

OPSEC KEY TO CURRENT, FUTURE OPERATIONS

CAPTAIN TIMOTHY HSIA

This article was first published in the Small Wars Journal at www.smallwarsjournal.com.

The world today is indeed flat. It is possible now to quickly disseminate and share information globally in seconds rather than days. On today's battlefield, any Soldier or insurgent can collaborate with his comrades across the globe in real time to influence or alter future decisions. If intelligence drives operations, then it is paramount that the U.S. military conceal its intelligence capabilities. The digital boom of the past 15 years is considered a blessing for the majority of people in the world; however, it also poses a unique operational security (OPSEC) threat. Today's military leaders in the Middle East face a difficult conundrum concerning

how to reduce OPSEC vulnerabilities when planning and executing future operations. The threat the military faces in terms of OPSEC ranges from the profundity of open source information readily available to the problems arising from joint operations can no longer be overlooked as our enemies actively seek to gain the upper hand by closely monitoring our activities.

Military leaders have come to realize that globalization has allowed Soldiers to quickly relay information to family members back home by posting thoughts on chat rooms and activities on personal blogs. Today, a common joke deployed Soldiers share is the fact that spouses "back in the rear" are probably more discerning of future operations in the unit than they are. The amount of open source news that anyone can retrieve from the internet is simply staggering. Anyone from insurgents to interested family members can essentially create a link diagram of key leaders within a unit. They can read biographies, past assignments, accomplishments, and quotations of leaders from platoon leader and above. Essentially, on the internet there

exists an asymmetric amount of information which the enemy can collect on U.S. military units in comparison to the dearth of information we can research about the insurgents we are fighting. Interested observers do not have to be in the unit to know when a unit has displaced. All they have to do is scour the internet and read the latest open source reports regarding the unit in question.

OPSEC has long been a concern of military commanders and the rapid growth of information technology has only exacerbated it. Even GEN Dwight Eisenhower, Supreme Allied Commander in Europe in World War II, and the planners of the invasion of Normandy practiced OPSEC. GEN Eisenhower was perhaps fortunate that his Soldiers did not have access to the internet or phones. Imagine today an operation of that magnitude and whether or not the enemy would be able to clue in on

A Soldier with the 4th Brigade Combat Team, 3rd Infantry Division uses a radio during a joint mission in Iraq February 8.

SPC Angelica Golindano



American intentions. Even the simplest hints to loved ones such as, "I won't be calling home for a couple weeks, we are really busy" to "we are practicing loading and unloading boats for what I can only guess is a beachhead invasion" can have disastrous effects. But the truth today is that such information can be instantaneously leaked. It is foreseeable that in the future it may not only be the enemy with his bayonet greeting the U.S. military at the beachhead, but also the media with its cameras. The consequences of this information being leaked would be unpardonable. However, this possibility now exists today as deployed Soldiers unwittingly pass sensitive information to loved ones back home. The military mantra that "every Soldier is a sensor," is intended to imply that every Soldier is an intelligence collection node. In this case, however, the sensor is also an emitter.

OPSEC has become further diminished as intimate relationships have developed between embedded media and senior service members. These relationships between the media and the military require a deep level of trust and understanding. The same journalist that is discussing matters off the record with a division general could possibly be doing the same with key leaders of the insurgency the next day. How far does the military desire to publicly reach out to the fourth estate, and at what point does a military commander decide to evade answering further questions and refrain from volunteering additional information? The case of Geraldo Rivera leaking military plans about a future operation by showcasing a terrain model on the news is not an anomaly. The military has opted to allow for transparency in order to paint a more complete portrayal of the U.S. military. But at what point does transparency work against the military? Is the military today sacrificing the element of surprise for the chance to better its public relations? Units in Iraq today often find themselves with an abundance of media personnel right before the initiation of a major operation. This is not merely a coincidence as news reporters have stated that they indeed have been told about the pending operation. Thus, the onus on maintaining OPSEC resides not only at the rifleman level but also at the senior military commander level.

The military's dependence on contractors, U.S. and foreign, also has heightened the OPSEC dilemma. Contractors on military bases in Iraq are often the first to realize that military units are being moved. In this regard they are often the most attentive individuals

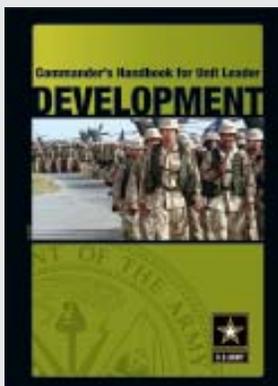
on the forward operating bases because their jobs usually involve life support functions such as housing and transportation. Contractors do not consist of solely patriotic Americans but are mostly foreign contractors whose intentions and values may not always align with America's military. Like deployed Soldiers, these local and third country nationals possess numerous ways to contact the outside world: cell phones, satellite phones, and internet access. Information they intentionally or unintentionally relay to friends and family across the globe has the potential impact of greatly affecting how America's enemies respond to our operations. Given this situation, it is very difficult if not impossible to achieve complete surprise against the enemy for units operating within Iraq.

Joint operations also pose a threat to OPSEC, especially if our partners are Iraqi. It is well known that some elements of the Iraqi Security Forces have been infiltrated by insurgents. Anytime U.S. forces conduct combined operations with their Iraqi counterparts they must share information and synchronize execution at the lowest levels. It is easy to imagine how such operations could be compromised purposely by enemy infiltrators or accidentally through carelessness on either side. Further compounding the problem is that Iraqi units simply do not have secured communication. Iraqi units rely on commercial cell phones, or worse, unsecured walkie-talkies at the tactical level. The problem is further compounded at the strategic level, when Iraqi officials announce publicly future joint operations in a certain region to the chagrin of tactical commanders who are planning to have the element of surprise when moving into a certain region.

In the future, the U.S. military must be extremely vigilant at concealing its hand in operations. OPSEC is a problem that will only exponentially increase in complexity as the digital revolution expands and as technology spreads outward from the western world to third world countries where future combat operations could occur. As today's operations in Iraq suggest, the digital revolution in information technology is one of the few areas where the U.S. military does not hold a distinct advantage over its adversaries. Tomorrow's adversaries will be less forgiving of our leaked intelligence and the consequences of compromised OPSEC will be far more deadly.

CPT Timothy Hsia is an infantry officer assigned to the 2nd Stryker Cavalry Regiment.

COMBINED ARMS CENTER - CENTER FOR ARMY LEADERSHIP



Visit the Center for Army Leadership's Web sites
for leadership information, publications,
discussion, and additional links:

CAL AKO — <https://www.us.army.mil/suite/page/376783>

LeaderNet — <https://leadernet.bcks.army.mil>

CAL public website — <http://usacac.army.mil/cac2/cal/index.asp>

Contact CAL at leav-web-cal@conus.army.mil

