
Technology Transfer—Doing It Right!

By

Ronald Tom
The Rail Company

Today's global climate requires the United States to continue its efforts to adapt and strengthen existing alliances and coalitions to meet the challenges of an evolving and dynamic security environment. Technology transfer plays a key military role in supporting a national security strategy that embraces the building of coalitions and the shaping of the international environment to protect United States interests. The 1997 Presidential national security strategy document, *A National Security Strategy for a New Century*, states that "Through means such as . . . defense cooperation and security assistance . . . our armed forces help to promote regional stability, deter aggression and coercion, prevent and reduce conflicts and threats, and serve as role models for militaries in emerging democracies."

According to its definition in the *Security Assistance Management Manual (SAMM)*, technology transfer is the process of transferring, from an industry in one country to another or between governments themselves, technical information and know-how relating to the design, engineering, manufacture, production, and use of goods. Technology transfer is here to stay and will be important as the level of defense and industrial activity increases in the international arena. The *National Security Science and Technology Strategy 1995* states that while recognizing the risks, "This Administration is committed to striking a balance between sharing our technology and protecting it so that the benefits continue to outweigh these risks. . . . We will continue to encourage international cooperation in defense technology because the payoff can be great. . . . And we will continue to strike a judicious balance between risks and benefits to ensure that all our international science and technology cooperation activities make positive contributions to our national security and economic well-being." Properly planned and implemented international cooperative program activities will contribute significantly to the achievement of United States national security, and to science and technology strategic goals and objectives. Paradoxically, disjointed or haphazard planning could result in serious damage to United States national security, which is characterized by the loss of critical technology, compromise of operational capability or tactical advantage, fiduciary shortfalls or waste of funding, and possibly the unnecessary loss of lives on the battlefield.

The SAMM also points out that "before a decision is made to transfer technology, the USG must (1) consider whether the technology should be shared with the country concerned, and (2) conduct a policy review, technical evaluation, and mission impact and intelligence assessment of the proposed transfer." However, far too often, the factors being considered for a technology transfer decision are generated without the benefit or understanding of the general concept of the international aspects of a program.

Regardless of the nature of any international defense cooperative effort involving the United States (i.e., security assistance, scientist and engineer exchange, cooperative research and development, etc.), it is imperative that thorough internal coordination be accomplished among all activities involved in international program support to minimize the risks of inadvertent technology loss. This coordination effort should include, but not be limited to, the following types of activities:

- Political-Military Affairs
- Security Assistance

-
- Cooperative Research and Development Programs
 - Intelligence (includes all disciplines)
 - Strategy and War Plans
 - Project Management
 - Training (as appropriate)
 - Legal (International Law)

Examples of the potential for inadvertent loss of critical technology due to the lack of thorough coordination are reflected in the following cases:

- *Case #1* involves separate and independent international programs, specifically a weapon acquisition program and a data exchange annex (DEA) activity. The essential program information, technology, and system (EPITS) or the most critical technology(ies) of any classified acquisition program could clearly and easily be jeopardized, albeit inadvertently, through a related DEA action if the technical project officer is not aware of the EPITS or does not coordinate with the appropriate program executive officer (PEO) or program manager (PM). In this case, an inadvertent disclosure of the EPITS would not only compromise critical technology, but also leave a weapon system open to the possible development of countermeasures. The successful development of countermeasures jeopardizes the capability of the weapon system and the monetary investment in the program, and would likely result in the additional investment of resources (manpower and funding) to develop a counter-countermeasure.
- *Case #2* is somewhat related to the above scenario in that it deals with two weapons acquisition programs. Program A leverages technology from Program B. The leveraged technology is an EPITS; however, in Program A, it is not deemed critical technology. In this situation, the PMs of both programs must coordinate closely to ensure Program A does not transfer the leveraged technology without the concurrence of Program B. To do otherwise could have an adverse impact on Program B similar to that discussed in Case #1.
- *Case #3* deals with munitions licenses that are submitted through and are under the purview of the Department of State. Personnel coordinating Service and ultimate DoD positions on munitions license application requests by U.S. industry contractors could jeopardize critical technology and/or information if they are not aware of the extent of its application in defense weapon systems. If a licensing official is not aware of the use of a specific technology and fails to coordinate correctly within a Service, an approval position could result, thereby risking the compromise of that technology and/or information which may be critical to one weapons program but not necessarily to another project.

Finally, decisionmakers in international activities must ensure that established policies can be implemented by those charged with carrying out the program. The analogy is: "Do not establish rules that cannot be enforced." This facet of any program should be obvious to all involved; however, it is often overlooked or taken for granted. The following examples illustrate the importance of ensuring that implementation of an international activity can be accomplished within the conditions and limitations set forth in any policy:

- *Case #1* addresses the controversial and sensitive issue of software and software source code (SSC), which is usually restricted from release in conjunction with any foreign military sale (FMS) case. However, any policy which permits the transfer of an in-country reprogramming capability to FMS customers for their user data files

(UDFs) with the proviso that no software source code (SSC) be released makes implementation impossible to execute. SSC is required to provide this capability to the FMS customer. This inconsistency would have been avoided by proper coordination with the appropriate program software engineers.

- *Case #2* centers on the training of foreign students as part of the “total package approach” for the sale of a weapon system. The general Department of Defense (DOD) policy on training consistently prohibits the release of United States tactics to foreign students, particularly when tactical United States Air Force (USAF) and USN fighter aircraft are involved. This limitation has made it virtually impossible for USN training commands to create a course of instruction to train foreign students on the proper operation of a United States fighter aircraft. Coordination with the appropriate training command prior to the establishment of policy would have addressed and resolved this discrepancy.

The engineering, disclosure, or international programs coordinator at the lowest level must understand the general concept, policy guidelines, and conditions under which the project is being executed. Interaction must not only be vertical and horizontal within a Service, but also include interagency coordination as necessary. It would not be imprudent to over-coordinate (in terms of activities, agencies, etc.) any effort that has international technology transfer implications.

The business of defense cooperation, whether it is security assistance or one of the plethora of related international activities, is the responsibility of every individual who remotely plays in the international arena. Just as the security or technology transfer/foreign disclosure specialists play a significant role in international activities, the engineer or scientist or technical project officer has an equally significant responsibility to provide decisionmakers with the best available information to make decisions in support of our national security strategy goals and objectives. We do not necessarily have to re-invent the proverbial “wheel” by designing new structures and policies. We only have to do our jobs thoroughly and efficiently!

ABOUT THE AUTHOR

Ronald Tom, a retired United States Army Lieutenant Colonel, works for the Maryland-based RAIL Company as an International Programs specialist. His last assignments in the Army were in the Pentagon as the Army’s Chief for Technology Transfer (Office of the Chief of Staff for Intelligence) and Politico-Military Officer (Officer of the Deputy Chief of Staff for Operations). Mr. Tom’s background includes assignments in strategic and foreign intelligence, and as a foreign area officer with specialty in China as well as the Pacific Rim countries. During his recent tenure with RAIL Company, Mr. Tom has supported United States Army and Navy programs in the areas of foreign disclosure, technology transfer, technology security, and export policy.