Statement for the Record

The Honorable Michael Chertoff

Co-Founder and Managing Principal of The Chertoff Group

Before the

United States House of Representatives

Subcommittee on Crime, Terrorism and Homeland Security

November 15, 2011

Mr. Chairman, Representative Gohmert**,** Members of the Subcommittee:

Thank you for the opportunity to be here today and to contribute to the important effort being undertaken to better secure our most critical systems and networks operating in cyberspace. These operations are essential to our daily lives, global commerce and national security – and as a result – they continue to be targeted and attacked daily by a variety of actors ranging from today's modern-day criminals interested in pure financial gain to nation states seeking stronger advantages for their own global competitiveness. In my opinion, this persistent cyber threat represents one of the most novel and seriously disruptive threats to our national security since the onset of the nuclear age sixty years ago.

Since I left government in January 2009, I have continued to work on cyber security matters and have a greater appreciation of the challenges being faced by BOTH the private and public sector. I do want to make sure to inform this Committee from the start that within my private capacity as both Co-Founder of The Chertoff Group and Senior of Counsel with Covington and Burling, LLP, I do consult with companies on cybersecurity-related issues that could be discussed here today. However, my opinion and testimony today is wholly my own. In addition, these points being presented in my written statement will also appear in a cyber-security publication to be published by the Aspen Institute later this year.

In 2008, President George W. Bush ordered the launch of the Comprehensive National Cyber Security Initiative (CNCI), a now-declassified twelve point strategy to address cyber security threats across the civilian and military, government and private domains. The Department of Defense and the Department of Homeland Security convened a group of government and business leaders to address cyber security issues, under the rubric Enduring Security Framework. Shortly after taking office, President Barack Obama ordered a review of the CNCI, and subsequently reaffirmed the mandate to proceed with a national cyber initiative. President Obama appointed a White House official to coordinate strategy and Congress has taken up possible legislation.

Despite these various government initiatives, there is in place no comprehensive strategy for cyber defense and security. Recently, Deputy Secretary of Defense William Lynn described the Defense Department's evolving

approach to defending against cyber attacks, which are escalating as a serious counterintelligence and warfighting issue. Soon thereafter, Deputy Homeland Security Secretary Jane Lute responded with an opinion piece asserting that the internet is not a war zone, and arguing for a number of measures that the private sector can undertake to reduce its vulnerabilities to cyber attacks. This was followed by a Department of Homeland Security paper that elaborated on some characteristics of a more secure cyber "ecosystem". This summer, the Department of State issued an international cyber-strategy and the Department of Defense announced a cyber security information sharing pilot with certain major defense companies. At the same time, the Administration offered a legislative proposal to promote cyber security among operations of critical infrastructure.

But while these pieces approach and characterize the challenge of threats to our cyber systems, they do not yet amount to a unified vision of the problem and solution sets. Indeed, it sometimes seems that those examining the problem are talking past each other. At one end of the spectrum are those who portray cyber risks as verging on the catastrophic, sketching cyber combat scenarios that result in extinguishing our civilization. At the other end of the spectrum, are those who claim it's all overblown, and that the issue of cyber security is about updating virus protection and good police work.

To those who have been around the security community over the last decade, this will sound much like the familiar debate about terrorism, between those who claim it's a criminal problem to be addressed by law enforcement, and those who argue that terrorists have declared a war that must be fought with military capabilities.

In fact, the dichotomy between these approaches is oversimplified in the case of terrorism, and even more inadequate to define a strategy for protecting our cyber assets. Forcing cyber security into a simplified unitary framework limits our choices and underestimates the complexity of the most novel and serious disruptive threat to our national security in decades. Cyber threats will sometimes be a central dimension of military posturing and warfighting, and when they are critical will require the response of all elements of national power. On the other hand, much destructive activity is occurring at the commercial and individual level where military-type approaches are ill suited and where the actors are largely part of the

private sector. If we debate the way forward in protecting cyber assets as a philosophical choice between "militarizing the internet" or letting the market play the primary role, we rob ourselves of the full range of resources that we might mobilize.

Our ability to fully develop and implement national strategies for cyber security is hampered also by a tendency of the government agencies who participate to examine the problem from the perspective of their own authorities and capabilities. Abraham Maslow famously said that when you carry a hammer, everything looks like a nail. Our agencies carry different tool sets and often regard problems as whatever they can fix using the tools they carry. Our intelligence agencies in particular are rightly strongly conditioned to sharply restricting their activities within the United States and as relating to United States persons. But while there are legal rules that require this, at least the nonconstitutional limitations can be modified by lawmaking if there is good reason to do so. Likewise, Congress can use legislation to affect the respective roles of the government and the private sector in incentivizing or driving certain forms of cyber behavior. The point is that our solutions to cyber threats should not be a function of what we think we can do with the rules and tools that we have; those rules and tools should be crafted based on the development of a cyber defense and security (CDS) doctrine that sets forth our strategic objectives and the roles and responsibilities of government and private institutions across all the domains touched by cyber activities.

How do we develop a comprehensive CDS doctrine? Doing so begins with an appreciation of the scope and the nature of the threats. From that understanding, we should elaborate a doctrine that sets forth our national objectives in securing ourselves and the allocation of responsibilities between government and the private sector defense. The doctrine should also address allocation of government responsibilities among agencies, delineating which objectives each is responsible for achieving. A critical feature of developing this doctrine is balancing the various goals of security, privacy, freedom and economic prosperity. With that framework set, Congress can enact or adjust the authorities appropriate to allow execution of the doctrine subject to constitutional or civil liberties constraints. This article begins the process of posing questions that must be answered to develop the strategy under the preceding template.

Threats and Consequences.

While it is fair to say that the internet is not a war zone, it could certainly become one. Moreover, war-like activity has been experienced as recently as 2007 and 2008. In the former year, Estonian government and financial institutions were the object of massive denial of service attacks aimed at disrupting and denying their ability to function. And when Russia invaded Georgia in 2008, ground movements were accompanied by cyber attacks aimed at disrupting Georgian command and control functions. Indeed, the United States-China Security Commission – a Congressionally-mandated body – has identified cyber warfare as an explicit part of Chinese military doctrine.

But the most cyber attacks are not this dramatic nor so obviously tied to classically war related activities. Recent media reporting reveals intrusions into financial institutions such as Nasdaq; theft of data from energy companies; exfiltration of data from Google; massive identity thefts and financial frauds. Much of this activity is directed from criminal groups, although nation states can also use the internet for intelligence purposes. While these are not destructive cyber activities, they can cause extremely serious personal and economic damage on a national scale. As Deputy Secretary Lynn's article last year made clear, huge volumes of sensitive commercial information and intellectual property are stolen on a regular basis. These data thefts directly affect our global competitiveness. Identity theft and credit fraud erode public trust in the internet which in turns has negative impact on investment and trade activity. On a personal level, there are heart rending stories of personal financial and reputational trauma caused by organized cyber crime and thievery.

While all of these threats can have serious consequences, the responses to each may be different in scale and type, and the appropriate allocation of responsibility will vary. Accordingly, it is helpful to disaggregate the cyber threats which we face into several categories.

Data theft involves the unauthorized and often undiscovered exfiltration of confidential or proprietary data from a system. This may include intellectual property, business sensitive information, confidential government information, and classified national security information.

Fraud involves using cyber tools to steal or deprive a victim of money, information or property (including personal information), by deceiving the victim into paying the money or furnishing the property or information under false pretenses.

Denial of service attacks interfere with access to or use of networks by overwhelming the network with data or commands so that its capacity to process additional data or commands is exceeded. This disrupts but does not necessarily damage or destroy the system under attack.

Destructive attacks damage or destroy or otherwise take control of the victim's computer systems. The consequences may range from denial of use, to corruption, to outright destruction of networks and systems, including those elements of physical infrastructure that are dependent on those systems.

Although popular culture reinforces the impression that the most significant threats are launched by attacks over the network by hacking into targeted systems, in fact devastating attacks can originate from different *vectors*. To be sure, malware can be introduced over the network by hacking remotely. But malware is often introduced through a *corruption of the supply chain* that embeds it within hardware or software. Equally dangerous are viruses that are introduced into a network by deceiving an authorized user into inviting it (for example, phishing, etc.), or through accidental or intentional compromise by an insider.

Foundations of a Cyber Defense and Security doctrine.

What are the ends of a CDS strategy? To establish a secure cyber environment within which public and private institutions can operate without excessive risk that systems will be crippled or damaged, or that valuable assets will be misappropriated or injured. But those ends coexist with other important objectives, such as fostering economic efficiency and creativity, and protecting privacy and individual rights. The development of a strategy for securing cyberspace, therefore, must balance these objectives and all consider the cost-effectiveness of various approaches. That amounts to cyber risk management.

From a defense and security standpoint, cyber risks differ from traditional security risks because of the degree to which they play out in the private sector.

Traditional consequential defense and security responsibilities are largely exercised by public authorities, such as the military or police. While private institutions may equip themselves against relatively low-level security threats, using private guards, locks and alarm systems, modern civil society does not expect – or even accept – that the responsibilities or authorities for security against major physical threats should be largely in private hands. No one suggests that civilian society equip itself with the responsibility to repel enemy invasions, and outside of private enclaves, we do not rely on private entities to police our streets.

What should be the government's responsibility and objectives in the realm of cyber defense and security (CDS)? Unlike the physical world, where major national security threats are largely – although not entirely – external, cyber attacks on privately owned networks might well be carried out – and even mounted – from or through platforms that were privately owned and domestic. Crippling of the power grid or our major financial institutions could have a catastrophic national impact, comparable to the effects of a major physical attack. But traditional perimeter military defenses would be irrelevant.

Some argue that cyber defense and security, therefore, is best left to the market and individual initiative and innovation. While it is true that the private sector has unleashed enormous creativity in developing aspects of our cyber economy, it is far from clear that market incentives will be sufficient to spur adequate investment in cyber security. Left to their own devices, few private companies would invest more in securing their cyber assets than the actual value of those assets. Yet in an interconnected and interdependent world, the failure of one part of the network can have devastating collateral and cascading effects across a wide range of physical, economic and social systems. Thus, the market place is likely to fail in allocating the correct amount of investment to manage risk across the breadth of the networks on which our society relies.

At one extreme, one could argue that the government should own a monopoly over cyber defense and security, assuming total responsibility for protecting public and private networks, and operating network defenses, accrediting hardware and software, and developing rules to reduce insider threats. At the other extreme, government would disclaim any responsibility in this sphere,

leaving the market and individual initiative to address these problems. Both of these are unrealistic.

Rather, in allocating responsibilities for CDS among government and private actors, therefore, we need to consider

(1) Who owns the network, asset, or system we seek to protect;
(2) How critical that network, asset or system is to vital or critical national interests, especially the interests of collateral or third parties;
(3) The nature and potential effects of the threat to be addressed;
(4) Whether government or private parties are best situated to respond quickly and effectively to the threat given architectural and economic features of the internet;
(5) Civil liberties and privacy constraints.

Naturally, the government's greatest role and responsibility will be directed at defense and government systems. These are owned by government agencies, and by definition most will be of national importance or at least networked to systems of national importance. As owner of military of civilian government systems, government is positioned operationally and legally to maintain awareness of what occurs in these systems, and to protect them.

Responsibility should be shared – but with a fair degree of government involvement – for those privately owned networks and systems which are deemed critical infrastructure based on interdependency or the essential nature of the services provided. Ownership and control of these networks are in private hands, but the ramifications of security failure in critical networks have much broader scope. Because the effect of intrusions into these critical systems can be magnified for interdependent third parties, merely market-based incentives may not be sufficient to drive enough investment in security for these systems. And government is a particularly important partner because it can leverage what Deputy Secretary Lynn described as "government intelligence capabilities to provide highly specialized active defenses."

But even if government is to be an active partner in managing cyber defense and security for privately held critical infrastructure, the specific methods and tools which government employs can still be sculpted to minimize intrusions on private

economic concerns and civil liberties. For the government can promote defense and security in several (overlapping) ways:

Warning and situational awareness. Alerting potential targets about detected threats. One possibility is shared situational awareness through a common operating picture of the network.

Defense. Actively blocking malware or other attack tools.

Target hardening. Taking measures to make target networks and systems less vulnerable, such as by encrypting data; using hardware and software to promote better "cyber hygiene", including access controls, limits on downloading, internal network monitoring and tracking; and validating hardware and software from the supply chain.

Investigation and forensics. Actions taken to discover penetrations that already have occurred and to investigate their source. Where practical and appropriate, this effort can include prosecution of those who have mounted the attack.

Prevention. Preventing attacks before they are launched by incapacitating the attack vector or the individuals trying to mount the attack. Incapacitation can be accomplished using legal process, cyber means or even physical means.

Resilience. Building capabilities to survive and mitigate the effects of cyber attacks by creating redundancies, traffic management tools, etc.

In the case of each of these approaches, the government can in theory choose to execute the approach itself, or to encourage, enable, and/or require the private sector to execute the approach. For example, government will want to maintain a monopoly of control over acts of prevention that involve incapacitating attackers operating from platforms or servers overseas. That means that government alone could exercise the legal authority to defend against persistent cyber attacks by attacking the offending platform either using cyber tools or even physical means.

By contrast, it is likely government would want to leave in private hands much of the responsibility for hardening or reducing vulnerabilities of private systems, albeit with the encouragement and possibly enabling from the

government. In these areas where the government is not likely to intervene directly – say in building resilience across private networks, it can still deploy a variety of measures to prompt the private sector to execute defensive or security measures. These tools include (in increasing order of coerciveness) : (1) providing actionable information and best practices; (2) creating legal incentives and immunities for private action (including liability protection); (3) monitoring and assisting in operating defenses upon invitation or consent; and (4) forcing action through regulatory mandate or disclosure obligations.

The more intrusive and coercive techniques for driving various security measures into the private sector are obviously more likely to clash with protection of private property and civil liberties. By the same token, less heavy-handed tools such as information sharing and legal incentives and immunities are far less likely to engage controversy, and should be considered in the first instance in dealing with the kinds of threats – such as data theft or computer crime -- that are relatively lower on the consequence scale. Promoting government engagement in these less controversial ways provides an early opportunity to manage down cyber risks, even which we debate the role of government in addressing more sophisticated and higher consequence cyber threats, such as national security espionage or sabotage of our cyber infrastructure.

Evolving a doctrine.

The foregoing landscape of risks, capabilities, and public and private interests provides the canvas on which decision makers must strike the balance between competing goals of security, efficiency, privacy, and free movement over the internet. Where the government assumes responsibility for executing cyber security, doctrine refines specific policy principles.

For example, if the government exercises a monopoly over the right to prevent attacks by responding with force, using either cyber or physical tools, it must decide under how and when it will trigger the response in connection with different types of threats. For example, acts of espionage or data theft – which are the modern analog to old-fashioned spying – may well be regarded as insufficient to trigger retaliatory or preemptive action because the United States government has not generally treated espionage by foreign powers as in itself an act of war

warranting forceful response. On the other hand, a foreign nation's attack on the integrity of important command and control systems or critical infrastructure may well be sufficiently consequential to warrant response in force. Indeed, as during the Cold War, one element of a response doctrine in such cases should be announcement of a declared policy of active prevention or retaliation under certain specified circumstances. Another important element of a response in force doctrine would be elaboration of the type and nature of evidence deemed sufficient to attribute an attack to a particular actor.

At the other end of the security spectrum, where government shares security responsibilities with the private sector, doctrine will be necessary to set forth with clarity the expectations of both the public and private sectors regarding their shared obligations. When the government chooses to enable private sector security measures by engaging in warning, the doctrine should set forth when, how and with what degree of assurance warning will occur. A further decision is whether by invitation the government should actually share tools for gaining situational awareness with operators of a private network.

When the government chooses to regulate, doctrine determines whether the regulation will be highly prescriptive or simply set objectives and broad metrics, leaving flexibility for implementation to the private sector. And where the government engages in active monitoring or defense, the doctrine sets forth how government agencies will treat and share information they obtain.

Finally, once whole government doctrine is set, leaders should turn to the subsidiary issue of how to allocate any responsibilities which the government bears among various agencies, including intelligence agencies, law enforcement agencies, and regulators. All too often, evolution of government doctrine begins with agencies forging policies that are designed to expand or enhance their existing capabilities or authorities. But strategy should not be the handmaiden of interagency bureaucratic competition. Only when government roles, responsibilities, and functions have been formulated does it make sense which organizations are best suited to execute these based on their intrinsic capabilities and statutory purposes.

<u>Rewriting authorities.</u>

After doctrine is designed, it must be matched against existing authorities to determine whether these need to be amended or new ones created. The outer boundaries are of course set by the Constitution. Within those bounds, the doctrine should reflect privacy and other civil liberties concerns. Authorities can then be constructed to protect those concerns against encroachment. In dividing authorities among agencies, a balance should be struck between, on the one hand, assignment of authority to those who are best situated to discharge responsibility and, on the other, the desire to prevent undue concentration of power and to assure institutional mechanisms to prevent abuse in an area with sensitivity about freedom of communication.

But authorities should not be drafted as a means to ring fence bureaucratic turf against encroachment. And some long held legal restraints on agency action will have to be revisited if government is to play a serious role in promoting cyber defense and security. For example, venerable and strongly-held restrictions against intelligence agencies collecting information inside the United States or involving U.S. persons are difficult to apply when agencies are ask to participate in monitoring or defending global cyber networks that route packets through the United States as a matter of network traffic management. Should the monitor's ability to function depend on the happenstance whether a hop point in the routing process is located on a United States based server? Should the restriction be modified or lifted where the monitoring is not designed to collect the content of the cyber traffic, but simply to inspect individual packets to determine whether malicious code is embedded, or to watch traffic flow patterns to look for anomalies or suspect IP addresses?

If our strategy and doctrine concludes that the government should play a role in network monitoring and shared situational awareness – at least with the consent of the network owner and operator – then it makes no sense to exclude the appropriate intelligence agencies from that mission or should their authorities be adjusted to permit those activities. In that way, the legal rules of the road are crafted to enable government to execute our national cyber strategy, rather than subordinating the optimal strategy and doctrine to a set of legal rules largely built in a different era.

Thank you for inviting me to testify here today. I am happy to answer any questions.