Remarks on the Department of Defense Cyber Strategy

As Delivered by Deputy Secretary of Defense William J. Lynn, III, National Defense University, Washington, D.C., Thursday, July 14, 2011
Thank you Hans.

Returning to NDU is especially meaningful for me. I was a fellow here at an evocative time. Reagan was President. Nuclear conflict with the Soviet Union dominated defense scenarios. And the Berlin Wall appeared to forever separate two mutually-antagonistic world-systems.

Yet even at the height of the Cold War, epoch-making forces were at work. We did not know it at the time, but the fall of communism was less than a decade away. Nor did we foresee the explosion and global spread of information technologies. The networks that became the internet were up and running the year I was here. We had no idea they would change history.

For all the capability information technology enables in our military and beyond, it also introduces new vulnerabilities. In 2008, a foreign intelligence agency penetrated our classified computer systems. Today, the cyber threat poses dangers to our security that far exceed what happened three years ago.

My purpose today is to outline a strategy for confronting these threats – the Department's first ever Strategy for Operating in Cyberspace.

The cyber environment we face is dynamic. As such, our strategy must be dynamic as well. So while today is an important milestone, it is only one part of the Department's efforts to learn and adjust through time.

Addressing hostile cyber activities against our nation will necessarily involve many parts of our government. White House Cyber Security Coordinator Howard Schmidt is here today, as are friends and colleagues at other departments and agencies. From DoD, I want to particularly thank Principal Deputy Undersecretary for Policy Jim Miller, cyber policy lead Bob Butler, DoD CIO Teri Takai, Cybercom Commander General Keith Alexander, and General James Cartwright, Vice Chairman of the Joint Chiefs of Staff. Keeping cyberspace secure will also require the perspectives and capabilities of those with whom we share this space—especially private and commercial users.

Many of these users have already been affected by criminal activity. And while identifying criminal activity in cyberspace is of concern, this is not the Defense Department's primary concern. Rather, our concern is specific to activities that threaten our mission to protect the security of the Nation. We do not know the exact way in which cyber will figure in the execution of this mission, or the precise scenarios that will arise. But the centrality of information technology to our military operations and our society virtually guarantees that future adversaries will target our dependence on it. Our assessment is that

cyber attacks will be a significant component of any future conflict, whether it involves major nations, rogue states, or terrorist groups.

Tools capable of disrupting or destroying critical networks, causing physical damage, or altering the performance of key systems, exist today. The advent of these tools mark a strategic shift in the cyber threat—a threat that continues to evolve. As a result of this threat, keystrokes originating in one country can impact the other side of the globe in the blink of an eye. In the 21st Century, bits and bytes can be as threatening as bullets and bombs.

But disruptive and destructive attacks are only one end of a continuum of malicious activity in cyberspace that includes espionage, intellectual property theft, and fraud. Although in the future we are likely to see destructive or disruptive cyber attacks that could have an impact analogous to physical hostilities, the vast majority of malicious cyber activity today does not cross this threshold.

In looking at the current landscape of malicious activity, the most prevalent cyber threat to date has been exploitation—the theft of information and intellectual property from government and commercial networks. This kind of cyber exploitation does not have the sudden payoff of a bank heist or the dramatic impact of a conventional military attack. But by blunting our edge in military technology, and enabling foreign competitors to copy the fruits of our commercial innovation, it has a deeply corrosive effect over the long-term. It is hard to know how much damage this digital thievery does to our economic competitiveness and national security, but a recent estimate pegged cumulative economic losses at over a trillion dollars.

Today, sophisticated cyber capabilities reside almost exclusively in nation-states. Here, U.S. military power offers a strong deterrent against overtly destructive attacks. Although attribution in cyberspace can be difficult, the risk of discovery and response for a major nation is still too great to risk launching destructive attacks against the United States. We must nevertheless guard against the possibility that circumstances could change, and we will have to defend against a sophisticated adversary who is not deterred from launching a cyber attack.

Terrorist groups and rogue states must be considered separately. They have few or no assets to hold at risk and a greater willingness to provoke. They are thus harder to deter. If a terrorist group gains disruptive or destructive cyber tools, we have to assume they will strike with little hesitation. And it is clear that terrorist groups, as well as rogue states, are intent on acquiring, refining, and expanding their cyber capabilities.

So we stand at an important juncture in the development of the cyber threat. More destructive tools are being developed, but have not yet been widely used. And the most malicious actors have not yet obtained the most harmful capabilities. But this situation will not hold forever. There will eventually be a marriage of capability and intent, where those who mean us harm will gain the ability to launch damaging cyber attacks. We need to develop stronger defenses before this occurs. We have a window

of opportunity—of uncertain length—in which to protect our networks against more perilous threats.

To prepare our military for emerging cyber threats, we have developed a DoD Cyber Strategy. This strategy holds that our posture in cyberspace must mirror the posture we assume to provide security for our nation overall. Namely, our first goal is to prevent war. We do this in part by preparing for it. And we do so while acknowledging and protecting the basic freedoms of our citizens.

The steps we have taken to respond to the cyber threat has prompted discussion in recent weeks about "cyber-war" and its implications. As we release the DoD Cyber Strategy, it is important to address this topic head on.

Commentators have asked whether and how the U.S. would respond militarily to attacks on our networks. And this speculation has prompted concerns that cyberspace is at risk of being militarized—that a domain overwhelmingly used by civilians and for peaceful purposes could be fundamentally altered by the military's efforts to defend it. The concern here, as in other areas of our security, is that the measures put in place to prevent hostile actions will negate the very benefits of cyberspace we seek to protect.

We have designed our DoD Cyber Strategy to address this concern.

It should come as no surprise that the United States is prepared to defend itself. It would be irresponsible, and a failure of the Defense Department's mission, to leave the nation vulnerable to a known threat. Just as our military organizes to defend against hostile acts from land, air, and sea, we must also be prepared to respond to hostile acts in cyberspace. Accordingly, the United States reserves the right, under the laws of armed conflict, to respond to serious cyber attacks with a proportional and justified military response at the time and place of our choosing.

Our ability to identify and respond to a serious cyber attack is however only part of our strategy. Our strategy's overriding emphasis is on denying the benefit of an attack. Rather than rely on the threat of retaliation alone to deter attacks in cyberspace, we aim to change our adversaries' incentives in a more fundamental way. If an attack will not have its intended effect, those who wish us harm will have less reason to target us through cyberspace in the first place.

The logic behind denying the benefit of an attack rather than relying exclusively on the threat of retaliation flows from the nature of cyberspace itself. The internet was designed to be open, transparent, and interoperable. Security and identity management were secondary objectives in system design. This lower emphasis on security in the internet's initial design not only gives attackers a built-in advantage. It can also make intrusions difficult to attribute, especially in real time. This structural property of the current architecture of cyberspace means that we cannot rely on the threat of retaliation alone to deter potential attackers. Some adversaries might gamble that they could attack us and escape detection.

An important element of our strategy is therefore focused on denying or at least minimizing the benefit of an attack. If we can minimize the impact of attacks on our operations, and attribute them quickly and definitively, we may be able to change the decision calculus of an attacker. Enhancing our defenses also increases the resources needed to mount a successful attack, thereby making cyber attacks even less attractive to our adversaries.

This emphasis on cyber defenses illustrates how we are both mindful of those who would do us harm using cyber means, but also committed to protecting the peaceful use of cyberspace. Far from "militarizing" cyberspace, our strategy of securing networks to deny the benefit of an attack will help dissuade military actors from using cyberspace for hostile purposes. Indeed, establishing robust cyber defenses no more militarizes cyberspace than having a navy militarizes the ocean. This commitment to peace through preventive defense is at the heart of our DoD Cyber Strategy and the Administration's overall approach to cyberspace.

With this understanding, let me turn to the five primary pillars of our strategy.

First, as a doctrinal matter, the Defense Department is treating cyberspace as an operational domain, like land, air, sea, and space. Treating cyberspace as a domain means that the military needs to operate and defend its networks, and to organize, train, and equip our forces to perform cyber missions.

Second, we are introducing new operating concepts on our networks, including active cyber defenses. These active defenses use sensors, software, and signatures to detect and stop malicious code before it affects our operations—thereby denying the benefit of an attack.

The third and fourth pillars of our strategy recognize the interconnectedness of cyberspace and the diversity of uses to which it is put, by individuals, in our economies, and across nations. Because cyberspace is composed of many interwoven networks that perform many different functions, ensuring its peaceful use will require efforts on many fronts. The men and women of the military, other government agencies, our allies, the private sector, and indeed, the citizens of cyberspace must all play a role.

The third pillar specifically recognizes that a number of non-military networks support important military functions. This is especially true when it comes to the power grid, transportation system, and financial sector. So to protect our military capability, we must work with the Department of Homeland Security and the private sector to protect the nation's critical infrastructure.

Our fourth pillar carries this logic of interconnectedness to our allies and international partners. Our goal with them is to build collective cyber defenses. Collective cyber defenses will help expand our awareness of malicious activity and speed our ability to defend against ongoing attacks.

Fifth, our strategy aims to fundamentally shift the technological landscape of cyber security. Simply put, we want to enhance network security to reduce the advantages the attacker presently enjoys relative to

the defender on the internet. Leveraging the nation's technological and human resources to increase the security of network technology is not only in our best interest. A more secure and resilient internet is in everyone's interest.

Over the past year, we have made progress in each of these five pillars.

To centralize the operation and defense of our networks, we stood up U.S. Cyber Command and made it fully operational. We have established supporting activities in each of the military services. And we are now training our forces to thwart attacks that compromise our operations. Although no network will ever be perfectly secure, our military networks today are better defended, and our cyber hygiene more effective, than before.

On the international front, we have partnered with Australia, Canada, the United Kingdom, and our NATO allies. And under the President's International Strategy, we will seek greater cooperation with more nations in the coming months.

We have also committed half a billion dollars in R&D funds to accelerate research on advanced defensive technologies. Our research agenda includes novel approaches to improving network security and defense. We imagine a time when computers innately and automatically adapt to new threats. We hope for a world when we can not only transmit information in encrypted form, but also keep data encrypted as we perform regular computer operations. Having data encrypted 100% of the time would be a revolution in computer security, greatly enhancing our ability to operate in un-trusted environments.

Lastly, we have made substantial progress in working with private industry and the rest of government to make our critical infrastructure more secure. I would like to spend the final part of my remarks discussing this crucial area and its importance to national security.

To date, malicious cyber activity has been directed at nearly every sector of our infrastructure and economy. The I.M.F., Citibank, Sony's PlayStation Network, the secure token provider RSA, Google, NASDAQ, and multiple energy firms have been targeted. Cyber intruders have been so effective that even companies employing sophisticated commercial defenses have also fallen victim. In fact, our venue here today, the National Defense University, has been struck. The NDU website and its associated server were recently compromised by an intrusion that turned over system control to an unknown intruder.

The country's critical infrastructure has also been probed. Because much of this critical infrastructure supports military operations, its failure could compromise our abilities to protect the nation. Our military bases and installations are part of—and not separate from—the critical infrastructure on which all Americans depend. Ninety-nine percent of the electricity the U.S. military uses comes from civilian sources. Ninety percent of U.S. military voice and internet communications travel over the same private networks that service homes and offices. We also rely on the transportation system to move military personnel and freight, on commercial refineries to provide fuel, and on the financial industry to process

our payments.

Significant disruptions to any one of these sectors could impact defense operations. A cyber attack against more than one could be devastating. The integrity of the networks that undergird critical infrastructure must therefore be considered as we assess our ability to carry out national security missions.

In the United States, the Department of Homeland Security has responsibility for protecting critical infrastructure. In the past year, we have signed a memorandum of agreement with DHS to seamlessly coordinate our cyber security efforts. Wehave established a joint planning capability and exchange of personnel in our cyber operations centers. And we are helping Homeland Security deploy advanced defensive technologies on our government networks.

The critical infrastructure the military depends upon also extends to the private companies that build the equipment and technology we use. Their networks hold valuable information about our weapons systems and their capabilities. The theft of design data and engineering information from within these networks undermines the technological edge we hold over potential adversaries.

It is a significant concern that over the past decade, terabytes of data have been extracted by foreign intruders from corporate networks of defense companies. In a single intrusion this March, 24,000 files were taken.

When looking across the intrusions of the last few years, some of the stolen data is mundane, like the specifications for small parts of tanks, airplanes, and submarines. But a great deal of it concerns our most sensitive systems, including aircraft avionics, surveillance technologies, satellite communications systems, and network security protocols. The cyber exploitation being perpetrated against the defense industry cuts across a wide swath of crucial military hardware, extending from missile tracking systems and satellite navigation devices to UAVs and the Joint Strike Fighter.

Current countermeasures have not stopped this outflow of sensitive information. We need to do more to guard our digital storehouses of design innovation.

Toward that end, the Department of Defense, in partnership with DHS, has established a pilot program with a handful of defense companies. This program provides these companies with more robust protection for their networks. In this Defense Industrial Base—or DIB—Cyber Pilot, classified threat intelligence is shared with defense contractors or their commercial internet service providers along with the know-how to employ it in network defense. By furnishing this threat intelligence, we are able to help strengthen these companies' existing cyber defenses.

In this way, the DIB Cyber Pilot builds off existing capabilities that are widely deployed through the commercial sector. By leveraging infrastructure that already exists, the pilot suggests we can provide substantial additional protections across our critical infrastructure for only a fractional increase in cost.

In the DIB Cyber Pilot, the U.S. government is not monitoring, intercepting, or storing any private sector communications. Rather, threat intelligence provided by the government is helping the companies themselves, or the internet service providers working on their behalf, to identify and stop malicious activity within their networks. The pilot is also voluntary for all participants.

Although we are only beginning to evaluate the effectiveness of the pilot, it has already stopped intrusions for some participating industry partners. And through the information sharing the pilot promotes, we not only halted intrusions. We also learned more about the diversity of techniques used to perpetrate them.

The DIB Cyber Pilot breaks new ground in recognizing the interconnectedness of cyber and the important role of stakeholders in thwarting attacks. We have much to do to protect our critical infrastructure from sophisticated intrusions and attacks. But by establishing a lawful and effective framework for the government to help operators of critical infrastructure defend their networks, we hope the DIB Cyber Pilot can measurably enhance the security of our nation's critical infrastructure.

We are a long way from the world I knew while a fellow at NDU. Superpower competition has faded, yielding a strategic environment that is unlike anything we could have imagined. Whereas the Berlin Wall once divided us, now we are more interconnected than ever.

Our responsibility is to acknowledge this new environment and adapt our security instruments to it. That is the purpose of the DoD Cyber Strategy. We must prepare. We must recognize the interconnectedness of cyber. And we must be mindful of the many ways cyberspace is used–as a peaceful instrument of global communications, as a tool for economic growth–and, also, as an instrument to threaten and sometimes cause harm. Given this broad landscape of activity in cyberspace, we must both protect its peaceful, shared uses as well as prepare for hostile cyber acts that threaten our national security. The strategy we are announcing today helps establish that balance. It provides a framework for us to promote our nation's values in this vital civilian space while carrying out our duty to protect the nation.

Thank you.