The military and the news media have competing objectives when it comes to access to, and reporting of, information during times of military conflict. The operational commander has his sights set on mission accomplishment and preservation of U.S. lives. On the other hand, the media has its eyes set on public awareness and the next big story. The collision of these competing objectives illuminates a fine line between operational security (OPSEC) of military operations and the “public’s right to know.” The military understands the importance of the media as a link to the American people and public support. Public support is paramount to government and military success. As such, the military allows media access to military operations. Historical case studies of U.S. military conflict illustrate varying degrees of media access and their impact on operational security. The modern media environment powered by globalization, multinationalism, engaging reporting techniques, and technology also affects OPSEC. A combination of the media’s historic performance, and the current media environment, causes modern media coverage of military conflict to be a risk to operational security. The operational commander must mitigate this OPSEC risk by educating the media, educating the troops, matching reporters to assignments, and ensuring media accountability.
THE NEWS MEDIA: KEEPING THE PUBLIC INFORMED OR INTELLIGENCE FOR THE ENEMY

By

Eugene L. McFeely
Major, U.S. Air Force

A paper submitted to the faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: ______________________

9 February 2004
ABSTRACT

THE NEWS MEDIA: KEEPING THE PUBLIC INFORMED OR INTELLIGENCE FOR THE ENEMY

The military and the news media have competing objectives when it comes to access to, and reporting of, information during times of military conflict. The operational commander has his sights set on mission accomplishment and preservation of U.S. lives. On the other hand, the media has its eyes set on public awareness and the next big story. The collision of these competing objectives illuminates a fine line between operational security (OPSEC) of military operations and the “public’s right to know.” The military understands the importance of the media as a link to the American people and public support. Public support is paramount to government and military success. As such, the military allows media access to military operations. Historical case studies of U.S. military conflict illustrate varying degrees of media access and their impact on operational security. The modern media environment powered by globalization, multinationalism, engaging reporting techniques, and technology also affects OPSEC. A combination of the media’s historic performance, and the current media environment, causes modern media coverage of military conflict to be a risk to operational security. The operational commander must mitigate this OPSEC risk by educating the media, educating the troops, matching reporters to assignments, and ensuring media accountability.
# TABLE OF CONTENTS

INTRODUCTION ...................................................................................................1

ANALYZING THE MEDIA RISK ...........................................................................2
   The Media’s Right to Know and Role ...............................................................3
   Media Ethics and Motivation .........................................................................5
   The Media and Operational Security through History ..................................6
      The War of 1812 to the Civil War ...............................................................6
      World War I and II .......................................................................................8
      The Korean and Vietnam Wars .................................................................9
      Operations *Urgent Fury* and *Just Cause* ..............................................10
      The 1991 Gulf War .....................................................................................11
      Operations *Restore Hope, Uphold Democracy*, and *Allied Force* .......12
      Operations *Enduring Freedom* and *Iraqi Freedom* .............................13
      The Modern Media Environment – Why the Media is a Threat ..............16

MITIGATING THE MEDIA RISK .........................................................................18

CONCLUSION ......................................................................................................20

NOTES ...................................................................................................................21

BIBLIOGRAPHY ..................................................................................................25

APPENDICES
   A  SPJ CODE OF ETHICS ............................................................................. A-1
   B  PUBLIC AFFAIRS GUIDANCE EXTRACTS ............................................B-1
INTRODUCTION

The first issue in military operations is that no information of value shall be given to the enemy. The first issue in newspaper work and broadcasting is wide open publicity. It is your job and mine to try and reconcile those sometimes diverse considerations.

These words were spoken by General Dwight D. Eisenhower prior to the Normandy invasion sixty years ago, and they are as true today as they were in 1944. Ever since the United States of America has been a nation, the military and the news media have had competing objectives in times of U.S. military conflict. Today, these competing objectives continue to be a source of friction driven by three factors: military concerns, media concerns, and the modern media environment.

The military commander’s primary concern is mission accomplishment. The commander is responsible for setting the conditions for success. At the heart of the commander’s ability to do so is operational security (OPSEC). In the OPSEC process, “one of the most critical tasks is to obtain and maintain the highest degree of secrecy about capabilities and intentions of one’s forces.”

To accomplish this task, the commander must control information. This is the same information that the media wants to access. The media’s primary concern is “the public’s right to know.” The media wants to keep the public informed on all matters of government, including military operations. It wants to collect and disseminate detailed information on current issues such as military conflict. Over the years, the media environment has transformed through globalization, multinationalism, engaging reporting techniques, and technology. This transformation to a modern media environment allows the media to disseminate more information, to more people, with greater detail, at greater speed. The detailed media information produced is a source of operational intelligence for a “tuned-in” enemy. Allowing unchecked media access and dissemination of
information creates risk for military operations. In essence, modern media coverage of military conflict is a risk to operational security. This OPSEC risk can affect military operations to varying degrees.

The impact of an operational security breach, caused by a release of sensitive information through the media, can range from minor to catastrophic. Intelligence gleaned from the media can help the enemy hinder U.S. operations and put U.S. military personnel in danger, or cause the mission to fail and cost U.S lives. This is unacceptable. The military commander and the media must reconcile their competing objectives to find a solution where, as the Sidle Panel stated, “the twin imperatives of genuine mission security/troop safety on one hand and a free flow of information to the American public on the other will be achieved.”iii

To illustrate the underlying issues that influence the “twin imperatives,” this author examines military-media interaction during U.S. military conflict from the operational security perspective. From this information are drawn conclusions about the modern media’s impact on operational security, and recommendations to help operational commanders mitigate OPSEC risk.

ANALYZING THE MEDIA RISK

The media will be present during U.S. military operations well into the foreseeable future. Thus, it is important to examine how the media derives its legitimacy and role in military operations. These two factors set the media’s boundaries, which with ethics and motivation; determine the media’s course of action. An examination of military conflict case studies from the War of 1812 to Operation Iraqi Freedom affords a baseline of media
behavior with respect to OPSEC. This baseline can then be extrapolated to the modern media environment to draw conclusions about the news media and its perceived risk to operational security.

The Media’s Right to Know and Role

As a democratic society, American life includes a deeply rooted free and open press. The media cites the First Amendment to the Constitution of the United States as its legal authority to access information, particularly that regarding military operations. The First Amendment states, “Congress shall make no law…abridging the freedom of speech, or of the press….”iv The First Amendment is a negative command and does not specifically define freedom of access or how the government should facilitate the press.v As a result, there is much room for interpretation. When the issue of national security arises, the question is, “what is it that they [the media] have the right to know, how much, and most importantly, when do they have a right to know.”vi The media interprets the First Amendment to guarantee access under “public right to know,” whereas the military blocks this interpretation with the “need to know.” It is on the grounds of “need to know” and operational security that the military seeks to deny full access to the media when secrecy is critical to preserve life or mission success. The First Amendment ambiguity, and the difference in opinion between the media and government, has led to court disputes.

The battle over media access has appeared before the Supreme Court on several occasions. Although the court has not ruled or set precedents on media access to military information during times of conflict,vii it has made several opinions that have given the media a de facto watchdog role. Referring to the press, Supreme Court Justice Potter Stewart stated
that the primary purpose of the First Amendment was, “to create a fourth institution outside
the government as an additional check on the three official branches.”

Supreme Court Justice Hugo Black during *New York Times Co. v. United States* enforced the media’s
watchdog role when he stated:

> The press was protected so that it could bare secrets of government and inform the people. Only a free and unrestrained press can effectively expose deception in government. And paramount among the responsibilities of a free press is the duty to prevent any part of the government from deceiving the people and sending them off to distant lands to die of foreign fevers and foreign shot or shell.

The media argues that the Court, through these opinions, gives it a clear right to full access of
military operations as our Nation’s watchdog. During *New York Times Co. v. United States*,
Justice Stewart opined that, “in the area of basic national defense the frequent need for
absolute secrecy is, of course, self-evident.” In the court’s proceedings, the precedent often
applied to determine access or disclosure is: will the outcome “result in direct, immediate,
and irreparable damage to our Nation or its people.”

Judicial law case study conducted by Joseph Avery concludes that the media is limited in its right to access military information
and its right is no greater than that of the general public. The end result is that the media
must rely on the operational commander to provide access and release information when
national security or our people are at risk.

The U.S. military’s obligation to the American people is twofold. First, it is an
organization of Americans. Second, it represents the might of the people’s government. The
U.S. military has sworn to defend the same Constitution that the media uses as its legal
justification for access to military operational information. This being said, military
commanders know that it is in the best interest of both the military and the American people
to provide media access as long as it does not jeopardize the mission or the lives of U.S.
troops. In our democratic society, the will of the people and public support are paramount to
government and military success. The conduit that allows the people to exert their will and
demonstrate their public support is a well informed media with access to military operations. The level of media access is controlled by the operational commander. How the media treats this access is driven by media ethics and motivation.

Media Ethics and Motivation

The media, unlike the military, is fragmented and does not have a set of broad professional standards that applies to its community. The media garners its ethical standards from two sources. These sources are employers and professional organizations. The ethical standards provided by these sources can vary widely from employer to employer and organization to organization. In addition, not all ethical standards are viewed as mandatory, but some are viewed as guidelines for behavior. One organization, the Society of Professional Journalists (SPJ), published a “code of ethics” that contains common themes found in most media ethical standards (Appendix A). In the SPJ code of ethics, there are no provisions that specifically address security issues associated with military operations. The closest relevant guidance is found under the “minimize harm” section. In this section the SPJ states:

- Show compassion for those who may be affected adversely by news coverage.
- Recognize that gathering and reporting information may cause harm or discomfort. Pursuit of the news is not a license for arrogance.

With this guidance, it is evident that the information disseminated by the media is at the discretion of the reporter covering the story. The reporter’s discretion can easily conflict with the operational commander’s OPSEC goals.
Another issue that can be at odds with the commander’s OPSEC goals is the media’s motivation for reporting a story. Reporters have several sources of motivation, but the two primary sources are personal and employer imposed. On the personal side, the reporter can be motivated by curiosity, the need for personal recognition, the challenge, the duty to be a watchdog, or the ability to influence public opinion. On the employer side, the reporter can be driven by story deadlines or the need to increase circulation and ratings. Military commanders fear that the driving factors of reporter discretion and motivation will lead reporters to “publish stories or images that breach security, cost lives, or undermine public support.” A historical study of military conflict and media interaction with respect to operational security reveals whether the commanders’ fears are founded in fact.

The Media and Operational Security through History

Since our creation as a Nation, the media has been present to report on U.S. military conflict. Through these conflicts, the military-media relationship has changed along with the level of military operational access granted to the media and its impact on OPSEC. This relationship and level of access have reached both high and low points. The predominant factors driving this ebb and flow have been military-media attitudes, experiences from past conflicts, nature of the conflict, technology, and globalization.

The War of 1812 to the Civil War

During the War of 1812, newspapers were printed frequently and widely distributed. This war possibly produced the first occurrence where the media reported directly from the battlefield. James M. Bradford was the editor for the Orleans Gazette. He enlisted in the
Army under General Andrew Jackson and wrote detailed letters to his paper describing military operations.\textsuperscript{xix} Operational security was not yet an issue because it took a great deal of time for the reports to reach the paper and be printed. As a result, the information was of no value to the enemy.

In the Mexican War, battlefield reporters were common. They used the Pony Express to carry stories from the battlefield to their papers. The newly invented telegraph was also used, but it was unreliable. These transmission methods helped reduce the time from event occurrence to public dissemination.

The potential to transmit reports rapidly from the battlefield to the public was not truly realized until the Civil War. During the Civil War, the reliability of the telegraph had increased significantly and the “Penny Press” had emerged in America.\textsuperscript{xx} The telegraph enabled reporters to transmit stories rapidly from the battlefield, and the “Penny Press” enabled newspapers to print and distribute news quickly to a large and expanding client base.\textsuperscript{xxi} The result was the emergence of the first level of “real-time” reporting.\textsuperscript{xxii} The impact was so dramatic that news from the battlefield appeared in the press before it was received through official channels, which still relied on carrier pigeons and trains.\textsuperscript{xxiii} The technology that reduced the media’s turnaround time also created OPSEC problems for the operational commander. The media had reached the point where information they reported was timely enough to be of value to the enemy.

The press exhibited poor judgment during the Civil War and was guilty of compromising military operations on several occasions. In one incident, a newspaper discovered and printed that the Union was able to decode Confederate signal flags used to
pass sensitive information to the South. On another occasion, as recounted by General William T. Sherman:

Now in these modern times a class of men has been begotten & attend our camps & armies gathering minute information of our strength, plans & purpose & publishes them so as to reach the enemy in time to serve his purposes. Such publications do not add a man to our strength, in noways benefit us, but are invaluable to the enemy. You know that this class published in advance all the plans of the Manassas Movement [which] enabled [General Joseph E. Johnston]...to reinforce Beauregard whereby McDowell was defeated & the enemy gained tremendous strength & we lost in comparison....

General Sherman despised the media because of this type of reporting and described reporters as “dirty newspaper scribblers who have the impudence of Satan,” as well as “spies and defamers.” As a result, the military-media relationship was poor. To mitigate OPSEC risk caused by poor media judgment, the government took control of telegraph lines leading to Washington and commanders limited media access to the battlefield.

World War I and II

World War I was marked by media censorship and controlled access. The government passed The Espionage Act of 1917 and the Sedition Act of 1918. These Acts prohibited publishing information that could aid the enemy, as well as justified censorship. Reporters had to be accredited to gain access to the battlefield. The accreditation process involved an interview, a sworn statement of truth, a signed censorship agreement, and a $10,000 bond. If the reporters violated ground rules, they were removed from the theater and forfeited the $10,000 bond. Reporters were free to report, but the review process would eliminate OPSEC information, as well as negative reporting or criticism of the war.

In World War II, patriotism and the spirit of cooperation were very high between the military and the media. Reporters enjoyed increased access to troops and military operations. WW II was the first time the military formally created “pools” and “embedding” to enhance
media access. The level of access was best characterized by Drew Middleton when he wrote, “As long as all copy was submitted to censors before transmission, people in the field, from generals down, felt free to discuss top secret material with reporters.” WW II had the same basic censorship controls in place as World War I. WW II correspondents had to be accredited but did not require an interview or a monetary bond. “Reporters whose attitudes were ‘suspect’ or whose reporting ‘had proven obnoxious’ were banned.” In addition, if reporters and censors had a difference of opinion on report content, the reporter had the right to an appeal. Home media was not subject to direct censorship but participated in voluntary censorship to guard national security. The military’s goal was to allow the free flow of information as long as it did not endanger national security.

The Korean and Vietnam Wars

In the Korean War, reporting technology was the same as during WW II. The war started with no censorship or media guidelines. The reporters had unlimited access and were free to report as they saw fit. Some reporters were informed about upcoming operations. Unfortunately, there were several severe OPSEC breaches. Reporters committed OPSEC violations when they disclosed troop locations and movements. In one instance, Newsweek published an article that contained maps depicting classified UN troop locations. General MacArthur requested the reporters voluntarily censor themselves, but this did not work. In the end, the media asked the military to set up a formal censorship program modeled after the WW II system. The military complied and there was a marked increase in OPSEC.
Media coverage during Vietnam was uncensored for the entire war.xxxvi “General William C. Westmoreland, in consultation with agencies in Washington, opted for a policy of voluntary guidelines for the press over censorship because he trusted the good will of the American correspondents reporting the war.”xxxvii The media was guided by a set of voluntary rules and had free access to the entire theater, limited only by transportation. The military requested the media to withhold troop movements, unit identification, casualty numbers, and casualty names until next of kin were notified.xxxviii According to Barry Zorthian, a former Saigon U.S. mission spokesman, there were only four or five security violations by the media; two of which were unintentional.xxxix Greater technology and media access brought the war into American homes. Vietnam was, as Morely Safer wrote, “television’s first war.”xl People no longer went to the cinema to watch war footage because it was on the six o’clock news every night. Printed reports from the battlefield were rapidly transmitted back to the United States while television footage took two to three days.xli Vietnam War television images painted a powerful picture and had a tremendous influence on the public.

Operations Urgent Fury and Just Cause

Media access to the battlefield hit an all time low during 1983 military operations in Grenada. Military commanders blocked media access for the first two days of Operation Urgent Fury for security reasons.xlii Restrictions were eventually eased, but many journalists were stranded without stories as hostilities ended by the time they gained access. The media was outraged and filed a complaint. The Sidle Panel was formed to address media issues raised during Grenada. It recommended that the press be given greater access to operations
and follow security guidelines on a voluntary basis. The panel also recommended that a media pool system be created to help with media access to the battlefield. These recommendations were in place prior to the invasion of Panama in 1989.

During Operation *Just Cause*, the Secretary of Defense did not entrust the media with information about upcoming operations and delayed activation of the media pool for OPSEC reasons. Inadvertently, the media reported airborne troop movements the night of the operation. As a result, news of troop movements aired on television prior to H-hour for the invasion of Panama. This was a huge operational security problem. Eventually, the media pool was activated and reporters gained limited access to the battle.

**The 1990-91 Gulf War**

Media access during the Gulf War, Operation *Desert Shield/Storm*, was tightly controlled. The military produced and distributed guidelines outlining procedures and releasable information. Of the approximately 1,600 media representatives in theater, 30 reporters were with frontline units while the remainder formed media pools or covered news from the rear. Media pools, eventually numbering 24, deployed to cover units and events in the field, while reporters in the rear covered the daily CENTCOM briefings. Media pool reports were subject to military review for OPSEC whereas live television coverage and copy filed from the rear was not. Some reporters were informed of future operations, such as the famous left hook, and did a good job protecting the information until the maneuver was well underway, thus maintaining operational security.

Even though live television coverage was available during Grenada and Panama, it was not used to the extent that it was during the Gulf War. In contrast, media coverage of the
Gulf War was revolutionary. Leaps in technology, advances in the media industry, and globalization gave the world around-the-clock coverage of the Gulf War, seven days a week. The media provided reports from both friendly and enemy cities as the war was fought live via satellite. Television stations employed retired military officers as experts to comment on operations as they unfolded. Media audiences were bigger than ever, 105 countries for CNN, including Iraq. “In Desert Shield/Storm, it was clear that the Iraqis used CNN television as an intelligence source.”

This new type of real-time reporting added a dimension to operational security. After the first day of the war, numerous live television reports showed aircraft launching from Saudi airfields bound for Iraq and reports of SCUD missile impacts. By televising this information to a tuned-in enemy, the media unwittingly gave Iraqis intelligence about follow-on air attacks, timing, and battle damage assessment (BDA) for their SCUD missiles. Technology and modern media reporting were creating new seams in the OPSEC armor.

Operations Restore Hope, Uphold Democracy, and Allied Force

The Marines planned and executed their Somalia operations with media coordination. In Operation Restore Hope, 20 journalists trained with and accompanied the Marines during their amphibious assault on Mogadishu. An operational security issue arose when journalists, who had not coordinated with the Marines, were waiting on the beach and filmed the assault live using bright lights to illuminate the scene. This OPSEC breach put both the Marines and journalists at risk. Conversely, in Operation United Shield, the Marines successfully coordinated and briefed all media organizations covering the UN departure from
Somalia. The media kept operational details secret until the mission was underway and maintained good mission OPSEC.\textsuperscript{lv}

During preparation for Operation Uphold Democracy in Haiti, operational commanders included the media in initial planning and briefed them on execution details.\textsuperscript{lvi} The media was also briefed that General Cedras watched CNN and that this was an OPSEC concern. As a result, the media agreed to a news embargo for the initial U.S. troop airdrops and to avoid showing troop locations.\textsuperscript{lvii} The coordination was successful and resulted in no media leaks.\textsuperscript{lviii}

Operation Allied Force in Kosovo started off on a bad note when a 24-hour news station televised live video of U.S. warplanes taking off to conduct bombing missions in Serbia.\textsuperscript{lix} This OPSEC breach unnecessarily put U.S. lives at risk by alerting the Serbian government and air defense network. NATO responded by restricting media access to operational information and instituted a “gag order” on military commanders and members.\textsuperscript{lx} The media again compromised the NATO war effort when the Washington Post published an article identifying two Belgrade targets on the NATO target list that had not been hit.\textsuperscript{lxi} As a result, additional information restrictions were levied against the media. NATO gradually reduced its information restrictions and allowed greater information flow to the media and public.

Operations Enduring Freedom and Iraqi Freedom

When the Global War on Terror (GWOT) started in 2001, it was clear that it was going to be a different kind of war with different restrictions on the media. Operation Enduring Freedom (OEF) was the first manifestation of the GWOT. Initially, it was a
Special Forces heavy operation against an adversary who had, and used, news media information for intelligence. OPSEC was a key component to engage the elusive Al-Qaeda. President George W. Bush told the American public that certain aspects of the GWOT would be seen by the public whereas others would not be covered by the media. Very limited media access was granted during OEF with a few media pools aboard aircraft carriers and eventually some in Afghanistan. Little information came from the media pool system that was not already covered by reporters in Washington news briefs. As OEF progressed, small groups of reporters were allowed to embed with U.S. forces during major operations such as Anaconda. The media released one story with serious operational security implications during OEF. The media revealed that Taliban and Al-Qaeda forces communicated with satellite phones that the United States was able to track and use to locate the enemy. Making this information available to a media-aware enemy was irresponsible and damaging. Not only did the information release affect the current operation, but it informed future U.S. enemies about a U.S. capability that was easy to thwart once revealed.

The next step in the GWOT was Operation Iraqi Freedom (OIF). Three major media environmental changes took place prior to OIF: technology, embedding, and access. Technology advances in data transmission equipment (size and capability) greatly improved mobile media reporting. Reporters used satellite phones, satellite videophones, and high-tech transmission trucks to send live reports directly to their parent companies. David Bloom’s truck could transmit live video to NBC, via satellite, while traveling at 50 mph. True “real-time” reports were now being broadcast from the battle as it was taking place. This was made possible by the military’s new policy to fully embed journalists. Of the 2500 journalists in theater for OIF, approximately 500 were embedded with U.S. and British
units. Some embedded reporters received training prior to OIF to educate them on military procedures and familiarize them with the combat environment. As part of the arrangement, “embeds” were required to follow a set of guidelines that focused on maintaining operational security for the mission. See Appendix B for guideline extracts. Embeds were granted unrestricted access within the limits of reasonable operational security and their reports did not undergo military review. Release of information for on-going engagements and upcoming operations was at the discretion of the on-scene commander. If the commander felt the reporter was trustworthy, the reporter was briefed on critical operational details as long as he agreed to a military review of his reports.

On the whole, military-media cooperation was good. Reporters agreed to several media embargos for operational security reasons and most were trustworthy with sensitive information. Despite these facts, there were several incidents that raised OPSEC concerns. One of the most prominent was when Geraldo Rivera of Fox revealed the mission and location of the 101st Airborne Division while conducting a live television broadcast. Other OPSEC problems arose from reporters who were not embedded, but were in the field unsponsored by the military. These reporters, referred to as “unilaterals,” were not bound by the guidelines and tended to show less discretion than the “embeds.” One reporter, Fred Francis, fielded a story that identified secret airfields being built by Special Forces and the CIA in Northern Iraq. Another “unilateral” reporter, Scott Pelley of CBS, reported live as U.S. helicopters shot Hellfires at Iraqi troops, in the opening hours of the war, during a Department of Defense requested embargo period. Neither of these reports contained vital information that the American public needed to know immediately, but both compromised operational security. One final OPSEC issue during OIF was the use of
Thuraya satellite phones by embedded reporters. These phones transmitted the global positioning system (GPS) location of the user and could have been exploited by the Iraqis to locate U.S. troop positions.\textsuperscript{\textit{lxxv}} CENTCOM banned the use of Thuraya phones, but some embeds continued to use them until they were forced to leave the theater due to their repeated OPSEC violations.

The Modern Media Environment - Why the Media is a Threat

Some might argue that the media is not a risk to operational security because, through historical study, it has demonstrated the ability to work with the military and withhold operationally sensitive information from the public. This theory, although mostly true, is not absolute. A small percentage of reporters have demonstrated that they are not trustworthy with sensitive information, and have caused OPSEC breaches both intentionally and unintentionally. The problem is that it only takes one report with sensitive information to compromise OPSEC, and put the mission and lives in danger. This fact, coupled with the modern media environment, makes media coverage of U.S. conflicts a risk to operational security.

The modern media environment is characterized by globalization, multinationalism, engaging reporting techniques, and technology. This modern environment directly affects military operations. Globalization has opened a huge market for the media, with a vast audience that spans the globe, and operates 24 hours a day, seven days a week. This vast audience often includes adversaries against whom the United States must act on the global stage in military conflict. The Husseins, Aidids, and Milosevics of the world are tuned-in to
this information smorgasbord watching the U.S. military’s every move as reported by the news media.

The U.S. military is operating ever more frequently in a multinational environment. We rely on our allies to execute the GWOT through combined operations. As such, the media environment is increasingly multinational as well. Foreign journalists and media organizations are gaining greater access to U.S. operations. The foreign media covering recent U.S. conflicts included countries that were hostile to our cause. In addition, some traditional American media companies claim status as international entities, not just American. An example of this is CNN. Thus, this author argues that the U.S. media in general should not be assumed to support U.S. objectives, and OPSEC in the multinational media should be considered always at risk.

Engaging reporting techniques employed by the media yield vast quantities of information about military operations from the strategic to tactical levels. The recent application of military subject matter experts (SME) and embedded reporters has added a new dimension. The media uses retired military officers as SMEs to comment on, or assess and interpret, military information. These pundits often surmise what they think the U.S. course of action for an operation will be, how the U.S. military might react to a situation, and criticize what they perceive to be flaws in current courses of action. In essence, this gives the public and our enemy a look inside the U.S. military mind. Embedded reporting yields an up-close look at our troops and their missions. It gives the public and our enemy a look at the tactical situation and how our troops deal with the combat mission. In the case of the suicide car bombers and the civilian deaths during the OIF road block incidents, the Iraqis could glean instant feedback on how their campaign was affecting U.S. operations and
morale because the media was documenting it from the field. Both standard and embedded reporting sheds light on the intangible elements of the operational factor of force. It gives the enemy insight into public support, will to fight, and morale and discipline of the troops. This is an obvious operational security concern.

Valuable intelligence information is available in open source media. The United States takes advantage of this fact and so does the enemy. All information has a time value associated with it. If information is not received and processed before this time, it is of no value to the enemy. What makes the modern media environment so dangerous is the speed with which information can go from the source or battlefield to the public. Through history, media transmission time has decreased to the point where the media has true “real-time” capability. Technology increases the likelihood that the enemy will receive media information in time to make use of it. The technology revolution has made censorship of media information almost impossible, and now commanders must rely on security at the source to keep sensitive information out of the media.

MITIGATING THE MEDIA RISK

To mitigate the media risk, operational commanders should educate and inform the media, educate their troops, match reporters to assignments, and insist upon media accountability.

Educating and informing the media is important because an informed media is more likely to make sound decisions and show greater discretion with respect to OPSEC. Educate the media on the military and combat environment, and how both function. This is best accomplished utilizing media boot camps prior to deployment and should be a prerequisite
for reporters to gain access to U.S. units. Once in theater, tell reporters what is expected of them and give them boundaries through a set of guidelines. Let the media know the type of information that is harmful to OPSEC, and the implications of OPSEC breaches in terms of mission and life. Give the media access so it will not seek it elsewhere. If security allows, inform the media of upcoming operations and how the mission will unfold. This will reduce speculation and info-seek outside the military media structure. Let reporters know what critical information must be guarded at each stage of the operation, and if they are in doubt, tell them to consult the on-scene commander. Operational commanders must arm the media so they can make the right decisions with respect to operational security.

The troops also need to be educated on the role of the media and how they should interact with reporters. Security at the source is essential in today’s media environment and troops must understand this fact. Servicemen should be taught that:

- Statements are always on the record
- Never lie; if OPSEC is at risk then decline to comment due to OPSEC reasons
- Statements can have political ramifications; servicemen are spokesmen for their country
- Speak only about what is known and avoid speculation
- Educate the media on the mission and military professionalism through actions

Troop education should take place throughout a serviceman’s career utilizing briefings and media input during training exercises. The operational commander should brief troops on media concerns once in theater, as well as distribute media rules of engagement (ROE) cards for reference in the field. Servicemen utilizing the concept of “security at the source” are the key to operational security in the modern media environment.

It is important for the operational commander to identify which reporters or media organizations pose the greatest threat to operational security, and to match assignments to these high risk groups as appropriate. This is important because some reporters, such as
Geraldo Rivera, have proved time and again to be irresponsible with access to sensitive information. In addition, the multinational nature of the media brings reporters and organizations to the theater that are opposed to U.S. military operations. These high-risk reporters, and organizations, are more likely to breach OPSEC. As such, they should be assigned where they will not be able to access sensitive information that is critical to the mission. The operational commander should also insure that these risk groups are carefully monitored to avoid OPSEC violations.

Finally, the commander should ensure that the media is held accountable for OPSEC violations. The current policy is to remove offenders from the theater of operations. This policy is too mild and often fails to deter reporters from stepping over the line. The media should have to sign a disclosure agreement with the U.S. government in order to gain access to the theater and U.S. units. The agreement should be similar to what servicemen sign for security clearances. This document should authorize judicial punishment for OPSEC violations that threaten the mission or servicemember’s lives, and include jail time and a fine for both the reporter and the reporter’s company. Increased deterrence is essential to increase OPSEC.

CONCLUSION

In our democratic society, public support and the will of the people are paramount to government and military success. The media plays a significant role in informing the people so they can exert their will on the government. As such, the media is an important part of U.S. military operations and will always be present in times of U.S. military conflict. Operational commanders must not ignore or shut out the media. They must work with the media to achieve mission success. Commanders must assess the risk posed by the media
with respect to OPSEC versus the benefit it provides in order to determine the level of media access. Operational commanders must then mitigate the risk caused by modern media coverage of U.S. military conflict while simultaneously maintaining public support. This is no small task for any man or woman in uniform.
NOTES


ii Milan Vego, Operational Warfare (Newport, RI: Naval War College, 2000), 281.


iv U.S. Constitution, amend. 1, sec. 1.

v Baroody, 21.


xi Ibid.

xii Joseph P. Avery, “Achieving a Working Relationship: An Historical Study of News Media-Military Relations to Identify and Evaluate Factors Affecting the Conflict Between National Security Requirements versus the News Media’s Right to Know” (Ph.D. diss., Graduate School of the Union Institute, 1994), 116-118.


xvi Porch, 6.

xvii Ibid.

xviii Aukofer and Lawrence, 35.

xxi Ibid.

xxii Aukofer and Lawrence, 36


xxvi Ibid., 19.

xxvii Aukofer and Lawrence, 36.

xxviii Ibid., 38.

xxix Ibid.


xxsiii Twentieth Century Fund Task Force and Braestrup, 29.

xxsiv Ibid., 60.

xxsv Ibid., 50.

xxsvi Aukofer and Lawrence, 40.


xxsviii Twentieth Century Fund Task Force and Braestrup, 65.

xxsiv Ibid.

xl Ibid., 67.


xlii Fox, 136.
xliii Kemper, 48.
xliv Snyder, 14.


xlvi Fox, 141.
"xlvii Kemper, 56.
xlviii Fox, 141.
xlix Ibid., 142.

lixii Baroody, 191.
lixiii Brent Baker, 64.
lixiv Baroody, 191.


lixviii John Shalikashvili, quoted in Aukofer and Lawrence, 161.

lixix Venable, 70.


lix x Ibid.


lix xv Ibid.


lxx Secretary of Defense, “Public Affairs Guidance (PAG) on Embedding Media.”


lxxiv Ibid.


lxxvi Baroody, 205.
BIBLIOGRAPHY


<http://www.journalism.wisc.edu/~drechsel/j559/readings/PentagonPapaers.html> [1 Feb 2004].


Ricchiardi, Sherry. “Preparing for War.” American Journalism Review. March 2003, 


Sheehan, Daniel B. “TV War Coverage in Iraq could have been Better.” U.S. Naval Institute Proceedings (October 2003): 73.


APPENDIX A

SOCIETY OF PROFESSIONAL JOURNALISTS CODE OF ETHICS
SOCIETY OF PROFESSIONAL JOURNALISTS
Code of Ethics

Seek Truth and Report It

Journalists should be honest, fair and courageous in gathering, reporting and interpreting information.

Journalists should:

• Test the accuracy of information from all sources and exercise care to avoid inadvertent error. Deliberate distortion is never permissible.

• Diligently seek out subjects of news stories to give them the opportunity to respond to allegations of wrongdoing.

• Identify sources whenever feasible. The public is entitled to as much information as possible on sources' reliability.

• Always question sources’ motives before promising anonymity. Clarify conditions attached to any promise made in exchange for information. Keep promises.

• Make certain that headlines, news teases and promotional material, photos, video, audio, graphics, sound bites and quotations do not misrepresent. They should not oversimplify or highlight incidents out of context.

• Never distort the content of news photos or video. Image enhancement for technical clarity is always permissible. Label montages and photo illustrations.

• Avoid misleading re-enactments or staged news events. If re-enactment is necessary to tell a story, label it.

• Avoid undercover or other surreptitious methods of gathering information except when traditional open methods will not yield information vital to the public. Use of such methods should be explained as part of the story.

• Never plagiarize.

• Tell the story of the diversity and magnitude of the human experience boldly, even when it is unpopular to do so.

• Examine their own cultural values and avoid imposing those values on others.

• Avoid stereotyping by race, gender, age, religion, ethnicity, geography, sexual orientation, disability, physical appearance or social status.

• Support the open exchange of views, even views they find repugnant.

• Give voice to the voiceless; official and unofficial sources of information can be equally valid.

• Distinguish between advocacy and news reporting. Analysis and commentary should be labeled and not misrepresent fact or context.

• Distinguish news from advertising and shun hybrids that blur the lines between the two.

• Recognize a special obligation to ensure that the public’s business is conducted in the open and that government records are open to inspection.
Minimize Harm

Ethical journalists treat sources, subjects and colleagues as human beings deserving of respect.

Journalists should:

- Show compassion for those who may be affected adversely by news coverage. Use special sensitivity when dealing with children and inexperienced sources or subjects.
- Be sensitive when seeking or using interviews or photographs of those affected by tragedy or grief.
- Recognize that gathering and reporting information may cause harm or discomfort. Pursuit of the news is not a license for arrogance.
- Recognize that private people have a greater right to control information about themselves than do public officials and others who seek power, influence or attention. Only an overriding public need can justify intrusion into anyone’s privacy.
- Show good taste. Avoid pandering to lurid curiosity.
- Be cautious about identifying juvenile suspects or victims of sex crimes.
- Be judicious about naming criminal suspects before the formal filing of charges.
- Balance a criminal suspect’s fair trial rights with the public’s right to be informed.

Act Independently

Journalists should be free of obligation to any interest other than the public's right to know.

Journalists should:

- Avoid conflicts of interest, real or perceived.
- Remain free of associations and activities that may compromise integrity or damage credibility.
- Refuse gifts, favors, fees, free travel and special treatment, and shun secondary employment, political involvement, public office and service in community organizations if they compromise journalistic integrity.
- Disclose unavoidable conflicts.
- Be vigilant and courageous about holding those with power accountable.
- Deny favored treatment to advertisers and special interests and resist their pressure to influence news coverage.
- Be wary of sources offering information for favors or money; avoid bidding for news.

Be Accountable

Journalists are accountable to their readers, listeners, viewers and each other.

Journalists should:

- Clarify and explain news coverage and invite dialogue with the public over journalistic conduct.
• Encourage the public to voice grievances against the news media.

• Admit mistakes and correct them promptly.

• Expose unethical practices of journalists and the news media.

• Abide by the same high standards to which they hold others.

The SPJ Code of Ethics is voluntarily embraced by thousands of writers, editors and other news professionals. The present version of the code was adopted by the 1996 SPJ National Convention, after months of study and debate among the Society's members.
APPENDIX B

EXTRACTS OF PUBLIC AFFAIRS GUIDANCE (PAG) ON EMBEDDING MEDIA DURING POSSIBLE FUTURE OPERATIONS/DEPLOYMENTS IN THE U.S. CENTRAL COMMANDS (CENTCOM) AREA OF RESPONSIBILITY (AOR).
1. PURPOSE. This message provides guidance, policies and procedures on embedding news media during possible future operations/deployments in the CENTCOM AOR. It can be adapted for use in other unified command AORs as necessary.

2. POLICY.

2.A. The Department of Defense (DOD) policy on media coverage of future military operations is that media will have long-term, minimally restrictive access to U.S. air, ground and naval forces through embedding. Media coverage of any future operation will, to a large extent, shape public perception of the national security environment now and in the years ahead. This holds true for the U.S. public; the public in allied countries whose opinion can affect the durability of our coalition; and publics in countries where we conduct operations, whose perceptions of us can affect the cost and duration of our involvement. Our ultimate strategic success in bringing peace and security to this region will come in our long-term commitment to supporting our democratic ideals. We need to tell the factual story - good or bad - before others seed the media with disinformation and distortions, as they most certainly will continue to do. Our people in the field need to tell our story – only commanders can ensure the media get to the story alongside the troops. We must organize for and facilitate access of national and international media to our forces, including those forces engaged in ground operations, with the goal of doing so right from the start. To accomplish this, we will embed media with our units. These embedded media will live, work and travel as part of the units with which they are embedded to facilitate maximum, in-depth coverage of U.S. forces
in combat and related operations. Commanders and public affairs officers must work together to balance the need for media access with the need for operational security.

2.C.4. No communications equipment for use by media in the conduct of their duties will be specifically prohibited. However, unit commanders may impose temporary restrictions on electronic transmissions for operational security reasons. Media will seek approval to use electronic devices in a combat/hostile environment, unless otherwise directed by the unit commander or his/her designated representative. The use of communications equipment will be discussed in full when the media arrive at their assigned unit.

3. PROCEDUERS

3.F. Embedded media operate as part of their assigned unit. An escort may be assigned at the discretion of the unit commander. The absence of a PA escort is not a reason to preclude media access to operations.

3.G. Commanders will ensure the media are provided with every opportunity to observe actual combat operations. The personal safety of correspondents is not a reason to exclude them from combat areas.

3.M. Media will agree to abide by the CENTCOM/OASD(PA) ground rules stated in para. 4 of this message in exchange for command/unit-provided support and access to service members, information and other previously-stated privileges. Any violation of the ground rules could result in termination of that media's embed opportunity.

3.N. Disputes/difficulties. Issues, questions, difficulties or disputes associated with ground rules or other aspects of embedding media that cannot be resolved at the unit level, or through the chain of command, will be forwarded through PA channels for resolution. Commanders who wish to terminate an embed for cause must notify CENTCOM/PA prior to termination. If a dispute cannot be resolved at a lower level, OASD(PA) will be the final resolution authority. In all cases, this should be done as expeditiously as possible to preserve the news value of the situation.

3.Q. The standard for release of information should be to ask "why not release" vice "why release." Decisions should be made ASAP, preferably in minutes, not hours.

3.R. There is no general review process for media products. See para 6.A. for further detail concerning security at the source.

4. GROUND RULES. For the safety and security of U.S. forces and embedded media, media will adhere to established ground rules. Ground rules will be agreed to in advance and signed by media prior to embedding. Violation of the ground rules may result in the immediate termination of the embed and removal from the AOR. These ground rules recognize the right of the media to cover military operations and are in no way intended to
prevent release of derogatory, embarrassing, negative or uncomplimentary information. Any modification to the standard ground rules will be forwarded through the PA channels to CENTCOM/PA for approval. Standard ground rules are:

4.A. All interviews with service members will be on the record. Security at the source is the policy. Interviews with pilots and aircrew members are authorized upon completion of missions; however, release of information must conform to these media ground rules.

4.B. Print or broadcast stories will be datelined according to local ground rules. Local ground rules will be coordinated through command channels with CENTCOM.

4.C. Media embedded with U.S. forces are not permitted to carry personal firearms.

4.D. Light discipline restrictions will be followed. Visible light sources, including flash or television lights, flash cameras will not be used when operating with forces at night unless specifically approved in advance by the on-scene commander.

4.E. Embargoes may be imposed to protect operational security. Embargoes will only be used for operational security and will be lifted as soon as the operational security issue has passed.

4.F. The following categories of information are releasable.
4.F.1. Approximate friendly force strength figures.
4.F.2. Approximate friendly casualty figures by service. Embedded media may, within opsec limits, confirm unit casualties they have witnessed.
4.F.3. Confirmed figures of enemy personnel detained or captured.
4.F.4. Size of friendly force participating in an action or operation can be disclosed using approximate terms. Specific force or unit identification may be released when it no longer warrants security protection.
4.F.5. Information and location of military targets and objectives previously under attack.
4.F.6. Generic description of origin of air operations, such as "land-based."
4.F.7. Date, time or location of previous conventional military missions and actions, as well as mission results are releasable only if described in general terms.
4.F.8. Types of ordnance expended in general terms.
4.F.9. Number of aerial combat or reconnaissance missions or sorties flown in CENTCOM's area of operation.
4.F.10. Type of forces involved (e.g., air defense, infantry, armor, marines).
4.F.11. Allied participation by type of operation (ships, aircraft, ground units, etc.) After approval of the allied unit commander.
4.F.14. Service members' names and home towns with the individuals' consent.

4.G. The following categories of information are not releasable since their publication or broadcast could jeopardize operations and endanger lives.
4.G.1. Specific number of troops in units below Corps/MEF level.
4.G.2. Specific number of aircraft in units at or below the Air Expeditionary Wing level.
4.G.3. Specific numbers regarding other equipment or critical supplies (e.g. artillery, tanks, landing craft, radars, trucks, water, etc.).
4.G.4. Specific numbers of ships in units below the Carrier Battle Group level.
4.G.5. Names of military installations or specific geographic locations of military units in the CENTCOM area of responsibility, unless specifically released by the Department of Defense or authorized by the CENTCOM commander. News and imagery products that identify or include identifiable features of these locations are not authorized for release.
4.G.7. Information regarding force protection measures at military installations or encampments (except those which are visible or readily apparent).
4.G.8. Photography showing level of security at military installations or encampments.
4.G.10. Information on intelligence collection activities compromising tactics, techniques or procedures.
4.G.11. Extra precautions in reporting will be required at the commencement of hostilities to maximize operational surprise. Live broadcasts from airfields, on the ground or afloat, by embedded media are prohibited until the safe return of the initial strike package or until authorized by the unit commander.
4.G.12. During an operation, specific information on friendly force troop movements, tactical deployments, and dispositions that would jeopardize operational security or lives. Information on on-going engagements will not be released unless authorized for release by on-scene commander.
4.G.13. Information on special operations units, unique operations methodology or tactics, for example, air operations, angles of attack, and speeds; naval tactical or evasive maneuvers, etc. General terms such as "low" or "fast" may be used.
4.G.15. Information identifying postponed or canceled operations.
4.G.16. Information on missing or downed aircraft or missing vessels while search and rescue and recovery operations are being planned or underway.
4.G.17. Information on effectiveness of enemy camouflage, cover, deception, targeting, direct and indirect fire, intelligence collection, or security measures.
4.G.18. No photographs or other visual media showing an enemy prisoner of war or detainee's recognizable face, nametag or other identifying feature or item may be taken.
4.G.19. Still or video imagery of custody operations or interviews with persons under custody.

4.H. The following procedures and policies apply to coverage of wounded, injured, and ill personnel:
4.H.1. Media representatives will be reminded of the sensitivity of using names of individual casualties or photographs they may have taken which clearly identify casualties until after notification of the NOK and release by OASD(PA).
4.H.2. Battlefield casualties may be covered by embedded media as long as the service member's identity is protected from disclosure for 72 hours or upon verification of NOK notification, whichever is first.
6. SECURITY

6.A. Media products will not be subject to security review or censorship except as indicated in para. 6.A.1. Security at the source will be the rule. U.S. military personnel shall protect classified information from unauthorized or inadvertent disclosure. Media provided access to sensitive information, information which is not classified but which may be of operational value to an adversary or when combined with other unclassified information may reveal classified information, will be informed in advance by the unit commander or his/her designated representative of the restrictions on the use or disclosure of such information. When in doubt, media will consult with the unit commander or his/her designated representative.

6.A.1. The nature of the embedding process may involve observation of sensitive information, including troop movements, battle preparations, materiel capabilities and vulnerabilities and other information as listed in para. 4.G. When a commander or his/her designated representative has reason to believe that a media member will have access to this type of sensitive information, prior to allowing such access, he/she will take prudent precautions to ensure the security of that information. The primary safeguard will be to brief media in advance about what information is sensitive and what the parameters are for covering this type of information. If media are inadvertently exposed to sensitive information they should be briefed after exposure on what information they should avoid covering. In instances where a unit commander or the designated representative determines that coverage of a story will involve exposure to sensitive information beyond the scope of what may be protected by prebriefing or debriefing, but coverage of which is in the best interests of the DOD, the commander may offer access if the reporter agrees to a security review of their coverage. Agreement to security review in exchange for this type of access must be strictly voluntary and if the reporter does not agree, then access may not be granted. If a security review is agreed to, it will not involve any editorial changes; it will be conducted solely to ensure that no sensitive or classified information is included in the product. If such information is found, the media will be asked to remove that information from the product and/or embargo the product until such information is no longer classified or sensitive. Reviews are to be done as soon as practical so as not to interrupt combat operations nor delay reporting. If there are disputes resulting from the security review process they may be appealed through the chain of command, or through PA channels to OASD/PA. This paragraph does not authorize commanders to allow media access to classified information.

6.A.2. Media products will not be confiscated or otherwise impounded. If it is believed that classified information has been compromised and the media representative refuses to remove that information notify the CPIC and/or OASD/PA as soon as possible so the issue may be addressed with the media organization's management.