UNCLASSIFIED

Previous Next Contents

Daunting Challenges, Hard Decisions

The Intelligence Community: 2001-2015

Aris A Pappas *and* ***James M. Simon, Jr.***

Editor's Note: The authors intend this article to provoke a broad discussion of the role of intelligence in a constitutional republic during an era of accelerating change and terrible new dangers. The effort was inspired by workshops held under the auspices of the Deputy Director of Central Intelligence for Community Management, where government, private sector, and academic experts reviewed the challenges facing the Intelligence Community between now and 2015. Participants were guided by the National Intelligence Council's "Global Trends 2015: A Dialogue About The Future, With Non-governmental Experts."

* * *

A smart man never suffers certain defeat

—Chinese Proverb

The American Intelligence Community was born in 1947 with the passage of the National Security Act. It was conceived, however, on 7 December 1941 by the surprise attack on Pearl Harbor. The experiences of Pearl Harbor and World War II, and, later, the Cold War, shaped America's views of how intelligence would support defense and foreign policy for the rest of the century. Overall, a finely honed and highly specialized intelligence architecture achieved indisputable success. Its occasional failures illustrate the incredibly high expectations that came to be the norm.

The events of 11 September 2001 are another watershed, another chance to reconsider concepts and architectures. Over the past decade, commission upon commission has urged reform of the loose confederation that is the US Intelligence Community. Opposed by implacable champions of the status quo, precious few of these commissions have provoked meaningful change.

Ten years after the end of the Cold War, the threat of a nuclear Armageddon has receded, but the collapse of world communism and its repercussions are still works in progress. In a world with only one remaining superpower, even small and materially poor states and groups can pose terrible threats.

This is a paper about decisions that must be made now. The problems we face are immediate and compelling. If we cannot identify effective responses to these challenges now, the shape of the future will evolve in ever more dangerous and unknown directions.

Are we capable of proactive reform, or will change in intelligence practices and policies require yet another unforeseen disaster? History argues for the latter, but the nation demands that we continue to strive for the former.

The Future is Upon Us—2015 is Now

The focus provided by the battle against world communism and the balance of nuclear terror disappeared in the early 1990s. The smaller, less obvious dangers that remained bred a sense of confidence and well being that, ironically, may have contributed to this year's unexpected tragedies.

The collapse of the Soviet Union closed one era and opened another defined by instability. Instability in Russia, China, and other states reverberates well beyond their borders, reflecting the dangers inherent in the collapse of an empire. Monitoring the implications of that collapse will remain a task of US intelligence for the foreseeable future. Although stability has long been a goal of the world's last remaining superpower, after September 11th, it has become our key objective.

The single, massive threat of the Soviet Union has been replaced by a series of smaller, but individually highly destructive threats that are harder to monitor. Regional conflicts will continue, and may worsen. Some smaller states will avoid direct military confrontation and seek novel means to press their objectives.

Terrorists and criminal gangs will remain disruptive and confrontational. Global economic, communications, and financial networks will blur the traditional understanding of national borders, which may be seriously weakened by 2015. Meanwhile, corporate integration and the world economy will draw international attention to otherwise local financial setbacks or product and resource shortages. The social unrest of the industrial revolution may well return on an international scale as those opposed to globalism increasingly resort to violence.

Potential opponents will often be driven by emotional agendas that make them unpredictable. Their access to advanced technologies will grow. Efforts with the consequence of a Manhattan Project will be possible in small and hidden workshops, fueled by publicly available information.

Surprise must be anticipated. This is not a contradiction in terms. Unanticipated crises occur in each administration. Terrorists are dependent upon their ability to strike without warning. Highly precise missiles may give preemptive strike strategies greater significance in modern military planning. Our ability to warn against such attacks, or to monitor any growing capability to launch one, relies upon a global US intelligence effort.

Destabilizing and damaging surprises can arise in any quarter and the damage may be even more profound than loss of life or property. Our constitutional republic is dependent upon consistency and the rule of law, conditions that are essential to our freedoms and our identity as a nation. Surprise, whether political or military, can damage our society by provoking exaggerated and threatening responses as, for example, the internment of American citizens during World War II.

Outdated Systems

Human and technical collection procedures as well as our analytic capabilities are all in need of repair or replacement. Most of our systems and organizations were designed to observe a slowly evolving and enormous target, the Soviet Union. The stability of the Cold War meant that "bolt from the blue" attacks were considered extremely unlikely. Dramatic policy swings and unforeseen initiatives or threats were abnormal.

Warning was obtained by regularly monitoring the status of large forces to determine any changes in their position or alert status. Observation of each and every unit was not required on a daily basis. Sampling the force, principally by technical means, was sufficient for most requirements. Indeed, some units were never seen or heard from. The scattered and episodic nature of today's threats, however, requires much more precise and constant monitoring.

Recruiting spies against our main adversary was difficult given the closed nature of communist states. Our clandestine service was deployed and sized principally based on the activities and presence of Soviet personnel. Today, our needs are more disparate and numerous. We must recruit in more places and against more targets. Terrorist groups, in particular, are small and physically dispersed, but have tight, almost family-like cohesion. These new realities all increase significantly our need for a larger, broadly deployed, and well supported clandestine service.

Problems such as the social instability of disintegrating powers, failed governments, regional conflict, and terrorist activities require intelligence that can see deeply and beyond externally obvious signs. But, seeing is not understanding. US intelligence also requires sufficient expertise to understand the social, political, and economic dynamics of our targets. The increasingly multi-polar nature of international affairs and the ability of minor actors to have major impact place a premium on detailed understanding as well as actionable intelligence.

Changing Priorities

The attacks of September 11 th profoundly affected the US military's ability to rely on priority support from the national Intelligence Community. Previously, when the likely threats were from foreign military forces, the armed forces were able to presume that their support was the nation's highest priority. They could count on the Intelligence Community focusing its efforts on building systems to enable victory on the battlefield.

One consequence of the certainty of priority was that organic military intelligence capabilities and force structure were early and frequent casualties of the search for a peace dividend. Reductions were made possible by the elevation of support to military operations as the priority for national intelligence capabilities. In effect, organic military intelligence capabilities were traded for reliance on national systems. This, in turn, affected the systems themselves so that greater shares of intelligence resources went to the provision of real-time data to operating forces rather than strategic intelligence and warning.

The recognition that there is a genuine threat to the homeland from other than foreign military forces means that there is a new, powerful dynamic now in play. The physics of national intelligence is such that collection is not a major issue. In fact, we generally collect as much in as many places now as before September 11 th . The stress is on processing, exploitation, and analysis, where our precious few resources have had to be diverted to other tasks. Before September 11 th , the priority of support to US forces operating in Afghanistan would have been unquestioned; afterward, security for the Olympics in Salt Lake City had a higher priority. No one questions this change—after all, we exist to defend our fellow citizens.

The war on terrorism continues, however, making it imperative that our armed forces rebuild their own capabilities to ensure the level and quality of intelligence support necessary for success in battle. Complicating this new priority is the fact that monitoring the strategic military capabilities of Russia and China will remain important to the nation. In addition, over the next 15 years, other countries such as North Korea, Iran, and Iraq may obtain the capability to strike the United States.

National security and regional military priorities, once in synchronization, are now widely separate. The demands to provide intelligence in support of local contingencies can conflict or compete with other pressing, long-term needs.

As the number of contingencies grows, our ability to obtain detailed collection and to perform in-depth analyses to protect against surprise and strategic reversal declines. For example, when our most capable collection assets provide day-to-day support to monitoring flights over the restricted zone in southern Iraq, our ability to monitor longer term and even more deadly concerns outside the zone or in nearby countries is reduced. We run a real risk of becoming blind, deaf, and ignorant in key areas of the world, trusting to providence for our safety.

US weapons define the cutting edge of modern warfare. Designed to produce massive and precise destruction of their targets, they were used effectively in Afghanistan, during the Gulf War, and elsewhere, to reduce risk and battlefield loss. As the mistaken bombing of the Chinese Embassy in Belgrade demonstrated, designing a weapon to hit a particular target is a technical problem, but accurately identifying the correct target is an intelligence problem. The precision and accuracy of our weapons must be equaled by our intelligence.

Cyber Threats

The world in 2015 will depend upon computer networks for communication, energy, transportation, financial transactions, public safety, and thousands of other tasks. Hostile nations and groups seeking to disrupt critical infrastructures will have access to the technology needed to pursue cyber espionage and cyber attack. Computers are inexpensive, as compared to traditional weapons, and require no large industrial base. They are globally available and connectivity is widespread and increasing.

Effective response demands timely and confident warning as well as accurate intruder identification. Difficult procedural and legal issues complicate the ability to discern foreign from domestic cyber threats. Under present law and policy, cyber intrusions are presumed domestic in origin unless demonstrated otherwise. This limits the participation of the US Intelligence Community in detecting and tracking cyber attack.

The expansion of information systems, news organizations, and network connectivity has produced an "information tidal wave" that can overwhelm information management systems. The enormous flow of data impedes the production of intelligence as processing ability fails to keep up. Information alone, without analysis, is not useful. Artificial intelligence and other expert systems offer only a faint hope that a solution to this glut is forthcoming.

R&D Edge Lost

Technology is no longer a US monopoly. The US has always assumed that we could and would come up with whatever technological solution called for by any problem. An embarrassment like the Soviet launch of Sputnik, for example, resulted in an explosion of scientific, technical, and engineering efforts. The Soviets, self-designated exemplars of the modern "scientific man," virtually worshipped at the feet of the technology god. The problem was that their god lived in the West, in fact, in the United States. Now we are facing the same reality that confronted the Soviets: technology is, and has always been, ideologically neutral. It benefits anyone with access and means. This simple fact now represents an enormous challenge to US intelligence.

The technology used by the Intelligence Community has become antiquated. New solutions remain undiscovered and new funding will take time to have an effect. This is a strange and unprecedented condition for the United States, long accustomed to having technology as an ally. For most of the Cold War, technological advances were almost always initiated by the US government and driven by huge budgets directed at victory over communism. Advanced technological development is no longer the sole purview of governments, and access to the fruits of that development is now available, in virtual and actual marketplaces, to anyone worldwide.

US intelligence has relied upon our possession of advanced technology and our opponents' ignorance of our actual capabilities. Both sides of this equation have now changed. Virtually all the technical capabilities developed over the last several decades are now public knowledge. What we can do, and how we do it, is effectively in the public domain. Traditional evolutionary improvements to our existing capabilities cannot provide the same relative advantage once provided by the deployment of a new system.

Already, two of our most important collection capabilities have been seriously affected. Satellite imagery is now commonly understood. Commercial interests, convinced that they can do a better job and provide necessary services to a wider customer base, have increasingly challenged the government's traditional dominance of imagery. Signals and communications intercept capabilities have been degraded by the digital and fiber optic revolution and the marked increase in commercially available and effective encryption. The public availability of secure communications means that security is now affordable and accessible to terrorists, organized criminals, and others.

Even our traditional agent-based operations are affected. Modern and widely available technology makes it more and more difficult to sustain assumed identities and other aspects of case officer tradecraft. Disguises, special documents, and communications all continue to benefit from advances in technology, but the public availability of countermeasures and detection devices balances many of these advantages. The new emphasis on security to hinder the free movement of terrorists also complicates the government's clandestine activities.

The United States will continue to provide worldwide leadership in science and technology. Our ability to maintain advantages in intelligence collection systems will diminish, however, as the rest of the world gains greater access to technology through advanced, commercial, "off-the-shelf" tools. Technology that was once the exclusive domain of relatively few countries will become increasingly available to anyone with the interest and the necessary funds. As a consequence, the Intelligence Community will encounter surprises from both the use of known technology in unexpected ways and the innovative application of combinations of new technologies.

During the Cold War—indeed throughout the Industrial Age—great-power status depended in good measure upon a sizable population, capital investment, and possession of, or access to, vast stores of natural resources. In the Computer Age, however, possession of, or mere access to, advanced technology can confer superpower-like status almost overnight to small, materially poor nations and even groups. Absent most of the attributes of traditional superpowers, otherwise minor players are now able to take actions wholly out of proportion to their size or wealth.

What Can We Do?

Good Ideas are not adopted automatically. They must be driven into practice with courageous patience.

—Admiral Hyman Rickover

We must maintain a unilateral advantage in key technologies, even though disclosures have compromised many of our sources and methods. Full advantage from our technology, however, can only be realized by staying clearly and unambiguously in first place. US intelligence requires a special effort to focus future development on capabilities that are not only advanced, but a leap into areas unknown or insufficiently understood by our opponents and targets. The mere application, no matter how elegant, of existing technology will never provide the degree of advantage afforded by the application of genuinely new capabilities.

Technological change is certain, but our ability to recognize that change and use it, depends on long-term commitment. We are justifiably proud of our satellites, but must remember that they resulted from "leaps of

faith" requiring technical brilliance and managerial daring backed by equally courageous support from the Congress and the President.

US dominance in space is an unambiguous advantage to our national security. Access to space and from space remains key because it provides an unimpeded platform for observation. By 2015, greater numbers of potential adversaries will learn to "work around" US remote sensing systems and develop new deception techniques. Increasingly, fiber optics and encryption will be used to deny us critical information. By 2015, this trend toward denying and deceiving US intelligence will be on a global scale.

Existing systems were designed for monitoring relatively static facilities. We need new systems that can establish and maintain a closer and more constant watch on smaller, fleeting targets like terrorists and mobile missiles bearing weapons of mass destruction. "Needle in a haystack" targets like these will remain the most difficult challenges. We require an integrated architecture that is as agile as our targets.

Three technologies offer potentially high rewards for intelligence, but even greater danger if developed and used by others.

- Parallel processing and quantum computing have tremendous implications for cryptography, real-time translation, and transcription of intercepted communications.

- Nanotechnology offers new ways to get closer to targets. Undetected penetration of a terrorist camp, for example, enables both collection and attack. Potential applications include "labs on a chip" to provide long-term detection of biological, chemical, radiological, or other weapons of mass destruction, and miniature cameras for real-time video used in precision targeting.

- Maxwell's Rainbow—referring to the spectrum beyond the visual and electromagnetic bands—provides thermal, atomic, and other signatures. Properly used, it may be possible to look through camouflage, identify the function of underground facilities, and find chemical, biological, or nuclear weapons.

Integration is Key

The guiding principle for the development and eventual operation of all advanced intelligence systems should be integration. Information that is collected but cannot be processed or assimilated is not intelligence, and therefore potentially useless. We can use business approaches to insure proper alignment among technology strategies and related collection, analysis, and general business strategies.

Entire agencies have grown up around collection techniques because of the enormous concentration of skills required to succeed. Each agency develops its own new technologies, principally in reference to its existing area of specialization. These tend to be straight-line improvements of existing systems. The result is a system unsuited to clients, who are responding to even more rapidly evolving challenges.

The measure of merit for new technical systems should be mission accomplishment, not performance enhancement. Scarce funds ought to be spent where they will do the most good, as defined by customer requirements, and not for development that is driven principally by technical feasibility. Needs should be derived through extensive contact with and participation by analysts serving as proxies for the ultimate customers of intelligence products. A "whole system" approach to advanced R&D and systems development is a necessity. Only in this way can the needs of all our intelligence agencies and disciplines be considered and brought to bear.

Information Processing Demands

The right knowledge must get to the right people at the right time. The upsurge in demand for intelligence, coupled with declining budgets and manpower, has made merely processing the vast amounts of data a daunting task. Our existing information-processing tools were developed to provide the process of substantive analysis with an orderly flow of information. As a result of increased volume, tighter timelines, and reduced resources, these tools now drive the very process they were designed to support. Enormous gains in our capacity to handle this volume have been overshadowed by a concomitant reduction in our ability to usefully synthesize, analyze, and simply understand what we have.

This is a critical issue with regard to our need to integrate intelligence and law enforcement data in support of effective Homeland Security. Information and data moving at the speed of analysis must now be moved at the speed of warning. Specific information that could lead to the identification and apprehension of a terrorist must flow unimpeded from the most classified and integrated data bases to the patrolman making a routine traffic stop.

We must intensify our cooperation and collaboration with business and academia. Analysts' traditional, but informal, relationships with experts in industry and universities are not sufficient to meet rising demands for complex intelligence products. For example, private scientific and technical sectors will be critical to our ability to stay even with scientific developments, much less remain in the vanguard. "Breakthrough" scientific advances may occur well away from the traditional large, government-supported labs and research establishments.

The remedy, however, requires US intelligence agencies to overcome ingrained resistance to our overtures of cooperation. Large segments of the public, news media, and academic and scientific communities have a highly developed suspicion of the motives of the Intelligence Community. Despite improvements driven by the events of September 11 th , serious efforts must be made by all parties concerned to overcome these suspicions in pursuit of a common defense.

We must increase our investment in analysis. Long-term analysis and basic research is in decline. The daily demand to support immediate policy needs exceeds existing analytic capabilities. Resources, therefore, are unavailable for the long-term analysis required for the accumulation of substantive capital. Furthermore, absent long-term analytic programs, analysts are not developing core skills and in-depth familiarity. The strategic pursuit and elimination of terrorists, for example, has proven to require much more than nominal name checks and border watches. Any systemic attack on sophisticated command, control, logistic, and financial support structures requires at least as sophisticated and intense analytic support.

We already lack satisfactory capability to analyze a substantial body of material on foreign and security policy, domestic policy, crime and corruption, space and aerospace technology, advanced materials, biographic information, and military doctrine and strategy. In the future, knowledge of culture, history, and language will be even more critical as the amount of open-source material increases.

Inadequate American foreign language skills are a mismatch for the exponential growth in foreign language materials. The Intelligence Community requires a real-time system that allows analysts to search in English against foreign language media. This system must automatically index, store, and retrieve materials in all formats; it must provide machine translations that allow analysts to select textual components for professional translation.

We must change how we process information. There is now almost universally open access and communication to places that once were totally denied to us. News about internal instability and destabilization now flows over the Internet. There is no reason that the collection, processing, and presentation of such information to the

government could not be left to trusted commercial partners. Huge advantages could accrue from focusing intelligence collection and analysis on information that is denied or secret.

A weather analogy is pertinent. During World War II, entire operations were mounted in pursuit of information about weather, then considered an intelligence function. Many soldiers, sailors, and airmen lost their lives in these efforts. Today, such information is in the public domain. Any serious review of intelligence would yield similar opportunities for divestiture.

We must outsource whole business areas. While we were focused on the Soviet Union, nearly all the information obtained by US intelligence was, by definition, denied and secret. It was processed within the intelligence agencies and reported out within highly restricted channels. US Intelligence became a collection of vertical monopolies. This was never desirable and is no longer acceptable. Commercial imagery from space, for example, recently provided the world a view of a US reconnaissance aircraft parked on a Chinese airfield. Not long ago, such an image could only have come from government satellites. In the modern world, public access to pertinent data through media news networks, the Internet, and even private "intelligence" services, is pervasive and nearly instantaneous. As a result, both intelligence producers and intelligence consumers are increasingly confused as they attempt to differentiate intelligence products from news analysis and opinion, and from disinformation and deception.

Outsourcing could sharpen the focus, increase the efficiency, and enhance the value of intelligence to clients. It could clarify the true role of intelligence and allow a more rational allocation of resources. Outsourcing cannot simply mean throwing work "over the transom" to the private sector. It must be a thoughtful process that creates strategic partnerships and joint ventures with commercial and academic organizations.

Streamlining the Decision Process

Over the course of the Cold War, we grew to resemble our former adversary: too large, too slow, and too rigid. We are at risk of being consistently unable to make decisions or take actions faster than our opponents. Closer ties to commercial and academic partners will force the government to move at a quicker pace. In some areas, such as research and development, a business ethic that credits efficiency and quick turnaround is a necessity.

We must review existing authorities. Foreign intelligence capabilities must be able to assist in the defense of the homeland. Existing legal and executive authorities impede our ability to cooperate with domestic government organizations concerning threatened attacks on the United States. Appropriate safeguards and oversight can be devised that will protect Constitutional guarantees, but still allow our society to defend itself using all the means and assets at its disposal. Intelligence operations must be strictly legal, and designed not to infringe on the rights of our citizens.

The US Intelligence Community is composed of fiercely independent agencies, each with strong traditions, authorities, and loyalties. They define the world from individual perches, with little time and less incentive to consider grand problems or grand solutions. In many quarters, this has resulted in a call for their dissolution—in effect, advocating starting over with a clean sheet of paper. Beside the obvious point that there is no guarantee that this would work, such an attempt would be so bureaucratically and politically stressful that the result could be a larger disaster than the one we are trying to avoid.

So, what to do? The existence of the so-called vertical "stovepipes" stems from the need to provide organizational coherence to people and systems doing related work. Orbital mechanics is not the same as agent recruitment. Furthermore, the organizations are naturally interested in doing an effective job. The solution emerges at a higher level of aggregation.

Decisionmaking must be driven by the mission: the right tool for the right job. Hostages do not much care whether it is a Marine or an Army Ranger who rescues them: the instrument employed is based on circumstances, expertise required, and availability. Similarly, our clients do not much care if the intelligence that supports their policy initiatives, prevents surprise, or insures victory is collected, analyzed, and disseminated by CIA, NSA, DIA, NIMA, or any of the other ten agencies that comprise the Intelligence Community. What they care about is results.

If we are to forge a true community out of the existing loose confederacy, the Intelligence Community must have a leader accountable to the President and the Congress. That leader must have no other conflicting or distracting responsibilities. Finally, such a person must have the resources and legal authorities necessary to discharge all responsibilities effectively and efficiently.

The only reasonable candidate for this task is the Director of Central Intelligence (DCI), supported by a staff analogous to the Joint Chiefs of Staff. No one else has the interest, focus, and undiluted responsibility to deliver intelligence. Responsibility without authority, however, is worthless. In government, authority derives from control over budgets and key personnel. Today's DCI has neither.

Today, moneys are appropriated directly to the intelligence stovepipes. Unsurprisingly, the execution of the existing program gets the lion's share of attention and resources. New strategies or revolutionary technologies that do not fit easily in the existing program have a difficult time. Without a central authority able to redirect funds, new initiatives are starved for resources. In times of great challenge and rapid technological change, this is the wrong way to do business. These moneys all should be appropriated to the DCI so that the allocation of resources to technological development can be made in the interest of the whole enterprise.

Doing Nothing is Easy—Change is Hard

It is only when we demand a solution with no cost that there are no solutions.

—Lester Thurow

This paper argues for a fundamental review and change in a strong and heavily traditional community of proud organizations. No less than the cavalry of a distant past, they, too, point to a glorious history of success and victory. Now, these organizations are challenged by attacks on what may be their most treasured measure of self-worth: their relevancy.

It is difficult to abandon the comfort of routine. But, intelligence must be shaped to reflect the world in which it lives. Success will not be measured by our ability to find marginally better ways to use our existing resources, but in our ability to seek out and employ whatever is needed to do the new job. Neither easy nor cheap, the costs and risks of doing anything else are simply unacceptable. When the world changes, the single most important requirement for intelligence is to change with it.

Aris A. Pappas and James M. Simon, Jr., are senior officers on the Intelligence Community Management Staff under the Director of Central Intelligence.

Previous Next Contents

UNCLASSIFIED