OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
Public Affairs Office
LEADING INTELLIGENCE INTEGRATION

Remarks as delivered by
James R. Clapper
Director of National Intelligence

Worldwide Threat Assessment to the Senate Select Committee on Intelligence

January 31, 2012

Thank you, Chairman Feinstein, Vice Chairman Chambliss, distinguished members of the Committee for inviting us to present the 2012 Worldwide Threat Assessment.

These remarks and our Statement for the Record reflect the collective insights of the extraordinary men and women of the United States Intelligence Community, whom it is our privilege and honor to lead. And on their behalf, I would thank you both for your acknowledgment and recognition of the great work that these men and women do, all over the world, day in and day out, in many cases at some hazard.

I won't attempt to cover the full scope of worldwide threats in these brief oral remarks, so I'd like to highlight just some of the issues that we identified for the coming year.

Never has there been, in my almost 49-year career in intelligence, a more complex and interdependent array of challenges than that we face today. Capabilities, technologies, know-how, communications, and environmental forces aren't confined by borders, and can trigger transnational disruptions with astonishing speed, as we have seen.

Never before has the Intelligence Community been called upon to master such complexity on so many issues in such a resource-constrained environment. We're rising to the challenge by continuing to integrate the Intelligence Community, as you've both alluded, taking advantage of new technologies, implementing new efficiencies, and, as always, simply working hard. But candidly, maintaining the world's premier intelligence enterprise in the face of shrinking budgets will be difficult. We'll be accepting and managing risk, more so than we've had to do in the last decade.

We begin our threat assessment, as we did last year, with the global issues of Terrorism and Proliferation.

The Intelligence Community sees the next two or three years as a critical transition phase for the terrorist threat, particularly for al-Qa'ida and like-minded groups. With Usama bin Ladin's death, the global jihadist movement lost its most iconic and inspirational leader. The new al-Qa'ida commander is less charismatic, and the death or capture of prominent al-Qa'ida figures has shrunk the group's top leadership layer. However, even with its degraded capabilities and its focus on smaller, simpler plots, al-Qa'ida remains a threat. As long as we sustain the pressure on it, we judge that core al-Qa'ida will be of largely symbolic importance to the global jihadist movement. But regional affiliates, as the ones you mentioned , and to a lesser extent, small cells and individuals, will drive the global jihad agenda.

Proliferation – that is, efforts to develop, acquire, or spread weapons of mass destruction – is also a major global strategic threat. Among nation-states, Iran's technical advances, particularly in uranium enrichment, strengthen our assessment that Iran is well capable of producing enough highly enriched uranium for a weapon, if its political leaders, specifically the Supreme Leader himself, choose to do so. North Korea's export of ballistic missiles and associated materials to several countries, including Iran and Syria, illustrate the reach of the North's proliferation activities. We don't expect Kim Jong Un, North Korea's new young leader, to change Pyongyang's policy of attempting to export most of its weapons systems.

I would note that, in this year's Statement for the Record, we elevated our discussion of Cyber Threats to follow Terrorism and Proliferation. The cyber threat is one of the most challenging ones we face, as you alluded. We foresee a cyber environment in which emerging technologies are developed and implemented before security responses can be put in place. Among state actors, we're particularly concerned about entities within China and Russia conducting intrusions into U.S. computer networks and stealing U.S. data. And the growing role that non-state actors are playing in cyberspace is a great example of the easy access to potentially disruptive and even lethal technology and know-how by such groups. Two of our greatest strategic cyber challenges are: First, definitive, real-time attribution of cyber attacks – that is, knowing who carried out such attacks and where these perpetrators are located. And second, managing the enormous vulnerabilities within the I.T. supply chain for U.S. networks.

Briefly, looking geographically around the world.

In Afghanistan, during the past year, the Taliban lost some ground, but that was mainly in places where the International Security Assistance Forces, or ISAF, are concentrated. And the Taliban senior leaders continue to enjoy safe haven in Pakistan. ISAF's efforts to partner with Afghan National Security Forces are encouraging, but corruption and governance challenges continue to threaten the Afghan Forces' operational effectiveness. Most provinces have established basic governance structures, but they struggle to provide essential services. The ISAF and the support of Afghanistan's neighbors, notably and particularly Pakistan, will remain essential to sustain the gains that have been achieved. And although there's broad international political support for the Afghan Government, there are doubts in many capitals, particularly in Europe, about how to fund Afghanistan initiatives after 2014.

In Iraq, violence and sporadic high-profile attacks continue. Prime Minister Maliki's recent aggressive moves against Sunni political leaders have heightened political tensions. But for now, the Sunnis continue to view the political process as the best venue to pursue change.

Elsewhere across the Middle East and North Africa, those pushing for change are: Confronting ruling elites; sectarian, ethnic, and tribal divisions; lack of experience with democracy; stalled economic development; military and security force resistance; and regional power initiatives. These are fluid political environments that offer openings for extremists to participate more assertively in political life. States where authoritarian leaders have been toppled, like Tunisia, Egypt, and Libya, have to reconstruct their political systems through complex negotiations among competing factions. In Syria, regime intransigence and social divisions are prolonging internal struggles, and could potentially turn domestic upheavals into regional crises. In Yemen, although a political transition is under way, the security situation continues to be marred by violence, and fragmentation of the country is a real possibility.

As the ancient Roman historian Tacitus once observed: “The best day after a bad emperor is the first.” After that, I would add, things get very problematic.

The Intelligence Community is also paying close attention to developments across the African continent, throughout the Western Hemisphere, Europe, and across Asia. Here, too, few issues are self-contained. Virtually every region has a bearing on our key concerns of terrorism, proliferation, cybersecurity, and instability. And throughout the globe, wherever there are environmental stresses on water, food, and natural resources, as well as health threats, economic crises, and organized crime, we see ripple-effects around the world and impacts on U.S. interests.

Amidst these extraordinary challenges, it’s important to remind this distinguished body and the American people that, in all of our work, the U.S. Intelligence Community strives to exemplify American values. We carry out our missions with respect for the rule of law and the protection of civil liberties and privacy.

And that pledge leads me to a crucial recommendation on our highest legislative priority this year, and it requires the support of this committee and both Houses of Congress. The Foreign Intelligence Surveillance Act Amendments Act, or FAA, is set to expire at the end of this year. Title VII of FISA allows the Intelligence Community to collect vital information about international terrorists and other important targets overseas. The law authorizes surveillance of non-U.S. persons located overseas who are of foreign intelligence importance, meaning they have a connection to, or information about, threats such as terrorism or proliferation. It also provides for comprehensive oversight by all three branches of Government to protect the privacy and civil liberties of U.S. persons. The Department of Justice and my office conduct extensive oversight reviews of these activities, and we report to Congress on implementation and compliance twice a year.

Intelligence collection under FISA produces crucial intelligence that is vital to protect the nation against international terrorism and other threats. We’re always considering whether there are changes that could be made to improve the law; but our first priority is reauthorization of these authorities in their current form. We look forward to working with you to ensure the speedy enactment of legislation reauthorizing the FISA Amendments Act, so that there is no interruption in our ability to use these authorities to protect the American people.

So I’ll end this brief statement where I began: The fiscal environment we face as a nation and in our Intelligence Community will require careful identification and management of the challenges the IC focuses on, and the risks that we must mutually assume.

With that, I thank you and the members of this Committee for your dedication to the security of our nation, your support for our men and women of the Intelligence Community, and for your attention today. My colleagues and I look forward to your questions and our discussion. Thank you.

###