The Low-Tech Side of Information Warfare

by
Capt Alex Berger

High-tech terrorists employed by the Cali drug cartel electronically blind early warning radar scopes all along the southern US border. USAF F-16s scramble to intercept an armada of inbound drug smuggling aircraft, but their radar scopes suddenly go blank due to a logic bomb placed in their flight computers months before. A computer virus is surreptitiously placed in the US banking system, zeroing out the account balances of every American service member assigned to US Southern Command and creating widespread panic. The President wants to launch a retaliatory strike, but his military advisors can't prove who did it or who to retaliate against. Although fictitious, this scenario now sounds more feasible than ever before.

Information Warfare (IW) emerged as the hot, new topic of debate for military thinkers. At the highest levels of the Department of Defense (DOD), IW is called the latest "revolution in military affairs." The Air Force is posturing itself to fight these high-tech wars by creating the Air Force Information Warfare Center and, more recently, the 609th Information Warfare Squadron. But are we on the right track for preparing to fight these "information wars" of the future?

The move toward an "information-based society" is changing the way we'll fight future wars, just as the move from the agrarian age to the industrial age forced a change in war fighting. This article looks at the background of IW and Command and Control Warfare (C2W), and then addresses a major point of disagreement; whether IW is our inevitable future in the technology age or it is a misguided attempt at phasing out traditional means of warfighting. Finally, it will look at the impact of IW on the "human side" of warfare and how the Air Force must make improvements in the future.

Fighting for control of the "information battlespace" is not new to the military, although many argue a rapid rise in technology is driving the move toward a new form of warfare we are calling IW. DOD defines IW as "actions taken to achieve information superiority by affecting adversary information, information-based processes, and information systems while defending one's own information, information-based processes, and information systems." (DOD Dir 3600.1) IW is a very broad concept incorporating all aspects of our National Information Infrastructure, including DOD, other government agencies, and corporate America. Because IW involves more than just DOD, it's actually C2W we in the military should focus on, not IW. C2W is the strategy that applies IW to the military battlefield. However, DOD now uses the term "Information Warfare" synonymously with C2W concepts.

C2W is "the integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and

control (C2) capabilities, while protecting friendly C2 capabilities against such actions." (CJCS MOP 30) This definition is almost identical to IW's definition, but it deals strictly with IW's military aspects. C2W's objective is to decapitate the enemy's command structure from its body of combat forces. This concept is not new, but we've only recently made a concerted effort to coordinate C2W's five elements in a joint, high-tech environment.

According to these two definitions, we're already fighting the "information war" and have been for a long time. Ever since man began conducting war, it's been advantageous to get into the enemy's mind and to interfere with their decision-making processes. IW theorists talk about the "OODA loop" describing the decision-making process humans use to observe, orient, decide, and act. Although new technology increases the speed we can complete this decision-making process, the actual process has not changed. Today's high-tech systems simply give us another means of affecting the cycle, but they're not a replacement for good old military operations.

An example of a leader who defeated his enemies with C2W is Mongol leader Genghis Khan. According to Paul Linebarger in his book Psychological Warfare, Khan was widely known for leading hordes of savage horsemen across Russia and into Europe. While not totally unfounded, the Mongols' image of total, barbaric domination was greatly enhanced by Khan's use of PSYOP, deception, OPSEC, and targeting his adversaries' decision-making process. "Agents of influence" were sent in advance of his armies to do face-to-face PSYOP, telling of brutality and large numbers in the Mongol army. Khan also used deception to create the illusion of invincible numbers by using rapid troop maneuver, making his army look larger than it really was. He had a network of horsemen called "arrow riders" to communicate quickly with his commanders, and he targeted enemy messengers to prevent enemy commanders from communicating with each other. All these actions caused a weakness in their enemy's psyche, and the Mongols were feared wherever they went. If Genghis Kahn were alive today, he may have employed CNN's Peter Arnett instead of his agents of influence. He may have used Hollywood movie techniques to create propaganda films depicting the barbaric treatment enemies would face if they challenged the Mongols. He could have used satellite communications to talk with his commanders and electronic jamming to interfere with his enemies' communications. No matter what the technology, the effect would have been the same. Genghis Khan still would have controlled the information battlespace.

IW is a much-debated topic, and for every advocate there's also a critic. IW supporters say we're already under attack and, because of our reliance on technology, we have much to lose from our inactivity. IW critics see an unjustified obsession with technology that will divert money from more reliable, traditional capabilities. Indeed, there's a danger in relying solely on technology when conducting warfare. For example, a human intelligence asset is much less likely to be tricked by a decoy tank or aircraft than an intelligence analyst looking at satellite imagery. This is not to say we should ignore the new capabilities technology gives us today, but neither should we fixate on technology as a magical new way to employ forces. IW includes all operations where we attempt to influence a perception or behavior using information, and this information doesn't have to be technology based. High-technology weapons and equipment can certainly support or augment traditional military operations, but they'll never replace them. IW and C2W are simply coordinating all means available to get the job done.

There's also a common misperception in the military that C2W can only be applied in war-time, while IW can be used throughout the spectrum of conflict. This is not true. Of C2W's five elements, only physical destruction and EW are limited to wartime roles. For example, Overt Peacetime PSYOP Programs exist in every region of the world. These programs are ongoing and support such peacetime missions as de-mining and counterdrug efforts. Operational PSYOP can be used throughout wartime, and consolidation PSYOP can help rebuild support after the fighting is over. The same can be said for deception and OPSEC which are also done throughout the operational continuum.

One of IW's biggest criticisms is that it assumes conflict in a high-tech environment. How can we fight information wars with countries like Haiti or Somalia still fighting in the industrial or even agrarian age? Arguments fly between the "techies" and the "dinosaurs" over the fact that most current adversaries are not high-tech entities, but low-tech groups. Debates rage over the validity of putting airmen at risk when we could instead use cruise missiles or unmanned aerial vehicles (UAV) to conduct missions. With reduced funding available for military operations, some argue attacking systems with computers is cheaper than using costly munitions. Others argue if a system is not physically destroyed it may still be capable of causing damage. These debates are valid, and each side has convincing arguments. What everyone agrees on is enormous growth in information technologies gives us opportunities we never had before, and we must adapt our doctrine and strategy to take advantage of them. IW is a new form of warfare resulting from changing technology, combined with an old strategy of war fighting targeting our adversaries' decision-making process.

With decreasing military budgets, decisions often come down to choosing between expensive, high-end systems or cheaper, time-proven equipment. Going back to the IW and C2W definitions, these concepts focus on the actions taken to fight and defend, not the equipment used. It really shouldn't matter what means we use to fight a war, as long as those means allow us to complete the decision-making process more quickly than our adversary. No matter if our adversaries are high-tech hackers or low-tech guerrilla fighters, human beings have the same basic wants, needs, and desires. Without a doubt, technology will play a significant role in the Air Force's future, and we must take advantage of it. But, it's just as important to understand our adversaries' cultural, ethnic, and religious beliefs as it is to be able to electronically attack their C2 nodes.

Traditionally, the Air Force has been weak on considering what Prussian strategist Carl von Clausewitz called the "moral factors" of warfare, the fact that there is a human side to warfare. Somehow things seem much less personal when dropping bombs from 10,000 feet or launching cruise missiles at an enemy hundreds of miles away. We focus more on the impact our bombs have on production capabilities than on an enemy's will to fight. Similarly, we are focusing too much on the impact of IW on enemy systems and not enough on the people. Now is the time for the Air Force to realize the importance of understanding our enemy as a group of people who are led, motivated, and directed by other people, not just a collection of weapon systems.

Collecting information on our adversaries is essential, but we must also be able to understand how this information can be used to better understand our adversaries' intentions and exploit their weaknesses. For example, very few Air Force personnel have been educated in PSYOP, yet

it is one of the five elements of C2W we all must understand. An effective PSYOP campaign is tailored to appeal to a specific target group based on our knowledge of their language and culture, and the same should be true with IW. Recently, the Air Force has headed in a dangerous direction. Human intelligence assets are being replaced by electronic sensors and data bases, and we are losing the capability to understand what the enemy is thinking and what he intends to do. Junior officers are no longer encouraged to pursue postgraduate education, and the intelligence community has cut back on training regional specialists. As Sun Tzu said, the only way to defeat the enemy is to know the enemy. We can only do this by studying the enemy. Technology allows us to collect and process information much more rapidly than ever before, but technology won't get us into the heads of the local population or leadership to let us know what they are thinking. Despite all we've heard about IW recently, there is a low-tech side to IW. It's time we, as the Air Force and as a nation, realized the world does not share the same cultural, religious, and moral beliefs that America does. No amount of technology will give us this broader understanding of humankind. The only way to truly know the enemy is to study their history, culture, and language. We can do this by providing opportunities for our personnel to attend schools that give a cultural awareness or regional orientation. We must maintain a large number of regional specialists and human intelligence assets. We ought to support foreign exchange programs and use our military-to-military contacts to better learn about other countries. We should encourage our junior intelligence officers to pursue postgraduate programs in political science or international relations. We must not turn warfare into a computer simulation that discounts the intricacies of human behavior.

There is no doubt IW is changing the way we will fight future wars. At this point we can only speculate how to best shape our force for the next 25 years, and there are some very high-level people thinking about this problem every day. But it is crucial to remember IW is not the only way we will fight in the future, and because we don't have an unlimited budget we will have to make some very tough decisions. We must find the right balance between procuring high-tech systems and maintaining our "traditional" systems. To ignore either would be disastrous. We must also remember there is a "human side" of warfare that can't be attacked or deciphered by a computer. We must maintain a pool of highly trained specialists who understand the history, religion, and culture of every potential adversary. Only then will IW be useful in almost every situation.

The author, Captain Alex Berger, is an Air Force Intelligence Officer. He is the Director of the Joint Psychological Operations Course at the USAF Special Operations School, Hurlburt Field FL, and will be attending the Naval Postgraduate School this summer.
