Joint Interagency Task Force – Influence: The New Global Engagement Center

by

Lieutenant Colonel Bradley M. Carr
United States Army

Under the Direction of:
Dr. Steven K. Metz

United States Army War College
Class of 2017

DISTRIBUTION STATEMENT: A
Approved for Public Release
Distribution is Unlimited

The views expressed herein are those of the author(s) and do not necessarily reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.
The United States Government and Department of Defense (DoD) placed more priority on influence operations from WWII through the Cold War. It appears the US Government has forgotten historical lessons on the importance of dealing with threats in the information environment, especially when current threats are rapidly increasing their sophisticated influence efforts. Even with current emphasis on grey zone conflicts, hybrid warfare, or third offset strategies, it is apparent that the US does not have a construct to re-weaponize the “I” in DIME as part of any strategic vision, policy, or overall strategy. Failure to adequately shape and dominate the information environment places US national security at risk. Using Mintzberg’s organizational design concepts as a guide, this paper proposes a DoD-led influence joint interagency task for creation at the national level to develop, plan, coordinate, synchronize, execute and assess full-spectrum influence activities in the multi-domain environment.
Abstract

The United States Government and Department of Defense (DoD) placed more priority on influence operations from WWII through the Cold War. It appears the US Government has forgotten historical lessons on the importance of dealing with threats in the information environment, especially when current threats are rapidly increasing their sophisticated influence efforts. Even with current emphasis on grey zone conflicts, hybrid warfare, or third offset strategies, it is apparent that the US does not have a construct to re-weaponize the “I” in DIME as part of any strategic vision, policy, or overall strategy. Failure to adequately shape and dominate the information environment places US national security at risk. Using Mintzberg’s organizational design concepts as a guide, this paper proposes a DoD-led influence joint interagency task for creation at the national level to develop, plan, coordinate, synchronize, execute and assess full-spectrum influence activities in the multi-domain environment.
Joint Interagency Task Force – Influence: The New Global Engagement Center

The United States Government and Department of Defense (DoD) placed more priority on influence operations from WWII through the Cold War. It appears the US Government has forgotten historical lessons on the importance of dealing with threats in the information environment, especially when current threats are rapidly increasing their sophisticated influence efforts. Even with current emphasis on grey zone conflicts, hybrid warfare, or third offset strategies, it is apparent that the US does not have a construct to re-weaponize the “I” in DIME as part of any strategic vision, policy, or overall strategy. Failure to adequately shape and dominate the information environment places US national security at risk. Using Mintzberg’s organizational design concepts as a guide, this paper proposes a DoD-led influence joint interagency task for creation at the national level to develop, plan, coordinate, synchronize, execute and assess full-spectrum influence activities in the multi-domain environment.

Defining Influence Operations

The term influence operations refers to the combined and synchronized activities of public diplomacy, strategic denial and deception, military deception, cyber electromagnetic activities, psychological operations / military information support operations, information operations, public affairs activities, offensive intelligence or counterintelligence operations, along with certain planned kinetic actions ultimately focused on the cognitive dimension of the information environment for purposes of eliciting a specific behavior or decision.\(^1\) Essentially, influence operations are the “weaponized” portion of the information instrument of national power.
Background

In 2006, Secretary of Defense Donald Rumsfeld stated that the US would “probably deserve a D or D-plus as a country as to how well we’re doing in the battle of ideas that's taking place in the world today.”

Ten years later in 2016, the United States is still trying to decide how to handle influence in the evolving modern information environment. Section 1287 of The National Defense Authorization Act of 2017 orders the State Department to increase its influence efforts through the Global Engagement Center (GEC).

However, things have not always been so disjointed. From World War II through the end of the Cold War, the United States placed a priority on the conduct of influence operations.

**United State Influence Operations in World War II**

The United States developed and executed some of the most comprehensive influence operations efforts across the globe during World War II. The Office of Strategic Services (OSS), specifically its Morale Branch, along with the Office of War Information (OWI) began operations in 1942. Prior to 1942, different organizations across the government were conducting various unconnected influence efforts, but the creation of OWI and OSS helped to coordinate and centralize efforts. Eventually, DoD established a Psychological Warfare Division (PWD). These three organizations allowed the United States to conduct a range of overt to covert influence operations synchronized from the tactical to strategic level.

World War II is the backdrop for some of history’s most famous influence operations, and were conducted by the OSS, OWI, and PWD. Modern deception practitioners still use the vignettes of Operation Mincemeat and the Normandy deception as textbook example of proper deception planning, coordination, and
execution. Likewise, much of the tactical influence techniques developed during World War II, such as loudspeaker operations, are still in use today. Even though the US Government shut down OWI and the OSS after World War II, it took the lessons from the war and still conducted large scale influence operations throughout the Cold War.

**United States Influence Operations during the Cold War**

After World War II with the friction between the US and the Soviet Union heating up, the OSS transferred most of its covert influence infrastructure to the fledgling Central Intelligence Agency. Likewise the OWI transferred much of its capabilities to the State Department who had control of Voice of America. However, while this worked for a short period of time, the fear of communist ideology spreading and threatening US interests persuaded President Eisenhower to develop a Committee on International Information Activities. This led to the creation of the United States Information Agency (USIA) in 1953 which was responsible for communicating US objectives and policies through various communication techniques. Simultaneously, DoD established the U.S. Army Psychological Warfare Center and School at Fort Bragg, NC, and began placing a higher emphasis on strategic denial and deception activities. This allowed the United States to once again conduct coordinated overt to covert influence operations from the tactical to strategic level.

The United States executed several effective influence operations during the Cold War period. Two of the more well-known examples include the Cuban missile crisis and the “Star Wars” missile defense shield. In 1962, the director of the USIA, Edward R. Murrow, had a seat on the National Security Council. This position allowed him efficiently take President Kennedy’s statements and broadcast them to the world given a poor infrastructure of diplomatic communications as the time.
other overt and covert influence operations, allowed the US to shape the strategic environment toward achieving US objectives in a very tense environment. Likewise, beginning in March of 1983, the United States government began an extensive influence operation in promoting the “Star Wars” anti-ballistic missile shield. Since Soviet strategy was based on offensive capability, this comprehensive influence effort caused the Soviets to expend numerous resources against a technology that did not actually exist, creating one more step to reaching the end of the Cold War. However, the end of the Cold War resulted in a drastic decline in the focus of influence operations for the United States.

Decline in Influence Operations after the End of the Cold War

The end of the Cold War led to the dismantling of the USIA, and a rapid decline in influence operations as a whole for the US. Without a major foe, it was hard to justify the existence of the USIA and the large influence operations network associated with it. During the same time period the results of the Goldwater-Nichols Act, moved psychological operations of DoD under the Under Secretary for Policy while maintaining military deception activities with the Under Secretary for Intelligence. The US did see some initial successes after the Cold War with Desert Storm being an example. However, the evolution of 24-hour cable and satellite news along with the birth of the internet quickly outpaced the ability for the US to keep up with no central entity to coordinate efforts.

The events of 9/11, Iraq, Afghanistan, and the rise of ISIS quickly showed the shortfalls in US influence efforts. The United States Government, and particularly DoD, has been repeatedly reprimanded by Congress and the media for its shortfalls in its execution of influence activities as well as their measurement. Things finally moved to
a point where President Obama directed the establishment of the Center for Strategic Counterterrorism Communications (CSCC) in September 2011 to begin coordinating US Government messaging against al-Qa’ida. However, even this organization was unable to meet the task and has been restructured again into the Global Engagement Center (GEC). The GEC is responsible for counter ISIS messaging as well as countering adversarial nation-state disinformation and propaganda with the signing of the latest National Defense Authorization Act. Unfortunately, given the GEC’s structure, authority, and budget, along with the overall current layout of the US Government’s influence operations network, it is unlikely that the GEC is adequately prepared to adequately challenge its competition in the information environment.

The Competition: Russian and Chinese Approach to Conducting Multi-Domain, Multifunctional Influence Operations

In General Dunford’s posture statement to Congress in March of 2016, he stated that the countries of Russia and China have become peer competitors, or even surpassed the United States in Cyber capabilities. The Chairman also stated that Russia has made significant advancements in the execution of hybrid operations. What General Dunford’s testimony alluded to but did not address directly was Russia and China’s major advancements in using the Cyber domain and overall information environment to execute a comprehensive influence strategy radically different and exceedingly advanced compared to the United States’ efforts. Specifically, Russia’s "information confrontation" doctrine and China’s "three warfares" are in stark contrast to how the United States views and executes inform and influence activities across domains and functions.
Russia

Russia bases its approach to influence activities on a multi-domain, multifunctional concept described as “information confrontation.” Updated in 2014, information confrontation links tactical inform and influence activities from the tactical to grand strategic level,\textsuperscript{21} and includes everything from cyber, media activities, electronic warfare, non-lethal weaponry, and information protection, all the way to special pharmacological means, psychotronic means, and special intelligence collection to support these operations.\textsuperscript{22} What makes this doctrine so powerful is that is integrated and synchronized across all elements of national power. Essentially, the information confrontation framework helps drive and synchronize diplomatic, military, and intelligence functions across the range of overt, clandestine, and covert activities. Information confrontation doctrine is the manifestation of how Russian theorists describe a vision of war that will not be won through physical contact, but through the “psychosphere.”\textsuperscript{23} To that end, Russian has poured immense resources into dominating the psychosphere across domains and functions.

Russia’s Information Confrontation Structure and Budget

Although little is known about the actual structure and full scale of Russian information confrontation efforts as they permeate all facets of the Russian government, the size of Russian internet trolls and information confrontation budget estimates provide a level of scale. For example, in recent years there has been increasing exposure of Russia’s “Army of Trolls” also known as “Web Brigades” which is only one small facet of Russian information confrontation efforts. Russian trolls are paid roughly $800-1200 a month to work 12 hours a day posting comments online. Packed in groups of 20 and controlled by three supervisors, a single operator can post
hundreds to thousands of comments per day. In 2015, A New York Times story in 2015 estimated just one single troll office employed around 400 people with an estimated budget of approximately $400,000 per month. This is just a mere fraction of the overall budget Russia spends on media.

From their own admissions, Russia states it spends approximately $700 million on media activities per year. However, the Centre of Military-Political Studies (CMPS) estimates that Russia spends approximately $3.5 billion dollars per year on information confrontation activities. To provide comparison, DoD spent only $158 million in FY15 on information operations. Even with Department of State’s budget of approximately $1.8 billion for the entirety of its Public Diplomacy efforts, the overall unified US Government effort is still behind Russia in focused spending on influence. Regardless of spending, Russia has achieved significant effects with its information confrontation construct.

Ukraine, the European Union, and US Elections: Russian Information Confrontation in Action

Russian actions in Ukraine, provocative activities toward the European Union, and perceived meddling in US election provide contemporary examples of Russian information confrontation in action. All three provide examples of Russians integrated, whole of government use of disinformation, metanarratives, support to physical actions, and dominate use of the cyber domain for influence effect. Specifically, all three examples show the execution of information confrontation principles through the use of asymmetry, domination, clandestine activities, surprise, aiming balance of power in Russia’s favor, exploiting lack of international regulations, focusing on long term impact, and use of divide and rule through exploitation of allies and adversaries. Along with
Russian successes in increasing its influence capabilities, China has also made significant improvements recently.

**China**

China has an extensive multi-domain and multifunctional approach to conducting inform and influence activities. Chinese doctrine, refers to this approach as the “three warfares.” The three warfares consist of three intertwined strategies. First is public opinion, or media, warfare to influence perceptions and attitudes using all forms of media to gain “dominance over the venue for implementing psychological and legal warfare.” The second is psychological warfare which are efforts to disrupt, deceive, demoralize, and deter that are targeted at an opponent’s cognition and decision making. Last is legal warfare which leverages public opinion and psychological warfare through exploitation of international and domestic law to further Chinese national interests. The three warfares doctrine has increased the organic view of national strategy driving China to “innovate in the application of these concepts to new contexts, such as counterterrorism and stability protection, international peacekeeping, protecting transportation and escort, and closing and controlling borders.” To that end, China has restructured the People’s Liberation Army (PLA) to better execute the three warfares doctrine.

**Three Warfares Structure and Budget**

China’s defense budget is projected to “increase by an annual average of seven percent,” and it has placed a greater emphasis on cyber activities and overall information operations. Put into a three warfares construct, this indicates a drastic expansion of influence related capability. To that end, China has initiated several structural changes in its military with the most notable being the construction of the
Strategic Support Force (SSF). In late 2015, the PLA created the SSF consolidating cyber, electronic warfare, and intelligence gathering under one service-level command equivalent to the army, navy, and air force.\textsuperscript{38}

Essentially, China has consolidated the major tools for three warfares doctrine under one unified command. According to Chinese President Xi Jinping, the SSF will “facilitate cooperation between defense and civilian sectors”\textsuperscript{39} highlighting a unified, whole of government approach to executing inform and influence activities. Some open source reports from 2010 estimated China’s web of hackers alone to around 50,000-100,000 individuals at that time.\textsuperscript{40} The increasing Chinese defense budget along with the creation of the SSF would indicate a significant potential increase in capability. Likewise, China has already demonstrated the employment of the three warfare doctrine with these expanding capabilities.

South China Sea: How China Executes the Three Warfares Concept

China’s activities concerning the South China Sea provide a glimpse into how China executes its three warfares doctrine. As one example regarding overt public opinion/media warfare, China Central Television (CCTV), China’s flagship state broadcasting service including a 24-hour global international news satellite channel has increased tenfold since 2011.\textsuperscript{41} Simultaneous with its increase in viewership, CCTV along with other Chinese media outlets, has drastically increased its coverage of South China Sea stories positively promoting Chinese interests in the area.\textsuperscript{42} This expansive media base helps mutually support the psychological and legal warfare elements.\textsuperscript{43}

China has employed economic, political, and military means as part of its psychological warfare component relating to the South China Sea. For example, China has used financial incentives with Cambodia to shape Cambodia’s perceptions and
increase its economic dependence on China. Additionally, China has used political means through aggressive diplomacy to isolate countries such as Vietnam from receiving assistance from fellow members of the Association of Southeast Asian Nations (ASEAN) relating to the South China Sea. Lastly, China has used military means to create artificial islands in the South China Sea, placing military weaponry and aircraft on them all while increasing naval and air patrols in the area. However, these psychological and media warfare efforts are only effective with linked use of legal warfare.

China use of legal warfare in disputing claims in the South China Sea is extensive. China has used “idiosyncratic interpretations” of the U.N. Convention on the Law of the Sea (UNCLOS) to facilitate its territorial claims. Thus, this coercive use of international law provides China operational space to better facilitate and adeptly execute the public opinion/media warfare and psychological warfare aspects of the three warfares doctrine which in turn greatly amplifies the overall effect. Unfortunately, even though Russia and China have made substantial investments in evolving their capabilities and holistic, synchronized execution of influence-related activities across domains and functions, the United States is lagging behind.

Gaps in United States Influence Efforts

While the United States may still have kinetic overmatch against Russia and China, the US still has substantial gaps if it wants to compete with Russia and China for influence in the information environment. However, the issue of the United States lagging in the information environment is nothing new. In 2006 a Rand study assessing US messaging efforts since early 2002 stated that the United States was already lagging behind in its efforts to counter violent extremist ideology. Fast forward to 2010,
confusion and frustration resulted in Congress slashing the budget for DoD Information Operations efforts.\textsuperscript{50} Although there have been recent efforts to address and improve how the US will confront Russian and Chinese influence efforts,\textsuperscript{51} the United States still has gaps it must address in budget, compartmentalization of influence capabilities, authorities and permissions, and unity of narrative if it wishes to compete with Russia and China in the information environment.

**Budget**

If dominating the information environment is critical to national interests in the future strategic environment, the money spent by the United States Government toward influence activities unfortunately would say otherwise. For example, DoD budget on information operations under Operations and Maintenance (O&M) appropriations for Fiscal Year (FY) 2015 was $158 Million.\textsuperscript{52} The overall FY 2015 DoD O&M appropriation was $195.5 billion.\textsuperscript{53} That means only 0.08\% of just the O&M appropriation alone was spent on information operations. This would be even a smaller percentage if compared to the entire Defense Budget. Likewise, the Department of State only spent approximately 3.5\% of its entire International Affairs budget on public diplomacy, broadcasting, etc.\textsuperscript{54} This is troubling when compared to the increased commitment and premium Russia and China are placing on influence operations.

One common counterpoint to the above argument is the increasing amount of money the United States Government is committing to increasing its cyber capabilities. For example, in 2016, President Obama asked for $19 billion for cyber security.\textsuperscript{55} While encouraging, this effort is focused on defensive measures with a greater priority to physical dimension of the information environment and cyber domain over the informational and cognitive aspects that are critical in conducting more offensive
influence activities like those conducted by China and Russia. However, budget priority is only one of the gaps the United States most overcome.

**Compartmented and Siloed Nature of US Influence Efforts**

The second gap the United States has compared to near peer competitors in conducting influence operations is the compartmented nature of the arrangement of various capabilities needed to conduct multi-domain and multifunctional influence. There are many hurdles just in DoD alone. Various capabilities are broken up across the department, with each office having its own unique policies, structure, and culture. For example, Military Deception (MILDEC) is nested within the Under Secretary of Defense for Intelligence (USD(I)). Military Information Support Operations (MISO)/Psychological Operations (PSYOP) is nested within the Under Secretary of Defense for Policy (USD(P)) underneath the Deputy Assistant Secretary of Defense for Special Operations & Combatting Terrorism which reports to the Assistant Secretary of Defense for Special Operations/Low-Intensity Conflict. However, although Cyber activities are within USD(P) they are located under the Deputy Assistant Secretary of Defense for Cyber Policy which reports to the Assistant Secretary of Defense for Homeland Defense and Global Security. Adding to the bureaucracy, the Under Secretary of Defense for Acquisition, Technology and Logistics acquire the portfolio for electronic warfare. Trying to bounce back and forth internal to USD(P) or across to USD(I) is less than efficient. This makes streamlining policy and decisions at the speed of information exceedingly difficult, but it is not confined to DoD.

Compartmentalization internal to DoD and Title 10 of the US Code is only one portion of a larger puzzle. Messaging and influence capability rests with State Department under Title 22 as well as various covert influence capabilities that reside
under the intelligence functions with Title 50. The result of all this structural compartmentalization is inefficiency in rapidly coordinating, synchronizing and executing multidomain and multifunctional influence efforts across the US government with the ability to leverage all the instruments of national power for innovative influence effect. Unfortunately, compartmented structure creates other gaps that the United States must overcome.

Varying Authorities and Permissions

Over time, placing related influence capabilities under different organizations has created various conflicting authorities and permissions for their use. For example, in the last few years, MISO activities and their funding have become a special interest item for Congress requiring its own unique reporting requirements and increased oversight. At the same time, cyber capabilities and permissions are increasing concurrent with authority to execute various cyber activities. This can lead to friction. While a cyber entity could have full authority and permission to execute a cyber-enabled MISO activity, MISO elements may be slow in receiving permission or have the authority for the message that needs to be delivered through cyber means. The need for better unified authorities and permissions for influence capabilities has existed for some time and still needs to be addressed to compete with adversarial efforts. Overall, compartmented capabilities combined with varying authorities and/or permissions ultimately leads to mediocre performance.

Lack of Unified Narrative

The cumulative result of compartmentalization and misaligned authorities and permissions is disjointed, and sometimes even conflicting narratives produced by the United States Government. There are a few examples in recent years of misaligned
narratives. First, was the aftermath of the bin Laden raid. For an operation that was so long in the making, there were several conflicting narratives emanating from various government agencies in the hours and days after the raid. The most conflicting accounts related to what were done with bin Laden’s body as well as the issue of how he died. White House spokesman Jay Carney and Jay Brennan, the assistant to the president for homeland security and counterterrorism gave conflicting accounts along with several other conflicting stories from across the government.\textsuperscript{59} For something so long in the making where the US was in control of the narrative to have such disparate narratives does not bode well for more complex influence tasks which provides context for the next point.

A second example of narrative failure by the United States Government has been how it has addressed the Islamic State in Iraq and Syria (ISIS). A six-part series produced by The Brookings Institution includes the opinions of former heads of the CSCC highlights in detail the challenges in developing, synchronizing, and even maintaining any solid narrative against ISIS. An insightful portion by Clint Watts, specifically addresses how compartmentalization and misaligned authorities have prevented unity in narrative. Specifically, he states that compartmentalization has “complicat[ed] ownership and authority over engagement” where competing organizations only lightly work “to counter ISIS’s narrative while focusing on their primary functions, in what [he] call[s] counterterrorism by PowerPoint bullets.”\textsuperscript{60} Without real changes in budget priority for the importance of influence operations as well as structural changes, the United States will continue to see gaps in its capabilities to
compete with competitors in the information environment. Fortunately, Henry Mintzberg
provides some guidance in how to overcome some of these structural challenges.

What Henry Mintzberg’s Principles Say about Organizations That Operate in the
Information Environment

In the early 1980’s, Henry Mintzberg wrote a book about how the structure of an
organization can determine how efficient the organization will be when matched with the
operational environment it must operate in. This is of extreme importance when
dealing with influence operations in the current and future information environment.
More importantly, it is critical when with dealing with competitors such as Russia and
China as mentioned earlier in ensuring the safety of national interests. A mismatch
between an organization and its organization will lead to failure. Based on Mintzberg’s
five possible structures, an adhocracy is the best organizational design to meet the
requirements of the information environment.

Organizational Fit

Mintzberg states that the environment an organization interacts in helps dictate
its optimal structure. Specifically, he states that the stability, complexity, market
diversity, and hostility of the environment help determine the best structure. First, the
more dynamic the environment, the more organic the structure should be. Second, the
more complex the environment, the more decentralized the structure should be with a
greater emphasis on mutual adjustment. Third, the more diversified the markets for an
organization creates a drive to split into market-based units. Lastly, increased hostility in
an environment leads to temporary centralization. Describing the information
environment that an organization conducting influence operations in helps dictate the
best structure.
The Department of Defense *Strategy for Operations in the Information Environment* describes the modern information environment as “dynamic” and ever changing, thus unstable. Additionally, it describes the environment as complex due to its layered, globally networked, multi-domain nature. Likewise, the environment has an immense diverse market with state, non-state, civilian, and corporate entities all operating within the same spaces vying for advantage. Lastly, the information environment has the potential for hostility when used for ideological narrative battles. This description provides the basis for determining the most efficient structure.

According to Mintzberg, the best organization for dealing with an unstable, complex, diverse, and potentially hostile environment is an adhocracy. An adhocracy is a “flat” organization with a focus on mutual adjustment and extensive liaison devices having a decentralized organic structure and horizontal job specialization. An adhocracy would be akin to a space agency, a research and development firm, or similar type organization. Mintzberg states that an adhocracy must “hire and give power to experts- professionals whose knowledge and skills have been highly developed in training programs.” He goes on to say that in an adhocracy cannot rely on “standardized skills,” but rather it “must treat existing knowledge and skills merely as a basis on which to build new ones.” Although it seems strange, an adhocracy can co-exist in a bureaucracy.

**Administrative Adhocracy for Conducting Influence Operations**

There are two types adhocracies: an operating adhocracy, and an administrative adhocracy. While an operating adhocracy is associated mostly with young organizations, the administrative adhocracy is of value for conducting influence operations. An administrative adhocracy requires a sophisticated technical system to
help support mutual adjustment and the ability to innovate. Many bureaucracies have complex and robust communication and administrative systems which if harnessed, according to Mintzberg, can facilitate the efficiency of the administrative adhocracy. The US Government is a giant bureaucracy with sophisticated communication systems that an influence-focused organization could harness if done properly. However, an adhocracy does come with challenges.

**Shortfalls of an Adhocracy**

Mintzberg states that even when an adhocracy is the best fit with the environment, there are still three potential pitfalls with using an adhocracy. First, an adhocracy must not focus on executing ordinary tasks. Its purpose according to Mintzberg is to conduct the extraordinary. Next, an adhocracy must maintain and improve its advanced technical communication and administrative systems to remain competitive. This may lead to higher costs to maintain the organization. Lastly, an adhocracy will constantly fight the pressure to bureaucratize. An adhocracy that avoids these pitfalls will maintain efficiency.

**How Would Mintzberg Describe the GEC?**

The GEC is currently divided into four core areas including partnerships, data analytics, content, and interagency engagement. Because the GEC is focused on these core areas which requires standardization of skills leading to horizontal job specialization and vertical/horizontal decentralization, Mintzberg would describe the GEC as a professional bureaucracy. However, as mentioned earlier, this is a mismatch with the current and future information and operating environments.

When looking at the history and current status of US influence operations, the growing multifunctional, multi-domain influence competition the US will face with China
and Russia, along with current shortfalls in US influence operations efforts and Mintzberg’s lessons about organizational structures, a possible recommendation to improve US influence operations emerges.

Recommendation – A DoD Led Joint Interagency Task Force for Influence (JIATF-I) to Replace the GEC.

Based on the analysis of potential competition in the information environment, the information environment itself, and current shortfalls, potential recommendations for obtaining relative superiority in the information environment take shape. Taking Mintzberg’s principles into account, it becomes apparent that the current structure of the US Government influence operations is not adequate. Specifically, even though the GEC should be compatible with USIA and OWI before it, the GEC’s structure is incongruent with the current and future environment it must operate in. This paper recommends a complete restructure to the GEC, creating a DoD-led Joint Interagency Task Force for Influence (JIATF-I) with an administrative adhocracy framework/structure whose director reports directly to the National Security Council, much like USIA did during the Cold War. Figure 1 depicts a potential unit structure. However, this structure is not meant to be prescriptive, but to open a dialogue to further exploration and development.

Why a DoD led JIATF-I?

The nature of the mission, the competition, risk to national security, and the environment make DoD the optimal choice to be the executive agent for influence operations for the US Government. Specifically, DoD is the top choice for four reasons. First, DoD has a better innovation and capability development systems/processes along with tested planning/execution capabilities. Two, it has the sophisticated technical
Figure 1. Proposed JIATF-I Structure
support communication and administrative systems necessary for administrative adhocracy efficiency. Third, the leadership culture of DoD and its expansive network facilitates mutual adjustment. Finally, DoD has extensive horizontal specialization it can provide to an influence operations focused task force. Overall, DoD can help re-“weaponize” the information instrument of national power to compete with future adversaries.

Innovation and Planning/Execution Capability

Compared to other government departments, DoD has better innovation, planning, and assessment systems which will be critical in operating, maintaining, and improving an influence operations task force. For example, the Joint Capabilities Integration and Development System (JCIDS) and the Defense Acquisition System\textsuperscript{72} incorporates a robust research and development process and budget, along with an urgent operational needs process for developing and procuring cutting edge capabilities. Likewise, DoD has extensive planning and assessment systems such as the Joint Staff Planning System. Few other government agencies have such comparable systems or processes.

Technical Support Systems

In addition to planning and capability development, DoD also contains a robust, sophisticated technical support system for communications and administration. This is critical to the effective operation of an adhocracy which is necessary to be successful in the current and future information environment. For example, the department has robust unclassified, classified, and coalition global communication systems with extensive administrative knowledge management systems for the sifting and organization of
data. This becomes of great benefit considering roughly half of the organizations of the intelligence community are affiliated with the DoD.

**Mutual Adjustment**

The robust connections DoD has across the US Government and intelligence community allow for extensive mutual adjustment critical in the function of an adhocracy. When tied with an extensive liaison network and backed by a robust technical support structure, and environment of mutual adjustment allows for more rapid self-correction. Additionally, it allows for that ability to identify and capitalize on opportunities potentially operating at the “speed of information.”

**Horizontal Specialization**

Compared to other government departments, DoD has extensive specialization. This allows an organization to build a comprehensive and diverse group of capabilities to achieve mutual objectives. For example, under one organization, DoD can internally acquire cyber experts, language experts, targeters, intelligence experts across multiple fields, functional experts, domain experts, and others. When combined with liaison and communications capabilities, DoD can also tap into an even greater specialized capability network.

**General Overview of Proposed JIATF-I**

The proposed JIATF-I depicted in Figure 1 is an example of a possible DoD-led administrative adhocracy as a replacement for the GEC. In addition to the beneficial characteristics for a DoD-led structure mentioned above, there are three other elements of the structure that deserve highlighting. The Interagency Operations and Intelligence Center (IOIC), the extensive liaison and intelligence network, and the construct of the planning teams provide an updated approach for the conduct of influence operations.
Interagency Operations and Intelligence Center (IOIC)

The construct of the IOIC is to mirror the concept that exists in the National Joint Operations and Intelligence Center (NJOIC) under the Joint Staff. This 24/7 operations center would monitor the global information environment for operations and assessment purposes. Combining intelligence and operations together would help speed up intelligence collection management and operational feedback mechanisms.

Extensive Liaison and Intelligence Network

Influence operations require extensive information and thorough analysis to be successful. This is even more critical when dealing with highly classified operations. This JIATF-I would have an extensive and diverse liaison and intelligence network to support its planning and operations. It would be a network/enterprise concept that can rapidly access the 17 organizations of the intelligence community, other organizations of the interagency, combatant commands, partner nations, etc. for intelligence support (at all levels of classification), as well as open source intelligence, social media analysis, cultural intelligence, etc. Liaison network would also extend beyond the government with access to academia, non-governmental organizations, and commercial entities. The vision is a network that can “move at the speed of information” to hone the most accurate influence related analysis for operations and assessment.

Planning Teams

The planning teams under the Future Plans Directorate and the Future Operations Branch will be unique. Along with being regionally aligned with language and cultural experts on the team, planning teams will also include experts on Russia, China, terrorist threats, and applicable regional threats such as North Korea or Iran. Additionally, teams will include experts with various functional or domain focus. This will
allow better integration of plans across regions, functions, and domains with encouraged mutual adjustment collaboration.

Conclusion

Just looking at history from World War II until today, the importance the US Government placed on conducting influence operations has ebbed and flowed. However, regardless of the actual priority given to these operations, the US Government always acknowledges their consistency of importance in the nature of warfare. The explosion and rapid evolution of technology over the last few decades though is changing the character of warfare and how influence operations can be conducted against an adversary. Russia and China are pushing forward with significant changes to doctrine and structure to prioritize influence operations as even more critical in this changing character of warfare.

Unfortunately, the United States is lagging behind. If the US wants to achieve parity, and even overmatch, with Russia and China in the information environment, it must be willing to prioritize the importance of influence operations as well and make significant changes. While it in essence recreated the shell of the OWI and USIA in the form of the GEC, the GEC is not structured properly based on Mintzberg’s organizational structure principles to be effective. In addition to increasing budgets for influence operations, the US Government needs to restructure the GEC to make it agile and effective. To this end, turning the GEC into an administrative adhocracy in the form of a JIATF and making DoD the executive agent is a first step. The proposed JIATF-I structure presented in this paper is meant to begin a dialogue to begin the process of truly reemploying and re-“weaponizing” information as an instrument of national power.
Failure to harness information and the efficacy of influence operations puts US national security at risk in the future strategic environment.

Endnotes


8 Ibid., 49.


13 Ibid., 482-485.


22 Ibid., 17.


34 Cheng, “Winning Without Fighting.”

35 Kania, “The PLA’s Latest Strategic Thinking on the Three Warfares.”


37 Ibid., 63-65.


44 Halper, China: The Three Warfares, 389.

45 Ibid., 393.


47 Cheng, “Winning Without Fighting.”

48 Halper, China: The Three Warfares, 426.


53 Ibid., 4.


62 Ibid., 136-143.


64 Ibid., 4.

65 Ibid., 2.

67 Ibid., 255.

68 Ibid., 274.

69 Ibid., 277.


71 Mintzberg, Structure in Fives: Designing Effective Organizations, 189.

