From Risk to Resilience:
The Global Mission to Secure Cyberspace

Good morning ladies and gentlemen.

First, I would like to thank the several sponsors of this conference for their invitation. It is a pleasure to join you. The digital world is full of promise and of peril. It has neither geographic nor political boundaries. It has an ever expanding cohort of attackers – nation states, hacktivists, organized crime, individuals. The attack surface expands

everyday as does the level of complexity and sophistication of the malicious code. Cyber-attacks are a global menace and meeting the challenges to manage those risks and to build a culture of resiliency within an organization is critical to its survival and success. I am pleased to offer my thoughts on these and related subjects at your conference today.

I have had the opportunity to serve my community and my country in many difference capacities. Those experiences, from my time as an infantry soldier in Vietnam to my service as the first Secretary of the U.S. Department of Homeland Security,

have provided priceless opportunities to observe, learn, perform and lead. The totality of those experiences provide the foundation for the thoughts and opinions I share with you.

I am old enough to have witnessed the dawn of the internet, the growth and ascendancy of the hyper connected, inter dependent digital world and bold enough to predict the opportunities and challenges of the digital forevermore are permanent. The digital sun will never set.

It wasn't that long ago that the original computer based data transmission

protocol was created to facilitate communication between the U.S. Department of Defense and major research universities. While certainly primitive compared to the digital global ecosystem that drives commerce and culture throughout the world today, its core features remain the same.

The internet is an open system based on anonymity. It was not designed to be a secure communication platform. The opportunities and vulnerabilities within this global network, with electrons racing everywhere, and the capacity, uncertainty and inter dependency within the network bring

us together at this conference. The ubiquity of the internet is its strength. The ubiquity is also its weakness. We are all exposed to the potential malicious and malignant use of the internet. We all have a role and a need to combat its improper use. The risk escalates every day. It is a clear, present and permanent danger!

The malicious actors are known to all of us. Nations, organized crime, hacktivists, and individuals. Some governments are complicit with these actors. Some are indifferent to their activity. Others are fully aware, but unable to control it. Their motivations and desired outcomes are known to us

as well. Disruption, sabotage, theft, espionage. We also know that these digital trespassers are motivated, resourceful, focused and often well financed. As the former U.S. Secretary of Defense Donald Rumsfeld once observed about certain conditions on the battlefield, all of these elements in the digital space are "known knowns".

A comparison with contemporary war fighting, particularly with special operations, illustrates the challenges faced by those responsible to defend their country, company or organization from exploitation by the cyber guerrilla warrior. Cyber soldiers are asymmetric fighters. They eschew traditional

battlefield strategy and tactics. They camouflage their identity and activity in the vast, open and often undefended spaces of the internet. Their reconnaissance capabilities are both varied and effective. They constantly probe for weakness, an unauthorized point of entry, a "crack in the defense." They often use low tech weapons to inflict damage, yet they are able to design and build hi tech weapons to overcome specific defenses and hit specific targets.

The major American retailer, Home Depot, recently reported that a unique previously unseen malware was

responsible for the exfiltration of over 56 million pieces of personal information. Attackers have the ability to adapt. Defenders must do so as well.

Holding your enemy accountable from the air, land or sea is easier than in the digital space. A military sentry on guard at the perimeter can eliminate the aggressor on sight. Attributing a digital breach to a specific actor and holding him accountable in a meaningful way is often impossible.

Let's be clear. A digital perimeter defense, at one time the most important barrier to attack, is now just part of a multilayered defense strategy. In the 21st century, there are only two

kinds of organizations: those that have been hacked and know it and those that have been hacked and don't know it. There is a Chinese proverb that states "flies never visit an egg with no crack." Well, the internet is full of cracks. The barbarians are no longer at the gate. They are inside and often exquisitely concealed. That is the chilling and permanent reality of the digital universe forevermore.

If this is the reality, then how do governments and companies organize themselves to deal with it? Are they built to play offense, defense or both?

For centuries, governments have fought to gain information about their adversaries.

As Sun Tsu wrote: "It is only the enlightened ruler and the wise general who will use the highest intelligence of the army for purposes of spying and thereby they achieve great results."

First, by intercepting letters. By the 19th century, the efforts included intercepting telegraph messages. And, in the 20th century, radio and telephonic communications. But today, cyber traffic is more than just communicating. The digital world is connected to critical industrial control systems, financial systems, life sustaining systems and

more. All susceptible to attach and destruction.

There have never been any international norms around such behavior. And the possibility of a cyber-attack or attacks escalating into conflict is real. Nations will always act to protect, promote and improve their national and economic security interests.

But ultimately, the problem is not digital technology. The problem does not evolve around ones and zeroes, or bit, bytes and platforms. The problem is people. How far is leadership willing

to go to advance its interests? Many global citizens have concerns about miscalculations in the digital space. When does one country interpret another's aggressive exploitation of its military or corporate secrets or the clandestine insertion of malicious code in the industrial control systems of critical infrastructure as either a precursor to an attack or an act of war? Does the infected country respond with an equally sever digital attack or does it use conventional military weapons?

These types of situations give rise to political and military tensions, charges and counter charges. It is the unfortunate reality of our time. It may

be the unfortunate reality for all future time.

But in the midst of such national self-interest, countries can certainly find common ground and mutual interests which lend themselves to cooperation and collaboration in the digital arena. Even when countries offensive capabilities are a point of concern and friction, there are numerous defensive actions that can be jointly undertaken. Combatting organized crime that preys on companies and citizens, terrorists that recruit and finance, drug cartels and money launderers - bilateral and multilateral efforts to confront these

digital trespassers should be an international priority.

I am neither naive nor cynical. Even if common ground is found and these types of issues are addressed successfully, it may never alter how countries aggressively use the internet to advance their interest. One can only hope, however, that such success would open a path to an honest discussion about such use, and a means to reduce that risk and the dangers associated with it.

Governments can play offense, the private sector cannot. Government and

the private actor can and must play defense together since the infrastructure upon which most governments rely is primarily owned and operated by the private sector. In the United States it has been estimated that 85 percent of those critical assets are owned privately.

The definition of critical infrastructure is universal. They are systems or assets, virtual or physical, the impairment or destruction of which would have a "debilitating" impact on national and economic security, national public health or safety or any combination of those matters. Many are obvious.

Financial services, telecommunications, transportation, energy.

Defending critical infrastructure in the US has meant that both the public and private sectors have taken on new roles and responsibilities. A cornerstone of this undertaking was laid in February 2013 when President Obama issued an Executive Order entitled "Improving Critical Infrastructure Cybersecurity." Three of its most important components involve the creation of cyber security standards, information sharing and an administration and oversight panel to ensure that the government can achieve these

outcomes without violating the privacy and civil liberties of citizens.

Our National Institute of Standards and Technology was tasked to work with private companies to create a blueprint of operational checks and practices that would become part of a company's business and cyber risk mitigation strategy. The standards were built around the need to identify and detect the threat, protect against it, and build the capacity to respond and recover from an attack. Different cabinet agencies were given oversight responsibility over the sixteen different economic sectors that house these critical, nationally relevant assets.

Whether the battle is being fought on the ground or in the digital space, defenders must have as much information as possible to conduct effective operations to defend themselves. Situational awareness is a critical component of that effort. The order directed federal agencies to share relevant information with the private sector when they have identified a threat to a sector or to a specific piece of critical infrastructure. In the years prior to the executive order, different sectors had established ISACs - information sharing analysis centers, wherein businesses shared information among themselves relative to physical,

criminal and cyber risks. The president's order provides timely access to more and better information. It addresses the dual responsibility of the federal government to provide for the common defense and a safe and secure country while maintaining safeguards to protect the privacy and civil liberties of its citizens. In the age of multi-tasking, there are no greater missions for the U.S. Government to undertake.

People interact with the internet as users, consumers and citizens. Most are totally unaware of the amount of personal information the government and the commercial sector has about them. Much of it is mandated,

unprecedented levels are volunteered, and yes, some surreptitiously acquired. The United Nations Human Rights Council addressed the issue several years ago when it affirmed for the first time that human rights in the digital realm should be afforded the same protection as human rights in the physical world. One of the participants in the council meeting, Ambassador Hans Schumacher of Germany, observed that "every person is entitled to a 'private sphere' free from undue interference or surveillance by the State or, other actors. He urged the global community to "strike a balance between legitimate public and security

concerns and the fundamental human right to privacy in the digital age."

The relationship between countries and their citizens on this matter varies dramatically. Rarely is there complete transparency of the government's role. Governments for legitimate reasons have access to and retain substantial personal information about its citizens. With the advent of Facebook, Twitter, Linked In, and so many social media alternatives, citizens living in the modern world surrender information about themselves with astonishing regularity. Devices used by the population every day can be used to determine where you are, what you are

doing, who you are with and what you are thinking about at that moment. Some or all of the info can be collected, sorted, analyzed and used to profile and target individuals and groups through their digital networks for economic, social, national security, or political reasons.

This embrace of all that is digital, which means all that is accessible, may suggest that we don't cherish our privacy. Be assured, we do.

Preserving our civil liberties and privacy was clearly a concern of the U.S. Administration and Congress when, in response to the attack by Islamic fundamentalism on September 11,

2001, the Department of Homeland Security was created and the first ever Congressionally mandated Privacy Office was included. The country believed then and believes now that no matter how effective the technology might be to identify terrorists before they strike, no matter how grave the threat might be, protecting civil liberties is itself an essential part of protecting the homeland.

The privacy office was built to look carefully at what was collected, how it should be stored, when or if it should be collated, and whether it contained personally identifiable information. We looked at how long the data should be

held, who should have access to it and under what circumstances. To paraphrase one of America's iconic and historic figures, Benjamin Franklin, "he who is willing to surrender Liberty in exchange for security deserves neither". Limiting government's reach into the private domain of the citizen will be a permanent challenge in this digital, dangerous world. Technology must surely be an instrument of government to combat threats regardless of their nature. It should never be a weapon against its citizens!

I think it is important, if for only a moment or two, to celebrate the

potential benefits of the Information Age. There are an estimated 14 billion devices currently connected to the internet. The "internet of things" is upon us. The digital universe is expanding and no one can predict when it will stop. Forbes magazine recently estimated that, by the end of this decade, there will be 41 billion devices connected to the internet.

I recently read that the amount of stored information grows four times faster than the economy, while the processing power of computers has grown nine times faster. But as authors Victor Mayer-Schonenberger and Kenneth Clark concluded, "The real

revolution is not in the machines but in the data itself and how we use it.

The analysis of big data has, and will, contribute to more efficient manufacturing, more productive agriculture, improved health care, safer transportation, a cleaner environment - the actual and potential benefits are almost limitless. We can celebrate the positive but we cannot ignore the negative. The benefits are derived from using complicated math algorithms to make predictions. When the analysis involves personal information and the possibility or probability of certain actions or behavior, government and society must proceed with caution.

Data accumulation and analysis is not the epicenter of our concern, but its use. There must be rules circumscribing who has access to the data and how it is used. It has been written that Native Americans often refused to have their photograph taken because they thought it stole their soul. In the Information Age pieces of our digital DNA, our digital soul, are scattered everywhere. We must be ever vigilant that government never gathers the information that steals our soul and subjects it to the "tyranny of the algorithm. "

And as countries and individuals adjust to their ever changing digital

relationship, the government and the private sector must also modify their relationship to advance their joint commitment to economic and national security.

No government, corporation or entity can build an impregnable defense against cyber-attacks. Attackers have first mover advantage. They need only penetrate one point of entry to launch their attack. Given their persistence, patience and capabilities, it must be assumed that breaches will occur and damage will ensue. Unlike hurricanes, terrorists attacks and other potential disruptions of the operations of

government and business, cyber-attacks are a permanent 24/7 threat in the digital forevermore. They cannot ever be eliminated, they can and must be managed aggressively. To do so requires the creation of a culture of resiliency.

In the 20th century, W. Edwards Deeming introduced a novel concept to the global marketplace - total quality management. TQM was a philosophy, a mindset and a practice. Companies were challenged to view every single step as a critical juncture where performance and quality met. Everyone involved with the enterprise, employees, vendors, suppliers, all were

held to the highest possible performance standard to ensure that the end product was as good as it could be. No short cuts. No cutting corners. Every step along the way was view as a potential source of product enhancement or failure. The commitment to quality was nurtured and sustained throughout the entire organization and all that supported it. This was transformative to the business culture in the last century. Markets rewarded those who adopted the practice and punished those who rejected it.

In the 21st century, the adoption of a culture of resiliency will be

transformative. Black swan events, Mother Nature's fury, terrorists, major accidents and cyber-attacks all have the potential to be not only disruptive, but destructive. Organizations that are resilient - prepared to adjust and bounce back after the crisis - will also be rewarded by the markets. Those who fail to recognize the need to change will be left out. All those having digital access to the network must embrace and sustain the mind set and best practice. Access to the network can be hundreds or thousands of miles away and where access exists, so does potential vulnerability. Physical proximity to the enterprise is no longer

necessary. Proprietary information, industrial control systems, personal information - all vulnerable through the multiple nodes of connectivity that require 24/7 vigilance and protection. And since no defensive system is fail safe, a culture of resiliency requires plans to continue the operation after the attack.

In the US, business leaders have begun to embrace this approach. Cybersecurity is now more frequently viewed as a business risk, not an IT problem. Leaders have finally figured out that the impact of a cyber-attack is real, not virtual. More and more companies have begun to integrate

their information technology, operational technology and consumer technology under a unified Cybersecurity plan. Security spending has increased, enterprise wide cyber education has become a part of the culture and as previously mentioned a new relationship with the government is emerging. Perimeter defenses have given way to integrated strategies. A reactive mentality has been replaced by a preemptive approach. This mindset within the broader business community is not universally adapted, but everywhere I look I see significant change, I am reminded of the work done by Charles Darwin, the English

naturalist and geologist. His use of the phrase "survival of the fittest" has often been misinterpreted. When he wrote about evolution he was not contending that the smartest, strongest, and fastest survived, but rather those species that were able to adapt to change. Companies that adapt and develop a risk informed process of continuous improvement, security upgrades and a culture of resiliency will survive. The goal for all connected to and dependent on the internet is to manage digital risk, before it manages you!

There is no doubt in my mind that all of you in the audience have technical and operational knowledge of the World

Wide Web that exceeds that of most of your fellow global citizens. Unlike most, you can probably visualize, in all its complexity, the digital web that blankets the earth. And we know that on top of all those digital devices, servers, routers and other digital tools rests governments, millions of companies and billions of people. All are dependent upon it. All are connected with and through it.

There is doubt in my mind, however, about our ability to comprehend fully, the importance, fragility and the dependency of the Worldwide Web has created. I believe that no political leader, business executive, or citizen

can ever appreciate the breadth and depth of our global connectivity. We are intertwined more than we will ever know or ever understand.

Regardless of where we work, or what we do, we should all commit ourselves to the constructive use of the internet. We know the world is full of bad actors. We must work to combat them. They must also be reminded that an attack against another, may, in fact, be an attack against one's own self-interest. This is the nature of a hyper connected world. Or, as the saying goes, "though my left hand defeat the right, who wins?"

There are many answers to the questions raised to the challenges discussed. I believe many answers can be found by working together, though the path will involve a long and complicated journey.

But, I think it's our duty to try, as much for our children as it is for us! We don't inherit the earth from our ancestors, we borrow it from our children. Let's return it to them as a better and safer place. As the proverb say, "the journey of a thousand miles begins with a single step." Thank you for letting me take my first step with you.