Summer 2007

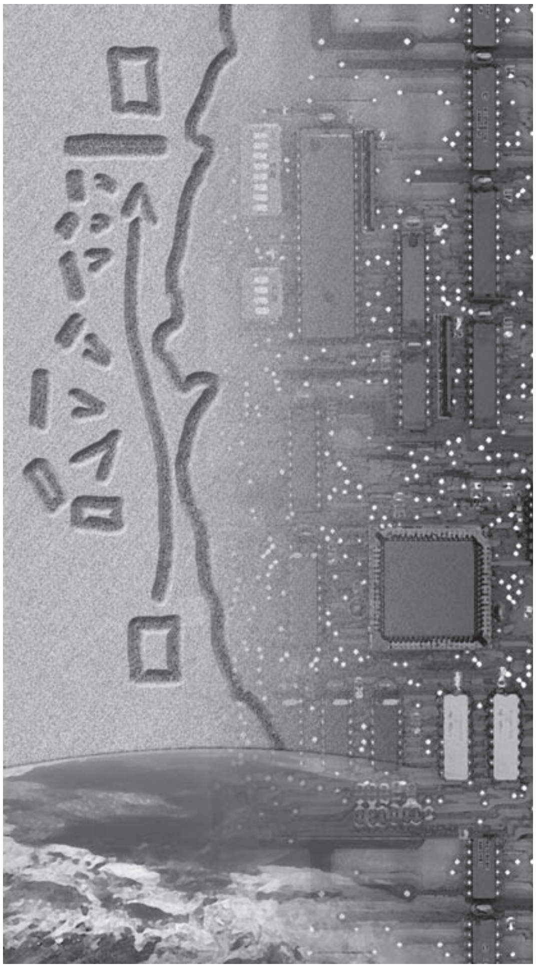
A Model for Managing Decision-Making Information in the GIG-Enabled Battlespace

Samuel D. Bass
United States Air Force

Rusty O. Baldwin
University of Dayton, rbaldwin1@udayton.edu

A Model for Managing Decision-Making Information in the GIG-Enabled Battlespace

Maj Samuel D. Bass, USAF
Maj Rusty O. Baldwin, PhD, USAF, Retired



Editorial Abstract: The Defense Department is transforming information-technology systems into a Global Information Grid (GIG) that will connect sensors to weapons systems and provide unprecedented situational awareness. The authors suggest that if not properly implemented, the GIG may overwhelm war fighters with information presented at the wrong time, at the wrong level of detail, and without proper analysis. This article proposes a model to direct the flow of information in the GIG.

THE DEPARTMENT of Defense (DOD) is in the midst of transforming its vast collection of information-technology systems into an interconnected Global Information Grid (GIG), which will ultimately connect sensors to weapons systems, enable personnel to share information at will, and provide unprecedented levels of situational awareness to commanders at all levels. However, if we do not implement the GIG with a proper level of restriction on the flow of information, war fighters risk being overwhelmed not only by too much information but also by information presented at the wrong time, at the wrong level of detail, and without proper analysis and interpretation. This article proposes a model to prevent this situation by directing the flow of information based on its classification level, integrity, and relevance to the end user.

The Global Information Grid

In response to increasing difficulties associated with sharing information between various platforms and information systems operating in the joint environment, the DOD created the concept of the GIG.[1] DOD policy defines this grid as "a globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel."[2] Established GIG policies also implement key components of the Clinger-Cohen Information Technology Management Reform Act of 1996, including information security, revised acquisition strategies, and best practices for handling data at all levels of the DOD.[3] Although many of the efforts in developing the GIG might simply entail the application of the DOD's best practices in acquisitions to the still-maturing field of information technology, the goal of achieving information superiority remains paramount—the primary objective of the overall GIG effort. Connecting personnel and equipment with advanced information-sharing tools will likely revolutionize our capabilities, but we must carefully manage the quality and volume of information presented to the war fighters of tomorrow.

The Sand Table

For centuries, military commanders have used various models to understand the battlespace. In the seventeenth century, campaign planners used intricate, craftsmen-built scale models of fortifications to analyze points of vulnerability and routes of attack.[4] In the field, leaders have long used sticks and stones in the sand to rehearse maneuvers and depict unit locations and terrain. Aircraft and antiaircraft technology increased the complexity of the "sand table" by adding important air components to the planning process. New technology used in Operation Desert Storm provided commanders and bomb-damage analysts a live view from the cockpit and, in many cases, from the weapons themselves as they flew into targets. Today, command centers of all levels are equipped with large data walls, on which interesting computer or video feeds provide a constant flow of data. Live video from remotely piloted Predator aircraft feeds into air and space operations centers, giving commanders and intelligence analysts what some people call "Predator Crack" or "Kill TV" because of the display's ability to divert viewers' full attention away from their primary duties.[5] The frequently asked question concerning what shows on the displays and who has responsibility for the content raises an even broader and more important question about the future GIG-enabled command center: how will we manage all of the data available on all of the interconnected platforms?

Although the GIG's influence on the development and acquisition of weapons systems is evident in requirements for common data standards and supported communications protocols, the military services are actively developing ways to inject network technology everywhere. Army projects such as Future Force Warrior will provide each soldier with a complex array of networked information sensors and displays, reminiscent of the gear worn by the futuristic space marines in the science-fiction movie *Aliens*.[6] One scene in that movie depicts a frighteningly realistic scenario in which the team commander watches health monitors go silent as each member falls and the confusion of battle grinds his decision-making ability to a halt. Several years later, real commanders orbiting in Black Hawk helicopters over Somalia tried to command a rescue convoy through a decaying urban environment. The communications delay between the airborne command post and the trucks introduced chaos significant enough to confuse the convoy, effectively driving it into a dead end.[7] Future systems must be able to create a timely flow of critical information in both directions, and we need to establish processes to help us manage and respond to that flow effectively.

Because of the rapidly increasing volume of available information, numerous research projects now under way seek to design virtual environments that integrate, analyze, and display every piece of information in an immersive, four-dimensional battlespace, where mission planners and commanders can manipulate time and perspective to suit their needs.[8] One can easily imagine the demands placed on commanders trying to conduct a war from inside a virtual, real-time sand table with data from thousands of sources pouring in at incredible rates. Additionally, the GIG notionally gives personnel anywhere in the battlespace the ability to have similar representations streamed to their locations by various means. An obvious hazard of this capability—beyond information overload—is the danger of commanders making tactical decisions based on data intended for a strategic perspective and war fighters on the ground adjusting their tactics based on information intended only for strategic planners.

The Problem of Inverted Perspectives

As prescribed in joint doctrine, planners design operations to follow the principles of war, which include surprise, simplicity, security, and unity of command.[9] Numerous historical examples illustrate how friendly or hostile knowledge of certain components of plans drastically altered the results of those plans. Still others demonstrate that reaction or failure to respond to evolving circumstances has a drastic impact on the operation and effectiveness of the leadership involved. Rather than explore the success and failure of operations with respect to the principles of war, we should consider the implications of operating a GIG-enhanced command center of the future.

For example, a suite of sensors programmed to detect personnel and vehicle movement could collect and report status for display on a command center's data wall, indicating maneuver by an unknown unit. If we can attribute this maneuver to a friendly special-operations mission planned and executed in secrecy, we should restrict access to this sensor data at the same classification level of the mission and not automatically display it on a data wall for viewing by personnel without an appropriate clearance. Conversely, if a similar sensor suite detected the footsteps of an individual in a restricted area, we should present the data collected by this sensor (probably not displayed on the same data wall) only to appropriate security personnel. Commanders directing their attention to an unprocessed data point like this could experience an *inverted perspective*, whereby a single piece of potentially irrelevant data diverts focus from the broader picture. Similar scenarios could illustrate how a tactical unit on the ground might see data intended only for a strategic view; any changes to the actions of that tactical unit might eliminate a key component of a strategic plan. We assert that such an inverted perspective constitutes a very real hazard of information that might exist in a GIG-enhanced battlefield.

In an ideal environment, we would deploy thousands if not millions of sensors across the battlespace to collect climate, audio, video, and electromagnetic signal data. Additionally, airborne command and control (C2) assets would compose an integrated picture of the battlespace. Current processes and tools such as air tasking orders help deconflict the airspace, but some operations conducted on the ground or at sea might not be coordinated with all components. A robust sensor net would provide a bridge between these dissimilar components of the battlespace to help prevent incidents of friendly fire, but the composite picture would likely not have relevance to some war fighters. In total, the amount of information collected will be immense, and the details of the battlespace available for display will prove tempting to war fighters and leaders at all levels. GIG-enhanced aircraft will have access to a vast store of information. However, with this comes the possibility that unprocessed sensor data might make its way into the cockpit, forcing pilots with increased sensitivity to collateral damage and escalation to change tactics, select alternate targets, or abort the engagement.

Ground units would need time to analyze the data from sensors detecting a nearby firefight before determining the location of units in the area and perhaps requesting additional airborne or spaceborne surveillance. Those units not aware of friendly forces in covert operations could alter their tactics or maneuver in response to indications of a nearby firefight—particularly if sensors indicated activity in a unit's area of responsibility. Hopefully, all parties in that area would have already received briefings on operations to an appropriate level of detail, but any GIG-enhanced capabilities for examining additional sensor data could affect the commander on the ground in a number of ways—hence the need for clear rules for using this data in order to avoid inverted perspectives.

One could present any number of examples demonstrating avoidance of inverted perspectives by limiting exposure of data in the GIG, and still more examples could illustrate that any restrictions on information flow could reduce flexibility. Considering both sides of this argument, we assert that we should place limits on the places that *automatically* receive data as well as on the people authorized to access it. We must also consider that some platforms—as William T. Hobbins, a lieutenant general at the time, indicated during an interview with *Airman Magazine*—will produce data at different rates while operators in varying roles will consume data feeds at different rates, thus adding more considerations for a potential solution.[10] Clearly, this paints an amazingly complex picture with fuzzy and continuously evolving operational requirements.

Current Management of Information Flow

We are all familiar with the classification levels defined by the National Security Agency. Only users holding a secret or higher clearance and having a need to know can read data protected by a secret classification level. Similarly, readers with a high classification level can normally read any material at or below that level, assuming they have a need to know. In a conceptual, GIG-enabled virtual command center, we could classify information specific to a sensitive operation at a sufficiently high level to prevent those who hold lower-level classifications from reading the data. Furthermore, we could reserve display of data relevant to those classified operations for individuals with the required need to know. Additionally, we must assure that data on a command center's displays remains at the lowest clearance level of personnel with access to those displays.

Using a well-disciplined approach, we could properly secure or sanitize data from all sources to prevent users from seeing information not cleared for their consumption. Thus far, however, we have addressed only the proper treatment of data with respect to confidentiality. The integrity or trustworthiness of the data is also of prime importance, particularly in urban areas, where we have a great need for very accurate and timely data and, therefore, a need to evaluate raw data rapidly and prepare it for presentation to leadership. Normal data-classification techniques do not classify information based on its integrity, so we need to explore a method to help categorize data that could cause an inverted-perspective hazard in a GIG-enhanced picture of the battlefield, whether it is unprocessed remote-sensor data or imagery not yet evaluated by intelligence personnel.

Biba's Integrity Model

While working on an Air Force computer-security research project in 1977, K. J. Biba wrote what has since become the seminal paper on information integrity.[11] In it, he examined a method for maintaining the validity of data on information-processing systems, choosing to use the concept of *integrity* as a measure of information's validity. That is, information from a known, trustworthy source would have high integrity, while information based on rumor or from unknown sources would have low integrity. Similarly, password-protected information stored in electronic form would have higher integrity than data available for reading or editing without any access controls at all. If we extrapolated this concept for application to our GIG-enhanced command center, the integrity of the reader—that is, the reader's response to data—is influenced by the information consumed. New and startling information will affect the reader's behavior to varying degrees, based on the integrity of the source of that data. For example, a commander might decide to take some risks after reading information from a reliable source but not do so in reaction to the same information from an unreliable source. Similarly, one should not interpret a report that included a data point from a low-integrity source as factual.

In the strict formulation of Biba's integrity model, three rules apply to reading, writing, or acting upon information from sources of various integrity levels. This model refers to things that can create and consume data as subjects and to products produced as objects. The rules rely on the notion of dominance, which implies some sort of permission granted to the dominant over the subordinate, whether that permission involves reading, accessing, or in some way modifying something. Using security clearances to demonstrate dominance, Biba shows that one object dominates another when its security clearance level is the same as or higher than that of the other object. For example, a secret clearance dominates secret or unclassified clearances, while top secret dominates top secret, secret, and unclassified clearance levels. When a subject dominates an object, the subject can read the object. If the subject does not dominate the object, the subject cannot read the object, just as someone with a secret clearance cannot read a top-secret document but can read secret or unclassified documents. Biba uses the concept of integrity and the rule of dominance to determine access controls in his computer-security research. The three integrity-preserving rules from Biba's integrity model are as follows:

1. A subject can read an object if and only if the object's integrity level dominates (is greater than or equal to) the subject's integrity level. That is, a subject can only read objects with equal or *higher* integrity.

2. A subject can write data into an object if and only if the subject's integrity level dominates the object's integrity level. Since the subject must have integrity at least as high as the object, the object's integrity is preserved.

3. A subject can execute (or direct the action of) another subject if and only if the first subject's integrity level dominates the second subject's integrity level. Someone of lower integrity cannot operate on someone else's behalf.[12]

In plain terms, rule one means that a subject can read an object only if the data will not have a deceptive or misleading effect on the reader. In our command center, we would not normally present data (an object) to the commander (a subject) unless the data had undergone proper vetting using prudent processes. Rule two means that some data source of a lower integrity level can't inject information that one might interpret as accurate or valid. Again using our command center example, we would not display raw data on the data wall until we have validated it, much like we would not present the actions of a unit to the commander as confirmed results until we have conducted proper battle damage assessment or a mission debriefing. Rule three would prevent unnecessary reaction to deceptive acts or preprocessed data from sensors, which could prove useful in avoiding inverted perspectives.

Together, these rules address some of the concerns we have explored so far with respect to unprocessed sensor data. Therefore, it seems reasonable that application of the Biba integrity model to a notional command center can form the basis of a system implemented to help prevent inverted perspectives. This model could assist in defining specific requirements for automatically filtering information and controlling access, but commander flexibility and the ability to share information would experience necessary limitations to some degree. Joint doctrine emphasizes information dissemination as a key component of intelligence support: "Intelligence will play a critical and continuous role in supporting warfighting. Advances in computer processing, precise global positioning, and telecommunications will provide joint force commanders . . . with the capability to determine accurate locations of friendly and enemy forces, as well as to collect, process, and disseminate relevant data to thousands of locations."[13]

A key point entails the use of the word *relevant* to describe the dissemination of data. Further discussion in doctrine defines this term as a key attribute of intelligence that describes the scope of intelligence gathering and sharing efforts; moreover, it delineates who needs specific pieces of information and, more importantly, who shouldn't be distracted by irrelevant data.[14] Therefore, a model that combines the DOD's traditional classification levels with data integrity *and* relevance holds the key to formulating policy for data-sharing mechanisms developed for future command centers.

Classification, Integrity, and Relevance

The war fighter's need for relevant and accurate information is thoroughly understood and well defined in doctrine and operational art, but defining the scope, sources, and format of the data would require continuously updating vast amounts of information. Efforts to build systems that provide data in predefined formats or follow predefined message-sharing rules normally result in products difficult to integrate or expensive to update. To avoid the problems of updating systems to keep pace with continually evolving technologies, we propose to control information flow using a data-sharing mechanism based on classification, integrity, and relevance. The following summarizes our definitions so far:

- *classification*: a rating assigned to information in order to provide appropriate protection and restrict access
- *integrity*: a measure of a subject's or object's trustworthiness
- *relevance*: a measure of applicability to a purpose or a customer
- *dominance*: the condition in effect when one entity has the same or higher rating as another

Our information-sharing mechanism must enable meaningful and adaptive information-sharing capabilities within a command center. Consider such a center staffed with personnel of varying clearances and areas of functional expertise, similar to other command centers such as wing command posts, expeditionary operations centers, or air and space operations centers. As in Biba's model, both personnel and systems can create and consume data and are referred to as subjects, while the documents or virtual products produced are referred to as objects. Our information-sharing mechanism assigns three ratings to every subject and object: classification, relevance, and integrity.

Suppose the classification levels for subjects and objects are unclassified, for official use only, secret, or top secret. For simplicity's sake, our model will not address clearance caveats or clearances for personnel from other countries, but we could readily incorporate them. The relevance and integrity levels of subjects and objects will be low, medium, or high. Personnel-classification levels normally do not change over time, but personnel can induce and experience changes in integrity levels and will produce objects of varying relevance levels. Similarly, documents and processing systems often have the same ratings as their content or inputs. For our command center, we propose the following rules, which govern all information-sharing transactions and which we enumerate below prior to discussing their implications in the next section:

1. A subject can read or process an object if and only if the subject's classification level dominates the object's classification level.
2. Initially, all trusted subjects have a high integrity rating, and all subjects and objects are assigned appropriate classification ratings. All untrusted subjects have a low integrity rating.
3. The integrity level of a subject or object can be raised only through a well-controlled process.
4. When a subject creates an object, the created object will have an integrity level equal to the subject that created it, or if the newly created object contains information from other subjects or objects, in full or in part, the new object will have the lowest integrity level of the component information.

5. The relevance level of a subject or object is determined through another well-controlled process.
6. If a subject reads an object of a lower integrity level, the subject's integrity level will take on the object's lower integrity level. The subject can return to its previous integrity level only in accordance with the process defined in rule three.
7. A subject can process and then manually or automatically forward an object to another subject only if the forwarded object dominates the receiving subject's integrity and relevance levels and if the receiving subject's classification level dominates the object's classification.[15]

Rule Analysis and Clarification

Rule one ensures observation of the fundamental requirements of need to know, security, and proper access-control mechanisms.

Rule two ensures that personnel and information-processing systems can share information following our basic rules. Trusted subjects include sources trusted in a wide context, whether that involves coalition partners; our own personnel- and information-processing systems and equipment; and intelligence, surveillance, and reconnaissance resources. Untrusted subjects include those systems and personnel not under the command center's control, possibly including subjects such as the domestic and international media, informants, or any source of questionable origin.

Rule three dictates establishment of a formal process to change the integrity level of a subject or object. The intelligence community uses similar procedures to mark the level of trust in an intelligence resource; multiple sources of lower integrity levels could provide enough corroboration to support raising the integrity level of a subject or object, but the process of doing so should be well understood and performed by a designated entity. This process will obviously represent one of the most important components of this model since improperly raising integrity levels of a poor information source could compromise the entire scheme.

Rule four requires that personnel or systems creating information attribute the source accordingly and properly mark data at the appropriate integrity level. Doing so will ensure that a receiver places the suitable level of trust or skepticism on the information. New information compiled from multiple sources will not automatically assume the integrity level of the subject compiling the information; instead, the integrity level of the new object will reflect the lowest such level of the compiled information until application of the process defined in rule three.

The process suggested by rule five can be more flexible than that in rule three, depending on the role of the receiving subject. For example, a tactical ground unit would have a much smaller "sphere of relevance" than would a C2 aircraft orbiting over an area of responsibility. The ground unit would typically be interested in information about an opponent's nearby ground forces, in-range artillery units, or status of aircraft flying close air support, but not in mission tracks of long-range friendly aircraft, threats from enemy air defenses, or air-refueling tracks. However, the C2 aircraft might want to display locations of friendly ground forces in the area of a specific operation. Some process must define an appropriate sphere of relevance for each subject, based on mission needs. At the operational level, each subject should also be able to customize its sphere of relevance to assure the addition of data of interest or the removal of information deemed no longer pertinent.

Rule six prohibits the forwarding of any low-integrity information as higher-integrity information without proper analysis and consideration. Similarly, personnel who read low-integrity information must be careful not to make decisions or pass on the information without putting it into proper context. This particular rule is more difficult to implement for personnel than for data-processing equipment. For example, one could interpret a system's report of erratic and illogical readings from a sensor as a malfunction; additionally, one could include the appropriate caveats with low-integrity data added to a report. However, when the subject is a person rather than an automated system, preventing him or her from acting on or up-channeling information without regard for its lower integrity will present a problem.

Rule seven ensures the proper filtering of information in accordance with integrity and relevance rules. A tactical display is useless if it exhibits irrelevant or misleading information at the wrong time, and unprocessed or incomplete data could cause premature or incorrect decisions. The final caveat guarantees that sensitive operations are not compromised—data must undergo sanitizing or proper declassification before transmission to subjects not involved in the operation. In effect, this rule provides the "push and pull"—preventing information overload from unneeded automated pushes while preserving flexibility for pulling useful data.

Back in the Command Center

In order to implement these rules in a command center, we need to completely automate some processes, let personnel in various career fields or leadership positions handle the others exclusively, and see that both systems and personnel implement several rules. After the transfer of objects to paper form, traditional processes such as classification controls and need-to-know restrictions become personnel responsibilities, while various mechanisms can restrict the flow of digital information. Rules three and five, however, require humans to interpret data and make changes to integrity and relevance levels, based on that interpretation. Intelligence and operations personnel will normally be in the best position to change these levels, depending on the specifics of the situation. In order to enforce both rules, personnel must have a good understanding of the processes and must properly restrict mechanisms that effect changes to integrity and relevance.

Conclusion

Clearly, we operate in a politically complex environment, and many operations occur in the focal point of a 24-hour news cycle. Missed opportunities to engage high-value targets and incidents of collateral damage have equal probability of becoming headlines; both can raise questions about our military effectiveness. As a result, a commander's appetite for information will continue to grow, as will demands that future systems be interconnected via the GIG. Our efficiency and ability to rapidly fuse, analyze, and convert raw data into actionable intelligence will depend on the capabilities of future systems and the processes that govern their implementation. We believe that the classification, integrity, and relevance rules described above will help guide the development of systems for maximizing data fusion and avoid the pitfalls of conditions such as inverted perspectives. Because of the benefits associated with these rules, we need to utilize a simulated command center and information-processing systems to develop them significantly. ❑

Notes

[1] Deputy Secretary of Defense Memorandum, *DOD Chief Information Officer (CIO) Guidance and Policy Memorandum (G&PM) No. 11-8450: Department of Defense (DoD) Global Information Grid (GIG) Computing*, 6 April 2001, http://www.dtic.mil/whs/directives/corres/memos/gigmemo.pdf.

[2] Department of Defense Directive (DODD) 8100.1, *Global Information Grid (GIG) Overarching Policy*, 19 September 2002, 8, http://www.dtic.mil/whs/directives/corres/pdf/810001_091902/810001p.pdf.

[3] *Clinger-Cohen Information Technology Management Reform Act of 1996*, 40 *US Code* 1424, 104th Cong., 2d sess., 3 January 1996, http://www.cio.gov/Documents/it_management_reform_act_Feb_1996.html.

[4] See, for example, Musée des Plans-Reliefs National Monument, http://www.monum.fr/visitez/decouvrir/fiche.dml?id=102&lang=en.

[5] Personal experience of Major Bass.

[6] US Army Future Combat Systems, http://www.army.mil/fcs.

7. Mark Bowden, *Black Hawk Down: A Story of Modern War* (New York: Atlantic Monthly Press, 1999), 136–37, 148–51, 193.

8. House, *Statement of Mr. James B. Engle, Deputy Assistant Secretary of the Air Force (Science, Technology and Engineering), to the House Science Committee on Air Force Information Technology Program*, 107th Cong., 2d sess., June 2002, http://gop.science.house.gov/hearings/full02/jun24/engle.htm.

9. Joint Publication (JP) 3-0, *Joint Operations*, 17 September 2006, II-2, http://www.dtic.mil/doctrine/jel/new_pubs/jp3_0.pdf.

10. John A. Tirpak, "The Network Way of War," *Airman Magazine*, March 2005, 26–31, http://www.afa.org/magazine/March2005/0305network.pdf.

11. Matthew Bishop, *Computer Security: Art and Science* (Boston: Addison-Wesley, 2003), 153.

12. K. J. Biba, *Integrity Considerations for Secure Computer Systems*, Technical Report ESD-TR-76-372 (Bedford, MA: USAF Electronic Systems Division, April 1977), 33.

13. JP 2-0, *Doctrine for Intelligence Support to Joint Operations*, 9 March 2000, I-1, http://www.dtic.mil/doctrine/jel/new_pubs/jp2_0.pdf.

14. Ibid., II-15.

15. Steven B. Lipner, "Non-Discretionary Controls for Commercial Applications," in *Proceedings of the 1982 IEEE Symposium on Privacy and Security* (Oakland, CA: Institute of Electrical and Electronics Engineers, April 1982), 2–10.

> *We stand ready to conduct a large-scale, long-duration irregular warfare campaign as an integral part of the Joint Team, to include counterinsurgency, security, stability, transition and reconstruction operations.*
>
> *—2007 U.S. Air Force Posture Statement*