

**Lieutenant General Thomas Goslin, CD USSTRATCOM
GIG-2010 -- Canadian Science and Tech Symposium
21 April 2004**

**Information Block: Up to 30-minute speech on theme:
“The GIG out to Year 2010” -- followed by approximately
15 minutes of Q&A at the Science and Technology
Symposium of Defence Research and Development
Canada.**

- **Good morning. Thank you for that generous introduction and for your invitation to be with you in Ottawa and play a small part in your work here.**
- **In my remarks today, I'll try to heed the advice of George Burns. He said the secret of a good speech is to have a good beginning and a good ending -- and have the two as close together as possible.**
- **That's good advice for us to heed for any communication we send in this information age. While computers and networks have become absolutely essential to both our military capabilities and our commercial prosperity, the quality of the message still relies on the capability of the messenger.**

- **It can be argued that the most significant developments in the technical revolution have come within the lifetime of today's college graduates, even though the first computers were built before I entered grade school.**
- **Let me take you back to the days before my youth. A "Popular Mechanics" article from March 1949 made this prediction... "A calculator on the ENIAC today is equipped with 18,000 vacuum tubes and weighs 30 tons. Computers in the future may have only 1,000 vacuum tubes and perhaps weigh only one ton."**
- **Transistors and microchips were definitely "out-of-the-box" thinking back then. But as humorous as a one-ton computer may seem today, we continue to be burdened by "one-ton" solutions to some of the issues we face right now in both sharing and protecting information.**
- **That's true even as we pursue the full potential of today's Global Information Grid. The GIG is a globally interconnected, end-to-end set of information capabilities.**

- **It collects, stores, processes and disseminates information to warfighters, policy makers, and support personnel all over the world.**
- **The GIG includes both owned and leased communications and computing systems.**
- **It takes in services, software, data, and security services. The Department of Defense relies on the GIG for all its missions. The GIG also supports National Security and related Intelligence Community missions and functions in war and in peace. That means, operational, tactical, and business as well as a word that's near and dear to my heart -- Strategic.**
- **The GIG is designed to provide capabilities from all operating locations, whether they be bases, posts, or camps – or even mobile platforms and deployed sites. And the GIG provides interface to our allies, including our good friends here in Canada.**

- **When I was invited to appear here and share some of my thoughts on the status of the Global Information Grid in the year 2010, the first thing that struck me was the short time frame involved. The year 2010 is just six years from now.**
- **Predicting the future is always difficult, as the writer of that old Popular Mechanics article certainly found out.**
- **However, if there is one area of the GIG that truly requires our strict attention, it is information assurance.**
- **Not too many years after the Popular Mechanics article, the Defense Department created the acronym “COMSEC” for Communications Security. It dealt exclusively with protecting classified information against disclosure to unauthorized parties when the information was transmitted.**
- **Black boxes were built to provide high-grade encryption to protect information.**

- **By the early 1980s, the personal computer brought a new discipline that gave birth to a new acronym – COMPUSEC, for “Computer Security.” It not only focused on protecting information, it also met new challenges and threats, such as malicious code and the theft of data on magnetic tape and disks.**
- **As computing technology and communications became virtually inseparable, the division between COMSEC and COMPUSEC disappeared and the NSA blended the functions into INFOSEC, or Information Systems Security.**
- **While we continue protecting the United States against unauthorized disclosure of information and maintaining confidentiality, our focus has changed with the development of local and wide area networks, and Internet Protocol Networks – both classified and unclassified.**
- **The concerns we face go beyond confidentiality as we address the challenges of protecting against unauthorized modification of information, or what we refer to today as data integrity.**

- **The basic challenge continues to be sharing information at the same time we protect it.**
- **Our systems are constantly being probed and attacked and it's increasingly important that we build operational responsiveness to detect and react to this growing threat. These Defensive Information Operations will be even more critical in the months and years to come.**
- **As we approach the year 2010, we are once again at a crossroads. America's military organizations have experienced rapid change during the past two years that were necessary to meet the challenges of the very different threats we face in today's world.**
- **As some have noted, a thousand snakes have replaced a single dragon. Our information systems must change dramatically to respond to this revolution, or we'll be mired in the equivalent of the "one-ton" computer conceived in that old "Popular Mechanics" article.**

- **To underscore this determination to change, one need only refer to an earlier point in history – the years just before World War II.**
- **At that time, European allies struggled to adapt to the new realities of warfare brought about by rapidly evolving military technology.**
- **Witnessing the lack of willingness to change, Winston Churchill said, “The era of procrastination, of half-measures, of soothing and baffling expedience, of delays, is coming to a close. In its place we are entering a period of consequences.”**
- **In our time, for our people, a period of consequences arrived in the United States on September 11, 2001. A similar date of reckoning occurred last month when terrorist bombs ripped through the Madrid train system.**
- **The realities of warfare have changed again, and so must our strategy and our tactics. In today’s world, the big no longer overtake the small. It’s the fast that overtake the slow.**

- **In this new world we must not allow adversaries to set the pace.**
- **Instead of a threat-based strategy, the United States has moved to a capabilities-based strategy. We will play to our strengths and those of our allies, not those of any adversary.**
- **We cannot always predict who may choose to confront us, but we can and must prepare to deal with whatever methods they choose to employ.**
- **Today's United States Strategic Command is on the cutting edge of change. On 1 October 2002, the President and Secretary of Defense ordered the merger of the former USSTRATCOM and USSPACECOM. This merger capitalized on the synergy generated by combining the command and control of our strategic forces and our space-based operations.**
- **Just 16-months ago, the President and Secretary of Defense challenged the new USSTRATCOM by adding four previously unassigned missions.**

- **Those missions are global strike planning and execution; integration of Department of Defense information operations; global ballistic missile defense; and global command, control, communications, computers, intelligence, surveillance and reconnaissance – what we refer to by the awkward acronym C4ISR.**
- **The intent is creating a global command to better employ our global capabilities to meet what is, increasingly, a global national security challenge.**
- **Since these added missions include responsibilities for both Computer Network Defense and Attack, Information assurance is absolutely critical to the success of our Global Information Grid.**
- **I am not an expert on all the technology embodied in our information assets. I rely on a talented team of experts from the military, academia and the private sector for their insight and advice.**

- I do understand the vast potential of computers and communications to enhance the security of America and her allies.
- The free world stands at a pivotal point in history. The fabric, theory and practice of the world security environment continue to change dramatically.
- The United States Strategic Command is bringing a global perspective and focus to every American military operation. While most unified commands have a geographic area of responsibility, our AOR extends around the world, up into the vast reaches of outer space, and certainly to the still evolving inner space of the Global Information Grid.
- Our goal is to integrate operations and serve all commands by providing a global, mission-based focus without regard to ownership issues. The GIG is absolutely essential to this purpose. While technical advances open new military options, they also bring a host of challenges, both domestic and diplomatic.

- **We're working with our partners at US Joint Forces Command, the Defense Information Systems Agency, and the Assistant Secretary of Defense for Command Control Communications and Integration to craft a new national-level C4 system.**
- **This system must provide improved information flow, rapid decision-making, and dramatic improvements to our current bandwidth limitations.**
- **The template for this effort is our existing nuclear command and control system - hardened, redundant and capable of operating in highly stressed environments.**
- **New systems will be more flexible and have additional redundancy built in, but not necessarily have the same hardened features.**
- **One of the current technical initiatives is GIG – Broadband Expansion, incorporating OC192 fiber-optic lines to achieve nearly ten-Gigabits-per-second throughput.**

- **The Transformational Communications office at OSD is working to develop 100 Gigabits per-second broadband-throughput in an effort to dramatically minimize communications bandwidth as a constraint by the year 2030. Laser satellite communications are envisioned to provide this capability.**
- **In addition to this widening of the communication pipes, the Department of Defense is planning to take us from a broadband push of information to an improved “smart-pull” environment. This concept is at the heart of Net-Centric operations.**
- **Bandwidth, processing and storage costs have dropped low enough to permit the development of this concept. The Defense Information Systems Agency’s Net-Centric Enterprise Services will enable the end user to execute an intelligent pull of mission-tailored information from anywhere within the network environment with minimal latency, ensuring the timeliness and relevance of the data.**

- **We must continue the drive towards this “Net-Centric,” robust, collaborative planning environment that allows commanders to share planning data and generate integrated lists of appropriate courses of action in greatly compressed timeframes, making options and recommendations readily available to the Secretary of Defense and the President of the United States, and our coalition partners.**
- **We know we’ll face major challenges in creating this system.**
- **One challenge is simply storage capacity. Information is fluid and it seems to fill up every container we develop.**
- **How many times and in how many places must we store something to make it available when we need it?**
- **We must enhance our capability to translate data to information, information to knowledge, and knowledge to wisdom in the wink of an eye.**

- It must be prioritized, de-conflicted and available everywhere, all the time.
- That's not easy.
- Just consider the monumental task of keeping up on your e-mail. It's not unusual to return from a business trip to find 300 e-mails in an Inbox. The first ones we open tend to be from the boss.
- However, there is no way to really know which e-mail is really most important.
- We all know stories of good ideas that got buried. That's why we must do a better job at pooling data and fusing it into user-friendly information.
- That requires guarding against a garbage-in, garbage-out system to make sure we screen and quantify data appropriately.
- To help us sift through this rapidly-growing information environment we need automated tools that can accomplish these tasks.

- **Our existing tools must be upgraded or replaced. Running a 3000 rpm engine at 6000 rpm doesn't work -- at least not for long.**
- **Data interoperability and protection are both critical to new systems. Conversion of all systems to comply with a specified standard will allow for flexible data interoperability.**
- **The Internet Protocol version-six standard is being pursued as we look at the transition from an application-centric environment to a data-centric environment.**
- **With common data exchange standards, the problems of hardware and software incompatibility can be eliminated.**
- **That brings me back to the issue of data security.**
- **We know information assurance is crucial, yet I would submit that 100-percent network protection is not achievable. Firewalls may not be the answer – no matter how thick they become.**

- **We need a system of protected compartments acting like water-tight doors in modern ships. Just as sealed compartments keep the vessel afloat, we'll need an equivalent computer system to protect information.**
- **Bad actors may crack one information compartment, but they'll be stopped and counter-measures engaged before they get to the next compartment.**
- **We need to build a multi-level security environment that balances interoperable connectivity with appropriate security concerns.**
- **Today we have systems that have multi-level security, but they tend to be reserved for the intelligence community and special technical operations.**
- **As we strive to develop greater operational capability in information operations, such multi-level security systems are crucial throughout the department to improve shared awareness of multi-level information.**

- **Another challenge will be identification of an attack on our system. We will need monitoring systems that sense the smallest abnormalities.**
- **An attack may be so subtle we might not initially recognize the threat. So we must expect the unexpected to be able to respond and restore our capabilities.**
- **We've made great strides in joint and combined interoperability, but there's much yet to do.**
- **Among the efforts underway today is the establishment of a multi-national Computer Network Defense Coordination Working Group that includes the United States, United Kingdom, Australia, New Zealand, as well of representatives from our friends here in Canada.**
- **The result has been significant, robust operational cooperation between our Joint Task Force-Computer Network Operations and the Canadian Forces Network Operations Center to increase the defense in depth of all parties' defense computer networks.**

- **As we move forward, Integration remains at the heart of a commander's ability to attain information superiority. New systems and improved technologies still need to be developed and woven into a network with stand-alone and network functionality.**
- **To develop these tools we must make it a priority to ensure we're developing the next generation of talented experts.**
- **Government professionals in and out of uniform must increase our collective technical capability through our partnerships with academia and industry to give us a steady stream of top talent.**
- **The price of admission must be excellence. We cannot accept mediocrity, because the global responsibilities of free nations will not allow it.**
- **As I envision the year 2010, I already know what success will look like. We'll see it when we exceed the expectations of the men and women who rely on our global information systems.**

- If there is only one fact you take away from my remarks, it is this -- The achievements we must strive for are *not optional*. As former Secretary of State Henry Kissinger said, “The absence of alternatives clears the mind marvelously.”
- The efforts we must make on behalf of achieving true information assurance within the GIG will not be easy. Almost nothing worth doing ever is.
- However, I have every confidence we will accomplish our goals.
- The rewards for success are too high, and the price for failure is far too great.
- Thank you for inviting me to be with you today, and thank for your continued efforts to enhance the security of Canada, the United States of America and of freedom-loving people everywhere.