Confronting Cyber Uncertainty

We live in a truly global society shaped by the advent of the telephone, the data network, the jet airliner, and, now, the Internet. As the impact of globalization spreads, all of us – in business, government, and our private lives – have come to depend on the Internet. Its influence cannot be overstated. The Internet is pervasive, accessible to a growing number of people, and it enables us to do things we would have thought impossible not long ago. I wish I could say all this was good, but like so many technologies, there are downsides. Information can be stolen, damaged, and denied on the Internet. Personal identities, intellectual capital, even valuable military data, can be compromised and manipulated. Criminals, terrorists, and nations can – and do – exploit the vulnerabilities in computers and networks for their own purposes. In spite of all the growth and advancement we have seen, the global strategic environment is increasingly defined by uncertainty.

Confronting uncertainty demands increased agility, and agility can be enhanced by unlocking the power of information – making it visible, understandable, shared, and, above all, trusted. The security of our nation rests on being able to share information in an environment free from unnecessary limitations and constraints. In the past, we moved and shared information inside our agencies and departments or between them, but only if our specific needs were known. The interface for moving information had to be engineered ahead of time and the determination that someone might want or need the information had to be made well in advance. It was very difficult to share information on an ad-hoc basis.

Today, we produce data that is timely and useful to others, but predetermined formats must be used. Information can be made accessible and secure, but only if we stay within departmental boundaries and systems. Today, information collection and analysis is ready for posting, but only if you know where to find it. What if we could remove those obstacles and migrate to a completely net-centric information environment? What if we could shift from a culture of hoarding data to a culture that readily shares it? Imagine how much more effective we would be.

To transition to a sharing culture, national and Department of Defense (DoD) information sharing strategies and plans have been put in place to ensure interagency sharing of information. Within the DoD, our key goals have been to build the Net, populate the Net, operate the Net, and protect the Net across the enterprise.

I cannot overemphasize how vital information sharing is to our national leadership under all conditions. Network cyber-security and infrastructure are critical to our national economy and security. From the President to the warfighter, leading-edge information technology has made it possible for users to say, “I can get the information I need to perform my mission,” and *that* is net-centric transformation.

We have to remember that we are stewards of government information – we don’t own it – and we have a responsibility to share it.

The Honorable John G. Grimes
Sponsor