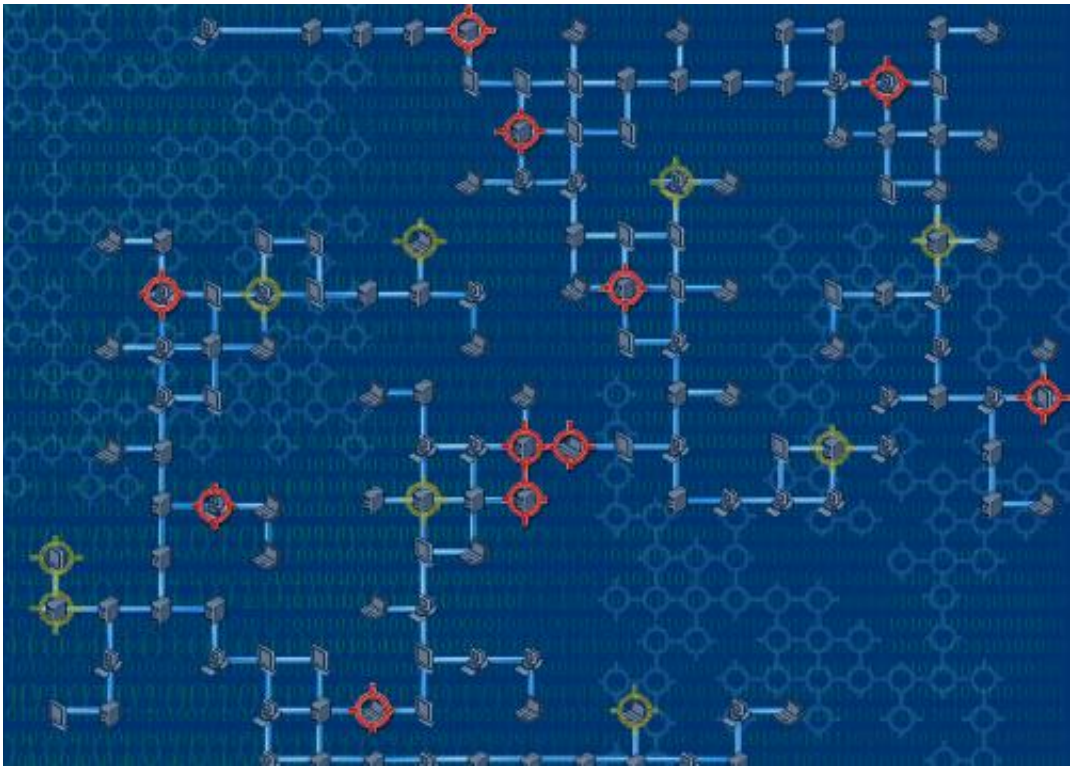
New program looks at how information is connected to stay ahead of the cyber threat

January 23 2013



The Department of Defense (DoD) maintains one of the largest computer networks in the world. The network follows DoD personnel across the globe collecting, transferring and processing information in forms as diverse as data warehouses, in-the-field mobile devices and mission computers on board F-18's. This network is also constantly

changing in size and shape as new missions are undertaken and new technology is deployed. In military terms, that means the cyber terrain of the DoD network is constantly shifting.

Traditional approaches to protecting networks involve static cyber firewalls around the network perimeter and patching any discovered holes. DARPA researchers seek a new approach, one that relies on knowing the cyber terrain within the network and understanding how information across the enterprise is connected to find actions associated with an attack buried under or within all the normal data.

DARPA's new Cyber Targeted-Attack Analyzer program will attempt to automatically correlate all of a network's disparate data sources—even those that are as large and complex as those within the DoD—to understand how information is connected as the network grows, shifts and changes. Once all of the data sources are correlated, the program will attempt to integrate them on a network to allow the defenders to understand the connections—like injecting a contrasting smoke into the air to see how it flows. The third phase of the program also seeks to build tools that use this information for cyber defense of the network.

"The Cyber Targeted-Attack Analyzer program relies on a new approach to security, seeking to quickly understand the interconnections of the systems within a network without a human having to direct it," said Richard Guidorizzi, DARPA program manager. "Cyber defenders should then be capable of more quickly discovering attacks hidden in normal activities."

Performers for the program will address three challenges: Automatically indexing data sources on a network without human intervention; Integration of all data structures through a common language for security-related data, and; Development of tools to allow reasoning over the federated database

It is anticipated that the BAA for this effort will be posted to www.fbo.gov within the next month.

Provided by DARPA