POSTSCRIPT

POSTSCRIPT: FUTURE INTELLIGENCE CHALLENGES

No commission could examine every important issue facing the Intelligence Community. Our Commission encountered issues that were tangential to our mandate but that are likely to be crucial to the Intelligence Community and the DNI in coming years. We record in this postscript three of the issues that fall into this category.

SECURITY, COUNTERINTELLIGENCE, AND INFORMATION ASSURANCE

This country's security policies—considered in their broadest form to include physical security, infrastructure security, personnel security, and information and cyber security—are in need of serious review. Today we face new threats and vulnerabilities that are in many ways more encompassing, complex, and subtle than those we confronted in the past century. We begin with several broad observations:

- Security is a highly decentralized government function. Today there is no single advisor to the President who deals with the full spectrum of security-related issues.

- Effectively addressing security generates costs that must be balanced against risk and threats.

- Security, as a discipline, has historically been dominated by "police" type management, processes, and enforcement approaches. Although the police function is still required, today's security vulnerabilities are increasingly technical in nature and related to information technology systems, software, and hardware.

Several contemporary security challenges threaten to undermine not only intelligence sources and methods, but also the national security at large. These include: unauthorized leaks, which are now beginning to rival espionage in frequency, scope, and cumulative damage; the deterioration of the concept of need-to-know, and an increasing need to balance security concerns against the need for more robust information sharing; the particular vulnerability of communication and information sharing systems; foreign information warfare programs; and the persistent incentives for overclassification of information. To respond to these challenges, the Intelligence Community must harness the power of digital and biometric "identity"; improve the efficiency of the investigation, clearance, and adjudication process; develop mechanisms designed to protect sources, methods, and capabilities; effectively manage compartmentation; and certify secure spaces and improve physical security for people, facilities, and critical infrastructure.

Intelligence analysts have been placed in a difficult position. On the one hand, analysts must protect new and extremely sensitive sources and methods. On the other hand, analysts are expected to facilitate the broadest possible forms of information sharing, both amongst fellow analysts and with outside customers who increasingly want direct access to raw data and want to collaborate directly with the most knowledgeable and credible analysts.

We have considered many of these issues and offer recommendations that we believe will help address aspects of the security challenge, including our recommendations on Information Sharing (Chapter 9), and on authorized and unauthorized disclosures (Chapter 7, Collection). Yet we know we have only scratched the surface of this complex problem. The issue of security writ large requires a separate inquiry. Accordingly, this Commission recommends early action to define new strategies for managing security in the 21st century.

RETHINKING OVERHEAD COLLECTION

Some of the most difficult issues for the Intelligence Community in the next few years concern satellite surveillance systems. These systems are extremely costly, so that cost overruns in satellite systems tend to suck resources from the rest of the intelligence budget. Increasingly, too, there are air-breathing alternatives to satellite surveillance. Satellites can sometimes gather weapons of mass destruction intelligence not available in any other way, but sometimes satellites provide little assistance in targeting other WMD activities. They also play a crucial role for the military. Choosing which satellite systems are best in this evolving environment is an enormous challenge.

The DNI will need to make tough choices about our future imagery capabilities; doing so will require a strong Planning, Programming, and Budgeting

Execution System capable of comparing the marginal values of the respective collection disciplines. We did not believe that it was within our competence to make specific judgments about whether and how to overhaul future satellite intelligence plans, although we have offered recommendations that we believe will better enable the DNI to make these judgments. Given the importance of the issue, we recommend that the DNI specifically visit this issue early in his tenure.

MAXIMIZING INTELLIGENCE SUPPORT TO PUBLIC DIPLOMACY AND INFORMATION WARFARE

We live in an information age, and the United States needs an Intelligence Community willing and able to support the demands of our public diplomacy efforts. Moreover, we need a sophisticated capability to defend our own information environments and infrastructures from attack. The Intelligence Community has already developed some capabilities of this sort, but they require further investment and attention in order to address our current weaknesses. Our computer network defense capabilities lag considerably, making us vulnerable to countries with growing offensive capabilities.

Our intelligence organizations collect information about adversaries to enable public diplomacy. They also seek information on hostile intentions and possible attacks on U.S. and allied systems. Intelligence must be able to support all of these activities. Some aspects of the Intelligence Community's capabilities in this area cannot be discussed in an unclassified format.

Although our information warfare capabilities are still evolving, this large and complex subject merits further inquiry. Many components of the discipline are also controversial. But intelligence has a major role to play in this job.

The United States, as well as the entire modern global economy, is utterly dependent on its information systems as well as the sources that move, store, and display that information. The Intelligence Community must be focused and well-postured to address any vulnerabilities to these systems.

We did not fully explore these issues; they cut across government and private sector interests, and we believe that the Intelligence Community needs to: participate in initiatives designed to define the country's information warfare policies and doctrine; fund its activities; establish appropriate oversight; and provide for better integration, coordination, and collaboration across agencies. This is an appropriate job for a Presidential Task Force.