# DEFENDING NETWORKS THAT HELP DEFEND ON THE BATTLEFIELD

Todd Hicks

Preparing for the front lines is a vital, proactive step that necessitates deft thinking across all lines of battle. To that end, anticipating and guarding ourselves against future cyber-attacks requires a near-identical process of preparation.

As our reliance on computer systems grows, and the Internet of Things (IoT) continues to evolve in tandem, the more imperative it becomes that we are protecting the Network which enables our reliance on having access to digital information. Cybersecurity is one of the U.S. Army and Department of Defense's (DOD) top priorities. With the DOD's recently released strategy - the first in fifteen years—it outlines how to combat cyber-attacks on these platforms, featuring five key action elements including build a more lethal force, compete and deter in cyberspace, expand alliances and partnerships, reform DoD and cultivate talent.

While the DOD continues to communicate the importance of preparing for malicious attacks, the industry must be committed to making these technologies resilient, in order to keep the machines prepared and safeguarded ensuring Soldier safety, which in turn, ensures civilian safety.

As the U.S. Army presses forward with modernization efforts, a combination of new and legacy platforms will remain in the fleet—all of them with mission-critical Network requirements. The vehicle-mounted tactical computer has the ability to significantly disrupt the current posture of tactical cybersecurity. The Army's Mounted Computing Environment (MCE), is an interoperable common suite of mission-critical hardware capable of meeting tactical computing needs including situational awareness, sensor integration, networking, logistics applications, vehicle system management and a variety of other capabilities.

This system of computers and displays represents the most advanced generation of COTS-based mission computing solutions ever engineered for tactical platform use. Further enforcing that Networks wired to work in any extreme, physical environment are just as reliable to remain resilient in cyber-attack attempts. As future Army technologies mature, sensor analytics, artificial intelligence, and vehicle autonomy continue to move to the forefront of where the evolution of our machinery and mission-critical systems are headed.

The development of cybersecurity provides the foundation for this protection, by fortifying and securing down to the hardware level with no Soldier effort required. It is designed specifically for the tactical environment and runs in the background to ensure ease of use and minimal burden for the Soldier. The commercially available cybersecurity solutions and technologies are intended for use on enterprise Networks that have reliable internet connectivity, whereas tactical computing fleets have limited Network connectivity, along with limited access to patches and updates. Cybersecurity closes this gap by providing multiple layers of cybersecurity protection and resiliency for the harsh tactical environment.

Resiliency being a requirement at the tactical level means that computers are now being built to detect integrity changes, auto-deployed countermeasures, and can auto-recover as well as resist cyber-attacks. As electronic warfare continues to emerge as a leading peril, with an increasing role in shaping the outcomes of conflict across the globe, it is a universal imperative that in the world of defense, we have full awareness and understanding of EW. The future of cybersecurity is synonymous with nimbleness; preparing the warfighter for worst-case scenarios at every turn.

7200 Redstone Gateway SW
Huntsville, AL 35808-2002
marketing@drs.com
+1 256 895 2000

100 North Babcock Street
Melbourne, FL 32935
marketing@drs.com
+1 321 622 1500