NCIX
NATIONAL COUNTERINTELLIGENCE EXECUTIVE

Honorable Michelle Van Cleave
National Counterintelligence Executive
remarks prepared for delivery
Conference on Counterintelligence for the 21st Century
Bush School of Intelligence, Texas A&M University
March 5, 2005

The National Counterintelligence Strategy of the United States

Today marks the anniversary of one of the most celebrated speeches in the history of freedom. At the invitation of President Truman, Winston Churchill traveled to Fulton, Missouri on March 5, 1946 to speak at the small college of Westminister. We have come to know this address for Churchill's vivid warning that an Iron Curtain had fallen across the Continent of Europe. But he entitled the speech, "The Sinews of Peace" because his message was far more than a warning – it was an overall strategic concept and a call to duty to ensure peace through strength.

His words speak to us across the decades:

> **The United States stands at this time at the pinnacle of world power. It is a solemn moment for the American democracy. For with this primacy in power is also joined an awe-inspiring accountability to the future.**

As Churchill spoke, we were on the eve of Cold War. Dean Acheson, in his great work *Present at the Creation*, described the national security demands of the post World War II years as just a little less daunting than the task in Genesis. There, the challenge was to create a new world out of chaos; "ours," he said, "to create half a world – the free half – out of the same stuff."

For much of the time since then, the Cold War setting was a kind of artificial peaceful coexistence. We told ourselves that the Soviet Union's hold over the captive nations of Eastern Europe had to be accepted, that this was the price demanded if there was to be stability and peace. And for many years, the nations of Eastern Europe submitted to this fate. As Vaclev Havel explains in his book *The Power of the Powerless*, Communist control succeeded by reason of the consent of the governed. Not in the positive sense that democracies use those words, but because not enough people were willing to stand up and say no.

But finally, the people of Eastern Europe and within the former Soviet Union itself found the will to say no. All of the enormous military strength and institutionalized

terror of the Soviet totalitarian regime was not enough in the face of brave people determined to be free. The courage of those who said no should cause us to reflect with some seriousness on our own values, and on the responsibilities we believe the democracies should assume in looking toward the future, and the opportunities – and dangers – that lie ahead.

Again, the wisdom of Churchill's counsel endures:

> **[T]he old doctrine of a balance of power is unsound. We cannot afford, if we can help it, to work on narrow margins, offering temptations to a trial of strength… [W]hat we have to consider here today while time remains, is the permanent prevention of war and the establishment of conditions of freedom and democracy as rapidly as possible in all countries.**

Today the threat posed by terrorist networks is different in kind and scope from dangers past. But it should come as no new thought to Americans to hear Churchill's vision reflected in the Inaugural address President Bush delivered this past January: In plain talk the President said:

> **[I]t is the policy of the United States to seek and support the growth of democratic movements and institutions in every nation and culture, with the ultimate goal of ending tyranny in our world.**

Since the founding of our republic, the pursuit of democracy and freedom has been both an ideal and a bedrock of our security. In the President's words,

> **The great objective of ending tyranny is the concentrated work of generations. The difficulty of the task is no excuse for avoiding it. America's influence is not unlimited, but fortunately for the oppressed, America's influence is considerable, and we will use it confidently in freedom's cause.**

U.S. counterintelligence also has a role in freedom's cause.

Each of the major challenges confronting our Nation's security – defeating global terrorism, countering weapons of mass destruction, ensuring the security of the homeland, transforming defense capabilities, fostering cooperation with other global powers, promoting global economic growth – has an embedded counterintelligence imperative. Specifically, terrorists and tyrants, foreign adversaries and economic competitors, engage in a range of intelligence activities directed against us in order to advance their interests and defeat U.S. objectives. Too often these foreign intelligence activities against the United States have been successful. Collectively, they present strategic threats to the Nation's security and prosperity. The United States requires a

national, systematic perspective and coherent policies to counter them, including a strategic counterintelligence response.

The National Counterintelligence Strategy

It is my privilege today to share with you the principles set forth in the *National Counterintelligence Strategy of the United States*. The official document, which will be issued later this month by President Bush, will be the first unclassified national strategy for U.S. counterintelligence. It is also significant because it will be the first formal mission statement for strategic CI as an instrument of national security.

Individual departments and agencies may have tailored CI mission statements, for example, to enforce the espionage laws, or to ensure the success of their operations – but never before has the United States set forth the strategic mission of counterintelligence in protecting and advancing the Nation's security.

The Strategy also foreshadows the elements of a national CI system that will be needed to integrate, direct and enhance U.S. counterintelligence including its role in support of national security decision-making. These are the tools needed to be able to execute the strategic CI mission. It is especially fitting that these matters should be on the table as the first Director of National Intelligence assumes office.

Here are the seven pillars of the counterintelligence strategy of the United States.

First, we will extend the safeguards of strategic counterintelligence to the Global War on Terrorism.

In recent history, the United States has sustained stunning losses to foreign intelligence services, which penetrated virtually every one of the most secret, highly guarded institutions of our national security apparatus. Some of this harm can be attributed to protective security vulnerabilities and failures. But these losses also represent a strategic failure of our CI capabilities. Any one of these major compromises could have had devastating consequences in war. Thankfully, the Cold War ended, as President Reagan said, without either side firing a shot.

Today our Nation is at war, and the potential consequences of intelligence failure more immediate, placing in jeopardy U.S. operations, deployed forces and our citizenry.

September 11 brought home our vulnerabilities and the face of evil. In the President's words, "My most solemn duty is to protect this nation and its people against further attacks and emerging threats." All who serve U.S. counterintelligence share that solemn duty.

The intelligence services of state sponsors may represent key links in the global terrorist support network. Terrorist groups perform traditional intelligence activities in

the way they gather information, recruit sources, and use assets. Their operations require intelligence preparation – preplanning stages, compartmentation. They may also engage in practices designed to deceive U.S. intelligence and mislead decision makers.

We must ensure that the global war on terrorism is armor-plated with an effective CI strategy to identify and exploit offensive opportunities against terrorist networks, to provide CI support to force protection and operations security in the field, and to help filter truth from deception. And it is vital that we have the ability to execute that strategy.

Historically, CI has grown up around an allocation of responsibility that divided foreign from domestic, and intelligence from law enforcement. While each of these domains has their proper place and rules, the national need for unity of effort far outweighs the legacy practices of division. The global war on terrorism has driven home the truth that there is no longer room for bureaucratic parochialism. Terrorist threats, like threats from foreign intelligence services, are global in reach. They do not respect borders. Our challenge is to ensure that U.S. intelligence and security operations are not rendered less effective by structural divides which the enemy does not recognize.

In particular, we must have actionable and reliable intelligence to support a proactive strategy of prevention to counter terrorist threats. The national strategy of prevention places a premium on effective CI to ensure the reliability of enabling intelligence, and to protect operational initiatives. It also requires that U.S. counterintelligence in all its dimensions – strategy and execution – seize the initiative and become more proactive.

And that is the second pillar of the *National Counterintelligence Strategy*: We will shift emphasis from a posture of reacting to a proactive strategy of seizing advantage.

The proactive strategic approach to counterintelligence is a departure from past practices. If you look back on the record of U.S. CI, especially counter-espionage, you will see that most CI has been based on tolerating some level of loss – extremely grave loss in the case of some long-serving, well-placed spies – that, once discovered, triggers intensive investigations and prosecutions. This ability to react quickly and effectively will always be a vital core of CI. But U.S. CI also needs to go on the offense.

What does it mean to go on the offense? Conceptually, there are two parts: First, a global CI assessment and engagement of adversary presence, capabilities and intentions; and second, a CI doctrine for attacking foreign intelligence services systematically via strategic CI operations

The proactive approach to counterintelligence requires a generous dose of creativity to turn threat into opportunity. We don't want to sit back and discover, years and years after the fact, that while we have investigated every reported security breach,

spies have stolen our secrets or cyber thieves have exploited our networks. Instead, we need to think offensively.

We need to ask, what are the indicators that might give us early warning of intelligence operations against us? We need to ask, what can we do to discern and defeat such operations? Investigations are one among a suite of tools that the operational CI elements can employ; and there are others. And I look to the security-focused CI offices within the Cabinet departments and agencies to provide the knowledge, programs, and creative insights to engage the operational CI resources of the government to proactive ends.

In wartime, we must be able to defeat the adversary's intelligence capabilities, including their ability to deceive or mislead us. Experience with Iraq reminded us that neutralizing the intelligence services of the adversary is a crucial element in winning the war; and that it is far better to plan well in advance than on a last minute basis. We need to ensure that the lessons learned from the CI successes against Iraq are applied to all future war planning. Standing operational planning should include a national-level strategy for defeating the adversary's intelligence objectives, as well as tactical CI operational plans and order of battle. Strategic CI planning can also increase the options available to decision makers for advancing national objectives while avoiding war.

At home, the strategic CI mission calls for a coordinated, community-wide effort of aggressive operational activity and analysis to obtain the intelligence necessary to neutralize the inevitable penetrations of our government. Within the United States, the operational and analytic focus must transform from a case-driven approach to a strategic CI assessment and engagement of adversary presence, capabilities and intentions. Strategic CI analysis must drive operations. This will also require looking beyond the customary targets of known intelligence officers to the larger population of diverse foreign visitors and others serving foreign intelligence purposes, who find our free and open society a rich playing field for the illicit collection of national security secrets and other valuable information that confers advantage.

Which brings me to the third pillar of the Strategy: It is the objective of U.S. counterintelligence to help protect the vital technology secrets that are the bedrock of our strategic security.

America's national defense rests on its continuing technological superiority. The United States cannot maintain its dynamic technological superiority without a corresponding intelligence and counterintelligence superiority.

A national defense strategy based on transformation places a premium on the sensitive capabilities and technologies that give advantage. The single most effective strategy to defeat U.S. plans to ensure superiority through transformation is to capture those essential secrets, in order to incorporate them into adversary weapons systems and to develop countermeasures. Foreign militaries that acquire controlled U.S. technologies

are able to leapfrog technological barriers that would otherwise slow or even prevent the production of more sophisticated weapons.

Espionage has long proven the most cost-effective means of defeating U.S. capabilities. We may spend billions of dollars to develop a given weapons system, the effectiveness of which rests on essential technological, operational or design secrets that give us advantage. If those essential secrets are stolen, both our investments and our advantage can be lost. The cost-benefit ratio of espionage is sharply in the adversary's favor.

The most successful espionage – the kind that goes undetected – is all the more effective, because what is not known cannot be remedied. And the risks are growing. The marvels of modern information technology and microelectronics have revolutionized espionage tradecraft, enabling the clandestine extraction of vast volumes of data in miniaturized storage media or across computer networks at the press of a "send" button.

The key to protecting America's qualitative defense advantage is to draw upon all of the tools of statecraft, national policy, law enforcement and public awareness to deny adversary acquisition of essential technology secrets. These things must be done in concert. That is a policy call. But CI needs to supply insights into the foreign intelligence threats against vital technologies, and options to counter those threats. That will require focused and creative collection activities, strategic analytic exploitation, and coordinated operational discipline. In this manner, CI can make a seminal contribution to the overall national technology protection effort.

Fourth, it is the objective of U.S. counterintelligence to safeguard the integrity of intelligence and to identify and defeat foreign denial, deception and covert influence operations.

Successful foreign penetrations both human and technical have netted foreign intelligence services an enormous amount of U.S. classified information, enabling debilitating countermeasures to U.S. intelligence collection and analysis. There is a market for stolen U.S. secrets, which can be sold or bartered to third party states or terrorist organizations that have their own uses for the information. The knowledge gained of U.S. intelligence sources and methods – through spies, unauthorized disclosures, and even some authorized disclosures – has aided in extensive concealment and denial programs that increase our uncertainty about foreign capabilities and intentions, and deception operations to mislead us.

As a result of sensitive knowledge gained about U.S. intelligence, many nations have learned how to deny and deceive the United States in order to present a false picture of reality. These foreign denial and deception practices may lead analysts to faulty judgments, when vital information has not been collected, or when deception distorts understanding. The danger is that useless or deceptive information – whether from human or technical collection – may be integrated into U.S. intelligence and disseminated

to policymakers, weapons designers, war-fighters and even the warning community as if it were true. It is the job of counterintelligence collection and analysis to protect and validate U.S. intelligence and to reveal otherwise unknown strengths and weaknesses and threats posed by U.S. adversaries.

It has been said that "counterintelligence is to intelligence as epistemology is to philosophy. Both go back to the fundamental question of how we know things, [and] both challenge what we are inclined to take most for granted…" (Thomas Powers, *The Man Who Kept Secrets*).

If that is too esoteric for you, consider that risk is inherent in the pursuit of intelligence: in technical collection, in clandestine operations, and in analytic judgments. It is the job of CI – integrated into system design and operations security, validation of assets and information, and counter-D&D analyses – to help minimize that risk while supporting the positive intelligence mission. CI supplies the techniques by which the reliability of a collection system, the bona fides of an asset, or the soundness of an analytic judgment, can be established, operationally tested, and revalidated to ensure the integrity of the product. The statesman's maxim of "trust – but verify" is the clarion call for effective counterintelligence.

Fifth, it is the objective of U.S. counterintelligence to help level the economic playing field so that U.S. business and industry are not disadvantaged by unfair intelligence practices of foreign competitors.

The protection of American strategic information and technology has long been an element of the nation's security, including the propriety commercial information that brings competitive advantage. Lead responsibility for that job of course falls to the private sector owners of that information and technology. But government also has a role to play. As a first and obvious step, government can provide information about the threat, to the extent that intelligence is available and can be confidently shared. But it is up to business and industry to decide what to do. There will always be some level of risk. Deciding how to manage that risk, in order to carry out operations effectively, is the real security challenge.

CI and security cannot be afterthoughts imposed on corporate R&D personnel, businessmen or mid-level managers. Heightened awareness, and intelligent security practices that protect the valuable secrets of the corporation, are the best guarantors of success against the foreign intelligence threat. While our principal focus must remain the terrorist threat, we will also enhance outreach to the private sector to increase awareness of the economic intelligence threat facing our Nation as a whole, through providing threat information, and educating especially the S&T community, to the variety of ways our adversaries acquire and steal information from us.

Sixth, the Strategy directs that the national security decision-making process be informed by counterintelligence insights.

The intelligence activities of adversaries or allies, competitors or partners, are a window into their respective interests, purposes and plans. For instance, our insights into the foreign intelligence activities of the other main centers of global power will confirm or otherwise shape prospects for cooperative action. In other words, solid counterintelligence information, properly analyzed, always has a positive intelligence dimension.

In this manner, CI can supply insights into the actions of our adversaries and the actions directed against us, as well as opportunities for advancing our interests, which can inform and enable sound policy decisions. Good CI analysis can help discover and connect the seemingly disconnected, illuminate hidden relationships, identify unseen linkages, or reveal patterns of activity and behavior heretofore unobserved. CI analysts are the ones who zero in on the things Yoggi Berra deemed "too coincidental to be a coincidence." Damage assessments of espionage cases also have insights to contribute to decision-makers. These include the direct impact of the damage on U.S. intelligence and national security plans and programs, as well as the vulnerabilities revealed, and managerial, security and operational lessons learned.

In effect, under this Strategy counterintelligence will have a guest seat at the policy table, in order to present an array of strategic CI insights and operational options in foreign and defense policy for the President and his national security leadership team. Proactive CI operations, put into a larger context, may be useful in shaping a threat, influencing adversary decisions, masking vulnerabilities, advancing diplomatic objectives, or conferring advantage at the negotiating table or on the battlefield. Such an iterative process will also enable the policy direction and integration of CI operations with other national goals and instruments.

Finally, the Strategy directs that we build a national CI system to enable its execution.

The recently passed Intelligence reform legislation represents the most sweeping revision of the basic National Security Act in the almost 50 years since its passage. The Counterintelligence Enhancement Act, which is incorporated within the new law, places my office and the strategic CI mission directly under the new DNI. Our job is to provide strategic direction, comprehensive threat assessments, global operational priorities, and effective program and budget guidance to execute the national CI mission.

This mission extends far beyond any individual Department or Agency's ability to fulfill. Nor is this mission simply the sum of the individual elements supporting their Department or Agency mission. Today there is a great deal of bilateral cooperation and information sharing across the several agencies responsible for U.S. counterintelligence.

But that is not the same thing as orchestrating the diverse CI resources of the government to achieve common objectives against a defined intelligence threat.

Foreign intelligence services don't target an individual FBI field office, or a CIA station, or a military unit; they target the United States. The several arms of the federal government, along with state and local authorities and industry partners, must work as one team. For the future, each of the participating members of this community must be prepared to assume new responsibilities, and join together in a unity of effort, as the National CI Strategy matures. This necessary systemic transformation will not happen overnight but it has begun with the issuance of the national Strategy. We are already working on national-level implementation guidance, and detailed guidance will also need to be developed and incorporated into the CI planning, programs, budgets and ethos of the individual Departments and Agencies.

We must also look to the professionalization of the CI discipline. U.S. counterintelligence capabilities are only as strong as the quality of the people entrusted with their execution. The complexity of the subject requires the mastery of many disciplines and skills, including the strategic perspective of CI. The CI profession needs its own set of standards that are common across the many CI missions as well as specific to CI specialties. We will need to reach across the several Departments and Agencies to find the centers of training excellence, address deficiencies, and upgrade the content, quality and availability of CI instruction. We also need to recruit new entrants into the profession, who bring creativity and imagination, along with the highest standards of integrity and dedication, to the CI workforce – a select profession in which all Americans have invested so much trust.

To the students here today, let me say if you have these qualities, please check in with the recruiters.

Conclusion

The National Counterintelligence Strategy of the United States is a sharp departure from past practices. Historically, by waiting for intelligence threats to mature before taking action, we have ceded the initiative to the adversary. No longer will we wait until we have been harmed to act. The President has charged U.S. counterintelligence with a clear strategic mission: 1) to identify and assess what foreign intelligence services are doing against U.S. interests and how they are doing it, and 2) to develop doctrine, assign resources and implement operations to neutralize those activities proactively at home and abroad.

This is the mission. Under the President's leadership, and in freedom's cause, U.S. counterintelligence in the 21st century will step forward to help meet the "awe-inspiring accountability to the future" of which Winston Churchill spoke on this date, not so very long ago.