

Force Templates: A Blueprint for Coalition Interaction within an Infosphere

Robert E. Marmelstein, *Air Force Research Laboratory*

Future military operations will require close coordination and information sharing among heterogeneous units, coalition forces, and other civil and nongovernmental organizations. Although the US increasingly relies on coalitions to achieve its military objectives, the technological infrastructure necessary to support this strategy has

been lacking. The gulf between the desired and the possible is especially glaring in the area of command, control, and intelligence.

This article introduces the force template concept by defining what it might contain and how it can support successful coalition operations. It also presents a model for using force templates to integrate and control the interaction of operational entities within the Joint Battlespace Infosphere (JBI). Ultimately, force templates serve as a repository for mission-critical information about a battlespace entity; this information includes its identity, what it wants, what it has to offer, and how it intends to operate within the theater. With these items, the infosphere can perform contextual brokering of each infosphere member's available resources. The net result is that infospheres become flexible platforms for the exchange of information and services among coalition partners, insuring (to the extent possible) that the right resource gets to the right member at the right time. With the infosphere's emphasis on resource exchange and control, force templates provide the flexibility needed to seamlessly share information among members of ad hoc coalitions.

Lessons learned

To bridge the current gap between technology and military strategy and doctrine, we must examine

what we've learned from past experiments. Consider a 1999 effort to integrate coalition members into a *combined air operations center*.¹ The experiment failed for three reasons: it used US-only applications within core systems, it used the Secret Internet Protocol Router Network (SIPRNET) as the CAOC backbone, and it populated CAOC databases with US-only information. The difficult changes required to remedy this situation were sufficient to cancel a planned follow-up test in 2000.²

However, a key recommendation from the 1999 experiment was to develop a CAOC backbone that all coalition users could access.¹ Although some approaches include explicitly tagging releasable database elements, a cleaner solution requires a new paradigm that manages information in terms of standardized, discrete objects. Such an approach would

- Segregate information objects from their source applications and databases
- Enable publish, subscribe, query, and transformation capabilities for producers and consumers of these information objects
- Specify the policy governing how to disseminate published object types in an infosphere

Currently, information potentially releasable to

Emerging architectures, such as the Joint Battlespace Infosphere, leverage Web and e-commerce technologies to streamline command, control, and intelligence operations. Force templates provide a mechanism for seamlessly integrating diverse coalition forces into these new information systems.

coalition partners is often combined with other, sensitive data in client applications and databases. The unfortunate result is a denial of useful information to coalition partners because the aggregated data is at the highest system security level. Segregating information into small, coherent, discrete packages makes it easier to control and thus distribute to other coalition members.

Converting sensitive data into a releasable form is also desirable. In many cases, highly trusted, lightweight programs (called *fuselets*) help accomplish such transformations. Policy associated with information objects (nominally defined by the publishers) will determine to whom, and in what form, to disseminate specific objects. Therefore, the combination of an infosphere, better information packaging, and fuselets would facilitate the controlled, secure sharing of information within a coalition.

The Joint Battlespace Infosphere

The JBI is a system of systems that integrates, aggregates, and distributes information to users at all echelons, from the command center to the battlefield. Infospheres are a critical stepping-stone to solving the problems of a coalition's command, control, and intelligence integration because they inherently provide many of the capabilities described earlier. Two consecutive US Air Force Scientific Advisory Board (SAB) reports outlined the JBI's conceptual framework,^{3,4} encompassing four key concepts (see Figure 1):

- Information exchange through publish, subscribe, and query
- Transformation of data to knowledge via fuselets
- Distributed collaboration through shared, updateable knowledge objects
- Assigned unit incorporation via force templates

Force template concepts

Although the JBI provides a platform for information transfer, others must provide the content. For an infosphere to have value, the participating entities must quickly "plug in" and use it to exchange information and service resources. The force template contains the information that enables operational entities in the battlespace (and their clients) to quickly interact using the JBI platform.

The force template also includes the context and policy that define an entity's con-

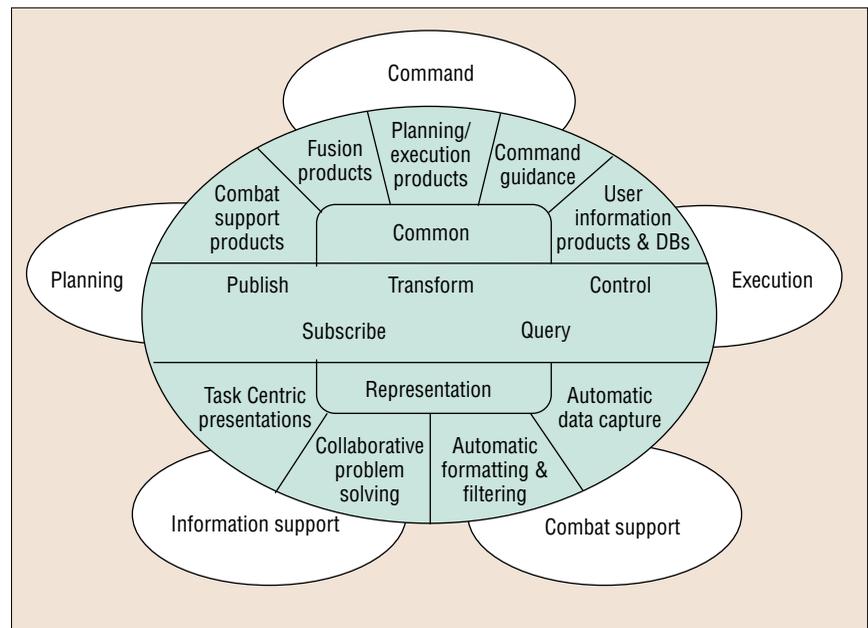


Figure 1. The Joint Battlespace Infosphere's capabilities. The JBI core services of publish, subscribe, and query provide the foundation for knowledge creation and collaboration applications supporting key command and control functions.

tract with the JBI. A key motivation for developing the force template concept is the JBI's need to grow (or shrink) in a modular fashion that reflects the associated military operation's phase. The JBI must handle dramatic and sudden content changes while maintaining an acceptable service level. Without the force template mechanism, tracking and managing JBI content changes due to the arrival and departure of coalition units becomes extremely difficult.

Entities, clients, and passes

An *entity* is an organization that decomposes into multiple components. These components can be other entities (child entities) or *clients*. In the force template model, entities primarily correspond to operational military units and the organizations that support them. Both parent and child entities can have their own force templates (for example, a wing and its associated squadrons can each have their own force templates). These templates could be separate but linked, based on their relationship. The level at which force templates are required should reflect the force's modularity (for example, the level at which forces can be mixed, matched, or tasked).

Ownership

Clients should correspond to specific individuals, systems, applications, repositories, or platforms (for example, a fighter squadron entity can own an F-15 client). A client interfaces directly with the JBI on its owner's behalf.

Unlike entities, clients cannot decompose into subcomponents. However, the entity that owns a client must be registered before the client can connect to the JBI platform. Entities at any level may own a distinct set of clients. Figure 2 illustrates the entity-client relationship.

A *pass* is an electronic description of a client that lets it interface with the JBI. The pass defines what a client may do when connected to the JBI. This is primarily expressed in terms of authorized client publications and subscriptions. The information in the pass must be consistent with the force template of the entity that owns the client. Table 1 summarizes the differences between force templates and passes.

Force template contents

There is a wide spectrum of information that the force template could potentially provide the JBI. Some items are essential for operating the JBI; others are extensions of the capabilities outlined in the SAB report. Basically, three separate categories characterize force template content: necessary, desired, and speculative (see Figure 3).

Necessary contents

Necessary content describes the information force templates must possess to support basic JBI core services (publish, subscribe, and query) and trusted operations.

Information the entity needs in the theater. The entity can request information in terms

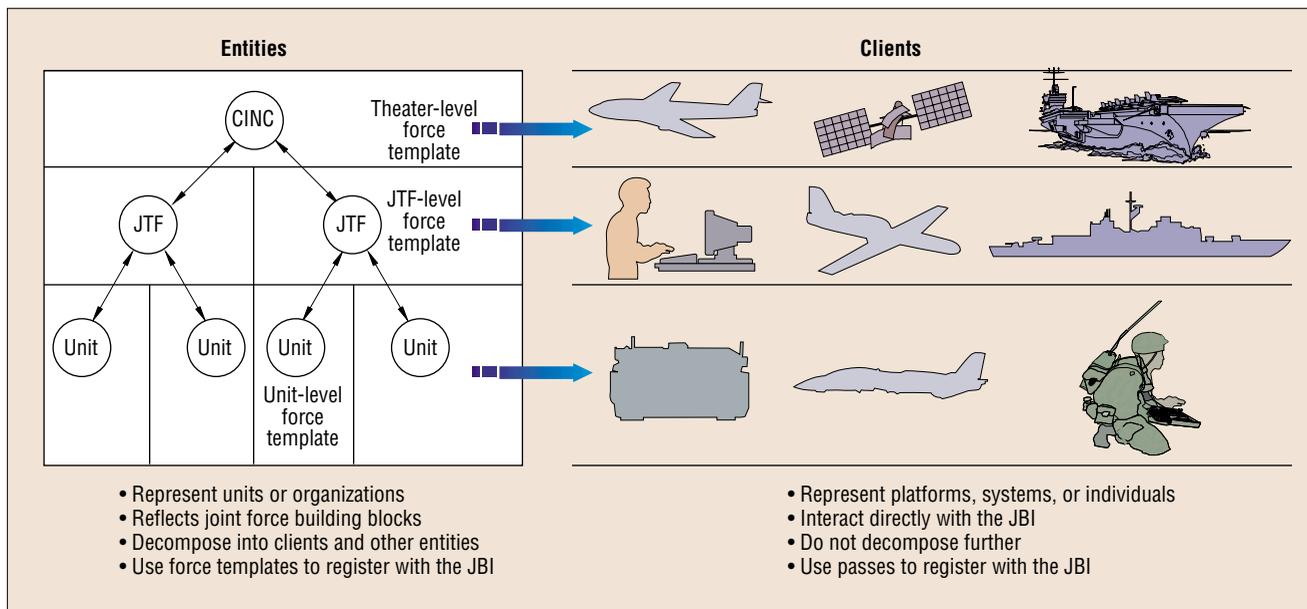


Figure 2. The entity–client relationship.

of categorical requirements (expressed as a metadata query) or in terms of specific information object types (predefined subscription requests).

Information the entity provides in the theater. Likewise, the entity can express information using metadata descriptions or in terms of specific information object types (advertisements).

Associated constraints. In many cases, information provided or requested will have constraints associated with it. Examples of subscriber constraints include desired quality of service, pedigree, preferred sources, and required delivery windows. Examples of publisher constraints include anticipated publication times and rates and dissemination limitations. These constraints can also be expressed in terms of rules about information object content. In this case, publisher advertisements can include information on

publisher capabilities (such as filtering and query capabilities). The JBI platform can use these constraints to broker information requirements against available information products.

Security information. The force template could provide several security-related items to the JBI, including

- Identity and security credentials for individuals occupying key unit positions
- Public keys for specific clients (individuals, platforms, or systems)
- Dissemination limitations on published information

Desired contents

Desired content augments the force template structure to support more contextual, intelligent information brokering and increased

availability of information transformation options.

Information pedigree. Indicators of the quality, reliability, and integrity of entity publications comprise the information’s pedigree. As such, pedigree ratings might be provided in part by the entity (self-assessment) and in part by the JBI (based on previous history or consumer experience).

Entity description. Ideally, the description of the entity interfacing with the JBI should take the form of a “resource map” that describes all entity components (devices, clients, data sources, and people) visible to the JBI. It also includes the child entities that compose the entity (for example, squadrons within a wing). Each item on the map should list the characteristics of the particular resources. Examples of some unit characteristics include mission description, unit organizational structure, loca-

Table 1. Comparison of force templates and passes.

	Force template	Pass
Purpose	Register entities with JBI	Register clients with JBI
Activation prerequisites	Approval of Joint Force Commander or parent entity	Registration of owner entity’s force template with the JBI
JBI interface	Force template controller	Client adaptor
Content characteristics	Distributed, hierarchical, decomposable	Consolidated; cannot be decomposed
Minimum contents	Entity information requirements and products, entity-level constraints, and passes for the clients the entity owns	Information object and advertisements, subscription requests, and client-level constraints

tion, capability description, resource maps, and pointers to associated force templates.

Fuselets associated with publications or subscriptions. Examples of fuselets associated with publishing or subscribing include XSLT, Excel spreadsheets, Active-X components, or Java Beans. Ideally, the force template would contain references to fuselets available from the entity. These fuselets should be associated with specific publications within the JBI (but not necessarily by the providing entity). A rigorous certification process must be established for any fuselet introduced into the JBI.

Speculative contents

Speculative content extends the force template structure to help the JBI support the brokering of solutions composed of both information and computational or agent-based services. It also provides the knowledge base needed to facilitate seamless interaction between diverse coalition members.

Ontologies and ontology mappings. The more diverse the coalition, the greater the importance of shared semantics. For coalition operations to be successful, a consistent set of terms must be used to facilitate information sharing.⁵ As a result, including ontologies specific to an entity, system, or related domain is essential. Whenever possible, these ontologies should come with mappings to common ontologies used within the JBI.

Process models, rules, and constraints. Items describing how the entity does business in the theater of operations include models, rules, and constraints. Ideally, they will be specified in terms of the included ontologies.

Available services or agents. Service and agent items describe benefits provided by the entity for use by other (appropriate) JBI entities. Examples of services might include computation of look angles for satellites, requests for surveillance of certain areas, and agent services for determining unit personnel location and status.

Entity-client interaction model

The SAB report painted a general picture of what the JBI should do and what technologies it might leverage. It did not, however, provide guidance on how the JBI should behave. There is no official model for interaction with the JBI, so let's take a first cut at

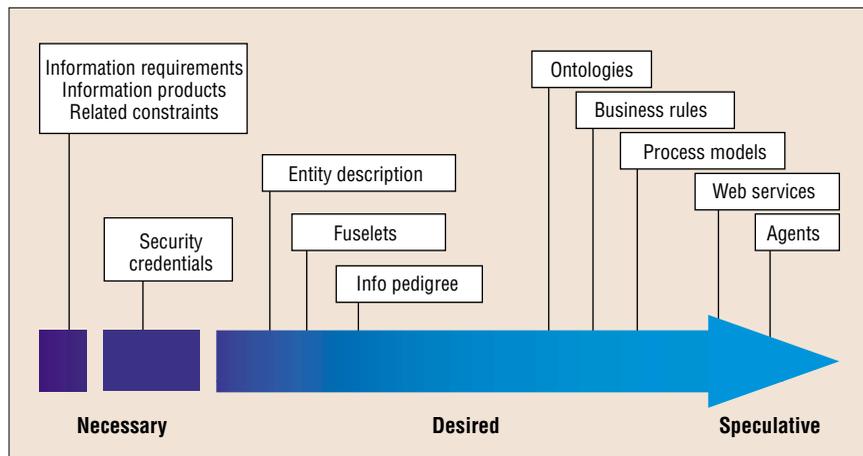


Figure 3. Force template content.

developing one. The model proposed here (see Figure 4) ensures that the following requirements are met:

- The JBI platform has visibility and control over its inputs and outputs.
- Entities maintain control over what their clients are allowed to do within the JBI through the force template infrastructure.
- Dynamic changes to the force template can be made after registration, allowing the flow of information to evolve during the mission.
- The integrity and consistency of associated force templates and passes are maintained.

The model assumes that the entity has already registered with the JBI platform. The notional steps needed to register entities are

1. The entity locates the appropriate JBI.
2. The entity requests permission to connect to the JBI platform.
3. The JBI requests a force template package from the entity.
4. The entity transmits its force template to the JBI platform.
5. The JBI processes the force template package.
6. The JBI tenders response: acceptance, partial acceptance, or rejection.
7. If acceptance is granted, a controller process is elaborated for the force template.

As discussed earlier, the entity must register prior to registration of its clients. Clients cannot register with the JBI until an acceptance or partial acceptance is tendered. It is assumed that child entities are not required to register before their parents. This feature

offers flexibility in extending the JBI in cases such as when individual squadrons deploy to a theater without their parent wing. Here are the steps for registering individual clients:

1. The force template controller (FTC) ensures that adapter processes are elaborated for each client associated with the entity's force template.
2. The passes associated with the clients are cleared for activation in the JBI. Individual clients could attempt connection to the JBI.
3. The client registers with the JBI through its associated adapter.
4. The adapter validates the client. It then receives permission to interact with the JBI in accordance with its pass.
5. If the pass is not validated, permission to interact is denied.

The acceptance of the entity's force template triggers the allocation of an FTC in the JBI platform. The FTC is a gatekeeper that ensures clients behave in a manner consistent with the force template. It also controls changes to the force template that can occur during the entity's JBI session. These changes could be initiated from the bottom up (for example, the client wishes to publish a new information object type) or from the top down (parent of entity or JBI information staff mandates changes to the force template).

As discussed earlier, the force template contains all passes associated with the entity's clients. The pass contains the approved advertisements and subscriptions for a given client (see Table 1). After the entity registers, the JBI platform maintains its passes. When the client registers, it submits an encoded reference to the pass that resides on the JBI. If they match, the client is given permission to interact with the JBI;

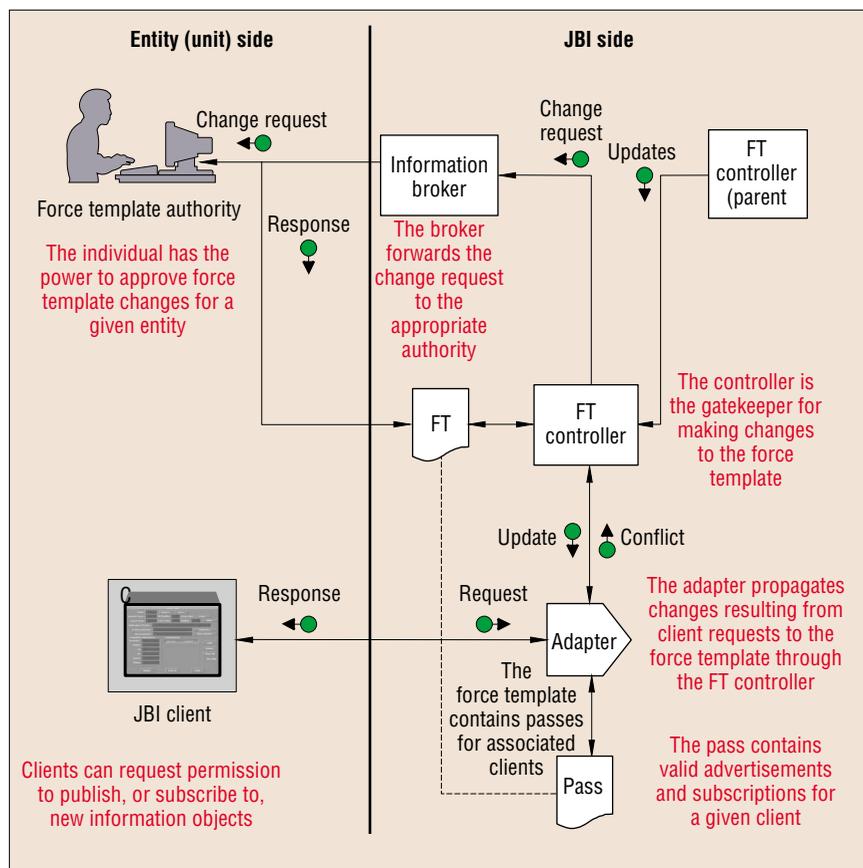


Figure 4. Strawman force template interaction model.

otherwise, permission is denied.

Once successfully registered, the client can then initiate JBI transactions (advertise, publish, subscribe, and query) for approved information objects. If the client needs to change its profile, this request is forwarded to the corresponding FTC (through the client's adapter). If the request is consistent with the force template permissions, then an affirmative response is sent back to the client. As a result, the client's adapter on the JBI platform updates the pass. If a negative response is given, however, the request is forwarded to the appropriate authorizing authority for further consideration. The authorizing authority can then decide what, if any, changes to make to its force template in response to the request. This lets the authorizing authority for a given information object be the final arbiter of who has access to it. Nominally, the entity publishing an information object will be the authorizing authority, but this might not hold true in all cases.

Correspondingly, if changes are directed from above (by a parent of the entity or by the JBI information staff), those changes are

routed through the FTC. Because these changes are directed (not requested), the force template is automatically updated. This causes the changes to propagate back down to the affected clients' passes. These updates will result in the expansion or contraction of the client's transaction privileges in the JBI.

The JBI platform maintains the copy of the force template (and its associated passes) updated during the mission. The entity still retains its copy of the original force template submitted. Because the entity can access (copy) the current force template at any time, it can choose to save versions of the force template as it evolves. If desired, these saved versions can then be used in the future (instead of starting over with the original).

The impact on coalition operations

Now that we've seen how the force template model works, let's examine how it enhances coalition operations. For the sake of this exercise, assume that all in-theater coalitions possess the credentials and systems necessary to interface with the JBI. Recall that when each coalition member registers with

the JBI, its force template will (at a minimum) define what information it needs, what it has, and the constraints associated with each.

Although the JBI is primarily oriented toward military forces, the force template mechanism has the flexibility to accommodate relatively ad hoc coalitions. To be successful, military operations other than war will require the participation of several organizations, including local civil authorities and nongovernmental organizations.⁶ As a result, future command, control, and intelligence systems must be designed with these organizations in mind and provide flexible, appropriate mechanisms for interfacing with them. In cases where these organizations are operating in-theater, they can help provide essential services, such as humanitarian relief, and could (indirectly) serve as important sources of intelligence. In turn, these organizations must be protected without compromising military operations. Successfully integrating them into a common command, control, and intelligence environment is complicated by the fact that they have fundamentally different missions, practices, ontologies, and equipment from the involved military units. Although it's not a total solution, the force template acts as a general-purpose repository for information that describes aspects of each entity; future command, control, and intelligence applications can draw on these building blocks to overcome problems.

Regardless of the coalition member's identity, his or her validated force template will serve as the basis for deciding how the member's information is used and by whom. Once an entity registers with the JBI, the JBI platform can broker the information products it promises to provide according to its specified constraints. This enables each coalition member's information requirements to be intelligently matched with the resources designated as accessible to that member. As part of this process, the JBI can identify the available fuselets that can transform sensitive published information into a form that is releasable to the coalition member. The JBI user will also be able to browse resource directories and identify useful categories of information objects not currently available (if those entries are not masked). Once identified, the member can use his or her force template as the basis for negotiating access to these resources from the publisher.

Although there is no guarantee that this process will satisfy all of a coalition member's information requirements, it lets him or

her leverage the full range of resources (both information and services) available to meet the member's needs. Given this, the coalition member could satisfy his or her needs from an ad hoc collection of available sources, rather than relying on a single source. Thus, instead of the wholesale denial of information that commonly occurs today, the JBI infrastructure will make it possible for the member to get some subset of what he or she needs. Within this context, the force template serves as an important enabling mechanism to fashion flexible, information solutions for a diverse set of coalition users.

If the last decade is any guide, dynamic, diverse coalitions composed of military, civil, and nongovernmental organization members will carry out our future military operations. The key to success in these operations will be insuring that these entities can quickly exchange both information and service resources within an information-centric infrastructure or infosphere. Force templates can facilitate this interaction.

The US Air Force Research Laboratory is evolving, refining, and translating the force template concepts introduced here into requirements as part of the JBI systems engineering process. AFRL plans to design a pro-

totype force template structure and the associated set of processing services and integrate them into its JBI core implementation within the next two years.

References

1. US Air Force Execution Office, *Final Report—Joint Expeditionary Force Experiment 1999*, AFRL, Langley AFB, Va., 3 Dec. 1999, pp. 44–45.
2. US Air Force Execution Office, "Alliance Participation Lessons Learned Supplement," *Final Report—Joint Expeditionary Force Experiment 2000*, AFRL, Langley AFB, Va., 2000.
3. US Air Force Scientific Advisory Board, *Report on Information Management to Support the Warrior*, tech. report SAB-TR-98-02, US Air Force, Washington, D.C., 2000; www.sab.hq.af.mil/archives/reports/index.htm.
4. US Air Force Scientific Advisory Board, *Report on Building the Joint Battlespace Infosphere*, tech. report SAB-TR-99-02, US Air Force, Washington, D.C., 1999; www.sab.hq.af.mil/archives/reports/index.htm.
5. R.H. Anderson and W. Baer, *Potential Military Applications of Peer-to-Peer Computer Networks*, tech. report DRR-2670-RC, RAND Corp., Santa Monica, Calif., 2001.
6. R.A. Estilow, "US Military Force and Operations Other Than War: Necessary Questions to Avoid Strategic Failure," *The Maxwell Papers*, vol. 3, Aug. 1996.

The Author



Robert E. Marmelstein is a Lieutenant Colonel in the US Air Force. He is currently assigned to the Air Force Research Laboratory Information Directorate, where he is a program manager with

the Joint Battlespace Infosphere program. His research interests include applying machine learning, Web, and e-commerce technologies to the problems of Air Force command and control. He received his BS and MS in electrical engineering from Michigan Technological University and the University of Lowell, respectively; he received his PhD in computer science from the Air Force Institute of Technology. Contact him at AFRL, 525 Brooks Rd., Rome, NY 13441; robert.marmelstein@rl.af.mil.

For information on this or any other computing topic, please visit our digital library at <http://computer.org/publications/dlib>.