Opening Statement of Senator John McCain
Chairman, Senate Armed Services Committee

Room SDG-50
Dirksen Senate Office Building
Thursday, March 19, 2015

To receive testimony on U.S. Strategic Command, U.S. Transportation Command, and U.S. Cyber Command in review of the Defense Authorization Request for Fiscal Year 2016 and the Future Years Defense Program

The Committee meets today for its annual posture hearing on U.S. Strategic Command, U.S. Transportation Command, and U.S. Cyber Command. I'd like to welcome our witnesses today, and thank them for their honorable service.

For nearly seventy years during the Cold War, deterrence provided a strong foundation for strategic stability and predictability. Despite frequent tensions throughout this time, we knew who our enemies were. We knew what they were capable of. And as a result, we were able to develop deterrence strategies by making our intent known, regularly demonstrating our capabilities, and continuously training to hone our skills. Asymmetric threats were a concern, but global stability was won or lost at the nuclear level. And the U.S. Homeland was beyond the reach of all but the most advanced long-range missiles.

As Henry Kissinger explained to us in January, world order today is being defined not by "objective strength" but by "psychological contests and asymmetric war." The existing world order is being redefined. Our hearing today, while part of our annual Combatant Command posture hearings, provides us with an opportunity to hear from our witnesses how this changing world order impacts their missions and strategic thinking.

Dr. Kissinger also noted that "serious attention must be given to the lagging modernization of our strategic forces." Indeed, while spending on U.S. nuclear forces has declined over the last two and a half decades, Russia and other nuclear powers are increasing reliance on their nuclear forces.

Today Russia thinks strategically about the role of nuclear weapons, space, and cyber in its national security strategy and, in particular, its strategy in Eastern Europe.

- Russia used cyber capabilities in Estonia, Georgia, and Ukraine.
- It is weaponizing space with new anti-satellite capabilities.
- It has updated its nuclear doctrine and has threatened to deploy dual-capable systems in Crimea.
- Its Long-range bombers penetrate U.S. and allied defensive zones more frequently.
- Russia is developing a nuclear ground-launched cruise missile in violation of the 1987 INF Treaty.
- And the Russia military is pursuing modernization across the entire suite of nuclear systems.

Russia likely is using its nuclear and cyber capabilities to intimidate and coerce NATO as part of its broader strategy to prevent the West from intervening in its invasion of the Ukraine.

It's not just Russia. Admiral Haney notes that "nuclear weapon ambitions…are increasing the risk that others will resort to weapons of mass destruction coercion in regional crises or WMD use in future conflicts." This warning is more dire given the decline in NATO Europe's military capabilities and the deterioration in U.S. readiness from budget constraints. We will want to hear from Admiral Haney whether the President's budget request for nuclear forces allows us to maintain and modernize the U.S. nuclear Triad – and ensure that replacement systems are available when our aging nuclear submarines, bombers, and ICBMs face retirement next decade.

Admiral Haney: We also look forward to your assessment of the increasingly serious threats that the United States faces in space. The fact is, some states are actively militarizing space to our detriment, and we need to develop a strategy—with full resourcing of the ways and means—to defend against this growing threat.

With respect to Cyber Command, the North Korean attack on Sony illustrated how cyber warfare has reshaped the battlefield. As I have said, this incident and its apparent success will breed future – and more significant – attacks and has exposed serious flaws in the Administration's cyber strategy. The failure to develop a meaningful cyber deterrence strategy has increased the resolve of our adversaries and will continue to do so at a growing risk to our national security until we demonstrate that the consequences of exploiting the United States through cyber greatly outweigh any perceived benefit.

Our ability to keep pace with the cyber threat and deter aggression requires that we effectively train, arm, and equip the over 6,000 person cyber force we are currently building. The FY16 budget included $5.5 billion in cyber investments. Unfortunately, as it turns out the budget is disproportionally focused on network infrastructure with only 8 percent of that $5.5 billion allocated for Cyber Command and the development of our Cyber Mission Forces. I am concerned that a strategy too heavily weighted towards defense is a losing strategy. Moreover, at the current levels of investment, we are at great risk of having a hollow cyber force.

For U.S. Transportation Command, just last year this Committee conducted an exhaustive investigation of the cyber threats facing TRANSCOM. According to the Pentagon, Chinese military analysts, for example, have identified logistics and mobilization as potential U.S. vulnerabilities. Given Transportation Command's dependence upon the private sector, and the fact that the vast majority of their business is conducted on unclassified networks, this Committee felt it important to enhance the Department's ability to share information with its critical transportation contractors and assist them in detecting and mitigating cyber attacks.

Additionally, U.S. Transportation Command faces challenges from the reduction of the size and scope of U.S. forces and their deployments overseas. As a result, Transportation Command must intelligently reduce and streamline its budget and management infrastructure while maintaining the ability to expand rapidly to react to future contingencies.

As Dr. Kissinger stated, "[T]he role of the United States in indispensable. Especially in a time of global upheaval." Failing to maintain nuclear deterrence, modernize the nuclear triad, defend ourselves in space, and establish effective cyber deterrence will threaten American leadership.