REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
05/08/2017	Master's Thesis	SEP 2016 - MAY 2017

4. TITLE AND SUBTITLE
Combined Arms Starts before the First Shot

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Ortiz, Pedro, Major, USMC

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)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The author proposes a concept for the application of human-machine collaboration that will benefit information warfare (IW) planners, subject matter experts and tactical practitioners and enable MAGTFs to conduct IW successfully against a more experienced and less restrained adversary. The right mix of may assist in creating a cohesive and synergistic approach to conducting IW at the MAGTF-level and below. Should this come to pass, the Marine Corps will be capable of deploying MAGTFs that conduct IW by incorporating people and capabilities on the immediate battlefield, in the theater and at home station during all phases of an operation.

15. SUBJECT TERMS
information warfare; human-machine collaboration; Russian-Georgian War (2008); Marine Expeditionary Force Information Group

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College
					19b. TELEPHONE NUMBER *(Include area code)*
Unclass	Unclass	Unclass	UU	73	(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:
Combined Arms Starts before the First Shot

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR:

Major Pedro Ortiz

AY 16-17

Mentor and Oral Defense Committee Member: Benjamin Jensen PhD
Approved: _____
Date: 8 MAY 17

Oral Defense Committee Member: Paul Chelpe PhD
Approved: _____
Date: 8 May 2017

Executive Summary

Title: Combined Arms Starts before the First Shot

Author: Major Pedro Ortiz, United States Marine Corps

Thesis: The Marine Corps must use current and emerging technologies to ensure success in the future information environment, leveraging human-machine collaboration to the maximum extent possible. To that end, the author proposes a concept for the application of human-machine collaboration that will benefit information warfare (IW) planners, subject matter experts and tactical practitioners and enable MAGTFs to conduct IW successfully against a more experienced and less restrained adversary.

Discussion: Nowadays "smart" devices do the work for humans and the humans are free to do other things with their time or focus their attention on other tasks. This is the goal of human-machine collaboration (HM-C) applied to information warfare (IW). The goal is to enable IW planners to focus on planning, IW subject matter expert to focus on their expertise, and tactical IW practitioners to focus on tactics. By offloading some of the work to a machine, these individuals will be able to do more and focus on the most important parts of information warfare. A warfighting functions analysis of the Russian-Georgian war validates the claim that information warfare can be incorporated into combined arms, even in a scenario where the enemy has a low dependency on technology and friendly forces information warfare actions are not closely coordinated. The lessons identified in this case study highlight the importance of information warfare, supporting the future operating environment captured in the Marine Corp Operating Concept. Therefore, it is in the best interest of the service and the nation for the Marine Corp to leverage human-machine collaboration in the conduct of information warfare to the maximum extent possible.

Conclusion: This concept proposes human-machine collaboration capabilities in each of the four operational categories that would benefit IW planners, IW subject matter experts and low-level tactical IW practitioners. The right mix of capabilities like these may assist in creating a cohesive and synergistic approach to conducting IW at the MAGTF-level and below. Should this come to pass, the Marine Corps will be capable of deploying MAGTFs that conduct IW incorporating people and capabilities on the immediate battlefield, in the theater and at home station during all phases of an operation.

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.

Table of Contents

Preface

I arrived at this research topic by way of an interest in cyberspace operations. As a communications officer, I carried certain biases that led me to believe that cyberspace operations could be approached independent of other parts of information warfare. I have since remedied that bias, but no doubt it has been replaced by others that can be attributed to my communications training and computer science degree. However, I firmly believe that the area of information warfare deserves careful attention in the coming years. This will necessarily entail the extensive use of technology, but we need to be careful to not make technology the focus. The Marine Corps maintains its reputation as the world's premier expeditionary fighting force due to hard-fighting, hard-working Marines that have embraced maneuver warfare. A renewed emphasis on information warfare should not and will not change this. However, the Marine Corps approach to developing and acquiring technology in support of information warfare should leverage current and emerging technologies that create the ideal environment for human-machine collaboration.

I would like to thank my wife, Elizabeth Ortiz, for giving me the time and space to complete this work, while she took care of our son, Alex, and carried our soon to be daughter, Emma. Without your love and support, none of this work would have been possible. I would like to thank Dr. Ben Jensen and Dr. Paul Gelpi for shepherding the ASP group and encouraging us to "fire shots" in the "war for information." I would like to thank all of the players of my operational decision game for providing the fuel for my intellectual fire. Lastly, I would like to thank the faculty advisors and member of conference group 16 for making this a memorable and meaningful year.

Introduction

In 2008, Russia and Georgia fought a war in which the outcome had been almost predetermined. The primary cause of Russia's assured victory was its adept use of information as part of a holistic approach to warfare that completely isolated Georgia. This left the country of Georgia isolated from its international partners, the government of Georgia isolated from its people, and the military of Georgia isolated from any hope of victory. While this conflict is an interesting case study that will serve as the basis for this investigation, almost nine years have passed; the world has become even more volatile; and information affects the other instruments of national power like no other time in history. To this end, the Marine Corps must prepare to fight future wars not just in five domains, but in the information environment as well. This preparation will necessarily require the use of technology, but technology should not become an end in itself. The Marine Corps must use current and emerging technologies to ensure success in the future information environment, leveraging human-machine collaboration to the maximum extent possible. To that end, the author proposes a concept for the application of human-machine collaboration that will benefit information warfare (IW) planners, subject matter experts and tactical practitioners and enable MAGTFs to conduct IW successfully against a more experienced and less restrained adversary.

Human-Machine Collaboration (HM-C)

Human-machine collaboration is exactly that; a human works with a machine (e.g. computer, smartphone, or tablet) on a problem. This type of collaboration takes place every day and allows humans to accomplish more tasks and different tasks than they could before personal computers were widely available. One of the simplest and most common examples is driving from one location to another using a GPS application on a smartphone. The problem could be

described as traveling from point A to point B. The phone does its part by planning out a route and providing turn-by-turn directions; the driver does their part by driving the car in accordance with those directions. The end result is that the problem is solved by interaction between a human and a machine. While this example is overly simplistic and commonplace, it highlights some key aspects of HM-C that will aid in conceptualizing how HM-C might be used in the conduct of information warfare. First, the human had to do almost no thinking and very little work to arrive at the desired end state. Before GPS applications, people had to look at a map, find both locations, and plan a route. Now, a "smart" device does the work for the human and the human is free to do other things with their time or focus their attention on other tasks. This is the goal of HM-C applied to information warfare. The goal is to enable planners to focus on planning, subject matter experts to focus on their expertise, and tactical practitioners to focus on tactics. By offloading some of the work to a machine, these individuals will be able to do more and focus on the most important parts of information warfare.

Historical Case: Russian-Georgian War (2008)

It has come into vogue to discuss information warfare as a part of a combined arms approach to current and future wars. However, if one was to posit the question, "how do you integrate information warfare as a part of combined arms?" the conversation would most likely quickly degenerate into a discussion about what is information warfare and little if any headway would be made as to how to actually integrate it into combined arms. As one of the many topics addressed in the Marine Corps Operating Concept (MOC) and Marine Corps Force 2025, the integration of information warfare is of paramount importance. With little widespread institutional knowledge on the employment of information warfare, the Marine Corps is forced to look at what some of the United States' near-peer competitors are doing in this area. A

warfighting functions analysis of the Russian-Georgian war validates the claim that information warfare can be incorporated into combined arms, even in a scenario where the enemy has a low dependency on technology and friendly forces information warfare actions are not closely coordinated. The lessons identified in this case study highlight the importance of information warfare, supporting the future operating environment captured in the Marine Corp Operating Concept.

The first order of business in presenting this case is to provide the context for the conflict that occurred in the summer of 2008. The uneasy relationship between Georgia and South Ossetia dates back to the early 20th century. In 1918, after the October Revolution, Georgia declared its independence as the Democratic Republic of Georgia.

[1] However, by February of 1921, the Red Army invaded Georgia, expelled the standing government and incorporated it into the Trans-Caucasian Soviet Federalist Republic along with Armenia and Azerbaijan.[2] In 1922, the South Ossetian Autonomous Oblast was established in the Soviet Socialist Republic of Georgia as an autonomous district.[3] From the mid-1920s to 1989, Georgia and South Ossetia remained in relative peace. However, the ethnic and political tensions that remained provided the fuel for the explosion of conflict in the early 1990s.

In 1989, census data showed two-thirds of the South Ossetian population to be Ossetian and another 29% to be Georgian.[4] However, these statistics did not stop the Georgian parliament from changing the official language of South Ossetia to Georgian.[5] In August of 1990, South Ossetia declared its independence as a republic.[6] However, parliamentary elections held in December of 1990 resulted in a victory by a coalition backed by Georgian President Zviad Gamsakhurdia, who believed in a "Georgia for Georgians."[7] The newly elected parliament revoked South Ossetia's status as an oblast, or autonomous district, effectively blocking South

Ossetia's efforts to secede from Georgia.[8] The following month, January 1991, Georgian troops entered the South Ossetian capital, Tskhinvali, launching a civil war with Georgian military and militias on one side against South Ossetian separatists and Russia volunteers from North Ossetia on the other side.[9] After the conclusion of the month-long civil war and amidst continuing sporadic violence, Georgia seceded from the Union of Soviet Socialist Republics in April 1991.[10] However, it was not until June of 1992 that any headway was made toward peace. Georgia and Russia agreed to cease fire and signed the Sochi Agreement, establishing the Joint Control Commission (JCC) and framework for introducing and supervising peacekeeping forces.[11] In 1994, the JCC established peacekeeping forces comprised of three battalions, one Russian, one Ossetian, and one Georgian, leading to relative peace for almost a decade.[12]

Just after the turn of the century, Georgia began a pro-western/pro-American transition of leadership that would set the stage for the events of 2008. In November of 2003, Mikhail Saakashvili assumed power after the Rose Revolution. The rise of the young pro-American politician would set the stage for small scale fighting on the border of South Ossetia in 2004. [13] In 2005, the Georgian government proposed a peace initiative at a large European forum, but South Ossetia rejected the proposal.[14]

Meanwhile, Russia would begin a series of actions in support of South Ossetia, such as issuing Russian passports to South Ossetians.[15] In 2006, Russia would continue this trend with bans on Georgian imports, like Georgian wine.[16] In 2007, Russia went a step further than rejecting Georgian goods by rejecting its people and deporting Georgian citizens as well. Around this time, Russia was developing its offensive cyber capability. This capability became known to the world when Russia hacked Estonia in April of 2007. Since these cyber attacks were incited by a group rather than a nation, it is difficult to attribute them directly to Russia,[17] even though

they exhibit the same characteristics as the Russian attack (again not directly attributable) on Georgia. Thus the stage was set for the series of events that unfolded in 2008.

The spring of 2008 found Russian-Georgian relations the most strained that they had been since the early 1990s. In April 2008, NATO did not admit Ukraine and Georgia, but did give them reassurance that they would become members of NATO in the future, reinforcing Russia's paranoia of NATO encroachment.[18] Later that month, Georgia accused Russia of downing a Georgian drone over Abkhazia; Russia denied responsibility for the event.[19] In May, a United Nations investigation concluded that a Russian air craft had in fact destroyed the Georgian drone.[20] On the 10th of July, Russia announced that troops were prepared to assist peacekeepers in South Ossetia and a week later conducted an exercise focused on peace enforcement.[21] Two days later, on 19 July, a distributed denial of service (DDoS) attack originating from a server in the United States overwhelmed Georgian government servers, including the Georgian President's website, with a messages containing "win+love+in+Russia."[22] The situation would only continue to deteriorate in the following month.

The first week of August 2008 saw an increase in conventional combat activity as well as cyber activity. In the conventional vein, there was an uptick in skirmishes along the cease fire line.[23] On 5 August, Georgia began its own cyber activities by hacking South Ossetian media websites.[24] Late in the evening on 7 August, President Saakashvili announced a unilateral cease fire while deploying forces to the area; however, South Ossetian militants responded by shelling the Georgian villages of Prisi and Tamarashenil,[25] located on the South Ossetian side of the cease fire line. This use of conventional force as part of a civil war marked the start of the war.[26] The Georgian military responded by attacking with a massive artillery barrage on the town of

Tskhinvali,[27] resulting in the death of 50 Russian peacekeepers.[28] Russian cyber attacks against government and news sites started late on the evening of the 7th, marking Russia's entrance into the conflict as a cyber belligerent before applying conventional means of force.

Russia officially entered the war on 8 August, when Russian troops crossed the Caucasus Mountains and began ground attacks.[29] As the Russian ground attacks started, the DDoS attacks against Georgian government and news sites became more substantial.[30] While the start of the Russian information warfare campaign focused on cyber attacks, Georgia took a different approach. The Georgian government established a press center in the town of Gori and gave reporters access to the internet and guidelines for how to conduct themselves.[31] Furthermore, the website OS-inform.com (OS-inform.ru is a real new website is South Ossetia) was stood up with fake messages from the South Ossetian president. While the Georgians initial focus was on information, they did take measures to maneuver in cyberspace. Tulip Systems contacted Georgia and offered assistance to restore service to the Georgian websites.[32] The Georgian government also maneuvered on its own by using Google BlogSpot to release news and to host government news sites.[33] By the end of the August 8th, the information war and the conventional war was in full swing.

The events of the next four days would be a mix of both kinetic and cyber events that would lead to the end of the war on 13 August. On the 9th, Russia and Abkhazia opened a second front in Western Georgia near Kodori Gorg[34], resulting in Georgia declaring a state of war.[35] The Russian media reported the death of a dozen peacekeepers, which the Russia government used to justify their response. On the cyber front, the website StopGeorgia.ru went online as a means to recruit Russian cyber hacktivists to participate in the still on-going cyber attacks.[36] During this time, the National Bank of Georgia had come under attack and was forced

to shut down all electronic services.[37] By the 10th of August, most Georgian government websites were inoperative.[38] On the 11th of August, Russia declared that the information war was at its height.[39] In an attempt to continue to control the international narrative, Russia cancelled the satellite feed of a Russian correspondent who reported that Russia was bombing Georgia. On August 12, Russia announced the end of military operations. However, on 13 August, Russian troops entered the Georgian city of Gori.

Even though the conflict had come to a relative halt, it would take weeks for the effects to dissipate. On the 12th of August the Estonian Computer Emergency Response Team (CERT) visited Georgia to aid in restoring its cyber operations to normal; they left Georgia on the 16th of August.[40] The national bank took a few more days to recover and began normal operations on the 18th of August.[41] That same day Russian forces occupied the Georgian port of Poti.[42] On the 22nd of August, Russia withdrew her troops from Gori.[43] Less than a week later, Russia announced its recognition of Abkhazia and South Ossetia as independent republics[44], ending the conflict as a swift and obvious Russian victory.

Having given an overview of the historical case, the next task is to analyze the conflict using the joint warfighting functions as a framework. The purpose of this research is add to the understanding of how information warfare may be used successfully as part of a combined arms approach to combat. Thus, the analysis will concentrate primarily on Russian successes in this arena, but will include some analysis of Georgian efforts when it serves to make a particular point. Before beginning the analysis it must be stated for absolute clarity that the cyber attacks have not been directly attributed to the Russian government, but a review of the literature indicates that the Russian government must have been involved either through action or complicity. Therefore, the following analysis will assume that the Russian government did

actively participate in order to bring about the desired outcome as this will best aid in teasing out recommend practices and courses of action for American military operations.

The first joint war fighting function is command and control (C2). Joint Publication (JP) 1 states that "Command at all levels is the art of motivating and directing people and organizations into action to accomplish missions. To control is to manage and direct forces and functions … [and] helps commanders and staffs compute requirements, allocate means, and integrate efforts."[45] As any warfighter knows, the ideal, yet difficult to achieve, outcome is to disrupt the enemy C2 while most effectively commanding and controlling one's own forces. In many theoretical discussions about this topic, the picture is often painted that that military communications systems or essential C2 nodes, such as command posts, must be destroyed or disrupted. However, this conflict demonstrates that there are other ways to disrupt C2. In this conflict, the Russian government did an effective job of disrupting Georgian C2 at the strategic level. By cutting off access to outside media sites and preventing Georgian media from reporting on the conflict, Russia eliminated the Georgian ability to quickly assess and report the political effectiveness of their military actions. By attacking government websites, the Russian government de-legitimized the standing government of Georgia. The overall effect was that it was difficult for the civilian leadership to integrate the efforts between the Georgian government and the Georgian military, let alone to motivate the local populace and the military leadership.

It is unclear what this means for future U.S. operations. While this analysis assumes that the Russian government was involved in the cyber attacks, Russian officials still maintain that it was the work of an organized crime organization, leaving the door open for plausible deniability. In order for the U.S. to replicate the same results, it would have to consciously make the decision to conduct reconnaissance and attacks on enemy civilian infrastructure and privately owned

civilian companies in order to achieve the desired effect. This is why cyber authorities typically reside at the President of the United States (POTUS) level. However, this should not deter U.S. forces from requesting such effects when warranted, nor should the military and policy makers stop efforts to make the request process timelier. The goal would be similar to pre-planned targets for kinetic fires; tactical units should be able to call for information warfare (IW) "fires" on preplanned targets. Additionally, the Department of Defense should pursue technological solutions that could produce localized effects that would make these "calls for fire" more palatable to decision makers. In the case presented, distributed denial of service attacks overwhelmed the target servers. A U.S. solution to execute this would look more like denying a specific set of people access to media and government sites, which is an infinitely more complicated problem, but might be possible. Furthermore, an unanswered question is whether or not the U.S. would be willing to leverage U.S. companies like Twitter, Facebook, and Google for information warfare effects. This could take the form of cutting off Twitter or Facebook access to a specific country or having a U.S. hosted media site shutdown by the service provider. While the Russians were effective at severing C2 at the highest echelons, it is difficult to say whether or not the United States has the will or desire to take the measures necessary to do the same.

The next warfighting function is intelligence. JP 1 states, "Intelligence helps commanders and staffs understand the operational environment and achieve information superiority… [by] identif[ing] enemy capabilities and vulnerabilities."[46] Clearly, Russia achieved information superiority, but not just in the classical sense of understanding the enemy; it did so in the sense that the Russian government controlled the flow of and access to information. This lends weight to the claim that this conflict was the birth of operational cyber.[47] Russia correctly assessed online media and government websites as a vulnerability, despite the fact that only seven percent

of the population had access to the Internet.[48] The Russian planners correctly assumed that the seven percent included the right audience for the cyber attacks to be an effective part of a combined arms approach. Russian hackers had tactical targets of specific websites that created the operational effect of preventing the Georgian government from shaping their own narrative and exercising command and control from the strategic level down to the operational level. This operational effect contributed to the overall Russian strategic goal emplacing de facto pro-Russia governments in the Abkhazia and South Ossetia. This case demonstrates the power of actionable intelligence that contributed to operations at all levels of war.

For future American military operations, this represents a gold standard to be emulated. All too often military professionals focus on the tactical level, where they are most comfortable. Clearly, in the case presented cyber was being used in an operational capacity. In the future, U.S. military planners will need to identify specific tactical targets such as particular media outlets and key government or non-state actor websites; this is what is often referred to as key cyber terrain. However, the end goal is not destroying or neutralizing a tactical capability, but creating a disadvantage where the enemy may win tactical engagements (or not), but cannot link those successes to the operational, strategic and political goals through a cohesive, consistent narrative. The desired end state being that the enemy may win engagements but cannot achieve an overall military or political victory.

The next warfighting function is the most commonly referred to when speaking about cyber operations, fires. JP 1 states, "To employ fires is to use available weapons and other systems to create a specific lethal or nonlethal effect on a target…Fires typically produce destructive effects, but some ways and means…can be employed with little or no associated physical destruction."[49] Russia clearly used cyber systems to achieve a specific nonlethal effect

on cyber targets with no associated physical destruction. So, according to the joint definition Russia did employ its cyber capability as fires. But did Russia employ cyber "fires" as part of a combined arms approach to the conflict? According to MCDP 1, "Combined arms is the full integration of arms in such a way that to counteract one, the enemy must become more vulnerable to another. We pose the enemy not just with a problem, but with a dilemma—a no-win situation."[50] The classic example of this is to employ indirect fires or close air support in conjunction with direct fire; the enemy is forced to choose between death by artillery shells and death by .556 millimeter rounds. The question posed here is "Did Russia create not just a problem, but a dilemma?" While a case might be made for either "yes" or "no", the fact that attacks were perpetrated by a Russian criminal organization and hacktivist makes it very difficult to make the case that the cyber attacks were coordinated enough to create dilemma; although they certainly do create a problem.

So, if Russia was unable to create a dilemma using cyber fires, how can U.S. forces do so in the future? In the future this could possibly take two forms. Assuming that the enemy has the capability to mount a significant cyber defense, unlike Georgia, the first method would be to attack so many pieces of key cyber terrain that choices would have to be made on what to defend. This dilemma could be further complicated by attacking media, social media, government websites and military logistics systems, creating a much more difficult choice. The second method would be to change or corrupt some of the data on the particular cyber targets, not to the extent of creating fake news or deleting logistics databases, but enough to make the system unreliable. The dilemma would be to keep using the assets knowing that the U.S. is inside the system and that some of the data is not right or to abandon using the system all together. Either way, in order to create such dilemmas, the U.S. military will have to change the way it

views cyber and policies will have to change in order to facilitate access to the resources necessary to create the required effects.

While the cyber and cognitive domains are not physical, the joint warfighting function of movement and maneuver is still very much relevant. JP 1 states "movement and maneuver encompasses the… [use of] organic and supporting means and methods that allow a commander to choose where and when to engage an adversary." [51] Russia certainly did use supporting means by using an organized criminal organization and hacktivists to conduct its cyber attacks. With the assumption that the Russian government did participate in some way, there was a significant amount of preparation that went into creating the conditions for the attacks to occur just prior to the outset of combat operations, as well as, throughout the duration of the war. Some make the argument that Georgia also used movement and maneuver by moving some of its capabilities to the United States, compared to Estonia that did not.[52]

In future conflicts with a near-peer cyber belligerent, the United States will have to conduct significant preparation of the cyber battlespace, just as Russia did. If U.S. operational plans do not include these types of considerations, the U.S. will miss out on opportunities to put the enemy in a dilemma. Furthermore, much thought is required about cyber defense. What does a Clausewitzian cyber defense look like where U.S. cyber defenders maintain the initiative? Where will the U.S. move its key cyber capabilities if it comes down to it? What will be the legal ramifications for helpful allies that provide sanctuary? All of the questions remain unanswered, but will be of paramount importance if the U.S. is going to dominate the cyber domain.

The final warfighting function is protection. JP 1 states, "The protection function focuses on conserving the joint force's fighting potential through active defensive measures that protect the joint force from an adversary's attack; passive defensive measures that make friendly forces,

systems, and facilities difficult to locate, strike, and destroy."[53] Based on the outcome of both the cyber fight and the kinetic fight, it is clear that Georgia failed to place any emphasis on this function in the cyber domain. Russia, on the other hand, did thwart the response actions of the Georgian cyber forces and ultimately achieved victory of both the cyber fight and the conventional fight.

If the U.S. military hopes to not repeat Georgia's fate, much work must be done prior to future conflicts. First, U.S. forces must have a good concept of cyber key terrain and developing methods to actively defend it. Second, the Department of Defense must move past the annual computer based cyber training check in the box as a passive defense measure. This should become an emphasis from commanders at all levels and should be integrated into the combined arms approach to fighting future wars. Lastly, much thought should be given by military and civilians alike as to what measures will be given to what level of command to conduct cyber defensive response actions, so that cyber defenders can maintain the initiative even in the defense.

Having applied the warfighting functions to the case, it is obvious that the tools to develop an American combined arms approach to information warfare exists. Furthermore, the need for this approach is highlighted in the Marine Corps Operating Concept (MOC). A cursory review of the MOC reveals that information warfare, information operations and cyber warfare are mentioned at least a dozen times in the short document. Centered around this are three common themes: 1) conducting IW everywhere 24/7; 2) manning, training and equipping to conduct IW; and 3) developing leadership at all levels that knows how to use information and conduct IW.

Without any specifics and as a starting point to the conversation about the IW as maneuver warfare and combined arms, the MOC places a tall order for tomorrow's Marines and Marine Corps. The case demonstrates that the U.S.'s adversaries are conducting IW at the operational and strategic level; in the near future, forward deployed Marine units will need to do the same by "conducting IW everywhere 24/7." The case also demonstrates that adversaries, like Russia, are manning, training and equipping to conduct IW. The Marine Corps is working on how to evolve the MAGTF to include the incorporations of units and Marines that will conduct IW. But, the Marine Corps has just begun the development of Marine Information Group. Much work is still required to develop the correct mix of personnel, equipment and training that will make for effective use of information to help carry Marine forces to victory against any enemy. However, if this new organization is to be effective, the Marine Corps will require leaders that "know how to use information and conduct IW." Thus far, there are limited training opportunities, stove piped communities and no incentives for leaders to develop themselves in this area. This is where the Marine Corps will face the most difficult challenges.

Thus, a warfighting functions analysis of the Russian-Georgian war validates the claim that information warfare can be incorporated into combined arms and highlight the importance of information warfare in the future operating environment, captured in the Marine Corp Operating Concept. Georgia was clearly unprepared for an information war; where as Russia prepared well in advance and created an IW problem, but not a necessarily an IW dilemma, for Georgia. Russia was successful in applying IW across the warfighting functions, which is probably why the information campaign was so successful. By being so successful in the cognitive and cyber domains, it is doubtful that Georgia could have created a political victory even with a military victory. While the case demonstrates that it is difficult to create a dilemma for an overwhelmed

force, the U.S. should codify the integration of information warfare into doctrine in order to address threats in the near future. In doing so, the U.S. will have to give some serious thought to how to conduct movement and maneuver. How does one maintain the initiative when offense actions may be slow or limited and the primary mode of fighting will be defensive? If physical maneuver of cyber capabilities is required, to where would the U.S. maneuver? By focusing along these lines of thought, it is clear the case presented reinforces the portions of the MOC that address IW. Although this means that there will be significant technological, organizational and political challenges, the biggest challenge will be creating the leaders necessary to lead this type of fight by 2025. In order to win the information wars of the future, the Marine Corps will need, "individuals both of action and of intellect, skilled at 'getting things done' while at the same time conversant in the military art"[54] for they will dictate the future security and success of the United States and her armed forces.

Operational Decision Game – Design

Based on the historical case, it is clear that information environment operations (IEO) will become increasing relevant for the foreseeable future. In order to explore what IEO may look like in future conflicts, 10 participants played the decision game in Appendix A. The Russian-Georgian war in 2008 did not end conclusively, as South Ossetia is not recognized as an independent nation. Therefore it is feasible that Russia and Georgia might replay these events. In order to leverage this scenario, the events of 2007-2008 unfold exactly the same way again in 2032, but the war game introduces a Marine Expeditionary Brigade (MEB) ashore in support of a U.S.-Georgia coalition. The MEB is tasked with blocking the Roki pass, protecting the port of Poti and providing information warfare support. Of these tasks, the decision game focuses on providing IW support. The decision game further leverages the current draft of MAGTF *Concept*

of Employment for Operating in the Information Environment (dated 22 February 2017). From this concept, the decision game introduces the four IW operational categories (Electromagnetic Spectrum Operations (EMSO), Cyberspace Operations (CO), Influence or Deceive Activities, and Inform Activities) as well as newly constituted unit, the Marine Expeditionary Force (MEF) Information Group (MIG). The game player is asked to frame the problem by providing a problem statement, a description of tensions between current and desired conditions, a list of changes necessary to achieve the desired conditions, and a list of opportunities, threats and limitations. The game player must then provide a course of action (COA) description and narrative that includes a description by IW operational category, a mission statement, the overall intent, and a list of key tasks. The results of the game are consolidated in Appendix B.

Operational Decision Game – Problem Framing

All players provided a problem statement and either focus on Russia/Russian capabilities or the U.S./U.S capabilities. The players that focused on potential external friction caused by Russia and Russian capabilities identified three key aspects. First, some players believe that Russian initiative and dominance in the information domain, as well as, their experience using information related capabilities (IRCs) as part of combined arms, particularly offensive cyber operations (OCO), posed the most significant problem. Secondly, Russia is subject to less moral and legal restraints, which allows them freedom of maneuver in the information environment and allows them to attempt to justify their actions in the name of western values. Finally, in such a conflict, Russia has a "home field" advantage and local knowledge that U.S. forces will find difficult to overcome without significant help from Georgia. These three factors continue to continue to appear in other parts of problem framing.

The players that focused on the U.S. and U.S. capabilities identified several areas that will be a challenge for U.S. forces. First, some players identified the need to keep Russia on their side of the border; while other identified the problem as having to neutralize Russian IRCs using the MEF Information Group/Information Warfare Coordination Center (MIG/IWCC) as the problem. Some players thought this might be complicated for the need to do this in a coalition environment, instead of a U.S.-only environment. These factors also continue to appear in other parts of problem framing.

Next the players were asked to identify the tensions between the current conditions and the desired conditions. In doing so, several players identified the ongoing Russian exercise and freedom of maneuver on the Russian side of the borders as creating tension and gave Russia an opportunity to prepare the battlespace with regards to OCO and electro-magnetic spectrum operations (EMSO). Other players went on to say that while Russia is just exercising they must be deterred. Some players identified the potential for escalation as a producer of tension, due to the U.S.'s desire to preserve Georgian sovereignty and Russia's desire for credibility as a superpower. One player identified that there may be a capability gap that would prevent U.S. forces from protecting Georgian networks and to protect Georgians from being influenced by Russian information operations. Another player took this one step further and posited that if the U.S. can undermine Russian IRCs it must do so without discrediting the U.S. initiative and within the approved rules of engagement (ROE). These observations identify potential tensions at all levels of war.

Having identified the tensions, players were asked to identify elements that must change in order to arrive at the desired end state. It is important to note that two players identified action on the part of Georgia, specifically, that Georgia must improve its relations with South Ossetia

and that this will require Georgia changing the South Ossetian perception. However, such actions are outside the scope of this study. The rest of the players focused on actions U.S. forces must take. One player identified the need to inject doubt into Russian command and control (C2). Another player agreed and went one step further to say that it is necessary to infiltrate Russian networks and disrupt or influence enemy systems. Two players mentioned influencing Russia to not enter Georgia, while two others carried this thought further to disrupting the government, the economy and shifting public opinion to deter Russia from entering Georgia. All but one player focused on actions during the conflict; this player identified a longer term action of staffing units with expertise and granting the authorities to use IRC to a lower of command. If it were possible to change any of these elements, there would most likely be an effect on Russia's desire to replay the events of 2008.

Next the players were asked to identify opportunities to achieve the desired conditions. Two players identified that the Russians rely on a C2 network and that since Russian tactics, techniques, and procedures are well know this will make them easier to identify and detect. The rest of the players focused on U.S. and coalition capabilities. Three players identified the MIG capabilities as creating opportunities for success, but that they would need to be distributed throughout the Marine Air Ground Task Force (MAGTF) in order to generate tempo. One of these players also identified the need for the appropriate authorities at the tactical level. One player, pointed to civil affairs teams as providing a unique capability to combat Russian messaging. Another player even thought that the U.S could leverage the North Atlantic Treaty Organization (NATO) in order to deter Russian attacks on coalition networks and from other adversaries in the future. Having identified the opportunities to reach the desire end state, the next task given to the players was to identify the threats.

In identifying the threats to arriving at the desired end state, most players identified Russian threats, but some identified U.S. threats as well. With regard to Russia, the themes from the problem statements re-emerged. Players believed that Russia is bound by less constraints and has more well-developed TTPs that will enable them to use EMSO and OCO effectively. Additionally, some players believed that Russia would become aware of any U.S. cyber intrusions and could potential justify entering Georgia or further strategic escalation. Other players thought that there was a danger that U.S. forces could not evolve fast enough to counter Russian IRCs and might stay in a reactive state. Another player was slightly more optimistic and thought that the technology would amount to a zero sum game, but that the information fight would come down to cultural awareness. All of these represent credible threats to U.S. forces in the information domain during future conflicts.

Lastly, the players were asked to complete their problem framing by identifying any limitations. There were three major areas that received comments. First, most players believed that authorities would be limited, particularly with OCO. Some players commented that these authorities needed to be delegated to the tactical level, but even then, the approval process might still make U.S. forces slow to counter Russian IRCs. Second, several players identified that the U.S. would be limited by its desire to avoid escalation to all-out war, be it nuclear war, conventional war, or a proxy war. Third, most players believed that American values and the importance of truth would limit the application of deception, the ability to influence the population along the border, and the threshold for collateral damage in the electro-magnetic spectrum and cyberspace.

Operational Decision Game – Course of Action Mission and Intent

Of the 10 players, seven focused their mission statement on "full-dimensional" IW or IW support; two focused on specific IRCs (Cyber and EMSO); one focused on blocking Russian forces. Of the four players that focused on "full-dimensional" IW, two stated their intent as having the Russians conclude their exercise and return to the status quo. Another player focused on the coalition operating unencumbered by Russian IRCs; while the last player focused on the undermining Russia's confidence in its system and using IW as part of multi-domain targeting.

Of the three players that focused on IW support, all three identified discouraging Russian forces from entering Georgia and protecting the port of Poti in the "in order to" portion of their mission statement. One player specifically tasked the MIG with providing the IW support; while the other two believed this was part of the overall mission of 2d MEB. All three player expressed the idea that IW capabilities needed to be "leveraged" to achieve all parts of the mission. All three provided tasking to the MIG, ranging from conducting IW tasks on behalf of the entire MAGTF to being the coordinator for all IW tasks assigned to IW elements throughout the MAGTF. One player noted that developing a sustainable coalition capablility is part of the mission, as well as, leveraging some of NATO's existing cloud technologies. Another player (previously mentioned) explicitly incorporated civil affairs teams conducting civil-military operations along the border as part of the mission.

Two players decided to focus their mission on specific IRCs, cyber operations (CO) and EMSO. The player that focused on cyber operations envisioned it as part of deception in support of a sector defense that would disrupt Russian offensive operations. This player elaborated and mentioned "breaking up Russian Army formations" as they moved south, using spoofing of commanders' and civilian's online personas to disrupt movements and redirect formations away from objectives. The player that focused on EMSO thought EMSO would be the primary method

to “defeat Russian aggression.” However, in the intent section, this player went on to elaborate, that cyber and media would serve as a supporting role and that airpower would also be part of shaping operations.

The last player did not mention IW or IW support at all in the mission statement, focusing on blocking “in order to protect Russian sovereignty and key infrastructure (port of Poti).” However, as part of their intent the player identified information operations as the main effort because this would remove any legitimate justification for Russia entering Georgia. This player envisioned that the MIG would “fix, confuse and provide indications regarding Russian movements.”

Operational Decision Game – Course of Action Narrative by IW Operational Category

Each player was asked to provide a COA narrative by IW operational category. The first category presented was electromagnetic spectrum operations (EMSO). Most players identified the need to conduct traditional electronic warfare (EW) functions such as electronic protection (EP), EW support and electronic attack (EA). Ideally, this would “enable SIGINT/ELINT dynamic targeting in both the friendly and coalition while denying Russian EMSO.” These activities took the form of passive and active monitoring in order to identify order of battle and to track Russian movements, as well as, jamming of radio and satellite signals. Some of the players identified capabilities or functions that are either not widely available or do not exist today. Two players indicated that active on-call jamming should be available as a means of suppression and should be directly targeted at enemy leadership and C2 nodes. Two players identified the need to spoof and jam position, navigation and timing devices, such as GPS. One player identified the need to integrate decoy emitters as part of the deception plan. One player indicated that EMSO has become so complex that artificial intelligence is necessary to gain

sufficient understanding of enemy EMSO and to combat emerging threats such as unmanned vehicle swarms.

Next the players were asked to focus on cyber operations which are comprised of Department of Defense information network (DODIN) operations, defensive cyberspace operations (DCO), and offensive cyberspace operations (OCO). There was a single comment identifying that DODIN operations would be necessary to conduct IW. The rest of the comments were focused on DCO and OCO, where there were a few comments that could be categorized as either DCO, OCO, a combination of both or not cyber at all.

With regards to DCO, the focus of the comments tended toward defense against Russian cyber threats or cyber threats in general. Most of these comments mentioned protecting networks, while one player commented specifically on protecting C2 networks. One player identified that U.S. forces may need to protect partner networks and may even need to augment and support civilian infrastructure. One player addressed the fact that DCO could be used to "canalize" Russian cyber operations, making Russian cyber efforts appear effective when they are not being effective.

When it came to OCO, the comments centered around three main ideas. First, OCO would be directed at Russian cyber operations, including Russian offensive and defensive capabilities, cyber collection capabilities, or ability to maintain cyber networks. Second, some players thought OCO should be directed at C2 nodes and critical infrastructure. However, one player did note that every effort should be made to limit cyber effects to military targets and to avoid damaging Georgian networks and infrastructure. One player extend the definition of targets to include unmanned vehicles (air and ground), and another went as far as targeting the Russian banking system and the power grid.

Aside from the comments about DODIN operations, OCO and DCO, several players made comments that were difficult to categorize and may not even be cyber at all but involve activities in the cyber domain. One player thought that cyber operations included spoofing Russian C4ISR system to give Russia a more optimistic blue force common operational picture (COP) of their force distribution. Another player believed creating social media posts to "counter enemy disposition" was part of cyber operations. Yet, another player took this idea even further as to use these posts to duplicate civil unrest. One player included creating a red COP from social media post fell under cyber operations. While another player thought that the MIG should scrub social media to prevent the Russians from doing the same to U.S. forces. Depending on what vantage point these comments are approached, each one might fall inside of cyber operations or it might not.

After providing their concept for cyber operations, the players were then asked to address the IW operational category of influence or deceive activities. When it came to influence activities one player addressed overarching scheme as leveraging all forms of media (social, print, television, etc.) to participate in the local and international narrative. One player expressed a form of this by using media to establish an overt presence at Poti and along the border. Two other players thought that media could be used to delegitimize Russian intentions and actions and to garner local support for the coalition. Two players thought that social media bots could be used to flood social media with pro-western posts and negative Russian posts or could be used to erode the trust within Russian forces by generating synthetic communications between U.S. forces and Russian political and military leaders

With regards to deceive activities, the comments from players all focused on obscuring the size, location and movement of U.S. units. Two players thought that this would require the

use of tactical decoys and the employment of military deception (MILDEC) company detachments down to a low level. Some players thought this could be augmented by EMS signature spoofing and artificial intelligence (AI) that could generate radio chatter that mimic live U.S. units. Other players thought these activities would involve spoofing units that did not actually exist. This might look like social media posts that depict special operations forces (SOF) in the Russian rear area, giving impression unconventional warfare efforts underway where none exist, i.e. "synthetic little green men." Yet another player envisioned using computer generated images (CGI) in conjunction with combat camera to create video footage showing areas more heavily saturated with troops than they actually are.

Lastly, each player was asked to determine what inform activities would be necessary to achieve the end state. When it came to inform activities, the players' responses gravitated toward two main focus areas, messaging and espousing American/western values. Some players believed that conducting inform activities would entail painting Russia as the "bad guy" in this situation, but at the same time making it clear to domestic and international audiences that the enemy was the Russian government and not the Russian people. Additionally, some players thought this would include messaging to inform Georgian and U.S. audiences. One player explicitly mentioned messaging the South Ossetians, conveying the benefits of reintegration with Georgia and highlighting the underlying negative intentions of the Russian government. Some players believed this would involve broadcasting U.S. activities to build trust with all audiences and broadcasting Russian activities to reveal the real intentions of the Russian government. With regards to espousing American and western values, several players focused on being first with the truth. One player went on to emphasize that all inform activities should be truthful and

accurate. Another player believed that this should be taken even further and that it was necessary to promote transparency in peacekeeping, Georgian and U.S. operations.

Concept for Human-Machine Collaboration in Support of Information Warfare

In envisioning a concept for Human-Machine Collaboration (HM-C) in support of information warfare (IW), the first step is to describe the military problem in order to provide context, to clarify the type of mission to be accomplished, to outline the physical environment, to describe the security environment, and limit the scope of the concept. Across the Marine Corps attitudes about IW vary, with comment ranging from "Break out the voodoo sticks" to "This is an information operation with physical characteristics." Regardless of individual attitudes about the subject, current Marine Corps activities demonstrate that IW is a contemporary and relevant topic to the service. At the institutional level, the Commandant of the Marine Corps has made the creation of a Deputy Commandant for Information a top priority. Furthermore, the Marine Expeditionary Force (MEF) will start to see the force structure for the MEF Information Group (MIG) in the near future. This will include force structure for the Information Warfare Coordination Center. The Deputy Commandant for Combat Development and Integration (DC, CD&I) has a draft concept for employment for MAGTFs operating in the information environment. All this activity has had a trickle-down effect in discussions about the creation of a cyber military occupational specialty (MOS) and an unmanned aerial vehicle (UVA) electronic warfare officer MOS.

Amidst this volume of activity, it is easy to posit what possible missions might be required of a future MAGTF. One could easily make the argument that future MAGTFs will be required to defeat, destroy or neutralize an enemy's IW capabilities. With regard to the friendly force, future MAGTFs will most likely have to defend the force and to project power and

influence in the information environment. In any case, the overall objective will be to gain an advantage for Marine Forces in the pursuit of whatever its military objective may be. This will be complicated by the fact that the physical environment and geography play a less important role in the information environment that in the domains of land, air, sea, and space. This will require future MAGTF to leverage technology while they wrestle with how to apply maneuver warfare to what could easily be perceived as a battle of technology. Due to the nature of the information environment, IW will necessarily be enabled by technology, but technology should not become the focus.

All of these missions will be occurring in the environment described in the *Marine Corps Operating Concept*. Imagine having to conduct a forcible entry from the Baltic Sea or the Black Sea facing a Russian opponent that mixes conventional force, unconventional warfare and information operations seamlessly. Information warfare and "little green men" will begin shaping the battlefield even before the first shot is fired. Perhaps, an transnational criminal organization will join the fight for information, evading every type of retaliation and preventative measure allowed by the rules of engagement. Technology that is in its infancy today such as data mining, cyber attacks, GPS spoofing, UAV swarms and automated target detection will be common place. The Russian government will be better versed in using western values to justify their actions and to allege a double standard that they are today. The Russian population and the neighbors will be so desensitized to this type of activity that it will be considered common place.

Just as important as what problem this concept will address is what it will not address. This concept will not address an overall definition of information warfare or operations in the information environment. It will not prescribe force structure, manning level, specific technology or an ideal mix of conventional operations with IW. Furthermore, this concept will not attempt to

bin IW activities into warfighting functions or assign responsibility to specific staff sections or MOSs. This concept will address these issues in general term, so as to promote critical thought and meaningful discussion.

Therefore, the aim of this concept is to propose human-machine collaboration capabilities in each of the four operational categories that would benefit IW planners, IW subject matter experts and low-level tactical IW practitioners. Each of these three target audiences will have necessarily different requirements and considerations, but the overall goal should be to achieve the right mix so as to create a cohesive and synergistic approach to conducting IW at the MAGTF-level and below. Should the Marine Corps be successful in implementing this concept, it will have the ability to generate MAGTFs capable of conducting IW at all echelons, incorporating people and capabilities on the immediate battlefield, in the theater and at home station during all phases of an operation.

Human-Machine Collaboration – Electro-Magnetic Spectrum Operations

When it comes to electro-magnetic spectrum operations (EMSO), each target audience will have different needs. In general, planners will need to have situational awareness about EMSO platforms available and the force lay down of each side. When applying HM-C to this idea, this could mean capabilities like automatic importation of all available EW platforms and EM decoys from a program like GCCS-MC and enemy EMSO data from a program like Palintir into a program like C2PC. On top of simplifying this tedious task, planners would most likely want to have answers to questions like “are there gaps that the MAGTF cannot cover with EW assets?” or “are certain C2 nodes more vulnerable to enemy EMSO that others?” The main idea would be to give the planner a holistic picture of what operations are on-going or possible in the EMS.

The needs of a subject matter expert (SME), such as a spectrum manager or an electronic intelligence (ELINT) analyst, would be very different from those of a planner. EMSO SMEs would most likely want very in depth knowledge about their particular expertise and knowledge about how adjacent activities would affect their efforts. When incorporating HM-C into these specialized types of activities the goal would be to reduce the amount of time the expert spends on menial tasks and to maximize the time they spend on higher lever tasks. For example, the ELINT analyst is more than capable of reading broader intelligence reports and picking out the important parts and then generating a more specific ELINT report. But HM-C might be able to do this for them or reduce the amount of time through automatic text analysis and generation and then could possibly inject this data into the red COP. The spectrum manager can easily create the spectrum plan and then work through creating a joint restricted frequency list so that friendly forces do not have their communications jammed. But, using HM-C, it would be better to scrape all the available data sources and automatically identify conflicts and automatically generate restricted frequency lists; taking this one step further, HM-C could aid in identifying maneuver space in the EMS in the event of unintended blue force jamming or even highly congested areas of the spectrum. In any case the goal would to be to allow the SMEs to focus on applying their expertise and have more awareness of activities in other areas that may affect them.

The tactical practitioners of EMSO will also need some tools that employ HM-C. These tools would help tactical units to better employ EW platforms, conduct low-level EW and spectrum management without SME support, and allow them to conduct maneuver in the EMS. In order to achieve this, the Marine Corps should investigate adaptive EW platforms that use HM-C in order to deviate from a pre-planned EW payload, meaning platforms that are capable of sensing a new threat, classifying it as friendly or foe and then conduct localized jamming on that

threat. Similarly, the Marine Corps should investigate "smart" radios that can detect interference and recommend actions to maneuver in the EMS and then self-report the interference back to the SMEs and planners. All of this should be facilitated by smart tools that aggregate all available data sets and allow tactical units to conduct low-level EW and spectrum management without SME support.

Human-Machine Collaboration – Cyber Operations

As cyber operations (CO) have drawn much attention and debate over the past decade, it would be impossible to cover every aspect of HM-C applied to CO. Therefore, this section will focus on a few items so as to contribute to the on-going conversation and to elicit critical thought on how to apply to HM-C to Marine Corps CO in the future. The primary task for planners in the current environment where authorities are restricted to a high level is conduct defensive planning. Once a network is in operation, HM-C could be used to gain more situational activity about what devices are connected to a network and what there configuration of those devices might be. This might be compared to a pre-established baseline of what the network activity should look like. With this internal cyber COP established, the next level of planning would be to identify vulnerabilities; by applying HM-C this task might be completed automatically or at least greatly expedited. Additionally, planners will want to know about external threats. HM-C might provide a mechanism to automatically aggregate cyber intelligence and aid in building an external cyber COP. The overall goal would be to enable planners to conduct future operations where defensive activities are front-loaded into DOD information network (DODIN) operations and defense is more focus on active defense and possibly even response actions. Should authorities be delegated down to a lower level, HM-C could aid in offensive planning by

automating the targeting process or even mapping cyber actors to real world targets that could be prosecuted with lethal means.

From a SME perspective, HM-C would aid in focusing SME attention on the most important information. This might look like automatic log aggregation and analysis based on previously established network baselines and current cyber intelligence. One step further would be to remove the SME from the loop in identifying suspicious activity and recommend response actions to address that activity automatically. This could be thought of as automated counter-battery fire in the cyber domain. Regardless of the form, the goal would be to scope the data down to allow the SMEs to focus their efforts.

Tactical practitioners will need access to a much different set of capabilities. The first of which would be smart systems that notify low-level tactical units or users that they need to call for cyber defense assistance or could even provide some immediate or remedial actions that are automated. Secondly, this type of capability could be extended to report the activity and even request or recommend response action. Thirdly, should cyber authorities be delegated to a low enough level where tactical offensive cyber becomes possible and timely, low-level tactical units should be able to ask for a cyber affect where a smart system creates the technical profile of the actions to create that effect, on-call cyber fires.

Human-Machine Collaboration – Influence or Deceive Activities and Inform Activities

While the goal of these two operational activities are separate and distinct, the actual actions are very similar. For this reason, they will be addressed within the same section. When planning influence or deceive activities and inform activities, the goal of a planner should be to understand what means are available to influence, deceive, or inform different audiences and what means are effective in influencing, deceiving, or informing different audiences. To that end,

HM-C might look like automatic generation of decoy emplacement on top of a blue and red COP using the systems that are reported as available for tasking. Or, it might look like analytics of red and blue narratives would recommend points to reinforce the blue narrative and counterpoints to detract from the red narrative. In any case, the goal would be to create an understanding of where deception, influence, and information dissemination are happening and how they contribute to operations overall.

From a SME perspective, HM-C would simplify highly technical or highly time consuming processes, like social media scraping and analytics, or aid in assessing the effectiveness of activities. This might include generation of fake messages that mimic an individual's online persona, such as a key military or political figure. Or, this might include using computer generated images to create compelling video and photos with only a few mouse clicks. Other areas that HM-C might apply are the use of social media bots that serve as an online influence or deceive army. Regardless of the form, the goal would be to leverage technology to allow the SMEs to be more effective at influencing, deceiving or informing different audiences.

From the tactical perspective, HM-C might be used to better nest localized influence or deceived activities and inform activities or to allow tactical units to use influence or deceive activities and inform activities to achieve cognitive maneuver. This might look like software that takes a generic video or photo product and uses a data store of local videos and photos and merges them so that the narrative remains the same but the visual portion reflects what the local population sees through their windows or as they walk down the street. The software might even generate metrics that measure how far a product deviates from approved public affairs guidance. Or, with regards to deception, it might look like a sensor and software that allows a unit to

capture its EM signature and then makes recommendations on how to minimize or maximize that signature. Nonetheless, the aim is to enable tactical units to conduct influence or deceive activities and inform activities in the absence of SME support.

Spatial and Temporal Considerations

The characteristics of the information environment make it difficult to address spatial and temporal consideration with regards to IW in a concrete way. But, there are some generalizations that should be considered. First, space matters less, but IW does not happen in a vacuum. This means that activities of IW take on intangible forms when it comes to cyberspace and the cognitive realm, but the effects of IW can be very tangible. For example, a well-placed decoy paired with social media messaging, EM signature spoofing and a CGI video might be convincing enough to pull the enemy's main effort to an area that is disadvantageous to their efforts. In this way, deception, CO, and EMSO target at the enemy's perception of the battlespace produce a tangible effect. Second, because space matters less, IW can happen from around the world; in fact, a heavy reliance on sophisticated HM-C may make this even more necessary. This means that in the information fight, reach back capabilities could reside at higher echelons, in another part of the theater or back at home station; planners, SMEs and tactical practitioners would do well to remember that robust capability need not be co-located with them. Third, while IW may be heavily used during the shaping phase, it can be just as effective and integrated into the other phases of an operation. By using HM-C to make IW more accessible to planners, SMEs and tactical practitioners, this becomes more likely.

Conclusion

This concept proposes human-machine collaboration capabilities in each of the four operational categories that would benefit IW planners, IW subject matter experts and low-level

tactical IW practitioners. The right mix of capabilities like these may assist in creating a cohesive and synergistic approach to conducting IW at the MAGTF-level and below. Should this come to pass, the Marine Corps will be capable of deploying MAGTFs that conduct IW incorporating people and capabilities on the immediate battlefield, in the theater and at home station during all phases of an operation. While the Russian-Georgian War provides an excellent case study and the feedback from the players of the operational decision game provide insight in how to fight a future conflict where information is the weapon of choice, much work remains to be done. If the Marine Corp is to have a hope of being ready for such a conflict, it must embrace human-machine collaboration in such a way that planners can focus on holistic operations that incorporate information warfare as part of combined arms and maneuver warfare; that subject matter experts can focus on their areas of expertise while having more situational awareness of adjacent activities; and that gives tactical units the ability to leverage information without subject matter expert support in order to contribute to tactical victories.

---

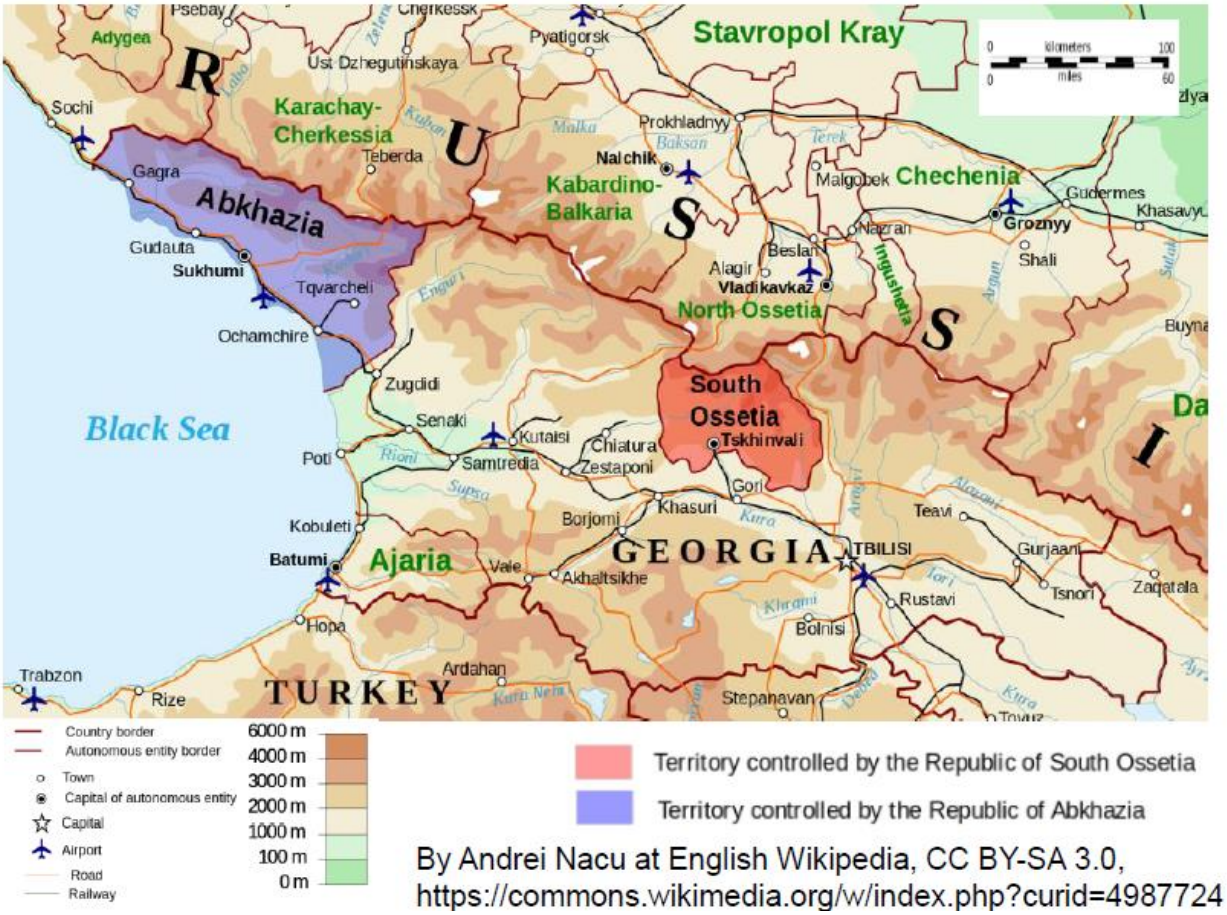
[1] Emmanuel Karagiannis, "The Russian Interventions in South Ossetia and Crimea Compared: Military Performance, Legitimacy and Goals," Contemporary Security Policy 35, no. 3 (Sep 2, 2014): 403. http://www.tandfonline.com/doi/abs/10.1080/13523260.2014.963965.
[2] Levan Z. Urushadze, "Democratic Republic of Georgia (1918-1921)" (unpublished manuscript, 2009), Portable Document File. https://www.scribd.com/document/19004888/Democratic-Republic-of-Georgia, 3.
[3] Karagiannis, 403.
[4] *Ibid*.
[5] Timothy L. Thomas, "The Bear Went through the Mountain: Russia Appraises its Five-Day War in South Ossetia," *The Journal of Slavic Military Studies* 22, no. 1 (Mar 4, 2009): 37, http://www.tandfonline.com/doi/abs/10.1080/13518040802695241; Karagiannis, 403.
[6] Thomas, 37.
[7] *Ibid*.
[8] *Ibid*.
[9] *Ibid*.
[10] Karagiannis, 403; Francis X. Clines, "Secession Decreed by Soviet Georgia," *The New York Times*. April 09, 1991. Accessed January 30, 2017. http://www.nytimes.com/1991/04/10/world/secession-decreed-by-soviet-georgia.html.
[11] Thomas, 37.
[12] Karagiannis, 405.
[13] *Ibid*, 403.
[14] *Ibid*.
[15] *Ibid*.
[16] *Ibid*, 404.

[17] Paulo Shakarian, "The 2008 Russian Cyber Campaign Against Georgia," Military Review 91, no. 6 (Nov 1, 2011): 64. http://search.proquest.com/docview/910124995; Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters* 38, no. 4 (Dec 22, 2008): 70. http://search.proquest.com/docview/198032208.
[18] Karagiannis, 406.
[19] "2008 Georgia Russia Conflict Fast Facts." *CNN*. Last modified March 31, 2016, http://www.cnn.com/2014/03/13/world/europe/2008-georgia-russia-conflict.
[20] *Ibid*.
[21] Thomas, 33.
[22] Korns and Kastenberg, 60 and 64;Thomas, 56; Shakarian, 66; David M. Hollis, "Cyberwar Case Study: Georgia 2008," Small Wars Journal, Vol. 6 (January 2011), 4. Available at http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf..
[23] Karagiannis, 404.
[24] Shakarian, 67.
[25] Thomas, 36.
[26] Hollis, 1.
[27] E. Lincoln, Bonner, "Cyber Power in 21st-Century Joint Warfare," *Joint Forces Quarterly* 74 (3rd Quarter 2014): 105.; Eneken Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified* (Tallin, Estonia: Cooperative Cyber Defence Centre of Excellence, 2008), 4.
[28] Thomas, 32.
[29] Shakarian, 63; Tikk et al., 4; Karagiannis, 404.
[30] Korns and Kastenberg, 60.
[31] Thomas, 50.
[32] Korns and Kastenberg, 60.
[33] *Ibid*.
[34] Karagiannis, 404.
[35] Tikk et al., 5.
[36] Shakarian, 64.
[37] Tikk et al., 16.
[38] Korns and Kastenberg, 60.
[39] Thomas, 51.
[40] Tikk et al., 15.
[41] *Ibid*,16.
[42] Karagiannis, 404.
[43] *Ibid*.
[44] *Ibid*.
[45] U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United State*, Joint Publication 1 (Washington, DC: Joint Chiefs of Staff, March 25, 2013), I-18.
[46] *Ibid*.
[47] Iain Thomson, "Georgia Gets Allies in Russian Cyberwar," vnunet.com, 12 August 2008, http://www.vnunet.com/vnunet/news/2223776/georgia-gets-allies-russian-cyberwar in Korns and Kastenberg, 65.
[48] Tikk et al., 5.
[49] U.S. Joint Chiefs of Staff, I-18.
[50] Headquarters U.S. Marine Corps, *Warfighting*, MCDP 1 (Washington, DC: Headquarters U.S. Marine Corps, June 20, 1997), 93.
[51] U.S. Joint Chiefs of Staff, I-18.
[52] Korns and Kastenberg, 68.
[53] U.S. Joint Chiefs of Staff, I-18-I-19.
[54] Headquarters U.S. Marine Corps, 56.

Appendix A: Operational Decision Game

- This operational decision game (ODG) is an unclassified fictitious scenario developed as part of the requirements for completion of the Advanced Studies Program at the USMC Command and Staff College.
- The purpose of this ODG is to test a future operational concept as part of a notional future threat. Your participation is extremely important to understand how different players approach the challenge through the employment of forces and technology. Your feedback will be used as input to the development of future concepts of employment for information warfare capabilities.

Orientation - Geography



By Andrei Nacu at English Wikipedia, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=4987724

Orientation – Oil Pipelines

By Thomas Blomberg - Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=4536714

Orientation – Pre-Russian-Georgian War

- **1918** - Independent Republic of Georgia establisted , post October Revolution
- **1921** - Russia invades Georgia and incorporates it into Trans-Caucasian Soviet Federalist Republic with Armenia and Azerbaijan
- **1922** - The South Ossentian Autonomous Oblast established in the Soviet Socialist Republic of Georgia
- **1989** - Georgia parliament makes Georgian the official language. Census data shows 2/3 of population ethnic Ossentian and 29% Georgian
- **1990**
    - **August** - S. Ossetia declares independence;
    - **December** - Georgian parliament blocks S. Ossetian secession

- **1991**
    - **January** - Georgian troops enter the capital, Tskhinvali, leading to civil war (Georgian military and militias vs S. Ossetian separatists and Russian volunteers (N. Ossetia);
    - **April -** Georgia separates from USSR
- **1992 June -** Georgia and Russia agree to cease fire and Sochi agreement signed; Joint Control Commission formed to supervise peacekeeping forces; S. Ossetia creates a president and parliament, but not recognized by the international community
- **1994 -** Joint Peace Keeping Force established with one battalion from Russia, S. Ossetia, and Georgia
- **2003 -** Rose Revolution leads to Mikhail Saakashvili, a young pro-American politician, assuming power
- **2004 -** Small scale fighting breaks out on border
- **2005 -** Georgia proposed peace initiative at a large European forum and it is rejected by Ossetia. Meanwhile, Russia is granting Russian citizenship to S. Ossetians; Russia bans the importation of Georgian wine
- **2007 -** Russia deports Georgians. Russia hacks Estonia

Orientation – Russian-Georgian War 2008

- **April -** Ukraine and Georgia not given a MAP (membership action plan), just reassurance that they would become members of NATO; Russia violations of Georgian airspace and cross border firings from S. Ossetia and Abkhazia.

- **July -** Georgian servers hacked (including President's website) with "win+love+in+Russia" ; Russia announces intentions to help peacekeepers in S. Ossetia ; Distributed Denial of Service (DDOS) attacks in Georgia reported
- **August (first week) -** Skirmishes along cease fire line ; South Ossetian websites hacked again; Unconfirmed movement of Russian troops moving through the Roki tunnel late on the 6th or early on the 7th
- **7 August** - Unilateral cease fire by Georgian President accompanied by deployment of forces
    - Militants in Tskhinvali shell Georgian villages, Prisi and Tamarasheni
    - Georgian forces attack S. Ossetia
    - Georgian government and news sites hacked
- **8 August** - Russian Ground attacks begin
    - More substantial DDoS attacks on Georgian servers
    - Tulips Systems (TSHost) contacts Georgia and offers assistance in defending their network
    - Georgia uses Google blogspot for media releases and government news sites.
    - Georgians establish a press center in Gori
    - Os-inform.com stood up with fake messages from S. Ossetian president
- **9 August -** Georgia declares state of war
    - Second conventional front opened by Russians and Abkhazians in Kodori Gorg
    - Russian media reports the death of a dozen peacekeepers and justification for Russian response
    - StopGeorgia.ru goes online as a means to recruit Russian hacktivists

    - National bank of Georgia shuts down electronic services
- **10 August -** Most Georgian govt websites inoperative
- **11 August -** Russia declares information war at its height
    - A Russian correspondent reports that Russia is bombing Georgia; his satellite feeds are cancelled
- **12 August -** Russia announces end of military operations
- **13 August -** Russian troops enter the city of Gori
- **18 August -** National bank of Georgia returns to normal operations
    - Elite Russian forces occupy the main Georgian port of Poti
- **22 August -** Russians leave Gori
- **26 August -** Russia recognizes Abkhazia and South Ossetia as independent

By Andrei Nacu at English Wikipedia, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=5712825

Situation – Destabilization of South Ossetia in 2032

- In 2022, South Ossetia abandoned their alliance with Russia and peacefully reintegrated with Georgia based on promises for better integration in Georgia
- Georgia does what it did in the early 2000s and alienates the Ossetian people
- The situation in South Ossetia began to deteriorate in Jan of 2032, exactly like it did in 2008
- There are 3 battalion of peacekeepers in S. Ossetia – 1 Russian, 1 Ossetian, 1 Georgian
- Russia is currently conducting "exercises" focused on peacekeeping just north of the Georgian border
- Russia is expected to uses the same tactics it used in 2008 with better information related capabilities

Russian IRCs and TTPs

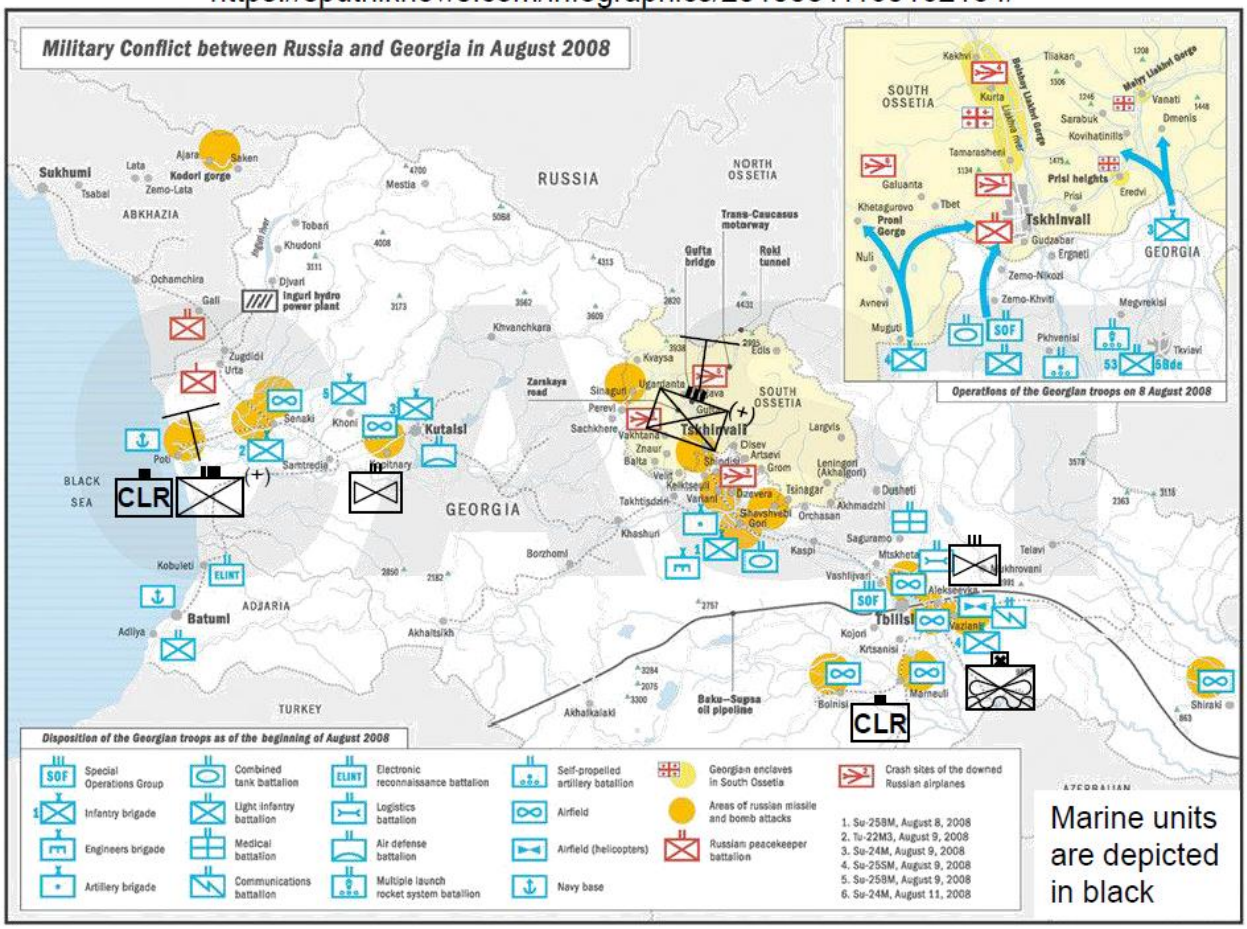
- Information Related Capabilities (IRCs)
    - Russia is capable of conducting effective offensive cyber
    - Russia is capable of disseminating mass information (both true and false) to domestic and foreign audiences, leveraging social media very well
    - Russia has a robust EW capability (collecting, jamming, GPS spoofing, etc)
- Tactics, Techniques and Procedures
    - Russia will not hesitate to use criminals and hacktivists for offensive cyber
    - Russia will post to social in real time, condemning Western actions and pointing to different standards for the West and the rest
    - Russia will frame US/Georgian actions as NATO aggression, requiring them to respond

EUCOM Guidance

- Expect the battle unfold exactly as it did on 8 Aug 2008, just like your approve CONOPS (below)
- Discourage Russian forces from crossing into Georgian territory, engaging in combat only if necessary
- Provide information warfare support to US and Georgian forces
- Use information to enable Georgian forces to be successful during combat operations and during follow-on stability operations
- The MEB CG will receive all authorities requested

EUCOM Approved CONOPS Graphic

https://sputniknews.com/infographics/20100811160162134/



EUCOM Approved CONOPS Narrative

- **Mission:** NLT 0800 on 8 Aug, 2d MEB deploys forces IOT discourage Russian forces from entering Georgia, protect the port of Poti, and provide coalition IW support
- **Intent:** My intent is to keep the Russians on their side of the border, keep the port open for continuous logistical support, and to leverage information during shaping and combat operations
- **Concept:**
    - The GCE will focus on setting up blocking positions IVO Port of Poti and Roki Pass. This will require close coordination and integration with our Georgian brothers in arms.
    - The LCE will focus on port operations and intra-theater logistics.
    - The ACE will provide the six functions of Marine aviation in support of US and coalition forces.
    - All elements of the MAGTF will use information to shape the environment should combat be necessary, to increase the likelihood of victory during combat operations and to aid in the transition back to Georgian-led stability operations

MEB Commander's Guidance

- I believe our CONOPS captures a simple and solid plan, but I think we need to give some serious though to how we will used information to our advantage
- The MEB has an Information Warfare Coordination Center and MEF Information Group (MIG) detachment. The MEF Commanding General will augment us with whatever IW capabilities we request. These capabilities can be pushed to all elements of the MAGTF.

- Develop an IW CONOPS to support our approved CONOPS. Feel free to think outside the box and to leverage COTS technology that exists today in 2032.

IW Operational Categories (from CD&I Draft Concept of Employment dtd 27 Feb 2017)

- **Electromagnetic Spectrum Operations (EMSO)**
    - EMSO merges electronic warfare (EW) with Electromagnetic Spectrum (EMS) management operations (EMSMO) and closely coordinates the efforts of EMS-dependent disciplines; particularly SIGINT, CO, space operations, and other EMS-dependent capabilities traditionally falling under the purview of information operations (IO).
- **Cyberspace Operations**
    - Cyberspace operations include three "lines of operation" (LOOs):
    - (1) Department of Defense information network (DODIN) operations,
    - (2) defensive cyberspace operations (DCO), and
    - (3) offensive cyberspace operations (OCO).
    - Of these LOOs, DODIN operations and DCO will represent the vast majority of cyberspace operations conducted or coordinated by the MAGTF.
- **Influence or Deceive Activities**
    - Influence or Deceive Activities represent those actions taken within the Information Environment which directly affect the perception or decision-making of adversaries or target audiences as a ***first order effect***.
    - A first order effect is the intended primary, immediate effect imposed on a target through the application of a capability.

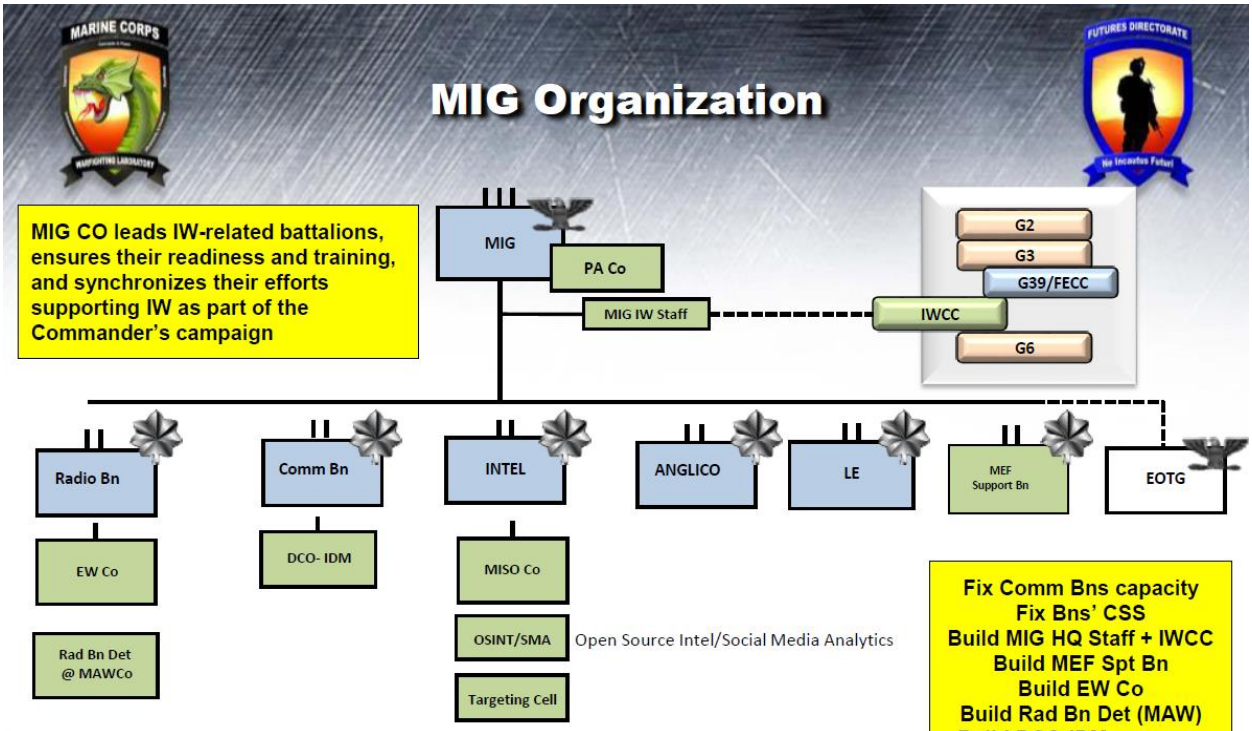
- A second order effect is the derivative, subsequent, unintended, or cumulative effect, of one or more first order effects.

- **Inform Activities**
  - Influence and Deceive Activities are strictly focused on affecting the perception or decision-making of foreign target audiences through the employment of technical and non-technical means
  - *Inform Activities* are focused on leveraging accurate, truthful information and visual imagery to support the commander's objectives, e.g. Public Affairs (PA), Civil Affairs (CA), and Combat Camera (COMCOM).
-

Example of IW Capabilities ISO MAGTF Shaping Operations (from CD&I Draft Concept of Employment dtd 27 Feb 2017)

IW Capabilities and Actions	MAGTF Shaping Objectives								
	Limit Enemy Freedom of Action	Deny Enemy Ability to Concentrate	Deceive Enemy About Friendly Intentions	Destroy Enemy Capability	Gain and Maintain Momentum	Alter the Tempo of Operations	Influence Perceptions & Decision-Making	Inform to Build Credibility, Trust, and Partnerships	Gain & Maintain EMS & Cyberspace Superiority
Cyberspace Operations (CO)									
DODIN Ops					X	X			X
DCO	X								X
OCO	X	X	X	X	X	X	X		X
Electromagnetic Spectrum Operations (EMSO)									
ES					X	X			X
EA	X	X	X	X	X	X	X		X
EP	X								X
Dynamic Spectrum Mgmt.					X	X			X
Influence Activities									
MISO			X		X	X	X		
Space Ops			X				X		
MILDEC		X	X		X	X	X		
Signature Mgmt.		X	X		X	X	X		X
Civil Affairs					X	X	X		
Combat Camera							X		
Key Leader Engagement					X		X	X	
Inform Activities									
Public Affairs								X	
Civil Affairs								X	
Combat Camera								X	

MEF Information Group



New capabilities – represent by new companies would be:

- A cyber protection company within the Comm Bns, for DCO capability – which can be assigned lower in the MAGTF dependent on network architecture.
- A MISO company and a Signature (or Military Deception) Company within Intel Bn.

Information Warfare Coordination Center Composition

Billet Title	Rank	Billet MOS
INFORMATION WARFARE COORDINATOR	LTCOL	8006
INFORMATION WARFARE OFFICER	MAJ	0550
INFORMATION WARFARE CHIEF	GYSGT	0551
CURRENT OPERATIONS – REAL TIME MISSION COORDINATION		
INFORMATION OPERATIONS OFFICER	MAJ	0550
MILITARY INFORMATION SUPPORT OPERATIONS OFFICER	MAJ	0520
ELECTRONIC WARFARE OFFICER	CAPT	7315
MILITARY INFORMATION SUPPORT OPERATIONS PLANNER	CAPT	0520
TACTICAL DECEPTION OFFICER	CAPT	0550
CYBER NETWORK OPERATIONS OFFICER	CAPT	0605
CIVIL MILITARY OPERATIONS PLANNER	CAPT	0530
SPECTRUM MANAGER	GYSGT	0648
TACTICAL DECEPTION SPECIALIST	GYSGT	0551
INFORMATION OPERATIONS CHIEF	GYSGT	0551
MILITARY INFORMATION SUPPORT OPERATIONS SPECIALIST	GYSGT	0521
CYBER NETWORK OPERATIONS PLANNER	SSGT	0659

Billet Title	Rank	Billet MOS
CURRENT OPERATIONS – FUTURE OPERATIONS PLANNING		
TECHNICAL INFORMATION OPERATIONS OFFICER	MAJ	8834
INFORMATION OPERATION OFFICER	CAPT	0510
ELECTRONIC WARFARE OFFICER	CAPT	7315
OPERATIONS SECURITY OFFICER	CAPT	0510
TACTICAL DECEPTION OFFICER	CAPT	0550
SPACE OPERATIONS PLANNER	CAPT	0540
CYBER NETWORK OPERATIONS OFFICER	CAPT	0605
CIVIL AFFAIRS PLANNER	CAPT	0530
TACTICAL DECEPTION SPECIALIST	GYSGT	0551
INFORMATION OPERATIONS CHIEF	GYSGT	0551
MILITARY INFORMATION SUPPORT OPERATIONS SPECIALIST	GYSGT	0521
INFORMATION OPERATIONS SPECIALIST	SSGT	0551
SPECIAL TECHNICAL OPERATIONS NCO	GYSGT	2651
CYBER NETWORK OPERATIONS PLANNER	SSGT	0659

Solution Set

Fill in the problem framing, COA description and Narrative, and theory of victory portions. Remember this is set in 2032, feel free to use any equipment or technology that the Marine Corps is using now or that it might have in the future.

Problem Framing

Problem Statement (incl. list of key facts and assumptions):
Tensions Between Current Conditions and Desired Conditions:
Elements that Must Change to Achieve the Desired Conditions:
Opportunities and Threats to Achieving the Desired Conditions:
Limitations:

COA Description and Narrative

COA DESCRIPTION BY CATEGORY:	**MISSION:**
Electromagnetic Spectrum Operations **Cyberspace Operations** **Influence and Deception Activities** **Inform Activities**	**INTENT:** **(purpose, method, desired condition)**
	CONCEPT: **(incl. key tasks and who you think will perform them)**

Theory of Victory

Synopsis of your Central Idea **(High-level description of how to achieve your desire end state)**	**Necessary Capabilities** **(People, Skill Sets, Processes, Equipment and Technology need to support the "how" – Reminder: it is 2032)**
Application & Integration of Military Functions **(Traditionally, C2, Movement and Maneuver, Fires, Intel, Sustainment and Protection – feel free to add your own)**	**Spatial & Temporal Dimensions** **(Where do capabilities physically reside? How does sequence play into your theory of success?)**

Additional information

Please include any questions, comments, or additional details here:

Appendix B: Operational Decision Game Results – Consolidated

Player	Problem Statement	Tensions & Elements that must change	Opportunities/Threats	Limitations
1	Dominate the EMS and Info Ops in a conflict where the opponent is not restrained by same rules as friendly forces	Must change: Staffing and expertise level -- delegation of authorities	Opportunities: capitalize on the MIG assets operating at lower levels --> faster and more accurate response Threats: inability to evolve fast enough to counter EN IW activities	Must maintain the appearance of walking the high road
2	Russians have enjoy "dominance" in the information domain as well as mass advantage	US needs to infiltrate enemy networks and be able to disrupt or influence enemy systems	Opportunity or Threats - Russian awareness of cyber intrusion	Limit signatures based on IWCC
3	Russia has the initiative (in IW) and local knowledge	Tension - How do you undermine Russian capability without discrediting my own initiative within the ROE Elements that must change - Inject doubt into Russian C2	Opportunities- Russians rely on C2 network Threats - Strategic escalation	how far can you go with OCO
4	Russia is using offensive and defensive IW with	Tensions: pressure and threat of annexation is escalating -- Desire - maintain the	Opportunities: Seize initiative	Don’t escalate to proxy war

Player	Problem Statement	Tensions & Elements that must change	Opportunities/Threats	Limitations
	combined arms to threaten a neighboring country	sovereignty of neighboring country	Threat: stay in reactive state	
5	2d MEB must prevent Russia from entering Georgia	Tensions: current - Russia exercises threatening anticipated invasion of Georgia similar to 2008 incursion. Desired - Russian forces prevented from entering Georgia	Opportunities: MEB CG has necessary IW authorities. Pro-American leadership in Goergia. IWCC and MIG det capabilities pushed to all elements of the MAGTF	Must discourage Russian forces from crossing into Georgian territory, engaging in combat only if necessary. Must provide IW support to US and Georgian Forces. Must use IO to enable Georgian forces to be successful during combat operations and during follow-on SASO.
		Must change: Russia must realize it is not in their best interest to enter Russia	Threats: Preponderance of Georgia S. Ossetian, history of civil war, S. Ossetians granted RUS citizenship, Russian exercises on Georgian border, Russian IRCs (OCO, fake news, EW)	
6	Use IW to support US and Georgian efforts to keep Russian forces north of the Georgian border	Tension: Russia will enter Georgian territory and use traditional combat if not deterred and compelled not to	Opportunities: MIG capabilities -- OCO, DCO, EMSO, influence and deceive activities	Limitations: near-peer or superior IW capabilities of Russians

Player	Problem Statement	Tensions & Elements that must change	Opportunities/Threats	Limitations
		Must change - Use IW so Russian forces cannot conduct combat operations or use IW so that disruption to Russian government, economy, public opinion requires Russian withdrawal		
7	How can MEB IWCC capabilities be applied to discouraging Russian forces from conducting operations within the sovereign state of Georgia? (Facts: Russians will have a 'home field advantage'; Assumptions: Russians possess similar IW capabilities as US, Russia will replay similar attacks as in 2008, but more sophisticated, Russians are already operating within Georgian networks, US will need to share a network with Georgian/coalition military to share intel/info/etc., tensions between other countries/interests will not be affected too adversely)	Tensions: There may be an inability to properly protect Georgian networks and their cognitive perceptions from Russian influence. Russian IW efforts may deceive Georgian and US military to anticipate or 'see' the battle replay as it did in 2008 while the Russians play a different CONOPS. Russian influence in this area may never go away or might increase. US/NATO will need to increase the capacity of Georgia to respond on its own while discouraging Russia through all instruments of UN/US/NATO power. Balancing IW capabilities with conventional means, while attempting to avoid escalation of tensions that could result in a nuclear	Opportunities: US/NATO can further influence/build Georgian/Coalition networks to become more resilient to attacks, showcase US capabilities IOT deter similar aggression in other geographic areas or domains;	Limitations: Avoid escalation to nuclear proportions; avoid drawing other nations into the conflict

Player	Problem Statement	Tensions & Elements that must change	Opportunities/Threats	Limitations
		showdown between superpowers.		
		Must change: Russian perceptions will need to change making the cost of influence/excursions into Georgia difficult and/or too costly(negative ROI)	Threats: technological advantages could be similar resulting in a zero sum game to some extent; keep apace with Russian technology and IW capabilities given the cultural 'upper hand' they have will need mitigation	
8	Georgian/Ossetian hostilities have created an opportunity for Russia to	Tensions: Russian exercise on the border is a potential precursor to invasion.	Opportunities:	Limited with regards to conduct of offensive cyber operations.

Player	Problem Statement	Tensions & Elements that must change	Opportunities/Threats	Limitations
	use "liberation of the Ossetian people" as a justified means for invasion into Georgia that will challenge Georgian sovereignty and possibly allow for Russian seizure of key Georgian infrastructure, namely the Port of Poti.		Threats: Russia appears to have more freedom of movement with less constraints in the conduct of information operations.	Being first with the truth will limit deceptive operations.
		Must Change:	Any action taken by the Georgians that can be viewed as aggressive by the Russians will be used to justify a Russian invasion into Georgia.	Delays in approval chain for information operations activities will make US response slower than the Russian efforts.
		Georgian/Ossetian relations must improve to further deny Russian justification for invasion.		
9	Russian aggression as demonstrated by its exercises will continue as long as there is tension and a lack of unity between the South Ossetians and Georgians. MEB forces must neautraliz Russian IRC's and support	Tensions: Russia's aggressive posture and Georgia's alienation of Ossetian people versus the desired state of South Ossetia peacefully existing as part of Georgia and Russian activity in the area reduced to its peacekeeping mission.	Opportunities and Threats	OCO requires SecDef/POTUS authorization. More moral restraints WRT mass deception and utilization of blackhats than adversaries.

Player	Problem Statement	Tensions & Elements that must change	Opportunities/Threats	Limitations
	messaging that degrades Russian legitimacy and bolsters Ossetian reintegration into Georgia. Facts and Assumptions: Our use of OCO will be limited. Russia will employ TCO's (cyber). Russia will use trolls to flood social media with fake news to delegitimize U.S. efforts.	Must Change: Georgia must change its perceived attitude towards Ossetian people. Russian aggression and escalation must be deterred through IW.	Russian TTP's are well-known globally. This will support our efforts to delegitimize them. Russian IW is well-developed and the EW and CO aspects may significantly challenge our electronic protection and DCO capabilities.	

10	Russian aggression will be masked through blocking and screening actions in cyberspace to obfuscate true intentions; conventional force capabilities to respond will be minimized by creating confusion Assumption: Russian cyberspace IW operations can be detected in advance	Tensions: Desired – Russia remains on its side of the border Current – Russia able to conduct operations relatively unimpeded on their side of border; masking intention through guide of exercises/peacekeeping operations Tension – Russia will set conditions to penetrate the border and occupy territory only once conditions are set to their satisfaction through preparatory close and deep fires in cyberspace and across EM spectrum Must Change: - Russian unfettered exploitation and manipulation of the "truth" must be re-baselined - Russian OCO must be neutralized - Detection of initial entry operations by Russian forces	- Russian OCO, jamming, and other EM ops must be identified and neutralized - Friendly units must have authorities to conduct OCO/DCO against Russian forces as part of coordinated tactical level multi-domain maneuver operations - Civil Affairs teams must have unrestricted access to Georgian side of border to provide a countervailing presence to Russian aggression, messaging - Russian multi-domain maneuver techniques provoke "aggression" prematurely - OCO once used are easily detected and can be used against us	Authorities and lines of coordination for cyberspace operations are not clear; require delegation of authority to conduct OCO to the tactical commander Language and cultural predilections predispose population along border to favor Russia - Threat of collateral damage is high in EM, cyberspace environment given military utilization of the civilian architecture

		must be detected and highlighted to int'l community - Discourage Russian government from determining conditions are ripe for offensive into Georgia		

Player	Mission	Intent	Concept
1	O/O MIG conducts full spectrum IW operations ISO MEB maneuver in Georgia IOT prevent Russian interference in Georgia	P:Out maneuver Russian IW operations M: Full spectrum IW Ops at the lowest level Condition: Maneuver forces able to operate unencumbered by EN IW Operations	N/A
2	O/O defend in sector, conduct cyber deception IOT to disrupt Russian offensive operations in South Ossetia	Disrupt Russian Cyber operations using cyber, EW, and Information IOT breakup Russian Army formations moving toward South Ossetia	Concept: Spoof Russian Commanders and spoof civilian presence to disrupt movement of formations and redirect away from objectives in South Ossetia
3	Conduct full-dimensional IW IOT win the fight for information	Undermine adversary confidence in their systems; Enable multi-domain targeting (dynamic) focusing on IW recon pull	1. Access systems and create EMSO/Cyber SITTEMP 2. ID CV and begin to amplify ("give fake confidence") 3. Blind and strike at key moment
4	Use EMSO to defeat Russian Aggression	1. Start with locating the enemy 2. Go offensive with cyber 3. Maintain defensive on vulnerable DCO systems 4. Use ACE for air power/shaping 5. Media campaign to maintain support	Deny Russians access to the population networks Defend friendly networks Attack Russian networks Exploit the cloud
5	NLT 0800 - Aug, 2d MEB deploys forces IOT discourage RUS forces from entering	My intent is to keep the RUS on their side of the border keep the port open for continuous logistical support and	**MIG:** Conduct EMSO, Cyberspace Operations, Influence and Deception Activities and Inform Activities IOT discourse RUS forces from entering Georgia.

Player	Mission	Intent	Concept
	Georgia, protect the port of Poti, and provide coalition IW support	to leverage information during shaping and combat operations.	**GCE:** Establish BPs ivo Port Poti and Roki Pass with close coordination with Georgians IOT discourage RUS forces from entering Georgia via these avenues of approach. **ACE:** Provide six functions of Marine aviation IOT support GCE and MIG efforts to discourage RUS forces from entering Georgia and protecting the port of Poti. **LCE:** Focus on port ops and intra-theater log. **(Coordinating relationship) USN**: Block eastern coast of Black Sea IOT deny RUS ability conduct operational maneuver from the sea into Georgia.
6	To plan an IW campaign that deters Russia from using traditional combat activities entering Georgian territory	Method – develop and IW campaign with a cohesive strategy employing EMSO, influence, cyber and inform activities Desired condition – Russian forces return to home bases	
7	NLT 0800 on 8 Aug, 2d MEB deploys forces IOT discourage Russian forces from entering Georgia, protect the port of Poti, and provide coalition IW support.	Purpose: Keep the Russians on their side of the border, keep the port open for continuous logistical support, and to leverage information during shaping and combat operations.	CE T1: Provide robust intelligence/information access/support from higher level (national) & coalition sources. Provide MAGTF-level synchronization of IW ops. CE T2: Host/support key Georgian information sources on a coalition and open source network to protect key sources of public information and distribution channels (leverage NATO cloud technologies).

Player	Mission	Intent	Concept
		Method: We will achieve this through leveraging all elements of the MAGTF that discourage/counter Russian involvement and influence within Georgia. The MEB will provide IW capabilities to all elements of the MAGTF to influence Russian activities across all warfighting domains and phases of operations. Desired condition: Russian aggression deterred, Georgian capacity to self-sustain Russian deterrence is increased, and increase positive support from the international community (IC) against Russian actions (now and future).	GCE T1: Deploy 'Company/battalion mimicking footprints' IW capabilities IOT deceive Russian units on locations/intentions GCE T2: Train Georgian units on NATO-level IW TTPs. GCE T3: Deploy organic intel collections assets for integration into HHQ intel processes ACE T1: Maintain continuous air superiority throughout the AOR. Employ swarm tech. that mimics various aircraft signatures IOT mask/protect operations/intentions of coalition forces LCE T1: Provide uninterrupted log. Support to MAGTF units

Player	Mission	Intent	Concept
			LCE T2: Leverage IW capabilities to protect SLOCS/ALOCS/APODS/SPODS
8	NLT 0800 on 8 August, 2D MEB blocks Russian forces IOT protect Georgian sovereignty and key infrastructure (Port of Poti).	Purpose: Our purpose is to protect Georgian sovereignty and key infrastructure, specifically the Port of Poti. Method: The MEB MAIN EFFORT will be focused on information operations IOT deny Russia the ability to justify an attack into Georgia that gains popular support. Desired Condition: Russian forces remain in Russian territory. Georgian sovereignty and infrastructure protected.	GCE – Defend likely avenues of approach and key infrastructure IOT protect Georgian sovereignty and key infrastructure. ACE – Provide six functions of Marine aviation in support of US and Georgian forces IOT protect Georgian sovereignty and key infrastructure. LCE – Conduct port operations and intra-theater logistics IOT support MEB efforts and Georgian forces defense of the homeland. CE – provide IO/Cyber/EW support fix, confuse, and provide indications regarding Russian movements in order to protect Georgian sovereignty and key infrastructure.

Player	Mission	Intent	Concept
9	O/O, conduct IW operations to protect friendly freedom of maneuver throughout cyberspace and the EMS, and provide messaging in support of Georgian and South Ossetian unification IOT restore peaceful relations between South Ossetia and Georgia and deter Russian escalation of hostilities.	Purpose: Set conditions for Russian de-escalation and the reintegration of South Ossetia into Georgia. Method: Execute IW IOT influence the affected area's populations and dominate the enemy in the EMS and cyberspace. End state: Russia has concluded its exercises and resumed peacekeeping role. South Ossetia begins reintegration into Georgia.	IWCC will plan, coordinate with MSC's and other G-3/G-2/G-6 entities, and oversee the IW missions. Comm Bn and Rad Bn detachments conducts CO and EW, respectively. MISO Co. conducts MILDEC and inform activities.
10	MIG provides IW support to 2d MEB forces IOT discourage Russian forces from entering Georgia and to protect the port of Poti.	Leverage full spectrum IW capabilities as part of a fully nested multi-domain maneuver approach incorporating by conducting close and deep fires through space and cyberspace in order to prevent Russian forces from entering Georgia and advancing on the port of Poti.	- MIG will coordinate with 2d MEB and supporting units to nest IW offensive and defensive maneuver as part of 2d MEB operations - Comms BNs will conduct harmonized DCO to protect both 2d MEB and assigned partner unit networks from attack - Civil Affairs will conduct CMO in Georgia along Russian border, establishing the presence and commitment of US to partner forces; - Jamming of Russian radio communications will be conducted by RadBN and joint forces as required to prevent messaging to local population Information campaign via PAO and MISO to inform international community and local population of coalition intent (proactively

Player	Mission	Intent	Concept
			create transparent environment to counter Russian propaganda) Exploitation and intelligence analysis across IW disciplines by Intel BN

Player	EMSO	CO	Deception and Influence	Inform
1	Passive monitor of systems in the port. Active airborne on-call jamming (suppression)	Social media scrub by zone (Det out the MIG assets to create a narrow focus area). Issue Conflicting social media posts to counter EN disposition	Electromagnetic spoofing to manipulate perceived force size and disposition	Portray Russian aggression as "bad guy". Control social and news posts narratives though minimizing exposure
2	Spoof enemy C2 to redirect enemy elements IOT to disjoin Russian operations	Establish Russian online presence to duplicate civilian unrest	Simulate objectives and dispersed elements in the Russian (cant read word)	Orders for subordinate units to diffused elements
3	Enable SIGINT/ELINT dynamic targeting in both the friendly and coalition while denying Russian EMSO	Defend friendly networks. Canalize Russian cyber ops (make it seem effective when it isn't)	Use tactical decoys to force Russians to reveal HVTs.	Broadcast Russian losses
4	Identify enemy order of battle through EMSO spectrum	Offensive campaign to disrupt and deny freedom	Campaign to populace about Russia's activities	Continuous loop of feedback IOT assess effects

		of cyber collection by the enemy.	IOT to garner local support	
5	Integrate decoy emitters with MILDEC to deceive enemy of friendly positions.	Spoof RUS C4ISR systems to give appearance that there are hundreds more friendly force positions saturating Georgia than true reality. Exploit RUS military social media (poor OPSEC) to correlate RUS positions.	1. Employ MILDEC Company to embed enablers down to company level that enables company to expand appearance of area covered through decoy equipment that replicates visual and EMS signatures. In coordination with COMCAM, record portions of friendly front lines. Work with CGI team to embed computer generated graphics (augmented reality similar to maintaining a first down marker on televised NFL games) that depict more heavily saturated friendly forces in zone than actually exists. Footage can then be rebroadcast through other channels.	COMCAM records portions of the front US lines and activities for later informative broadcasts by PA to regional and international audiences to build trust. Exploit RUS military poor OPSEC on social media to broadcast RUS mobilization and intentions to the global community. Inform RUS community our enemy is the RUS govt and not the RUS people.

			2. AI enabled MISO generates synthetic ground formations complete with routine radio and EMS chatter to influence RUS actual units exist. Good case study example: WWII Ghost Army. 3. Generate spoof social media posts that depict US SOF in RUS rear area, giving impression UW efforts underway where none exist. "Synthetic little green men." 4. Release synthetically generated communications between US forces and key RUS political and military leaders which erodes trust within RUS forces.	
6	employ MIG EMSO capabilities in order to jam and/or spoof PNT devices precluding release of weapons, accurate PPLI of air and ground assets, and C2 of forces	employ DCO to protect US networks and networked systems of air and ground assets; employ OCO to take control of Russian assets particularly UAVs,	use social media bots to flood Russian social media with positive Western news and negative Russian news.	employ inform activities to create a positive IO message to influence the Georgian and US populations.

		UGVs, and any equipment emitting with C2 node. Additionally, use OCO activities to disrupt banking and power gird activities within Russia		
7	Disrupt/deter/defeat/spoof/neutralize (D3SN) EN ES uses, while protecting friendly use of the ES. Understanding and controlling the ES for this operation will require the use of our AI-enabled spectrum management system. The complexity of managing swarm tech, commercial/mil./etc. ES uses, while understanding EN EMS warfare efforts has become too complex for human mgt. alone.	Our DCO/OCO efforts will focus on protecting key sources of friendly intel/information networks, while conducting D3SN on EN networks. Operations will ensure cyber-effects are limited to valid military targets, while avoiding damage to the extent possible, on Georgian networks and infrastructure.	US and Coalition forces will leverage all forms of social media, print media, television, etc. to conduct influence and deception operations. Understanding the current narrative within the AOR and the IC will be critical in developing counter & supporting narratives and deception operations	US and Coalition partners will partner with local and IC news sources to be the 'first with the truth.' Authorities must be delegated to the lowest levels to achieve the quickest response.
8	Electromagnetic Spectrum Operations	DODIN operations	Orient deception operations towards Russian forces with regards to MEB troop movements and operations (first order effect).	Employ PA, CA, and COMCOM to be "First with the truth."

	Employ SIGINT to track movement of Russian forces.	Defensive cyberspace operations to mitigate the Russian threat.	(Second order effect) – fix in place Russian forces to minimize their ability to position for possible invasion into Georgian territory and allow for Georgian forces the time to consolidate and make strides with establishing positive relations with the Ossetians.	Provide truthful, accurate information regarding
	Provide I/W regarding Russian movement and intentions along Georgian border.	BPT conduct offensive cyber operations in order to delay/deny Russian C2 and IO capabilities.		
9	Provide electronic warfare support and electronic protection to enable MEB and friendly C2. When directed, conduct electronic attack on enemy targets to exploit EMS vulnerabilities.	Conduct DODIN operations and DCO to maintain and defend C2 networks against enemy offensive cyber actions. As required, employ OCO to target significant enemy C2 node or critical infrastructure.	Employ MILDEC to deceive enemy's assessment of force strength and location. Provide media campaign that delegitimizes Russian intentions and actions.	Target South Ossetian and Georgian populations with messages highlighting the benefits of reintegration. Message them with the negative intentions of Russia and South Ossetia will be lessened if annexed by Russia.
10	- Jamming of Russian radio signals	- DCO to protect partner force networks; augment and support civilian infrastructure as	- Establish an overt presence at Port Poti and along border through	- Promote transparency in peacekeeping, Georgian, and US force operations among

		requested and approved by higher HQ	media campaign and messaging	population and international community; introduce direct accountability to counter Russian propaganda
	- GPS denial of Russian troop formations along border	- Exploitation of cyber environment to identify and neutralize the origin of Russian cyber attacks; conduct IPB and identify key targets to support higher HQ mission	- Provide appearance of larger US footprint than is physically present through MISO, OCO, PAO	
	- SATCOM jamming of identified leadership and C2 nodes to disrupt communication coordination	- OCO to target operational plans and communication, interfering the effective C3 between Russian forces (requires advance delegation of authorities to MEB)		
	- Jamming of GCI uplinks to Russian aircraft operating along border to prevent cross-queue of assets			

Bibliography

"2008 Georgia Russia Conflict Fast Facts." CNN. March 31, 2016. Accessed January 30, 2017. http://www.cnn.com/2014/03/13/world/europe/2008-georgia-russia-conflict/.

Bonner, E. Lincoln. Cyber Power in 21st-Century Joint Warfare. *Joint Forces Quarterly* 74 (3rd Quarter 2014): 102-109.

Clines, Francis X. "Secession Decreed by Soviet Georgia." *The New York Times*. April 09, 1991. Accessed January 30, 2017. http://www.nytimes.com/1991/04/10/world/secession-decreed-by-soviet-georgia.html.

Headquarters U.S. Marine Corps. *Warfighting*. MCDP 1. Washington, DC: Headquarters U.S. Marine Corps, June 20, 1997.

Hollis, David M. "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, Vol. 6 (January 2011). Available at http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.

Karagiannis, Emmanuel. "The Russian Interventions in South Ossetia and Crimea Compared: Military Performance, Legitimacy and Goals." *Contemporary Security Policy* 35, no. 3 (Sep 2, 2014): 400-420. http://www.tandfonline.com/doi/abs/10.1080/13523260.2014.963965.

Korns, Stephen W. and Joshua E. Kastenberg. "Georgia's Cyber Left Hook." *Parameters* 38, no. 4 (Dec 22, 2008): 60-76. http://search.proquest.com/docview/198032208.

Shakarian, Paulo. "The 2008 Russian Cyber Campaign against Georgia." *Military Review* 91, no. 6 (Nov 1, 2011): 63-68. http://search.proquest.com/docview/910124995.

Thomas, Timothy L. "The Bear Went through the Mountain: Russia Appraises its Five-Day War in South Ossetia." *The Journal of Slavic Military Studies* 22, no. 1 (Mar 4, 2009): 31-67. http://www.tandfonline.com/doi/abs/10.1080/13518040802695241.

Tikk, Eneken, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, and Liis Vihul. *Cyber Attacks Against Georgia: Legal Lessons Identified*. Tallin, Estonia: Cooperative Cyber Defence Centre of Excellence, 2008.

Urushadze, Levan Z. "Democratic Republic of Georgia (1918-1921)." Unpublished manuscript, last modified 2009. Portable Document File. https://www.scribd.com/document/19004888/Democratic-Republic-of-Georgia.

U.S. Joint Chiefs of Staff. *Doctrine for the Armed Forces of the United State*. Joint Publication 1. Washington, DC: Joint Chiefs of Staff, March 25, 2013.