Remarks by the Principal Deputy Director of National Intelligence
Dr. Donald M. Kerr

The Association for Intelligence Officers (AFIO)
Annual Intelligence Symposium

The Sheraton-Premiere Hotel
McLean, Virginia

October 24, 2008

AS PREPARED FOR DELIVERY

It's a pleasure to be with you all tonight, to celebrate the 34th Anniversary of the AFIO.

I'd like to take a moment to reflect on the importance of this organization and the work that it has accomplished since its founding in 1975. Many of us in this room recall the turmoil that wracked the Intelligence Community in the 1970s, culminating in the Church and Pike investigations. At a time when public support for a strong Intelligence Community was arguably at an all-time low, it was this organization's founder, David Atlee Phillips, who recognized the value of public outreach and education, and the importance of building an informed and engaged constituency for intelligence as a profession. Phillips traveled extensively, publicly talking about the need for a strong intelligence community. Through this organization, he sought to reach out to academia, the media, and the general public to explain the function of intelligence, and outline what we as intelligence officers can and cannot do.

It seems that today, we often find ourselves in the same position. As we work to build a more integrated and collaborative intelligence enterprise, we must continue our outreach efforts to explain not only the nature of what we do—and the vital importance of this work to the policy community, academia, the media, and the American people—but the changing nature of our work in response to the global changes around us. To that end, the AFIO has a critical role to play; in many ways, this group is the public face of the Intelligence Community.

<u>Globalization</u>

As we consider the theme of this conference – "Threats to U.S. Security" – it is easy for us simply to jump ahead to the actual threats, such as terrorism, proliferation, and organized crime, without thoughtfully taking a look at the larger context within which these threats have emerged, as well as questioning our own mindsets against the backdrop of globalization. What is the impact of globalization to our models and methodologies – our short-term and long-term strategies?

I don't think I am overstating the situation by saying that the United States is facing arguably the most serious economic and national security challenges in our history. These challenges are compounded by our inability to protect intellectual property and government secrets against the very real threat of adversarial individuals, hacker groups, terrorist networks, organized criminal groups, rogue states, and advanced nation states. And there is no time like the present to ask ourselves whether we have truly moved beyond our Cold War approaches in the intelligence arena. For example:

- Have we crafted appropriate strategies and responses to such threats in this new and ever-changing, technology-driven environment?

- What are the most dangerous threats we will face in the next three-to-five years and how do those threats fit into our current intelligence construct?

- Are we truly operating within a strategic vision in our approach to threats, or are we simply in reactive mode, relying on some of the same time-worn strategies of the past?

In addition to rethinking whether we are operating within a new strategic framework designed to address 21st century threats, we also need to recognize an inherent bias within the Intelligence Community, which has the potential to undermine our short and long-term strategies. We are a very insular crowd—it's truly a special club that we're in—and while I do not intend to demean the dedication, innovation and talent of our Community, I do believe that many of the answers and opportunities we need to seek lie outside of our traditional intelligence universe. Most importantly, we need to recognize the limitations of an insular bias in a global context. I read a recent editorial in which Norm Augustine noted that more than half of the increase in the U.S. Gross Domestic Product has been attributed to advancements in science, technology, and innovation. The solution to many of our and the world's greatest challenges depends on advancements in science and technology. I have a deep concern, however, that the Intelligence Community has still not properly aligned its response to what I would call this period of amazing innovation – the "technological wild west" – by grasping the full range of opportunities and threats that technology provides to us. There were times in the history of the intelligence discipline – when we were much smaller – when we eagerly sought out external expertise to challenge and fuel our own thinking.

In thinking about threats and the strategic vision necessary to retain – or perhaps *regain* – competitive advantage, I want to focus on the discipline of Counterintelligence, which typifies how we as a Community are grappling with threats and strategic vulnerabilities in the changing environment, and demonstrates where we need to significantly focus our efforts.

CI Overview

Counterintelligence serves as an interesting example of how we are attempting to update our thinking about an intelligence discipline in a very different and ever-changing environment. For the past year, I have been asking what CI looks like in the 21st Century. I believe that our approach to strategic CI issues will directly impact our ability to respond to key transnational threats, such as the growing threat to cyberspace or the prospect of supply chain attacks that could disrupt or even cripple critical infrastructure, defense and information systems.

The scope of counterintelligence is not widely understood, even across the IC. There is a tendency to equate counterintelligence (CI) with counterespionage (CE) or even security. Counterespionage—also known as "catching spies"—is part of CI, but CI extends to all efforts to detect, neutralize, defeat or exploit foreign intelligence threats. CI is not security either; while they are closely related and coordinated among their practitioners, they should remain distinct from one another. CI is a broader, more forward-leaning enterprise to protect and defend our national interests. While CI collects, analyzes, operates, and investigates, it must be visionary in identifying future threats and vulnerabilities in order to be of significant value to our key customers.

The Office of the National Counterintelligence Executive (ONCIX) was created specifically to further develop counterintelligence as a strategic capability. The NCIX has a specific challenge, mandated in legislation, to build a strategic, coordinated and integrated capability from the individual actions of CI programs and better align CI activities to national security objectives. And I cannot emphasize enough that a robust strategic CI effort is imperative to protecting our critical infrastructure and information systems, upon which our national security is directly reliant.

Strategic Vulnerabilities

So let me touch on the strategic vulnerabilities we are facing right now. First, in the cyber security arena, our national welfare involves our ability to exploit and protect the timely flow of vital information. Malicious activity in cyberspace is a threat to everyone. The current landscape is this: adversary capabilities are improving. Virtual reality offers ever-expanding possibilities--both good and bad. Attacks on U.S. systems are increasing. Remotely acquiring and exploiting information or disrupting critical infrastructure is increasingly an effective way for a growing number of hackers—including criminal entities and foreign governments—to disadvantage U.S. interests around the world, including and especially our economic interests.

In a globalized IT arena, our adversaries are exploiting our broad exposure and can steal sensitive and proprietary information from a target; corrupt the integrity of the information; deny the owner the use of a system; and/or destroy or deliberately insert erroneous data to render a system unreliable or inoperable. In many cases, as we look at the range of threats, we are playing catch-up and defense. We need to do more – we can no longer afford to assume this reactive posture. We need to aggressively work the offense – looking for the new centers of technology, identifying future threats, and determining how our practices and processes might need to change in order for us to move beyond playing catch-up.

The National Cybersecurity Initiative is a critical vehicle to engage all instruments of national power, including CI, in protecting our interests in cyberspace. Much more needs to be done, however. We need to work to shore up international alliances and work hand-in-hand with the private sector to come together on this issue. In fact, I would argue that we need a *fundamental rethinking* of our government's traditional relationship with the private sector – a high percentage of our critical information infrastructure is privately owned, and both government and industry must recognize that an individual vulnerability is a common weakness.

Acquisition risk is another area of significant concern. Government—including intelligence agencies—and businesses buy communications and other equipment in the open international market. Government and industry need to partner with each other, to deal with supply chain attacks – attacks that are difficult to counter given the international nature of our markets and acquisition practices. Supply chain attacks, using intelligence tradecraft, can plant vulnerabilities that can be used later to bring down systems or cripple our infrastructure.

Conclusion

If we consider our competitive advantage as a nation, it all comes down to the dedication, innovation, and talent of our people. But we cannot take that for granted. We need to challenge and guide our officers, by establishing a comprehensive and cohesive vision for how intelligence itself needs to change in the global environment. For example, as we deploy our officers, are we sending them to the same old locations or are we sending them to the centers of new technologies? Are we directing our analytic horsepower toward identifying *emerging* and future threats, deeply understanding the impact of those threats on our national security, and effectively articulating that impact to the policymaker to determine a course of action? For example, what might a covert action directed against our country a decade from now look like? Are we integrating the various intelligence disciplines in order to fully inform policy decisions? Finally, how do we create an intelligence enterprise that can shed its bureaucratic reaction time to anticipate—and not just respond—to an incredibly fast and ever-changing global environment.

The future is here; threats that once seemed only a remote possibility are increasingly a reality. I welcome AFIO's role in helping us think through how the intelligence profession might and should change against this new backdrop in order to be relevant and effective. Thank you for this opportunity tonight, and I welcome any questions or comments you might have.