THE ROLE AND NATURE OF ANTI-TAMPER TECHNIQUES IN U.S. DEFENSE ACQUISITION

Lt Col Arthur F. Huber II, USAF and Jennifer M. Scott

Military technology can be compromised following foreign sales to an ally, accidental loss, or capture during a conflict by an enemy. Because U.S. military hardware and software have a high technical content that provides a qualitative edge, protection of this technological superiority is a high priority. Program managers can mitigate such risks with a relatively new set of technologies inclusively known as “anti-tamper.” Program managers need to know the state of the art in anti-tamper technology and of the emerging DoD and U.S. Air Force policy on its use. This article covers anti-tamper policies; explains how, where, and when to insert these technologies; and describes some anti-tamper technologies now in use.

At a time of some future conflict The Ops Center was alive with the buzz created from the most recent news flash. The first loss in the war of a Banshee UCAV (uninhabited combat air vehicle) was causing a bit of consternation. The loss itself was unfortunate enough, although some were taking solace from the fact that it didn’t come about as a result of enemy fire. Instead, a failure of some sort—likely an engine malfunction—had resulted in the aircraft going down while on a deep strike escort mission.

While the continued conduct of the strike occupied the thoughts and energy of most in the room, a small contingent was crowded around a screen where the latest overhead imagery was being displayed. The initial reaction was one of surprise and then muted murmurings. If the imagery was to be believed, it was showing that the aircraft had survived the resulting crash in rather good condition. Although most of the nose and control surfaces were damaged beyond repair, the fuselage itself was fairly intact. One sidebay weapons door appeared to be flung to the side and there on the ground in full view was an advanced AIM-172 air-to-air missile. And apparently it was undamaged!

This new missile variant had been developed in response to the latest electronic countermeasures (ECM) deployed on the enemy's fighters and now it appeared he was going to gain access to the missile intact. While the new missile's capabilities against ECM were judged very effective, they were considered "fragile" because they depended heavily on special software algorithms contained in the missile's processor. If the enemy were able to recover the processor and download the operational flight program (OFP) containing these algorithms, then as everyone knew, his ECM system could be easily updated to defeat the missile. The air superiority that had been gained over the past few days of the war would be jeopardized very quickly.…

While this scenario at first blush might appear to be the stuff of science fiction, it is a vital concern today. The loss or compromise of critical U.S. technologies is a constant threat and one that our operational forces take very seriously. Unfortunately, protection of our weapon systems through inherent design has not been the standard practice for industry weapons makers nor of their government partners, that is, our fellow acquisition program managers. However, changes in technology, in the military and political environments, and in defense acquisition policies favor an approach to weapons systems development that addresses this potential weakness. The name for this new approach is "anti-tamper."

WHAT IS ANTI-TAMPER? WHY HAVE IT?

Anti-tamper (AT) is defined as the systems engineering activities intended to prevent or delay exploitation of essential or critical technologies in U.S. weapon systems. According to Department of Defense (DoD) 5200.1-M, an essential or critical technology is one that "if compromised would degrade combat effectiveness, shorten the expected combat-effective life of the system, or significantly alter program direction." Access to such information could force undesirable changes to tactics and concepts of operations (conops), premature retirement of a weapons system, or major system design changes to regain some level of effectiveness.

The use of AT protective techniques will vary depending on the technology being protected. For example, state-of-the-art technology of a critical nature typically requires more sophisticated AT applications. Some examples of AT techniques include software encryption, integrated circuit protective coatings, and hardware access denial systems.

Until most recently, documented U.S. defense policies say little specifically about AT. Accordingly, there has been limited motivation for, knowledge of, or enthusiasm by program managers to incorporate AT techniques into the weapon systems whose development they oversee.

We believe, however, that even without specific language mandating the use of AT techniques, the direction that has existed provides ample reason for program managers to consider incorporating them. For an example of such direction we need look no further than DoD 5200.1-M, which says in part that program managers are to "selectively and effectively apply security countermeasures to protect essential technology." The manual emphasizes that such countermeasures are "required to prevent foreign intelligence collection and unauthorized disclosure of essential program information, technology, and/or systems." Furthermore, this protection is "mandatory for use by all of the DoD components."

Now one might argue that the manual's original intent in making these statements was solely to focus our community on the importance of developing a robust program protection plan that affords adequate acquisition program protection. The program protection plan defines and refines a system security baseline for the implementation of security countermeasures and to man-age security costs as well as risks through-out the life cycle of the system. Program protection planning provides program managers, system managers, and users with an overall view of system-specific threats.

Traditionally, the program protection plan has been interpreted to mean a set of processes and infrastructure that guard or limits the exposure of information about critical technologies or operational employment schemes during the development and initial fielding phases of a system's life cycle. Such a perspective is true enough, but incomplete. It fails to recognize the cradle-to-grave perspective that acquisition personnel are to take when developing a new weapon system and sustaining it.

As defined by DoD 5200.1-M, acquisition program protection "integrates all security disciplines, counterintelligence, and other defensive methods to deny foreign collection efforts and prevent unauthorized disclosure to deliver to our forces uncompromised combat effectiveness *over the life expectancy of the system"* (emphasis added). Obviously, from this last statement, it is clear that protection of critical technologies extends well into the deployment phase of a weapon system and even unto its retirement. Thus, we argue that a broader interpretation of DoD guidance is perfectly legitimate and within the spirit and intent of the originators of these directives. Despite these arguments, it is clear from the current situation that such an interpretation does not flow down into program development strategies.

> "Some examples of AT techniques include software encryption, integrated circuit protective coatings, and hardware access denial systems."

WHY EMPHASIZE ANTI-TAMPER NOW?

The primary goal of AT techniques is to protect the combat advantage of the U.S. warfighter. This goal is accomplished by inhibiting exploitation and the development of countermeasures against critical U.S. technologies.

Within the past few years, U.S. policy has strongly encouraged the sale or transfer of certain military equipment to allied and friendly foreign governments. Increasingly, this equipment contains the latest in U.S. technological advances. Whereas in the past, U.S. policy has been relatively reluctant to permit such sales, the current cost-conscious environment motivates the

The introduction of the AIM–9 air-to-air missile provided a performance advantage that far exceeded its U.S. designers' expectations.

leveraging of reduced unit prices that is afforded by increased production quantities. Additionally, the DoD is seeking increased foreign participation in acquisition programs from the requirements definition phase through production, fielding, and life-cycle management. While these efforts have the potential to enhance interoperability, standardization, and commonality, reduce unit costs, and strengthen U.S. industry, they also risk making critical U.S. technologies vulnerable to possible exploitation.

Another threat that increases the opportunities for exploitation is the increased exposure of U.S. weapons and the technologies they contain during contingency operations. As has been widely reported, U.S. forces are now deploying abroad at a much higher rate than at any time during the Cold War. Invariably, as was demonstrated by the shootdown of Capt Scott O'Grady, military systems will be lost in battle or by accident. There is no guarantee that such losses will be mitigated by damage to the equipment and in most

The Soviets were able to acquire the AIM–9 air-to-air missile technology and quickly reverse-engineer it into an AIM–9 clone.

cases we must make the assumption that such systems have been compromised.

Lastly, the threat of espionage has not withered with the demise of the former Soviet Union. In fact, the “rainbow threat” makes counter-espionage activities even more difficult today than during the Cold War. Still, our experiences during that period provide ample evidence that our technological advantages can be compromised. As an example, the *Journal of Electronic Defense* reports that in the 1950s the introduction of the AIM–9 air-to-air missile provided a performance advantage that far exceeded its U.S. designers’ expectations. Yet the Soviets were able to acquire the technology inherent in this missile and quickly reverse-engineer it into an AIM–9 clone known by the NATO code name of AA–2 “Atoll” (Taylor, 1999).

Incorporating Anti-Tamper

The process for incorporating AT techniques rests upon the firm foundation of the systems engineering discipline. As with all complex engineering tasks, if one is to succeed in developing a solution to satisfy some need, the need itself must be thoroughly understood and properly translated into performance and technical requirements. The means by which we determine what, if any, AT techniques should be incorporated into a weapon system and how is no different. Figure 1 illustrates the process for determining AT requirements.

The process of interest can be divided into two main parts: the front half, which involves developing an estimate of the means and probability of exploitation, and

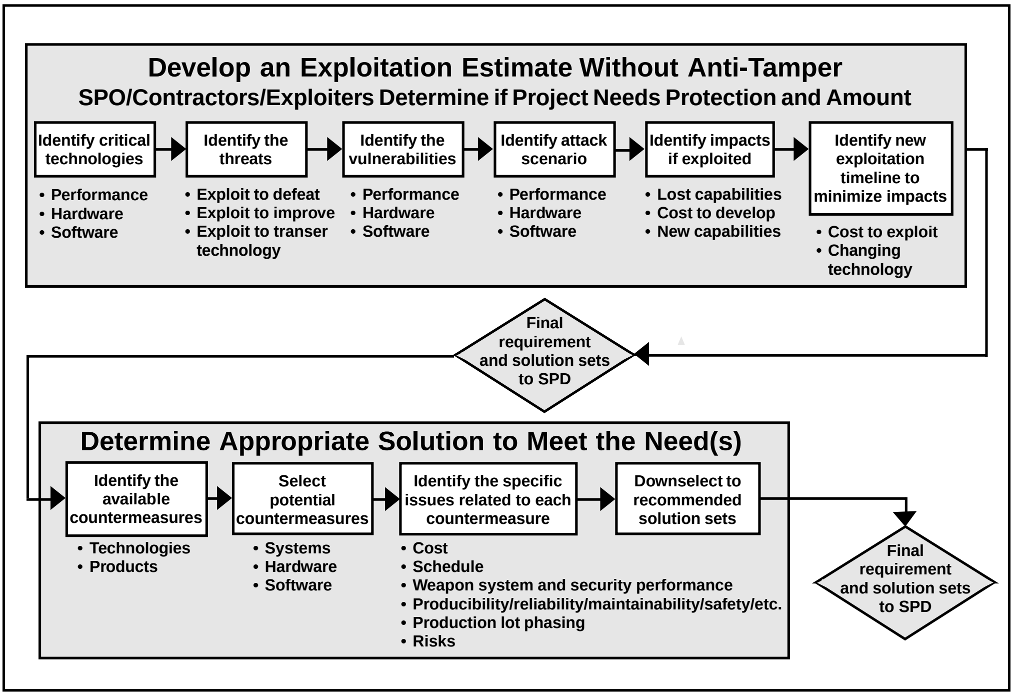
Develop an Exploitation Estimate Without Anti-Tamper
SPO/Contractors/Exploiters Determine if Project Needs Protection and Amount
Identify critical technologies
• Performance
• Hardware
• Software
Identify the threats
• Exploit to defeat
• Exploit to improve
• Exploit to transer technology
Identify the vulnerabilities
• Performance
• Hardware
• Software
Identify attack scenario
• Performance
• Hardware
• Software
Identify impacts if exploited
• Lost capabilities
• Cost to develop
• New capabilities
Identify new exploitation timeline to minimize impacts
• Cost to exploit
• Changing technology
Final requirement and solution sets to SPD
Determine Appropriate Solution to Meet the Need(s)
Identify the available countermeasures
• Technologies
• Products
Select potential countermeasures
• Systems
• Hardware
• Software
Identify the specific issues related to each countermeasure
• Cost
• Schedule
• Weapon system and security performance
• Producibility/reliability/maintainability/safety/etc.
• Production lot phasing
• Risks
Downselect to recommended solution sets
Final requirement and solution sets to SPD

Figure 1. Determining Anti-Tamper Requirements

the back half, where one determines an appropriate solution to the need once it has been properly characterized. The first main part is depicted in the top half of Figure 1 and consists of six steps. These first six steps are usually performed by the contractor in cooperation with government engineers.

The first of these steps is to identify the critical technologies that are under consideration for design into a weapon system. What constitutes a "critical technology" was defined earlier. Critical technologies include both software and hardware. Once these technologies have been identified, the "threats" to them are usually ascertained through some process involving "red-teaming" or scrutiny by those experts in friendly and adversarial exploitation. This step consists not only of identifying who might be interested and capable of exploiting identified critical technologies, but why and how they might be exploited. Technologies can be exploited to determine how they can be defeated or how they can be reengineered and improved upon.

According to DoD 5200.1-M, when a program contains critical technologies that may require protection:

> …a multidisciplinary counterintelligence threat assessment and a risk assessment are conducted. These assessments provide the basis for any decision pertaining to the protection of the [critical technologies] as part of the overall risk management strategy and the implementation of cost-effective risk mitigation measures (i.e., countermeasures).

It is important to emphasize here that as the DoD manual implicitly recognizes, there exists no need to consider the incorporation of AT techniques absent a critical technology or threat. Only those systems that contain critical technology need go through this process.

The next two steps consist of identifying both vulnerabilities of critical technologies to exploitation and the actual means by which they might be exploited. Again, these assessments must look to the hardware and software aspects of a system and their relationship to system performance. These steps are critical to the design efforts going into the weapon system proper, since they usually indicate if and where measures must be taken to protect the constituent critical technologies. Performing these steps may also provide important insights—for example, that exploitation may be possible but very difficult. This information can be extremely useful for tradeoffs to be conducted later in the process.

While understanding how a critical technology can be exploited is very insightful, so is projecting what the impacts would be if exploitation efforts were indeed successful. For example, if a critical technology is exploited, it may result in countermeasure developments that render the weapon system performance inadequate to do the job. By the same token, exploitation may not result in lost capability if other factors are important to the realization of a weapon system's full performance potential. Another factor that should be considered is the cost to develop replacement technology or to find other means to regain lost military advantage. Such data can be important for determining if the cost of incorporating protective schemes are worthwhile compared to the cost of measures that must be taken once a technology is compromised.

The last step in the front half of the requirements process is to assess possible exploitation timelines that serve to mitigate the need for, or required amount of, AT necessary for a weapon system. To illustrate, consider the impact of the pace of technological advancement in the microprocessor field. When a certain microprocessor, let us say an application-specific integrated circuit (ASIC), is designed into a weapon system, it may indeed represent a critical technology. But when one considers that similar commercial technology will match and overcome the ASIC's performance capabilities within 3 to 5 years, it may not make much sense to invest heavily in its protection through AT. The technological advantage will be lost in a relatively short amount of time through means available on the open market.

In contrast, consider the case of protection of software through encryption. Use of more sophisticated means for encryption may not render a software code absolutely secure, but it might increase the time it takes to break the encryption code by an order of magnitude—ensuring that the weapon cannot be exploited during its expected life. (A bit more detail on this form of AT will be discussed below.) Again, such information becomes very important in the tradeoff process for choosing and incorporating affordable AT techniques.

Once the first six steps of the process are complete, then a preliminary requirement for AT can be stipulated. Like all requirements in the weapon system development process, the AT requirement should not be considered absolute, but is something that must be balanced with cost, schedule, and military utility. Anti-tamper is not immune to tradeoffs that must be made as mandated by the policy of cost as an independent variable (CAIV).

The second main part or back half of the requirements process consists of four steps. The first of these is to identify AT techniques that are available to counter the exploitation threats. The nature of the critical technologies requiring protection will naturally provide a first filter for those techniques that may have application. At this stage the alternatives being considered may be quite different even if they have the same end result, that is, to inhibit exploitation. The second step is to select a preliminary set of potential countermeasures that are identified for more in-depth analysis. This first "cut" can usually be accomplished by eliminating those options whose affordability or efficacy are clearly unattractive compared to the other options. Typically a top-level look at the countermeasures proposed will surface relative strengths and weaknesses that facilitate this initial tradeoff.

"Like all requirements in the weapon system development process, the AT requirement should not be considered absolute..."

During the third step a traditional engineering design analysis is conducted in which all considerations are accounted for and evaluated. On the weapon system design side such considerations include life-cycle cost, implications for schedule (both development and production), impact on weapon system performance, ease of manufacture, reliability and maintainability, and safety. But a proper analysis also accounts for the relative merit of an AT technique for inhibiting exploitation, the anticipated timeline and cost that exploitation efforts will take, and the likely time-frame over which the technologies to be protected will remain critical or essential. For example, if a program only gains five years of protection from AT for a $10 million investment and the program is only spending $50 million on the entire RDT&E process, one may question the wisdom of spending the additional 20 percent for such limited results. However, if that same technique could give another program 10 years of protection for the same cost and if the total program budget is larger, then the relative benefit appears much more attractive.

> "The last step in the AT requirements process is final selection of the favored solution set."

To systems engineers, this evaluation methodology is nothing new or unfamiliar. It simply incorporates another "performance" requirement that is subject to the same kinds of analyses and tradeoffs that they are used to making. It may make final design choices a bit more complex, but it is no less subject to CAIV considerations as any other decision in the engineering design process.

The last step in the AT requirements process is final selection of the favored solution set. This solution may not be unique; another choice may achieve similar results at a similar cost. The dimension that wins the day may not be intuitively obvious, and that is why a thorough analysis should not be overlooked. It does little good to protect one avenue of exploitation if another is left open. As the adage goes, putting a special lock or bolt on the outside of the front door will not protect the back gate.

ANTI-TAMPER TECHNIQUES

For self-evident reasons, a detailed description of AT techniques can not be presented in an unclassified forum. It is U.S. policy to acknowledge that AT techniques are incorporated into the designs of its weapon systems, but to say nothing of their detailed nature. Many techniques are "fragile" in that the very knowledge of their specific application to protect a particular technology will greatly aid the exploitation process. No AT technique is fool-proof, and it defeats the purpose of incorporating it if an adversary is tipped off to what he is dealing with as he attempts to exploit the technology that has fallen into his hands. Since these techniques are not fool-proof, an "onion layered" approach may be necessary. Generally speaking, overlaid techniques provide more robust protection.

Nevertheless, it is possible to list a few generic examples that illustrate the kinds of options available to the program manager. These examples include:

- nonetchable thin opaque coatings applied to semiconductor wafers;
- self-destructing components; and
- cryptography to include encryption and decryption.

Coatings serve to make it very difficult to extract or dissect microelectronic components without greatly damaging them in the process. Self-destructing components may seem akin to the assignment tapes from the Mission Impossible series, yet in their essential respects they really are no different. After use or when exposed to certain environments, devices employing this form of AT damage themselves beyond reconstruction. However, a lesson learned from this technique is that employing it can have important implications for system operation and maintenance. For instance, if a system needs to go to a depot for repairs, it may be difficult to remove a cover or open a lid if an explosive is primed and ready to erupt upon doing so.

We can examine the last example—encryption—in more detail because it is a common technique found in the commercial as well as military world to protect software code and various forms of communication. Encryption can be defined in simple terms as the scrambling of instructions to make them unintelligible without first being reprocessed through some sort of deciphering technique. Anyone looking at encrypted data sees only cipher text, that is, a bunch of nonsense letters, numerals and symbols. The mathematical formula for accomplishing the deciphering process is an algorithm that takes time to solve. Depending to some degree on the type of algorithm used, the larger the number of bits used in the encryption process, the longer the time it will take to complete the deciphering process. The adjacent table provides some insight into the nature of this relationship (Krey, 1997). Obviously, in this example, the bit length the designer will shoot for will depend on what the technology will support for a given engineering application, the associated cost, the nature of the exploitation threat, and the anticipated time the protected information is expected to remain critical.

LESSONS LEARNED

A number of acquisition programs have already embraced AT techniques to make

Table 1. Code Breaking Times

No. of bits	Time
40	2 seconds
56	35 hours
64	1 year
80	70,000 years
112	10^{14} years
128	10^{19} years

their weapon systems more secure. Such action has facilitated the process to permit sales of these systems to allies and other foreign customers. One of the lessons learned from these programs is that incorporation of AT after the system design has been frozen is extremely expensive. It is not that all AT techniques are in themselves expensive, but their affordability is critically dependent on when they are introduced into the design process. If AT is treated as a performance requirement from the beginning, it is much easier and cost-effective to incorporate as compared to "bolting it on" later.

Another lesson learned is that system engineers should thoroughly explore the use of existing AT applications before committing to development of a brand new technique. Such "re-use" will often fulfill a requirement and obviate the need to "reinvent the wheel." For example, algorithms used for encryption can be modified slightly to provide a completely different type of protection than was originally envisioned.

"Unfortunately, few have arrived at the enlightened position that AT is a viable option to fulfill broadly applicable program protection policies."

Still another lesson learned is that many program managers will not address AT concerns unless the need is specified within program management directives or operational requirements documents.

Unfortunately, few have arrived at the enlightened position that AT is a viable option to fulfill broadly applicable program protection policies. The short-term answer to this dilemma is to have the operational requirements development community specify the need to protect critical technologies inherent in weapon systems from compromise or reverse engineering. Alternately, the program management directives can be used to task program managers to do the same. Unfortunately, these actions may be the only way to ensure adoption of AT techniques until they enjoy more widespread acceptance.

Policy Update

A big boost for the AT cause came about on February 11, 1999, when Jacques Gansler, Assistant Secretary of Defense for Acquisition and Technology, signed out a memorandum fostering implementation of AT techniques in military acquisition programs (1999):

> The Department seeks to preserve the U.S. and [friendly] Foreign Governments' investment in critical technologies through implementation of Anti-Tamper (AT) techniques and practices…Anti-Tamper is based on existing DoD5200.1M program security requirements… Once [a new policy is] approved, AT will be incorporated in new programs and modifications to programs where appropriate.

The memo stipulates that the director for Strategic and Tactical Systems (S&TS) is to assume Office of the Secretary of Defense oversight, coordination, and policy responsibilities for AT within the DoD. The memo further directs that S&TS

convene an integrated product team to prepare a DoD AT policy. Additionally, Service, U.S. Special Operations Command, Ballistic Missile Defense Organization, and Agency acquisition executives are to assess all acquisition category weapon system programs to determine the extent of AT implementation and to report on their observations.

In parallel, efforts are under way to revise DoD 5000.1-M to explicitly state that program managers will assess AT for incorporation into their weapon system acquisitions as part of the program security process. Once accomplished, program managers may elect not to incorporate AT techniques into their weapons developments, but the onus will be on them to demonstrate why and how they intend to address the exploitation threat.

SUMMARY

From the foregoing discussion it should be clear that the incorporation of AT techniques provides significant benefits.

- Anti-tamper prevents or mitigates the unauthorized or inadvertent disclosure of U.S. technology as well as its exploitation.
- Anti-tamper protects the U.S. warfighter from countermeasures development.
- Anti-tamper enables foreign military sales to be consummated with greater confidence that U.S. technologies will not be compromised.
- Anti-tamper reduces the burden on the taxpayer by helping to sustain U.S. technological advantages.

At the beginning of this article we postulated a speculative future scenario in which advanced military technology was lost into enemy hands with the distinct probability that it would soon be compromised. Perhaps some will find such a scenario difficult to accept as possible or likely. For those who continue to resist the imperative for assessing what role, if any, AT techniques should play in their program, we offer up this historical vignette.

> "From the foregoing discussion it should be clear that the incorporation of AT techniques provides significant benefits."

In 1915 during World War I, Anthony Fokker, the great Dutch aviation pioneer, revolutionized aerial combat when he developed a synchronizing system to permit a forward-firing machine gun to shoot through an airplane's nose-mounted whirling propeller blades. Prior to Fokker's invention, airmen wishing to engage enemy aircraft were forced to armor their wooden propellers with steel liners and risk hitting them or fire their guns over the top or to the side of the aircraft, which was much less accurate. With Fokker's mechanism, German aircraft gained the advantage over the Allies and established air superiority.

But the advantage was short-lived, because soon thereafter a German pilot was captured with his aircraft behind French lines when he became lost in bad weather. The Allies quickly copied the Fokker mechanism and even improved upon it by devising a hydraulic synchronizer that interrupted the gun's firing pattern so bullets were prevented from being fired when a blade passed through the line of fire. With equivalent capability in hand, the Allies quickly reestablished parity in the air (Hildreth and Nalty, 1969).

The reality of exploitation is inescapable. It is supported by historical precedent and current threat assessments. Anti-tamper technology is an affordable means to provide life-cycle program protection to essential or critical U.S. military technologies. Recently established DoD policy mandates that program managers assess whether AT techniques are appropriate for their acquisition programs, be they new or upgrades. The time to act is now.

Lt Col Art Huber, U.S. Air Force, is presently serving as Commander, 413th Flight Test Squadron, Edwards Air Force Base, CA. The material provided in this paper was developed during his previous assignment to the Pentagon in the Office of the Assistant Secretary of the Air Force (Acquisition). He has presented and published a variety of papers dealing with technical and military topics. He is a graduate of DSMC's APMC 97-3 and the USAF Test Pilot School. He has an M.S. degree in aerospace engineering from the University of Notre Dame as well as bachelor degrees in government and international relations and aerospace engineering, also from Notre Dame.

(E-mail address: art.huber@edwards.af.mil)

Jennifer M. Scott is currently an Air-to-Air Missile Research Analyst for Analytical Services Incorporated in Crystal City, VA. She is responsible for assisting the Program Element Monitor in the acquisition and monitoring of the AMRAAM (Advanced Medium-Range Air-to-Air Missile) Program. She has a Bachelor of Science degree in mathematics and a minor in physics. Directly after obtaining her Bachelors degree she went to work for ANSER as an intern working with the F-15 and F-16 programs. After her intership, she began working the Anti-Tamper program.

(E-mail address: scottjm@pentagon.af.mil)

REFERENCES

DoD 5200.1-M, *Acquisition Systems Program Protection*, the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, March 1994.

Gansler, J. S. (1999, February 4). *Implementation of anti-tamper (AT) techniques in acquisition programs* (DoD memorandum).

Hildreth, C. H., & Nalty, B. C. (1969). *1001 Questions answered about aviation history.* New York: Dodd, Mead & Company.

Krey, M. (1997, October 1). Decrypting the verbiage of encryption. *Investors' Business Daily.*

Taylor, W. (1999, February). Understanding the infrared threat. *Journal of Electronic Defense,* 35–43.