Cyberspace Situational Awareness Demands Mimic Traditional Command Requirements

Experience gained from battlefields helps military prepare information operations defenses.

By Tim Bass

Future military cyberspace security may require next-generation network management and intrusion detection systems that combine both short-term sensor information and long-term knowledge databases to provide decision-support systems and cyberspace command and control. Sophisticated computer hardware and software would identify a myriad of objects against a noise-saturated environment. Cyberspace command and control systems would track the objects, calculate the velocity, estimate the projected threats, and furnish other critical decision-support functions.

Numerous constructs used to monitor and control objects in traditional airspace apply to monitoring information-based objects in data networks. These concepts are evolutionarily similar to the situational awareness required in current-generation air traffic control. Lt. Col. David Gruber, USAF, communications squadron commander, Hickam Air Force Base, Hawaii, is convinced that an analogous fusion paradigm is required between network management, Internet traffic control and future intrusion detection systems if U.S. military organizations are to maintain information superiority in cyberspace.

This new, globally reachable battlespace has some unique warfare characteristics, as recently discussed by Brig. Gen. Dale W. Meyerrose, USAF, director of communications and information systems, Headquarters Air Combat Command, Langley Air Force Base, Virginia. In traditional warfare, the air and space media for operations and deployment are natural resources that do not have to be created or maintained by the warfighter. Cyberspace and critical electronic infrastructures, on the other hand, must be artificially created and sustained before information operations occur.

Network communications have evolved from a subordinate operational support function to a major warfighting element with unique doctrine and operational constructs. However, because information operations in cyberspace take place in an artificially created medium, the doctrine of cyberwarfare is much different than traditional warfare, which occurs in a natural media for transportation and deployment. In global information operations, the communications organization creates and maintains the air in which information flies. Officials at Langley have implemented initiatives to examine how the concept of creating and sustaining information infrastructures will affect future U.S. Air Force doctrine.

In a typical command and control (C2) system, sensors observe electromagnetic radiation, acoustic noise, thermal energy, nuclear particles, infrared radiation and other signals. Cyberspace C2 (CC2) systems feature different sensors and constructs because the environment has changed. Instead of a missile launch and supersonic transport through the atmosphere, cyberspace sensors observe information flowing in networks. Yet, just as traditional command and control operational personnel are interested in the origin, velocity, threat and targets of a warhead, CC2 personnel are concerned about the identity, rate of attacks, threats and targets of both friendly and hostile information objects in cyberspace. Air Force representatives explain.

The input into CC2 fusion systems will consist of sensor information, commands and deductive data from established short- and long-term knowledge centers. For example, the CC2 system input will consistent of information from numerous distributed packet sniffers, system log files, simple network management protocol traps and queries, signature-based intrusion detection systems, user profile databases, system messages, threat databases and operator commands. Traditional signature-based network intrusion detection will perform an architectural role similar to signature-based antiviral software.

Military experts consider visualization of attack scenarios critical for future CC2 decision makers. Researchers at the University of Illinois–Urbana-Champaign have creat-
ed illustrations that represent future CC² decision-support systems. These examples describe virtual-reality-based global World Wide Web traffic analysis and a geographic mapping of network-based attacks on the Internet. In one model from the ip2ll server project, a database containing long-term knowledge of the relationship between Internet protocol addresses and geographic space is used to illustrate global Internet data flows. These visualizations, which map cyberspace to geographic space, could provide critical information to decision makers, Air Force officials offer.

The output of fusion-based CC² systems are estimates of the identity, and possibly the location, of a threat source as well as the malicious activity, taxonomy of the threats, attack rates, an assessment of the potential severity of the threat to the projected target, and CC² decision-support visualizations and simulations. A number of command and control constructs map directly to future CC² systems. The detection performance of a CC² sensor is the detection characteristic, including the false alarm rate, detection probabilities and ranges for the information-object of interest tracked against a network-centric noise background. For example, when detecting malicious activity, nonmalicious activity will be modeled as noise.

The capability to distinguish between two or more network-centric objects in space or time is the spatial and temporal resolution. The spatial coverage is the span, or field of view, of the sensor. For example, the spatial coverage of a system log-file is the computer system processes and system calls being monitored. The mode of operation of the sensors scanning single- or multiple-network object capability is important for CC² sensor classification and system integration. Command and control concepts apply to the CC² target revisit rate, the measurement accuracy and information-object measurement dimensionally.

In hard and soft cyberspace command and control, sensor reporting characteristics refer to the decision status of sensor reports. Commanders need to know if a critical operational decision can be made without sensor correlation or if the CC² sensor requires confirmation.

For effective CC², situational data is collected from numerous network objects with elementary observation primitives, including information-object identifiers, times of observations and other technical attributes. Every network device and object has the potential to be used as a CC² sensor, providing both low-level data and refined information to CC² distributed processors. Current-generation intrusion detection systems rely on in-band processing, which can only achieve limited temporal resolution. Extremely critical real-time systems will require out-of-band cyberspace command and control networks.

The Defense Advanced Research Projects Agency (DARPA) recently began examining next-generation information CC² systems. DARPA's future information assurance vision is a strategic cyberspace decision-support system that enables leaders to understand strategic network situations and react quickly to these situations.

CC² decision support envisioned by DARPA would provide battle management over systems under attack by helping users understand the activities and objectives of adversaries operating within the network environment. Increased confidence and situational awareness provide the foundation for determining the most effective courses of action to counter future hostile activities in the emerging network-centric battle and information spaces.

The emerging DARPA research initiatives will help prepare the United States to develop a more comprehensive understanding of cyberspace command and control operations as the military creates, deploys and flies missions in globally connected networks. Experts from across the nation who gathered at a joint U.S. Department of Energy, National Security Council and Office of Science and Technology workshop concluded that commercial off-the-shelf products are behind the power curve dramatically in situational and visual command and control support tools. DARPA and workshop participants stated that it is critical for the United States to clearly define the underlying scientific and technical constructs of internal cyberspace command and control operations before funding large CC² programs.

CC² systems that provide long-term threat, countermeasure and other security-related information to fusion systems are emerging as critical scientific research and development areas. Cyberspace situational awareness is required to operate and survive in complex global network infrastructures where both friendly and hostile activities coexist. According to Lt. Col. David Uhrich, USAF, chief of network plans, Headquarters Air Combat Command, Langley, current-generation intrusion detection technologies are inadequate. Future cyberspace rules-of-engagement doctrines depend on the timeliness, fidelity and accuracy of CC²-based knowledge. These emerging requirements call for highly sophisticated cyberspace decision-support systems in order for U.S. forces to maintain information superiority, he says.

Tim Bass provides network-centric subject matter expertise to the U.S. Air Force Communications and Information Center, the U.S. Department of Energy, and multinational financial institutions.