

# US Navy Experiments with Secure Cloud Computing

This week in San Diego, CA the US Navy held the initial planning conference for Trident Warrior '10. The Trident Warrior series is the premier annual FORCEnet Sea Trial Event sponsored by Naval Network Warfare Command (NETWARCOM). FORCEnet's experimental results are incorporated into a definitive technical report used to develop Military Utility Assessment (MUA) recommendations. This report is provided to the Sea Trial Executive Steering Group (STESG) for consideration and acquisition recommendations.

The primary goal of FORCEnet experimentation is to influence accelerated fielding of improved Command and Control (C2) capabilities to the fleet through Program of Record (POR) acceleration or transition of new technologies into PORs. Additional goals include evaluating Tactics, Techniques, and Procedures (TTP) that best exploit, promote, expand, and incorporate new FORCEnet capabilities in support of optimizing execution of Naval operations; increasing warfighter effectiveness through discovery and development of enhanced capabilities; and encouraging Government, industry, and academia use of experimentation to advance new concepts and capabilities.



This year, for the first time, the event has been expanded to include a lab-based venue designed to experiment with lower Technology Readiness Level (TRL) candidates. The goal of this added activity is to demonstrate technologies that have the potential to fill mid- and far-term warfighting gaps. One of these lab-based experiments is secure cloud computing.

Sponsored by **Dataline, LLC**, the Secure Cloud Computing experiment has been designed to explore the use of a commercial Infrastructure as a Service (IaaS) platform as a viable means of supporting a specified subset of US Navy mission requirements for global connectivity, server failover and application access. Goals for the experiment include:

- Demonstrating the establishment and use of trusted communication paths on a global public computing infrastructure; and
- Demonstrating dynamic, mission driven, provisioning of information via trusted communication paths on a global public computing infrastructure

Working with Amazon Web Services and Security First Corporation, the Dataline-led team will explore the ability of cloud computing technologies to support humanitarian assistance and disaster relief military missions. As currently planned, the test scenario will simulate the secure use of a cloud-based collaboration environment. Both synchronous and asynchronous collaboration technologies will be leveraged. Information and data access among multiple operational groups will be dynamically managed based on simulated ad-hoc mission requirements. Expected mission advantages of this new approach include:

- **Increased IT infrastructure resiliency** through the use of dynamic and automatic provisioning of compute and storage resources;
- The ability to provide **virtually unlimited IT infrastructure scalability** through the elastic nature of an infrastructure-as-a-service platform; and
- **Increased mission flexibility** through a globally distributed and accessible IT infrastructure that is also open to use by Non-Government Organizations (NGOs), civilian first responders and non-US military forces.

The use of a government sponsored "Red Team" is also being requested as a means of validating the security of the proposed infrastructure.

For further information on the Trident Warrior lab based experiments, please contact LCDR Caroline Lahman (caroline.lahman@navy.mil)

For further information on the Dataline Secure Cloud Computing experiment, please contact Kevin Jackson (kevin.jackson@dataline.com)

[ Thank you. If you enjoyed this article, get free updates by email or RSS - KLJ ]

## TRIDENT WARRIOR '09

Follow me at [http://Twitter.com/Kevin\\_Jackson](http://Twitter.com/Kevin_Jackson)