The Iatrogenic Paradox

When Information Operations Undermine Strategic Objectives

By Daniel Eerhart

INTRODUCTION

Shortly following the traumatic events of September 11, 2001, the U.S. military entered Afghanistan to topple the Taliban government and dismantle al-Qaeda, costing the United States over $2 trillion and 2,324 American military lives.[1] Counterinsurgency doctrine served as the core strategy in Afghanistan and attempted to win "hearts and minds" to reduce popular support for the Taliban.[2] Despite two decades of advanced information operations integrated into tactical successes, the Taliban's strength grew from approximately 45,000 personnel in 2001 to a current reported strength of 164,918 in 2024.[3] The alarming iatrogenic impact of America's most protracted war demands reevaluating the U.S. military approach to information operations, particularly the concept of iatrogenic influence, where information operations produce outcomes contrary to their intent. As U.S. policymakers grapple with their strategies in a global information war, evaluating historical roles and responsibilities will help illuminate the most efficient areas to concentrate resources. This paper argues that ineffective and often counterproductive military information operations necessitate a fundamental reassessment of their role within U.S. strategy. The iatrogenic outcomes of the Afghanistan war demonstrate that rather than serving as a panacea for influence, military information operations must be narrowly focused, carefully integrated with non-military efforts, and isolated against strategic backlash.

The lessons drawn from Afghanistan extend beyond counterinsurgency and raise questions about how the United States should engage in the global information environment against state and non-state actors alike. Throughout history, propaganda, information, and influence have been necessary tools of war. However, the formalized existence of information operations organizations within the military is relatively new. Historically, non-military actors have led operations to inform and influence populations. As the military

Daniel Eerhart is a Psychological Operations Officer and Research Scientist for the Army Cyber Institute at West Point. With a Master's Degree from the University of California, Los Angeles (UCLA), he completed the USSOCOM Cybersecurity Professionals Program, and holds numerous professional/graduate certifications in Cybersecurity and Data Analytics.

transitions away from the counterinsurgency strategies of the Global War on Terror (GWOT) and develops expertise for large-scale combat operations (LSCO), it should reevaluate the utility and limitations of military information operations. This paper examines the U.S. information operations landscape and assesses current capabilities. Then, the role of information operations and iatrogenic influence is examined in the context of the war in Afghanistan to explore whether military information operations are a viable tool for achieving strategic objectives. This paper offers recommendations to refine the role of military information operations and better integrate U.S. information efforts to reduce iatrogenic influence and maximize effectiveness. The analysis aims to generate greater effectiveness and strategic impact in the information domain by addressing the limitations of military information operations.

INFORMATION OPERATIONS: CONCEPTS AND CHALLENGES

The Department of Defense (DOD) defines Information Operations within Joint Publication 3-13 as "the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries."[4] This definition emphasizes that information operations occur during military operations and have a specific purpose to support military objectives. Successful information operations rely upon the effective integration of information-related capabilities. While integrating multiple information-related capabilities generates a comprehensive information strategy, this analysis primarily focuses on the capabilities that involve disseminating an information product (such as leaflets, radio broadcasts, or internet posts) to a target audience. Joint Publication 3-13 outlines fourteen information-related capabilities.[5] The following

Central Command Area of Responsibility (Mar. 21, 2003) Coalition aircraft dropped leaflets urging Iraqi personnel to stay clear of military operations. Leaflets also laid out the consequences of such actions in an effort to ensure local civilian populations are properly informed.

are particularly relevant, as they frequently involve the dissemination of products or influencing the transfer of information:

1. Electronic warfare: using the electromagnetic spectrum to disrupt or degrade adversary communications and systems.[6] During the war in Ukraine, military forces have jammed adversary Global Positioning System (GPS) signals to disrupt the ability to guide precision munitions, such as the Excalibur GPS-guided artillery shells and High Mobility Artillery Rocket Systems (HIMARS).[7]
2. Cyberspace Operations: activities conducted in the cyber domain to achieve objectives, often grouped into offensive, defensive, and Department of Defense Information Network (DODIN).[8] Prior to the Russian invasion of Ukraine, hackers disrupted the Viasat communication network in an attempt to provide a tactical advantage to invading forces.
3. Military Information Support Operations (MISO): activities that seek to influence a target audience's perceptions, attitudes, and behaviors.[9] Sometimes referred to as Psychological Operations. During the 2003 U.S. invasion

of Iraq, psychological operations forces used leaflets and radios to persuade Baath Party fighters to surrender.

4. Civil-Military Operations: operations that foster a relationship between military and civilian populations, governments, or organizations.[10] Civil affairs soldiers deployed to Africa have provided training and medical care to the local populations.[11]
5. Military Deception: involves deliberately misleading adversaries to influence their decision-making.[12] During World War II, British intelligence officials led *Operation Mincemeat*, which allowed Spanish soldiers to discover a fictitious British officer as part of plans to disguise the 1943 Allied invasion of Sicily.[13]
6. Public Affairs: activities to provide public audiences with accurate and timely communication of military operations and objectives.[14] Following the capture of Saddam Hussein, U.S. military officials spoke with reporters and held a press conference to discuss the capture.[15]

Within information operations, there is potential for an operation to result in iatrogenic influence, which draws from the medical term of iatrogenesis, where the effects of disease treatment create adverse outcomes that are often worse than the disease.[16] For example, in 2002, the U.S. military established Camp X-Ray in Guantanamo Bay, Cuba.[17] During the camp opening, U.S. military public affairs took photos of the detainees in orange jumpsuits, surrounded by barbed wire with their eyes and ears covered.[18] The intent for the deliberate release of the photos was to build trust within the international community that the United States was treating prisoners within the guidelines of the Geneva Convention.[19] However, the photos spurred outrage throughout the world. Throughout the GWOT, violent extremist organizations used the Camp X-Ray photos as evidence of American cruelty.[20] Had the public affairs officials understood the indicators of iatrogenic influence, they may have modified their communication plan. Table 1 summarizes key indicators of iatrogenic influence, providing practitioners with a framework to identify potential risks.

Two US Army Military Police escort a detainee to a cell at Camp X-Ray, Guantanamo Bay Navy Base, Cuba, the holding facility for detainees held at the US Navy Base during *Operation Enduring Freedom*.

Within information operations, iatrogenic influence primarily occurs when there is a lack of credibility within the target audience, a lack of planning by disseminating forces, or information fratricide contradicting other messaging. Information fratricide occurs when different information-related capabilities inadvertently conflict, undermining each other's effectiveness.[21] For example, if a leaflet asks the audience to call a phone number, then the Soldiers jam phones. Similarly, a MISO campaign to counter adversary propaganda may inadvertently amplify adversary messages if it fails to anticipate how the target audience processes information, particularly among broad general audiences. Cultural competence and an awareness of the iatrogenic influence indicators enable commanders to reduce the risks of negative externalities if they understand the information environment rooted in examples of iatrogenic influence.

The information-influence relational framework is a core component of information operation planning, which provides a structured approach to

shaping audience behavior.[22] Information Operations practitioners perform the integrated application of information-related capabilities within the information-influence relational framework to identify a target audience, cultivate an understanding of how the target audience receives information, and utilize information-related capabilities to achieve the desired behavior. The information-influence relational framework serves as a tool for planning and supporting all phases of military operations. It uses designated means and ways to achieve an end through the influence of a target audience.

Information operations primarily serve as a means of influencing, disrupting, corrupting, or usurping adversary decision-making. Within military planning, there is frequent consideration of the "OODA Loop," a decision-making process that involves observing the operating environment,

Table 1: Iatrogenic Influence Indicators
(First Presented by Daniel Eerhart at Post-9/11 Lessons Learned Conference)

Indicator	Description	Risk
Broad General Audience	The operation targets a broad, general audience rather than a specific group, which makes performing target audience analysis difficult.	The messages may be misrepresented or misinterpreted, resulting in rejection, resentment, confusion, or opposition.
Inconsistent Delivery Mechanism	The dissemination method is inconsistent with the desired behavior or outcome.	The target audience may question the nature of the messages and perceive them as superficial.
False Cultural Lens	The operation's disseminators view products through their own cultural lens rather than the target audience's perspective.	Messages may inadvertently provoke backlash or negative emotions for violating the target audience's cultural norms, beliefs, or values.
Inconsistent Messaging/ Information Fratricide	Inconsistent or contradictory messaging among various stakeholders that are supposed to be mutually supportive.	Undermines credibility and leads to skepticism or confusion about messaging and the messengers.
Historical Mistrust	The target audience has a history of mistrust or negative perceptions towards the source.	Messages are more likely to be dismissed or viewed skeptically, exacerbating existing tensions.
Deceptive Tactics	The campaign relies on deception, disinformation, or manipulation.	Loss of credibility and trust if deception is uncovered; adversaries can exploit to discredit the campaign.
Ethical and Moral Concerns	Tactics or messages raise ethical or moral concerns.	It provokes outrage and condemnation, undermining the operation's legitimacy and enabling adversary propaganda.
Insufficient Feedback Mechanisms	There are no mechanisms to gather and respond to feedback from the target audience.	Adverse reactions may go unnoticed and unaddressed, allowing iatrogenic influence to grow.
Over-Simplification of Issues	Campaign oversimplifies complex issues.	They are perceived as superficial or patronizing, failing to resonate and potentially reinforcing adversary narratives.
Dynamic and Rapidly Changing Environment	The environment is dynamic and rapidly changing.	Messages can become outdated or irrelevant, perceived as incompetent or detached from current realities.

Figure 1: Normalized Search Engine Results 2017 - 2018

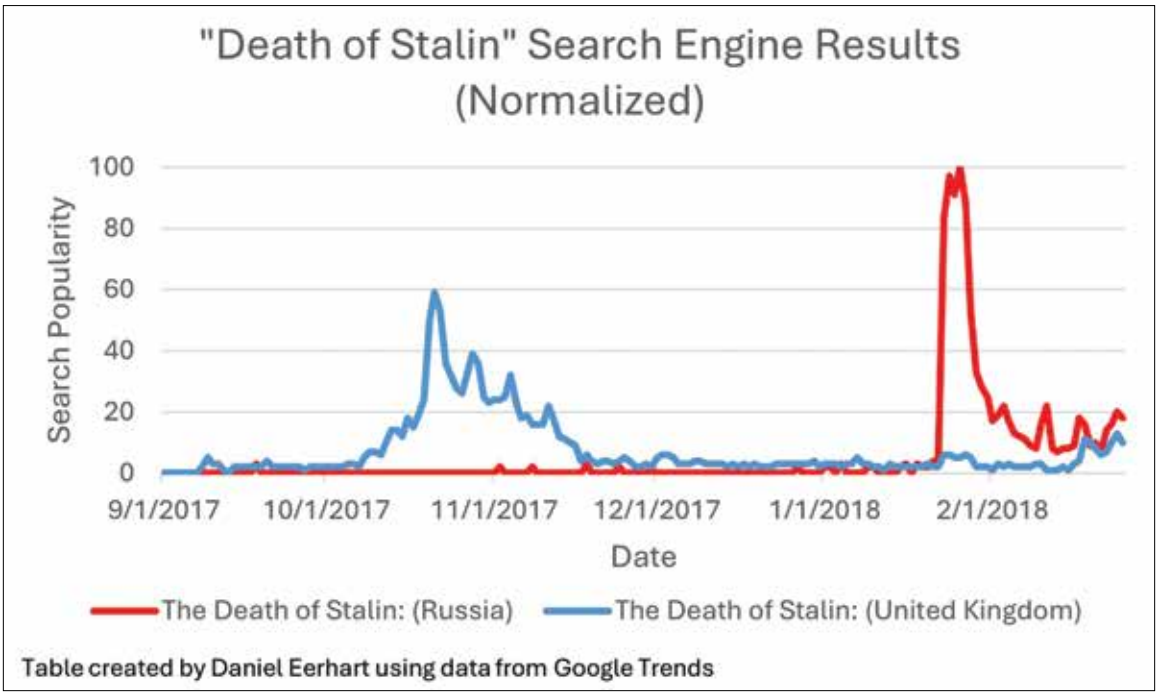


Table created by Daniel Eerhart using data from Google Trends

orienting observations, deciding on an optimal course of action, and then acting on the course of action.[23] By integrating an operational option that does not involve the tactical application of force, Commanders gain an alternative for disrupting an adversary's OODA Loop, mitigating the risk to its tactical forces. The rise of ubiquitous digital communication platforms has transformed the application of information operations and transitioned controlled information flows to cascading networks.

A CASE STUDY IN IATROGENIC INFLUENCE: *THE DEATH OF STALIN*

An example of iatrogenic influence occurred in 2018 when the Russian government banned the satirical film *The Death of Stalin*. The film had low public awareness among the Russian people, had minimal promotion, and only anticipated a few screenings. On January 22, 2018, the Russian Ministry of Culture held a private movie screening for government and cultural figures.[24] Just before the movie's scheduled release on January 25, 2018, the Ministry of Culture revoked the movie's distribution license and banned the movie from public screenings.[25] The Russian government used a multi-medium approach in their attempt to decrease viewership of the film, including official statements to the press, critical commentaries, newspaper articles supporting the ban, and use of social media influencers on Vkontakte (VK) and Twitter.[26]

Despite being released in the United Kingdom in October of 2017,[27] search engine data indicates that the movie had very little publicity in the United Kingdom and almost no publicity within Russia. Search engine analytic data indicates that on January 23, 2018, when the government implemented the ban, the search engine interest experienced a dramatic spike, reaching 83 on the normalized scale (approximately 27 times higher than the previous day's value of 3). On January

26, the search interest rose again three days later, increasing to 100 on the normalized scale. This spike represents an interest level 33 times higher than the pre-ban value of 3. The Russian government's efforts to suppress interest in the film fueled public curiosity and piracy. One theater, the Pioneer Cinema in Moscow, played the movie despite the ban.[28]

Even for the Russian government, with complete control over dissemination methods and a synchronized cultural background, the iatrogenic effect of the ban far surpassed any fallout that may have occurred through allowing the film to show or limiting the showing license. One critical lesson within the information environment is that inaction is always an option. It can often be the most prudent approach to prevent cascading effects, even if it conflicts with a leader's desire to act. Achieving an information advantage necessitates a long-term strategy, where accepting a temporary setback can be preferable to enduring a prolonged and comprehensive failure.

The Russian movie ban is just one example of iatrogenic influence, where information operations inadvertently counteract the desired behavior. Throughout the GWOT, coalition forces repeatedly misstepped in the information environment, unable to achieve success in the war for "Hearts and Minds." Since September 11, 2001, the U.S. government has rapidly and meaningfully expanded its capabilities to operate within the information environment.[29] Military and non-military organizations keep expanding their capabilities to engage in the global "information war," even though such a conflict cannot be decisively "won." The information environment functions more like a stock market, with infinite potential participants and no clear signal of victory. Instead, state actors should concentrate on providing consistent and persistent influence while maintaining the ability for short, rapid spikes supporting tactical objectives. The military provides necessary short spikes, while non-military capabilities provide the enduring global influence. Achieving this end state requires an inventory of military and non-military information operations assets and clearly distinguishing areas for each asset's focus. The Russian government's experience illustrates how iatrogenic influence can amplify poorly calibrated information operations. The case study underscores the necessity for military and non-military organizations to refine their operational approaches to meet the challenges of a complex and dynamic information environment.

THE EVOLUTION OF NON-MILITARY INFORMATION OPERATIONS

The Russian government's difficulties during its ban on the Death of Stalin highlight the importance of well-planned information operations. As long as the military has existed, it has had a vested interest in competing in the information environment to enable commanders an advantage in battle, while non-military information operations have historically shouldered the responsibility for influencing populations. The Committee on Public Information (CPI), established during World War I, was the first non-military U.S. governmental organization concentrating on propaganda, disinformation, and influence activities.[30] Established in 1917 under President Woodrow Wilson, the CPI had domestic and foreign branches supporting and enabling U.S. efforts during World War One.[31] Domestically, the CPI generated public support for the war using speeches, films, leaflets, and posters to spread pro-American messages.[32] The foreign branches focused on Europe and Latin America, using similar mediums to build support for U.S. war efforts.[33] Despite serving as a temporary organization, the CPI was the U.S. government's first attempt at non-military information operations.

In 1940, President Franklin D. Roosevelt, concerned about intelligence gaps as the Second World

War loomed, directed General William Donovan to draft plans for an intelligence service based on the British MI6.[34] Donovan recommended establishing a single agency capable of performing specialized operations, including disinformation activities. In June 1942, President Roosevelt established the Office of Strategic Services with a Morale Operations Branch specializing in psychological warfare and propaganda being established in January of 1943.[35] While CPI primarily utilized overt propaganda to build popular support for American ideals openly, the OSS specialized in more clandestine methods such as spreading disinformation, forging documents, misattributed leaflets, and fake broadcasts.[36] The OSS covert operations complemented the Office of War Information's (OWI) more overt efforts and drove the potential for information operations into new territory.

After the disbanding of the OSS in 1945, the Central Intelligence Group became the immediate successor to centralized U.S. Intelligence Efforts.[37] Later, in 1947, the Central Intelligence Agency was established and adopted the OSS's previous roles in covert operations.[38] The CIA adopted psychological warfare and information operations capabilities, such as the establishment of Radio Free Europe/Radio Liberty (RFE/RL).[39] RFE/RL was established by the CIA in 1949, targeting Soviet satellite states and the Soviet Union to counter the appeal of communism.[40] In addition to radio broadcasts, the operations included leaflet drops through meteorological balloons, rallies, rumors, and movies as the CIA continued to evolve its information operations capabilities.[41]

President Dwight Eisenhower established the United States Information Agency to complement the CIA's covert operations, focusing on overt public diplomacy and influence campaigns.[42] The USIA aimed to counter the spread of communism globally by disseminating messages that told the American story to the world. Building a positive impression of the United States involved the establishment of Voice of America (VOA).[43] This pro-U.S. radio broadcast service provided uncensored news in regions where the governments may have restricted access to information.[44] In addition to radio, the USIA produced magazines, films, and pamphlets tailored for foreign audiences while providing traveling libraries of American literature and educational materials.[45]

Following the collapse of the Soviet Union in 1991, members of Congress began to question the utility of the USIA. The Foreign Affairs Reform and Restructuring Act of 1998, Division G of the Omnibus Consolidated and Emergency Supplemental Appropriations Act dissolved the USIA, with broadcast services transitioning to the Broadcasting Board of Governors, and the U.S. Department of State absorbed its remaining functions under the Undersecretary of State for Public Diplomacy.[46] The Undersecretary of State for Public Diplomacy leads overt U.S.-attributed information operations, providing a range of methods from digital media through traditional television and radio broadcasts and in-person exchanges like the Fulbright program and international visitor leadership program.

In 2011, President Barrack Obama issued Executive Order 13584 to expand the State Department's information Operations capabilities and establish the Center for Strategic Counterterrorism Communications (CSCC).[47] The center's mission was to support communication activities against violent extremism and terrorist organizations. In 2016, the organization was renamed the Global Engagement Center, and in 2017, the center's mission expanded to address foreign propaganda, misinformation, and disinformation operations.[48] Prior to its closure on December 23rd, 202, the center had five interconnected areas:[49]

1. Analytics and research
2. International partnerships
3. Programs and campaigns
4. Exposure

5. Technology assessment and engagement

During the COVID-19 pandemic, the Undersecretary of State for Public Diplomacy led the U.S. international effort to address disinformation about vaccine safety and influence global health efforts by disseminating factual information through embassies and international broadcasts.[50] In 2018, the Broadcasting Board of Governors, which oversaw the U.S. broadcasting entities, was renamed the United States Agency for Global Media.[51] Despite its roots in the CIA and State Department, the USAGM is an independent government organization that does not have any requirement to synchronize or coordinate with any other U.S. information operations-related agency. While its independent status lends credibility to its journalist qualifications, it remains a U.S. government organization operating within the information sphere without guidance or synchronization with other information-related organizations.

Outside the State Department, the Office of the Director of National Intelligence oversees the U.S. government's most significant non-military information operations capabilities. The Office of the Director of National Intelligence oversees the U.S. government's intelligence agencies.[52] Organizations with roles in Information Operations, such as the Central Intelligence Agency, National Security Agency, and Federal Bureau of Investigation, receive oversight from the ODNI. Additionally, the ODNI maintains five centers that have roles in the information environment. The five centers are:[53]

1. National Counterproliferation and Biosecurity Center
2. National Counterintelligence and Security Center
3. National Counterterrorism Center
4. Foreign Malign Influence Center
5. Cyber Threat Intelligence and Integration Center

Each ODNI center plays a role in the information environment. The NCTC publishes alerts and warnings, the NCSC performs outreach and awareness campaigns, the NCBC discourages and deters the acquisition of WMD resources, the CTIIC influences cyber threat actors, and the FMIC exposes and deters foreign influence threat actors.

Non-military government agencies shoulder the most considerable burden of information operations, leading efforts in both overt and covert operations. The immense resources devoted to influencing foreign populations and protecting U.S. citizens from foreign malign influence results in consistent and persistent messaging in the information environment to support U.S. national objectives. However, during times of crisis and conflict, the U.S. government turns to DOD to lead information operations in support of military objectives. While non-military agencies have led U.S. government information operations in both overt and covert capacities, times of crisis or conflict may necessitate the supplanting of civilian agencies by military information operations. DOD's primacy in areas of conflict is primarily due to the inability of civilian agencies to reach target audiences or have any immediacy in performing influence activities.

STRUCTURE AND CAPABILITIES OF MILITARY INFORMATION OPERATIONS

While non-military agencies lead U.S. information operations in most contexts, DOD's structure and capabilities require it to dominate during crises or conflicts. This section examines the organization and capabilities of military information operations. DOD maintains eleven Combatant Commands, each led by a four-star General and supported by Service Component Commands representing the various military branches.[54] For example, U.S. Central Command (CENTCOM) has the service component commands of U.S. Army Central (ARCENT), U.S.

Naval Forces Central Command (NAVCENT), U.S. Air Forces Central Command (AFCENT), U.S. Marine Corps Forces Central Command (MARCENT), U.S. Special Operations Command Central (SOCCENT), and U.S. Space Forces Central (SPACECENT).[55] Despite each service having a different lexicon regarding operations in the information environment,[56] each service maintains a deputy operations officer responsible for overseeing MISO, operations security, data science, and operations research to support the commander's objectives.[57]

Beyond the geographically aligned combatant commands, three functional combatant commands maintain significant information operations capabilities.[58] Under U.S. Special Operations Command, the Joint MISO Webops Center (JMWC) conducts internet-based MISO.[59] U.S. Strategic Command maintains the Joint Information Operations Warfare Center (JIOWC),[60] which coordinates and executes information operations at the strategic level in support of the Joint Chief of Staff to "meet combatant command information-related requirements, improve the development of information-related capabilities, and ensure operational integration and coherence across combatant commands and other DOD activities."[61] For instance, the Joint MISO WebOps Center conducts internet-based influence campaigns to counter adversary disinformation. At the same time, the Joint Information Operations Warfare Center supports strategic-level operations by integrating information-related capabilities across multiple domains. Lastly, there is the U.S. Cyber Command, which is building up the Theater Information Advantage Detachments.[62]

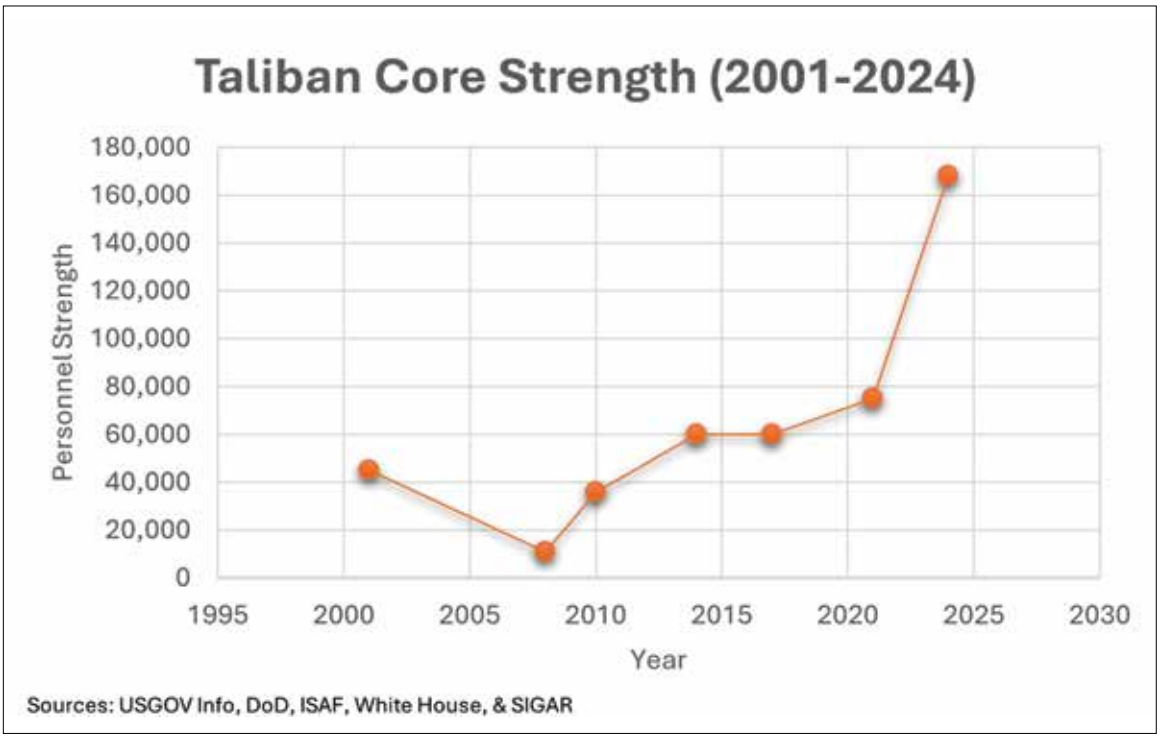
In February of 2024, the Army Force Structure Transformation Plan approved the creation of three TIADs.[63] One TIAD will support the European theater, a second will support the Pacific region, and the third will serve as an interterritorial detachment under the U.S. Army Cyber Command.[64] The TIADs combine information-related capabilities, such as cyber, electronic warfare, data system engineers, information operations, intelligence, and psychological operations, into a cohesive team capable of obtaining an information advantage.[65] The establishment of TIADs reflects a recognition of the increasing importance of integrated information capabilities in modern conflict. These detachments aim to give commanders a decisive information advantage in complex operational environments by consolidating cyber, intelligence, and psychological operations under a single framework.

As military information capabilities continue to expand, the question remains about what role the military should play within the information sphere. The military operates under strict legal frameworks that necessarily limit the ability to perform activities domestically. In the international realm, the military strictly follows international law and maintains domestic oversight of its activities. The result is an ethical military structure that performs its duties with restraint and can account for its activities publicly. What role should the military play in the grey zone of information operations, and can it even compete against adversaries not abiding by the same moral obligations? As the military continues to expand its information-related capabilities, its role in the information environment requires reevaluation. The following section explores the strategic and operational implications of the military's role in the information environment, asking whether the end of the GWOT is a signal to transition the military's information operations responsibilities back to civilian agencies.

REEVALUATING THE ROLE AND RELEVANCE OF MILITARY INFORMATION OPERATIONS

While DOD has robust structures capable of operating within the information environment, their effectiveness and relevance in modern conflicts require examination. This section reevaluates the role of military information operations in light of

Figure 2: Taliban Personnel Strength 2001 - 2024



lessons learned during the GWOT. The presence of robust non-military information operations capabilities for covert and overt operations begs the question: What role should military information operations play? Throughout the GWOT, United States and coalition military information operations actors shouldered the primary burden of waging an information war against violent extremist organizations. Despite numerous tactical successes, the Taliban's strength grew from approximately 45,000 personnel in 2001[66] to 60,000 in 2014[67] and 75,000 by 2021,[68] when they regained control of Afghanistan. The unfortunate reality of the data seems to be that the military is ineffective or incapable of competing with violent extremist organizations with the speed and granularity required to wage effective information operations. Violent extremist organizations operate with agility, leveraging local knowledge and decentralized networks to disseminate propaganda.

In contrast, military information campaigns often lack the speed and granularity to respond effectively to such dynamic threats. The U.S. war in Afghanistan had its iatrogenic effect on the Taliban, where they had more personnel and resources at the end of the war than at the beginning. This section explores three potential approaches: expanding military information operation capabilities, dissolving them in favor of non-military assets, or focusing on a specialized and refined mission set.

With evidence indicating that Al-Qaeda has experienced a similar iatrogenic boost in personnel followership, aggregating major affiliates in Syria, Yemen, and throughout Africa,[69] the question remains: How is it possible that twenty years of war increased the strength of the groups we set out to destroy? The negative externalities from years of iatrogenic influence have outweighed the

tactical successes achieved by coalition members in Afghanistan. The iatrogenic effects observed in Afghanistan highlight the need to reevaluate the military's role in information operations and refine its approach to avoid negative externalities.

The first option would be to dramatically expand U.S. military information operations capabilities to meet the demands of the global information war. This option would argue that the inability to influence populations in Afghanistan effectively was due to the lack of resources. As such, the answer is to increase resources to meet the challenge, which suggests that there is a correlation between budget and effectiveness. A 2012 report from RAND assessed the effectiveness of information operations themes in Afghanistan, and determined that all nine themes either had mixed effectiveness or were ineffective, despite annual changes in budget allocation.[70] Proponents of this option are misunderstanding the impacts of the GWOT. The most prominent iatrogenic influence effects occurred due to coalition forces lacking legitimacy with local populations and not understanding the cultural intricacies of Afghan society, that they are nonhomogenous and more closely identify with their tribe, ethnicity or region.[71] Western militaries could not compete with violent extremist organizations' dynamic and asymmetric influence capabilities because they could not understand their audiences as quickly or rapidly undergo the bureaucratic processes required to disseminate products. Occasionally, military forces attempted to expedite bureaucratic processes to increase dissemination speed, but this only exacerbated the lack of cultural knowledge and multiplied the impact of iatrogenic influence.

One example of this occurred in Parwan province, Afghanistan, in 2017. U.S. military forces propped leaflets with a white dog intended to represent the Taliban.[72] The white dog had the Shahada, the Muslim call to prayer, printed upon it.[73] The use of a Muslim symbol of faith on a dog deeply offended the local populace, and a Taliban suicide bomber later detonated outside an American base, claiming it was retaliation for the leaflet. Such a significant oversight would not have been prevented by simply increasing budgets or streamlining approval processes. The problem was that Western military actors were not the right actors to attempt to transition citizens away from the Taliban ideologically. In these situations, the widespread application of information operations is not only a waste of resources but is often counterproductive and should not be engaged in at all. Expanding information capabilities without addressing underlying issues risks amplifying existing inefficiencies and perpetuating iatrogenic effects.

The second option is to dissolve all information operations capabilities and rely entirely upon non-military assets for influence. The vast amount of non-military resources lends credibility to the argument that military capabilities are now transitioning into the realm of superfluous. This view would ignore the historical necessity for information operations and would be a flawed emotional reaction to the war in Afghanistan. While non-military agencies maintain significant capabilities, they lack the operational immediacy and scalability that the military provides during conflict. Eliminating military information operations would create a critical capability gap, exacerbating difficulties. All major militaries participating in the Great Power competition maintain an information operations capability and apply it where necessary. To dissolve the military's ability to perform these operations would unnecessarily give adversaries a competitive advantage and disregard the historical role information has played in the conflict. Furthermore, it would ignore the instances of success in Afghanistan, which occurred primarily through face-to-face communication. In conflict zones, the military has greater access and placement in areas that enable effective influence.

Information and psychological operations have been critical in operational success in U.S. military

history. While propaganda, influence, and information operations have played significant roles throughout the history of the United States, the U.S. military had no formalized capability prior to World War I.[74] Despite President Woodrow Wilson's opposition to the military's use of propaganda, a small section called the "Propaganda Section" printed 5.1 million leaflets during the war and had 3 million disseminated by volunteer pilots or hydrogen balloons.[75] Interrogations indicated the leaflets were effective at eroding adversary morale and increasing surrenders. However, the War Department dissolved the section after the war.[76]

During World War II, the military sought to relearn the lessons of influence, and the Psychological Warfare Branch used leaflets and radio broadcasts to demoralize adversaries and increase surrender rates.[77] Military information and psychological operations continued to function ad hoc throughout American history until July 1953, when the military established a permanent psychological operations capability.[78] A historical evaluation of information's use in military operations makes it clear that the military is necessary and effective in four areas:

- Defection/Surrender Campaigns: These operations target enemy forces, aiming to persuade them to abandon their positions, defect, or surrender.
- Civilian Protection/non-interference: These operations target civilian populations to persuade them to avoid conflict zones and not interfere in military operations. They often involve warnings about military action and instructions for safe evacuation.
- Enemy Demoralization: These operations seek to weaken the will and cohesion of enemy forces or disrupt their perceptions of the battlefield. Highlighting hardships or tactical losses is a common theme during these operations.
- Boosting Friendly Morale: These operations, often conducted by a public affairs officer, emphasize mission success and motivate friendly forces. Recognition of achievement and reassurance of progress toward mission success are common.

Observing these four critical mission areas leads to the third and best option for military information operations to specialize and excel in a limited mission set. Reviewing the Mission-Essential Task Lists (METL) for any maneuver organization will reveal a standard list of tasks that the unit refines and perfects to maintain its effectiveness on the battlefield. Conducting a movement to contact, conducting an attack, and conducting an area defense are typical tasks that any maneuver organization within the U.S. military will recognize and understand how to execute. However, a similar or comparable task list must be more present in the manuals and task list of influence actors. Just as maneuver units perfect a defined set of mission-essential tasks, information operations units should focus on mastering their core task, specifically within LSCO. Expertise in baseline skills enables the military to adapt and improvise during unexpected situations. By focusing on well-defined essential tasks and developing deep expertise in these areas, the military can ensure its information operations remain adequate and relevant in the needed areas. Rather than dominating all areas of influence, a limited approach focusing on LSCO helps achieve the specialization needed within the military.

RECOMMENDATIONS FOR MILITARY INFORMATION OPERATIONS

After identifying the most effective roles for military information operations, the next priority is to realign resources to meet the needs of its role. Four specific recommendations provide the most effi-

cient strategy to maximize operational effectiveness and mitigate the iatrogenic influence. As the U.S. military adapts its forces to concentrate on LSCO, it must likewise adapt its information forces to meet the challenges of a modern battlefield. The Western world must avoid repeating the mistakes of Afghanistan, where twenty years of information operations inadvertently increased ideological support for the Taliban. In preparation for the next conflict, the United States should adapt its information capabilities to maximize effectiveness and reduce the risk of iatrogenic influence.

First, non-military organizations must integrate and generate products based on their experience and spheres of influence rather than relying on military information and influence capabilities to lead global information operations. Countering violent extremist propaganda requires a long-term focus with specialized expertise that exists within non-military organizations, such as the National Counterterrorism Center. Their ability to integrate intelligence and influence efforts ensures precision while maintaining credibility with target audiences. The National Counterterrorism Center is a repository of intelligence and information about terrorist threats. Their Joint Operations Center should serve as the center of U.S. efforts to counter the influence of violent extremist organizations. However, they should concentrate only on counterterrorism influence and avoid creeping into different mission sets. Specific and concentrated efforts with the highest possible level of precision will produce the most significant information advantage for the United States, avoiding generalized approaches in the information environment, which is key to reducing incidents of iatrogenic influence.

Second, military information missions should align with the most historically effective ones. Rather than wasting resources in areas where Western militaries are incapable of competing or lacking legitimacy, concentrated expertise allows information actors to provide the most valuable benefits to their military commanders. For example, during World War II, the U.S. military successfully used leaflets to encourage mass defections among enemy forces. The surrender campaigns were well suited to the military's capabilities. Advocating for improving performance with ineffective military mission sets, such as persuading civilians to align with the United States ideologically, ignores the reality that some missions are inherently unachievable. However, there is no point in optimizing a mission set that should not exist, and the ideological persuasion of civilians away from the Taliban and toward the United States was a mission with no chance of success. The military must focus on mission sets that can be achieved in short deployments and utilize tactics uniquely available to them, such as face-to-face communication.

Third, the U.S. State Department should absorb the U.S. Agency for Global Media (USAGM). The Office for Public Affairs and Public Diplomacy is the most significant asset in the U.S. arsenal for performing overt foreign information activities. USAGM simultaneous broadcasting capabilities must be synchronized with public diplomacy efforts to maximize efficiency and effectiveness. USAGM's overt affiliation with the U.S. government inherently limits perceptions of neutrality and is not mitigated by claims of independent status. Merging with the State Department streamlines resources and reduces redundancy. Any perceived loss of credibility from moving to the State Department is negligible.

Fourth, clarify duties and responsibilities for all information operations organizations. With so many organizations participating in the information environment, senior leadership must specify and distinguish which efforts belong to each agency. Clear role delineation would ensure a unified approach, reducing information fratricide and enhancing operational efficiency. Eliminate wasteful overlap and reduce information fratricide

by hyper-focusing organizational lines of effort. U.S. Special Operations Command has done this well by designating its JMWC as its lead effort for internet-based MISO.[79] Other organizations can save time by outsourcing learning the legalities and intricacies of internet-based MISO to the JMWC.

Additionally, other organizations know where to go for synchronization, and the JMWC can develop expertise in its singular mission. The level of mission granularity demonstrated by the JMWC must permeate the other military and non-military organizations to eliminate waste and identify gaps. By implementing these recommendations, the United States can manage the execution of effective and precise information operations.

CONCLUSION

The recommendations of this paper aim to refine the roles and responsibilities of military information operations to maximize their effectiveness and minimize the risk of iatrogenic influence. Lessons from the GWOT, notably the iatrogenic surge in Taliban forces, illustrate the need to recalibrate the U.S. approach in the information environment. The military should exercise restraint in the information environment where it lacks a competitive advantage and instead focus primarily on tasks where it has historically excelled and supported operational missions, such as surrender appeals, civilian non-interference, and enemy demoralization. While these mission sets do not entirely encapsulate the U.S. military's influence abilities, they are optimized for deployment timelines and utilize the unique access and placement of military forces.

This paper does not advocate for the United States to abdicate its responsibilities to compete in the information environment. On the contrary, precise expertise in a few missions enables the military to execute its responsibilities efficiently and exposes information gaps for other agencies to fill. Strategic information operations require consistent and persistent messaging over long durations. In contrast, military deployments typically last six or nine months, barely enough time to approve a single MISO plan. The military's structural limitations make it ill-suited for consistent long-term messaging and stand in stark contrast to the multi-year assignments of State Department public affairs officers or CIA officers. Rather than haphazardly attempting to force long-term planning upon short-term deployers, the military should concentrate its efforts on achievable missions within their timeline.

The United States can leverage all agencies' strengths for a more comprehensive information plan by aligning the military with achievable goals and enhancing collaboration with civilian agencies. Centralizing dissemination methods within major agencies, such as the USAGM within the State Department, reduces the risks of information fratricide and enables narrative synchronization at the national level. While the military hones its expertise in core mission sets for LSCO, non-military agencies must simultaneously enhance their capabilities to disrupt adversary OODA loops, ensuring a coordinated and unified approach to the information environment.

As technology advances, the information environment will perpetually become more complex. The recommendations presented provide a pathway towards a strong information foundation and more significant strategic impact. The United States can maximize its ability to influence target audiences to support national security objectives by optimizing military and non-military missions to fit their strengths and limitations. Failing to learn from historical missteps risks cascading consequences in an increasingly interconnected world, where the stakes of influence operations are higher than ever. PRISM

Notes

[1] "Human and Budgetary Costs to Date of the U.S. War in Afghanistan, 2001-2022 | Figures | Costs of War," The Costs of War, accessed December 17, 2024, https://watson.brown.edu/costsofwar/figures/2021/human-and-budgetary-costs-date-us-war-afghanistan-2001-2022.
[2] Seth G. Jones, "Counterinsurgency in Afghanistan: RAND Counterinsurgency Study -- Volume 4" (RAND Corporation, May 6, 2008), https://www.rand.org/pubs/monographs/MG595.html.
[3] Special Inspector General for Afghanistan Reconstruction (SIGAR), *Quarterly Report to the United States Congress, January 30, 2024*, 30, https://www.sigar.mil/pdf/quarterlyreports/2024-01-30qr-section2.pdf#page=30.
[4] U.S. Department of Defense, *Joint Publication 3-13: Information Operations*, (Washington, D.C.: Joint Chiefs of Staff, November 27, 2012), https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/12102012_io1.pdf.
[5] U.S. Department of Defense, *Joint Publication 3-13: Information Operations*, (Washington, D.C.: Joint Chiefs of Staff, November 27, 2012), https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/12102012_io1.pdf.
[6] U.S. Department of Defense.
[7] "Russian Jamming Leaves Some High-Tech US Weapons Ineffective in Ukraine," Stars and Stripes, accessed December 17, 2024, https://www.stripes.com/theaters/europe/2024-05-24/russian-jamming-high-tech-weapons-ukraine-13964032.html.
[8] U.S. Department of Defense, "Joint Publication 3-13 Information Operations."
[9] U.S. Department of Defense, "Joint Publication 3-13 Information Operations."
[10] U.S. Department of Defense, "Joint Publication 3-13 Information Operations."
[11] "US Civil Affairs Soldiers Build Partnerships in Guinea-Bissau," www.army.mil, November 25, 2024, https://www.army.mil/article/281467/us_civil_affairs_soldiers_build_partnerships_in_guinea_bissau.
[12] U.S. Department of Defense, "Joint Publication 3-13 Information Operations."
[13] "What Was Operation Mincemeat?," HISTORY, September 28, 2023, https://www.history.com/news/what-was-operation-mincemeat.
[14] U.S. Department of Defense, "Joint Publication 3-13 Information Operations."
[15] "THE CAPTURE OF HUSSEIN; 'We Got Him,' and Then a Call by American and Iraqi Officials for Reconciliation," *The New York Times*, December 15, 2003, sec. World, https://www.nytimes.com/2003/12/15/world/capture-hussein-we-got-him-then-call-american-iraqi-officials-for-reconciliation.html.
[16] David M. Garner, "Iatrogenesis in Anorexia Nervosa and Bulimia Nervosa," *International Journal of Eating Disorders* 4, no. 4 (1985): 701–26, https://doi.org/10.1002/eat.2260040427.
[17] Fiza Gul Rind, "Camp X-Ray: The War on Terror, Memorialization, and Architecture" (Carleton University, September 20, 2016).
[18] "Camp X-Ray: A Ghost Prison," *The New York Times*, August 31, 2014, sec. U.S., https://www.nytimes.com/interactive/2014/09/01/us/guantanamo-camp-x-ray-ghost-prison-photographs.html, https://www.nytimes.com/interactive/2014/09/01/us/guantanamo-camp-x-ray-ghost-prison-photographs.html.
[19] "20 Years Later, the Story behind the Guantánamo Photo That Won't Go Away | World News - The Indian Express," accessed July 8, 2024, https://indianexpress.com/article/world/guantanamo-bay-prison-first-prisoners-photo-united-states-7717159/.
[20] "The Costs of Unlawful US Detentions and Interrogations Post-9/11 | Human Rights Watch," January 9, 2022, https://www.hrw.org/news/2022/01/09/legacy-dark-side.
[21] Deen de Ronde, "Information Fratricide as a Consequence of Strategic Communication: How Message Design Adversely Affects the Sender's Own Goals" (The Netherlands, Universiteit Leiden, 2022), https://studenttheses.universiteitleiden.nl/access/item%3A3484133/view.
[22] U.S. Department of Defense, "Joint Publication 3-13 Information Operations."
[23] "OODA Loop: A Blueprint for the Evolution of Military Decisions," accessed December 18, 2024, https://www.rti.com/blog/ooda-loop-a-blueprint-for-the-evolution-of-military-decisions.
[24] "Russia Bars 'extremist' British Comedy The Death of Stalin," January 23, 2018, https://www.bbc.com/news/world-europe-42793157.
[25] "Russia Bars 'extremist' British Comedy The Death of Stalin."
[26] "Russia Bans 'The Death of Stalin' – DW – 01/23/2018," dw.com, accessed December 18, 2024, https://www.dw.com/en/russia-bans-the-death-of-stalin-from-movie-theaters/a-42278029.

[27] "The Death of Stalin Release Date, Trailer, Cast and Everything You Need to Know | Metro News," accessed December 18, 2024, https://metro.co.uk/2017/10/11/the-death-of-stalin-release-date-trailer-cast-and-everything-you-need-to-know-6993198/.
[28] "Moscow Movie Theater Shows Stalin Film, Defies Official Ban," AP News, January 25, 2018, https://apnews.com/article/6df0e42f039545e2ae4ecf4b90ed27c6.
[29] U.S. Department of Defense, "Information Operations Roadmap (Declassified 2006)" (Department of Defense Publishing Directorate, October 30, 2003), https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Other/Information_Operations_Roadmap_30_October_2003.pdf.
[30] Nick Fischer, "The Committee on Public Information and the Birth of US State Propaganda," *Australasian Journal of American Studies* 35, no. 1 (2016): 51–78, https://www.jstor.org/stable/44779771.
[31] Fischer.
[32] Fischer.
[33] Fischer.
[34] Fischer.
[35] "Records of the Office of Strategic Services [OSS]," accessed December 19, 2024, https://www.archives.gov/research/guide-fed-records/groups/226.html?utm_source=chatgpt.com#226.12.
[36] "Records of the Office of Strategic Services [OSS]."
[37] "Historical Intelligence Documents: From COI to CIG - CSI," accessed December 19, 2024, https://www.cia.gov/resources/csi/studies-in-intelligence/archives/historical-intelligence-documents-from-coi-to-cig/?utm_source=chatgpt.com.
[38] 80th United States Congress, "National Security Act of 1947" (United States Congress, September 18, 1947), https://www.govinfo.gov/content/pkg/COMPS-1493/pdf/COMPS-1493.pdf.
[39] "Our History," Radio Free Europe/Radio Liberty, accessed December 19, 2024, https://about.rferl.org/our-history/.
[40] "Our History," Radio Free Europe/Radio Liberty, accessed December 19, 2024, https://about.rferl.org/our-history/.
[41] Central Intelligence Agency, "Annex I: List of Cold War Weapons and Techniques (Declassified 2001)" (Central Intelligence Agency: Approved for Public Release), accessed December 19, 2024, https://www.cia.gov/readingroom/docs/CIA-RDP80-01065A000400070033-1.pdf.
[42] Shawn J. Parry-Giles, "The Eisenhower Administration's Conceptualization of the USIA: The Development of Overt and Covert Propaganda Strategies," *Presidential Studies Quarterly* 24, no. 2 (1994): 263–76, https://www.jstor.org/stable/27551240.
[43] Parry-Giles.
[44] Curator, "The Voice of America Was Once a Serious Government Business – Cold War Radio Museum," accessed December 19, 2024, http://www.coldwarradiomuseum.com/the-voice-of-america-was-once-a-serious-government-business/.
[45] Parry-Giles, "The Eisenhower Administration's Conceptualization of the USIA."
[46] 105th Congress of the United States, "The Foreign Affairs Reform and Restructuring Act of 1998, Division G of the Omnibus Consolidated and Emergency Supplemental Appropriations Act," (U.S. Congress), accessed December 19, 2024, https://www.govinfo.gov/content/pkg/PLAW-105publ277/pdf/PLAW-105publ277.pdf.
[47] "Executive Order 13584 --Developing an Integrated Strategic Counterterrorism Communications Initiative," whitehouse.gov, September 9, 2011, https://obamawhitehouse.archives.gov/the-press-office/2011/09/09/executive-order-13584-developing-integrated-strategic-counterterrorism-c.
[48] "Executive Order 13721—Developing an Integrated Global Engagement Center To Support Government-Wide Counterterrorism Communications Activities Directed Abroad and Revoking Executive Order 13584 | The American Presidency Project," accessed December 19, 2024, https://www.presidency.ucsb.edu/documents/executive-order-13721-developing-integrated-global-engagement-center-support-government.
[49] "About Us - Global Engagement Center," *United States Department of State* (blog), accessed December 19, 2024, https://www.state.gov/about-us-global-engagement-center-2/.
[50] "Briefing With Special Envoy Lea Gabrielle, Global Engagement Center On Disinformation and Propaganda Related to COVID-19," *United States Department of State* (blog), accessed December 19, 2024, https://2017-2021.state.gov/briefing-with-special-envoy-lea-gabrielle-global-engagement-center-on-disinformation-and-propaganda-related-to-covid-19/.
[51] "Statement from CEO John F. Lansing on Agency Rebrand," USAGM, accessed December 19, 2024, https://www.usagm.gov/2018/08/22/statement-from-ceo-john-f-lansing-on-agency-rebrand/.
[52] "What We Do," accessed December 19, 2024, https://www.dni.gov/index.php/what-we-do.
[53] "Organization," accessed December 19, 2024, https://www.dni.gov/index.php/who-we-are/organizations.
[54] "Component Commands," accessed December 19, 2024, https://www.centcom.mil/about-us/component-commands/.
[55] "Component Commands."

[56] Mark Pomerleau, "The Military Services Should Get on the Same Page Regarding Information Warfare, Says Rep. Langevin," *DefenseScoop* (blog), December 2, 2022, https://defensescoop.com/2022/12/02/the-military-services-should-get-on-the-same-page-regarding-information-warfare-says-to-rep-langevin/.
[57] Mark Pomerleau, "US Space Command Created New 'information Warfare' Position Dedicated to Synchronizing and Coordinating Capabilities," *DefenseScoop* (blog), May 16, 2023, https://defensescoop.com/2023/05/16/us-space-command-created-information-warfare-positions-dedicated-to-synchronizing-and-coordinating-capabilities/.
[58] "COMPONENT COMMANDS."
[59] "Statement of General Richard D. Clarke, USA Commander, United States Special Operation Command Before the 117th Congress Senate Armed Services Committee," April 5, 2022, https://www.armed-services.senate.gov/imo/media/doc/2022%20USSOCOM%20Posture%20-%20Clarke%20-%20SASC%20(5APR22)%20(FINAL).pdf.
[60] Andrew Feickert, "The Unified Command Plan and Combatant Commands: Background and Issues for Congress," n.d.
[61] Chairman of the Joint Chiefs of Staff, "Chiarman of the Joint Chiefs of Staff Instruction 5125.01: Charter of the Joint Information Operations Warfare Center" (Department of Defense Publishing Directorate, September 1, 2011), https://www.jcs.mil/Portals/36/Documents/Library/Instructions/CJCSI%205125.01%C2%A0.pdf?ver=STao-knIhpkzbrMRKOaRDA%3D%3D&utm_source=chatgpt.com.
[62] "Army Cyber Command Leaders Outline Theater Information Detachment Concept," www.army.mil, October 22, 2024, https://www.army.mil/article/280728/army_cyber_command_leaders_outline_theater_information_detachment_concept.
[63] Mark Pomerleau, "Army Officially Resources 3 Theater Information Advantage Detachments," *DefenseScoop* (blog), May 23, 2024, https://defensescoop.com/2024/05/23/army-officially-resources-3-theater-information-advantage-detachments/.
[64] Pomerleau.
[65] "Army Speeds Information Warfare Detachments Creation | AFCEA International," August 22, 2024, https://www.afcea.org/signal-media/army-speeds-information-warfare-detachments-creation.
[66] "Taliban and the Northern Alliance," January 1, 2016, https://web.archive.org/web/20160101184625/http://usgovinfo.about.com/library/weekly/aa092801a.htm.
[67] "Despite Massive Taliban Death Toll No Drop in Insurgency," accessed December 20, 2024, https://web.archive.org/web/20160703023519/http://www.voanews.com/content/despite-massive-taliban-death-toll-no-drop-in-insurgency/1866009.html.
[68] The White House, "Remarks by President Biden on the Drawdown of U.S. Forces in Afghanistan," The White House, July 8, 2021, https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/07/08/remarks-by-president-biden-on-the-drawdown-of-u-s-forces-in-afghanistan/.
[69] Trine (Chair) Heimerback, "United Nations Security Council Report Concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and Associated Individuals, Groups" (United Nations Security Council, February 3, 2022), https://nordicmonitor.com/wp-content/uploads/2022/02/UNSC_report_al_Qaeda_ISIS.pdf.
[70] Arturo Munoz, "Assessing Military Information Operations in Afghanistan, 2001–2010" (RAND Corporation, April 30, 2012), https://www.rand.org/pubs/research_briefs/RB9659.html.
[71] Munoz.
[72] "U.S. Military Apologizes for 'highly Offensive' Leaflets It Distributed in Afghanistan," Los Angeles Times, September 6, 2017, https://www.latimes.com/world/asia/la-fg-afghanistan-usmilitary-apology-20170906-story.html.
[73] "U.S. Military Apologizes for 'highly Offensive' Leaflets It Distributed in Afghanistan."
[74] Livia Gershon, "The US Propaganda Machine of World War I," JSTOR Daily, November 17, 2023, https://daily.jstor.org/the-us-propaganda-machine-of-world-war-i/.
[75] "100 Years of Subterfuge: The History of Army Psychological Operations," www.army.mil, June 28, 2018, https://www.army.mil/article/199431/100_years_of_subterfuge_the_history_of_army_psychological_operations.
[76] "100 Years of Subterfuge."
[77] Patrick Porter, "Paper Bullets: American Psywar in the Pacific, 1944–1945," *War in History* 17, no. 4 (2010): 479–511, https://www.jstor.org/stable/26070823.
[78] "100 Years of Subterfuge."
[79] U.S. Special Operations Command, "Statement of General Richard D. Clarke, USA Commander, United States Special Operation Command Before the 117th Congress Senate Armed Services Committee."