Do We Need An Information Corps?

By MARTIN C. LIBICKI and JAMES A. HAZLETT

Warfare is a changing art, a fact clearly illustrated by the events in the Persian Gulf during 1990–91. The type of human behavior reflected by the Hundred Years War can now be manifest with modern technology in one hundred hours as Operation Desert Storm. Yet in the Gulf, for all the modern dimensions of that conflict, military operations were conducted with weapon systems that had been designed and fielded in the 1970s: Patriot missiles, surveillance satellites, and the like.

Summary

Warfare is about to enter a new phase that will upset the traditional balance between information and force. As firepower becomes an appendage to information, organizational transformations will begin to underpin a new architecture. A separate Information Corps could guide this revolution, create common doctrine for the diverse requirements of information warriors, and facilitate liaison among civilian information agencies. Such a corps could also obviate the need for the services to integrate their data systems because standardization would exist from the outset. Moreover, the corps could foster innovations more consonant with the logic of the information revolution than would be the case if the services were left to their own devices. But even though the proposal for such a corps has merit, a number of issues concerning its likely impact on operational autonomy, the critical functions of operational units, and certain joint imperatives must first be addressed.
### Title and Subtitle

**Do We Need An Information Corps?**

### Authors

Center for Counterproliferation Research
National Defense University
Washington, DC 20319-5066

### Abstract

The original document contains color images.

### Security Classification

<table>
<thead>
<tr>
<th>a. REPORT</th>
<th>b. ABSTRACT</th>
<th>c. THIS PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>unclassified</td>
<td>unclassified</td>
<td>unclassified</td>
</tr>
</tbody>
</table>

### Distribution/Availability Statement

Approved for public release, distribution unlimited

### Notes

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18
Abrams tanks, Aegis cruisers, and even the Airborne Warning and Control System (AWACS). At the same time, the operation of those platforms, and their augmentation by powerful information systems, suggests that the revolution in warfare is about to enter an entirely new phase. Future changes will be most successfully adopted by systems which have been the most thoroughly structured.

Information, in sum, is the principal difference between eras. Granted, the benefits of both strategic and tactical information have never gone unnoted; they have been decisive in many battles. What is new is the sheer size, speed, and volume of the information flow needed to achieve superiority in combat. Information superiority is emerging as a newly recognized—more intense—area of competition. The result may be the upending of the relationship between information and force. Thus it may be the time to form a future force to examine future warfare issues, like how to best deal with the information revolution by developing the requisite strategies to exploit it.

The existing relationship between weaponry and information is similar to the relationships among weapons systems and other supporting elements such as command and control, logistics, and personnel. Operations sit atop; all else supports them. Current weapons have accommodated the information revolution by taking advantage of additional data inputs, but the military remains organized around units of force. This architecture may soon become obsolete. Instead, those who prevail tomorrow may build their forces around a central information processing core. Such a core would launch information probes into the media of war (that is, in land, air, sea, or space warfare, or the entire spectrum), gather, transform, fuse, and harness the returning stream and ladle results in strategic synchrony directly to fire-control units or indirectly to operators. In either case, the traditional relationship between information and force will be turned on its head. Information no longer serves units of force—rather units of force are fire support for information systems.

The necessary and sufficient corollary to this transformation is about organization. Current structures are built around legions of operators, served by lesser communities, such as intelligence (as well as logistics, engineering, communications, etc.). In this context lesser is not meant in a strictly pejorative sense. However, in any unit which combines this discipline, the operators take command. Moreover, although career tracks are similar up to a certain level, operators clearly make up a much higher percentage of the top ranks (O8s and above) than they do of the officer corps as a whole. On the other hand, if information warriors belonged to a separate organization (be it a corps, service, or command), their relationship to the whole would undergo a concomitant and perhaps necessary adjustment.

Rationalizing a Corps

The purpose of the Armed Forces is to fight and win wars. Winners in the future will take advantage of the fruits of the information revolution—including global positioning systems, global surveillance, and space-based sensors—while the losers will not. To win one must be organized to take advantage of the opportunities offered by the information revolution.

A separate corps and an associated command structure linking operations and intelligence will facilitate effective joint operations, promote the information revolution in warfare, unify the disparate information elements and give them an identity, create a common ethos for information warriors, and provide a unified interface with civilian information infrastructures.

Jointness. The farther platforms can see and shoot, the larger their battlespace, and the more service-specific battlespaces intersect with each other. Aircraft of the Navy and Air Force use the same Air Tasking Order. Data collected by Air Force assets guide Army movements. National sensors alert anti-tactical ballistic missile forces of missile launches.

Martin C. Libicki and Commander James A. Hazlett, USN, are both senior fellows in the Institute for National Strategic Studies, National Defense University.
All the services use the same satellite systems. Another factor that demands interoperable, or single, information systems is the tremendous annual increase in the volume and variety of data collected.

Most importantly, there is transition in how wars are fought and the diminished local ties between seeking and shooting. Today the two are closely linked. Although prepared by intelligence reports, a tank must both find and kill the target itself. Yet, other forms of warfare have already experienced the separation: strike operations are planned from externally collected data, anti-submarine warfare operations use an elaborate localizing program prior to administering a coup de grace. The Joint Surveillance and Target Attack Radar System (JSTARS) and AWACS support an efficient cue-and-pining system. The advent of precision-strike systems that use both absolute and relative positioning (that is, latitude, longitude, bearing, range, course, and speed) is at hand. The growing proliferation of sensor systems implies that the targeting systems of tomorrow must be able to fuse data collected from a wide variety of sources. Such fusion means that seamless interoperability is being demanded for missions ranging from single-shot targeting all the way to situational awareness by CINCs.

To illustrate the value of an integrated perspective consider a hypothetical Unmanned Aerial Vehicle (UAV) sensor package and how it might be developed—not only its hardware, but also its software, communications, integration with other data units, and most importantly its doctrine and concept of operations. UAVs can serve all services, and on their own each service would develop a package to fit its own mission profiles and support their own platforms. Yet, it can be expected that the data flows from UAVs would go to common data receptors and would have to meld with other joint data collection assets including ground-based sensors, higher-altitude aircraft, and space sensors. To the extent that each sensor package performs its own on-board processing, it may wish to take advantage of common neural training regimens and pattern recognition tools. Data from the various sensor packages—which could come from any of the services—have to be analyzed in real time to determine where follow-on data collection efforts have to be focused, or whether and when fire control solutions have to be generated. The interoperability requirements of such a package are therefore demanding.

The need for interoperable information systems has been widely recognized by the senior leadership within DOD. Earlier this year Secretary of Defense Les Aspin observed in a graduation address at the National Defense University, “Most of our systems for the dissemination of intelligence imagery cannot talk to each other.” The principal joint command and control initiative (“C*I for the Warrior”) is exclusively about interoperability, and all new information systems must be able to communicate jointly. Unfortunately, history suggests that after-the-fact standardization frequently leads to unsatisfactory results. Why?

- Standardization is a long-term process that accommodates new developments only after long delays. Over the next twenty years the percentage of new applications to existing ones is apt to grow greatly; intelligent filters that correlate and process multispectral and nonelectromagnetic sensory data are on the threshold of major growth.
- Standards developed by competing interests often choose a least-common-denominator approach, letting each side agree to disagree at the expense of interoperability.
- Emphasis on data interoperability ignores the growing role of software interoperability. Therefore, in the case of the sensor package, development by different platforms groups increases the possibility that each system stands alone and makes complete data fusion that much harder to achieve.

An Information Corps is an alternate route to data integration. Instead of the services and DOD agencies (and the multiple communities within them) attempting to merge information collection and dissemination systems, the functions would be carried out by a single organization that operated under centralized doctrine and command. Data would be standardized from the start; internecine politics that allow components to agree to disagree would be, if not eliminated, then substantially muted. What would otherwise be a conflict between
the need for innovations in data collection, and the subsequent need to report only that which has been standardized, would be muted as well. Successful innovations would be integrated into the whole much earlier in their development.

A related rationale emerges from the emphasis on Joint Task Forces (JTFs). Today and in the future the services will be increasingly cobbled together by JTFs. Such organizations, which usually are made up of a chunk of this and a chunk of that, demand that most chunk commanders (and key staff members) know each other beforehand. A coterie of information warriors whose specialty is preparing the battlefield image but who are attached to different operating units is already integrated. Acting as the glue, they can help bring together far more fine-grained units.

Innovation. The information revolution is almost a cliche. Less well accepted is the threat that it will pose to the concept of putting men and women in steel, titanium, or ceramic boxes to fight wars. Why are platforms at risk? As more data is collected over the battlefield, the grid atop it grows tighter, smaller, and stealthier. Objects can be found faster and tracked more reliably. True, today’s weavers—and the United States has the best—are themselves large platforms and are thus tomorrow’s targets. Yet as sensors, processors, and communicators grow smaller and cheaper, comparably effective grids can be built from networks of distributed sensors which collectively would be more robust than complex platforms (e.g., it is harder to take down a million balloons than a dozen JSTARS). The contest between industrial-era platforms and information-era networks will increasingly favor the latter (even though stealth will postpone the inevitable for some). Forces with fewer manned platforms suggest radically different capabilities for the military of today. History suggests that organizations may resist change but to their ultimate disadvantage.

No one questions the overwhelming relative superiority of the U.S. Armed Forces, and for that reason our manned platforms would logically be the last to be threatened or copied. A potential competitor would be foolish to challenge our dominance by a strategy
that copied our force structure. Forces built around information systems constructed from commercially available components, however, would pose a more serious threat—one which contests our reigning paradigm. Thus, it would be far more attractive to challenge us in that way.

Although an Information Corps may not be inherently more innovative than the services, it is more likely to pursue the kinds of innovations that accord with the logic of the information revolution. Left to themselves, the Armed Forces will incorporate information into weaponry, but with information technologies as platform support rather than with platforms as fire support to an information grid. An Information Corps, however, would take an entirely different approach from the outset, emphasizing the information grid as central. Constituent elements and doctrine for such a grid would be evaluated on their ability to locate, track, and evaluate objects and events passed for conversion into fire-control solutions and servicing. Such a service or corps would be an institutional advocate for a paradigm shift, and would, by its advocacy, better prepare for a threat which comes from a different direction.

Unity. The common argument against creating a completely new organization is that its planned functions are all being done by someone else. When this question is posed, however, the composition of the group varies widely: the Director for Command, Control, Communication and Computer Systems (J–6) on the Joint Staff, Defense Information Systems Agency, Defense Mapping Agency, Space Command, and intelligence agencies—all without going into the services. Under the latter are functions such as command and control, electronic warfare, meteorology, oceanography, information processing, and high-information platforms such as Aegis, AWACS, JSTARS, and UAV contingents. Other functions which technology may soon enable are not even listed for obvious reasons; when they do emerge the soup will be even thicker. This is just the point. The various sub-communities in the information-based warfare community see themselves as disparate players. Each relates to one or two others at most, and they all lack the common unifying doctrine of operations. Information warriors are more than simply communicators, data processors, or intelligence agents. They are all part of a global structure that would become apparent with the creation of an Information Corps.

Culture. A related reason for integrating various DOD informational elements into a single corps is to provide information warriors with status, culture, and an ethic. The issue of respect is relatively straightforward. As information becomes more important, so does cultivating the ability to develop and
manipulate it. DOD needs to attract these people not only as contractors but more importantly as operators. Successful military organizations must deploy not only superior information systems, they must also be able to fix, adapt, and maintain them in battle in real time. Yet an aspiring officer today would be advised to specialize not in information but in operations. Even the Air Force—the most information-intensive service—is oriented toward its fighter pilots as the Navy is to ship and submarine drivers and naval aviators. Top echelons in other specialties such as administration, material management, and command and control are often assigned from the ranks of operators. This procedure makes sense if various specialties call for similar skills and the best are attracted to operations; an elite is an elite regardless of what it does, and it could as easily be mergers and acquisitions. However, if the skills required to be a good information warrior are different from the qualities and ethos needed to be an operator or these skills require long, specialized training, then the system makes less sense. The best people avoid information and those who remain do not get the consideration their views deserve.

An Information Corps offers the possibility of separate and more appropriate training and career management as well as an ethos for an information warrior. As computers get more sophisticated, training necessary for their effective use may get longer. The information warrior must know not only programming but systems integration and systems theory, communications, security, artificial intelligence, logic in all its many forms (classical, fuzzy, and convergent), and statistical techniques. The information warrior must also know the customer’s needs: the commander’s intent, doctrine, and strategies. In addition, the information warrior should know something about specific media (land, sea, and space). Sending a college graduate to the field for a few tours of general expertise interspersed with training classes and then expecting first-rate information techniques in a more specialized tour later may not be adequate. The amount of information necessary to be an information warrior is immense, and the time required to master it
will have to at the expense of more general command instruction. If this tradeoff is to be made voluntarily, the results have to be rewarded commensurately. An integrated Information Corps with clear career paths and opportunities for command and success would do this.

As for ethos, a divergence between operators and information warriors must be expected. Discipline under fire places a premium on certain qualities: courage, decisionmaking, instinct, self-control, loyalty, and so forth. The information warrior, by contrast, must be highly intelligent, creative, independent, flexible, tenacious (to counter infamous 3 a.m. computer bugs), and maybe somewhat eccentric. The example of Admiral Grace Hopper will not excite a tank commander any more than General George Patton excites a bit twiddler. These qualities are not necessarily antithetical, and some qualities—common sense, judgment, contrapuntal thinking, decisiveness—are uniquely common to all warriors regardless of weapons. To seek such qualities in operators and not information warriors further relegates the latter to subordinate status.

Ethos, status, and training issues suggest the need for an Information Corps as well as a unified or specified information command. The latter could produce unity of operation, advocates for change, and liaison, but not doctrine, status, or continuity (e.g., information warriors who are evaluated by other information warriors) that such a corps needs.

Like the sign which reads "Call Miss Utility Before You Dig," both communities will have to shake hands before one or the other adds, subtracts, or alters its infrastructures. DOD used to formally liaise with AT&T when the latter was still dominant in telephony in the United States. Since then, the number of information players has multiplied, and not just because AT&T has been rent asunder. In addition, as the DOD need for information intensifies, and its assets commingle with commercial systems, the volume of interaction will greatly exceed what one community can cope with. A common point of contact on the civilian side—with its public and private players—will never happen; but a common point of contact on the military side is quite possible. A separate Information Corps would provide not only a common point of contact but common doctrine and outlook. With a national information strategy and a national military information strategy human protocols would not have to be reestablished every time the two worlds come in contact.

Functions of a Corps

Determining what an Information Corps does (on formation, its duties will be those of the units which comprise it) is thus tantamount to delineating the borders between the corps and the services from which it would grow. The first concern is doctrine. The transformation of the Army Air Corps into the Air Force was more than a catch-all for those who flew planes; it was also an expression of a theory of war, to wit: the ability of airpower to transcend the ground situation and transform strategic conflict through Liaison. Just as the information space of the various services is converging, so too is the information space of the defense and commercial sectors. DOD uses commercial communications satellites and bought the bulk of Spot's imagery in the Gulf War; and boaters use the DOD Global Positioning System. The defense and commercial sectors swap weather data, and the DOD Global Grid is the military version of the National Information Infrastructure (which is a component of a global infrastructure). An Information Corps would play a major role in the development of a national information strategy and a complementary national military information strategy.
aerial bombardment. The Marine Corps, in its evolution as a separate service, similarly has built a doctrine of amphibious warfare. Each service maintains its ability to comprehend war from its perspective.

An Information Corps would also have its doctrine. As alluded to above, the doctrine would support a primary mission of the Armed Forces to develop and exploit a common integrated image of the battlespace. This integrated image would, of course, be divided and apportioned to meet the needs of various warfighters. Slicing and dicing would entail analysis, filtering, enhancement, correlation, data fusion, and whatever else is required to assist decisionmaking.

The image, in turn, is an important component for decisions which range from strategy to weapons control. The bounds of such a system would vary from situation to situation. In some cases a coherent image would be used for centralized decisionmaking (such as an Air Tasking Order); in other cases an image would call forth efforts to collect further information (launching sensors). Some fire control solutions would be automatic, to take advantage of evanescent opportunities that a decisionmaking hierarchy would only slow down. Other images are background to on-the-spot decisions (tanks should not have to relay pictures of targets to a central grid for a go-ahead before engaging them). Clearly the usefulness of a unified image depends on what percentage of the information involved in making a decision is generated by the shooter (coupled with what share of the processing necessary to transform data into decisions is supplied by external algorithms). The doctrine is predicated on the assumption that nonlocal information (from other units or remote sensors) and analysis (from artificial intelligence) will rise in relative importance.

Two other reasons for organizing an Information Corps are only now beginning to emerge. One is the concept of information as a realm of battle; just as tanks fight tanks, and subs fight subs, so too would data corpsmen on one side fight those on another. More specifically, data corpsmen would spend their time confounding the other side’s operations in the electromagnetic spectrum or disrupting the operations of their net. This concept alone may be too narrow a basis for a corps and is susceptible to improvements in telematics technology, which may make it harder to interfere with information systems. A second and contentious notion is that any operation that involves information, or alternatively command and control, in its broadest context should be part of a corps. But this is too broad a definition. Not only does everyone deal in one respect or another with information, but command and control tends to involve the top level of a hierarchy. To suggest an Information Corps would become the top-level corps within DOD to which the services must report is presumptuous. However to use such a corps to collect, process, transmit, and present information and then convey the resulting orders is not.

The core of a compact corps and its associated command would consist of elements which gather, assess, and distribute both silicon- and human-based information; an infosphere (see figure on page 93). Space would be a central component, since virtually every current use of space (viz., surveillance, communications, navigation) is directly involved in information. Added to that would be chunks of the intelligence business, and the creation, operation, and maintenance of fixed-site command and control assets, information collection such as ground-based radar and the Sound Surveillance System (SSUS), mapping, and meteorology.

How far an Information Corps should extend into mobile information collection, in the infosphere, is a difficult question. Platforms as diverse as AWACS, JSTARS, Aegis, P-3 squadrons, unmanned aerial vehicles, artillery trajectory indicators, portable radars, and the like are information-intensive and thus similar to fixed-site information systems; but not every function (like airplane driving) on such platforms is appropriate for the data corps. Consider an Aegis cruiser; it certainly collects a considerable volume of data, and much of it could be transformed into actionable targets for other platforms, but most of its functions call for...
other skills. Which among equipment maintainers, screen watchers, situation assessors, and communicators should be data corpsmen? Should they be permanently or temporarily assigned?

A tougher question will involve the mix of military and civilians in an Information Corps. Should it be a defense or joint organization? Some functions of an information service can be best performed by military personnel with varying degrees of expertise and experience of the weapons systems with which they must interface. Other positions will have to be filled by computer geeks who are not disposed to military service.

Objections to a Corps

The difficulty in delineating an Information Corps suggests that creating one is somewhat problematic: it must interface with other command and control organizations, will remove critical functions of an operational unit, and may perhaps relieve some of the pressure of jointness. Autonomy. Single-service cohorts are generally capable of operating autonomously in tactical environments, with little help needed from the others. For the most part an Information Corps could not. If the corps would be limited to fixed-site facilities, it could at least function autonomously, but its value would depend on its ability to provide data to others—it could complete few military missions on its own. But with dispersed sensors and emitters (e.g., UAVs, buoys, listening posts) gathering a larger share of the total data, a fixed-site data corps would become increasingly marginal. It would be valuable for strategic surveillance and distributed interactive simulations.

Including mobile elements in an Information Corps introduces command problems. Each unit of an Information Corps would have to report through its administrative chain of command, but it would have to respond to the operational chain of command as well. Who, below the CINC or JTF commander, determines, for instance, when and where to deploy sensors? Who determines whether an aircraft is used for reconnaissance, electronic warfare, strike operations, or emitter dispersion? Do such needs respond to the requirements of the travelling unit (ship) or the deployed units of some information command (or under centralized control if not command)? All of these issues can be resolved over time or may be eclipsed by circumstances (if ships disappear from the inventory, shipboard problems do also), but that will take some effort.

A related objection is that even platforms whose exclusive mission today is to gather information may not necessarily retain that character. Consider the vignette about UAV sensor packages. If the developers of this hardware and doctrine are information warriors rather than operators, they may not appreciate the potential of a UAV as a weapon rather than simply as a data collector. This problem can be managed and should be addressed as the acquisition process is adjusted to the post-Cold War era.

Criticality. Every organization is an information organization; moreover, information is power. Removing information cadres from such an organization could lead to several unintended consequences. The latter may be tempted to duplicate its lost capabilities—no important organization in the Federal Government, for instance, leaves policy analysis to others. Besides wasting resources it reintroduces the very coordination shortfalls an Information Corps was designed to overcome. Alternatively, affected military units may simply ignore the information
they cannot control, relying on time-proven but obsolescent means of gathering information (reconnaissance in strength) rather than methods which technology makes more appropriate (sophisticated sensors). Thus, the very modernization that an Information Corps was meant to induce would be retarded by its formation. To avoid this strong leadership will be required inside and outside the corps.

Jointness. Finally, while creating an Information Corps may promote a joint battlespace image, it may retard other aspects of jointness. Having removed the most important reason for the services to work together (they would instead liaise with an Information Corps) removes a large part of the impetus for operational units to work and meet across service lines. The need for joint deployment, joint operations, and, most important, joint thinking, remains, but the day-to-day practice of working jointly would be undercut by the act of shoving off certain joint duties to separate organizations. When the time came to act jointly, the various components would be far less prepared than if they had interacted on a day-to-day basis. Again, good leadership should overcome this problem. When it comes to radical reorganization—and forming an independent Information Corps certainly qualifies—a first rule of thumb may be: when in doubt, don’t. As wars are currently fought, the need for a data corps is, while perhaps inevitable, not necessarily urgent. Unlike, say, the Army Air Corps, which was a single identifiable operational arm, an Information Corps would have to be merged from several disparate organizations. By taking from all services, it would be opposed by all. This will be difficult to overcome.

The logical conclusion is that DOD should form an Information Corps. The argument is that a corps would promote jointness where it is critically needed (information interoperability), elevate information as an element of war, develop an information warrior ethos and curriculum, and heighten DOD attention to the global civilian net. When threatened with the loss of personnel and resources, the services may respond that they are doing all of this and more. The greater the threat, the more meaningfully the services may respond. But their response is likely to address problems—integration, doctrine, or ethos—that would otherwise call for an Information Corps. Solving these problems, after all, was the original point. But they cannot do it as effectively as an Information Corps.

One approach to mastering future warfare that should be considered is the creation of a future force cell of forward-thinking officers and civilian specialists charged with taking a long-term look at the nature of warfare and how best to cope with it. To attract, recruit, and maintain what would have to be a highly talented and motivated group of individuals, a separate career field should be established (not unlike the acquisition corps) that breaks off officers and civilians from their contemporaries at the O4/O5 and the GS-13/GS-14 levels and provides them with requisite guarantees of promotion and career enhancement (probably with certain limits like time-in-service). Such a group could ultimately form the nucleus of a corps, draft a national information strategy, and bring the fruits of the information revolution to the Armed Forces. These men and women would serve a unique role in the Department of Defense and provide a joint, quality test-bed for future ideas and concepts.

An Information Corps would increase the effectiveness of the Armed Forces. It would allow us to do the job better, cheaper, and faster. It would give us an edge that would be hard to beat or even challenge. It would keep the United States in the forefront of the ongoing revolution in military affairs. 