Army Cyber Command Ball Keynote

Event Theme – "Innovation"

Hilton Old Town, Alexandria, VA – Aug 15, 2014

- I would like to thank LTG Cardon for inviting me to speak at this great event tonight.

- LTG Cardon has a very impressive record, with several tours in Iraq and Bosnia, and is extremely well suited to his current challenging assignment leading this Army's efforts in the new domain of cyberspace.

- You and Command Sargent Major Harris have been given an incredibly vital mission to train, equip, and lead the Army's cyber warriors as they defend the Army's networks and protect U.S. national security interests throughout the cyberspace domain. As we move through the uncharted terrain of the cyber domain, the work you are all doing in developing the necessary cyber tools, tactics and procedures will be vital to our national and economic security for decades to come. You are writing the book on Army cyber operations.

- I would like to thank the two of you for your outstanding work leading Army Cyber Command and for your dedicated service to your nation. While I'm at it, I would like to thank all the service men and women here in the audience tonight for all your hard work and sacrifices over the years to keep us all safe.

- It's been a rough couple of weeks in the Middle East and the terrorist group ISIL has taken control of large swathes of Iraq and Syria. With events like this in the news just about every day, it might be hard for the men and women of Army Cyber Command to stay focused on their cyber security work. I would, however, urge you to stay focused on the important task at hand.

- I don't diminish for a second the threat that terrorist groups like ISIL pose to the U.S. and our allies. But as I am sure you all know, there are cyber threats also looming that can be just as dangerous to U.S. national security, and in some cases, even more dangerous.

- Our adversaries, and potential adversaries, in places like Iran, China, and Russia, are always looking for asymmetric means to challenge the U.S. military. They

know they are no match for us if they fight us on our terms, so they look for ways to change the game. There is probably no better and cost-effective way to change those rules than to do it in cyberspace.

- Not surprisingly, these and other countries are hard at work developing cyber tools and weapons to gain asymmetric advantages over the U.S. and our allies. We must work hard to maintain our dominance of the cyber domain. I can, therefore, think of no better theme for tonight's event than "innovation." Innovation will be the key to the ability of the Army, the rest of our military, and the rest of our nation to defend ourselves and U.S. national security interests in the cyber domain.

- I must say that I have often been impressed over the last decade and more of war by the U.S. military's ability to adapt and innovate in the face of the many challenges we have been confronted by. Even this pace of innovation, however, will not be sufficient if we are to maintain the cyber dominance that is necessary to defend the security of the United States. I am confident, however, that we are up to the task of innovating our cyber tactics and tools faster than our adversaries.

- Despite many predictions to the contrary early in the 20th Century, air power never replaced military ground and naval operations. The many Combat Infantry Badges in this room tonight so recently earned in places like Iraq and Afghanistan are a clear testament to that. U.S. domination of the air domain remains vital to the effectiveness of our military operations, but it will always work in concert with our operations on the land and on the sea.

- Just the same, I don't think operations in the cyber domain will replace the need for the U.S. military to operate in the other physical domains of land, air and sea any time soon. Like air power, however, I believe cyber is already a vital capability and will remain so in the future.

- The cyber work you all do will be vital not just for the defense of Army and DoD networks, but also for over-all U.S. national and economic security.

- Take, for example, China's unprecedented economic cyber espionage campaign against the U.S. and our allies. China's corrupt and inefficient economic system does not allow them to innovate like we do here in the U.S., so they try instead to steal our innovation and trade secrets so they can compete against American companies in international markets.

- The technological leadership and national security of the United States is at risk because some of our most innovative ideas and sensitive information are being brazenly stolen by this cyber espionage. The Chinese intelligence services that conduct these attacks have little to fear because we have no practical deterrents.

- China's economic cyber espionage is not the only threat we now face. American financial institutions were subjected to an intense campaign of "distributed denial of service" (DDoS) attacks on their networks last year. While the DDoS tactic isn't new, the scale and speed with which it happened was unprecedented and made the attacks very difficult to defend against.

- While the U.S. government has not yet publicly attributed these attacks to a particular source, the attacks have been widely attributed in the press to Iran and the Iranian government. When you consider the level of sophistication of these attacks and the level of resources that have been devoted to them, it can only be a nation-state entity.

- Moreover, in our conversations with elements of the private sector that are involved with dealing with these attacks, I have heard nothing to dissuade me from the conclusion that the Iranian government is behind these attacks.

- It's not hard to imagine what the next wave of Iranian attacks on the U.S. will look like if we do nothing to deter them. A very sophisticated virus called Shamoon infected computers in the Saudi Arabian State Oil Company Aramco in 2012. Shamoon has been widely attributed in the press to Iran and the Iranian government.

- Shamoon replaced crucial systems files with an image of a burning U.S. flag and overwrote all the real data on the machine. More than 30,000 of Aramco's computers that it infected were rendered useless and had to be replaced.

- There was a similar attack days later on RasGas of Qatar, a major energy company in the region. The Shamoon virus has been described as the most destructive attack that the private sector has seen to date. These same tactics can be used by Iran and our other adversaries to degrade or damage American critical infrastructure.

- The picture I am painting for you is, of course, very grim. I don't sleep very well at night, so why should you? I'm only 25 years old – look at what this job has done to me!

- All kidding aside, the challenges and threats we face in cyberspace are serious, but I am confident that like so many times before in our nation's history that we will rise to the challenge.

- It will not be easy, but I know that the men and women of Army Cyber Command are up to the task of working hard and innovating new tools, tactics and procedures to meet the many cyber threats we face. Hooah!