Attaining and Maintaining National Security Advantage: Information Operations and Secrecy

By Michael G. Miller, Lt Col, USAF (Retired)
JIOC/J38

Editorial Abstract: *Secrecy has a fundamental role in our national security affairs. It's oftentimes challenging to determine whether something should be considered secret and to what level of secrecy it should be—a relentless decision cycle with the ultimate goal of attaining the best national security advantage. Appropriately crafting the types and levels of secrecy is especially important when conducting information operations (IO). Mr. Michael G. Miller (Lt Col, USAF, Retired), a principal analyst with Science Applications International Corporation (SAIC) at the JIOC, defines some basic theses and accompanying techniques that give analytic reasoning for underpinning the determination of classification.*

The National Discussions

Recently, there have been spates of commentaries in the national media regarding the inadequacies of our processes for classifying materials or information vital to our national security. It's not that these discussions are new: talking about how we determine what is secret—and just how secret we want it to be—has in recent years been (and not without reason) a fairly popular topic. During these discussion cycles, national security analysts usually argue that too much information is classified without adequate reason and that some seemingly innocuous information remains classified for periods that seem excessive. These analysts, rightly, would like to understand the analytic reasoning underpinning these classification determinations.

When national security pundits are discussing these topics in general, and decrying the inadequacies of the security classification system in particular, an overriding theme emerges: the government uses secrecy to hide things that the people have a right to know; the government cannot be trusted. This theme is really at the heart of the discussions on secrecy and security classification—it is, at bottom, a question of the level of the people's trust in their government.

One of the major reasons that the government's trustworthiness is questioned is because there ***have*** been ***some*** breaches of trust. Because there have been some, however, does not mean that this is the norm. This article acknowledges that this is an issue, but the focus here is not on the trust aspect—at least, not directly. Instead, this article focuses on the other troubling component of the problem—the analytic reasoning underpinning the classification determinations. The difficulty, some assert quite strongly, is that there doesn't seem to be a rigorous, well understood system or framework by which we determine what needs to be secret, and to what level of secrecy it needs to be.

Joint Combat Camera Photo

The B-2 Stealth Bomber is one example of a top secret weapon eventually released to the public.

A Lack of Theory

Writing about the difficulty, Dr. Bruce Berkowitz observed recently in the summer issue of The Hoover Digest:

> *"One underlying problem is that there is no theory—that is, a clear and widely accepted set of general principles—that tells us how to use secrecy, how much to use, when to use it, and how best to protect a secret. "Theory" may suggest "ivory tower," but in reality theories are always essential to sound policy. They explain the logical relationships between whatever it is that policies try to influence. Theories describe how to reconcile two goals that are both desirable but mutually exclusive: for example, the dilemma that secrecy can provide an information advantage over an adversary but security rules almost always make it harder to use the information that is being protected. Unfortunately, no one has a good understanding of the exact trade-off—let alone how to strike a balance."*

I can agree with Dr. Berkowitz that there is no really useful, existing general

Joint Combat Camera Photo

The F-117 stealth fighter is another program brought to public light after being veiled in secrecy for years.

theory or framework for understanding how we determine the amount and type of secrecy to be applied. From personal experience, though, I can cite some analytic techniques that have been developed (and are indeed in use) to determine when and how much to use *certain* aspects of secrecy in *certain situations*. In the absence of a *general* theory or principles that can be used to make these secrecy determinations, the decisions to do so can be, and in fact are viewed by some, as being completely arbitrary. It is the seemingly arbitrary nature of the determination to classify things at certain levels of secrecy that perplexes reasonable analysts.

Given the current and projected international security climate, it's important that we examine carefully the need to apply appropriate levels of secrecy to national security operations, with the emphasis on the term "appropriate." During the Cold War, we faced a cunning adversary with great skill and a massive intelligence collection infrastructure. Adversary intelligence operatives were masters at assembling seemingly insignificant bits of disparate information into an accurate portrayal of our actual intelligence, systems acquisition, and operational activities. Combine this with the traitorous actions of some, as well as the "goof factor"—throwing away the real war plans in the "dumpster," for instance—and it's understandable that the security classification system defaulted to the "everything is sensitive and should be classified" mode. The existence and actions of traitors, however, are system aberrations, as are dumpster episodes. The potential for these situations to occur must be acknowledged. The analytic framework applied to determine types and levels of secrecy to be applied should acknowledge these unusual cases, but not use them as the principal analytic basis for secrecy. We can't forget, however, that we have a new adversary, just as ruthless and cunning as our Cold War adversary, who is driven by an ideology that puts no curbs on the nature of the conflict. By and large, we face an "all or none" struggle, and the secrecy scheme that we apply must be crafted with this in mind.

Crafting the types and levels of secrecy appropriately is especially important when conducting information operations (IO). Sometimes, what is said openly (meaning it is not classified per the standard Department of Defense scheme) in the Public Affairs or related "strategic communications" arena is intended to signal intentions or operations whose details ***will*** be classified. There is, then, a level of artistry involved in making sure what is said openly reinforces, instead of undermines, the probability of success of future operations that may be highly classified.

"we have a new adversary…who is driven by an ideology that puts no curbs on the nature of the conflict"

Some Secrecy Theses and Principles

To begin our discussions on how we might decide what should be secret and how secret it should be, let's present for consideration some basic theses and accompanying principles.

Thesis One. No prudent national security analyst would argue against the need to maintain appropriate levels of secrecy—those that allow us to attain and maintain a ***national security advantage.*** Indeed, the need to attain and maintain national security advantage is the sole reason for imposing certain levels of secrecy in national security matters. Our nation's founders acknowledged in their writings and actions the importance of secrecy in conducting foreign affairs. So, **Principle I**: Secrecy is appropriate and necessary when conducting national security affairs.

Thesis Two. In a free society, the people have a right to know what their government is doing, and why. There is an accompanying thesis that holds that the people *expect* their government to keep certain things secret, if doing so will create an overall national security advantage. Historical precedent and current practice assign the responsibility for determining how secrecy will be used to the Executive Branch of government. In our government of the people, by the people and for the people, however, the people also have a right to know what their government is up to, and so the Executive Branch keeps the Legislative Branch—the people's representatives—apprised of its secret operations. Hence, **Principle II**: The Executive Branch determines how to apply secrecy and keeps the Legislative Branch informed regarding secret operations.

Thesis Three. There are general categories of things that need to be kept secret. Let's pick some categories of things that we think we might want to keep secret. In general, I can think of three major ones "right off the bat:"

- Military plans and operations;
- Intelligence plans and operations; and
- Military systems development plans and acquisition operations.

Though there are certainly others, for the purposes of this article, we'll focus on these three because these categories are the most important when conducting IO. So, we come to **Principle Three**: When conducting IO, there are inextricable relationships among systems

acquisition and development, intelligence, and military plans and operations, and secrecy is an integral element of all three. These are, in turn, tied to declaratory policy statements, which should bolster, not inhibit, the success of the other three.

Let's apply these three principles as we prepare and conduct a hypothetical information operation, and show how we can apply a set of rules that help us determine what can be divulged and what can be kept secret.

The "I've Got a Stick" Example

The following example is illustrative of the types of secrecy thinking that must be employed when conducting an information operation. Keep in mind, as the example is developed, that the purpose of applying a secrecy framework is to make sure that we attain and maintain a national security advantage in a particular situation—*and that every situation is different.*

Let's talk first about our adversary. Our adversary is formidable: bold, brutal, cunning and elusive. Our adversary has little regard for what we would term "civilized behavior." Instead, our adversary depends on terror to wage war. He will strike wherever and whenever he can without regard for the traditional notions of what constitutes a military target. For this adversary, anyone or anything can be considered a fair target. He measures success by the amount of damage he inflicts, how many are killed, and how much fear is created in the minds of the attacked. The only thing that will deter our adversary is a sustained demonstration of our overwhelming strength and a realization on his part that our will to use this overwhelming strength against him is unwavering.

Keeping our adversary's nature in mind, we decide to counter our adversary's efforts in a particular area by conducting an information operation. The operation will have three major components:

- Intelligence collection, processing and reporting as to the adversary target system status;
- Selection of a weapon's capability that will be specifically modified to affect the adversary target system; and,
- The operation to conduct the attack.

The operation's commander (in this case, the US President) would like the adversary to know the attack is coming. This is because he would like the adversary to *worry* about the impending attack. He also wants to say enough about the coming operation that it will cause the adversary to react in a way that will facilitate—or at least fail to inhibit—the attack. The President, however, does not want to "telegraph" which targets will be affected, which units will conduct the attack, or how much and what type of information we possess regarding the adversary's force dispositions. The President knows that the adversary, though misguided, is courageous and is committed to his cause; he also knows the adversary respects US might and desires to survive to continue his fight and preserve the forces and resources he has amassed.

The President has a certain weapons capability at his disposal—the hypothetical "stick." He wants to know which of the following two options will cause more national security advantage to accrue: telling the adversary, in essence, "I've got this stick and I'm going to beat you with it"; or saying nothing about the stick and just keeping it hidden and ready for use when needed? The following is an example of a secrecy decision matrix that could be used to assess the relative national security advantage of the two options. Should the President speak openly in general terms about the stick? "Openly in general terms" means that the President will acknowledge that there IS an operation that will be conducted and a weapon that can be used, not what it is, how it works or where/when it will be used or by whom. Again, bear in mind that this is an ***example***.

It can be seen that in the matrix we have established sample criteria, and each criterion is weighted; the individual weights, when added together, total one. Yes-No values are either one or zero, respectively, depending on which box gets the check mark. So, taking the criteria weight times the Yes-No value yields a score. In this example, the sum of individual scores adds to 0.8 out of 1.0. This indicates that, in this simple example, based on:

- the scale chosen (the higher the better); and
- our evaluations of the criteria,

more national security advantage accrues from announcing that the stick will be used to attack the adversary than from keeping the stick's existence secret.

So, based on the answers, the President decides to make the announcement: Principles I and II have been followed. The Executive Branch has made a secrecy decision and the Legislative Branch will be informed of it and its attendant components in greater

Criteria *(value)*	**True** *(1)*	**False** *(0)*	**Detailed** *(varies)*
Announcement of the operation will not affect its probability of success. (weight = .3)	X .3		Means that more criteria and additional analysis are needed
Announcement of the operation will not invite a pre-emptive attack by the adversary. (weight = .3)	X .3		Means that more criteria and additional analysis are needed
Announcement of the operation will cause the adversary concern, negatively affecting his decision making process (weight = .2)		X 0	Means that more criteria and additional analysis are needed
Announcement of the operation will cause the enemy to expend resources to protect himself (weight = .2)	X .2		Means that more criteria and additional analysis are needed
Total Score	**.8**		

Figure 1. Decision Matrix.

Reuters

The President and his cabinet make daily decisions about what national security information will be divulged through cost-benefit analysis.

(classified) detail, based on the need of the people's elected representatives to know. Also, to a certain degree, the people themselves are informed when they hear the President's declaration.

Since the President has now decided that making an open declaration about an impending operation will enhance our national security advantage, we must apply Principle III. Now we must assess other aspects of the information operation and determine what secrecy levels need to be applied. A similar matrix using different criteria can be used to assess just how much secrecy should surround the associated intelligence, weapons modification and unit operations aspects of the "stick attack." There will probably be some aspects that will be protected at high levels of secrecy: for example, plans identifying operational components—attacking units, timing, tactics and departure points. Items that are associated with units that will conduct the attack but that are not, in themselves, classified—for example, scheduling the units for special training in stick use—will be subject to operations security review and monitoring. We don't want unclassified signatures and observables associated with stick training to give the adversary any clues that identify the stick as the weapon to be used, or the nature and timing of the attack.

We could also develop a matrix that examines the use of stick technology in this situation to determine whether or not more advantage accrues from using this technology. We might find that the stick relies on technology that at one time was highly sensitive, perishable and expensive to develop. Now, however, a better technology has emerged, so nothing is lost by exposing the older technology that supports the stick. This sort of assessment must be done before the President decides whether or not to announce the stick operation, because the attendant costs of exposing the technology should be a significant factor in the President's decision.

Similarly, we would construct a matrix that assesses the advantage accrued from protecting the security level and types of intelligence needed but, in the interest of brevity, this will not be discussed further. The point is that determining the type of secrecy needed, as well as the inter-relationships among intelligence, operations, weapons capabilities and public affairs or "strategic communications" is possible using simple analytic techniques that allow a repeatable and verifiable result.

Sticks (and Stones…and Words, too)

Hopefully, this article has served to remind us that secrecy has a critical and fundamental role to play in our national security affairs. In using secrecy as a national security tool, there are several principles that should be followed, as outlined herein. There are also simple analytical techniques that can be used to determine whether something should be considered secret and how secret it should be. These techniques are best developed individually and applied to a particular situation. If we "generalize" them, we run the risk of over-classifying the operation, which causes the whole "trust" question to re-enter the equation.

Here's a final thought. Our ability to view near-instantaneous visual and audio coverage of the pronouncements of international leaders, as well as other soul-stirring events, will improve dramatically in the coming years. These pronouncements can cause emotions of the watcher/listener to be quickly stirred, and actions quickly taken, based on those emotions. It is thus prudent to decide carefully whether what we say, how we say it and indeed, if we say it, will cause us to gain or lose national security advantage. We can control what we say and when we say it, but we can't control how those hearing the message might react. We ought to then, at least, be able to think through what their reactions might be, and determine if we're better served to say nothing at all. Silence is said, after all, to be golden.