

Unclassified Paper

NAVAL WAR COLLEGE
Newport, RI

The Role of Special Operations Forces in Information Warfare:

Enablers, Not Cyber Warriors

by

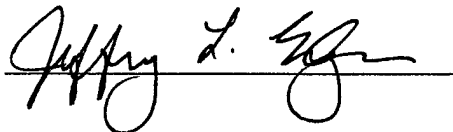
Jeffrey L. Edgar

Commander, United States Navy

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:

A handwritten signature in black ink, appearing to read "Jeffrey L. Edgar", written over a horizontal line.

16 May 2000

BTIS QUALITY INSPECTED 4
20000914 024

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED			
2. Security Classification Authority:			
3. Declassification/Downgrading Schedule:			
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.			
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT			
6. Office Symbol: C		7. Address: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207	
8. Title (Include Security Classification): The Role of Special Operations Forces (SOF) in Information Warfare (IW): Enablers, not Cyber Warriors (U)			
9. Personal Authors: Jeffry L. Edgar, <i>CDR, USN</i>			
10. Type of Report: FINAL		11. Date of Report: 16 May 2000	
12. Page Count: 26		12A Paper Advisor (if any):	
13. Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.			
14. Ten key words that relate to your paper: Special Operations Forces (SOF), Information Warfare (IW), Information Operations (IO), Computer Network Attack (CNA), U.S. Special Operations Command (SOCOM), Roles and Missions, Principal Missions, Collateral Activities, Electronic Warfare.			
15. Abstract: Of the nine principal missions the United States Special Operations Command (SOCOM) is assigned, one - Information Warfare (IW) - is not unique to SOF. Conventional forces also execute IW. As a result, SOF runs the risk of losing its unique character as it tries to assume a role that conventional forces can fulfill. Thus, IW should be downgraded from a principal mission for SOF to a collateral activity, or secondary mission. SOF, because of the close access they maintain to many targets and the unique regional focus of the majority of SOCOM assets, can fill a critical void in U.S. military IW. As IW matures and missions evolve for both special operations and conventional forces, SOF must stake a claim that allows them to retain their core competencies but not duplicate conventional missions, and must invest in those aspects of IW that complement currently assigned tasks. They must act as enablers for U.S. IW efforts as they offer unique capabilities that no other force can bring to bear. They literally cannot afford to become cyber warriors or cyber illiterates.			
16. Distribution / Availability of Abstract:	Unclassified X	Same As Rpt	DTIC Users
17. Abstract Security Classification: UNCLASSIFIED			
18. Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT			
19. Telephone: 841-6461		20. Office Symbol: C	

Table of Contents

<u>Item</u>	<u>Page</u>
Introduction	1
Special Operations Missions	2
Information Warfare - What Is It?	5
What Should SOF Missions Be?	6
What are the Risks Associated with Inappropriate Missions?	8
Should IW Be a Principal Mission for SOF?	9
What are the Implications of IW as a Collateral Activity?	13
Conclusion	15
Endnotes	16
Glossary	18
Bibliography	24

The Role of Special Operations Forces in Information Warfare: Enablers, Not Cyber Warriors

The United States' Special Operations Forces (SOF) are arguably the world's premier fighting units. Their training and operations are among the most grueling in the world, and as a result they conduct precision tactical missions that due to their sensitive nature have operational or even potentially strategic impact.

As commandos and unconventional warriors, SOF excel in specific missions that U.S. military conventional forces are unable to accomplish because the tasking requires specialized forces using unique training, methods, equipment and intelligence. Of the nine principal missions the United States Special Operations Command (SOCOM) is assigned, one - Information Warfare (IW) - is not unique to SOF. Conventional forces also execute IW. As a result, SOF runs the risk of losing its unique character as it tries to assume a role that conventional forces can fulfill. Thus, IW should be downgraded from a principal mission for SOF to a collateral activity, or secondary mission.

So what should the role of SOF in IW be? Are special operators to sit in headquarters facilities and engage in Computer Network Attack (CNA) versus adversary systems? That would seem to duplicate civil as well as conventional military capabilities, and is thus not "SOF-unique." Conversely, should SOF personnel remain essentially ignorant of IW, allowing conventional forces to fulfill the IW requirements SOCOM determines are necessary for warfighting? This too, would be less than optimal as personnel not intimately familiar with SOF requirements would attempt to provide critical mission support.

The truth lies in the middle. SOF, because of the close access they maintain to many targets and the unique regional focus of the majority of SOCOM assets, can fill a critical void in U.S. military IW. As IW matures and missions evolve for both special operations and conventional forces, SOF must stake a claim that allows them to retain their core competencies but not duplicate conventional missions, and must invest in those aspects of IW that complement currently assigned tasks. They must act as enablers for U.S. IW efforts as they offer unique capabilities that no other force can bring to bear. They literally cannot afford to become cyber warriors or cyber illiterates.

Special Operations Missions

The critical failure of Operation Rice Bowl – better known as Desert One - in the Iranian desert in April 1980 was the catalyst that resulted in the 1987 Cohen-Nunn amendment to the Goldwater-Nichols Act of 1986.¹ This historic legislation led to the creation of an Assistant Secretary of Defense for Special Operations / Low Intensity Conflict (ASD-SO/LIC), and SOCOM, with a four-star general officer assigned as Commander in Chief (CINC) of all Army, Navy and Air Force SOF assets. In addition, SOCOM was given its own Major Force Program and budget line (MFP-11; the “SOF checkbook”); authority to research, develop and acquire specialized equipment peculiar to special operations; and, perhaps most unusually, assigned specific missions. No other CINC has had their missions spelled out in legislation. A primary reason for the specificity in the legislation was the acrimonious atmosphere within the Department of Defense (DoD) that led Congress to force a

solution to the “broken SOF” problem on the services in the first place. To ensure the conventional forces did not either ignore or run roughshod over the new command, the legislation detailed what SOCOM would do and how they would do it. MFP-11 authority was the real key to the services’ forced acceptance of SOF. It allowed SOCOM to operate out from under the thumb of the services, and to develop SO-peculiar equipment without being dependent on them either, since the services had shown a propensity in the past to cut SOF operations, forces and budgets quickly and utterly.

The missions assigned originally by the statute were “Direct Action (DA), Strategic Reconnaissance (SR), Unconventional Warfare (UW), Foreign Internal Defense (FID), Civil Affairs (CA), Psychological Operations (PSYOP), Counterterrorism (CT), Humanitarian Assistance (HA), theater Search and Rescue (SAR) [and] other such activities as may be specified by the President and the Secretary of Defense.”² (See glossary for explanation of terms.) Since the amendment was passed, its direction has been modified somewhat. Strategic Reconnaissance is now known as Special Reconnaissance. The intent of including the theater SAR mission in the law was to have SOF provide all SAR services regardless of the branch of the downed pilot. Due to continued service rivalry, however, SOCOM provides dedicated SAR services for SOF aviation and for conventional forces only when tasked. The CT mission has been combined with anti-terrorism, and is now known as Combatting Terrorism (CBT). SOF has a primary role with DoD for counterterrorism, but is responsible as with any other military organization for anti-terrorism measures.

In addition, SOF have taken on additional tasks, and have divided up all assignments into two categories, *principal missions* and *collateral activities*. The result is a refined mix of functions derived from legislation, operational experience and the ever-changing international security environment.³ Although not strictly defined, principal missions are taken to be those requiring specialized personnel, equipment, training and tactics that go beyond the routine capabilities of conventional U.S. military forces.⁴ The formal nine principal missions are DA, SR, FID, UW, CBT, Counterproliferation of Weapons of Mass Destruction (CP), CA, PSYOP and Information Warfare (IW). Collateral activities are those that have frequently been assigned by geographic CINCs, and are derived from SOF ability to conduct principal missions.⁵ The collateral activities are Coalition Support, Combat SAR, Counterdrug (CD) activities, Countermine (CM) activities, Humanitarian Assistance (HA), Security Assistance (SA) and Special activities.⁶ SOCOM can potentially alter principal missions and collateral activities as it sees fit, and has. CP, IW, Coalition Support, CD, CM, HA and SA are all missions SOCOM added since the original legislation was passed.

As stated previously, principal missions are those that SOF execute because they have a unique capability or contribution within that area that conventional forces do not possess. With one glaring exception, in each of those principal missions, SOF do not duplicate or overlap conventional capabilities and play the major role in DoD as the acknowledged experts in those specialties. The exception is IW; SOF are by no means the IW “pros from Dover” within the U.S. military.

Information Warfare – What Is It?

Information Warfare (IW) is a subset of Information Operations (IO). The primary distinction between the two is the time of employment. IW is conducted during crisis or conflict, so the emphasis is on the “W” in IW. IO is conducted throughout the continuum of conflict from peace to crisis to war and back again.

IW involves more than just machines and injections of viruses into computers. It exploits, targets, and protects information itself, plus information systems and processes, and the human element that uses that information from those systems and via those processes.⁷ IW attempts to deny, degrade, deceive or disrupt the adversary’s decision cycle while preventing him from doing the same to you.

There are both offensive and defensive (IW-D) components to IW. Offensively, there are numerous examples of potential targets of IW. Leadership at the national or operational level to include key personnel, ADP support, strategic communications, and power base; military infrastructure to include commanders, command and control (C2) communications links and nodes, and intelligence collectors; civil infrastructure to include communications links and nodes, industry, finance and populace; and weapons systems to include platforms, artillery, precision-guided munitions (PGMs) and air defense are all examples of legitimate IW targets.⁸ These are specific enemy functions, systems or people to be possibly attacked subtly or overtly with IW weapons. The net effect is a slowing or disruption of the ability to make decisions, thus allowing U.S. or coalition forces to seize an information and corresponding military advantage. Again, the emphasis is not necessarily on machines, but on the

human that requires the machines and the information they process to make decisions in time of crisis.

Defensively, the target sets are the same, except now they belong to the United States. Fundamentally, U.S. IW-D must be able to stop the enemy from doing to us what we are attempting to do to him. Since the United States as a nation is arguably more dependent on information than any other, this defensive effort is vital to the success of military operations. Although not as “glamorous” as offensive IW, defensive IW plays perhaps a greater role because of our inherent vulnerabilities.

IW and IO are obviously national level concerns. The most recent National Security Strategy (NSS) states that protection of our critical infrastructures from cyber and physical attacks is a vital national interest – of broad overriding importance to the safety of our nation.⁹ Given the variety of targets on both sides, the opportunities and threats are strategic, operational and tactical. Therefore, it is highly unlikely that such a crucial mission would ever be assigned primarily to DoD, let alone one military service or CINC. Thus SOF cannot be expected to assume a lion’s share role in IW for the nation or DoD.

What Should SOF Missions Be?

As stated at the outset, SOF when operational generally assume one of two generic, traditional roles; one is that of a commando, and the other is an unconventional warrior. All principal missions and collateral activities can be categorized in one of these two roles. Therefore if a mission does not fit into one of these groupings, it is most likely not a special operation, and ought not to be a

principal mission for SOF. The converse is also true; if a mission fits into one of these two roles, it is most likely a SOF mission and not appropriate for conventional forces.¹⁰

In a commando role, SOF use covert or clandestine techniques to conduct specific, limited operations directly against an adversary. As such, they will use essentially all five requirements that distinguish special operations from conventional military operations: unconventional training and equipment, political sensitivity, unorthodox approaches, limited opportunity and specialized intelligence.¹¹ Examples of commando missions are DA, SR and CT.

The unconventional warfare role entails training, advising, or otherwise interacting with foreign forces. In essence the only SOF special requirement necessary for this role is political sensitivity, to include regional and cultural awareness, but this is still a discrete capacity that general-purpose forces do not normally possess. Unconventional warfare operations are conducted indirectly against an enemy via a proxy. Examples are FID, CA and PSYOP.

IW is the mission most recently added to SOCOM's principal missions list. As an emerging mission area, IW has received considerable attention within the U.S. military as the nation's forces come to grips with how to "fight with or against electrons." The services and indeed the nation are struggling with how to defend against cyber attacks on infrastructure and assets. SOF are no different. Should IW in fact, be a principal mission for SOCOM? To help decide, it is useful to take into account four rules of thumb when considering any new mission for SOF.

First, does the mission have as a necessary condition of success that commandos or unconventional warriors undertake it? If so, it should be considered a SOF principal mission. Second, will the chances for mission success significantly increase if SOF perform or participate in the mission? If yes, then it might be a collateral activity. It is often an attribute of collateral activities that SOF cannot accomplish them single-handedly. Third, will the task only be better performed marginally by SOF? If so, it is most likely not a SOF mission. In these cases, the mission should not be assigned to SOF formally, but the theater CINC makes this decision dependent on the situation. Fourth, if the mission is not better performed by SOF, or is better performed by conventional forces, then it is obviously inappropriate for SOF.¹²

What are the Risks Associated with Inappropriate Missions?

If the guidelines above are ignored, four disadvantages might result. The first is that using SOF for conventional missions that can and should be carried out by conventional operators infringes on general purpose capabilities and wastes precious SOF resources. SO-peculiar development is supposed to preclude expending SOF resources on service-common items. It also stands to reason that in an era of stagnant budgets and manpower shortages, undertaking additional missions without an increase in the resources essential to accomplish them means other capabilities must necessarily suffer. SOF cannot do more with the same amount. Other taskings will most likely be negatively impacted, and ultimately, SOF will be accused of attempting to infringe on conventional force missions. SOF might also be accused, as has been done in the past, of depleting conventional forces of talent and capital more

appropriately needed for these conventional tasks. Second, by undertaking these non-special missions, SOF begin to lose the unconventional mindset, approach and assets that make them special in the first place. These missions would not necessarily need unconventional training, equipment, or approaches or specialized intelligence, and SOF operators might begin to “think conventional.” Third, if SOF advertises or intimates that they can carry out a non-appropriate mission, a CINC or Joint Task Force (JTF) commander may take that to mean that SOF can undertake any mission within that area, and thus SOF might be assigned completely inappropriate and potentially disastrous missions. This would be the result of a broad misinterpretation of the meaning of a principal mission. Finally, and most importantly, should SOF become more general purpose, there would be those who argue that this blurs the distinction between SOF and conventional forces, and potentially obviates the need for SOF in the first place. Why do we need these special warriors if they are doing things conventional forces already do?

Should IW Be a Principal Mission for SOF?

With these rules of thumb as guidance, let us examine the role of IW within SOF. The first rule indicates SOF should be assigned IW as a principal mission only if they above all others are the key to mission success. Since IW is a vital national interest, it will entail civil-military involvement. Civil authorities, with the military as a willing partner, will undoubtedly lead defensive IW efforts, as the U.S. information infrastructure is so vast. The National Command Authority (NCA), through the regional CINCs, will most likely lead offensive IW efforts in execution of appropriate

warplans, with each service and numerous governmental agencies playing a role. Thus since no one organization in a theater, including SOF, can be considered as crucial to success in IW, certainly SOF are not sine quo non, and therefore should not assume IW as a principal mission.

The next rule of thumb states that if the odds for mission success significantly increase if SOF perform or participate in the mission, then it might be a collateral activity. In this case, SOF can contribute significantly within certain contexts.

SOCOM advocates that PSYOP, Operations Security (OPSEC), Military Deception (MILDEC), physical destruction, Electronic Warfare (EW), and CNA are the six elements of SOF IO.¹³ Within these areas, SOF is a role player in each theater. They can contribute significantly to each in time of crisis or war. Since all PSYOP forces in the U.S. military are assigned to SOCOM, they are the sole source of expertise in projecting selected messages to target audiences. OPSEC is critical to successful mission accomplishment for SOF, but is more of an Operational Protection issue than anything else. MILDEC for SOF most often means supporting a conventional forces deception effort. For example, in Desert Storm, Naval Special Warfare personnel (SEALs) provided deception to persuade the Iraqis that an amphibious assault was underway.¹⁴ Physical destruction has always been part of the SOF repertoire, especially within the DA mission area. Actions at the objective are the prime focus of the DA mission, and more often than not that action has been to destroy a target of significant military value to the enemy.

EW is a sensible component to add to the SOF IW mix. Each of the three phases of EW has potential for SOF gain. SOF can always benefit from Electronic Warfare

Support (ES), which produces threat warning information and combat direction finding. Thus enemy forces may be potentially located, and their intentions possibly revealed. As well, Electronic Protection (EP) provides security for SOF equipment and operations against enemy attempts at electronic interference. Electronic Attack (EA) is a sensitive area for SOF because unlike ES and EP, which are primarily passive and require no emanations, almost every EA action will require radiation of electronic emissions. Because SOF normally operate in a covert or clandestine mode, most operators would be hesitant to use EA measures directly from their own troops or positions unless in an extremis situation. The most likely employment of EA would be by a third party in support of SOF operations, such as via an EC-130 Compass Call communications jamming aircraft, or a radar jammer like the Navy and Marine Corps EA-6B Prowlers.

The final SOF IO element, CNA, is problematic. It is difficult to envision a Navy SEAL or Army ranger hunkered down over a keyboard, using a computer as his weapon to attack the enemy. This is not to say that SOF personnel are not capable of such tasks, but with the rigorous training they undertake to maintain their superior proficiency in current core competencies, it would be an extreme challenge to require them to become expert "hackers" as well. Proficiency to the level required to attack enemy computer systems would require years of training and practice at the expense of other skills; that is time SOF operators cannot afford.

As this again is not a SOF-unique mission, the aspect of CNA that would have to apply to SOF would be in only one of two distinct areas. First, CNA could be used to deny the adversary indications that SOF personnel were conducting actions behind

his lines. Enemy command and control (C²) networks could be interfered with so that ongoing SOF operations would either not be detected, or the detection and subsequent reporting efforts would be severely hindered, facilitating SOF mission success. This is a parallel to the radar or communications jamming aircraft in that it is a form of attack that would more optimally be employed by personnel other than the SOF mission operators, as a third party in support. The other distinct area in which SOF could be involved with CNA is if the attack itself was only possible through a critical SOF capability; i.e., close access to a target. The target of the attack would have to be completely inaccessible via normal CNA channels, and would necessitate SOF personnel making a physical interface during a DA mission. SOF would then enable distant personnel to perform the attack via remote link, or be trained to perform the attack themselves. Again, the former scenario is much more plausible. The attack is much more likely to succeed if the SOF mission personnel can emplace relay and injection devices and quickly exfiltrate, rather than having to remain on station and try to “hack” into the affected system.

Returning to our rules of thumb, the third asks whether SOF will perform the mission only marginally better than conventional forces. If so, it is most likely not a SOF mission. As we saw from the last rule, SOF can perform the mission much better than general purpose forces when it requires SOF-unique characteristics. In other cases, SOF is not likely the asset of choice for IW missions. So in certain limited situations, SOF can perform the mission not just marginally better than conventional forces, but significantly. In many other instances, however, SOF will not be able to conduct IW on anywhere near the scale as general purpose forces.

The final rule states that if the mission is not better performed by SOF, or is better performed by conventional forces, then it is obviously inappropriate for SOF. Again, we have shown that there is at least one case where this is not true, therefore IW is appropriate for SOF.

Considering our four rules in total, it is apparent that SOF satisfies our criteria for the second rule with respect to IW but not the first, third or fourth. Therefore we can conclude that IW should be a collateral activity for SOF. As such, it has differing implications than it would as a principal mission.

What Are The Implications of IW as a Collateral Activity?

IW for SOF fulfills the two-part definition of a collateral activity in that (a) it is derived from the ability to conduct principal missions, and (b) will undoubtedly be assigned as per geographic CINCs direction in fulfillment of crisis or wartime requirements. With respect to (a), as illustrated above SOF can conduct DA missions with an IW attack as an ultimate goal, but mission remains DA, not IW. In examples like these, the fact that SOF conducts principal missions leads directly to the ability to carry out a secondary mission, in this case IW. Detailing the myriad of ways in which IW can support each principal mission is beyond the scope of this paper, but in doctrine SOCOM shows how SOF efforts support conventional forces' execution of IW, and gives examples of how SOF limited IW could be employed. For example, "...direct action missions against key command and control nodes may destroy the enemy's ability to coordinate counterattacks, furthering friendly forces in massing and maneuvering..." and "...SOF can help conventional forces achieve surprise by the

timely disruption or degradation of enemy early warning capabilities and C4I facilities prior to conventional force attack.”¹⁵ Also, SOF could take advantage of technology that allows forces to “...electronically mimic foreign languages and dialects.”¹⁶

Regarding the second half of the collateral activity definition, the geographic CINCs will assign or coordinate the vast majority of wartime or crisis tasking in their theater. The coordination will be based on Joint Targeting Coordination Board decisions, which will include determining whether SOF are the right asset for the job. This determination will take into account overall SOF tasking and capabilities. As a collateral activity, SOF will much more likely be assigned principal missions, with which they are all already intimately familiar, that could support an IW campaign for conventional forces, as noted earlier.

As a collateral activity for SOF, IW can provide offensive, defensive and exploitation support to all principal missions equally. From a broad perspective, SOCOM must ensure all SOF IW efforts are geared towards one fundamental tenet: the research and development, acquisition, training, doctrine and operational use of tools that facilitate principal missions. In other words, SOF must concentrate on IW instruments that directly support DA, SR, CT, CP, etc. As a collateral mission, IW is an enabler for SOF. The tools used in IW should enhance the things that make SOF unique, including access to the target and regional specialization. They should not duplicate or compete with conventional tools. SOCOM IW planners must get operators closer to the target and allow them to stay there longer, or provide them an increased awareness of host countries and areas of focus. These are the elements of special

operations that no other military branch can match. SOF must focus all IW effort towards emphasizing distinctive, SOF-unique strengths, and avoiding IW endeavors that do not.

Creating cyber warriors within SOF would entail too much additional training for personnel already tasked with the most demanding training our military has. It would also bleed over into conventional forces' areas of expertise, which would be at cross-purposes to SOF roles and missions, and would drain precious SOF time and resources, which could better spent refining principal mission activities.

Conversely, ignoring IW would put SOF at peril. Certainly from a defensive standpoint, U.S. information systems are under attack every day, peace or war. SOF must deal with this problem at every echelon of command, as does every military unit and government agency. There are as well offensive capabilities of which SOF could take advantage to facilitate mission success. To disregard these would be to put personnel at an extreme disadvantage in the field, which directly impacts mission success.

Therefore, special operations forces can not be cyber warriors or cyber illiterates. They must act as IW enablers, supporting conventional force IW, and using IW tools to maintain their tactical advantages.

Conclusion

The creation of the Special Operations Command in 1987 and the assignment of all special operations personnel and assets to that CINC are a resounding success. The drawbacks of previous SOF acquisition, training, manning, operations and missions

have largely been eliminated by the intelligent crafting of the legislation, which led to increased cooperation with the services and a much more robust fighting force.

In carving out new roles and missions for the command in the post-Cold War era however, SOCOM must exercise great care and fight the natural tendency to want to get involved in evolving missions merely because they are new, or do not want to become obsolete or overlooked in the new area. SOF cannot run the risk of losing their unique capabilities just because there is an emerging field of technology. The dangers are great in that a mission over-stretch will have long-term effects on SOF. The net result possibly could affect the foundations of special operations themselves and the reasons why the United States continues to maintain SOF.

There is a role for special operations forces within Information Warfare. It is a narrowly defined role though because the requirements necessary to execute most IW missions exclude SOF since special operations are so narrowly focused, whereas IW is overly broad. To find the niche within which SOF can operate in IW requires careful analysis of SOF operating principles. Deciding whether a task is a principal mission, collateral activity or inappropriate is a significant undertaking, and must be considered in the full light of how roles and missions are defined. In the case of IW, SOCOM should execute it as a collateral activity, which would support not only their principal missions but also enable conventional force operations. As an elite force that requires every advantage to succeed, SOF can use IW to their great benefit or can ignore or misapply it at their peril.

¹ Susan L. Marquis, Unconventional Warfare: Rebuilding U.S. Special Operations Forces, (Washington, D.C.: Brookings Institution 1997), 1-3.

² *Ibid.*, 146.

-
- ³ Special Operations Command, Special Operations in Peace and War (SOCOM Pub 1) (Washington, D.C.: January 25, 1996), 3-1.
- ⁴ Department of Defense, United States Special Operations Forces: Posture Statement 1998. (Washington, D.C.: Department of Defense (OSD-SO/LIC), 1998), 2.
- ⁵ SOCOM Pub 1, 3-1.
- ⁶ Ibid.
- ⁷ Special Operations Command, USSOCOM Information Operations (IO) Policy, Policy Memorandum 98-17 (Tampa, FL: September 30, 1998), 5.
- ⁸ Joint Chiefs of Staff, Information Warfare: A Strategy for Peace...The Decisive Edge in War, (Washington, D.C: Undated), 13.
- ⁹ United States, A National Security Strategy for a New Century, (Washington, D.C.: December 1999), 1.
- ¹⁰ Christopher J. Lamb, "Perspectives on Emerging SOF Roles and Missions: The View from the Office of the Secretary of Defense," in Roles and Missions of SOF in the Aftermath of the Cold War ed. Richard H. Schultz, Jr., Robert L. Pfaltzgraff, Jr., and W. Bradley Stock (Undated), 201.
- ¹¹ SOF Posture Statement 1998, 1.
- ¹² Lamb, 206.
- ¹³ SOCOM Information Operations (IO) Policy, 7.
- ¹⁴ SOCOM Pub 1, 2-22.
- ¹⁵ SOF Posture Statement 1998, p. 10.
- ¹⁶ General Hugh H. Shelton, "Special Operations Forces: Looking Ahead," Special Warfare, Spring 1997, 6.

Glossary

All definitions from Joint Pub 1-02 (as amended through 6 April 1999) unless otherwise noted.

Air Force special operations forces--Those active and reserve component Air Force forces designated by the Secretary of Defense that are specifically organized, trained, and equipped to conduct and support special operations. Also called **AFSOF**.

Army special operations forces--Those active and reserve component Army forces designated by the Secretary of Defense that are specifically organized, trained, and equipped to conduct and support special operations. Also called **ARSOF**.

Antiterrorism--Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces. Also called **AT**.

Civil affairs--The activities of a commander that establish, maintain, influence, or exploit relations between military forces and civil authorities, both governmental and nongovernmental, and the civilian populace in a friendly, neutral, or hostile area of operations in order to facilitate military operations and consolidate operational objectives. Civil affairs may include performance by military forces of activities and functions normally the responsibility of local government. These activities may occur prior to, during, or subsequent to other military actions. They may also occur, if directed, in the absence of other military operations. Also called **CA**.

Clandestine operation--An operation sponsored or conducted by governmental departments or agencies in such a way as to assure secrecy or concealment. A clandestine operation differs from a covert operation in that emphasis is placed on concealment of the operation rather than on concealment of identity of sponsor. In special operations, an activity may be both covert and clandestine and may focus equally on operational considerations and intelligence-related activities.

Coalition Support -- Improves the interaction of coalition partners and U.S. military forces. It includes training coalition partners on tactics and techniques, providing communications to integrate them into the coalition command and intelligence structure, and establishing liaison to coordinate for combat support and combat service support. (SOCOM Pub 1, p. 3-4)

Combatting terrorism--Actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts) and counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism), taken to oppose terrorism throughout the entire threat spectrum.

Command and control warfare--The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction,

mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and control warfare is an application of information operations in military operations. Also called **C2W**. C2W is both offensive and defensive: a. **C2-attack**. Prevent effective C2 of adversary forces by denying information to, influencing, degrading, or destroying the adversary C2 system. b. **C2-protect**. Maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C2 system.

Computer network attack--Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Also called **CNA**.

Counterdrug--Those active measures taken to detect, monitor, and counter the production, trafficking, and use of illegal drugs. Also called **CD**.

Countermine activities – attempts to reduce or eliminate the threat to noncombatants and friendly military forces posed by mines, booby traps, and other explosive devices. Countermine activity consists of demining and mine awareness. (From SOCOM Pub 1, p. 3-5)

Counterproliferation – Actions taken to locate, identify, seize, destroy, render safe, transport, capture, or recover weapons of mass destruction (WMD). (SOCOM Pub 1, p. 3-3)

Counterterrorism--Offensive measures taken to prevent, deter, and respond to terrorism. Also called **CT**.

Covert operation--An operation that is so planned and executed as to conceal the identity of or permit plausible denial by the sponsor. A covert operation differs from a clandestine operation in that emphasis is placed on concealment of identity of sponsor rather than on concealment of the operation.

Defensive information operations--The integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend information and information systems. Defensive information operations are conducted through information assurance, physical security, operations security, counter-deception, counter-psychological operations, counterintelligence, electronic warfare, and special information operations. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes.

Direct Action--Short-duration strikes and other small-scale offensive actions by special operations forces or special operations capable units to seize, destroy, capture, recover, or inflict damage on designated personnel or materiel. In the conduct of these operations,

special operations forces or special operations capable units may employ raid, ambush, or direct assault tactics; emplace mines and other munitions; conduct standoff attacks by fire from air, ground, or maritime platforms; provide terminal guidance for precision-guided munitions; conduct independent sabotage; and conduct anti-ship operations. Also called **DA**.

Electronic warfare--Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called **EW**. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support. **A. Electronic Attack.** That division of electronic warfare involving the use of electromagnetic, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. EA includes: 1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams). Also called **EA**. **B. Electronic Protection.** That division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. Also called **EP**. **C. Electronic Warfare Support.** That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition. Thus, electronic warfare support provides information required for immediate decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Also called **ES**. Electronic warfare support data can be used to produce signals intelligence, both communications intelligence, and electronics intelligence.

Foreign internal defense--Participation by civilian and military agencies of a government in any of the action programs taken by another government to free and protect its society from subversion, lawlessness, and insurgency. Also called **FID**.

Humanitarian assistance--Programs conducted to relieve or reduce the results of natural or manmade disasters or other endemic conditions such as human pain, disease, hunger, or privation that might present a serious threat to life or that can result in great damage to or loss of property. Humanitarian assistance provided by US forces is limited in scope and duration. The assistance provided is designed to supplement or complement the efforts of the host nation civil authorities or agencies that may have the primary responsibility for providing humanitarian assistance. Also called **HA**.

Information warfare--Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. Also called **IW**.

Information operations--Actions taken to affect adversary information and information systems while defending one's own information and information systems. Also called **IO**.

Military deception--Actions executed to deliberately mislead adversary military decisionmakers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.

Naval special warfare--A designated naval warfare specialty which conducts operations in the coastal, riverine, and maritime environments. Naval special warfare emphasizes small, flexible, mobile units operating under, on, and from the sea. These operations are characterized by stealth, speed, and precise, violent application of force. Also called **NSW**.

Naval special warfare forces--Those Active and Reserve component Navy forces designated by the Secretary of Defense that are specifically organized, trained, and equipped to support special operations. Also called **NSW forces** or **NAVSO**.

Offensive information operations--The integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decisionmakers to achieve or promote specific objectives. These capabilities and activities include, but are not limited to, operations security, military deception, psychological operations, electronic warfare, physical attack and/or destruction, and special information operations, and could include computer network attack.

Psychological operations--Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. Also called **PSYOP**.

Search and rescue--The use of aircraft, surface craft, submarines, specialized rescue teams, and equipment to search for and rescue personnel in distress on land or at sea. (DOD) Also called **SAR**.

Security assistance--Group of programs authorized by the Foreign Assistance Act of 1961, as amended, and the Arms Export Control Act of 1976, as amended, or other related statutes by which the United States provides defense articles, military training, and other defense-related services, by grant, loan, credit, or cash sales in furtherance of national policies and objectives.

Special activities--Activities conducted in support of national foreign policy objectives. Planned and executed so that the role of the US Government is not apparent or acknowledged publicly. They are also functions in support of such activities but are not intended to influence United States political processes, public opinion, policies, or media

and do not include diplomatic activities or the collection and production of intelligence or related support functions.

Special forces--US Army forces organized, trained, and equipped specifically to conduct special operations. Special forces have five primary missions: unconventional warfare, foreign internal defense, direct action, special reconnaissance, and counterterrorism. Counterterrorism is a special mission for specially organized, trained, and equipped Special Forces units designated in theater contingency plans. Also called **SF**.

Special operations--Operations conducted by specially organized, trained, and equipped military and paramilitary forces to achieve military, political, economic, or informational objectives by unconventional military means in hostile, denied, or politically sensitive areas. These operations are conducted across the full range of military operations, independently or in coordination with operations of conventional, non-special operations forces. Political-military considerations frequently shape special operations, requiring clandestine, covert, or low visibility techniques and oversight at the national level. Special operations differ from conventional operations in degree of physical and political risk, operational techniques, mode of employment, independence from friendly support, and dependence on detailed operational intelligence and indigenous assets. Also called **SO**.

Special operations command--A subordinate unified or other joint command established by a joint force commander to plan, coordinate, conduct, and support joint special operations within the joint force commander's assigned operational area. Also called **SOC**.

Special operations forces--Those active and reserve component forces of the military Services designated by the Secretary of Defense and specifically organized, trained, and equipped to conduct and support special operations. Also called **SOF**.

Special operations-peculiar--Equipment, material, supplies, and services required for special operations mission support for which there is no broad conventional force requirement. This includes standard items used by other DOD forces but modified for special operations forces (SOF); items initially designed for, or used by, SOF until adapted for use as Service-common by other DOD forces; and items approved by the Commander in Chief, US Special Operations Command (USCINCSOC) as critically urgent for the immediate accomplishment of a special operations mission but not normally procured by USCINCSOC. Also called **SO-peculiar**.

Special reconnaissance--Reconnaissance and surveillance actions conducted by special operations forces to obtain or verify, by visual observation or other collection methods, information concerning the capabilities, intentions, and activities of an actual or potential enemy or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area. It includes target acquisition, area assessment, and post-strike reconnaissance. Also called **SR**.

Unconventional warfare--A broad spectrum of military and paramilitary operations, normally of long duration, predominantly conducted by indigenous or surrogate forces who are organized, trained, equipped, supported, and directed in varying degrees by an external source. It includes guerrilla warfare and other direct offensive, low visibility, covert, or clandestine operations, as well as the indirect activities of subversion, sabotage, intelligence activities, and evasion and escape. Also called **UW**.

Bibliography

Department of Defense. United States Special Operations Forces: Posture Statement 1998. Washington, D.C.: Department of Defense (OSD-SO/LIC), 1998.

Marquis, Susan L. Unconventional Warfare: Rebuilding U.S. Special Operations Forces. Washington, D.C.: Brookings Institution, 1997.

Lamb, Christopher J. "Perspectives on Emerging SOF Roles and Missions: The View from the Office of the Secretary of Defense" in Roles and Missions of SOF in the Aftermath of the Cold War. ed. Richard H. Schultz, Jr., Robert L. Pfaltzgraff, Jr., and W. Bradley Stock (Undated).

Shelton, General Hugh H. "Special Operations Forces: Looking Ahead." Special Warfare, Spring 1997, 2-11.

United States. A National Security Strategy for a New Century. Washington, D.C.: December 1999.

U.S. Joint Chiefs of Staff. Information Warfare: A Strategy for Peace... The Decisive Edge in War. Washington, D.C: Undated.

U.S. Special Operations Command. Special Operations in Peace and War (SOCOM Pub 1). Washington, D.C.: January 25, 1996.