Iran entered into a state of armed conflict, the Iranian regime has demonstrated a capable use of artificial intelligence (AI)-generated video content to flood social media. Social media accounts linked to the Iranian Government have posted a significant number of photos and videos all designed around a core narrative: depict U.S. forces as vulnerable and exaggerate the damage caused by Iranian forces. For example, Iranian-linked social media accounts have posted and propagated AI-generated videos of high-rise buildings on fire, as well as doctored satellite images falsely showing the U.S. Navy's Bahrain-based Fifth Fleet Headquarters destroyed. While the ultimate reach or effectiveness of these videos has yet to be fully realized, these activities demonstrate that to

Iran, cognitive warfare is not a “bolt-on” to military operations, but a layered and integrated process. Iranian proxies are generating disinformation at the speed of strike to own narratives. Additionally, offensive technologies likely have an edge over defensive. The BBC has reported that AI-detection systems, such as X’s Grok, have struggled to recognize Iranian AI-generated content posted to X.

Iran effectively leverages domestic information controls to minimize regime dissent. Iran’s state broadcasting company, Islamic Republic of Iran Broadcasting (IRIB), functions as an agent of the state. IRIB produces regime-approved content designed to divide populations and minimize threats to its regime. In 2022, Iran experienced intense national protests after a woman was killed in police custody. IRIB media outlets routinely ignored or minimized violence caused by state security forces, while emphasizing the violence and chaos caused by protestors. Iran also utilized its control of the internet, shutting off domestic internet at critical junctures during the protests to disrupt protest organization. Of note, in the last seven days, the IRIB has been kinetically targeted by U.S. and Israeli forces due to links with Islamic Republican Guards Corps (IRGC) operations. These links demonstrate Iran’s whole-of-security state approach to media controls. Protests throughout 2025 and 2026 have also demonstrated Iran’s reliance on internet controls and weaponized narratives in its cognitive warfare toolkit. The International Institute for Counterterrorism’s analysis demonstrates that that while the Iranian regime initially sought to partially acknowledge protest grievances, the regime’s cognitive warfare strategy has combined “external actor” and “victory” narratives—seeking to maximize social cohesion and reframe the protests as a greater conflict with the U.S. and Israel—with internet restrictions. A notable exception to these controls was the March 4th hacking of IRIB Channels 1 and 2 in Iran; throughout Iran, IRIB lost control of its broadcast for several minutes while actors played a message from Reza Pahlavi—the son of the former Shah and presumed Crown Prince should the monarchy be restored—in which he argued for Iranian citizens to mobilize against the regime. London-based Iran International news network reported that the Iranian Regime has engaged directly with citizens suspected of using systems of bypass internet controls to coerce its population and maintain control of the domestic information environment. These narratives have been well-coordinated, disseminated and amplified through state and state-affiliated traditional and social media networks.

China

In contrast to Russia and Iran, China primarily sees cognitive warfare as a tool for controlling its public image and Chinese diaspora abroad. In recent years, however, China has increased its interference in Western political processes through pro-CCP narratives much like Russia and Iran. The Chinese state has devoted billions of dollars to build a global network of news and media agencies, all of whom work as agents of the Chinese state. The CCP uses this media network to promote positive views of China’s culture, history, and regime. In addition to this massive influence program, China has a global network of “police stations" and surveillance outposts to monitor—and when necessary, harass—Chinese diaspora abroad. The well-known Confucius Institutes also constitute an example of the Chinese approach to cognitive warfare. Confucius Institutes were established throughout the world as cultural and linguistic outreach centers, largely attached to universities. These institutes, however, were extensions of the Chinese government; Confucius Institutes hired based on political loyalty and censored topics or perspectives unfavorable to the CCP. This narrative framing censored free speech across western universities on topics such as Taiwan and effectively allowed the CCP to influence human perceptions as a precursor to behavior. China's approach to cognitive warfare successfully intertwines actions in the physical domain, such as the establishment of media networks or cultural institutions, and weaponized narratives to minimize dissent and maintain control over narratives regarding the CCP's regime.

Domestically, China's Great Firewall and Golden Shield also provide the regime effective controls over the domestic internet. Chinese internet controls isolate domestic audiences from foreign content, limit dissent, and enable domestic surveillance. These controls are effective cognitive warfare tools, as they manipulate information, allowing the regime to effectively frame and control its preferred narratives to create social compliance. Chinese security services and proxies have also been linked to bots and troll farms designed to discredit anti-Chinese narratives. While China has traditionally avoided direct meddling in Western affairs, in recent years it has increased its interference in Western elections, including Canadian parliamentary elections. Chinese agents have been known to purchase social media accounts and utilize AI to generate pro-China content, known as "spamouflage" campaigns. However, China has generally struggled with social media operations. For example, researchers have easily identified pro-Chinese false accounts as purchased spam or marketing accounts. China has been more effective through tactics like search engine flooding to control online conversations.

Analysis and Conclusions

Russia, Iran, and China have demonstrated sophisticated cognitive warfare capabilities, including covert media activities and the use of proxies to spread disinformation and weaponized narratives on foreign soil. More critically, however, is the focus that these countries place on narrative control and manipulation. Examples such as the Operation Doppelgänger, the IRGC's use of artificial intelligence to build and publish content on key issues such as Gaza, or China's use of bots to manipulate behavior all demonstrate the centrality of narrative control to their cognitive warfare campaigns. China and Russia have outlined cognitive warfare doctrines that seek to "control mental states" and manipulate perception and truth. This is a fundamentally different approach to cognitive warfare than western countries. NATO cognitive warfare efforts, for example, orient far more on the use of technological means to disrupt an adversary's decision-making cycle. While adversarial approaches to cognitive warfare leverage advanced technology, the role of narrative weaponization in subversion of domestic and foreign audiences is far more pronounced than in western models. Understanding these differences is critical to minimizing mirror imaging when conducting analysis of adversarial cognitive warfare.

An analysis of Russian, Iranian, and Chinese cognitive warfare demonstrates that modern technologies have provided authoritarian regimes with powerful tools for controlling their populations, protecting their regimes, and destabilizing open societies. The information space has highlighted a growing inequity between authoritarian and open political systems. Russia, China, and Iran can control domestic access to information and use systems of mass media to create false realities for their citizens. These regimes use these same systems of mass communication against open societies and those who seek openness. Russia, Iran, and China use intelligence operations to create unwitting proxies, sow discontent and division through social media, and promote state interests through a growing network of state-affiliated foreign media. Russia and Iran use cognitive warfare to attack Western societies, promote lies, and advance state interests at the expense of their adversaries. China continues to prioritize cognitive warfare to protect its image and limit dissent; however, Chinese offensive cognitive warfare designed to interfere in foreign elections and weaken Western social fabric appears to grow.

Adversaries see cognitive warfare as central to statecraft and regime survival and will be powerful actors in this space as the global order becomes more multipolar. Critical to this approach is narrative framing. Russia, Iran, and China prioritize narrative control and manipulation to erode social cohesion, de-mobilize populations, and limit Western government response options while slowing down policymaking. Western nations and NATO have begun to emphasize cognitive warfare's role in modern competition; recent actions include the U.S. Army's decision to create an information warfare branch. It is critical to continue expanding narrative-based resilience measures, taking into consideration the necessity of a whole-of-government approach to narrative control.