

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE (DD-MM-YYYY) 10-05-2019		2. REPORT TYPE Master's of Military Studies		3. DATES COVERED (From - To) SEP 2018 - APR 2019	
4. TITLE AND SUBTITLE Social Media Warfare, A New Cost-Imposition Strategy For Great Power Competition Through Education and Collaboration				5a. CONTRACT NUMBER N/A	
				5b. GRANT NUMBER N/A	
				5c. PROGRAM ELEMENT NUMBER N/A	
6. AUTHOR(S) Mulloy, Benjamin, M, Lieutenant Commander, USN				5d. PROJECT NUMBER N/A	
				5e. TASK NUMBER N/A	
				5f. WORK UNIT NUMBER N/A	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) USMC Command and Staff College Marine Corps University 2076 South Street Quantico, VA 22134-5068				8. PERFORMING ORGANIZATION REPORT NUMBER N/A	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) USMC Command and Staff College Marine Corps University 2076 South Street Quantico, VA 22134-5068				10. SPONSOR/MONITOR'S ACRONYM(S) Dr. Benjamin Jensen	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S) N/A	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited.					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT THIS PAPER WILL INTRODUCE TWO ENHANCED CONCEPTS FOR COPING WITH THE CHANGING CHARACTER OF INFORMATION WARFARE, AND EXAMINES SEVERAL MODERN CASE STUDIES INVOLVING BOTH POSITIVE AND NEGATIVE USES OF SOCIAL MEDIA. BY IMPOSING AN EVER-INCREASING COST ON OUR ADVERSARIES TO MANIPULATE AND CONTROL THEIR NATION'S INTERNET INFRASTRUCTURE, THE U.S. CAN BE ON THE WINNING END OF A NEW COST-BASED COMPETITIVE STRATEGY.					
15. SUBJECT TERMS SOCIAL MEDIA WARFARE, INFORMATION WARFARE, DISINFORMATION, INTERNET, COST-IMPOSITION, STRATEGY, INTERAGENCY, JOINT, RUSSIA, CHINA, ISIL					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (Include area code)
Unclass	Unclass	Unclass	UU	39	USMC Command and Staff College (703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE:

SOCIAL MEDIA WARFARE:
A NEW COST-IMPOSITION STRATEGY FOR GREAT POWER COMPETITION
THROUGH EDUCATION AND COLLABORATION

AUTHOR:

LCDR BENJAMIN M. MULLOY

AY 2018-19

Mentor and Oral Defense Committee Member: Dr. Benjamin Finn
Approved: [Signature]
Date: 4/29/19

Oral Defense Committee Member: Nathan M. Padgett, PhD
Approved: [Signature]
Date: 4/29/2019

Executive Summary

Title: Social Media Warfare: A New Cost-Imposition Strategy for Great Power Competition through Education and Collaboration

Author: Lieutenant Commander Benjamin M. Mulloy, United States Navy

Thesis: The United States' slow response to Russia's election meddling of 2016 and reactionary counter to ISIL's social media warfare campaigns requires inter-governmental collaboration and coordination as well as enhanced career path options to respond effectively in the information domain. An expanded unrestricted line officer information warfare subspecialty career path and a new joint interagency disinformation defense center (JIDDC) can unsustainably increase the financial burden of information control for America's autocratic adversaries.

Discussion: This paper will introduce two enhanced concepts for coping with the changing character of information warfare, and examines several modern case studies involving both positive and negative uses of social media. By imposing an ever-increasing cost on our adversaries to manipulate and control their nation's internet infrastructure, the U.S. can be on the winning end of a cost-based competitive strategy. America's first amendment creates an asymmetric opportunity for autocratic regimes like Russia, wishing to disrupt and dismantle western democracies through information warfare. However, the cost to maintain internet sovereignty is a heavy financial burden that should be exploited by America and its allies through interagency collaboration and higher education.

Conclusion: The JIDDC, as well as information warfare subspecialty codes within unrestricted line officers, will ensure information warfare is carried out with the highest degree of proficiency, contributing to the unsustainable increasing costs of internet surveillance and control for adversary's central governments.

Preface

I would like to thank my wife Lauren first and foremost for the love and support, without her compassion and trust I would not have had the time required to research and write this paper. Her ability to provide a stable household will never be appreciated enough. My two children Tenley and Tate are too young to understand the sacrifices they have made being born into a military family, but one day, through social media and the documented history of their lives I hope they look back at those photos, captions, and possibly even this paper, and think above all else, they were loved.

I would also like to thank @lu_mulloy, also my wife, and her 30,000 followers. If it were not for her, and the incredible impact she has made on thousands of lives, I would probably not have had the motivation to stop writing my thesis paper halfway through and change topics. While many rightfully see social media as a place for depression, extremists, trolls, and polarizing political rhetoric, I was able to see a more positive side firsthand. When I was with my wife during our son Tate's second ultrasound, it was discovered he would be born without his left hand. The fear of the unknown at that moment was paralyzing and the line of questions, unending. These feelings were quickly extinguished on the day of his birth, as fear gave way to love, and anguish turned to hope. What followed was a journey of discovery, for both my wife and I, but also her "followers". The expressions of support from all over the world, the life changing conversations with expecting moms going through the same thing, and the normalizing of limb differences, could not have been achieved without social media. The ability to impact and influence on social media is an incredible gift, but one that is not without nuance, skill, and hard work, something my wife has acquired over several years, skills I hope the U.S. military learns in the years to come.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

QUOTATION FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.

List of Illustrations

	Page
Figure 1: JIATF-South’s Integrated Team.....	10
Figure 2: Example Officers Potential Career Progression.....	14
Figure 3: Kylie Jenner’s Snapchat Tweet	18
Figure 4: Snapchat Stock’s Decline.....	18
Figure 5: Circular Error Probability (CEP) from WWII to 1998.....	20
Figure 6: Taylor Swift’s Instagram post during Tennessee Senate Race	21
Figure 7: Tennessee Senate race prior to Taylor Swift’s intervention.....	22
Figure 8: Tennessee Senate race after Taylor Swift’s intervention	23
Figure 9: ISIL Tweet frequency following GLOWING SYMPHONY	28
Figure 10: Traditional vs Enhanced Unrestricted Warfare Career Paths.....	30
Figure 11: Traditional + Enhanced Unrestricted Warfare Career Paths.....	31

Table of Contents

	Page
EXECUTIVE SUMMARY	2
PREFACE.....	3
GENERAL.....	7
PURPOSE.....	8
TIME HORIZONS, ASSUMPTIONS, AND RISKS.....	12
DESCRIPTION OF THE MILITARY PROBLEM AND OPPORTUNITY.....	15
CENTRAL IDEA.....	17
APPLICATION AND INTEGRATION OF MILITARY FUNCTIONS	25
NECESSARY CAPABILITIES	26
ISIL CASE STUDY	26
RECOMMENDATIONS.....	29
INSIGHTS FROM WAR GAMES.....	32
BIBLIOGRAPHY.....	34

General

The far-reaching impacts of social media, combined with the widespread availability of wireless communication are changing the character of war.¹ Actors ranging from violent extremists, autocratic regimes, and dictators, have manipulated its use, often with great success in furthering their causes and influencing populations well beyond what would have been possible just a decade prior.² The acceleration of its adoption is only increasing through the lowering cost of mobile phones and influx of cheap internet providers, resulting in less developed nations being more connected than ever before. The greatest increases in mobile phone and social media use are in areas that have historically been plagued by conflict or are currently experiencing conflict, such as the Middle East and Africa.³ Contrasting this acceleration in use, are the highly technical and capable nations of Russia and China. Both countries are developing exceedingly sophisticated networks and propaganda machines that challenge the global order. The United States should immediately create the JIDDC to counter sophisticated foreign disinformation attacks, as well as prepare all warfare communities for competing in the information space through the option of a new information warfare career path amongst unrestricted line officers.

There is currently no definition for information warfare within official U.S. government documents, however, the Congressional Research Service defines it as, “A strategy for the use and management of information to pursue a competitive advantage, including both offensive and defensive operations.”⁴ Disinformation is “intentionally false information, examples include planting false news stories in the media and tampering private and/or classified communications before their widespread release.”⁵ Title 10 U.S.C. 2241 prohibits Department of Defense (DOD) from domestic publicity or propaganda, although it stops short of defining these terms.⁶ All four U.S. military service branches post daily on their internationally accessible, official social media

accounts, representative of their liberal interpretation of this provision. There is a lack of clarity on this issue that should be handled by a new joint interagency team of highly capable information operators. A clear line should be drawn between education and indoctrination, between propaganda and identification. A new entity should be built around the education and identification of disinformation from Russia, China, Iran, North Korea, and ISIS, the five prioritized countries listed within the 2018 National Defense Strategy.⁷ The JIDDC should be tasked with educating the American public and key policy decision-makers on specific instances of disinformation, ensuring a clear distinction between propaganda and education.

Purpose

This paper introduces two integrated concepts for coping with the new operating challenges within the information warfare domain. The first is to establish the JIDDC, with the mission of identifying foreign disinformation campaigns directed at Americans on social media. The JIDDC should not be considered a replacement for the U.S. Information Agency (USIA), a now defunct agency created during the Cold War in response to Soviet Union propaganda.⁸ The USIA's primary mandate in the post-cold war era was to influence foreign audiences about U.S.-style democracy and markets.⁹ Prior to the 1990s, the mission of the USIA was inseparable from cold war geopolitics, whose main purpose was to win the battle of men's minds against Soviet propaganda.¹⁰ The JIDDC does not seek to win the battle of minds, instead it should present a clearer picture of reality by educating and disclosing to the public instances of foreign disinformation. Before its demise, however, the USIA managed to deliver a financial blow to the Soviet Union, contributing to the overall collapse. Internal memos from the USIA indicated, "Soviet pleading to suspend disinformation programs were a clear sign that America's efforts to raise the

cost of Soviet disinformation were working.”¹¹ As strategic competition becomes central to national security, utilizing any domain or concept capable of generating a cost advantage should be explored.

The Global Engagement Center (GEC), created in 2016 under the Department of State, is the current U.S. government entity mandated with countering propaganda and disinformation from international terrorist organizations and foreign countries.¹² The GEC has a FY19 budget request for \$55 million dollars.¹³ For comparison, a recent DOD audit by Ernst and Young discovered \$100 million worth of DOD assets that couldn’t be supported with evidence or documentation.¹⁴ The GEC requires significantly more funding, support, and coordination from the Department of Defense if it is to fulfil its mandate to counter disinformation. The U.S. military should integrate the GEC into the JIDDC by following the golden standard of interagency coordination, JIATF-South, as its model.

JIATF-South began as a response to a drug related shooting spree that took place in broad daylight at a suburban Miami mall in 1979. This represented the tipping point for the current presidential administration’s tolerance of drug related crime. What followed was “The Vice President’s Task Force on South Florida”, created in 1982.¹⁵ This new task force comprised hundreds of agents from the Drug Enforcement Agency (DEA), the Federal Bureau of Investigation (FBI), with support from the Army, and the Navy, to name a few. This new task force would later become responsible for over 50 percent of the total cocaine seized by U.S. law enforcement agencies.¹⁶ The graphic below demonstrates the enormous level of integration required to achieve organizational success.

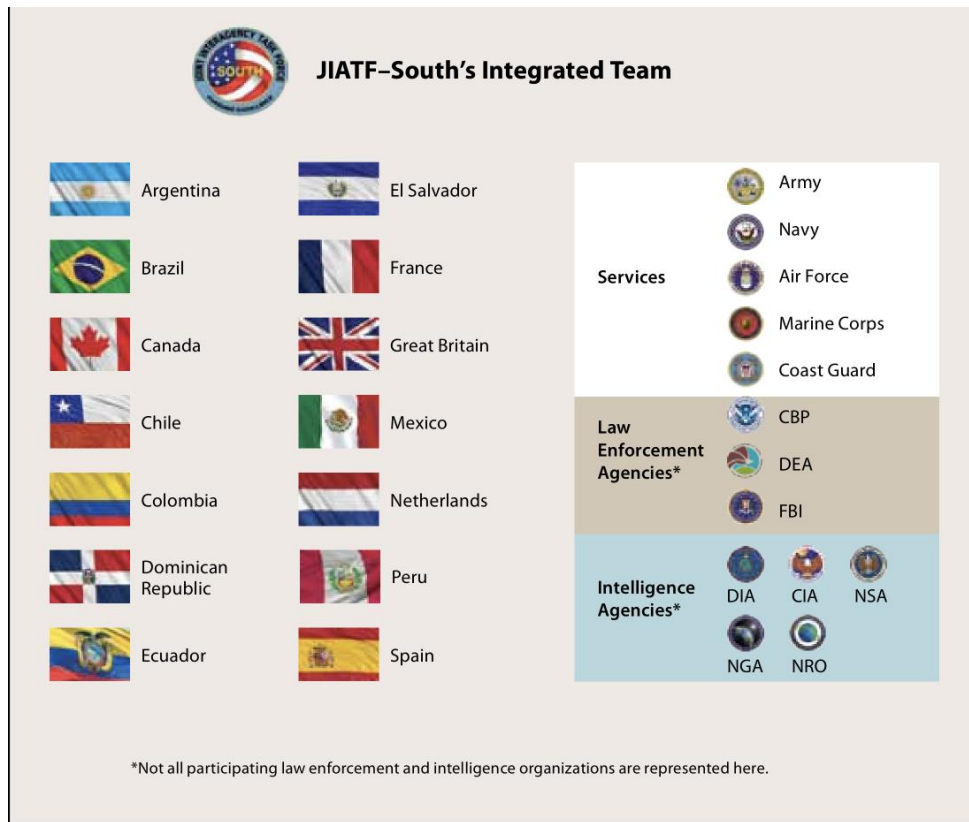


Figure 1: JIATF-South's Integrated Team

The figure above represents years of relationship building, along with appropriate legislation and authorities. The JIDDC would look similar to the above figure, but initially much smaller to increase the flexibility and agility needed to rapidly evolve the structure, decision-making, and culture of the organization. It would also center around NATO nations currently engaged in combating Russian disinformation campaigns, but would not exclude any country willing to participate. The one key factor the JIDDC has in common with JIATF-South is the evaluation metric. For JIATF-South, metric tons of illegal drugs seized is their implicit metric for operational success. For the JIDDC, the number of disinformation tweets, social media pages, hashtags, and posts revealed as disinformation would represent the metric for JIDDC's operational success. By attaching a clear metric, an organization can both demonstrate its value, while also streamlining organizational efficiencies to increase those metrics.

The second concept this paper will explore, is the establishment of an information warfare sub-specialty code for 10 to 20% of all new unrestricted line warfare officers, or line officers. This enhanced requirement is designed to ensure America is best postured to defeat adversaries within the information space during a future conflict, with the desired end state of creating a cost imbalance for China and Russia to continue their censorship over the content of their respective country's internet. By supplying every line officer community with an information warfare capability, synchronization and coordination of national level strategic messages will become more fluid within tactical and operational level planning. The case study on Joint Task Force (JTF) ARES presented later in this paper demonstrates how this level of integration can achieve a specific desired effect.

These potential military solutions enable the U.S. military to compete and win in the social media environment, in order to support the first and third pillars of the current National Security Strategy (NSS). The first pillar is to Protect the American People, the Homeland, and the American Way of Life.¹⁷ The DOD should be given sufficient authority and funding to assume the role as the leading government entity responsible for the identification and exposition of foreign disinformation campaigns designed to destabilize the American way of life. The President of the United States proposed budget requests for FY2020 are \$718 billion for the DOD, \$40 billion for Department of State (DOS) and USAID, and \$51.7 billion for the Department of Homeland Security (DHS).¹⁸ The DHS is mandated to defend and secure Federal cyberspace, The DOS is proposing over \$500 million to counter Russian malign influence, and the DOD budget prioritizes strategic competition with China and Russia.¹⁹ These three entities should centralize these missions within the JIDDC, with the DOD as the lead entity. The third pillar of the NSS is Preserve Peace Through Strength, this can be achieved through combining information warfare and

traditional warfare methods. To do this, every unrestricted line community should have within its ranks, a handful of officers capable of integrating information warfare within the remaining six warfighting functions. This integration will ensure information will no longer be an enabler of physical power, it will become an instrument of power in its own right.²⁰ By applying the lessons learned from modern social media case studies, as well as modern military case studies, the U.S. military can deny certain state actors like Russia, and ISIL, the capability to disrupt and fracture free democratic societies.

Subspecialties are professional disciplines secondary to an officer's primary specialty or designator earned through meeting Education Skill Requirements (ESRs) as well as Core Skill Requirements (CSRs). They require a Master's or higher degree program from an institution of higher learned from an accredited agency.²¹

Time Horizons, Assumptions, and Risks

Immediate implementation of the JIDDC for assuming the responsibility of defending against foreign interference on social media will convey to the American public that the DOD is capable of defending against all foreign enemies, in whatever domain they present themselves as a threat to the American way of life. Congressional approval for adopting the JIDDC, with private sector coordination and participation would potentially take years. However, the appetite amongst the U.S. population for some competent intervention on social media is reaching insatiable levels, as seen by the recent outrage at the New Zealand Mosque shooter's ability to proliferate his manifesto, as well as video of his shooting rampage on Facebook, YouTube, and Twitter. A recent revelation that Facebook stored millions of passwords in plain text, is an egregiously irresponsible misstep from such a well-resourced tech company, and further demon-

strates the requirement for a more competent authority to decipher and educate the public on social media disinformation.²² The concept for the JIDDC should be delivered and accepted to Congress as a bi-partisan issue that could reach approval within a few years, potentially shorter, depending on how many more security missteps social media companies will inevitably continue to make.

The creation of an enhanced requirement for an information warfare subspecialty within unrestricted warfare communities will take approximately a decade. This length is due to the challenges associated with service assignment requirements and coordination required across multiple services. For example, the United States Naval Academy will graduate approximately 1,069 midshipmen in the spring of 2019. Of these midshipmen, only twenty-one will go into the Cryptologic warfare community, and six will become information professionals. These twenty-seven are selected from a group of midshipmen not physically qualified to enter the unrestricted line community, severely limiting the talent pool of potential candidates. If the U.S. Navy wants to fight and win in the information environment, it must acquire the best and brightest talent available, and should allow physically qualified midshipmen, their fellow Officer Candidate School (OCS), and Reserve Officers' Training Corps (ROTC) brethren to select information warfare, both as a sub-specialty code, within their respective unrestricted line communities, and directly to restricted line communities. The Naval Academy currently offers computer science, cyber science, and information technology majors, with courses in advanced database systems, computer algorithms, social engineering, and cyber law and ethics, with all other service academies offering similar courses. These core skills translate well into careers as both an unrestricted line officer and an information warfare professional.

The Joint Concept for Operating in the Information Environment (JCOIE) states the Joint force must, “Understand information, the informational aspects of military activities, and informational power.”²³ There can be no substitute for understanding without education and experience. To achieve the level of education needed to compete in this rapidly adapting and complex environment, the U.S. military should support an information warfare sub-specialty for 10 to 20% of unrestricted line officer accessions. As an example of what this would look like in a typical career timeline, the figure below walks through an unrestricted line Naval aviator’s career in the first 11 years of service with the information warfare subspecialty track. The years after the initial 11 would follow a standard path from O-4 Department Head (DH) through O-5 Commanding Officer (CO) and flag ranks.

Aviation (H-60) Officer (I) Yearly Career Progression

	0-2	2-4	4-6	6-8	8-10	10-11
Flight School		Navy Expeditionary Seahawk Squadron				
Air Force for Primary Flight Training		Deploy with USMC ARG/MEU	Army Blackhawk Squadron	Resident Naval Post Graduate School Masters Degree	Air Force Pavement Squadron	Resident JPME I
Navy for Advanced Flight Training		First Sea Tour	Aircraft CDR Qual	Information Sciences	Aircraft CDR Tour	Non-Navy School
Computer or Cyber Science Major		Innovation Officer	PAO	None	MX Officer	None

Figure 2: Example Officer’s Potential Career Progression

This concept creates institutionalized legitimacy on the value of information warfare through new information warfare subspecialties. By endowing unrestricted line officers with the

tools required to compete in the joint information domain, the U.S. military can move from a reactionary force in this space to one capable of commanding the global narrative and seizing the initiative within this environment for years to come.

Description of the Military Problem and Opportunity

In 2016, the Kremlin attacked the United States through a coordinated influence operation targeting the presidential election. Russia's political warfare against the west has revealed its full spectrum strategy of undermining democratic institutions, sowing distrust amongst western allies, and destabilizing societies by amplifying what divides them.²⁴ While social media companies like Twitter and Facebook have taken steps to remove Russian-linked accounts as well as disinformation attacks, artificially intelligent accounts and deep-fakes are finding new ways around these measures.²⁵ The U.S. requires an immediate response through the implementation of the JIDDC, while planning for a more technically complex future through information warfare subspecialties within all warfare communities.

In 1998, China launched the beginnings of what is commonly referred to today as the Chinese Firewall.²⁶ Over the next two decades, China would continue to develop the most expansive internet surveillance network in history, positively controlling every word on the internet being disseminated throughout the entire country of China. For a time, the entire country of Panama disappeared from the Chinese internet because of the Panama Papers scandal the Chinese Government ordered to be deleted from their internet.²⁷ It is simply a matter of time before this marvel of cyber and social engineering is replicated amongst unfriendly non-democratic or autocratic adversaries. This represents a serious challenge for western society, but specifically the United States and its allies in a potential future conflict with one of these nations. If a Chinese destroyer is sunk in the Pacific and no one in China is around to hear it, did it really compel the

Chinese will? If Russian little green men are detained for war crimes and the Russian populace is not informed, how much impact does that have on the political will of its leaders? The challenges of fighting against an enemy with complete sovereignty over its internet and information requires innovative and educated officers for competing in this environment. The military opportunity is small, but like the Maginot line in France proved, nothing is impenetrable, and no defense is impermeable.

Britain cut Germany's transatlantic cables at the beginning of World War I, perhaps in the next war, new fiber optic cables will not be cut, but instead need to be laid.²⁸ Another opportunity for the United States lies in the massive amount of resources required to restrict the information of an entire nation. The cost for countries like China or Russia to maintain this level of control represents a cost advantage for America in a potential future conflict. Exploiting this advantage will require advanced knowledge in fields such as data science and local languages and cultures. The U.S. military must recognize the complexity and urgency of this problem and prepare through information defense at home while also developing the warriors of tomorrow that will be able to challenge any adversary in the information domain.

The cost advantage is realized after continued pressure on exposing Russian government's disinformation results in Russian parliament increasing controls and requirements from its national internet service providers (ISPs). A Russian newspaper, RBC, cites an estimate of 134 billion rubles, or \$2.1 billion, is required to compensate telecom operators each year for their compliance with the Kremlin's current internet regulations.²⁹ A new sovereign internet bill in Russian parliament passed the second round of voting on April 11, 2019. An additional \$304 million is estimated for procurement, installation, and refinement, to implement the new legisla-

tion.³⁰ To accelerate this cost-imposition strategy, the U.S. will have to continue to pressure Russia, and similar regimes, through more sophisticated disinformation capabilities like the JIDDC and enhancing the current military officer corps.

The dichotomy of too much enemy access to Americans during a potential conflict, and not enough access or influence for Americans to bend the enemy's will during a conflict is a challenge that needs to be answered.³¹ As the Chinese and Russian models of censorship spread to other autocratic and socialist regimes hostile to the American way of life, the asymmetric advantage for American enemies widens in their favor, but at significant cost. If the U.S. military is to become a global leader in controlling the narrative and managing perceptions within social media, it should rapidly adapt through increased responsibilities and authorities, education, and updated occupational subspecialty accession billets.

Central Idea

The following examples highlight both the complexities and intricacies of influence on social media within western societies. A generalized view of social media's capabilities and vulnerabilities also demonstrate the need for more education on the subject. On February 21, 2018 Kylie Jenner tweeted her displeasure with the social media application Snapchat. This seemingly innocent tweet by a 20-year-old reality TV star, seen by her 24.5 million Twitter followers at the time, would be widely attributed to a precipitous drop in the social media company Snapchat's stock price.³²



Figure 3: Kylie Jenner Snapchat Tweet

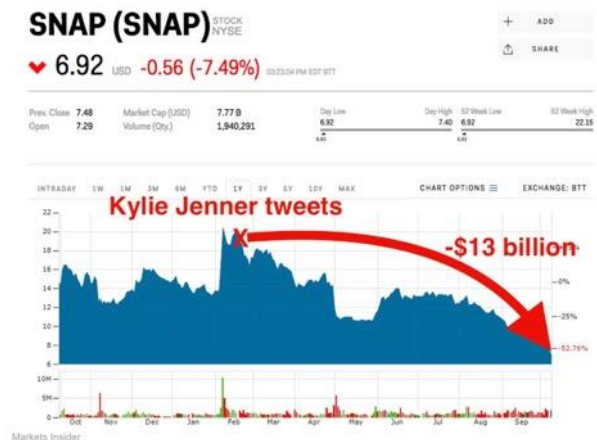


Figure 4: Snapchat Stock Decline

Her tweet was posted on a Wednesday evening, just after normal stock market trading hours, and by the end of closing the next day, the stock price dropped 6.1%, a total market value of \$1.3 billion.³³ Snapchat Inc.’s stock would continue to decline over the next several months, with many, including Market Insider, attributing her tweet to the stock’s demise. This line of thinking would be a classic case of directly attributing causation to correlation. A day prior to Kylie Jenner’s now famous tweet, Snap Inc. issued a statement in response to a change.org’s petition to remove the latest Snapchat update, which many millions of Snapchat users viewed as uncomfortable at best, and unusable at worst. The change.org’s petition of Snapchat’s new software update had reached over a million digital signatures by February 20th, the day before Jenner’s tweet, laying the groundwork for her tweet to capitalize on an existing narrative within her own personal sphere of influence, or brand.”³⁴

A similar cynosure of eyes fell upon Walter Cronkite during his now infamous, “Cronkite moment” of February 27th, 1968. American disapproval had been growing since the Vietnam war began failing to live up to American political leader’s optimism, and was reaching a boiling point. Following the Tet Offensive, an operation that did not leave a clear victor, Cronkite, a

mega-influencer, or super-spreader, would say during a televised broadcast, “The only rational way out then will be to negotiate, not as victors, but as an honorable people who lived up to their pledge to defend democracy, and did the best they could.”³⁵ This represented a turning point in American sentiment regarding the Vietnam war. The President at the time, Lyndon B. Johnson, was said to have reacted to this statement with, “If I have lost Cronkite, I have lost middle America.”³⁶ This statement’s authenticity is controversial, and its origins debatable, but has continued to be perpetuated as truth, including in the new best-selling book by P. W. Singer, “LikeWar”. By tapping into the existing narrative, Walter Cronkite’s authenticity and influence pushed his American audience to accept a stalemate, alter Lyndon Johnson’s plans for a re-election bid, and serve as lodestar to a captivated audience.

These two case studies, Jenner’s tweet and Cronkite’s moment, would fall closer in line with what Malcolm Gladwell would call “The Tipping Point”; a book describing how small things can make a big difference.³⁷ Both Kylie Jenner and Walter Cronkite can be viewed as means, in the traditional military equation of Strategy = Ends + Ways + Means. By adjusting the end-state to more closely align within a military objective, and utilizing social media as a means, military planners with an information warfare sub-specialty can provide commanders, or themselves, with an increasing pallet of options to achieve their strategic end-state. In Gladwell’s final sentence of his work, he concludes, “With the slightest push—in just the right place—it [the world] can be tipped.”³⁸ The key to Gladwell’s statement is determining where “just the right place” exists. In both the physical and information domains, targeting is challenging, but should be viewed similarly in application.

Similar to the targeting inaccuracies of aerial bombardments, information warfare requires time to develop, while also learning from the mistakes of the past. For decades, the aerial

bombardments of World War II through Vietnam were wildly inaccurate by modern standards, as measured by circular error of probability (CEP).

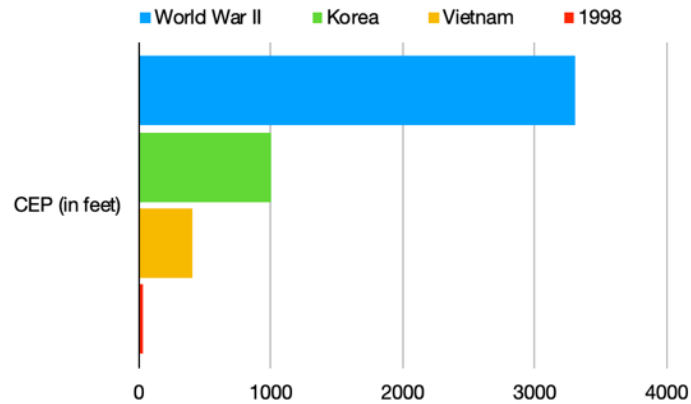


Figure 5: Circular Error Probability (CEP) from WWII to 1998

Determining just the right place was not the primary issue for the U.S. military during this time period, they generally knew where the targets were located, they just needed to hit them. The need for more accurate weaponry, led to the precision weapons revolution. The revolution began with the invention of laser guided munitions in the early 1970s, and reached the upper edge of its limits with the introduction of GPS guided munitions. A modern 500-pound Joint Direct Attack Munition (JDAM), can achieve a CEP of 5 meters when GPS data is available.³⁹ A new era of revolutionary thought, in treating tweets like bombs, and social media influencers like key nodes in an enemy's hierarchy, should similarly be applied to information warfare. Kylie Jenner's Snapchat tweet carried the weight of a modern JDAM, while Walter Cronkite's moment landed with laser guided precision. They both were applied at the right time, within the right narrative, and medium, resulting in a dramatic effect. These small events certainly had at least some effect in tipping the scales of perception amongst their audiences. In order to achieve this level of precision and effects, a high level of understanding in the social media environment is required.

To demonstrate the consequences of failing to adequately understand the information environment, a modern case study, revealed below, highlights the downside of inexperience and ignorance in this space.

This case study on the dangers of ineffective social media usage is a juxtaposition to the aforementioned effects generated from Kylie Jenner’s singular Snapchat tweet and Walter Cronkite’s three-minute monologue. At the time of this writing, Kylie Jenner had 129 million Instagram followers, Taylor Swift had a comparable 115 million. Below is a screenshot from October 7th, 2018, where Swift makes her first foray into political activism, throwing her entire support being the Democratic candidate; Phil Bredesen, in the Tennessee Senate race, and urging her followers to do the same.



Figure 6: Taylor Swift’s Instagram post during Tennessee Senate Race

The timing of this post was critical to its purpose. With only two days left to register to vote, Swift sought to galvanize support from her predominantly young female demographic, an age group with traditionally low voter turnout, to swing the election. Another key aspect to the timing of this post is how close the Senate race was at the time, as seen from the figure below.

The right edge of the graph's x-axis, represents the day before Swift's Instagram post, the race had been close since early September, only beginning to diverge in favor of Bredeesen's opponent, Marsha Blackburn, days before her post.

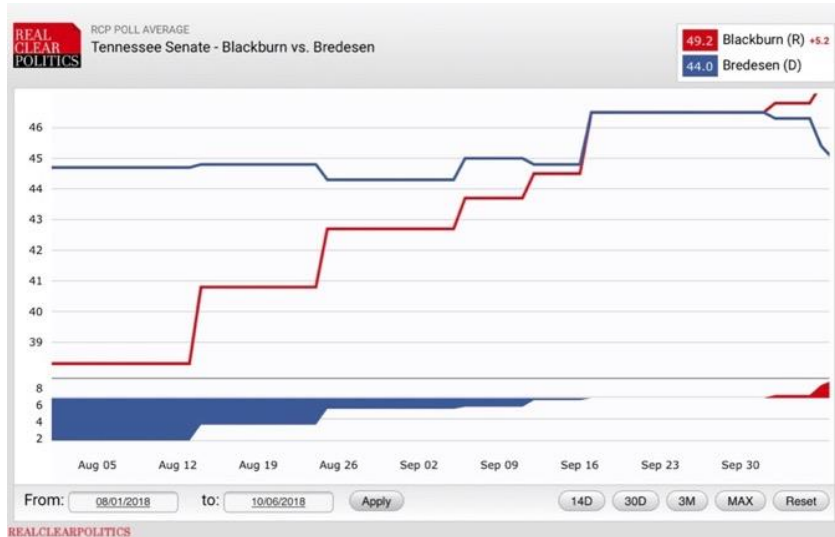


Figure 7: Tennessee Senate race prior to Taylor Swift's intervention

If we were to apply similar logic learned from the Kylie Jenner case, a reasonable conclusion would be to assume Swift's massive and loyal followers could be the tipping point in Democratic candidate, Phil Bredeesen's favor. Jenner and Swift both had similar sizes of devout followers and were authentic in their posts, however, two key differences remained. This was off-brand for Swift and she attempted to go against the presence of a strong counter-narrative. By ignoring these two key facts, the seemingly inevitable outcome of injecting one of the most influential people in America into a tightly run Senate race was flipped on its head. The following figure represents what happened immediately after Swift's Instagram post.

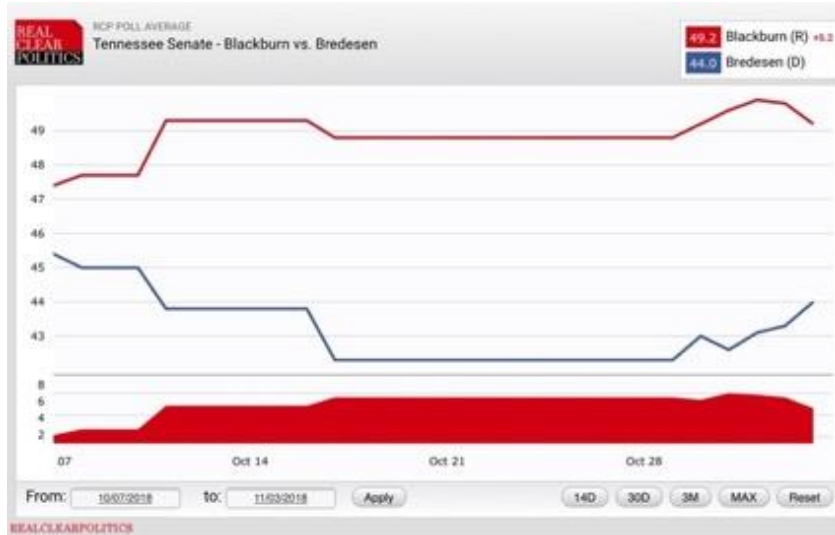


Figure 8: Tennessee Senate race after Taylor Swift’s intervention

The Republican candidate, Marsha Blackburn’s lead only widened after Swift’s plea to her fans. It should be noted, however, the day after Swift’s tweet, vote.org had its second-busiest day of the year with 155,940 unique visitors to its website, up from a daily average of 14,078 visitors a day.⁴⁰ It would appear realistic to conclude Swift’s post was able to generate action, in the form of registered voters. If the effect she was trying to achieve was an increase in voter turnout, she appeared to have achieved it. Unfortunately, that was not the desired effect, and Swift learned swiftly that politics is war by every means. Her attempt to negate Bredesen’s Republican opponent only created advertising for both parties. In Jenner’s case, a consensus was building in her favor, with few opposing her point of view that Snapchat’s update was a problem that needed to be solved.

In Swift’s case, it would be reckless to attribute an entire senate race to a single Instagram post or influencer, just as it is similarly imprudent to attribute \$1.3 billion in market value loss to a single tweet. Over 100 million followers have to count for something though, and fortunately we can quantify influence monetarily. As of July 2018, Kylie Jenner earned \$1 million for each sponsored Instagram post, or the equivalent to approximately eight hellfire missiles.⁴¹⁴²

This analogy would have been entirely irrelevant a decade ago, and even now seems blasphemous to say within military circles, but if war is truly politics by other means, and a battle of wills, social media influencers should not be discounted as a capability, or position to exploit. Suggesting an Instagram post should be used in place of hellfire missiles is also not the appropriate conclusion. However, if Kim Kardashian, a reality TV and social media superstar, with no college education or governmental position of authority, can be granted a meeting with the President of the United States, and convince him to pardon a woman convicted of conspiracy to sell cocaine and money laundering, is it too implausible to believe a similar social media influencer could shape the enemy's political will in favor of the United States?⁴³ The answer to how to use social media as an aspect of 21st century warfare lies somewhere between using tweets instead of Tomahawk missiles and dismissing social media warfare entirely. There is no substitute for experience and knowledge in any domain of warfare, just as it was in the early days of aerial bombardment.

The online battle within the information domain is complicated and at times counter-intuitive. Manipulators aren't trying to get journalists to say that witnesses to gun violence and terrorism are actually crisis actors. Their goal is to get the news media to negate that frame — and negate the conspirators who are propagating that frame. This may be counter-intuitive, but when news media negates a conspiratorial frame, the people who are most open to such a conspiracy will want to self-investigate precisely because they don't trust the news media. As a result, negation enables a boomerang effect.⁴⁴ By understanding how influence works online, the lexicon of this new domain, the new rules for this space, the U.S. military can shift from a reactionary posture to one driving the narrative and dominating the social media space. This continued pressure

will force America's adversaries to continue to invest in more expensive and sophisticated control mechanisms and technology to maintain their respective internet sovereignty.

Application and Integration of Military Functions

The development of respected, institutionalized information warfare professionals into the command and control structures of unrestricted line warfare communities is essential to controlling the will and influence of our future enemies. The current command and control structures of the U.S. military typically have information warfare professionals in a separate, coordinating, or supporting role. For example, in 2017, the information professionals within the O-5 led Special Operations Command Forward – East Africa (SOCFWD-EA) were supported in the information domain by an O-3 Army Captain, in the form of a Military Information Support Operations (MISO) Officer. This officer and small supporting staff were not co-located in the Joint Operations Center (JOC) during operations, nor were they on the same base. Information warfare officers are restricted line officers, and function within supporting roles. Instead of trying to change the entire culture of the military in breaking down the distinction between line and staff, this paper proposes integrating information warfare into unrestricted line communities themselves, to accelerate its integration into the operational art of warfare. If unrestricted warfare officers, with an information warfare subspecialty code, are placed in supported roles of power and authority, that commander is more likely to integrate information warfare strategies than a traditional unrestricted line warfighter's career path. Marines have a well-known mantra, "Every Marine a rifleman", this paper suggests, in the future, "Every officer an influencer" will become a common phrase.

Necessary Capabilities

The purpose of this paper is to enable the joint force to successfully defend an adversary's information warfare campaign and develop the future force capable of integrating information warfare into traditional warfare methods, in order to increase the burden of national internet sovereignty. Fortunately for the U.S. military, a crop of future social media warfare specialists is being developed without any DOD funds. 95% of teens in the United States report they have a smartphone or access to one, with 45% of all teens saying they are online on a near-constant basis.⁴⁵ While these teens cannot be considered social media experts, the data points to a broader acceptance of social media as a central aspect of future generation's lives. The knowledge and experience this next generation possesses, should be blended with the wisdom of senior military officers and NCOs in the JIDDC. The JIDDC should be an adaptive, lateral hierarchical structure, prioritizing collaboration and maximizing the exchange of ideas in order to produce the most creative and effective solutions to social media warfare problems. The JIDDC, as well as a future unrestricted line officer with an information warfare subspecialty, would seek to maximize effects on the battlespace in the cognitive dimension and produce enduring cost imposing strategic outcomes.

ISIL Case Study

At ISIL's peak ability to influence, it was able to recruit over 30,000 foreigners from nearly a hundred countries to its cause, predominantly through their highly effective social media marketing campaigns. Words like 'slick' were used over 5 million times to describe ISIL's collection of online images, videos, and websites.⁴⁶ The shock value created from videos of beheadings and other similar atrocities resulted in widespread fear, while at the same time garnered ad-

miration from like-minded radical extremists. In a 2014 poll; immediately after the highly publicized beheading of British aid worker James Foley, NBC News and the Wall Street Journal reported 47% of Americans believed the country was less safe than before the September 11, 2001 terror attacks. This news story reached an unprecedented 94% of Americans, an almost impossible media reach for the relatively small organization of ISIL.⁴⁷

The transformation of ISIL from a junior varsity terrorist organization to infecting an entire nation with fear caught many in the political and military establishments off-guard. United States Cyber Command (USCYBERCOM), a sub-unified command assigned to United States Strategic Command (USSTRATCOM), was created just four years earlier. This new physical and cognitive threat represented the first real global test of capabilities and resolve in the information and cyber domains. Although many of USCYBERCOM's activities are classified, a recently disclosed, but heavily redacted operation illuminates some of its capabilities. While relatively slow in reacting to ISIL, USCYBERCOM built a highly capable joint task force assigned to conduct cyberspace operations in support of United States Central Command (USCENTCOM) during Operation Inherent Resolve. CDR USCYBERCOM was directed to conduct Cyber Intelligence, Surveillance, and Reconnaissance (C-ISR), Cyber Operational Preparation of the Environment (C-OPE), counter ISIL media, and support coalition military operations against ISIL.⁴⁸ Under the direction of a three-star general, USCYBERCOM created Joint Task Force (JTF) ARES, to integrate, synchronize, and deconflict activities within the broader counter-ISIL mission. JTF-ARES was requested by USCENTCOM to integrate into key USCENTCOM/USSO-COM battle rhythm events, Commander's updates, target deconfliction processes, and operations synchronization meetings. Following the successful integration of JTF-ARES within USCENTCOM, under the guidance provided by the National Security Council, Operation GLOWING

SYMPHONY was approved for execution on November 8, 2016.⁴⁹ This Concept of Operation (CONOP), was the authorization for JTF-ARES to conduct actions in cyber space and on the internet.⁵⁰

Integral to determining the success of JTF-ARES and Operation GLOWING SYMPHONY, was evaluating its measures of performance. To do this, Audrey Alexander, a researcher at the George Washington University Program on Extremism, tracked terrorists use of social media, her results are below.

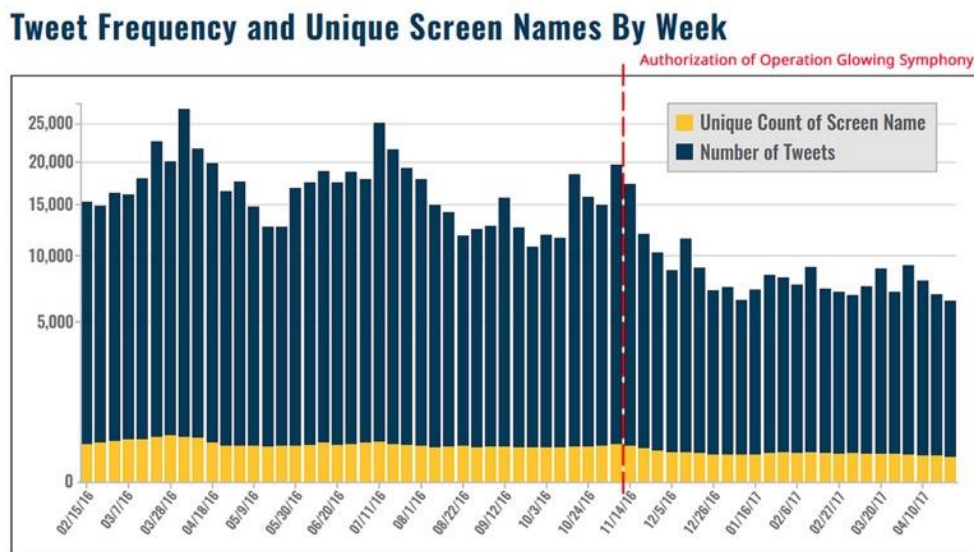


Figure 9: ISIL Tweet frequency following GLOWING SYMPHONY

Her research shows a significant reduction in online activity for English-language pro-ISIL Twitter accounts following the authorization date of Operation GLOWING SYMPHONY.⁵¹ As mentioned earlier, correlation does not always equate to causation, however, a reasonable conclusion can be made that a three-star general led JTF, with the defined end state of denying ISIL the use of cyberspace to enable their critical capabilities, had at least a partial effect on the reduction of ISIL’s online presence.⁵² This success, or at least perceived success, highlights the need for CYBERCOM’s integration, expertise, and resources at much lower levels of command, if the

U.S. military is to continue to compete and win in this battlespace. Integrating members of USCYBERCOM into the JIDDC will be essential to its success.

Recommendations

2018 will be remembered, amongst other headlines, for the repeated congressional testimonies from big tech CEOs of popular social media companies. Whether it was Disinformation campaigns, data breaches, foreign election interference, or the proliferation of hate and extremist views online, social media companies were forced to re-think their loyalties to shareholders. Unfortunately, CEOs are in contact drastically more with their shareholders than they are with Congress, and will likely take a minimalistic approach towards change that effects the bottom line. A JIDDC concept, one that links the U.S. military and social media companies in a coordinating capacity, should be implemented to defend against foreign actors attempting to undermine our nation's Democracy and Constitutional values as well as offensively impose costs for their burdensome internet restrictions. The U.S. military appears, at the moment, to be the only entity with enough resources, as well as resolve, to both offensively and defensively counter foreign interference. By dedicating the JIDDC to the social media disinformation defense, social media corporations will be able to divert resources elsewhere, creating an incentive for their engagement and involvement within the JIDDC. Adam Smith began *The Wealth of Nations* with, "The greatest improvement in the productive power of labour...seem to have been the effects of the division of labour."⁵³ With this thought in mind, transferring authority to the U.S. military can improve the bottom-line for social media companies through decreased resources dedicated to foreign interference themselves, and less time in front of Congress, creating an incentive for them to support the JIDDC, shortening the time to achieve the legislation and funding required to create such an entity.

When speaking about the future of warfare and social media battles online, UK Army Major General Felix Gedney stated at the Association of the United States Army in 2018, “This is not a battle that can be fought by public affairs writing lines to tape, it’s got to be operationalized down into a genuine multi-domain battle.”⁵⁴ General Gedney was speaking more specifically towards Russia’s information warfare capabilities. In order to sync efforts on the battle space, to operationalize the thoughts of General Gedney, the U.S. military should begin implementing information warfare subspecialty accessions to the unrestricted line community and continue to increase acquired diversity of information warfare across all warfighting domains. The diagram below is an interpretation of the current landscape within most of the DOD. The focus on personnel development with the U.S. military typically relies on developing warfighters within a single domain or warfare specialty until they reach tactical command at the O-5 level. Multiple service tours and an information subspecialty without an unrestricted warfare background lends itself to being focused on the operational and strategic level, without the authority or command and control capabilities to fully implement that knowledge.

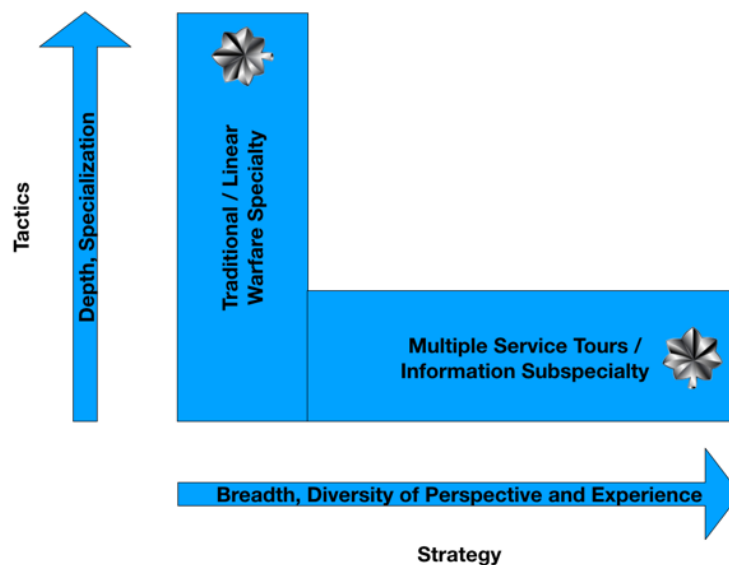


Figure 10: Traditional vs Enhanced Unrestricted Warfare Career Paths

With the addition of the information warfare subspecialty to unrestricted warfare communities, tactical level battlefield commanders are more capable of implementing the strategic messaging-based outcomes required from their respective combatant commanders.

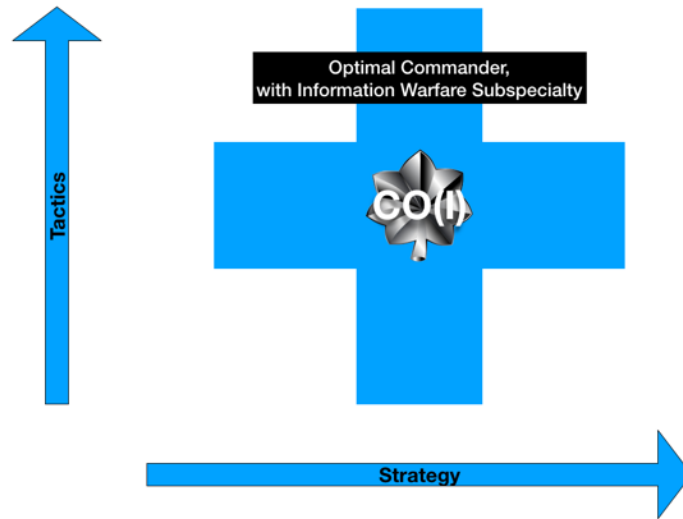


Figure 11: Traditional + Enhanced Unrestricted Warfare Career Paths

An unrestricted line commanding officer with the information warfare subspecialty attempts to successfully blend the strategic with the tactical through acquired diversity in education and experience across the breadth of the joint service prior to taking command. Central to this idea is the concept of acquired diversity. According to Harvard Business Review, acquired diversity involves traits you gain from experience. Through maximizing a career path's variety in service experience, the U.S. military can create leaders with a higher degree of acquired diversity that will enable them to out-innovate and out-perform their adversaries. This concept is supported by a statistical analysis of two-dimensional diversity in the business world.⁵⁵ This study concluded that employees at companies with a well-diversified leader are 45% likelier to report growth in market share over the previous year and 70% likelier that their firm captured a new market. While the U.S. military is not in the business of growing their market share or bottom

line, it does provide the empirical data justifying the need for acquired diversity to improve institutional metrics of success. Enhanced information warfare career paths institutionalize the technical skills required to out-innovate an adversary in the information domain as well as integrate informational power with traditional warfare elements of power.

Insights from War Games

During the second semester's war game, discussing Marine Forces Pacific's (MARFORPAC's) role as the inside force in strategic competition with China, a capability gap was revealed in the inform competition mechanism. Specifically, how the United States would inform the Chinese population of any actions taken within the contact layer, would be exceptionally difficult, given the strict oversight and architecture governing the Chinese internet. Working through, or around the Chinese Firewall would require a level of cyber and information warfare capabilities not achievable at the MARFORPAC level. Assistance from the JIDDC or having Marine combat leaders with an information warfare subspecialty could at the very least provide the commander of MARFORPAC with relevant ideas for overcoming these challenges.

¹ (Mattis, Information as a Joint Function 2017)

² (Brooking 2018)

³ (Kemp 2019)

⁴ (Congressional Research Service 2018)

⁵ (Congressional Research Service 2018)

⁶ (Theohary 2018)

⁷ (Mattis 2018)

⁸ (Snow 1997)

⁹ (Snow 1997)

¹⁰ (Snow 1997)

¹¹ (Lamb 2012)

¹² (U.S. Department of State n.d.)

¹³ (Groll 2019)

¹⁴ (Bender 2018)

¹⁵ (Lamb 2012)

¹⁶ (Lamb 2012)

¹⁷ (Trump 2017)

-
- ¹⁸ (P. D. Trump 2019)
¹⁹ (P. D. Trump 2019)
²⁰ (Joint Chiefs of Staff 2018)
²¹ (U.S. Navy n.d.)
²² (Ingber 2019)
²³ (Joint Chiefs of Staff 2018)
²⁴ (Polyakova 2018)
²⁵ (Polyakova, What do Russian disinformation campaigns look like, and how can we protect our elections? 2018)
²⁶ (Economy 2018)
²⁷ (Brooking 2018)
²⁸ (Corera 2017)
²⁹ (Bennetts 2019)
³⁰ (Bennetts 2019)
³¹ (Bloomberg News 2018)
³² (Vasquez 2018)
³³ (Vasquez 2018)
³⁴ (Snap Inc. 2018)
³⁵ (National Public Radio 2009)
³⁶ (Brooking 2018)
³⁷ (Gladwell 2000)
³⁸ (Gladwell 2000)
³⁹ (Official United States Air Force Website 2003)
⁴⁰ (McDermott 2018)
⁴¹ (Mejia 2018)
⁴² (The Economist 2012)
⁴³ (Timm 2018)
⁴⁴ (Owen 2018)
⁴⁵ (Jiang 2018)
⁴⁶ (Brooking 2018)
⁴⁷ (NBC News 2014)
⁴⁸ (Martelle 2018)
⁴⁹ (Martelle 2018)
⁵⁰ (Martelle 2018)
⁵¹ (Alexander 2017)
⁵² (Martelle 2018)
⁵³ (Conerly 2016)
⁵⁴ (Szoldra 2018)
⁵⁵ (Sylvia Ann Hewlett 2013)

Bibliography

- Alexander, Audrey. 2017. *Digital Decay*. October.
https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/DigitalDecayFinal_0.pdf.
- Bender, Bryan. 2018. *Exclusive: Massive Pentagon agency lost track of hundreds of millions of dollars*. February 5. <https://www.politico.com/story/2018/02/05/pentagon-logistics-agency-review-funds-322860>.
- Bennetts, Alex Hern and Marc. 2019. *Great Firewall fears as Russia plans to cut itself off from internet*. February 12. <https://www.theguardian.com/world/2019/feb/12/great-firewall-fears-as-russia-plans-to-cut-itself-off-from-internet>.
- Bloomberg News. 2018. *The Great Firewall of China*. November 5.
https://www.washingtonpost.com/business/the-great-firewall-of-china/2018/11/05/5dc0f85a-e16d-11e8-ba30-a7ded04d8fac_story.html?utm_term=.320f88f3baec.
- Brooking, P. W. Singer and Emerson T. 2018. *Like War, The Weaponization of Social Media*. Boston: Houghton Mifflin Harcourt Publishing Company.
- Conerly, Bill. 2016. *Specialization And Trade: The Key To Economic Prosperity*. October 6.
<https://www.forbes.com/sites/billconerly/2016/10/06/specialization-and-trade-the-key-to-economic-prosperity/#68f3a7c04ca0>.
- Congressional Research Service. 2018. *Defense Primer: Information Operations*. December 18.
<https://fas.org/sgp/crs/natsec/IF10771.pdf>.
- Corera, Gordon. 2017. *How Britain pioneered cable-cutting in World War One*. December 15.
<https://www.bbc.com/news/world-europe-42367551>.

-
- Economy, Elizabeth C. 2018. *The great firewall of China: Xi Jinping's internet shutdown*. June 29. <https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown>.
- Ferguson, Niall. 2018. *The Square and the Tower*. New York: Penguin Press.
- Gladwell, Malcolm. 2000. *The Tipping Point*. New York: Little, Brown and Company.
- Groll, Robbie Gramer and Elias. 2019. *With New Appointment, State Department Ramps Up War Against Foreign Propaganda*. February 7. <https://foreignpolicy.com/2019/02/07/with-new-appointment-state-department-ramps-up-war-against-foreign-propaganda/>.
- Ingber, Sasha. 2019. *Facebook Stored Millions Of User Passwords In Plain, Readable Text*. March 21. <https://www.npr.org/2019/03/21/705588364/facebook-stored-millions-of-user-passwords-in-plain-readable-text>.
- Jiang, Monica Anderson and JingJing. 2018. *Teens, Social Media & Technology 2018*. May 31. <http://www.pewinternet.org/2018/05/31/teens-social-media-technology-2018/>.
- Joint Chiefs of Staff. 2018. *Joint Concept for Operating in the Information Environment (JCOIE)*. July 25. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf?ver=2018-08-01-142119-830.
- Kemp, Simon. 2019. *DIGITAL 2019: GLOBAL INTERNET USE ACCELERATES*. January 30. <https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates>.
- Lamb, Fletcher Schoen and Christopher J. 2012. "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference." *Institute for National Strategic Studies Strategic Perspectives, No. 11*, June: 95.

-
- Martelle, Michael. 2018. *Joint Task Force ARES and Operation GLOWING SYMPHONY: Cyber Command's Internet War Against ISIL*. August 13. <https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-13/joint-task-force-ares-operation-glowing-symphony-cyber-commands-internet-war-against-isil>.
- Mattis, Jim. 2017. *Information as a Joint Function*. September 15. https://www.rmda.army.mil/records-management/docs/SECDEF-Endorsement_Information_Joint%20Function_Clean.pdf.
- . 2018. *Summary of the 2018 National Defense Strategy of The United States of America*. <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.
- McDermott, Maeve. 2018. *Taylor Swift inspired 65,000 people to register to vote, says Vote.org*. October 9. <https://www.usatoday.com/story/life/music/2018/10/09/taylor-swift-inspired-65-000-people-register-vote-says-vote-org-tennessee-phil-bredesen-trump/1574916002/>.
- Mejia, Zameena. 2018. *Kylie Jenner reportedly makes \$1 million per paid Instagram post—here's how much other top influencers get*. July 31. <https://www.cNBC.com/2018/07/31/kylie-jenner-makes-1-million-per-paid-instagram-post-hopper-hq-says.html>.
- National Public Radio. 2009. *Final Words: Cronkite's Vietnam Commentary*. July 18. <https://www.npr.org/templates/story/story.php?storyId=106775685>.
- NATO.int. 2009. *Launching NATO's New Strategic Concept*. July 10. https://www.nato.int/cps/en/natolive/events_55992.htm.

-
- NBC News. 2014. *ISIS Threat: Fear of Terror Attack Soars to 9/11 High, NBC News/WSJ Poll Finds*. September 9. <https://www.nbcnews.com/politics/first-read/isis-threat-fear-terror-attack-soars-9-11-high-nbc-n199496>.
- Official United States Air Force Website. 2003. *Joint Direct Attack Munition GBU-31/32/38*. June 18. <https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104572/joint-direct-attack-munition-gbu-313238/>.
- Owen, Laura Hazard. 2018. *Facebook's attempts to fight fake news seem to be working. (Twitter's? Not so much.)*. September 21. <http://www.niemanlab.org/2018/09/facebooks-attempts-to-fight-fake-news-seem-to-be-working-twitthers-not-so-much/>.
- Polyakova, Alina. 2018. "The Kremlin's Trojan Horses 3.0, Introduction." *Atlantic Council*. December 3. <https://www.atlanticcouncil.org/publications/reports/the-kremlins-trojan-horses-3-0>.
- . 2018. *What do Russian disinformation campaigns look like, and how can we protect our elections?* October 3. <https://www.brookings.edu/blog/brookings-now/2018/10/03/what-do-russian-disinformation-campaigns-look-like-and-how-can-we-protect-our-elections/>.
- Ritchie, Erika I. 2018. *More US Service Members Die Training Than At War. Can The Pentagon Change That?* May 13. <https://taskandpurpose.com/military-training-accidents-aviation>.
- Snap Inc. 2018. *Snap Inc.'s response*. February 20. <https://www.change.org/p/snap-inc-remove-the-new-snapchat-update/responses/40722>.
- Snow, Nancy. 1997. *United States Information Agency*. August 1. https://ips-dc.org/united_states_information_agency/.
- Sylvia Ann Hewlett, Melinda Marshall, and Laura Sherbin. 2013. *How Diversity Can Drive Innovation*. December. <https://hbr.org/2013/12/how-diversity-can-drive-innovation>.

-
- Szoldra, Paul. 2018. *Military Leaders Are Starting To Freak Out Over Russia's Information Warfare Dominance*. October 9. <https://taskandpurpose.com/russia-information-war>.
- The Economist. 2012. *Cheap smart weapons, Rockets galore*. September 29. <https://www.economist.com/science-and-technology/2012/09/29/rockets-galore>.
- Theohary, Catherine A. 2018. *Information Warfare: Issues for Congress*. March 5. <https://fas.org/sgp/crs/natsec/R45142.pdf>.
- Timm, Jane C. 2018. *Trump commutes sentence of grandmother serving life on drug charges after Kim Kardashian meeting*. June 6. <https://www.nbcnews.com/politics/donald-trump/trump-commutes-sentence-grandmother-serving-life-drug-charges-after-kim-n880291>.
- Trackalytics.com. 2019. *The Most Followed Instagram Profiles*. March 17. <https://www.trackalytics.com/the-most-followed-instagram-profiles/page/24/>.
- Trump, President Donald J. 2019. *A Budget for a Better America*. March 11. <https://www.whitehouse.gov/wp-content/uploads/2019/03/budget-fy2020.pdf>.
- Trump, President Donald. 2017. *National Security Strategy of the United States of America*. December. <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.
- U.S. Department of State. n.d. *Global Engagement Center*. <https://www.state.gov/r/gec/>.
- U.S. Navy. n.d. *PART B SUBSPECIALTY CODES Section 1: General*. Accessed April 24, 2019. https://www.public.navy.mil/bupers-npc/officer/Detailing/surfacewarfare/detailers/Documents/411%20Post%20DH/SUBSPECIALTY_CODES.pdf.

Vasquez, Justina. 2018. *In One Tweet, Kylie Jenner Wiped Out \$1.3 Billion Snap's Market*

Value. February 22. <https://www.bloomberg.com/news/articles/2018-02-22/snap-royalty-kylie-jenner-erased-a-billion-dollars-in-one-tweet>.