BROOKINGS INSTITUTION

Thursday, 27 June 2013

GENERAL MARTIN E. DEMPSEY

****AS PREPARED FOR DELIVERY****

Defending the Nation at Network Speed

Thank you Peter.

I am honored to be here at Brooking's Center for 21st Security and Intelligence.

When I asked my staff about the fellows at your Center, they told me that you have experts on drones, private security contractors, one of the people who discovered Stuxnet, the editor of the most controversial national security blog, and our former commander in Afghanistan, my good friend John Allen.

I should have brought body armor for the question and answer session.

Just remember Peter, you may write about drones, but I have them.

In all seriousness, I am thrilled to be with scholars who are looking to the future. Especially as the defense community focuses inward on the implications of sequester, it is important to look outward, at the changing world around us.

One person who always looked outward was Douglass Engelbart. After serving as a radar technician in World War II, Engelbart become an engineer at Stanford. It was a heady time in computer science. Forty-six years ago this week he submitted a patent application titled "X-Y position indicator for a display system." He nicknamed his invention the "mouse." Engelbart's research was funded by DARPA's predecessor. His lab at Stanford was one of the four original nodes of the Internet. And the mouse he invented with taxpayer funds was later licensed to Apple—for a meager $40,000.

The revolution in computing technology Engelbart helped start has transformed our world. More than a billion mice are in use today. Three

billion people have access to the web. By this time next year I'm sure my toaster will be connected to the internet and probably be tweeting about it. I can see it now -- hash-tag "burnedtoast@quarters6." But the spread of digital technology has not been without consequence. It has also introduced new dangers to our security and safety.

Since becoming Chairman, I have focused on what this revolution means for our military. I visited Silicon Valley, sat with the security teams of major tech companies, and spent time with an internet service provider. I sought out tech experts and even met with a venture capitalist.

One thing is clear. Cyber has escalated from an issue of moderate concern to one of the most serious threats to our national security. We now live in a world of weaponized bits and bytes, where an entire country can be disrupted by the click of mouse.

There are new missions we must take on as a military, and steps we must take as a nation, to defend ourselves from this threat.

Cyber incidents have steadily escalated over the past year. U.S. banks have been hit with sophisticated denial-of-service attacks. Last August, in the first large-scale destructive attack, the Shamoon virus wiped the hard drives of 30,000 computers at the Saudi Arabian state oil company, Saudi Aramco. Over 20 nations now have military units dedicated to employing cyber in war. And toxic malware continues to proliferate among militaries and hackers alike.

This is the new normal in cyberspace—disruptive and destructive cyber attacks are becoming a part of conflict between states, within states, and among non-state actors. Even if a state adversary does not engage in cyber conflict, global hacktivists might on its behalf. The borderless nature of cyberspace means anyone, anywhere in the world, can use cyber to affect someone else.

Strengthening cyber defenses on military systems is critically important, but it isn't enough to defend the nation. In cyber conflict, civilian infrastructure and businesses are often targeted first. Since I became Chairman, intrusions into our critical infrastructure have increased 17-fold. The computer control systems that operate our chemical, electrical, water, and transport sectors have all been probed. Several intruders have successfully gained system access.

The gap between the cyber defenses deployed across critical infrastructure and offensive tools we know exist presents a significant vulnerability for our nation. Secretary of Defense Chuck Hagel has called cyber an "insidious, dangerous threat." Former Secretary of Defense Panetta has noted we are at a "pre-911 moment" in which "attackers are plotting" but our nation stands underprepared. Today, I add my voice again to the chorus of concern.

In response to the threat, the Department is growing our capacity to protect our networks. We are also taking on a new mission—defending the nation from cyber attack. To do this we are integrating the cyber mission across the force and adding personnel to U.S. Cyber Command. Over the next four years 4,000 cyber operators will join the ranks. We are also investing $23 billion dollars in cybersecurity. We are doing all of this not to address run of the mill cyber intrusions, but to stop attacks of significant consequence – those that threaten life, limb, and the country's core economic functioning.

At Cyber Command, three kinds of teams will operate around-the-clock. National mission teams will counter adversary cyber attacks on our country. A second larger set of teams will support combatant commanders as they execute military missions. The largest set of teams will operate and defend the networks that support military operations worldwide.

These three teams constitute the cyber force that will defend our networks, defend military forces, and if called upon, defend the nation. Our most immediate priority is keeping the .mil domain secure. But in the event of a domestic cyber crisis, our cyber forces will work in support of the Department of Homeland Security and the FBI, who lead our nation's response in the .gov and .com domains.

To ensure this force is able to operate at network speed, rather than what I call "swivel-chair" speed, we now have a playbook for cyber. The President signed a directive that codifies how each part of the government will respond to a serious cyber attack. Under this directive, the Department of Defense has developed emergency procedures to guide our response to imminent, significant cyber threats. We are updating our rules of engagement—the first update for cyber in seven years—and improving command and control for cyber forces. We have more work to do, but these important steps significantly strengthen our ability to defend the nation at network speed.

While cyber may be our nation's greatest vulnerability, it also presents our military with a tremendous asymmetric advantage. The military that maintains the most agile and resilient networks will be the most effective in war. This is the kind of force we are building for the future, the Joint Force of 2020.

Each Service is doing its part. Cyber is strengthening the Air Force's ability to provide global reach. The Army is preparing to fight on battlefield that is as much defined by cyberspace as it is enabled by it. The Navy is putting its entire workforce through a cyber immersion program, and the Marines are smartly integrating cyber across the Corps. Collectively, the services are making the investments necessary to ensure the Joint Force can operate in cyberspace as capably as it can on land, sea, air, and space. This includes recruiting the right people for our cyber workforce, establishing common standards across the joint force, and achieving a higher degree of coordination in how we invest and manage our cyber resources.

The next step is making our networks joint. Today, the Department operates 15,000 networks. We are consolidating this sprawling mass of IT into a common set of enterprise services, all based in the cloud. The new "Joint Information Environment" will deepen collaboration across the services and mission areas. It will also be significantly more secure, helping ensure the integrity of our battle systems in the face of disruption.

As part of this new Joint Information Environment, we are building a secure 4G wireless network that will get iPads, iPhones, and Android devices online by mid-2014. In fact, I have a secure mobile phone with me here today.

This phone would make both Batman and James Bond jealous.

With tools like this, the smartphone generation joining our military will help us pioneer a new era of mobile command and control. This revolution will empower our greatest resource—the ingenuity of our people—and the philosophy of mission command we embrace.

To help unleash the potential for user-driven innovation, a federated appstore will allow any DoD user to write and share phone and tablet apps. By using off-the-shelf technology, we are bringing the full force of the tech revolution into the classified environment.

Although we have made significant progress embracing cyber within the military, our nation's effort to protect civilian critical infrastructure is lagging. Too few companies have invested adequately in cyber security. I worry that adversaries will seek to exploit this chink in our nation's armor. To them, our economy and infrastructure are softer targets than our military.

One of the most important ways we can strengthen cyber security across the private sector is by sharing threat information. Right now, threat information primarily runs in one direction—from the government to operators of critical infrastructure. Very little information flows back to the government. This must change. We can't stop an attack we can't see.

I am confident indicators of an impending attack can be shared in a way that preserves the privacy, anonymity, and civil liberties of network users. I understand that the country is debating the proper purpose, and limits, of intelligence collection for national security. Let me be clear -- these are two different things. One is collecting intelligence to locate foreign terrorists and their domestic co-conspirators; the other is sharing information about malware to protect our critical infrastructure from a different kind of attack. We cannot allow these separate debates to become conflated. The reality is that every day adversaries are injecting malware into our networks. The worst of this malware is equivalent to cyber bullets and bombs. We must share what it looks like so we can stop it before it detonates.

Ultimately, it will take legislation to significantly strengthen our ability to withstand cyber attacks while safeguarding civil liberties.

Information sharing is just one way to be safer. Improving cybersecurity standards is another. Still a third is to work with other nations to set norms of responsible behavior in cyberspace. One of our most important dialogues on cyber is with China. During my visit there last month I reinforced the need for us to address cyber in the working group that Secretary Kerry proposed. We are poised to make progress in meetings that begin next month.

Avoiding miscalculation in cyberspace is another important goal. Our agreement to open a cybersecurity link with Russia is a step in the right direction—a step we should eventually take with others.

So as you can see, we have our work cut out for us—as a military, a government, a nation, and an international community.

The rise of cyber is the most striking development in the post-9/11 national security landscape. Not only are military systems being targeted by tools that can cause physical destruction. Adversaries can increasingly hold our nation's critical infrastructure at risk. As a result, our military must be ready to defend the nation and to do so at network speed.

We are doing everything we can inside the military to be ready to operate in cyberspace. I call on our elected officials and the private sector to match the urgency. Together, we must place this nation on surer footing against the cyber threat.

Thank you.