Information Operations Doctrine and Non-state Conflict: Shaping the Information Environment to Fight Terrorism and Insurgencies

By Norman Emery, MAJ, USA
D.G. Mowles Jr., Maj, USAF
Jason Werchan, Maj, USAF

Editorial Abstract: *A review of the draft JP 3-13, Joint Information Operations, shows that it insufficiently addresses non-state threats such as terrorism and insurgencies. The US is stuck in the paradigm where it uses the construct of winning "hearts and minds" to enable its own success and failing to use it to counter the influence of non-state actors, who essentially operate in a different battlespace. The US military must adapt its traditional approach to warfare in the Physical Environment in order to better combat these threats, which enjoy considerable success in the Information Environment. The authors offer a recommendation for the new JP 3-13 of adapting a two-prong approach of simultaneously attacking non-states threats in the PE while countering prior non-state acts in IE to limit the residual effects of past successes. IO doctrine must show that IO is much more than using the elements of IO, but rather full spectrum capabilities to shape the IE to the US's advantage.*

In Iskandariyah, Iraq, approximately 30 miles south of Baghdad, a bomb explodes at an Iraqi police station, killing 50 Iraqis applying for the new police force. Consistent with standing policy and strategy, US forces respond by conducting operations to seek out and defeat those responsible for the bombings. Often, these forces are successful in finding, engaging, capturing or killing the insurgents who instigated these types of terrorist attacks. However, this traditional attrition-based approach to counter-insurgent operations does not adequately address the secondary effects and overall strategy of the insurgent movement. By attacking the police station, the Iraqi insurgents hoped to achieve their strategic objectives of influencing the Iraqi populace's perceptions of security and safety, contributing to the delay or cancellation of free elections, de-legitimizing an interim Iraqi government, and degrading overall domestic support for US policy in Iraq.

This scenario is characteristic of the overall limitation of US joint information operations (IO) doctrine in addressing a new approach to warfare. Non-state actors such as terrorists and insurgents will likely be the major threat to American national security and its interests for years to come. Since these actors cannot directly confront the US militarily, they must rely on an information advantage to marginalize US capabilities. A variety of high profile terrorist groups over the past decade have demonstrated a sound knowledge and coordinated use of IO. These groups' ability to successfully achieve objectives by shaping their battlespace in the information environment, coupled with their willingness to conduct non traditional warfare, makes them a significant threat to the United States.

Although Joint Publication (JP) 3-13, Joint Doctrine for Information Operations (1998), addresses a traditional IO approach against conventional forces such as China or North Korea, it does not sufficiently consider non-state threats such as terrorists and insurgents. The Joint Staff is currently updating JP 3-13, incorporating the revised Department of Defense (DoD) IO policy (also informally known as the Secretary of Defense's [SECDEF] IO roadmap), dated October 2003. To succeed in the new security environment facing the US, the new JP 3-13 must provide an overall IO approach that attempts to better define and shape operations in the information environment (IE) to enable ultimate victories in the physical environment (PE) against non-state actors.

Joint Combat Camera Photo

Non-state threats, such as terrorists, are oftentimes difficult to identify.

The Current and Future US Security Environment

The US is facing a drastically different security environment than what was present prior to September 11. In the past, potential adversaries confronted the United States with conventional armed forces backed by the industrial capabilities of a traditional nation-state. Today, however, a single non-state actor or terrorist group can attack the nation and create untold destruction.

The President's National Security Strategy (NSS) of the United States has defined a new security environment that includes not only these terrorist organizations, but also the nation-states and organizations that harbor them. "[T]he United States and countries cooperating with us must not allow the terrorists to develop new home bases. Together, we will seek to deny them sanctuary at every turn" (NSS, 2001).

Though terrorism can take many forms in the aftermath of September 11, the United States is primarily concerned with those terrorists who possess a global strike capability, and whose global reach makes them extremely elusive to define or engage. In response to this new security environment, Secretary of Defense (SECDEF) Rumsfeld changed the military strategy in the 2001 Quadrennial Defense Review (QDR) from a 'threat-based' approach to a 'capabilities' approach to better respond to the numerous potential conflicts facing the US By adopting this approach, defense planners can concentrate on how a potential enemy may engage the United States rather than specifically concerning themselves with who that enemy is or where he will attack.

Joint IO Doctrine

> *"Information operations are essential to achieving full spectrum dominance."*
>
> (Joint Vision 2020, 2000, p.28)

Numerous documents provide direction of overall Joint IO strategy, including JP 3-13, Joint Vision (JV) 2010, JV 2020, and the recently published SECDEF's IO Roadmap. JP 3-13 (1998) provides the overarching doctrinal guidance for Joint forces to conduct IO. Given the severe changes undergone in technology and information systems, this publication is currently under draft review and due to be updated soon. JV 2010, published in 1996, develops IO as a component and defines it as "[a]ctions taken to affect adversary information and information systems while defending one's own information and information systems" (Armistead, 2002). JV 2010 gives "a vision for how the United States military will operate in the uncertain future" and achieves the ultimate goal of full spectrum dominance (Armistead, 2002). A key element of full spectrum dominance is the emerging importance of information superiority. JV 2010 states that information superiority will mitigate the impact of the friction and fog of war, advocates ensuring an uninterrupted flow of information and advocates non-traditional actions (Joint Vision 2010, 1996, p. 16). JV 2020 added that "[t]he combined development of proliferation of information technologies will substantially change the conduct of military operations. These changes in the information environment make information superiority a key enabler of the transformation of the operational capabilities of the joint force and the evolution of joint command and control" (Joint Vision 2020, 2000, p. 3).

The SECDEF's October 2003 IO Roadmap provides strategic level IO guidance to support the current security environment defined in the latest QDR and NSS. The draft update of JP 3-13 incorporates the SECDEF's IO Roadmap and a new Department of Defense (DoD) IO definition: "The integrated employment of the specified core capabilities of Electronic Warfare, Computer Network Operations (CNO), PSYOP, Military Deception, and Operations Security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making, while protecting our own" (Joint Publication 3-13 [draft], p. I-6). The SECDEF's IO Roadmap also groups elements of IO in the following capabilities categories:

CORE CAPABILITIES	SUPPORTING CAPABILITIES	RELATED
Electronic Warfare	Information Assurance	Public Affairs
CNO	Physical Security	Civil-Military Operations
Operations Security	Counterintelligence	
Military Deception	Physical Attack	
PSYOP		

Joint Combat Camera Photo

The SECDEF signed the IO Roadmap in October 2003.

Concerns with Current and Draft Joint IO Doctrine

Although current and draft IO doctrine encompasses many aspects of warfare, it is the ability to deal with the new security environment that must be primarily scrutinized. The new definition focuses offensive IO against the adversarial decision-maker, ignoring the fact that there are many valuable targets in the IE that are not critical decision-makers. The 1998 definition of IO was considered "so broad, at once, IO is everything and it is nothing" (Armistead, 2002). The new draft definition limits itself in the application of IO to the listed core capabilities.

Additionally, JP 3-13 poorly defines and applies the concept of information superiority as it would apply to a non-

state actor. Information superiority is an imbalance in one's favor in the information domain with respect to an adversary. The power of superiority in the information domain mandates that the US achieve it as a first priority, even before hostilities begin. However, superior technology and equipment fuels the U.S.'s hubris that it will have information superiority over inferior adversaries. A non-state actor in his environment can decisively possess information superiority and an information advantage because he can see the US forces and remain unseen, and choose when to attack. Therefore, the U.S.'s information superiority can be very finite and fleeting, and its forces must recognize this and take direct and indirect actions to reduce the adversary's information advantage, thereby reducing his operational efficiency. Information superiority in the new security environment must include denying information helpful to a non state actor such as reducing Operations Security (OPSEC) violations or reducing information the population can provide.

Physical Environment versus Information Environment

"The operational target of IW lies in control rather than bloodshed."

-Shen Weiguang, PRC IW theorist
(ed. Neilson, 1997, p. 4)

Nothing is more important when conceptualizing Joint IO doctrine in the new security environment than understanding the relationship between the PE and the IE and how the US should approach IO in these areas against a non state actor. JP 3-0 defines the PE by the dimensions of land, sea, air, and space. Humans live, breathe, and walk in the PE, and see, hear, and touch objects that are real (Earl & Emery, 2003, p.18). Leaders generally conceive and measure gains and losses in the PE by the metrics of terrain, equipment, forces, and engagements. According to JP 3-13 (draft), the IE consists of information that resides in the mind, the physical world, and the electromagnetic spectrum (p. I 2). In the IE, the boundaries are "not limited to the linear battlespace that military commanders conceptualize, [and] activities in the IE often times shape a commander's understanding of the battle and can profoundly impact his decisions in the physical environment" (Earl & Emery, 2003, p. 19). For example, forces providing security to a population is an act in the PE; the population's perception of security is the IE.

Joint Combat Camera Photo

Marines making an impression by kinetic means in the PE.

Joint Combat Camera Photo

An Army spokesman in Iraq disseminating information in the IE.

Military leaders and planners must conceptualize that the domains of the PE and the IE exist in simultaneous yet separate battle-spaces. Non-state actors operate mainly in a the IE to leverage their advantage while state's tend to operate in the PE to achieve their goals. The US must adapt its approach to conflict to maximize its results while diminishing the adversary's.

Another key characteristic of the IE and the PE is to recognize that "wherever human activity occurs physically, such activity takes place simultaneously in the information dimension as well" (Joint Publication 3-13, 1998, p. I-2). This is important in recognizing those residual effects from actions taken in the physical environment that will shape the IE. JP 3-13 (draft) fails to address that there are factors that shape the IE in which military operations are planned and executed, and that success depends on US forces gaining and maintaining information superiority (pp. I-4, I-5). However, previous IO doctrine and US operations have traditionally sought to achieve finite victory in the PE battlespace and ignore the concurrent residual effects in the IE battlespace.

"Military leaders and planners must conceptualize that the domains of the PE and the IE exist in simultaneous yet separate battlespaces."

Current and draft Joint IO doctrine fails to adequately explain and emphasize the conceptual understanding of the IE and the art of its application against the U.S.'s diverse adversaries. The key to preparedness against current and potential security threats such as non-state actors lies in the art of IO, and not just the science. The science of IO can be the application of systems and capabilities to support the goal of affecting the adversary decision-making at a specific moment in time and space, while "art focuses on the fundamental methods and issues associated with synchronization of military effort" in the IE (Joint Publication 3-13 [draft], p. I-10). "Operational art is the use of military forces to achieve a strategic goal through the design, organization, integration and conduct of strategies, campaigns, major operations, and battles" (Joint Publication 3-13 [draft], p. I-10). To fight a non-state actor whose operational actions are planned to achieve strategic goals, the US must operate similarly. US planners must apply the facets of operational art in both the IE and PE. This is recognizing and understanding that there is more to IO than just affecting adversary decision making as proposed in the draft definition, but coordinated military actions to impact the information environment as a whole.

Although JP 3-13 (draft) establishes the conceptual context of the IE and military operations related to it, it fails to address the need to shape that environment as a result of friendly or adversary actions in the PE. The United States enjoys a force advantage over most of its adversaries and therefore seeks objectives and victories in the PE using actions in the IE as an enabler. In contrast, most non-state groups (terrorists, insurgents) who lack military parity, seek to achieve their ultimate objectives by way of success in the IE. They cannot successfully engage a superior force in the PE and are forced to conduct select acts in the PE (e.g. bombings, small scale attacks) to shape the IE (i.e. perceptions). These acts can help an organization achieve its objectives in the IE to ultimately achieve objectives indirectly in the PE. Therefore, a non-state actor recognizing this lack of parity may chose to avoid a decisive fight with US forces and instead select a more advantageous time and location for engagements. Non-state actors will avoid direct confrontation in a state's PE battlespace, but a state actor can beat them by reshaping the non-state's IE.

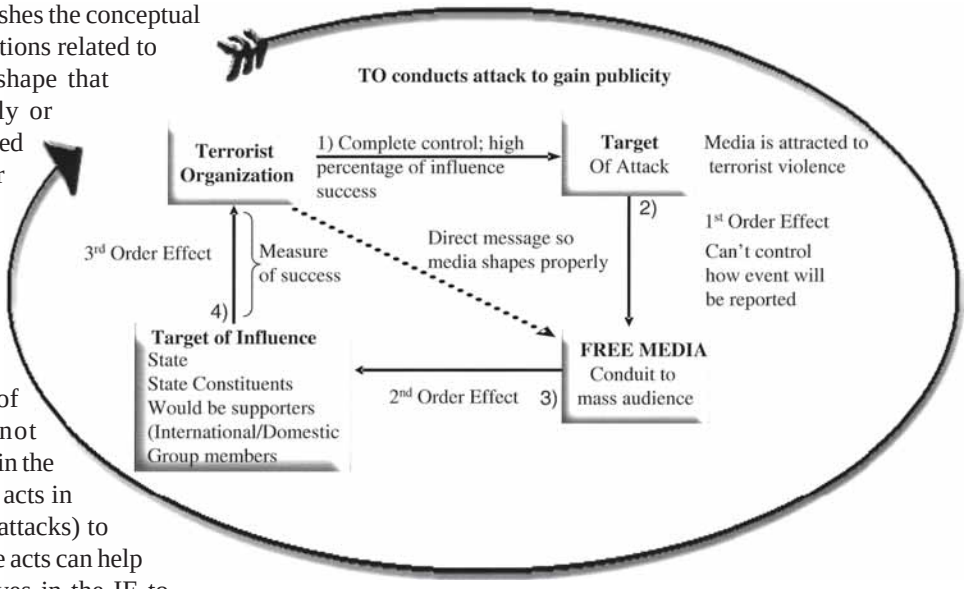

Figure 1. McCormick Influence Process Model.

How the US Forces Pursue Victory

Current doctrine directs US forces to fight for the decisive victory in the PE, while using the IE to support "objectives and reduce costs of war" (Earl & Emery, 2003, p. 44). Although US IO may often impact the adversary's perception or will to fight, the US normally relies on victory in the PE to win the battle (ed. Radvanyi, 1990, p. 121). This is a typical strategy of a military with a force advantage over the majority of its adversaries. Joint doctrine supports this by orienting on affecting adversary decision-making to influence decisions in the U.S.'s favor, and to prevent the adversary influencing US forces. While this approach is adequate for a conventional linear adversary such as Iraq or North Korea, it is inadequate for the non-state threats such as actors like insurgents and terrorists. The United States may understand how to strategically shape the IE, but at the operational level it often relies on its superior military might, or its force advantage, to achieve victory in the PE and neglects the efficient and effective use of the IE.

How Terrorists and Insurgents Pursue Victory

"Guerilla war is far more intellectual than a bayonet charge."

-T. E. Lawrence

In stark contrast to the US, terrorists and insurgents adopt a much different approach to achieving victory through the use of a complex IO strategy. A non-state actor develops the IE battlespace because of the benefits gained from its residual effects. "Terrorists act in the physical environment not to make tactical gains in the physical environment, but to wage strategic battle in the information environment; therefore the PE enables many of the activities in the IE to occur" (Earl & Emery, 2003, p. 44). The McCormick Influence Process Model (Figure 1) shows the process that nearly all terrorists follow to achieve their objectives by indirectly influencing a decision-maker (Earl & Emery, 2003, pp. 11 12). The process is applicable to select insurgencies.

The model's four steps and three orders of effects begin with a bombing or attack in the PE that is reported by the media or members of a population. These interpretations can shape perceptions of a populace or government in the IE. Terrorists then decide on follow on actions in the PE depending on the measure of success in the IE. It is difficult to easily change perceptions once developed, which can endure for days, months or decades. The model demonstrates not only that a specific act in the PE produces residual effects; it also offers an approach where US forces can interdict into the adversary's IE in order to reduce or reverse the effectiveness of PE actions. Therefore, any operation focusing on eliminating non-state actors and their influence must also employ forces operationally to counter the potential strategic impact and results of previous non-state operations. It is important to have effective counter operations to current and previous acts in the IE, and not just attrition warfare in the PE. Therefore, shaping the IE is not just merely denying information to adversary decision makers, but denying them the results from their actions.

The big difference between what current US doctrine is and should be is its approach to conflict. As long as US forces are denying a state foe his ability to make a decision, they are shaping his IE. The US may not be able to impact the ability of a non-state foe who maintains an information advantage to make a decision, but can affect his results in the IE, his chosen

battlespace. As long as the US conceptualizes all victories in the PE through decisive engagement rather than potential lengthy action in IE, it may not succeed as quickly. If the US adjusts its approach to non-state conflict, it can beat insurgents and terrorists at their own game in their own battlespace. This requires adopting a new approach to modern conflict that is different from traditional warfare.

Applying the Art of Information Operations

Figures 2 and 3 illustrate the US military's current approach to state and non-state conflict. This approach works when engaging a similarly structured adversary such as North Korea or Iraq in linear conventional warfare. Figure 2 shows conventional forces using actions in the IE, such as PSYOP campaigns, EW, deception and OPSEC measures supported by media messages and civil military operations to achieve a victory in the PE.

The problem with the approach in Figure 2 is that it does not work against non-state actors such as insurgents or terrorists, who operate by design in a slightly different battlespace.

Figure 3 relates to the Iraqi police station bombing vignette discussed at the beginning of the paper and shows how state and non-state forces can operate in different battlespaces, with the non-state force gaining the long-term advantage. US forces conduct operations in the PE to defeat or deter Iraqi insurgents responsible for a series of bombings; however, that is only a portion of the insurgent's battlespace, who have shaped the IE with residual effects from previous attacks (Figure 3). The attacks on Iraqi supporters of US programs perpetuate a perception of insecurity in the fearful population. This perception *does not* dissipate with a few US force victories against insurgents. The perception reaches audiences in the IE, which ultimately supports the insurgents' strategic objective in the PE, such as the UN choosing not to hold elections or the US withdrawing prematurely. To win, the US must realize and employ the art of IO as well as the science. The US must also understand that when its forces react negatively to the populace (i.e. door kicking night raids), they are drawn into a strategy to improve the insurgents' own IE. As a result of US forces' actions, annoyed citizens may no longer cooperate and may even actively support insurgents, becoming more anti-US than pro-insurgent. A silent population is defacto support to the insurgents, who maintain or increase their information advantage in the IE.

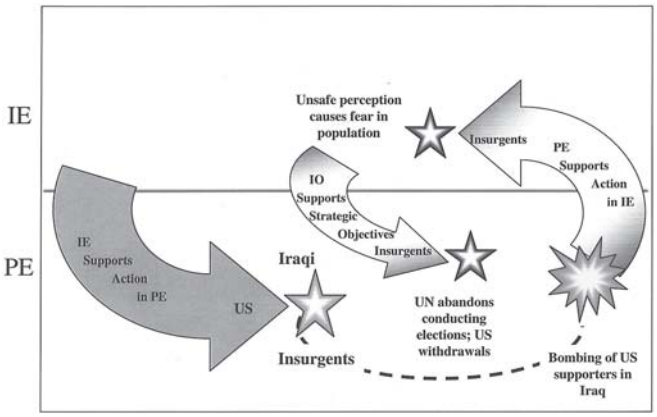

Figure 3. Strategy for Non-state Conflict.

"We recommend this IO definition for the new JP 3-13: 'the timely employment of specified capabilities to influence, disrupt, corrupt or usurp the adversarial information environment and decision making while protecting our own.'"

The effect insurgents have on the IE can be compared to the ripple effect caused by a stone dropped in a lake. Long after the stone has hit the bottom, the residual effects of the act carry on in all directions and are difficult to interdict, ultimately crashing into the banks of the lake. The current non-state conflict strategy focuses on the splash of the stone (the PE), and not enough on affecting the ripple (the IE) before it reaches the bank, which represents the strategic PE objective.

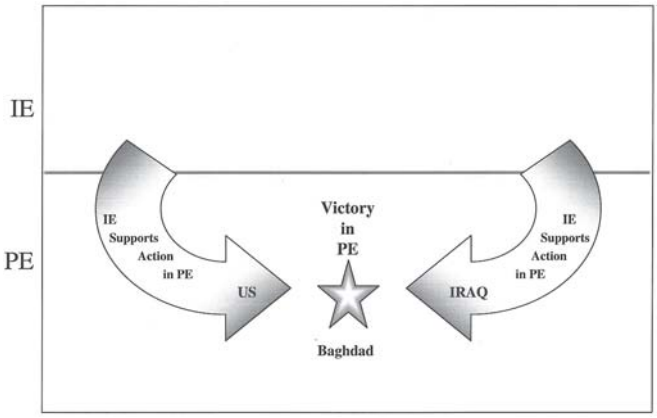

Figure 2. Application of IO in Conventional Conflict.

Recommendations

Revisers of the next draft of JP 3-13 should consider the following recommendations to improve the US military's ability to counter non-state threats. First, the doctrinal definition of IO needs modifying to better reflect operations in the IE. The proposed IO definition in the JP 3-13 (draft) limits what can be accomplished by limiting what capabilities are used. IO is the effect sought, and not just the tools to get that effect. The new definition of IO should reflect using all available capabilities in full spectrum operations to impact the IE instead of solely focusing on adversary decision-making capability in the PE. We recommend this IO definition be used in the new JP 3-13: 'the timely employment of specified capabilities to influence,

disrupt, corrupt or usurp the adversarial information environment and decision making while protecting our own.'

The second recommendation for changes to IO doctrine to meet the new security environment threat is placing emphasis on IO to influence and obtain information superiority. The US must break the mindset that information superiority is inherent with combat superiority. The most powerful force may not always have information superiority or be able to directly influence adversarial decision-makers in order to shape the IE. To achieve information superiority, IO doctrine should address actions and impacts in the IE to enhance US objectives against non-state actors whom rely on the IE as their primary battle space.

The third recommendation for future IO doctrine is to emphasize the art of IO as one of the core concepts of offensive IO. The Joint community has a prime opportunity to shape a new approach to warfare by placing emphasis on addressing actions and impacts in the IE and not just in the PE in order to enhance United States' effects against non-state actors, whom rely on the IE as their primary battlespace.

Lastly, IO doctrine should change its approach to non-state threats by conducting find, fix, and finish actions in the PE while shaping residual effects from previous actions in the IE. An adversary's residual effects may persist from previous actions in the IE following some act in the PE. To counter this, US IO doctrine should adopt a simultaneous two-prong approach against non-state threats through physical attacks as well as disrupting and minimizing their current and previous influence in the IE (Figure 4). JP 3-13 (draft) briefly addresses principles that would support the two-prong approach but insufficiently emphasize it as a core concept. It states that the focus of offensive IO is to directly affect information to indirectly affect human decision makers "by taking specific

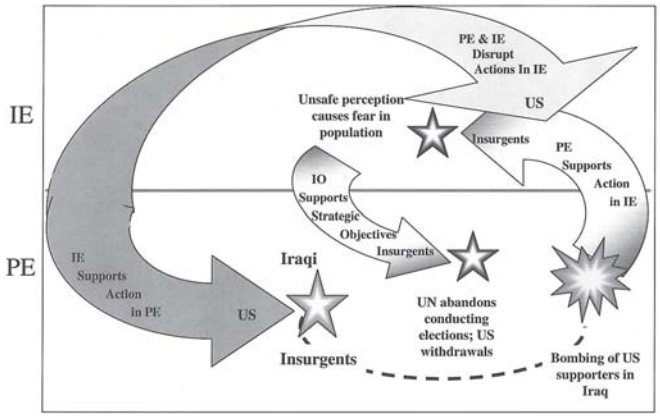

Figure 4. Proposed Strategy for Non-state Conflict.

psychological, electronic, or physical actions to add, modify, or remove information itself from the environment of various individuals or groups of decision makers" (Joint Publication 3-13 [draft], p. I-9). The simultaneous two-prong approach reduces non-state actors' operational effectiveness and support,

Joint Combat Camera Photo

Non-state actors operate mainly in the IE to leverage their advantages, while the US often chooses to leverage its force advantage in the PE.

causing them to either decrease operations or take greater risks in their activity, thereby increasing their exposure to defeat in the PE.

Summary

This study concludes that current Joint IO doctrine, published or drafted, insufficiently addresses the non-state conflicts facing the US such as the current War on Terrorism and the counter insurgency fight in Iraq. To succeed in the new security environment, the new JP 3-13 must place an emphasis on better defining IO and shaping operations in the information environment (IE) to enable ultimate victories in the physical environment (PE) against non-state actors. Military leaders and planners must conceptualize that the domains of the PE and the IE exist in simultaneous yet separate battlespaces. Non-state actors operate mainly in the IE to leverage their advantages, while the US often chooses to leverage its force advantage in the PE. Fighting non-state actors such as terrorists and insurgents requires an understanding of the residual effects of gains and losses in the IE based on actions in the PE, and the benefit of the residual effects in the IE from actions in the PE are far greater than the physical result from the act (i.e. deaths from a bombing). To combat these residual effects, the United States should seek to shape the IE in its favor by conducting simultaneous operations to find, fix, and finish in the PE while shaping residual affects in the IE from current and past adversary and friendly actions in the PE.

Shaping the IE requires a new way of thinking and a new approach to warfare for staffs. It requires planners and leaders to conceptualize non-state conflict differently than a traditional conflict. By not evolving, the military will continue to inadequately address an important dynamic in current and future warfare. Planners must not get caught up in seeking only

immediate effects and ignoring the value of gaining effects in the IE, since the results may be protracted and difficult to quantify. Military operations do not always produce tangible, visible, or immediate effects. By shaping the IE, military forces can impact the adversarial decision-maker by influencing his environment without ever changing his perception or decision. This battle of ideas requires more bytes than bullets. The military achieves this by using the science of IO to focus on decision-making in the PE and using the art of IO to simultaneously shape the IE; this synchronization achieves the victory in the PE and counters results in the IE from current and previous actions in the PE. As long as US IO are oriented solely on the PE victory and not also on the IE shaping victory, the US military is not poised to successfully engage and defeat the wide range of threats in the ever-changing security environment.

Bibliography

Armistead, E. (Ed). (2002). Information operations: the hard reality of soft power. Washington D.C: National Defense University.

Terrorist approach to information operations. Monterey, CA: Naval Postgraduate School.

Joint operations concepts. (2003) Washington, D.C.: The Secretary of Defense..

Joint Publication 3-0. (2001). Doctrine for joint operations. Washington DC: DoD Printing.

Joint Publication 3-13. (1998). Joint doctrine for information operations. Washington DC: DoD Printing.

Joint Publication 3-13 [Draft](unk) Joint doctrine for information operations.

Joint vision 2010. (1996). Washington D.C.: US Department of Defense.

Joint vision 2020. (2000). Washington D.C.: US Department of Defense.

National security strategy of the united states. (2002) Washington, DC: Government Printing Office.

Neilson, R. (Ed.). (1997) Sun Tzu and information warfare, National Defense University Pres, Washington, D.C., 1997.

Quadrennial defense review report. (2001) Washington, DC: Government Printing Office.

Radvanyi, J. (Ed.). (1990). Psychological operations and political warfare in long term planning. New York, NY: Praeger Publishers