

# National Cyber Defense Requires Close Cooperation

March 2009



Once of the most distinguishing characteristics of cyber warfare is that it is not fought on land, at sea or in the air. Cyber space is not an operational theatre that any military branch or relevant agency can lay claim to dominating. The necessities and challenges of defending the nation in the Information Age require a team approach. They also demand the ongoing sharing of ideas, best business practices and lessons learned.

Knowledge is power. Obviously, keeping our military knowledge from those who seek to harm us is sound defensive strategy and reinforces the need for strong operations security and information assurance programs. However, zealously protecting knowledge can be a two-edged sword if defensive actions are turned inward. The internal hoarding of knowledge and information for the sake of "territory" runs the risk of weakening the united defense that is necessary for success. The same can be said for competing strategies that counteract each other or cause confusion that enables the enemy to slip past our digital picket lines.

Any effective cyber security/information assurance defensive strategy must cross organizational boundaries and incorporate the best elements of the collective military/civilian expertise, experience and resources. The lone wolf mentality, so popular in the movies, doesn't cut it in cyber space.

With this in mind, DoD has tapped commands like U.S. Strategic Command (STRATCOM) and Joint Forces Command (JFCOM) to sponsor cooperative efforts among the Services and Agencies. One very impressive team stood up in 2003 to see the big picture and address strategic IA vulnerabilities is called the Information Assurance (IA) / Computer Network Defense (CND) Enterprise-wide Solutions Steering Group (ESSG). This group's mission is to provide IA/CND policy and implementation oversight, leadership, and advocacy across DoD. The ESSG consists of all military branches and joint commands and staff, plus other relevant agencies and organizations. This multi-disciplinary team provides the organization, consistency and cooperation to identify and promote effective cyber capabilities now and in the future. The ESSG, harnessing the collective will of its members, was the driving force behind DoD's mandate to deploy the Host Based Security System (HBSS). HBSS, the ESSG's most notable current initiative, integrates an impressive array of protection, detection, and monitoring capabilities that benefits the entire military community.

Yet no matter what information, recommendations, advice and expertise is available from this team of experts, it can be rendered ineffective by the aforementioned lone wolf mentality. Remember, the key to success is always cooperation. In the world of the Global Information Grid it is absolutely necessary because weaknesses can be exposed and digital walls breached in the wink of an eye.