NAVAL WAR COLLEGE
Newport, R.I.

INFORMATION OPERATIONS AND THE LAW OF PERFIDY

by

Gregory J. O'Brien
CDR, JAGC, USN

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.

18 May 2001

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

20011018 065

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): INFORMATION OPERATIONS AND THE LAW OF PERFIDY (UNCLASSIFIED)

9. Personal Authors: Commander Gregory J. O'Brien, JAGC, USN

10.Type of Report: FINAL	**11. Date of Report**: 18 MAY 2001

12.Page Count: 25 **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:

Information operations, Law of armed conflict, perfidy, ruses of war, deception operations, psychological operations, Principles of war, Hague Regulations, Geneva Protocol I, Operational factors

15.Abstract: The Department of Defense (DOD) Office of General Counsel concluded in an assessment of international law and information operations (IO) that using computer "morphing" techniques of an enemy leader to falsely broadcast that an armistice or cease-fire agreement had been signed would be a war crime under the law of perfidy.

The law of perfidy prohibits IO that would invite the confidence of the enemy to lead him to believe that he is entitled to, or obliged to accord, protection under the rules of international law applicable in armed conflict with the intent to betray that confidence. This standard is flexible, and deception and psychological operations being planned or executed now with IO methods will not be precluded by the General Counsel assessment described above.

16.Distribution / Availability of Abstract:	**Unclassified**	**Same As Rpt**	**DTIC Users**
	X		

17.Abstract Security Classification: UNCLASSIFIED

18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

19.Telephone: 841-6461	**20.Office Symbol**: C

Security Classification of This Page Unclassified

Abstract

INFORMATION OPERATIONS AND THE LAW OF PERFIDY

In 1999, the Department of Defense (DOD) Office of General Counsel concluded in an assessment of international law and information operations (IO) that using computer "morphing" techniques of an enemy leader to falsely broadcast that an armistice or cease-fire agreement had been signed would be a war crime under the law of perfidy, a principle of the law of armed conflict that proscribes the use of treacherous means to kill, injure or capture an adversary. This assessment was widely viewed as a severe limitation on the use of any such morphing techniques to conduct deception or psychological operations.

Such techniques could be a very effective tool for a commander to confuse and demoralize an enemy. The law of perfidy prohibits IO that would invite the confidence of the enemy to lead him to believe that he is entitled to, or obliged to accord, protection under the rules of international law applicable in armed conflict with the intent to betray that confidence. This standard is flexible, and commanders will find that deception and psychological operations being planned or executed now with IO methods will not be precluded by the General Counsel assessment described above.

Information Operations and the Law of Perfidy

. . . War is thus an act of force to compel our enemy to do our will[.] Attached to force are certain self-imposed, imperceptible limitations hardly worth mentioning, known as international law and custom, but they scarcely weaken it. Clausewitz.[i]

To subdue the enemy without fighting is the acme of skill. . . What is of supreme importance in war is to attack the enemy's strategy. Sun Tzu[ii]

Introduction

Imagine the following scenario -- shortly after nightfall one night during NATO's air operations in the Federal Republic of Yugoslavia (FRY) in the spring of 1999, regularly scheduled broadcasts on FRY state television are interrupted with an image of a tired and deflated President Slobodan Milosevic. He is seated at a desk, and behind him are the FRY and Serbian flags. With dark rings under his eyes, he looks directly into the camera, his face beamed into thousands of homes throughout the country. Simultaneously, radio broadcasts in thousands of other FRY homes are interrupted because of the important message to be delivered by President Milosevic.

In a quavering and tired voice, Milosevic recounts the unending bombing his country has endured for the preceding 7 days. He describes the damage done by NATO bombing on his nation's infrastructure and the devastating losses imposed on the FRY military and security forces. He paints a very bleak picture of the situation. Pausing for effect, Milosevic

states that he does not believe the FRY can continue to resist indefinitely against the NATO onslaught and that, in his considered view, the long term interests of the FRY may require that their country submit to the will of the international community. With this in mind, he continues in his sonorous monotone, he will be issuing "appropriate instructions" to his VJ military and MUP security force commanders in Kosovo. Milosevic intones the FRY citizenry to keep him in their prayers and promises to keep the citizens abreast of the "difficult" decisions he must soon make. He concludes his message with a lackluster exhortation that the Serbian spirit will never be fully defeated.

With that, regular television and radio broadcasts resume in thousands of bewildered homes and government offices in the FRY. Meanwhile, high overhead, CAPT Jim "the Producer" Fitzsimonds, Chief of the Information Operations cell on the staff of Joint Task Force Noble Anvil, turns off the Commando Solo broadcast switch in the EC-130E piloted by LtCol Joe "Crazy Legs" Dill, and their mission concludes with a safe return to base. Almost immediately, the confusion wrought by the bogus broadcast leads to mass desertions in the FRY military and security forces, public support for Milosevic quickly plummets and erodes and, within days, the FRY formally capitulates to the demands of the international community.

The major operation that actually took nearly three months to complete is thus completed in less than two weeks at a fraction of the loss in lives and the costs that were produced by Operation Allied Force.

This scenario highlights the potential importance and value of information operations (IO) in a major operation. The employment of IO to affect an adversary's information can yield a tremendous advantage to U.S. military forces during times of crisis and conflict.[iii] A key principle of joint IO doctrine, as reflected in the scenario above, is that human decision making processes are the ultimate target for offensive IO.[iv] Offensive IO can be conducted across the spectrum of conflict and at all levels of conflict, particularly at the strategic level.[v] Offensive IO at the strategic level seek to engage adversary leadership to deter crisis and end hostilities once they occur, while minimizing potentially devastating social, economic, and political effects normally associated with conventional military operations.[vi] Such IO continue to increase in importance in the post Cold-war era.[vii]

While the potential of IO as a significant part of a joint force commander's deliberate and crisis planning processes appears to be unbounded,[viii] there are some equally significant considerations of international law for which a

commander must take account before including particular types of IO in a selected course of action.

As IO exploded in the late 1990's, many planning and legal staffs found themselves unsure of the full range of the nature of the legal issues created by new IO technologies and capabilities. The Department of Defense General Counsel undertook to assess the international legal issues in information operations. In 1999, in a white paper possibly spurred by Operations Allied Force/Noble Anvil to a conclusion more quick than initially intended, DOD/GC identified the more salient issues of concern and, to the most practicable extent, assessed the application of available law to those issues.[ix]

Part of the DOD/GC white paper examined the application of the law of armed conflict to information operations. Part of the law of armed conflict, the concept of perfidy, prohibits the use of treacherous or dishonorable means in armed conflict to kill, injure or capture an enemy.[x] An example of an act of perfidy would be to feign surrender or to broadcast a false report of a cease-fire or armistice in order to kill, injure or capture the enemy.

In assessing this concept, DOD/GC stated in its white paper that, "[although] it might be possible to use computer 'morphing' techniques to create an image of the enemy's chief of state informing his troops that an armistice or cease-fire

agreement had been signed, [i]f false, this would be a war crime."[xi]

This assessment was quickly perceived by some as a flat prohibition on any IO that contemplated the use of such manufactured images or signals in the course of conducting deception operations.[xii] While the General Counsel undoubtedly did not intend in its white paper to exhaustively analyze this part of the law of armed conflict and its application to IO, the exact contours of this conclusion seem not to be clear. For example, can an IO such as the one described above be permissible? what affect does this assessment and the law of perfidy in general have on other information operations that seek to exploit enemy information systems? is the ability to digitally deceive an enemy so new and separate from prior methods of conducting psychological or deception operations that it is insusceptible to regulation by the traditional law of perfidy? in short, where is the line between a permitted act of deception and a prohibited act of perfidy?

The law of perfidy is more flexible than the standard suggested in the DOD/GC paper, and commanders will find that deception and psychological operations being planned or executed now with IO methods will not be precluded by the General Counsel assessment. This paper will analyze in more detail the law of perfidy and its application to information

operations. The purpose in doing so will be to clarify the points that a commander must consider in incorporating a particular IO into an operations plan.

The Law of Perfidy

The law of armed conflict permits deceiving the enemy through strategems and ruses of war intended to mislead him, to deter him from taking action, or to induce him to act recklessly, provided the ruses do not violate rules of international law applicable to armed conflict.[xiii] One of the three primary customary principles of the law of armed conflict[xiv] is the principle of chivalry. This principle provides that dishonorable (or treacherous) means, dishonorable expedients, and dishonorable conduct during armed conflict are forbidden.[xv]

This principle has been incorporated into the law of armed conflict. Article 23(b) of the 1907 Hague Regulations,[xvi] provides that it is forbidden to kill or wound treacherously individuals belonging to the hostile nation or army. Article 23(f) provides further that it is forbidden to make improper use of a flag of truce, of the national flag or of the military insignia and uniform of the enemy, as well as the distinctive badges of the Geneva Convention.[xvii] Article 24 provides, meanwhile, that ruses of war and the employment

of measures necessary for obtaining information about the enemy and the country are considered permissible.[xviii]

The Hague Regulations did not further define the meaning of the term treachery nor how an armed force could improperly use the various items described in Article 23(f). States were thus left to develop through custom and practice the meaning of these terms. After two World Wars and scores of international and internal armed conflicts later, an attempt was made to codify some of these practices.

Article 37(1) of the 1977 Geneva Protocol I[xix] provides that it is prohibited to kill, injure or capture an adversary by resort to perfidy. Further, perfidy was defined as acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence.[xx] Examples of perfidy include the feigning of an intent to negotiate under a flag of truce or of a surrender; the feigning of an incapacitation by wounds or sickness; the feigning of civilian, non-combatant status; and the feigning of protected status by the use of signs, emblems or uniforms of the United Nations or of neutral or other states not parties to the conflict.[xxi]

Article 38 of GP I prohibits the improper use of the distinctive emblem of the red cross, red crescent or red lion

and sun or of other emblems, signs or signals provided for by the Conventions or by this Protocol and to misuse deliberately in an armed conflict other internationally recognized protective emblems, signs or signals, including the flag of truce, and the protective emblem of cultural property, and the unauthorized use of the distinctive emblem of the United Nations.[xxii]

Finally, article 39 of GP I prohibits the use in an armed conflict of the flags or military emblems, insignia, or uniforms of neutral or other states not parties to the conflict; or the use of flags or military emblems, insignia, or uniforms of adverse parties while engaging in attacks or in order to shield, favor, protect or impede military operations.[xxiii]

Article 37(2) of GP I continues the Hague rules formulation that permits ruses but forbids perfidy. Article 37(2) provides that ruses of war are not prohibited. Ruses are acts which are intended to mislead an adversary or to induce him to act recklessly but which infringe no rule of international law applicable in armed conflict and which are not perfidious because they do not invite the confidence of an adversary with respect to protection under that law. Examples of such ruses are the use of camouflage, decoys, mock operations and misinformation.[xxiv]

The provisions in the Hague Regulations and in GP I provide the line between permissible acts of ruse or deception and prohibited acts of perfidy.[xxv]

Impact on traditional deception operations

Each of the military departments of the U.S. armed forces has discussed how the law of perfidy affects operations carried out at sea, on land, and in the air.[xxvi]

As reflected in the Hague Regulations and GP I, the use of a ruse is limited if the ruse invites the enemy's confidence with respect to a protected status. Thus, for example, while camouflage is permitted, a naval commander cannot disguise his ship as a hospital vessel, a ground commander cannot use the "PW" symbol to mark off a fake prisoner of war compound from which to attack the enemy, and an air commander cannot mark his aircraft with the emblem of the United Nations or falsely transmit an air distress signal in order to kill, injure or capture the enemy. Each of these examples implicates a protected status under the law of armed conflict which obligates the enemy to honor.

Similarly, the limitations on use of another's flags, insignia or uniforms affect military operations. With respect to neutral or enemy flags, insignia or uniforms, at sea, a belligerent warship may fly false colors or be disguised to

deceive the enemy into believing the vessel is neutral or other than an opposing warship. The warship must, though, first show her true colors before engaging the enemy; it is prohibited to go into action without showing true colors.[xxvii]

Aircraft may not enter combat with false or deceptive markings. This suggests that false aircraft markings may be employed prior to or after combat, but as a practical matter, those points may be too difficult to discern to be of any operational or tactical benefit to a commander.[xxviii]

On the ground, use of neutral flags, insignia or uniforms is never permitted. Obviously, this is counter to the rule for use of neutrals emblems in naval operations. The rationale for the rule for land warfare is that use of neutral emblems for any purpose by a belligerent would put at too great a risk actual neutrals and might also risk unnecessary escalation in an armed conflict.[xxix] Use of enemy flags, insignia or uniforms, meanwhile, is prohibited in combat. That is, prior to or after an armed engagement, use of such enemy items to deceive the enemy is permitted.[xxx]

A traditional way to signify an intention to surrender, and to acquire protection from being further targeted by an enemy, is by raising a white flag. Use of the white flag by a belligerent to gain a military advantage over the opposing belligerent is unlawful.[xxxi] Conversely, it is unlawful to

target enemy forces that in good faith clearly convey a timely offer of surrender, or, rather, demonstrate a manifest intent to surrender.[xxxii] Parenthetically, the use of a white flag is not in itself an indication of surrender.[xxxiii] It should be noted that one's forces are not required to cease firing when a white flag is raised. Such a cease fire is accomplished only after the opposing unit itself ceases firing and a representative of the opposing commander (a "parliamentaire" under the Hague Regulations) is sent forward to discuss cease fire terms.[xxxiv]

Impact on IO-based deception operations

Certainly, IO capabilities possessed by U.S. forces and an adversary provide fertile opportunities for executing effective deception operations. From the perspective of psychological operations, the objective is to manage perception, thereby contributing to the achievement of larger objectives.[xxxv] Typical military objectives include the creation of uncertainty and ambiguity, the countering of enemy propaganda, the encouragement of disaffection, and the focusing on specific subjects to degrade operational capability.[xxxvi] IO in support of psychological operations will use methods, for example, to infiltrate enemy communications systems such as television or radio networks and Internet or

local/wide area network systems. Techniques that duplicate adversary voices (by intercept, modification or retransmission) may not stand up to detailed scrutiny, but may be sufficient to obtain the desired objectives of bias, overload or insensitivity.[xxxvii]

From the standpoint of operational deception, IO in netwar expand the targets to include society at large, and have as their objective the inducing of behavior that contributes to the operational mission.[xxxviii] Two categories of misconception are pursued in deception operations: ambiguity to create uncertainty about the truth, and misdirection to create uncertainty about a falsehood.[xxxix] IO methods here could include infiltrating enemy communication systems to spread false messages to field commanders or through emitting deceptive signals to simulate enemy forces or to create virtual forces where none actually exist.

While these new methods of deceiving or influencing the enemy are being developed and employed, they are not so significantly different in their nature or effect that a departure from the principles of established law is required. In fact, it is possible to use the existing framework of analysis to distinguish ruse from perfidy in proposed IO.

The first point of analysis would be to examine whether an IO proposes use of a protective sign, signal or symbol. In

addition to the protective emblems and insignia set forth in GP I, other examples of such emblems or signals would include those of small coastal rescue craft, and transports (whether operating on land, water or in the air) on humanitarian missions, carrying civilian passengers, carrying cultural property under special protection, or guaranteed safe conduct by prior agreement among the parties to an armed conflict.[xl] Thus, IO to transmit the IFF code of a medical aircraft as a way of creating a safe passage corridor through an enemy air defense network would be unlawful. Likewise, manipulating an enemy surface contact radar to depict that your warship is apparently a vessel known to be under charter to the United Nations is not permissible.

One writer has questioned whether efforts to mask one's infrared emissions, thus appearing through an enemy's sensors to be giving off the body heat of a dead or dying soldier, would be perfidious.[xli] If that were the purpose and intent of masking one's infared picture, then doing so in order to kill, injure or capture the enemy would be perfidious. It is highly unlikely, though, that such a capability would be employed for such a narrowly limited purpose. If the real purpose of this capability is to evade detection, as opposed to simulating a wounded or killed status, then the law of perfidy would not preclude its use in this fashion.

The next line of analysis would be to assess whether an IO involves the simulation of a neutral or enemy. The use of another's virtual uniforms or insignia may become prominent in future operations conducted in a network-centric environment. The modern battlefield often is not physical.[xlii] Rather, forces use a combination of electronic sensors worn by their personnel or placed on their weapons or platforms. The sensors provide signals or emissions that are displayed on a video screen on which a battlespace is monitored.[xliii]

One way to exploit this technology might be to "wear" enemy sensors to look like a friendly force or to "steal" that signal and create virtual forces kilometers away to secure an advantage to attack a force commander. This tactic would not be prohibited by the proscription on not wearing enemy uniforms in combat. The prohibition in GP I refers only to concrete visual objects, including the national symbols marked on uniforms, military vehicles and aircraft. Thus, the prohibition does not apply to the ruse of using the adversary's electronic or signals emissions, codes, passwords and countersigns to aid military operations.[xliv]

This assessment leaves open, though, whether ground forces could use the signals of a neutral country or simulate the presence of neutral forces in order to secure an advantage over the enemy. On one hand, it would not involve the use of

concrete objects but only the emissions or signals that would simulate a neutral force. On the other hand, the risk of escalation of armed conflict to neutral countries in the mistaken belief that that neutral country had abandoned its neutrality that underpins GP I Article 39(1) exists here. On this basis, a sensible approach would be to conclude that it would be improper, if not unlawful, to do so.

Thus, we come to the point of assessing whether the scenario initially outlined above comports with the law of perfidy. The intent and substance of the morphed broadcast of President Milosevic is to sow confusion and undermine the morale of the Yugoslav citizenry and their support of Milosevic, encourage mass desertions of VJ and MUP personnel and, ideally, instigate a grass roots effort to force Milosevic from office. Variations of this morphed communication can be made at the tactical and operational levels as well so that VJ and MUP personnel in Kosovo receive similarly dismal reports from their commanders. There is nothing in the morphed message that conveys a manifest intent to surrender to NATO; the allusions to what Milosevic feels he must do are purposely phrased conditionally, so that the message he delivers is intentionally ambiguous. As such, there has been no false broadcast of an armistice or ceasefire. Accordingly, the scenario comports with the law of

perfidy. Policy-makers may determine that it would be unwise to employ such an IO, but their ground for doing so would be policy-based and not because of a potential violation of the law of armed conflict.

Conclusion

Much of the literature about the legal implications of IO has dealt with the broader issues concerning when certain IO can be deemed a use of force or an armed attack under the U.N. Charter or customary international law. It is important to clarify these points as IO capabilities become more defined and are actually used in conducting military operations. It is equally important, though, to be mindful of how the other parts of the law of armed conflict can affect IO. Since deception and psychological operations are a critical tool for a commander, the law concerning perfidy will need to be considered as such operations are developed. Planned properly within the deliberate or crisis planning process, these operations can be effective enabling and multiplying factors with potentially strategic benefits.

[i] Carl Clausewitz, *On War*, Michael Howard & Peter Paret, ed., (Princeton: Princeton University Press 1976), 75.

[ii] Sun Tzu, *The Art of War*, Samuel B. Griffith, ed., (Oxford: University Press 1963), 77.

[iii] Joint Chiefs of Staff, *Joint Doctrine for Information Operations,* Joint Publication 3-13 (Washington, DC: 9 October 1998), II-1.

[iv] Joint Pub. 3-13, II-1.

[v] Joint Pub. 3-13, II-10-11.

[vi] Joint Pub. 3-13, II-11.

[vii] Joint Pub. 3-13, II-11 (emphasis added).

[viii] Representative accounts of the importance of IO in military operations are reflected in Berkowitz, "War Logs On," *Foreign Affairs*, 79 (May/June 2000), 8-12; Wall, "USAF Expands Infowar Arsenal," *Aviation Week & Space Technology* 151 (15 November 1999), 102-103; "Asia: Nerd World War," *The Economist* 353 (30 October 1999), 46.

[ix] Department of Defense Office of General Counsel, *An Assessment of International Legal Issues in Information Operations*, (Washington DC 2d ed. November 1999).

[x] DOD/GC, 6.

[xi] DOD/GC, 8-9.

[xii] E.g., Daniel Verton, "Pentagon Labels Computer Morphing A War Crime," CNN.com, <http://www.cnn.com/TECH/computing/9911/16/computer.war.crimes.idg>, [April 23, 2001]; "Pentagon Ponders Legality of Cyber Weapons," <http://www.apbnews.com/newscenter/internetcrime/1999/11/09/pentagon1109_01.html>, [April 23, 2001]; "Information Warfare," <http://www.infowar.com/mil_c4i_110999b_j.shtml>, [accessed April 23, 2001].

[xiii] A.R. Thomas and J.C. Duncan, ed., *International Law Studies, Vol. 73, Annotated Supplement to the Commander's Handbook on the Law of Naval Operations* (Newport, R.I.: Naval War College Press 1999), 507.

[xiv] The other two principles are necessity and humanity. Adam Roberts and Richard Guelff, ed., *Documents on the Law of War* (2d ed.)(Oxford: Clarendon Press 1994), 5.

[xv] Roberts and Guelff, 5.

[xvi] The Hague Regulations annexed to the 1907 Hague Convention IV Respecting the Laws and Customs of War on Land (the Hague Regulations, or HR) reprinted in Roberts and Guelff, 39-59.

[xvii] Roberts and Guelff, 52-53. The Geneva Convention referred to in Article 23(f) was the Geneva Convention of 1874, which provided for the protected status of army medical personnel and vehicles of any belligerent bearing a red cross on a white background, an emblem whose significance has survived to the present time. Bothe, Partsch & Solf, *New Rules for Victims of Armed Conflict, Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949*, (Boston: Martinus Nijhoff Publishers 1982).

[xviii] Roberts and Guelff, 53.

[xix] Protocol I Additional to the Geneva Conventions of 1949 Relating to the Protection of Victims of International Armed Conflicts (Geneva Protocol I, or GP I), reprinted in Roberts and Guelff, 387-446.

[xx] GP I.

[xxi] GP I.

[xxii] GP I.

[xxiii] GP I.

[xxiv] GP I.

[xxv] Thomas Wingfield, "Legal Aspects of Information Operations in Space," *U.S. Air Force Academy Journal of Legal Studies*, 9 (1998/1999), 138; Mary T. Hall, "False Colors and Dummy Ships: The Use of Ruse in Naval Warfare," *Naval War College Review*, (Summer 1989), 53.

[xxvi] U.S. Navy, *The Commander's Handbook on the Law of Naval Operations*, Naval Warfare Publication (NWP) 1-14M (Washington, DC); U.S. Army, *The Law of Land Warfare*, Field Manual (FM) 27-10 (Washington, DC); U.S. Air Force, *International Law - The Conduct of Armed Conflict and Air Operations*, Air Force Pamphlet (AFP) 110-31 (Washington, DC). For armed conflict at sea, permissible ruses include such deceptions as camouflage, deceptive lighting, dummy ships and other armament, decoys, simulated forces, feigned attacks and withdrawals, ambushes, false intelligence information, electronic deceptions, and use of enemy codes, passwords, and countersigns. On land, other permissible deceptions include traps, mock operations, feigned retreats or flights; surprise attacks or simulation of quiet and inactivity; use of small units to simulate larger units; use of dummy aircraft, vehicles, airfields, weapons and mines to create a fictitious force; moving landmarks and route markers; pretending to communicate with fictitious forces or reinforcements; deceptive supply movements; and allowing false messages to fall into enemy hands. In addition to the foregoing examples, the following air-based ruses are permissible: use of aircraft decoys; staging air combats between two friendly aircraft to induce an enemy aircraft to join; imitating enemy signals; use of flares or fires away from a target area.

[xxvii] Thomas and Duncan, 511.

[xxviii] AFP 110-31, para. 7-4.

[xxix] Thomas and Duncan, 512, note 10.

[xxx] FM 27-10, para. 54. Article 39(2) of GP I also prohibits the use of enemy emblems in military operations other than attack engagements, but the United States does not support that prohibition. Thomas and Duncan, note 2, p. 508.

[xxxi] Thomas and Duncan, 510.

[xxxii] Thomas and Duncan, 407.

[xxxiii] Robertson, "The Obligation to Accept Surrender," *International Law Studies 1995: Readings on International Law from the Naval War College Review 1978-1994*, John Norton Moore and Robert F. Turner, ed. (Newport, R.I.: Naval War College Press 1995), 548-549. RADM Robertson notes that the methods for displaying an intent to surrender differ among the arms of combat: at sea, a warship indicates its intent to surrender by striking her colors, by hoisting a white flag, by surfacing (in the case of submarines), by stopping engines and responding to attacker's signals, or by taking to lifeboats. Surrender in aircraft is generally not offered because of the impossibility of verifying the true status of a seemingly disabled aircraft and the inability to enforce surrender. On land, there are varying "traditional" methods to signify an intent to surrender: raising a white flag, throwing down arms, or raising hands. Again, the standard for purposes of the law of perfidy is a manifest intent to surrender is typically what provides the protected status.

[xxxiv] Robertson, 510.

[xxxv] Edward Waltz, *Information Warfare Principles and Operations*, (Boston: Artech House 1998), 209.

[xxxvi] Waltz, 209.

[xxxvii] Waltz, 212.

[xxxviii] Waltz, 211.

[xxxix] Waltz, 211.

[xl] This list is taken from paragraph 110 of International Institute of Humanitarian Law, *The San Remo Manual on International Law Applicable to Armed Conflicts at Sea*, Louise Doswald-Beck, ed. (Cambridge: University Press 1995), 184-185. These examples are in addition to those protected persons and organizations identified in the Geneva Conventions and GP I -- for example, medical aircraft, sick and wounded, prisoners of war.

[xli] William Church, "Information Warfare," *International Review of the Red Cross*, 837 (31 March 2000), 205-216.

[xlii] The San Remo Manual discusses the relevance of any law of perfidy in this modern age where various means of deception are used in a technological battlespace. Such a discussion, though, logically leads to an untenable choice of outlawing any form of camouflage or other means of deception. In this respect, the interests of preserving an effective means of force protection and mission accomplishment could be said to outweigh other interests.

[xliii] San Remo Manual.

[xliv] Bothe, Partsch and Solf, 214.

Bibliography

Aldrich, Richard W., "The International Legal Implications of Information Warfare," Airpower Journal (Fall 1996): 99-110.

"Asia: Nerd World War," The Economist, 353 (30 October 1999): 46.

Associated Press, "Pentagon Ponders Legality of Cyber Weapons," The Associated Press. 9 November 1999. APBNews.com (23 April 2001).

Bayles, William J., "The Ethics of Computer Network Attack," Parameters. Spring 2001. <http://www.proquest.umi.com> [5 April 2001].

Berkowitz, Bruce D., "War Logs On," Foreign Affairs, 79(May/June 2000): 8-12.

Bothe, Michael, Karl Joseph Partsch, and Waldemar Solf, New Rules for Victims of Armed Conflicts, Commentary of the Two 1977 Protocols Additional to the Geneva Conventions of 1949 (Boston: Martinus Nijhoff Publishers, 1982), 201-215.

Burns, Robert, "Information Warfare," Military and C4I. 9 November 1999. <http://www.infowar.com/mil_c4i/99/mil_c4I_110999b_j.s html> [23 April 2001].

Coppernoll, Margaret-Anne, "The Nonlethal Weapons Debate," Naval War College Review, 52 (Spring 1999): 112-131.

Church, William, "Information Warfare," International Review of the Red Cross, 837 (31 March 2000): 205-216.

Greenspan, Morris, The Modern Law of Land Warfare (Berkeley: Univ. of California Press 1959), 318-326.

Hall, Mary T., "False Colors and Dummy Ships: The Use of Ruse in Naval Warfare," Naval War College Review (Summer 1989): 52-62.

International Committee of the Red Cross, Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (Jean Pictet and others, ed.)(Geneva: Martinus Nijhoff Publishers 1987), 429-471.

International Institute of Humanitarian Law, The San Remo Manual on International Law Applicable to Armed Conflicts At Sea (Louise Doswald-Beck, ed.)(Cambridge: University Press 1995), 184-185.

Robertson, Horace B., "The Obligation to Accept Surrender,"

in International Law Studies 1995: Readings on International Law from the Naval War College Review 1978-1994, ed. John Norton Moore and Robert F. Turner (Newport: Naval War College Press 1995), 541-552.

Roberts, Adam and Richard Guelff, Documents on the Law of War (2d ed.)(Oxford: Clarendon Press 1989).

Stanton, John J., "Rules of Cyberwar Baffle U.S. Government Agencies," National Defense, 84 (February 2000): 29-30.

Shulman, Mark W., "Discrimination in the Laws of Information Warfare," Columbia Journal of Transnational Law, 37 (1999) 939-968.

Terry, James P., "Responding to Attacks on Critical Computer Infrastructure: What Targets? What Rules of Engagement?"" Naval Law Review 46 (1999) 170-187.

Thomas, A.R. and James C. Duncan, eds., International Law Studies, Vol. 73, Annotated Supplement to The Commander's Handbook on the Law of Naval Operations (Newport: Naval War College Press 1999).

U.S. Air Force, International Law – The Conduct of Armed Conflict and Air Operations, Air Force Pamphlet 110-31, (Washington, DC).

U.S. Army, The Law of Land Warfare, Field Manual 27-10, (Washington, DC).

U.S. Navy, The Commander's Handbook on the Law of Naval Operations, Naval Warfare Publication 1-14M, (Washington, DC).

U.S. Department of Defense Office of General Counsel, An Assessment of International Legal Issues in Information Operations, (Washington, DC: 2d ed. November 1999).

U.S. Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Pub. 3-13, (Washington, DC: 9 October 1998).

Verton, Daniel, "Pentagon Labels Computer Morphing A Crime," CNN.com, 16 November 1999. CNN.com (23 April 2001).

Wall, Robert, "USAF Expands Infowar Arsenal," Aviation Week and Space Technology, 151 (15 November 1999), 102-103.

Waltz, Edward, Information Warfare Principles and Operations (Boston: Artech House 1998), 209-215.

Wingfield, Thomas C., "Legal Aspects of Offensive Information Operations in Space," U.S. Air Force Academy Journal of Legal Studies, 9 (1998/1999), 121-142.