Introduction

General Eberhart, thank you for that kind introduction, and thank you for inviting me here today. I greatly appreciate the work that you and the National Homeland Defense Foundation do to "Secure the Future of Liberty."[1] It is always a delight to return to Colorado Springs, where my Air Force career began more than a little while ago. And, it is my distinct honor to kick off this year's symposium on homeland security and defense, with some thoughts and perspectives that I hope will spur some discussion and debate, and perhaps table some ideas to push forward.

Reflections on the Effect of Infrastructure on American Culture

During my flight here, and in preparing for these remarks, I contemplated infrastructure—one of the themes of this symposium. I considered its vital role in our society, and the many significant developments that have occurred since my days as a cadet at the north end of town.

Some of these developments changed not just the face of our Nation, but its very culture. Consider this quote from a message to Congress:

> "Our unity as a nation is sustained by free communication of thought and by easy transportation of people and goods. The ceaseless flow of information throughout the Republic is matched by individual and commercial movement over a vast system of interconnected highways, crisscrossing the country and joining at our national borders with friendly neighbors to the north and south. Together, the united forces of our communication and transportation systems are dynamic elements in the very name we bear—United States. Without them, we would be a mere alliance of many separate parts."[2]

---

[1] NHDF mission statement: "The National Homeland Defense Foundation (NHDF) exists for the purpose of 'securing the future of liberty' through sharing of innovation, research, education, and information in the fields of homeland defense and security."

[2] Dwight D. Eisenhower, "Message to Congress re Highways," Abilene, Kansas: Dwight D. Eisenhower National Presidential Library Archives, February 22, 1955, http://www.fhwa.dot.gov/interstate/quotable.htm, accessed on 22 October 2010.

This was part of President Eisenhower's argument in favor of building the U.S. Interstate Highway System, and he wrote it more than a year before Congress approved his idea. As part of a statement about the Internet and our critical infrastructure, we probably could deliver a similar message to Congress today. President Eisenhower's landmark Federal-Aid Highway Act had just turned 13 when I began my freshman year at the Academy, and construction was far from complete. Yet, even at that time, Americans realized that the Nation had been transformed. As an article in *National Geographic* put it, "Americans are living in the midst of a miracle. A giant nationwide engineering project—the Interstate Highway System—is altering and circumventing geography on an unprecedented scale."[3] And, a piece in the *Atlanta Constitution* noted, "During the few short years of its existence, the word 'interstate' has become a part of the language of the American motorist…More than any other phenomenon of our time, the Interstate Highway System has irrevocably altered the way America must see itself. When Interstate comes, can anything once familiar ever be the same?"[4]

Reflections on the Effect of the Digital Revolution on the U.S. Air Force

As much as this new infrastructure had transformed America, one might argue that the interstate revolution was overshadowed in scope and magnitude by the digital revolution that soon followed. Upon graduating from the Academy, I was commissioned into an Air Force that ran almost entirely on paper. Across the force, forms monitors kept their eyes on hundreds of stocks of fill-in forms. It was an era of typewriters—which my father proudly sold and maintained, by the way—along with white-out, and carbon paper. Nobody owned a home computer, and few had them at the office. After all, the Apple II and TRS-80 hadn't even been invented yet.

In just a few short decades, all of that has changed. Today, forms are not only computer-generated; many now are routed, processed, approved, and stored digitally. One by one, the old standards of DoD culture have gone digital: medical

[3] Robert Paul Jordan, in *National Geographic*, February 1968, http://www.fhwa.dot.gov/interstate/quotable.htm, accessed on 22 October 2010.
[4] David Nordan, in the *Atlanta Constitution*, April 9, 1967, http://www.fhwa.dot.gov/interstate/quotable.htm, accessed on 22 October 2010.

records, performance reports, staff summary sheets, orders, and so on. To maximize the return on our investment in information technology, we transformed brick-and-mortar personnel offices, and created a virtual manpower and personnel office on the Internet. We slashed the number of airline ticket agents, and fielded the Defense Travel System. And, we haven't mailed a check or a pay stub in years; it's all direct deposit and paperless records now.

All of this is a mere sample of modern administrative processes. And, in the operational and mission support arena, the digital revolution continues to advance rapidly and relentlessly. For example, inspired by success in tracking cargo containers by using Radio Frequency Identification Devices, or "RFID," we are experimenting with "Total Asset Visibility" systems that tag individual assets, so that each shipped item can be tracked with greater accuracy and accountability, even after they have been unloaded from the cargo container. With this technology enabling the Expeditionary Combat Support System, or "ECSS," whose pilot version went "live" this past July at Hanscom Air Force Base in Massachusetts, logistics personnel and commanders worldwide soon will be able to more confidently and accurately determine the exact location of, ideally, every asset in the supply system. ECSS is designed to replace more than 240 Cold War–era systems in use today, few of which share data with each other, resulting in unnecessary duplication of effort and costly inaccuracies. Its potential to improve Air Force logistics operations represents a potential quantum leap in supply chain management. Along with Total Asset Visibility, ECSS will standardize and automate logistics processes, and provide an enterprise-wide view of the supply chain, ultimately making efforts more efficient and data more precise.

Increased Risk from Systems Vulnerabilities

But of course, there is a downside to this extraordinary technological progress. The more that we have grown to rely on this new and manmade domain of cyberspace, the more we have become vulnerable to threats to its safety, security, and reliability. As a Nation, we have some experience with addressing these concerns, having faced challenges to the security of our energy and critical infrastructure before. For instance, during my senior year at the Academy, when

America had become reliant on the personal automobile as the primary mode of transportation, the oil embargo caused gasoline supplies to plummet, prices to skyrocket, confidence to wane, and productivity to plunge.

However, the very pervasiveness of cyberspace throughout our society and critical infrastructure means that cyber security presents a challenge that is several orders of magnitude more complicated than the challenge of infrastructure protection, or managing oil supply interruptions, before the digital age. Case in point: during the oil embargo, gas pumps across the country were mechanical devices, and most purchases were made by cash.

Today, virtually every gas pump is computerized, as are various nodes in the fuel supply infrastructure; and, a very high percentage of transactions involve credit or debit cards. In today's security environment, all vendors—not just those who sell gasoline—must protect their customers' credit and debit card numbers. For that matter, vendors must also worry about the security of the electrical grid as well as the data link to credit card companies, in order to process sales.

So, referencing the passages that I quoted earlier, we could say that Americans are living in the midst of another miracle—another true revolution in which we either keep up or get left behind. During the relatively few years of its existence, a giant global information network—the Internet—has become a central part of American life, business, and culture. And, it has allowed a growing number of actors to circumvent international borders on an unprecedented scale. More than any other phenomenon of our time, the Internet has irrevocably altered the way in which American sees itself—and others. But, unfortunately, we now must also see ourselves as vulnerable in the largely unregulated domain of cyberspace, wherein aggressive and even malicious actors can act with relative anonymity and, therefore, impunity.

Responding to the Threat

Of course, analyzing vulnerabilities and assessing risks are but the first steps in planning an effective defense. As you might know, two years ago, the Defense Department received a rousing wake-up call concerning our vulnerabilities and related risks, when our networks were illicitly accessed. You may have heard

Deputy Secretary of Defense William Lynn speak about this incident, which he called “a seminal moment for cyber security in the Pentagon.” As Mr. Lynn explains, the investigation into the 2008 intrusion led to a new approach to cyber security for the DoD—a strategy with five pillars.

First, the DoD has recognized cyberspace for what it is: a new competitive domain—one in which we will operate and defend our most vital interests in a similar doctrinal manner with which we operate in the warfighting domains of air, space, land, and sea. This recognition is consistent with President Obama’s perspective on cyberspace. In his May 2009 address on securing our Nation’s cyber infrastructure, the President noted, “Al Qaeda and other terrorist groups have spoken of their desire to unleash a cyber attack on our country—attacks that are harder to detect and harder to defend against [than attacks in other domains].” We would do well to note that what President Obama calls “a weapon of mass disruption” can be unleashed by a few keystrokes and mere mouse clicks. President Obama concluded that the cyber threat is clearly “one of the most serious economic and national security challenges we face as a nation.” Therefore, we must harness the talent and effort of the entire Nation to meet these challenges.

Second, the DoD has determined that we require more active defenses to back up the useful but passive firewalls, and to create dynamic virtual environments instead of allowing static networks to remain vulnerable to potential aggressive action. Through innovative and promising technologies such as cloud computing, and massive network polymorphism that can alter virtual topologies in mere milliseconds, we can reduce the ability for potential aggressors to hunt through our networks, and increase our ability to find and disable any malware that manages to penetrate. This also makes aggressors more likely to leave forensic evidence of intrusion, which is vital for threat attribution, deterrence, and overall increased system resiliency.

Third, the DoD is committed to collaborating in the protection of our Nation’s critical infrastructure, such as the power grid, transportation networks, financial systems, and any other component that is critical to our economy and therefore, to our national security. The Department of Homeland Security is primarily

responsible for their protection, and just one month ago, Secretary Gates and Secretary Napolitano signed a memorandum of agreement on cyber security. Through this agreement, the DoD and DHS will step up collaborative efforts in planning for the Nation's cyber security, developing our capabilities in this field, and synchronizing our current operational cyber security efforts.

Fourth, the DoD has acknowledged that cyber defense is, internationally, a shared responsibility and endeavor. We have been collaborating on cyber defense with some of our closest allies, such as the United Kingdom, Australia, and Canada. The DoD now looks to NATO for possibilities of expanding this collective defense concept. There are a host of potential benefits to expanding our collective defense—benefits that are both diplomatic and technical in nature. As President Eisenhower might have put it, without collaborating with our NATO partners on cyber defense, we would be "a mere alliance of many separate parts."

Fifth, and finally, the DoD believes that we must continue to leverage the U.S. technological base not only to retain the edge that we currently enjoy to assure our ability to operate in cyberspace, but also to strengthen our cyber defenses and outmatch the ever-expanding and increasingly capable threats that challenge us in this domain. This is where cyber professionals in the private sector—like many gathered here today—play a key role, and also why fora such as this symposium are important, for the opportunities to foster genuine and productive collaboration.

Milestones in Cyber Defense

Let me briefly revisit DoD's recognition of cyberspace as an emerging competitive domain. Historically, the development of a new warfighting domain usually generated the requirements for new organizations, new doctrine, and new training to prepare those who would serve in the new domain. This was the case in the last century, with the development of air as a new domain of warfare, and of new organizations like the Army Air Service and the Army Air Corps, and of course, the U.S. Air Force.

Currently, this organizational requirement drove the recent establishment of the United States Cyber Command, the new sub-unified command whose mission includes "conducting full-spectrum military cyberspace operations in order to

enable actions in all domains, ensuring U.S. and Allied freedom of action in cyberspace, and denying the same to our adversaries." I am proud that the 24th Air Force—the Air Force component of USCYBERCOM—reached full operational capability earlier this month, which means that the Air Force is now more able to support the Joint team in meeting combatant commander requirements for missions in cyberspace.

In the doctrine arena, earlier this month, the Air Force's LeMay Center for Doctrine Development and Education announced final approval and publication of Air Force Doctrine Document 3-12, titled, "Cyberspace Operations." This document covers cyberspace fundamentals; the command and organization of our cyber forces; and processes for designing, planning, executing, and assessing the effectiveness of cyber operations.

And finally, in the training environment, the Air Force has fielded new courses that target two demographic groups key to our cyber defenses:

- our newly-recruited Airmen, so that they are inculcated with the fundamentals of information assurance and their everyday roles as cyber defenders; and
- our mid- to senior-level professional cyber warriors, who will team with our Joint, Interagency, and private sector partners to ensure our Nation's ability to operate in this newest of operating domains.

Earlier this month, in recognition of the fact that every Airman is the first line of defense in protecting Air Force networks, we expanded the Basic Military Training curriculum with four hours of cyber training, devoted to network defense and cyber operations. As the plan to further expand this training unfolds, trainees eventually will be using computers in the Basic Military Training classrooms—a first in the history of BMT.

Equally significant, on the 28th of October—tomorrow—over 100 students will graduate from the Air Force Institute of Technology's newest courses for cyber professionals preparing to assume intermediate-and higher-level responsibilities, including Airmen in the recently-established cyberspace operations career field. Courses like these will help keep our cyber Airmen and leaders up to date with the most recent developments in this exciting and fast-paced field.

Conclusion

As we recognize the enormous opportunities that cyberspace presents to our Nation, potential adversaries have taken note of our reliance on this critical domain. Therefore, as we leverage cyberspace, we must also address threats and challenges to our access to, and mission assurance in, that domain. My message to you this morning is this: While our Nation and its international partners and allies are vulnerable in cyberspace, which in turn creates risks to our critical infrastructure, disaster is far from a foregone conclusion. Instead, we can—indeed we must—leverage the abundant talent from all sectors of our country, including all here, to steel our networks and seek resiliency going forward, both simple and complex.

I assure you that your Air Force is fully engaged in cyber defense, eager to collaborate with others who are ready to rise to this challenge—our Joint and Interagency teammates, private industry partners and those in academia, and our international allies and friends as well. I am confident that we can prevail in defending our great Nation in this newest of competitive domains, just as I am confident that we will continue to prevail in the air and space, on the land, and at sea.

It has been an honor to spend this morning with you, and I thank you for your efforts to help defend our Nation, in whatever national defense sector you may serve. I wish you all the very best for a successful and productive symposium. Thank you.