LeMay Center Inspiring Doctrinal Innovation Essay

Modernizing Information Operations Doctrine to Meet New National Security Needs

Erin Grenier, USAF Intelligence Analyst (Civilian)

30 April 2023

About the author:

Ms. Erin Grenier is an Air Force civilian intelligence analyst currently serving as the Red Cell lead in the NORAD & NORTHCOM Wargaming Division and a Harvard University Extension School Master's degree candidate in International Relations- Nuclear Deterrence.

Air Force Doctrine Publication 3-13 - Information in Air Force Operations

U.S. Air Force doctrine on Information in Operations outlines yesterday's challenges for tomorrow's battle. While the United States has focused its military supremacy efforts on acquisition of highly advanced weapons and platforms, our adversaries have been adapting their strategy- primarily in the information domain to pose asymmetric threats to the U.S. at a fraction of the cost. As it currently stands, our adversaries are playing in our information sandbox uncontested, and we are unknowingly engaged in a battle for the hearts and minds of our own population. The number one priority in the National Defense Strategy is to defend the homeland, paced to the growing multi-domain threat posed by the PRC.[1] However, our current doctrine does not adequately reflect this "growing multi-domain" threat. The U.S. Air force has the opportunity to lead the Department with innovative and forward-leaning doctrine that provides modern tools and concepts to solve operational solutions to strategic challenges in the information domain. This can be accomplished by shifting our doctrinal approach and responsibly aligning a portion of our resources to non-military instruments of powers, greater whole of government collaboration, building civil society resiliency, exercising modernized concepts into wargames, and reaching our adversaries' populations.

Non-military Instruments of Power. While Diplomacy, Information, Military, and Economic (DIME) serves as a useful model to understand different levers and tools available to achieve national security objectives, it also suggests these domains live in separate worlds. To our adversaries, these four tools live under the same umbrella, used concurrently to execute a well-crafted strategy. Focusing on the, "I" domain, the PRC is rapidly altering its information warfare strategy to exploit perceived western vulnerabilities. According to a 2021 RAND study, the Chinese military views information as the single most critical domain for success in contemporary and next generation warfare, using information to influence foreign perceptions and behaviors against foreign entities, such as military and political forces.[2] China's perception on the future of warfare is the canary in the coal mine, warning of non-kinetic threats we will face in a potential future conflict. Our doctrinal concepts and perspectives must reflect this changing environment accordingly.

The United States spends more on defense than the next top ten countries combined.[3] Despite this massive annual price tag, we seem to be losing more ground than we are gaining. Our adversaries are learning and improving on information warfare strategies through development of creative and inexpensive nontraditional military tools and methods, challenging U.S. global dominance. By realigning national security requirements based on new adversarial threats (primarily in the information domain) the U.S. could increase its level of readiness and military strength while avoiding resource waste. Doctrine highlighting best practices in this domain can help refine these requirements

---

[1] Fact sheet: 2022 national defense strategy § (n.d.).
[2] Harold, Scott W., Nathan Beauchamp-Mustafaga, and Jeffrey W. Hornung, Chinese Disinformation Efforts on Social Media. Santa Monica, CA: RAND Corporation, 2021.
[3] "U.S. Defense Spending Compared to Other Countries." Peter G. Peterson Foundation, April 24, 2023.

Capture the Nuance, Lean Forward. Defining concepts is useful for the sake of baselining but should not stop there, we must rethink and redefine doctrine. To keep pace with the quickly evolving information domain, we must capture nuance and avoid vague generalizations. For example, in the "execution" section, there lies a recommendation that states, "Detect and counter emergent adversary disinformation and other OIE of concern." While this seems reasonable and logical, what is this really saying? Such recommendations are too vague to *mean* anything and leave commanders with little to work with. A much more useful recommendation for commanders would be: "Set up an interagency working group with each organization's responsibilities represented, discuss identified emerging threats and existing gaps through use of firsthand observations and advanced tools, develop whole of government response with path forward for each organization." While this may seem overly prescriptive, I believe this is the only way the U.S. can get out of its bureaucratic ways that our adversaries are actively exploiting and tackle the behemoth information battle that is quickly closing in on us.

Messaging Must Start at Home. The U.S. Air Force and the DoD writ large, cannot successfully achieve information superiority without first recognizing its own limitations. Due to the nature of modern technology, gone are the days that the United States can successfully promote democracy and the benefits of a free market without first keeping its own house in order. According to a 2023 RAND study, the advancement of American values, specifically belief in American democracy, serves as a core pillar of U.S. national security strategy, regardless of the political party in power. However, a January 2022 NPR/Ipsos poll found that 64 percent of Americans believed U.S. democracy was "in crisis and at risk of failing," highlighting Americans' doubts on the future of democracy. Americans' strong belief in a democratic system fuels U.S. foreign policy and as RAND notes, an increasing lack of internal belief in democracy undermines U.S. ability to promote democracy abroad.[4] While this may seem like more of a foreign policy issue, the DoD is facing new threats that do not conform to previously established lines. The success of military diplomacy and alliances depend on positive perceptions of the U.S. and its values as a nation- which are currently under threat.

In the same study, RAND explains the phenomenon of "truth decay" in American society. RAND defines truth decay as the diminishing role of facts and analysis in American public life, the blurring of lines between opinion and fact, increasing volume and influence of opinion over fact, and declining trust in formerly respected sources of fact. Truth decay has led to eroding civil discourse and causes political paralysis. This phenomenon has led to mass confusion and uncertainty on objective facts.[5] Traditionally, the explanation behind what RAND has labeled "truth decay" has been viewed as a domestic matter of little consequence to national security. However, the Department of Defense has missed the warning signs of disinformation and is losing time to reverse course. In a crisis or conflict involving the United States, the spread of

[4] Williams, Heather J and Caitlin Mcculloch. "Truth Decay and National Security- Intersections, Insights, and Questions for Future Research." EXPERT INSIGHTS ON A TIMELY POLICY ISSUE. RAND, April 2023.
[5] Williams, Heather J and Caitlin Mcculloch. "Truth Decay and National Security- Intersections, Insights, and Questions for Future Research." EXPERT INSIGHTS ON A TIMELY POLICY ISSUE. RAND, April 2023.

disinformation by our adversaries risks undermining both domestic and allied cohesiveness- perhaps even U.S. willingness to respond. In a similar vein, we ought to prepare for the adversary seeking to undermine public confidence in the U.S. intelligence community, leading to doubt in senior leader's credibility. The absence of public trust could easily complicate and limit political and military decision-making, thereby playing into the adversary's hand at low effort, low cost, and provide plausible deniability.

Currently, the U.S. is engaged in another Cold War-like ideological competition, specifically with the PRC. We are fighting for global human rights, while our adversaries are creating partnerships and alliances with the "no strings attached," approach, or in other words, a free pass for prospective partners to rule as they wish, no matter the human cost. For the United States to have effective messaging to foreign audiences, we must fix the internal rot- viewing this effort as a national security imperative. Doctrine at the service level can help to address this by encouraging commanders to collaborate with other government agencies and improve domestic perceptions of the military. Trust building exercises such as increased community outreach and engagement, even military hosted training on adversary targeting tactics with civilian audiences could help combat domestic truth decay and support national security objectives.

Ctrl + F "Social Media". The advent of social media as a military tool has contributed to the shift into modern and future warfare. While our understanding of the weaponization of social media is still in development, the concept of disinformation as a means for control and influence is well understood. President Xi and Putin continue to restrict domestic access to outside information while increasing its reach in western media. To our adversaries, the United States most prized possession of press and speech freedom is our greatest vulnerability.

In recent news, Chinese social media platform "Tik Tok" has grown to become one of the most popular social media platforms, with a total of 150 million American users,[6] at the likely expense of national security. Not only can our adversaries spread disinformation through social media outlets, but they can use the platform itself to gather potentially damaging data to U.S. interests. In late 2022, FBI director Christopher Wray testified to the House Homeland Security Committee that the Chinese government could use Tik Tok to control data collection on users or control the recommendation algorithm, which could be used for influence operations or to control software on millions of devices.[7] For many years, social media has been viewed as a valuable open-source intelligence platform, however, we've neglected to view it as a weapon. In a conflict scenario, it is likely our adversaries would leverage social media platforms to foment discontent, seeking to complicate the information space.[8]

2016 served as a pivotal year for America's understanding of the power the information domain holds as Russian meddling in U.S. elections exposed our soft underbelly. Rather than promoting one view over another in its campaign, Russia echoed and amplified voices on both sides of the U.S. ideological spectrum, thereby sowing deep division between party lines. Russia's campaign successfully fomented internal dissonance while distracting the U.S. populace from global

[6] TikTok. "Celebrating Our Thriving Community of 150 Million Americans." Newsroom. TikTok, August 16, 2019.
[7] Treisman, Rachel. "The FBI Alleges TikTok Poses National Security Concerns." NPR. NPR, November 17, 2022.
[8] Williams, Heather J and Caitlin Mcculloch. "Truth Decay and National Security- Intersections, Insights, and Questions for Future Research." EXPERT INSIGHTS ON A TIMELY POLICY ISSUE. RAND, April 2023.

events. Most of this was accomplished through trendy "memes" and viral twitter hashtags via social media platforms. Despite the relatively large success Russia experienced through its 2016 U.S. election inference campaign, there is only one appearance of the words "social media" in a ctrl + f search in Air Force Doctrine Publication 3-13. Our adversaries are growing more sophisticated in social engineering by the day, using it to wage psychological warfare on the U.S. population and it is merely a footnote in our military doctrine. Charged by both the NSS and NDS, the USAF has the opportunity to modernize its doctrine to reflect this changing battlefield and adopt a more proactive approach. It is crucial the USAF begins thinking of social media as a domain for warfare that must be doctrinally addressed so we can effectively defend our homeland from adversarial targeting and avoid surprise.

Whole-of-Government, Civil Society, Allied Collaboration Required. Information dominance cannot be achieved through one service, nor can it be achieved without total and absolute whole of government collaboration. The Department of Defense is neither structured, nor staffed to compete in the information war alone and certainly should not be conducted on an ad hoc basis. Doctrine must insist on coordination to achieve effects, this is the only way we can win. Short of this, the U.S. appears fragmented and stovepiped- highlighting seams and vulnerabilities to our adversaries. The National Security Strategy states "we are working with governments, civil society, independent media, and the private sector to prevent credible information from being crowded out, exposing disinformation campaigns, and strengthening the integrity of the media environment - a bedrock of thriving democracies." Civil society's role in combatting adversarial efforts is not mentioned in USAF Doctrine Publication 3-13, but it could. Air Force doctrine should encourage use of public affairs, international affairs, MISO, cyber forces, intelligence, information operations forces, etc. to combat disinformation and strengthen cyber resiliency. The combination of interagency working groups and civil society outreach to improve U.S. populace social media literacy could have a profound effect in creating an uncontested environment.

This concept applies to our allies as well. The U.S. cannot achieve information dominance or combat adversarial information warfare in a vacuum. While our allies' coordination and collaboration is vital, their perception of the U.S. is also key. A RAND study on the degradation of truth in the U.S. and the subsequent reaction from our allies suggests that truth decay and conspiracy theories among U.S. political and domestic populations can influence U.S. National Security. Shifting foreign public views on alliances within our partner's borders and consequent reaction from political leaders has the power to conflict with alliance cohesiveness and undermine allied forces actions or willingness to act.[9] Allied civil society perceptions of the U.S. matter almost as much as domestic perceptions. Doctrine must reflect the importance of collaborating with our partners and allies to combat adversary attempts to drive wedges in our most critical security relationships. USAF Doctrine Publication 3-13 can encourage commanders to prioritize partnership building across the service in the information domain.

---

[9] Williams, Heather J, and Caitlin Mcculloch. "Truth Decay and National Security- Intersections, Insights, and Questions for Future Research." EXPERT INSIGHTS ON A TIMELY POLICY ISSUE. RAND, April 2023.

Wargaming. Imagine it is 2040, tensions with China have escalated beyond repair and the U.S. is about to enter into a conflict. As the U.S. is rapidly preparing for kinetic exchange, portions of the U.S. electric grid collapse, clean water is inaccessible, and a majority of posts on social media are claiming the U.S. government cannot defend its citizens or its critical infrastructure.[10] Artificial intelligence and deep fakes make it difficult for American citizens to discern fact from fiction. Many forms of media coverage state that surrender and submission is the only option for reprieve or things will get much worse. American citizens begin protesting by the thousands outside of military bases and outside of the White House, demanding the U.S. avoid entrance into a conflict. What is the DoD's response to this scenario? Not a shot fired while we are staring down the barrel of defeat. Have we adequately prepared our decisionmakers for this future battle space? Does doctrine address this kind of warfare?

Executing wargames that focus on the latest, greatest, and future kinetic weapons systems is beneficial, after all, it is the most dangerous and thrilling event in a game. However, the U.S. needs to focus on gaming adversary information warfare in a wartime scenario. In a conflict scenario, not only would our adversaries seek to conduct destructive cyber attacks and target domestic audiences to create confusion, chaos, and distrust in government but also to generate discontent within the military ranks with the goal of influencing U.S. military personnel to refute orders. Disinformation campaigns accompanied by debilitating cyberattacks risk catastrophic internal consequences. This "soft", yet highly salient threat to military operations and domestic stability must to become a primary U.S. focus. In a 2021 study, RAND recommends that the United States military train its forces on recognizing disinformation in the lead up to and during a conflict.[11] Red cell wargame teams can help to achieve this training through command and joint staff level wargaming- testing blue capabilities to expose vulnerabilities. Focusing wargames on information warfare could not only help to identify gaps, but also help to sensitize military organizations and allies to the kind of effects we can expect to experience- helping the U.S. in preparing for potential future conflict. Doctrine highlighting the importance of wargaming in the information domain could be the genesis of service-wide change needed to launch the USAF into *planning* for next generation warfare, on par with our adversaries.

Deterrence by Denial. The information domain is an attractive tool to our adversaries because it's currently viewed as an available operating space. USAF information operations doctrine should focus on deterrence by denial. With our interagency collaboration, hardening of networks, consistent messaging, and efforts to combat disinformation, the adversary will not only find difficulty in operating in this contested environment, but find its information warfare efforts to be *costly and ineffective*.

The U.S. must raise the stakes for our adversaries to choose to fight in the information domain, which doctrine can address. Our adversaries' firewall and tight grip on its domestic narrative presents challenges to the United States' ability to contest the grip our adversaries have on the information domain, however, it is not impossible.[12] The U.S. must focus efforts on breaching

---

[10] Hodgson, Quentin E., Cyber Threats to Canada's Defence Infrastructure. Santa Monica, CA: RAND Corporation, 2023.
[11] Harold, Scott W., Nathan Beauchamp-Mustafaga, and Jeffrey W. Hornung, Chinese Disinformation Efforts on Social Media. Santa Monica, CA: RAND Corporation, 2021.
[12] Harold, Scott W., Nathan Beauchamp-Mustafaga, and Jeffrey W. Hornung, Chinese Disinformation Efforts on Social Media. Santa Monica, CA: RAND Corporation, 2021.

this virtual iron curtain and reaching the populations of Russia and China, thereby denying them the ability to control their populations through a government-controlled filter. Doctrine must promote U.S. attempts to fight back, challenging tyrant regimes and promoting human rights in adversary populations, while showing these efforts will not go unmatched.

In closing, the rapidly evolving information domain has made it difficult for a massive organization like the Department of Defense and subordinate services to grasp and reflect in doctrine. However, if the U.S. plans to maintain its role as the world superpower, we must alter our way of thinking and modernize, and it must happen now. With the role of social media, cyber, and AI changing at record speeds, our doctrine must reflect this changing environment and ensure whole of government collaboration is the norm. Current doctrine defines concepts well, but leaves too much room for interpretation, resulting in ad hoc and disjointed operations across the DoD. With the brilliant minds it employs, it is clear to me the USAF is the right candidate to lead this change.