DJIM Dalhousie Journal of Interdisciplinary Management

Volume 5 – Spring 2009
djim.management.dal.ca
doi: 10.5931/djim.v5i1.45

Information Warfare – Doing Battle in the 21st Century

Abstract: This paper outlines Information Warfare as perceived by Western militaries. It maps out and defines Information Warfare as a multi-faceted strategy that relies on coherent and synchronized application of virtual and physical actions to achieve an objective. The purpose of this paper is to demonstrate the importance of how all types of information need to be managed with regard to military force.

About the Author: Owen Hewitt is an MLIS candidate at the School of Information Management at Dalhousie University. He holds a BA (International History) from Carleton University and is a member of the Carleton University Counter-Terrorism Discussion Group. He has long had an interest in military history, civil-military affairs and how the application of coercive violence is justified.

An earlier version of this paper was submitted for INFO 5500: Information in Society, a class offered through the School of Information Management at Dalhousie University. Several people assisted with the preparation of this paper: Dr. Bertrum MacDonald offered constructive advice regarding the thesis of the paper, Lieutenant Commander James T. Hewitt, Royal Canadian Navy (ret'd) provided essential insights from a military perspective, Gregory Hayward offered helpful critical comments, and encouragement came from Dr. Jan Fedorowicz, Dr. Marc Tyrrell and Yannick Veilleux-LePage of the Carleton University Counter-Terrorism Discussion Group.

Introduction

On February 24, 1964, an episode of the science fiction program *Star Trek* entitled “A Taste of Armageddon” was aired, Captain James Kirk and a human ambassador attempt to open relations with an alien species locked in a 500-year-old war with a neighbouring planet. Upon arriving, Kirk is told that the planet he is on has just suffered an attack that killed millions of people and destroyed his starship. When Kirk can find no evidence of destruction, radiation, or dead bodies, his first officer deduces the truth: the war is fought completely with computers that calculate the level of damage and casualties that would occur in an actual attack. Citizens who have been “killed” are given 24 hours to report to a disintegration chamber to be “processed” or else the enemy from the other planet will launch a conventional attack, forcing a retaliation that will result in the destruction of both civilizations (Coon & Hamner, 1964). Kirk’s situation here could, in a sense, be considered the perfect war of information, clean and mathematically precise, while leaving the infrastructure of the belligerents intact and allowing their civilizations to exist without serious impact if one ignores the loss of life. As warped as this vision of a future society at war is, does it have within it the basic realities of a war with information as its focus?

Information Warfare in the 21st Century

The rapid development of information technology (IT) over the past three decades has led many in military and defence circles to discuss it in the context of a revolution in military affairs. This revolution is fueled by the increasing application of IT to battle-spaces where the prime commodity and source of action and change is information. This vision of warfare was termed in the 1990s as information warfare (IW). IW is an umbrella term for multi-faceted, interdisciplinary strategies that blend physical and virtual events where actors perform or do not perform actions. Thus, goals and objectives are achieved and maintained while preventing adversaries from doing the same. IW does not solely apply to defending national interests but also embraces marketing, public relations, diplomacy, politics, counter-intelligence, IT, and international and domestic dialogues. IW is not these functions renamed, but rather a coherent application and synchronized approach to these functions. A practitioner of IW in this sense is akin to a conductor leading an orchestra (Jones, Kovacich & Luzwich, 2002). The purpose of this paper is to demonstrate the importance, application, and relevance of IW in the information age in regard to military force.

Changing the Face of War?

War’s true nature, as defined by Carl Phillip Gottlieb von Clausewitz, is characterized by a series of relationships and interactions between rational and non-rational forces in an environment where uncertainty, violence, and confrontation are prominent resulting in infinite possibilities (Lonsdale, 2007). Clausewitz also noted that countless “minor incidents,” essentially the result of random chance even a military genius cannot foresee, combine to

lower an army's performance so that objectives become incrementally harder to attain (Lonsdale, 2007). With Clausewitz's observations in mind, 20th century warfare can be seen to have the following characteristics:

- Conflict occurred between nation-states chiefly concerning territory
- Mobilization of large elements of populations for the war effort was required
- Sustained effort to dovetail industrial production and the war effort was demonstrated – perhaps even to the extent of the nationalization of industries
- Participation involved huge numbers of combatants with massive casualties being sustained
- Planning a war as a whole was required, extending from takeover of industries and essential services to elaborate strategies drawn up by military commanders who decided how to best deploy their forces
- Harnessing media to assist the war effort by laying emphasis on the national interest and by censoring and directing information was required (Webster, 2003, p 61)

World War II was an industrial war that saw massive industrial capacity, technical progress, and populations willing to commit long and arduous national efforts in support of their respective governments' steps toward victory or final defeat. It must be acknowledged that the use of nuclear weapons in August 1945 forever changed the dynamic of industrial war, and that the influence of this dynamic was the primary reason the Cold War did not develop into an active state of conflict between the United States and the Soviet Union. Consequently, the relative importance of IW since 1945 has increased and the Cold War may be considered a transitional period from the predominance of industrial war in the 20th century to the predominance of IW in the 21st century.

Webster states that 21st century warfare is characterized by the unraveling of industrial war to be replaced by the accelerating development of IW. The radical changes in military technology, ranging from the digital soldier to the latest technologies involved unmanned weapons platforms, satellites, and computer assisted weaponry of increasing complexity (Webster, 2003). In contrast to industrial war, Webster presents to the following characteristics of IW:

- IW does not require mass mobilization; warfare relies on relatively small numbers of professionals adept in handling complex and computerized tools
- The changing character of the military machine is consonant with what have been described as post-military societies where one side inflicts overwhelming force on an enemy chiefly through bombing while few, if any, casualties are risked

- The expectation that future conflicts will be brief encounters, with active operations lasting only for days or a few weeks, in which western forces are victorious by virtue of the overwhelmingly superiority of their military resources. (Examples of this are the Persian Gulf War of 1991, the Balkans war of 1999 and the Afghanistan battles of 2001, each of which lasted between just six and eleven weeks)

- In contrast to the elaborate plans of industrial war, IW plans for flexibility of response; today with the incorporation of IT into weapons technology, enormous volumes of information are flowing, feeding into complex planning for war which prioritizes mobility, flexibility and rapid reaction

- Without mass mobilization, the general population has little direct involvement with IW, even when this is undertaken in its name. However, the population has an expanded second-hand experience through massively increased media coverage of conflicts (Webster, 2003, p 62-64)

With the proliferation of IT and the onset of the information age, some might believe that IW is a relatively new development and has changed the conduct of war completely, perhaps even rendering theorists such as Clausewitz obsolete, or at least less relevant. IW has raised numerous questions: Is it a completely new art? Is it the newest version of time-honoured features of warfare? Is it a new arena of conflict? Is it a unified application of operations or an ad-hoc assemblage of tactics (Libicki, 1995)? Libicki has argued that IW as a technique of warfare does not exist separately from other branches. He states that IW involves the protection, manipulation, degradation, and denial of information and has about as much analytic coherence as an information worker (Libicki, 1995). Information is not in of itself a medium of warfare except in the specific context of narrow aspects such as electronic jamming or disruption of enemy computer networks. The superiority of information and the ability to process and act on that information may make sense, but the idea that IW gives combatants sufficient battle-space supremacy to prevent enemies from engaging in battle is ludicrous (Libicki, 1995).

In fact, attempts to define IW are extremely difficult. Although some parts of the whole are closely related, both in form and function, taken together it appears that there is little that cannot reasonably be called IW. For example, could not the bombardment of British cities during World War II by the German Luftwaffe be considered IW because of the Germans' ability to demonstrate that the British could be attacked in their homes at will from the air, thus creating the impression that Britain was defenceless? Could the terrorist attacks of 9/11 be termed IW not only because of the demonstrative effect of showing Americans they could be struck anywhere at any time, but also in the massive loss of financial infrastructure and information that resulted from the destruction of the World Trade Center?

Is a comprehensive definition possible? There is a danger in accepting a single description. One aspect of IW, perhaps championed by a single interest group, may come to dominate the discourse, thus becoming overrepresented. A definition that is too broad may become bloated, thus making any common conception impossible to identify other than the painfully obvious (that IW involves both information and warfare) (Libicki, 1995). If it is merely the combination of using information in waging war, IW is as old as humanity itself and one can see this in espionage, observation balloons, and cryptography. However, merely stating that IW has always been present is glib and ignores the advances that have been made ever since the present revolution in military affairs. Many aspects of how to apply IW are in fact new (Jones, 2002).

Therefore, within the context of developing technology, this paper employs a working definition of IW offered by Jones, Kovacich and Luzwich (2002):

> IW is a coherent and synchronized blending of *physical and virtual actions to have countries, organizations and individual perform, or not perform, actions* so that your goals and objectives are attained and maintained, while simultaneously preventing competitors from doing the same. (p. 5, emphasis added)

In order to fall under this definition, the litmus test is that if information is used to perpetrate an act that has as its objective to influence another to respond or not respond in a way that is beneficial to the attacker, then the originating act should be considered IW. This definition embraces not only the new tactics of computer, network and communication based tactics, but also traditional acts of war such as media/propaganda, psychological operations, and espionage (Jones, 2002). In fact, in some cases the use of IT is not even necessary, such as using wire cutters to cut a phone line or distributing pictures of soldiers abusing civilians. As Winkler points out, IW can be exceptionally simple. Information that is secured, encrypted, and stored beneath a hundred layers of protection in a computer system becomes highly vulnerable when it is printed onto a piece of paper, crumpled up, and thrown into the trash (Winkler, 2003). IW is both virtual and physical; it can be high-, low-, or no-tech and can be deployed to attack an enemy's strength or to exploit a weakness.

IW and the Evolution of the Military

As not only militaries, but societies, become more reliant on IT and information services, it is essential that citizens and leaders maintain confidence in the confidentiality, integrity, and availability of the information that is the source of their military and economic strength. Unlike the wars of the 20th century, the source of threats to this confidence is not the physical power of the various state actors, but rather the activities of non-state actors which have come to influence the changing strategic landscape. The activities of hostile non-state actors within information-rich environments are designed to hamper military and political effectiveness

through deception and psychological operations, whether it be through the Internet, radio, television, wall graffiti, or word-of-mouth (Dearth, 1999).

In combating hostile non-state actors, it must be recognized that the battle-space is changing. In many ways, we have witnessed the death of distance as military technology has enabled leaders to receive information from satellites, allies, special forces, radar, and other resources in real-time (Dearth, 1999). The development of a virtual world through the Internet has also signalled the death of distance: as long as two computers are connected to one another, distance is merely an abstract concept.

In the early 20th century, when armies marched on foot with long supply trains, military commanders had time to make decisions and respond to changes. Media reporting was also slow and could be effectively controlled. In the 21st century, commanders have seconds, minutes if they are lucky, to make similar decisions thanks to the development of real-time IT. Should a commander hesitate or act too rashly, he or she may miss an opportunity for effective action and perhaps even cause severe collateral damage to the direct detriment of the strategic objectives. Therefore, the development of ways to assimilate and act on information, as well as methods to train leaders to recognize how to best use information as it becomes available, is a high priority for militaries, especially as many commanders may in fact be hundreds or thousands of miles away from the forces they command.

In terms of military doctrine, western militaries also need to rethink operational emphasis. The principles of firepower and mass, while important, may become less important when the speed of information increases and thus requires improved decision making on the battlefield by soldiers. By possessing not only the ability to process and interpret information, but also the speed and agility necessary to implement or rescind action, soldiers and their commanders will be able fight the battle chosen as opposed to the battle confronted. This implies that effect-based attacks, designed to manipulate the enemy, rather than a target-based attack designed to destroy, will become more common. This leads to the possibility that commanders will be able to better distinguish between situations where effectiveness is best achieved by not employing lethality (Dearth, 1999).

Brig. General David Fraser developed this point further during a lecture on his recent experience in Afghanistan. He stated that all members of the military, from generals to riflemen, must be aware of how the improper use of force might compromise the strategic goals of their mission, considering the “rule of 60 minutes.” Anytime a Canadian or allied soldier improperly used force, disrespected an Afghan, or otherwise acted improperly, within 60 minutes insurgents would disseminate a video or description of that action on the Internet for propaganda purposes. Obviously, the insurgents were conducting IW using all the resources at their command and so it was imperative for the soldiers under General Fraser’s command to understand that every single one of their actions was under scrutiny and that they

must act, at all times, towards attaining the strategic objectives that their governments had set (D. Fraser, Lecture at Dalhousie University, November 28, 2007).

Western militaries are not alone in recognizing the importance of IW. Natarajan and Chakraborty (1998) quote Maj. General Arjun Ray of the Indian military foreshadowing the observations of General Fraser:

> While battalions kill the militants, Generals must get on with the mission of winning the information war. In no other conflict is the principle of information so paramount…In a wider sense, information encompasses the public's right to know, openness in sharing information in real-time (as long it does not jeopardise security), cooperation with the media; psychological warfare and proactive campaigning to win over the people in the rest of the country…It is not a war of material, it is war between human beings. Consequently, a General cannot hope to achieve the overall goals of helping in restoring the socio-political goals, if he loses the information war…Media provides the oxygen of publicity...attention fans the flames...to think the militant's propaganda is only by the use of the gun is far from true. Militants under guidance from their political mentors have worked out specific media goals and a publicity strategy along well thought of and scientific lines. Such orchestration must be taken in account when we plan and fight information battles. (p. 97-99)

Natarajam and Chakraborty also examine how the Indian military's adoption of IW includes specifically stating in the Chief of Army Staff's Ten Commandants that officers and soldiers must: "(8) Develop media interaction modes – use it as a 'force multiplier' and not as a 'force degrader'" (p. 240). Military journals in Russia and China, among other states not aligned or consistently friendly to Western societies, have been actively discussing and developing IW capabilities since the late 1990s (Berkowitz, 2000).

IW and the Media

IW is present at all levels of military endeavours and is as much bottom-up as it is top-down. Soldiers and commanders must be aware of its presence and impact on operations. In the case of soldiers, they must be aware how their tactics, actions, and interactions with all forms of media serve their strategy while commanders must be aware of what tactics cannot be employed as a result of the information environment that has developed as a result of globalization and the spread of IT. Failing to educate soldiers in this regard can have disastrous consequences if soldiers begin using the information environment to carry out IW by themselves. An example of this is the YouTube video "Pork Bullets" in which an unidentified speaker taunts Islamic terrorists with an unclean death by dipping his bullets in pork (2008). Even if the person in the video is not a soldier, due to the many incidents of collateral damage resulting in civilian deaths in both the Afghan and Iraq wars, videos such as these, suggesting

Western militaries want to send Muslims to hell, may harm the public image of Western militaries in the eyes of Middle Eastern civilians.

The example of “Pork Bullets” establishes that all types of media, in the era of globalization, are themselves part of the battle-space. The media plays an integral role in the conduct and commencement of war. Since ancient times when human beings carved images of their enemies being impaled on stakes, the media has been harnessed to support war efforts. This is augmented by the fact that globalization has brought in different outlooks, practices, and opinions into a common information environment, where they may be appropriated, synthesized, and used for similar or even opposing ends (Webster, 2003). As a result of a common information environment, the ability of states to manage the perception of warfare has become increasingly difficult, especially as opponents are able to use a variety of technologies: Internet, video, pirate radio, and others to offer their own version of events.

While the majority of IT and companies developing IT capabilities are Western or nations friendly to Western societies (such as Japan), a media explosion has led to staggering amounts of information being available on 24-hour news channels, the Internet, and radio talk shows coming at such volume and velocity that any kind of control is impossible (Webster 2003). In this context, with regard to the media as a component of IW, two points are evident. The first is that war, of varying scales and intensities, is newsworthy and is therefore of interest and profit to the media. The second is that the media and the military can often run at cross-purposes to each other. Journalists operate from the premise that they will tell stories as they appear and will endeavour to accurately represent what transpired despite the fact that it may displease powerful interests.

Perhaps the most remembered example of these cross-purposes from the 20th century is the 1968 My Lai massacre carried out by US Army forces in Viet Nam. Although there had been efforts by individual soldiers to bring congressional and military attention to My Lai, the massacre was exposed to the American public at large by investigative journalist Seymour Hersh on November 12, 1969 after an interview with the platoon leader responsible, 2nd Lieutenant James Calley. Despite an effort by army officers to cover up the massacres and the army’s attempts to keep its investigation as quiet as possible, the story broke at great cost to the army’s domestic and international reputation and had a great impact on changing the whole moral tone of the Viet Nam war. A Canadian naval officer serving at the time recently commented:

> I clearly remember watching the first news report on this event [My Lai], with astonished disbelief as did everyone else I knew. When it was subsequently confirmed, then we knew at that moment something very, very, very bad had occurred. (James T. Hewitt, email message to the author, December 1, 2008)

As a result of this commitment to accurately tell stories “as they occur,” many war journalists subscribe to an ethic of resistance to the manipulation of news during war (Webster 2003). This is not to say that manipulation of the news media during wartime does not occur, as evidenced by Glenn Greenwald’s investigation of the NBC television network’s military consultants, ostensibly independent commentators, but who owned substantial shares in private military contractors operating in Iraq (2008).

In an effort to manage the perceptions of journalists, and their readers as a result, Western militaries have developed methods to handle journalists. Journalists are embedded with military personnel, with whom they are encouraged to form an emotional bond. They are also accompanied by a “minder” whose job it is to keep journalists from seeing things counter-productive to the war effort or to convince them to adopt a particular viewpoint. Military spokespeople are carefully groomed and reporters who are deemed to be unfriendly are restricted from entering the war zone. Efforts such as this to manage war coverage have had mixed results and have also served to bolster journalists’ scepticism and cynicism regarding military operations. Furthermore, when one calculates how many journalists from different countries and backgrounds are able to converge on a war zone, then one can begin to see how difficult the task of the military to keep the media “on side” has become (Webster, 2003).

For instance, there were an estimated 2000 journalists in the Kosovo region during the 1999 NATO air campaign. It was simply too complex a situation and the diversity of journalists too great for them to be straightforwardly controlled. This means that no matter how committed a military is to keeping the media on side as it attempts to manage perceptions of its military operations there will always be information seepage (Webster, 2003). This seepage is a persistent thorn in the side of a military engaged in war. As war waged by western societies usually tends to be in the name of democracy and the popular will of the public, then public approval is critical to its conduct. A corollary of this is that while the public is no longer mobilized as in industrial war, it is still involved in the role of spectator. When the conduct of war is scrutinized by those whose name it is being waged in, military and political leaders are impelled to try to manage information.

However, efforts to manage information so that it is interpreted correctly by democratic stakeholders who may decide to vote against the war flies in the face of having a free press and also serves to undermine the credibility of the war effort (Webster, 2003). Efforts to maintain freedom of the press while also managing perceptions and interpretations have, in fact, become part of the fog of war that exists in the information environment.

Coordinating IW

The battle-space has grown and changed, and areas of operation, interest, and influence are becoming increasingly blurred (Dearth, 1999). As a result, in order to maintain operational effectiveness as well as knowing when to apply force and when it is better to refrain from doing

so, militaries are becoming heavily reliant not only on information, but on processing and acting logically in response to information. General Fraser found that the mission he was assigned, to aid the Afghan government in rebuilding southern Afghanistan and promoting a healthy democracy, was beyond the scope of his military training and the abilities of his troops. While the Canadians could provide protection, they could not take effectively carry out building infrastructure and facilitating cooperation between communities, provinces, and sectors; their weakness in these areas was exploited by insurgents to the detriment of the Canadian mission.

Before the process of rebuilding Afghanistan's infrastructure and society could begin, a National Information Infrastructure (NII) needed to be developed that would facilitate protection against all forms of IW and give the Canadians and their allies the framework necessary to communicate with each other effectively (Stagg & Warren, 2003). General Fraser's efforts to build an NII involved engaging in multiple dialogues with the Afghan government, the Canadian government, and allies to craft a strategy where Canadian officials specializing in foreign affairs, corrections services, civilian police, and aid and development would join with the military to work with the Afghan government to pursue its objectives. It was only after the creation of a NII suited to receiving, assimilating, and acting on incoming information did General Fraser feel he could carry out his duty.

From this point, battle damage assessments may now be considered. Battle damage assessments have always been difficult, but with the integration of IT into combat operations, how does a commander know when he or she has won? How does the commander measure sufficient destruction of the opponent's strength, ability to regroup, and adaptation to new situations and challenges? How does the commander assess the need to re-strike targets? In situations such as the kind General Fraser faced in Afghanistan, there is no easy way to do this, especially when the use of physical violence may compromise positive perception management. For all the advances in IT, a fundamental uncertainty in all aspects of war is the effectiveness of military forces in conflict (Dearth, 1999).

From all of the factors described in this paper, we can deduce that IW is fundamentally not about IT. It is about people, both those in the military and civil society, both the supporters and opponents of military action, both the military and its enemies in the battle-space. It is what is done with IT which is important. While the sophistication of weaponry is important, ultimately it is people who are targets, and the battlefield is their perceptions of the information they are receiving. In order to win, or to avoid losing, militaries need to understand the aspirations, motivations, and intentions of people, their own, their enemies, and those who are observing from outside or who are caught in the middle (Dearth, 1999).

Iraq: A Cautionary Tale

Former US Secretary of Defense Donald Rumsfeld was an advocate of a transformed US military that would be a technologically networked and highly coordinated fighting force using its superior technology to speedily achieve goals, with minimal casualties, and require less troops than ever before to achieve strategic objectives. To this end, before the invasion of Iraq in 2003, Rumsfeld ordered new speed goals for future military operations that would enable the military to mobilize and deploy in 10 days, defeat an enemy in 30 days, and be ready for a new war within another 30 days. Rumsfeld's goals were highly dependent on improving the use of IT to coordinate units, the expansion of covert special forces, and the massive psychological effect that resulted from the superiority of American military technology (Lonsdale, 2007).

The American doctrine of "Shock and Awe" was the result, which had American forces quickly capturing Baghdad and deposing Iraqi despot Saddam Hussein in under three weeks by using overwhelming force to compel large segments of the Iraqi military to capitulate shortly after engagement or without engaging at all. Rumsfeld and his reliance on highly networked forces and massive acts of psychological warfare appeared to be vindicated.

Rumsfeld's strategies and tactics were in keeping with the contemporary revolution in military affairs. The speedy overthrow of Saddam Hussein's regime in Iraq seemed to indicate American forces possessed near-complete situational awareness that lifted the fog of war during Operation Iraqi Freedom. In many cases, the invasion of Iraq was an act of bombardment, in which victory came about through the destruction of a few key enemy targets with precision-guided munitions, usually through command of the airspace. The emphasis on command of airspace reflected not only the technological development of US forces, but also sensitivities in Western societies towards military casualties (Lonsdale, 2007). Yet while this desire to dominate from the air so that fewer ground troops are needed may seem attractive, US General Norman Schwarzkopf (ret'd), architect of the 1991 Persian Gulf War, said "[t]here is not a Commander in the entire world who would claim he had taken an objective by flying over it" (Lonsdale, 2007, p. 236).

The resulting insurgency and terrorist campaigns have painfully revealed that war, as Clausewitz states, is a realm of infinite possibilities and complex interactions depending not only on luck and chance, but also the realization that war is a non-linear activity (Lonsdale, 2007). In other words, American forces won the war but subsequently lost the peace by failing to enforce law and order. After more than six years of reconstruction, the new Iraqi government does not yet possess the ability to enforce lasting stability without the aid of the American military while insurgents continue to strike at American and Iraqi targets.

Rumsfeld's proclivity for military transformation, technological supremacy, and emphasis on speed, in essence a near total reliance on IT or IT-enhanced forces, did not prevent many of

the current problems in Iraq from occurring. In fact, many argue they exist because of Rumsfeld's refusal to send more troops to secure and enforce order in the post-Saddam Iraq (Lonsdale, 2007). Simply put, as law and order broke down, US forces demonstrated they could destroy Iraq, but they could not or would not govern it. It was this realization that allowed the insurgency to grow, as the insurgents and terrorists began exploiting the relatively low level of US troops to strike poorly guarded areas, hid among the general population to inflict heavy losses on American forces with low-tech booby traps, and began launching their own propaganda to offer a counter-narrative to that of the American forces. Simply put, the insurgents and terrorists in Iraq refused to play by the rulebook the Americans had written, exemplifying another key aspect of IW: asymmetry.

Conclusion – Scotty's Choice

IW has existed for a long time, but the methods we use to carry it out are developing at an unprecedented speed. With the spread of globalization, interconnectivity, and IT, the battle-space of the 21st century includes land, air, sea, virtual space, and the hearts and minds of people. Relying on technological superiority alone will result in disaster unless the technology is supported by sufficient ground forces to maintain law and order and backed up by psychological operations and an effective media campaign to present a convincing case for cooperation.

Returning to the example of *Star Trek* from the beginning of this essay, when Captain Kirk is told that he and his crew would have to sacrifice themselves to prevent a conventional attack on the alien planet, Kirk ordered his second officer, Lieutenant Commander Scott, to execute General Order 24, the complete and utter destruction of the alien world using the weapons of the Enterprise. When the alien leader threatened to kill Kirk, Scott replied that it was an empty threat; Kirk would be dead anyway when the Enterprise carried out General Order 24. Unable to destroy the Enterprise because of its defences, the alien leader was distracted while Kirk destroyed the computers the aliens used to fight their war. With the destruction of his IT capability and facing certain death at the hands of a well-armed starship, the alien leader had no choice but to unconditionally surrender to Kirk and enter into peace negotiations with his neighbours.

The answer to the question asked at the beginning of this essay can be drawn from Scotty's choice. While "A Taste of Armageddon" does incorporate important aspects of IW, ultimately war is about kinetic violence – the neutralization of enemy forces and the destruction or denial of their means of support. Only by studying the aliens' weakness and taking measures to destroy their IW capability, not only by physically destroying their equipment but also by overcoming their jamming capabilities to contact each other do Kirk and Scotty demonstrate the best application of IW. Possessing superior information as well as the capability to act on that information is essential if one wished to achieve victory in modern war, but to believe that IW alone gives enough battlefield dominance to guarantee success is foolish. It is necessary

for soldiers to be educated about IW but ultimately their primary purpose is to neutralize the enemy military or paramilitary forces.

References

Al Asqa TV. (2007, July 1). Farfour "martyred" by Israelis in final episode [Video file]. Video posted to http://www.youtube.com/watch?v=TrieBhaGgHM

Berkowitz, B. D. (2000, Winter). Information warfare: Time to prepare. *Issues in Science and Technology*, *(17)*2, 33-46.

Coon, G. L., & Hamner, R. (Writers), & Pevney, J. (Director). (1967, February 24). A taste of Armageddon [Television series episode]. In G. Roddenberry (Producer), *Star trek*. New York: Desilu.

Dearth, D. (1999). Imperatives of information operations and information warfare. In F. P. Harvey & A. L. Griffiths (Eds.), *Foreign and security policy in the information age* (pp. 99-114). Halifax: Dalhousie University Centre for Foreign Policy Studies.

Greenwald, G. (2008, November 30). The ongoing disgrace of NBC news and Brian Williams. *Salon*. Retrieved December 1, 2008, from http://www.salon.com/opinion/greenwald/2008/11/30/mccaffrey/

Jones, A., Kovacich, G. L., & Luzwich, P. G. (2002). *Global information warfare: How businesses, governments, and others achieve objectives and attain competitive advantages*. New York: Auerbach Publications.

Libicki, M. C. (1995). *What is information warfare?* Washington, DC: Center for Advanced Concepts and Technology Institute for National Strategic Studies.

Lonsdale, D. (2007). Clausewitz and information warfare. In H. Strachan, & A. Herberg-Rothe (Eds.), *Clausewitz in the twenty-first century* (pp. 231-250). Oxford: Oxford University Press.

Natarajan, V., & Chakraborty, A. (1998). *Information war in the defence strategy*. Gautaum Bush Nagar: Trishul Publications.

Pork Bullets [Video file]. (2007, February 13). Video posted to http://www.youtube.com/watch?v=nHZeHxnjCMI

Stagg, V., & Warren, M. (2003). A national information infrastructure model for information warfare defence. In R. Azari (Ed.), *Current security management & ethical issues of information technology* (pp. 97-110). London: IRM Press.

Webster, F. (2003). Information warfare in an age of globalization. In D. K. Thussu & D. Freedman (Eds.), *War and the media: Reporting conflict 24/7* (pp. 57-69). London: Sage Publications.

Winkler, I. S. (2003). Information security is information security. In D. J. Loundy, *Computer crime, information warfare, and economic espionage* (pp. 3-8). Durham, NC: Carolina Academic Press.