Network-Centric Systems Need Standards and Metrics

Warfighters must keep their eye on the metrics to manage and secure military networks.

By Paul A. Strassmann

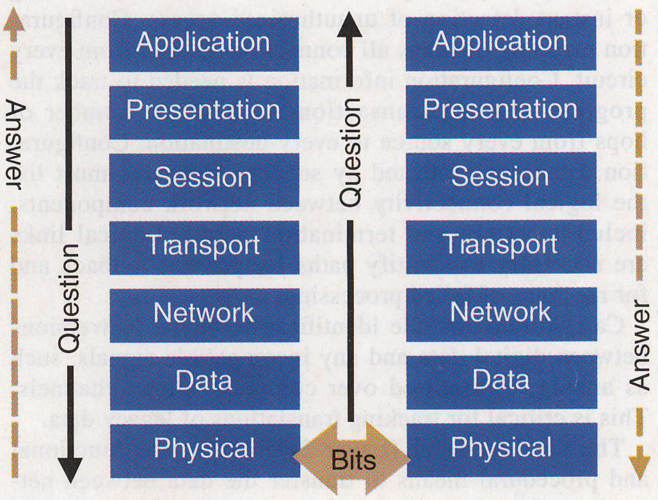
Network systems are similar to icebergs. Less than 10 percent of their volume is visible to the user of an application. Almost all of the hidden code, measured in hundreds of thousands of lines of logic, is invisible in the operating system, in the database management software, in security safeguards and in communication routines. The problem with such software is that for each application—and the U.S. Defense Department has more than 7,000 major software projects—contractors will develop the hidden coding to suit separate requirements.

Even the operating systems—some from the same vendor—will have sufficient variability so as not to be reusable. Contractors then will add special-purpose software routines from different vendors as custom "glue" to make the software code function. Contractors also will patch in custom code to make an application survive stringent testing requirements.

Such results are hugely expensive and hard to maintain. Applications developed separately will not share most of the common 90 percent of the code that remains submerged within the information infrastructure. Network systems will not be interoperable, except through additions of software connections that increase the costs, reduce performance and increase malfunction risks.

To deal with the software iceberg, the approach to software design must be revised to create a shared infrastructure. This communal infrastructure would enable the Defense Department to concentrate on the less than 10 percent of code that drives applications, rather than on the more than 90 percent that constitutes the software infrastructure. To achieve such a change calls for re-examining the organization of software.

Every transaction involved in cyber operations ultimately must communicate in the form of physical bits, such as 0s or 1s. Every question launched must originate and then be returned from an application.



Flow of information according to OSI.

For questions and answers to be converted into streams of physical bits calls for a seven-layered process, each controlled by standards, which define how the respective layers connect. These standards are described by an international standard, the Open Systems Interconnection (OSI) model.

Bandwidth for the passing of physical bits between layers is defined as "return latency" and is calculated in microseconds, depending on priority and on different methods to complete a transaction. How the delays in information flows are achieved is then a matter of tradeoffs across each of the OSI layers. Custom-made or improvised OSI connections will increase costs and the latency of a system.

For the Defense Department to migrate to high-performance cyber operations requires a design that allows for the sharing of at least three of the OSI layers for physical, data, network and transport. These layers may account for as much as three-quarters of infrastructure code that is written for each stand-alone application.

The OSI layers will be used to define capacity for cyber operations. The layers must function as a whole for the successful delivery of results. Except in cases that call for real-time—combat—responses, Defense Department components should field only applications using OSI layers that are shared as an enterprise infrastructure service.

The physical OSI layer (Layer 1) defines the electrical and physical specifications for components from which networks are constructed. This includes cable specifications, hubs, repeaters, network adapters, bus adapters and any devices that convey electronic signals.

Measurements call for capacity mapping that describes every element of the physical layer, defined as to its location description and capacity. Continuous monitoring of capacity, at the circuit level, keeps track of the cyber operations, such as traffic rerouting or instant detection of unauthorized access. Configuration mapping displays all connections to and from every circuit. Configuration information is needed to track the progress of every transaction, such as the number of hops from every source to every destination. Configuration databases protected by security measures must list the logical connectivity between network components, including origin and termination points. Logical links are necessary to identify paths for process fallback and for recovery of failed processing.

Calculations include identification of the conversions between digital data and any incompatible signals, such as analog, transmitted over communications channels. This is critical for tracking translations of legacy data.

The datalink layer (Layer 2) provides the functional and procedural means to transfer the data between networks and to detect and correct errors that may occur in the physical layer.

Measurements require tracking of all local area network connections used for network capacity determination, for network simplification or for identification of alternative paths for passing packets of data under condition of failure. Included is the tracking of all wide area network (WAN) connections used for network management, including re-routing of traffic under failure conditions. A WAN registry identifies circuits used for diverting communications under peak-load conditions.

The network layer (Layer 3) provides the functional and procedural means of transferring data from a source to a destination while maintaining a specified quality of service.

Calculating this layer requires tracking all Internet protocol (IP) addresses on the entire network, including devices such as desktops, laptops, smart phones and radio-frequency identification devices. The registry of IP addresses is managed in real time and is the main indicator of the size of the network managed by cyber operations. Router IP addresses specify the number and location of routers such as their function, capabilities and processing capabilities. Routers perform network functions such as re-assembly of packets and the reporting of delivery errors. Routers send data throughout the extended network and make connections possible through the transfer control protocol (TCP)/IP protocol.

The transport layer (Layer 4) provides transparent transfer of data between all points participating in the cyber operations.

Calculations require the evaluation of transport uptime, which is the percentage of hours of scheduled connectivity, minus hours of unavailability, divided by hours of scheduled connectivity, calculated over a one-year period. The unavailability of every link is tracked and recorded in a number of redundant network operations centers (NOCs). Individual downtime statistics cannot be averaged but must be displayed in terms of the number of IP addresses than cannot be served, such as any unavailability in excess of one minute.

Measurements of the transport layer define computing nodes as either redundant virtualized resources or as clustered resources.

The session layer (Layer 5) controls the connections between computers. It establishes, manages and terminates the connections between the local and remote application.

Calculations keep track of architectures, such as the service-oriented architecture (SOA), which is defined by the number of reusable components that are available for applications. The total number of reusable and certified software components divided by the total number of components in use quantifies the pervasiveness of SOA services. Measures include network service statistics such as the number of legacy applications as related to the total number of applications. This evaluates the extent to which legacy applications have not been integrated into cyber operations.

A second appraisal is the number of virtual servers with cached services. Cyber operations depend on virtual servers that deliver applications to the edge of networks for low-latency processing.

A third appraisal is the number of data dictionary services. This describes the number of unique metadata and data dictionary services available from communities of interest (COIs).

The presentation layer (Layer 6) is responsible for formatting information for display. Syntactical differences in inputs to the presentation layer will be reconciled by means of dictionaries that trace differences in data representation to the point of original data entry. Assessments include network service statistics such as the number of applications that use encrypted coding. This assesses the extent to which applications are delivered in the approved encrypted formats. Another calculation is the number of applications that rely on data warehouses for support. This gauges the use of data dictionaries to ensure consistent syntax.

Finally, a number of portals exist for unencrypted access to the public Internet. This provides a method for bypassing cyber operations for access to public network services. The portal blocks transfer of transactions or files to and from Internet to cyber operations.

The application layer is the OSI layer that is closest to the end user. The user interacts directly with applications. This layer interacts with software that implements end-to-end communication. Governance rules may allow the use of locally managed databases provided they are not connected to cyber operations.

Measurements include access milliseconds, counting from the send command to receipt of output in excess of defined delays. Latency is gauged in comparison to all active IP addresses and is not averaged but counted as the number of incidents.

Cyber operations networks must have end-to-end visibility, measurement and control of every keyboard associated with every IP address. This visibility should be present not only at the highly automated network control centers, but also as status displays offered for each local command.

Cyber operations are not comparable to commercial systems such as those for Google, Wal-Mart or Bank of America. None of these systems are subjected to information warfare attacks. Defense Department cyber operations must be viewed as having a high-security design for the OSI layers in its infrastructure. The department's designs must be based on parameters that far exceed whatever may be acceptable in commercial systems.

It may take 10 to 20 years for the Defense Department to change its current disjointed software to a shared infrastructure where the code residing in OSI layers will be calculated and shared. Budget realities will dictate that Defense Department components will have to execute such transitions largely within existing budgets while the scale of demand for services will rise. This will require the automation of all network metrics in order to cut the operating and maintenance costs that currently dominate the department's networks.

As the costs of computing hardware shrink to less than 8 percent of total information technology spending, the funding of network-centric systems will have to come from cost reductions in software. The cutbacks will become possible by departmental sharing across applications and by decreases in operating personnel.

The existing development, operating and maintenance costs for the Defense Department infrastructure are prohibitive. They absorb roughly a half of all information technology budgets. The acquisition of cyber operations must be driven by eliminating redundant systems and by sharing common OSI software layers. These performance measures can be viewed as the direction for the department's investment architecture in the years to come.

• • •— •—

Paul A. Strassmann is a distinguished professor of information science at George Mason University's School of Information Technology and Engineering. He is the former director of defense information at the Office of the Secretary of Defense and acting chief information officer of NASA.

WEB RESOURCES

International Telecommunication Union (ITU):
www.itu.int/ITU-T/index.html

Assistant Secretary of Defense
(Networks and Information Integration):
www.defenselink.mil/cio-nii/