PRIORITIZING INFORMATION WARFARE IN THE UNITED STATES: HOW A PANDEMIC DEMONSTRATED OUR INABILITY TO COMPETE IN THE INFORMATION ENVIRONMENT

Patrick G. Franck and Anthony J. Eastin
United States Air Force

WHITE PAPER

May 11, 2020

For any questions or further information please feel free to contact Anthony Eastin at ajeastin@gmail.com or Patrick Franck at patrick.g franck@gmail.com.
Acknowledgments

This work would not have been made possible without the help and support of various individuals in the United States Air Force and colleagues across the Department of Defense. We would like to personally acknowledge and thank Lt Col Matthew Linford (PhD) for guiding us in the creation of this white paper, his feedback and recommendations have been instrumental in the product that you see here today. We would also like to thank Dr. Robert Ehlers (USAF Col. Retired) for his feedback and expertise in understanding our current DoD Information Operations construct which further shaped our recommendation. Lastly, we would like to individually thank Lt Col Armin Blueggel, Lt Col Nikita Belikov, Maj Erik Armbrust, Capt Madeline Goff, Gregory Chapin, David Bryan, and Haley Wilson, their recommendations and insightful feedback was invaluable in the creation of this paper.
1. Introduction

On December 31, 2019 China warned the World Health Organization (WHO) that a pneumonia of unknown cause was detected in Wuhan, China. This virus would later be known as the Novel Coronavirus 2019 or COVID-19. On January 10, 2020 China reported its first COVID-19 casualty. Two days later the virus made its first appearance outside of mainland China and on January 21, a short twenty-one days after China’s initial warning, the United States announced its’ first COVID-19 case.2

As known cases of the virus spread, the world’s attention became increasingly focused on China with health experts, media, and government leaders seeking answers regarding this invisible enemy. Instead of opening its doors, allowing experts to help uncover the dangers of COVID-19, China waged a complex, multifaceted information warfare campaign in order to protect its interests and deflect blame for the virus.

Although not as easily observed and understood as a physical warfare campaign, the effects of this information warfare campaign are equally devastating. The confusion created by this campaign caused the world to delay recognizing the seriousness of the virus, created doubts and uncertainty regarding the best way to slow the virus, and enabling the virus to spread more widely and rapidly than it would have done had the world been able to mount a coordinated response. The overall cost of these actions has contributed to the U.S. losing more lives to the virus over the past eight weeks than the entirety of the Vietnam War and all subsequent armed conflicts in which the country has been involved4.

The United States Department of Defense (DoD) has long recognized the need to increase its ability to operate in the Information Environment (IE)5. Although some progress has been made, as the COVID-19 pandemic has highlighted, the United States remains woefully unprepared to combat complex information warfare campaigns such as the one currently being waged by China. This inability is directly harming U.S. interests and increasing the cost, in both lives and economic effects, of the pandemic. In this white paper, we argue that the United States must quickly close the gap in our ability to counter information warfare campaigns and defend our interests in the global IE by developing a rapid, whole of government capability.

This capability would enhance the U.S. ability to operate in the information environment, and, when needed, wage information warfare. This capability must include: the ability to understand how adversaries are shaping the IE; the ability to quickly identify and counter misinformation and propaganda; the ability to generate a rapid response that increases the cost to adversaries who choose to wage information warfare against the U.S. and her allies; and, most importantly, the ability to allow the U.S. to proactively shape the information environment in order to protect our national interests and advance our strategic priorities.

1 https://www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they-happen
5 DODI 3608.11, Nov 4, 2005.
We begin this paper by highlighting how the U.S. inability to compete in the information environment has allowed China to maneuver uncontested through the IE with regards to COVID-19 and the cost this created for the U.S. and the world. We then recommend creating a whole of government information warfare capability that would align the many disparate U.S. information capabilities in order to rapidly respond to actions in the IE. We recommend these capabilities align under the umbrella of a revived and restructured U.S. Information Agency (USIA) directly linked and co-located with a fully resourced and empowered DoD Joint Information Operations Warfare Center (JIOWC) as a possible solution to enhance the ability of the United States to counter information warfare.

2. China’s Information Warfare Campaign

China is in the process of a complicated, multi-faceted information warfare campaign. In the early stages of this campaign China focused on two main efforts: controlling the narrative and creating confusion. China focused on controlling the narrative surrounding COVID-19 by suppressing potentially damaging information that it perceived as endangering its reputation and worldwide investments. Simultaneously, borrowing a technique from the Russian playbook, China began to rapidly disseminate false information in an attempt to highlight its ability to deal with the pandemic, deflect blame regarding the cause of the pandemic, and create an overall sense of confusion about COVID-19 within the global IE. It is difficult to directly tie this information campaign to the Chinese Communist Party (CCP) because of the plausible deniability that information warfare allows adversaries. The evidence highlighted in the following paragraphs provides indications of an intentional Chinese information warfare campaign.

Suppressing Information

Although the first COVID-19 case was reported by China on December 31, 2019, thirteen days earlier on December 18, 2019 a cardiovascular specialist, Dr. Ai Fen, the director of the emergency department of the Central Hospital of Wuhan, came in contact with the virus and reported the incident to her superiors, who quickly reprimanded her. She recounted the reprimand in an essay titled, “The one who supplied the whistle,” which was published in China’s People (Renwu) magazine. Following the interview, the article was quickly deleted from Chinese social media sites, removed from China’s People magazine and Dr. Fen was reported missing. Chinese citizens who wanted to warn the public of this emerging threat were forced to find creative ways to evade CCPs strong censorship. The article was shared on various social media platforms through different means, some writing backwards, others inserting typos and emoji’s, and some of them even shared it in fictional languages such as Klingons.

On December 30, 2019 Dr. Li Wenliang, a Chinese ophthalmologist who worked as a physician at the Central Hospital of Wuhan, warned his colleagues about a possible outbreak of an illness

that resembled Severe Acute Respiratory Syndrome (SARS), which would later be identified as COVID-19. He became a whistleblower when his warnings were left unheeded and he decided to share his findings publicly. Because Dr. Li’s remarks were considered a violation under Article 19 subsection 6 (spreading rumors, disturbing social order, or disrupting social stability) of China’s Provisions on News Information Services, on January 3, 2020, Wuhan police, which are governed by the CCP’s Ministry of Public Security, summoned Dr. Li and threatened to detain him for “making false comments on the Internet.” Dr. Li returned to work and on January 10, 2020 he reported that he was beginning to show symptoms of this new disease. On February 7, 2020 he succumbed to COVID-19.

On December 31, 2019 when COVID-19 was finally reported to the World Health Organization (WHO), Chinese authorities stated that the virus could not be spread via human-to-human transmission despite evidence that it was spreading rapidly through the city of Wuhan, including multiple cases of doctors being infected by patients.

The “inability” of the virus to spread via human-to-human contact was used as justification for keeping the city of Wuhan, with more than 11 million people and 800,000 tourists per year, operating as normal through a major CCP conference that was held from January 11th-17th, with authorities claiming zero new cases in this period. Despite evidence to the contrary, China did not confirm human-to-human transmission of the virus until January 22, 2020, more than one month after the first case of the virus was identified. Following this announcement, Hubei province, including its largest city Wuhan, was put into lockdown. Importantly, although the state-run Chinese press reported on the announcement of the existence of a 'novel type of pneumonia' to the WHO on December 31, 2019 Wuhan's largest newspaper made no mention of the virus until January 20, 2020.

Although China has since conceded that the virus poses a significant risk to humans and has a high likelihood of spreading via standard human-to-human transmission, it has continued to suppress the number of COVID-19 deaths in the city of Wuhan and across China.

As of April 27, 2020, officials in Wuhan have reported that only 67,000 residents have tested positive for COVID-19 and 2,535 people have died from the virus in Hubei province. At the time of writing this, the U.S. already reported that over 1.3 million people have tested positive for COVID-19 with over 80,000 confirmed deaths. In New York City alone, over 180,000 people have tested positive with more than 14,000 deaths. Given the population size and density of Wuhan (11 Million) and NYC (8.4 Million), it seems improbable that Wuhan would have only one-fifth of the deaths of New York City.

The decision to suppress the number of cases of COVID-19 is connected to a larger strategy within China’s information warfare campaign. Throughout this global pandemic, China has consistently attempted to showcase itself as the model country for preventative measures by

9 https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(20)30382-2/fulltext
10 https://www.hrw.org/reports/2006/china0806/3.htm
11 https://www.refworld.org/docid/54648cbd4.html
13 https://www1.nyc.gov/site/doh/covid/covid-19-data.page
highlighting the quick and drastic actions it took in handling the virus. News organizations and social media posts began circulating in late January about China creating multiple hospital wings in Wuhan within a matter of days, forcing its citizens to adhere to strict quarantine regulations, and there were even reports of welding citizens in their apartment buildings to ensure they would not be able to spread the virus.\(^4\)

Although the CCP has historically demonstrated its ability to control information going in and out of China,\(^5\) our analysis indicates that it made no attempt to control information regarding its quarantine measures. Pictures and videos of Chinese citizens being welded shut inside their apartments demonstrated the actions that the CCP was willing to take to slow the spread of the virus. This evidence made it easier for them to defend their low mortality rate numbers and highlight the superiority of China’s response to the virus.

Despite China’s claims, the international community began to openly criticize China and doubt the validity of the data released. Reports of trucks delivering thousands of urns per day in Wuhan, crematoriums unable to keep up with the demand necessary to discard the bodies, and Wuhan citizens beginning to speak up against the CCP’s claim of a low mortality rate contributed evidence counter to China’s claims and helped expose the Chinese Information Warfare Campaign.

With increased pressure from the international community and from activists within its own country, China finally revised its total number of COVID-19 cases by increasing its death toll exactly 50\%, adding precisely 1,290 fatalities.\(^6\) However, this token adjustment is irrelevant when considering the damage of China’s response. The confusion sown by China’s suppression efforts had done its damage, leaving the international community unprepared to deal with the virus.

**Creating Misinformation**

Although Chinese efforts to control the narrative was a significant line of effort, it was not the only focus of their information warfare campaign. Since the beginning of COVID-19, several narratives can be observed in the IE. Although not all of these narratives can be directly tied to China, it has amplified false narratives that serve its interests. These include but are not limited to: a) COVID-19 was unable to spread via human-to-human contact b) COVID-19 was no more dangerous than seasonal influenza (flu), and c) the U.S. military was responsible for the epidemic.

1. **The “It Can’t Spread” Narrative**

As shown above, the first reported case from China to the WHO of human-to-human transmission of COVID-19 was on January 22, 2020. However, several Chinese physicians reported to their superiors, on December 18, 2019, about a potential infectious disease emerging

---

\(^4\) https://twitter.com/ASBreakingNews/status/1226131773576425473?s=20
\(^6\) http://photos.caixin.com/2020-03-26/101534542_6.html#picture
\(^7\) https://www.bbc.com/news/world-asia-china-52321529
out of Wuhan with some claiming it bore resemblance to SARS which is typically highly contagious. On December 25, 2019, Chinese medical staff in two separate hospitals in Wuhan were suspected of contracting viral pneumonia disease and were quarantined as a result. When physicians brought up their concerns, the Wuhan Public Security Bureau, a state-run institution18, issued a statement that these were wild allegations and the individuals would be reprimanded for spreading false rumors19.

On January 11, 2020, more than 700 people including 419 medical staff were forced to undergo medical observation. The Wuhan City Health Commission declared that most of these unexplained viral pneumonia cases had a history of exposure to the South China seafood market and posed no evidence of human-to-human transmission20 even though evidence showed that the medical staff was contracting the disease from their patients21.

Following China’s lead narrative regarding the severity of the virus, the WHO echoed China’s assessment that “Preliminary investigations conducted by the Chinese authorities found no clear evidence of human-to-human transmission of the novel coronavirus (COVID-19) identified in Wuhan, China”22. Had the WHO known that multiple Chinese doctors had reported in early December to Chinese officials, the existence of a patient with COVID-19 like symptoms—with no exposure to the South China seafood market—providing evidence of the virus spreading via human-to-human contact, the WHO might have come to a different conclusion that could have saved thousands of lives.23

b. The “It’s Just a Flu” Narrative

The emergence of the narrative that COVID-19 was no more dangerous than the flu can be traced back to early January. Social media posts began to emerge downplaying the seriousness of the new threat by relating it to seasonal influenza and emphasizing that the traditional flu was deadlier than COVID-1924. Analysis indicates that this narrative increased in popularity for more than 30 days before beginning to lose traction.

First emerging via Twitter posts from legitimate handles, the narrative was subsequently picked up and propagated widely by bots. Although these accounts cannot be traced to any specific
adversaries, they do follow the same tactics as known state sponsored actors. During this time, Chinese state media outlets ran pieces discussing the current U.S. flu season, portraying it as a parallel and comparable epidemic. Foreign Ministry officials used available opportunities to cite U.S. seasonal flu numbers as a counter to criticism over the CCP’s handling of the situation.

But the core of the CCP’s push to downplay the coronavirus as the flu lay in circulating misinformation about the 2009 H1N1 outbreak. On February 8, 2020, Chinese officials began to propagate misleading statistics encouraging people to make false comparisons between COVID-19 and what the CCP referred to as the “2009 American Swine Flu Pandemic”, which did not originate in the United States.

This barrage of misinformation diluted confidence regarding the seriousness of the disease and likely inhibited strong, swift measures that could have helped minimize the spread. Though private companies such as Facebook, Google, and Twitter have since indicated that they are taking steps to reduce the spread of misinformation on their platforms, the message reached its target audience resulting in misreporting, confusion and wasting valuable response time.

c. U.S. Biological Weapon Narrative

As the situation in Wuhan and across China became increasingly visible to the world, the CCP shifted their narrative in an attempt to limit the negative perceptions toward China. One of these narratives was that the U.S. was responsible for the virus.

On February 23, 2020 the People’s Daily’s English reprinted a Global Times article titled “Japanese TV report sparks speculations in China that COVID-19 may have originated in the U.S.”. The original Global Times article, which is no longer available online, associated the U.S. seasonal influenza deaths with the novel coronavirus, causing speculation that COVID-19 originated in the United States. Additionally, articles and social media posts emerged stating that the spread of the virus was a result of the U.S. Government’s incompetence and failure to understand the virus.

On March 4, 2020 a conspiracy website called GlobalResearch.ca published a piece based on the People’s Daily reprint which was titled “China’s Coronavirus: A shocking Update. Did the Virus Originate in the U.S.?”

25 Chinese and Russian tactics have been observed using bot accounts on several past disinformation campaigns. In August 2019 Chinese state media created several “official” reports that blamed the CIA for the Hong Kong protests. China-linked social media accounts then flooded the information environment via Facebook and Twitter with thousands of pro-Beijing posts and targeted advertisements.


27 https://m.chinanews.com/wap/detail/zw/gj/2020/02-02/9075869.shtml

28 https://twitter.com/zlj517/status/1224380878396149764

29 https://www.globaltimes.cn/content/1178873.shtml
website, however, the site has continued to produce articles alleging the virus was created and originated in the United States.\footnote{https://www.globalresearch.ca/covid-19-perfect-catalyst-trump-war-against-china/5711048}

On March 13, 2020, Zhao Lijian, the spokesman and Deputy Director General of the Chinese Ministry of Foreign Affairs information department tweeted a link to his 287,000 followers. This link directed his followers to the GlobalResearch.ca’s website alleging that the U.S. was responsible for the virus, claiming it was brought into Wuhan during the Military World Games in which U.S. military teams participated.\footnote{https://www.scmp.com/news/china/society/article/3075051/chinese-foreign-ministry-spokesman-tweets-claim-us-military}

Along with traditional news sources, social media posts on both Facebook and Twitter began to emerge that the virus may have been a funded U.S. biological weapon. On YouTube, as of March 22, 2020, when searching for “新冠病毒” (novel coronavirus) the second autocomplete search suggestion was “The novel coronavirus is an American genetic weapon”\footnote{https://fsi.stanford.edu/news/china-covid19-origin-narrative}. As of April 28, 2020, hashtags on twitter such as “USbioweapon”, “biologicalwarfare”, and various others, are still active on the platform. When conducting a Google Trends analysis, one can find that these narratives are still highly prevalent today with individuals from countries around the world with the belief that this virus is a result of malfeasance on the part of the United States.\footnote{https://trends.google.com/trends/explore?date=2019-12-01%202020-04-29&q=COVID-19%20biological%20weapon,US%20biological%20weapon,Chinese%20Biological%20weapon}

Along with the CCP pushing misinformation to blame the virus on the U.S. in order to distance itself from blame, Russian and Iranian actors have also pushed misinformation targeting the U.S. population by creating confusion about COVID-19 and on effective preventative measures against the virus.\footnote{https://www.nytimes.com/2020/03/28/us/politics/china-russia-coronavirus-disinformation.html}

3. The consequences of Information Warfare

We believe that the evidence above is a clear indication of China’s complex, multifaceted information warfare campaign to protect its interests in the face of COVID-19’s reality. We now look at the cost of this campaign to the U.S. and other countries around the world.

Cost of Suppression

The consequences of China’s information campaign not only cost the lives of tens of thousands of U.S. citizens but potentially millions of people from around the world.\footnote{https://www.aljazeera.com/news/2020/05/world-coronavirus-death-toll-exceeds-250000-live-updates-200504231301555.html} Their attempt to suppress information and ignore the warnings from their health experts at the early stages of the disease enabled the virus to spread uncontrollably. The deliberate inaccurate information provided to the WHO caused world leaders to not prioritize the seriousness of this new threat, leaving many unprepared for the upcoming challenge.
The global economic impact of China’s delayed reporting is just as significant. When China finally imposed travel restrictions, countries throughout Asia had already begun to see COVID-19 cases rise. The impact of COVID-19 caused foreign investors to pull $26 billion out of developing Asian economies, increasing concerns of a major economic recession in Asia. Current estimates also indicate that 29 million people in Latin America could fall into poverty, while the Eurozone economy contracted by 3.8%, the largest quarterly decline since tracking began in 1995. In the U.S., as of April 30, 2020, 30 million Americans filed for unemployment insurance, raising the prospect of a deep economic recession.

Protecting its Investment

China recognized the economic impact of the virus and as the virus was uncontrollably spreading across the world, China leveraged its information warfare capabilities to protect its own various investments abroad. It did this by attempting to shift blame for the virus to the U.S., its main economic competitor. At a press conference on February 27, 2020, a Chinese Doctor, Zhong Nanshan, stated that the virus “may not have originated in China.” Soon after, numerous Chinese politicians began what appeared to be a coordinated information campaign to spread this narrative, with several tweeting similar statements questioning the origin of the virus. On March 8, 2020, the Chinese ambassador to South Africa tweeted that, “Although the epidemic first broke out in China, it did not necessarily mean that the virus is originated from China, let alone ‘made in China.” South Africa is a key member of China’s Belt and Road initiative and it was in China’s best interest to shift blame to the U.S. to ensure that its investments across the world and in South Africa were protected. On April 8, 2020, South Africa’s president Cyril Ramaphosa, expressed “gratitude to China for its long-term support to South Africa and African countries” a significant indicator of the success of this campaign.

Cost of Misinformation

The increase of misinformation on traditional and social media caused confusion within the information environment. On March 5, 2020, the WHO announced that the wide spread of false information has resulted in an “infodemic”, making it increasingly difficult for individuals to find reliable information surrounding COVID-19. As a result, more than 38% of U.S. citizens believed that COVID-19 did not present a significant threat to them. Although U.S. officials and health experts have consistently attempted to correct false narratives through official channels, misleading social media posts and false information are still prevalent today.
Those who do take the threat of the virus seriously are also left with a flood of misinformation from various social media posts that include: conspiracy theories surrounding the U.S. government and private companies’ intent to get “everyone microchipped”\(^{44}\), dangerous COVID-19 cures that could inflict serious harm to individuals who try them\(^{45}\), or ineffective preventative measures that could increase the spread of the virus\(^{46}\). The cost of this misinformation is widespread as limited government resources must now be directed towards countering false narratives and educating the public rather than combating the virus and its effects.

4. Why the U.S. is incapable of competing in the IE

If the Department of Defense has recognized the need to increase information operations capabilities why are we still incapable of countering information warfare campaigns such as the one highlighted with regards to China and COVID-19? We argue that this inability centers on the fact that U.S. capabilities to compete in the information environment are spread across numerous entities and there is not a sufficient structure in place from which the U.S. can conduct a whole of government response. While there are many different organizations across multiple U.S. Government agencies with messaging capabilities and missions, the lack of centralized and coordinated shaping-and-influence efforts results in a dispersed capability with various entities constrained by resourcing, authority concerns and a cohesive narrative, preventing them from effectively engaging and protecting U.S. interests. These limitations leave the U.S. unable to provide a real-time, whole-of-government approach to address adversary shaping-and-influence campaigns or the capability to properly shape the IE in its favor.

In order to show why this is the case, it is helpful to look at the three most likely U.S. entities with capabilities to compete against adversary information warfare campaigns. These include: an independent U.S. government agency, the U.S. Agency for Global Media (USAGM); the Department of Defense’s Joint Information Operations Warfare Center (JIOWC); and the State Department’s Global Engagement Center (GEC). There are also numerous operational level DoD and Department of State entities existing at the Combatant Command and Embassy level, however, due to the strategic nature of the threat we limit our discussion to the three most strategic entities across the USG.

U.S. Agency for Global Media (USAGM)

Countering information warfare is not a new need for the United States. The Cold War was rife with Soviet attempts to control the information environment. In order to counter that challenge the United States created the United States Information Agency (USIA) in 1953. At the height of the Cold War, USIA had an annual operational budget of $2 billion and employed a professional staff of over 10,000 spread across 150 countries, it was also granted the authorities to protect U.S. interests in the information environment. However, following the Cold War, the USIA was disbanded in 1999 and broadcasting functions including the Voice of America, the Office of Cuba Broadcasting, Radio Free Europe, Radio Free Asia, Radio Liberty, and Middle East

\(^{44}\) https://www.factcheck.org/2020/04/conspiracy-theory-misinterprets-goals-of-gates-foundation/
\(^{46}\) https://www.pbs.org/newshour/show/the-dangerous-global-flood-of-misinformation-surrounding-covid-19
Broadcasting Networks were consolidated under an independent entity (separate from the State Department) known as the U.S. Agency for Global Media (formerly known as the Broadcasting Board of Governors)\(^7\). With the restructuring came a drastic cut in resources and mission scope. The USAGM serves as the governing body for all nonmilitary U.S. broadcasting and provides programming in 56 languages. The USAM mission is to inform, engage and connect people around the world in support of freedom and democracy, which is effective in shaping different national interests, however, unlike its predecessor the USIA, it is not chartered, funded, equipped, nor does it have the authority to conduct information operations to counter adversarial propaganda and misinformation. Thus, although USAGM is one of the best aligned U.S. organizations available to counter complex information warfare campaigns, it is under-resourced and does not possess the requisite authorities to do so.

**DoD Joint Information Operations Warfare Center (JIOWC)**

The JIOWC is the DoD’s highest-level IO entity and reports directly to the Joint Chiefs of Staff. As the DoD’s only strategic level IO entity not aligned to a Geographic or Functional Combatant Command it is positioned as the best Joint entity capable of countering a complex information warfare campaign. However, much like the USAGM, JIOWC is not resourced, chartered nor funded to do so. Most of the resourced Information Operations capability in the DoD exist under Geographic Combatant Commanders who can task these entities to protect U.S. interests under their geographically limited authorities. Additionally, outside of declared hostilities, the Department of State Ambassador in each country has the lead on U.S. messaging within that country. Thus, even though the DoD has the most resources to counter a complex information campaign, its ability is hindered by a lack of authority when no open conflict has been declared.

Although the JIOWC is not limited by specific combatant command authorities or lack thereof, its mission as currently constituted is to “support the Joint Staff in improving DoD ability to meet combatant command information-related requirements, improve development of information-related capabilities and ensure operational integration and coherence across combatant commands and other DoD activities”\(^8\). Nowhere in the Chairman of Joint Chief of Staff Instruction is the directive to assist with countering adversary narratives, or assist with disseminating a national narrative. The closest this organization comes to assisting with the development of a national narrative is the use of Military Information Support Operations (MISO) and Military Deception in support of a geographic or functional combatant commander. However, these activities are operationally dependent, rely on declared hostilities, and do not fit national-strategic messaging.

At the operational level, the DoD uses Information Operations, which is not a singular entity, but a conglomeration of various information related capabilities (IRCs). Each IRC has its own set of authorities and requires varying levels of coordination. Within the Combatant Commands and the Services Major Commands, there are organizations that are tasked with understanding current threats within the global IE. However, even if these organizations have the capability to disseminate messages in support of specific narratives, they must receive the proper legal authority, and receive approval through a complex chain of command. By the time this occurs,

\(^7\) https://www.federalregister.gov/agencies/broadcasting-board-of-governors
\(^8\) CJCSI 5125.01, 1 Sept 2011
the IE has evolved and the opportunity to shape and influence the IE has been missed. The DoD also has capabilities to counter the spread of misinformation and propaganda primarily through its Public Affairs (PA) and Military Information Support Operations (MISO) forces. Both capabilities are constrained under multiple layers of approval and in peacetime conditions struggle to get their capabilities into the fight in a timely manner.49

Thus, although the DoD is the most heavily resourced government entity capable of defending against information warfare campaigns, these campaigns often occur in the “grey zone” before active hostilities have been declared, limiting the authority of the DoD to act. When the DoD is able to act, it is usually under the direction of a geographic or functional command that is limited in scope.

United States Department of State Global Engagement Center (GEC)

The last remaining entity that could counter a complex information warfare campaign is the Department of State’s Global Engagement Center (GEC). Much like the DoD, the State Department has recognized its need to overcome the challenges created by the abolition of USIA and better compete in the information environment. In order to do this, the U.S. Government created the GEC in March 14, 2016 by executive order. The GEC is tasked to “lead the coordination, integration and synchronization of government-wide communications activities directed at foreign audiences abroad in order to counter the messaging and diminish the influence of international terrorist organizations”50. The GEC’s charter was expanded in December 2016 to "counter foreign state and non-state propaganda and disinformation efforts"5152.

Thus, unlike USAGM and JIOWC, the GEC is tasked with leading and synchronizing U.S. messaging efforts at the national level. The GEC is currently the lead entity for identifying the CCP’s misinformation campaign. Despite the authorities and charter to do so, it has faced numerous challenges including: funding shortfalls; political red tape;53 and questions regarding its ability to handle the crisis in front of it54. Again, unlike the USIA which was structured for a whole of government response, the current structure of the GEC is more like a Geographic Task Force with limited resources, authorities and capabilities. As the GEC coordinator stated regarding Information Warfare “this is a long-term challenge”55, however, as currently constituted the GEC is unable to meet this long-term challenge.

49 For PA specifically guidance originates from the Office of the Secretary of Defense, then to the Combatant Command for additional guidance, and finally to Major Command for final guidance and tasking. This process can take significant time.
51 https://fas.org/sgp/crs/row/IN10744.pdf
52 https://www.brookings.edu/blog/fixgov/2017/10/27/secretary-tillerson-is-doing-the-right-thing-so-why-is-congress-bashing-him/
53 https://foreignpolicy.com/2019/02/07/with-new-appointment-state-department-ramps-up-war-against-foreign-propaganda/


**Organizational Structure Concerns**

The inability to counter a complex information warfare campaign is not the fault of any of these organizations. Each organization is full of capable information experts doing their best to respond to complex challenges. The U.S. inability to respond to information warfare is a structural problem. The lack of a single, fully resourced, government function, will always leave fragmented, under resourced, and under authorized entities doing the best they can. Unfortunately, COVID-19 has reconfirmed that this U.S. approach results in delayed, disorganized responses, and missed opportunities to favorably shape the IE for the U.S. and its allies.

To summarize our argument thus far, the U.S. currently has an independent agency; the USAGM which is not able to counter adversarial IO due to lack of resources and authorities. The DoD’s highest IO related entity, the JIOWC, is restrained to assisting operational planning for combatant commands mostly during times of conflict. The U.S. State Department has an organization with relatively limited means—the GEC—which although its mission has recently expanded to identify, expose, and counter adversary information operations, it currently does not have the resources to provide a whole of government approach. Additionally, the GEC is not charged with conducting offensive Information Operations in order to increase the cost to adversaries who wage information warfare against the U.S. and its interests and potentially alter this damaging behavior. These organizations independently provide the U.S. capabilities, however their disjointed, often independent efforts have left a hole in the United States ability to counter complex information warfare campaigns.

An increased capability and synchronized effort to counter adversaries is required in order to shape the IE to favor the U.S. and its allies. One way to do this is to combine the shaping-and-influence efforts of USAGM, the authorities of the GEC, and the resources, regional expertise and offensive capabilities available to the DoD during times of conflict.

5. **Recommendation**

As we have argued, we believe the current structure of government entities with the capabilities to combating information warfare campaigns has left the U.S. unable to counter China’s active COVID-19 information warfare campaign. For the U.S. to successfully compete in the IE, it requires a whole of government approach to rapidly bring significant resources and capabilities to reduce the spread of misinformation and counter adversary tactics that endanger U.S. citizens and its allies. Our recommended approach is to reactivate the defunct USIA which existed from 1953 until 1999 to counter Soviet messaging, and provide this reactivated organization with similar, if not greater resources and authorities than it had during the Cold War. We believe an effort of this magnitude is required in order for the U.S. to successfully compete with China, Russia, Iran and other potential competitors in the IE.

The reactivated USIA should have two primary missions, a lead role in defensive information warfare to protect the U.S., its interests, and allies; a supporting role in offensive information warfare designed to increase the cost to adversaries who choose to wage information warfare against U.S. interests and to change adversarial decision making. The GEC could serve as the
core of this organization and expand to meet the new threat. The broadcasting capabilities of the USAGM should also be fully absorbed into the new organization and the USAGM dissolved. The GEC would bring with it the authorities established in its 2016 directive. Additionally, the new USIA should be granted additional authorities as it stands up. This realigned USIA with the GEC as its core and the broadcasting and other capabilities currently executed under the USAGM fully integrated would be the center of the United States defensive information warfare capability.

This defensive mission would focus on identifying adversary information warfare campaigns and, once identified, leveraging all available assets in a combined, whole of government response. Additionally, the new USIA would lead efforts to proactively shape the information environment against future adversary attempts at malign influence. The DoD would assist USIA in a supporting role to identify and counter information warfare campaigns and proactively shape the information environment.

When an information warfare campaign threatens vital U.S. interests or places U.S. citizens at risk, the U.S. should have a full offensive information warfare capability to protect the nation. Although USIA would serve as the lead synchronizer of U.S. efforts, the DoD would take the lead role in employing offensive information warfare capabilities against any adversaries. A fully resourced and empowered JIOWC, co-located with its USIA counterparts to ensure appropriate coordination, would be the supported command during offensive operations. Each functional and geographic combatant command would also supply Information Warfare liaisons to the JIOWC to ensure efforts were coordinated and that command interests were met.

These two entities, a reestablished and reinvigorated USIA along with the DoD and its fully resourced and empowered JIOWC, co-located and cross-pollinated with expertise and manpower would form the core of the whole of government information warfare capability. This capability would allow the U.S. to counter complex information warfare campaigns, to proactively shape the information environment, and protect its citizens and interests across the world.

---

56 This is opposite of the DoD’s current approach where JIOWC sends liaisons to the Combatant Commands. We argue in a whole of government and global approach the roles should be reversed with JIOWC empowered as the DoD lead and Global Combatant Commands providing support.

57 We envision the USIA as an independent agency, reporting directly to the National Security Council. It would have intense coordination with the State Department, DoD, and additional federal agencies. This ensures that whole-of-government coordination is achieved with foreign messaging. It can integrate State Department and DoD personnel; State Department foreign service officers, DoD PA members, IO officers and operators can integrate into the USIA on a regular, or as needed basis in order to provide assistance, surge capabilities, or expertise for specialized situations. Furthermore, DoD PA and IO guidance could be synchronized with USIA themes and message to ensure synchronization.

Operating in this manner would place the proper authorities within the USIA, and coordinating with the DoD would bring the funding, personnel, training, and organizational infrastructure the DoD already has. This would include analysts trained in Publicly Available Information (PAI), matched with DoD IO operatives who can identify, and counter misinformation through various media platforms. In addition to personnel necessary for running broadcasting programs and the current expertise employed by the USAGM and GEC, the USIA would also include
6. Conclusion

Our adversaries are currently waging information warfare against our interests. These efforts have been complex, widespread and effective. China’s uncontested ability to maneuver in the information environment has increased the challenge of combating the current global pandemic. China has sown confusion regarding the nature of the COVID-19 threat, attempted to promote their own response while discrediting the response of its competitors, and attempted to cast blame on the U.S. in an effort to reduce the negative effects to China’s global reputation.

Our proposed whole of government construct, that reinstitutes and resources the USIA, with various information capabilities either falling under this organization or directly partnering with it in the case of the DoD would vastly increase U.S. capabilities to operate in the information environment and when necessary wage information warfare. Having an organization such as the USIA proposed in place, with the necessary authorities and resources could have mitigated the success of China’s information warfare campaign and saved countless U.S. and worldwide lives, reduced worldwide economic impacts and protected U.S. interests.

Specifically, we believe the proposed USIA would have been able to quickly identify China’s attempt to suppress information regarding the transmissibility of COVID-19. This information could then have been used to warn the WHO and the world of the misinformation regarding the severity of the virus. This would have prompted the WHO to issue appropriate guidance that could have stopped or slowed the virus spread. Additionally, the USIA could also have proactively worked to shape the IE and limit the effects on the U.S. and the rest of the world against the spread of false and misleading narratives surrounding the virus emanating from China and other nefarious actors.

Second, as part of an offensive strategic shaping-and-influence campaign, the USIA in partnership with the DoD would have had the ability to expose China’s failures to contain the virus and used various capabilities to expose these failures to the rest of the world and increase the cost to China for engaging in this information warfare campaign.

It is important to recognize that while COVID-19 was the example used, these tactics can be, have been, and continue to be applied in order to affect the IE. Adversaries, or potential adversaries, such as Russia and Iran have also engaged in misinformation campaigns aimed at causing confusion and shifting blame in a variety of political, military or economic situations. Even when the world recovers from COVID-19, the U.S. and its allies are still at risk in the global IE without a whole-of-government approach.

specialists in strategic communications, social and political science. This enables the USIA to take adversarial narratives and map them against social and political trends while developing both counter and parallel narratives.

An example of this could be the amplification of China’s discrimination towards Africans potentially damaging China’s long-term investment strategy on the African continent.