Risk Management and National Reconnaissance From the Cold War Up to the Global War on Terrorism[1]

By Dennis D. Fitzgerald

The Executive and Legislative branches, subsequent to the 2004 Presidential election, focused on examining the Intelligence Community's structures, functions, and missions in light of the terrorist attacks of September 11, 2001. During these most recent reassessments, some have argued that the NRO has become risk averse, lost its technological edge, and lacks vision. In this article I will discuss the changing nature of risk and risk management as they relate to the NRO's mission, its technology, and its vision for national reconnaissance as we encounter the emerging national security challenges.

An important objective in implementing any realignment of Intelligence Community activities is to ensure there is an effective, efficient, and flexible application of resources in response to the wide range of both current and potential national security threats. As the National Reconnaissance Office (NRO) addresses the application of its resources to support the Global War on Terrorism, it is being faced not only with new emerging demands, but also with traditional demands, for its reconnaissance systems and intelligence output. However, the long-term fiscal experience has been one where the budgetary environment had been flat or declining. A strong correlation exists between the funding environment and the tolerance of oversight authorities for failures and the willingness of leaders to take risks.

By its nature, space reconnaissance is a high-risk enterprise. The technologies that are developed and employed define the state-of-the-art and are not commercially available. The history of the NRO is a story of consistently pushing technological boundaries to achieve breakthrough capabilities in the full spectrum of national reconnaissance systems and products. Pushing hard yielded many successes and innovations, but break-

[1] This article is an unclassified version of, "Risk Management and National Reconnaissance form 1960 to 2002," which CSNR published in the classified edition of *National Reconnaissance—Journal of the Discipline and Practice*, (Issue 2003-C1).

throughs sometimes came at a price. The NRO also suffered its share of setbacks and disappointments. These setbacks are endemic to the high-risk nature of the national reconnaissance enterprise and are a natural consequence of constantly redefining the state-of-the-art. As we explore risk management and national reconnaissance, we first need to frame the fiscal environment and define risk.

The Fiscal Environment

From the end of the Cold War until the events of September 11, 2001, the NRO operated in a constrained fiscal environment. This environment also was shared by other elements of the Intelligence Community. However, while the impact on the other Intelligence Community elements generally was immediate, the NRO did not show evidence of the impact immediately. The impact, however, was just as real and often far deeper. These other organizations are not as deeply involved in research, development, and acquisition as the NRO. Therefore, they generally experienced the budget impact in their current operations. In contrast, the NRO budget impact was directed in the areas of technological development and future acquisitions. This choice was made to avoid near-term degradation of national reconnaissance capability. The impact of the NRO's budget was delayed three to five years, and the impact became apparent when NRO systems and capabilities that were supposed to be ready for deployment were either delayed or not available. Another consequence of these budget reductions was that over time the national reconnaissance satellite constellation became more fragile. The budget reductions also put the NRO's space reconnaissance technological development at risk by eroding long-term investment in technology. This sets the stage for interaction with risk.

The Nature of Risk

Risk has multiple meanings and is dependent on a given set of circumstances at a specific point in time. Tolerance for risk is correlated directly with the operational environment, and this correlation is reflected in the NRO's history. Over the past four decades from the 1960s to the beginning of the 21st century, the risk environment has changed with regard to national reconnaissance programs.

When examining the issue of risk over this period of forty-five-plus years, there are two groups of actors who must be taken into consideration. The first group is internal to the discipline of national reconnaissance and includes senior NRO leaders, program managers, and the NRO's industry partners. The second group is external to national reconnaissance and is comprised of NRO oversight authorities to include the President, the National Security Council, and Congress. The interaction within and between these groups largely defines the level of acceptable risk and the tolerance for failure. To gain insight into the question of risk management for the NRO, it is useful when evaluating

the risk environment for the NRO over the past forty-five years to divide the period into four thematic eras: The Imperative for Intelligence; The Drive for Technology; The Expectation of a Peace Dividend; and The War on Terrorism.

The Imperative for Intelligence (1960–1970)

The first era, roughly 1960-1970, is defined by the intelligence imperative to collect national-level strategic intelligence on the capabilities and intentions of the Soviet Union and China. The NRO's operational emphasis was on obtaining reconnaissance imagery that could provide indications of military capabilities and intentions of the Soviet Union and China, specifically with regard to their strategic capabilities. At the time of the 1960 presidential election there was a public debate on whether the Soviet Union had surpassed the United States in terms of nuclear weapons and strategic delivery systems, specifically whether a "bomber gap" or "missile gap" existed. President Eisenhower lacked adequate and timely intelligence to provide him with insight into the strategic balance. The primary source of reconnaissance information came from politically and militarily risky U-2 overflights. These overflights came to an end in May 1960 when a U-2 piloted by Francis Gary Powers was shot down. Consequently, President Eisenhower found himself facing critical decisions related to the types and amounts of strategic weapons and delivery systems that were required to provide for the national defense, yet he was relatively blind in terms of timely and reliable intelligence on Soviet capabilities (McDonald, 1997; Pedlow & Welzenbach, 1998).

During this era, NRO leaders demonstrated a willingness to take significant technical and program risks because there was national-level support and a high degree of tolerance for failure among oversight authorities. In the 1950s the United States began to explore the possibility of conducting national reconnaissance from earth-orbiting satellites. Although the U-2 program was a success from its first flight in 1956, national leaders recognized that sooner or later the Soviets would develop countermeasures. Space-based reconnaissance systems were not yet ready in May 1960 when Powers was shot down. Project Corona, the film-return photoreconnaissance system, was in development and testing (along with other systems), but had experienced a number of technical failures. In fact, the program experienced twelve consecutive failures before the first mission returned film to Earth successfully in August 1960. Despite the repeated failures, this program remained a national priority for the Eisenhower administration, because that administration accepted the fact that failures inevitably occur during the development of new, high-risk systems and capabilities (Hall, 1997; McDonald, 1997).

There were other significant aspects of this era. Intelligence analysts were starved for data, so virtually every piece of collected intelligence carefully was reviewed, and every image that was produced was analyzed. The principal intelligence customers were national level policymakers including the President and the National Security Council.

The contractor base was small, in large part, because of the emphasis on secrecy and the resulting substantial security requirements (Laurie, 2001). In terms of the production of reconnaissance systems, a pipeline existed in which more than one copy of a system was built at a time. In the case of Corona there had to be a robust pipeline, because the first twelve either malfunctioned or ended up in the ocean. The lesson from this experience was that a production pipeline helps mitigate risk. In terms of funding, the NRO calculated the cost of a program and added twenty to thirty percent in anticipation of cost overruns (Kohler, 2005). This streamlined budget practice was possible, in part, because of the covert nature of the organization. There was limited oversight, and the NRO could buy its way out of a lot of problems without having to explain to Congress (Laurie, 2001). Finally, during this era, failure was often viewed as a learning experience both by NRO leadership and by the organization's oversight authorities.

The Drive for Technology (1970–1990)

The second era, roughly 1970-1990, was characterized by a drive for technology where enhancements to baseline systems and capabilities were aggressively pursued and developed. Specifically, enhancements to imagery systems included advancing from film-return to electro-optical systems and near real-time image transmission and processing (Helms, 2003). The NRO also improved SIGINT collection and processing capabilities (Hall, 1999). During this era the willingness to take risk by NRO leadership could be described as moderate, which also describes the tolerance for failure by NRO oversight authorities.

The 1973 Arab-Israeli War highlighted the urgent requirement for near-real-time imaging capability. Secretary of State Henry Kissinger, in consultation with President Richard Nixon, ordered the premature return of a film capsule in order to obtain battlefield imagery that was required to support diplomatic efforts. This requirement for near real-time imaging capability contributed to the transition from film-return systems to electro-optical systems.[2]

Intelligence analysts kept pace with the volume of collected intelligence until around the mid-1980s, when the collection capabilities of NRO systems advanced to the point where they overwhelmed analysts with data (Taubman, 2003). The number of intelligence consumers grew beyond just the senior levels of the Executive Branch to include a variety of Intelligence Community organizations who came to rely on this information to perform their missions. The contractor base was growing, which contributed to greater competition among contractors. There was still a production pipeline, and as new systems became operational, there invariably were design and technical problems and refinements that needed to be addressed. When failures occurred, NRO leaders and oversight authorities generally viewed them as the result of over-reaching in terms of attempting to extend the boundaries of technology.

[2] Source material is classified.

As a result of the successes and achievements of the first two eras, the NRO developed a reputation as an organization that was exceptionally successful at pushing the boundaries of technology and that always exceeded requirements. In these early years, the NRO never built systems to requirements, rather it built systems to the limits of what the technology would allow. This reputation and track record was, in no small part, because of the streamlined financial and oversight environment that existed. Key elements of that environment were adequate funding, the willingness to accept failure as a learning experience and a consequence of taking risks, and of pushing the limits of technology.

Expectation of Peace Dividend (1990–2002)

The third era, roughly 1990-2002, is defined by the expectation of reaping a peace dividend from saving as a result of the end of the Cold War. During this era the NRO was expected to continue to deliver the quantity and quality of intelligence data that national leaders had come to expect. This expectation and the resulting environment had the unintended consequence of reducing the resources that supported NRO research, development, and acquisitions. In turn, NRO engineers and program managers wanted to keep their programs alive, so they took on greater and greater risk. This increased risk to long-term operations and development was evident by behaviors that resulted in the acquisition of fewer spares, the reduction of testing and evaluation procedures, the shortening of systems integration times, and the lack of developing parallel high-risk projects. To complicate this situation, when the NRO was assuming greater risk, the national oversight authorities were reducing their tolerance for failure.

During this era, investment in capacity made in the 1980s resulted in ever more efficient and effective national reconnaissance systems. The sheer volume of imagery and SIGINT increased to the point that analysts became overwhelmed (Taubman, 2003). The military was also downsizing its forces at this time, and the reduction in the military's analytic workforce further exacerbated the problem of inadequate analytic capability to exploit advancing collection capabilities.

Other important changes also occurred. Following the successes of space systems in Operation Desert Storm, the NRO's primary customer base broadened and shifted from the Intelligence Community to the military. In industry, a period of consolidation among national security contractors radically changed the NRO's industrial base, and we are now approaching the end of that period. The production pipeline that existed during the first two eras disappeared, and the practice of procurement based on mean mission duration also came to an end. Instead, the NRO employed a process in which each system's functional availability is re-evaluated every year, and procurement is based upon mean life expectancy.

These risks were compounded when the NRO reformed its financial practices following the discovery in 1995 of $3.8 billion of forward funding.[3] The practice of forward

[3] The forward funding was a result of a number of contracting and accounting factors, including the use at the time of three district accounting systems. Other factors included disparities between budget allocations and contract obligations; disparities between contract obligations and execution rates; the withholding of award fees; and program delays. No funds were missing or misused.

funding provided a measurre of budgetary discretion and flexibility that assisted with risk management. However, oversight authorities objected to this practice and the NRO's senior leadership vowed, and has delivered on its assurances, that a similar situation would not happen again. One result of this experience was the transition from three accounting systems to a single integrated financial management system. In fact, the NRO was the only element of the Intelligence Community to successfully complete cash flow audits by an external accounting firm every year between 2000 to 2003.

In order to ensure that the NRO did not accumulate forward funding, and to be able to fund additional programs (particularly advanced research and development), the NRO developed an elaborate, detailed budget process that utilizes complex computer modeling and simulations that takes into account every piece of hardware and every line of code that is to be built. This acquisition methodology is particularly fragile when applied to first generation systems where there is little or no experience. When new systems push the state-of-the-art the amount of risk increases significantly, and some degree of failure is not only a possibility, it is virtually assured.

The War on Terrorism (2002 and Beyond)

The fourth and current era is defined by the War on Terrorism. This era entails a new operational environment and associated expectations regarding assured space reconnaissance capabilities. Current expectations are that there can be no coverage gaps in overhead intelligence collection capabilities because the military is heavily dependent upon NRO systems and products for planning and operations. The performance of NRO systems has been spectacular in terms of preventing the loss of lives, targeting of weapons with unprecedented accuracy, and obtaining a synoptic understanding of the battle space. For example, in Afghanistan and Iraq targeting is done with national reconnaissance assets because those assets can provide the geolocation that is required to target precision-guided munitions. SIGINT has also proven crucial in all aspects of military operations and planning.

This new environment in which coverage gaps are viewed as unacceptable has led the NRO to become increasingly conservative in terms of ensuring continued mission performance at a time when there is also tremendous pressure to move on to the next-generation systems. At the same time, intelligence analysts are being spread relatively thin and are now expected to pay attention to a broad range of targets in diverse geographic areas. In the meantime, other important targets are not getting the attention they require. This reduced attention translates into increased risk. The question for national and military decision makers and oversight authorities is how long can we tolerate this risk before we experience adverse consequences?

To summarize the present era, the willingness to take on risk by the NRO leadership is moderate. The primary customer is the military, and there is no production pipeline. The leadership is very tentatively moving the NRO toward a new budget and acquisition process. This change will reduce programmatic risks, but these steps cannot be sustained without the support of the Community Management Staff and Congress[4]. Presently, when funds are appropriated to the NRO, 100% of those funds must be obligated as planned which severely restricts the NRO's ability to manage risks across the national reconnaissance enterprise. Additionally, without adequate funding that includes program margin the NRO is constrained from aggressively pursuing new technologies.

At the same time it has become clear that tolerance for failure by oversight authorities has become virtually non-existent. Now when failures occur the issue is "Whom do we fire?" This causes one to wonder whether this trend eventually will lead to investigations and the potential criminalization of prudent high-risk engineering decisions that inadvertently result in failure for technical reasons. These trends will have a chilling effect on the willingness of an organization and its leadership to pursue programs with significant technical and financial risks. In turn, this will have the unintended effect of stifling innovation and creativity at a time when it is needed most.

Current Challenges

A comparison between the first two eras and the second two eras illustrates that during the first two periods, NRO oversight authorities recognized and accepted the reality that developing, deploying, maintaining, and improving a space-based national reconnaissance capability was a very high-risk enterprise. In contrast, during the latter eras much of the risk was implicit and driven largely by fiscal imperatives. In other words, cost became the primary decision variable and a number of programs and ground stations were consolidated or eliminated in the pursuit of lower costs. In several cases these decisions contributed to increased risk and vulnerability of the national reconnaissance satellite constellation and the supporting infrastructure.

Shrinking budgets are forcing the NRO to attempt to accomplish more with fewer resources, and without the security of production pipelines. For example, the Future Imagery Architecture (FIA) is a cost-driven system in which the system is being built to requirements rather than technical capability. However, with a shrinking budget and a mandate to accomplish more with fewer resources while being denied a production pipeline, the NRO has been forced to become increasingly conservative. In other words, the organizational imperative has shifted from advancing technology boundaries to meeting current mission requirements.

[4] The Community Management Staff (CMS) is being subsumed into the Office of the Director of National Intelligence (ODNI).

THE NRO and RISK: COMPARING FOUR ERAS

ERA	TIME FRAME	NRO WILLINGNESS TO TAKE RISK	OVERSIGHT TOLERANCE FOR FAILURE
Intelligence Imperative	1960-1969	High	High
Drive for Technology	1970-1990	Moderate	Moderate
Peace Dividend	1990-2001	High	Low
War on Terrorism	2002-?	Moderate	None

What Can Be Done?

The NRO's greatest asset continues to be the people in government and industry who do the research and development, acquire the systems, and fly the spacecraft. As a team, the people of today's NRO are as dedicated as any I have served with in my more than 25 years in the NRO. Today's workforce generally has more skills than the people I worked with 25 years ago in terms of the basic skills they bring into the organization. They tend, however, to be less experienced, and that presents a challenge because one way you obtain experience is by taking risks and exploring the unknown. But it is difficult to provide them with the room they need to gain valuable experience when the environment is risk averse in terms of technology and funding. The bottom line is that there is no shortage of good ideas in the NRO, but there is a shortage of funding.

Eight Rules for Managing Risk in National Reconnaissance Programs

A number of steps can be taken to avoid or mitigate some of the problems that I have identified. I offer eight rules to follow for building and managing realistic national reconnaissance programs:

1. **Avoid programs that require research and development in parallel with the program.**

   In the past, we almost always broke this rule. The problem is that if your research stalls so will your program, and that will leave you with a standing army burning money and going nowhere.

2. **Budget at 80% of the most probable cost for first-of-a-kind space systems.**

   There will be unforeseen problems with new systems, so plan for it, be proactive, and be prepared by ensuring there is margin in your budget over contract cost.

3. **Whenever possible, plan for a backup launch vehicle.**

   The launch vehicle has always been one of the highest risk elements of our programs. Launch failures (regardless of whether the payload is ours or someone else's) have an impact on schedules, and therefore cost, since the fleet has to stand down until the cause is determined and remedial steps taken to avoid duplicating the failure.

4. **Use multiple sources for high-risk components.**

   Generally, for budget reasons the NRO has not fully complied with this rule. Failure to adhere to this rule creates risk that must be mitigated in some way. When you are reliant on a single source for a critical component and the vendor fails, your program will stall and you will find yourself burning money and going nowhere.

5. **Test everything you can.**

   The space environment is especially hard on things built by humans and simulations are rarely an adequate substitute for real tests. There appears to be a "modern" trend to not build functional test assemblies to test hardware. This trend can be dangerous. Our experience has shown that simulators are seldom a substitute for real hardware when developing systems. On the ground a bad simulation or a failure to properly test can be a problem; in space it is generally a disaster because you cannot rework a system on-orbit to fix the things you forgot to test. Perhaps someday this will not be the rule, but until that day comes test and test again.

6. **Have sufficient test equipment.**

   Have enough equipment to test subsequent flight articles when the first one runs into trouble. We spent tens of millions of dollars buying more test equipment on a SIGINT program to avoid this problem. This was a worthwhile expenditure because when the first vehicle ran into problems we were able to use the second and third vehicles to try to see and understand what was going wrong.

7. **Allow for sufficient integration and test time.**

   We run into most of our surprises in the integration and test phase where almost everything is serial. A delay propagates through the schedule at a time when there is often no schedule margin left to work with. The NRO failed to adhere to this rule on a SIGINT program, and as a result we spent months testing the test equipment and software rather than testing the spacecraft.

8. **Manage your contractors aggressively.**

   You may not be their only customer, and their priorities may differ from yours.

Conclusion

The NRO looks forward to continuing to improve every aspect of the way we do business and to achieve the NRO vision of "One Team Revolutionizing Global Reconnaissance." The world is a significantly different place with different threats and challenges than in the NRO's formative years. If the NRO is to achieve its vision we will have to approach risk and risk management with the same commitment we had when we confronted the technical challenges of our early years. The NRO's primary objective should be to design, build, and operate best value, state-of-the-art national reconnaissance systems. I have every confidence that our people, both in government and industry, can excel in this endeavor.

References

Hall, R. C. (1997). "Post War Strategic Reconnaissance and the Genesis of Project Corona." In R. A. McDonald, 1997, *Corona: Between the Sun & the Earth—The First NRO Reconnaissance Eye in Space*, pp. 25-58, Bethesda, MD: American Association for Photogrammetry and Remote Sensing.

Hall, R. C. (1999, March-April). The National Reconnaissance Office: A Brief History of its Creation and Evolution. *Space Times*.

Helms, Richard, & Hood, William. (2003). *A Look Over My Shoulder: A Life in the Central Intelligence Agency*. New York: Random House.

Kohler, Robert. (2005). One Officer's Perspective: The Decline of the National Reconnaissance Office. *National Reconnaissance: Journal of the Discipline and Practice*, 2005-C1, pp. 35-44.

Laurie, Clayton D. (2001). *Congress and the National Reconnaissance Office*. Chantilly, VA: National Reconnaissance History Office.

McDonald, R. A. (1997). "Corona's Imagery: A Revolution in Intelligence and Buckets of Gold for National Security." In R. A. McDonald, 1997, *Corona: Between the Sun & the Earth—The First NRO Reconnaissance Eye in Space*, pp. 211-220, Bethesda, MD: American Association for Photogrammetry and Remote Sensing.

Pedlow, G. W. & Welzenbach, D. E. (1998). The CIA and the U-2 Program, 1954-1974, Washington, DC: CIA Center for the Study of Intelligence.

Taubman, Philip. (2003). *Secret Empire: Eisenhower, the CIA, and the Hidden Story of America's Space Espionage*. New York: Simon & Schuster.

Dennis D. Fitzgerald is the Deputy Director of the National Reconnaissance Office, a position he has held since August 2001. His most immediate prior assignment was as Associate Deputy Director for Science and Technology in the Central Intelligence Agency (CIA). Mr. Fitzgerald joined the CIA's Directorate of Science and Technology in 1974 and spent the majority of his career assigned to the CIA's Office of Development and Engineering (OD&E) with duty in the NRO. His many NRO assignments included service as the NRO's Acting Director between the retirement of Peter Teets and the appointment of Donald Kerr as DNRO, and Director, Signals Intelligence Systems Acquisition, and Operations with a concurrent appointment as CIA's Director of Development and Engineering. Mr. Fitzgerald began his professional career as a field engineer working on the Polaris and Poseidon missile program for Sperry Gyroscope.