THE INFOCORPS – A Unique Proposal For A Unique Mission

As Appearing In the 1998
Armed Forces Communications-Electronics Association (AFCEA) Book
CYBERWAR 2.0: Myths, Mysteries, and Reality.

For further information, copies of the book, or other information, contact author at
rforno@taoiw.org

ABOUT THE AUTHOR

Richard "Rick" Forno is a Florida native and currently the Security Officer for a major Internet Services firm in Herndon, VA.

Mr. Forno received an Army ROTC scholarship and earned an associate degree in management from Valley Forge Military College. Upon moving to Washington, D.C. in 1992, Mr. Forno received a B.A. from the American University School of International Service with a strong concentration in National Security Studies and Middle Eastern Affairs. In June 1997, he was recognized as the youngest graduate in the Naval War College's 110-year history.

Mr. Forno's federal work experience includes helping set up the Information Resources Security Office for the U.S. House of Representatives, where he was primarily responsible for developing security programs, conducting computer forensics, and investigating electronic crimes such as network attacks and e-mail threats against Members of Congress and the Executive Branch. Prior his federal service, he supported military command, control and intelligence systems as a US Army contractor in exercises in the United States and overseas. Mr. Forno was also a consultant to the Office of the Secretary of Defense where he assists in researching and developing capabilities needed to respond to information warfare attacks against the United States. The ideas in this essay sparked a Pentagon move to bring the InfoCorps to reality in 1999 with the White House announcing the "CyberCorps" initiative. Mr. Forno is thus known as the "father" of the Info/Cyber-Corps.

Mr. Forno is a frequent speaker at security community seminars and industry conferences. In his spare time, he has written *The Art of Information Warfare* and numerous articles on information warfare and security management. His articles and commentary have appeared on radio and in such publications as *Forbes, Federal Computer Week, Internet Week, Military Information Technology, Technology Week,* the *Journal of Operations Security,* and more.

Mr. Forno's professional affiliations include: the Operations Security Professionals Society; High-Technology Crime Investigations Association; United States Naval War College Foundation (life member); and the Valley Forge Military Academy and College Board of Directors.

Contact him at rforno@taoiw.org.

The Department of Defense (DoD) has historically designed and created technology to support war fighters within its own environment and kept such products "close to the vest." Unfortunately, in the Information Age, much of the technology development is done in the private, civilian sector, that the DoD does not control. Indeed, civilians are serving as the technology pathfinders for the government and the military sectors. It is natural to see, therefore, the DoD turning to civilian organizations for assistance in developing and deploying technology-particularly information technology-from the private sector, far from the "vest." It is, after all, the civilian experts that drive the United States technology and information industries.

It is crucial, therefore, that the DoD forge a relationship with the civilian IT experts since the defense department (and government in general) has grown reliant on civilian-owned and operated telecommunications systems. This is not for simply routine administrative data, but also encrypted operational communications as well. For example, during the 1991 Persian Gulf War, the civilians were crucial components in developing systems that could accommodate increased DoD communications requirements. For example, twelve commercial satellites supported military communications, backed by hundreds of civilian technicians from AT&T and other corporations that deployed to install and maintain a comprehensive telecommunications infrastructure that consisted of over 23 trunk lines and 30 automatic digital network circuits that carried over 700,000 telephone calls and 150,000 electronic mail messages daily. This is but one example of the integration and reliance of DoD on the commercial sector for information technology and bandwidth. At the time of the Gulf War, it was civilians who were sent-as contractors-to the region to work and interact with the military personnel on-station. Did their work differ that much from the military signals staff wearing uniforms and wearing dog tags?

Now, in 1998, with the many projects involving Information Warfare, there are a growing number of voices looking to develop a cadre of civilian specialists to complement the combat, combat-service, and combat-service-support forces of the United States. This concept-one that I hope comes to fruition in a timely fashion-has been referred to as an "Information Corps" by many theorists in the information warfare (IW) community from the National Defense University, service war colleges, and private academia. This unique organization is conceptualized to provide the much-needed information technology services to the military on a reliable, cost-effective basis. As is typical of today's military, doing more with less means either outsourcing to contractors or implementing a reserve forces program.

The need for an Information Corps

The DoD has recognized and acknowledged the fact that much of what it needs to develop a formidable Information Corps and effectively wage an Information War or conduct war in the Information Age lies in the civilian sector. From academics to system administrators, engineers, and field technicians, the private sector has the number of qualified, competent "bodies" the military needs to support information operations. If one examines the current (post-1991) force structure, most of the Total Force (combat, combat support, and service support) units are in the reserve components. This has its advantages, which will be evident in a moment. The mission of the Information Corps (InfoCorps) would be to provide support services to the military in the information arena from both rear-area and forward-deployed positions. In addition, they would

be responsible for executing activities in the information domain from an operational perspective under proper military guidance and coordination as per the operations plan they are working under. A third mission would be to provide support to the intelligence community on information warfare subjects. After all, the InfoCorps personnel know not just how electrons flow over the wire or how computers work, but the impact that information has on the civilian world, economics, and society at large.

By placing the Information Corps in the reserve, DoD receives a great, cost-effective, Congress-satisfying arrangement. Of paramount significance is the reduced training costs associated with this particular MOS.[1] For example, if one examines the composition of a typical Army Civil Affairs unit, one may find career fire, police, medical, and other public-safety, public-interest specialists among its ranks. When the unit deploys, the members of that unit can draw upon their regular, civilian work experience (such as police management of fire protection) into their military assignments wherever they are deployed. As such, while each member of the unit receives initial, basic, and advanced skills training at both the enlisted and officer levels, unit personnel receive ongoing training by the very nature of their civilian jobs. In return, unit personnel bring back to their civilian occupation additional skills (where possible) that will benefit their employers as well. The end result is a soldier who, while an expert in his field by nature of his civilian job, is also indoctrinated into the military organization, structure, and philosophy. For a small amount of government-sponsored professional, task- oriented military training (such as Advanced Individual Training or Officer Basic Course) the military receives a highly-competent soldier with skills that are constantly being kept current (at little or no cost to government) in as much the same way as a civilian paramedic must-by law-keep current his arsenal of lifesaving skills. The following charts describe potential career paths of an enlisted and officer InfoCorps soldier and compares their professional development with that of an infantryman.

Table 1. (Enlisted Career Development Matrix)

Grade	Infantryman	InfoWarrior Reservist
E-1/2	Trainee/Basic Advanced Training	Trainee Basic Training (IW)
E-3/4	Bradley Driver/Gunner Dismount Team Leader	Advanced Training (IW) IW Team Leader Systems Technician ***A+ Systems School***
E-5	Bradley Gunner Team Leader Squad Leader ***Ranger/Sniper Schools*** ***Basic NCO Course***	IW Team Leader IW Systems Specialist ***MSCE, CNA, etc.*** ***NCS Courses***
E-6	Platoon Sergeant Bradley Commander National Guard Advisor ***Pathfinder, Recruiting,*** ***Battlestaff, Mstr Gunner School*** ***Advanced NCO Course***	IW Section Leader Systems NCO ***OPSEC Program Mgr*** ***NCS Courses***
At this point in a soldier=s career, they move into command advisor, leadership, or other senior positions. Schooling at this stage is typically oriented toward staff planning processes and military theory such as the Sergeants Major Academy.		
E-7	Platoon Sergeant First Sergeant Observer Sergeant Operations Sergeant	IW Section Leader Systems Manager Network Services NCO First Sergeant
E-8 and Above	Senior NCO staff and command positions that depend on service and unit requirements.	

This is a rudimentary comparison between current military enlisted position (in this case, an Army 11M soldier, or Bradley Infantryman) and a proposed InfoCorps enlisted career progression. For the InfoCorps column there will naturally be professional development courses paid for by employers during a soldier=s civilian career.

Key: OPSEC: Operations Security
MSCE: Microsoft Certified Engineer
NCS: National Cryptologic School
CNA: Certified Netware Administrator

Table 2. (Officer Career Development Matrix)

Grade	Infantryman	InfoWarrior Reservist
N/A	Welcome to The Army! ***OCS/ROTC/Academy***	Welcome to InfoWar Reserves! ***ROTC/IWOCS***
O-1	Platoon Leader Unit Staff Position ***Infantry Officers Basic Course*** ***Airborne, Air Assault, etc.***	IW Section Leader Unit Staff Position
O-2	Platoon Leader Executive Officer/Unit Staff	IW Platoon Leader/Executive Officer Unit Staff Position
O-3	Battalion Staff Company Commander ***Infantry Officers Advanced Course***	IW Unit Commander IW Battalion Staff
O-4	Brigade Staff Battalion/Company Commander ***Command and Staff College***	IW Unit/Brigade Commander IW Brigade Staff ***Command and Staff College***
Officers at the O-4 and above would also serve as joint service or IW liaison, advisors, or IW team leaders to active components, commands, and defense agencies on IW issues.		
O-5	Brigade Staff Command Advisor ***Service/Joint War College***	IW Brigade Staff IW Command Advisor IW Unit Commander ***Service/Joint War College***
O-6	Brigade Commander ***National/Joint War College***	IW Brigade Commander ***National/Joint War College***
O-7 and Above	Senior Staff and Command positions that depend on service and unit requirements.	

The military has officer candidate schools and ROTC programs to prepare their future officers. The InfoCorps OCS model would include an orientation to the military, its organization, customs, protocols, uniforms, and operations in a four-to-six-week modified military training program. Personal educational schools and training (such as MSCE, A+, and other technical courses) for InfoCorps Reservist officers are not disclosed in this matrix for a good reason. If one takes the Civil Air Patrol approach mentioned in this paper, there are no enlisted grades in the organization. As such, junior CAP officers serve as technical specialists, communications officers, and other functional positions, as well as undertake any command positions they accept. As such, junior officers may be the MSCE, CNA, or other technical specialists in a unit.

Note that this proposal suggests that current Professional Military Education (PME) oportunities available for existing service people should be extended to InfoCorps reservists. This will not only foster closer ties with their combat component colleagues, but allow InfoCorps officers to be exposed in and participate in (through joint duty assignments) the operations and planning process as they advance in their careers.

Another key element in creating the Information Corps is the cost-effectiveness of specialized reserve units. How many active component functions have been nearly completely placed into the reserves? Several, including 90% of Army Civil Affairs and PSYOP,[2] the entire Air Force airborne radio/television interception/broadcast capability, and much of the Navy's mine sweeping capability.[3] The Pentagon has learned that it is cheaper to fund weekend and annual training periods and the infrastructure associated with such training than to fund a complete, full-time, active component organization. By being reserve components, the military receives a full complement of competent specialists (with supporting infrastructure) able to deploy quickly, at a fraction of the cost of a regular, active component unit.

Many of the civilians most likely to be solicited to join (or who have interest in joining) the InfoCorps have probably little or no military training experience. They will more than likely have no concept of military hierarchy, protocol, or philosophies. Given that this is a provisional concept that takes civilians into this unique military environment, it is essential to review and explore the personnel areas of this proposal.

Organization and accountability

As information serves all services, the Information Corps should be-by definition-a "purple" or joint services organization with separate administrative and operational chains of command. One vision is to create a direct office[4] under the Assistant Secretary of Defense for Command Control Communications and Intelligence (ASD C^3I) for the InfoCorps to report to with a two-star in command, just as the DIA is subordinate to the Joint Staff. Another option is to create a Joint Information Operations Center as a separate Defense Agency. Yet another option is to maintain the status quo of forming InfoCorps units within existing service lines. However, this may only stovepipe innovation, accountability, and responsibility, not to mention hinder information-sharing and operational responsibilities on joint information operations. What would be ideal is to have the InfoCorps units report to CINCCONUS. This new CINC would oversee CONUS security, anti/counter-terrorism, information operations, and domestic NBC defense activities.

The location and dispersal of such reserve units can be handled one of two ways. First, the Pentagon may wish to stand up a fixed number of units in the initial InfoCorps development. Such units would naturally be spread around the country near major technological or academic institutions. Silicon Valley, Seattle, Philadelphia, New York, and Washington, DC would be excellent geographic starting points, with either supporting elements or good relationships at/with major technological institutions like MIT and UCLA. The alternative is to create an InfoCorps Individual Mobilization Agreement (IMA) with individual citizens whose expertise the military requires. Being less formal, IMA agreements are a more decentralized alternative that poses issues regarding training certifications, standardization, currencies, and formal links to the military. Should the InfoCorps concept become reality and grow beyond initial

billets, the original units could serve as intermediate headquarter organizations for subordinate teams in less-dense geographic areas.

In keeping with the structure and success of certain specialized military units, the other units in the InfoCorps should be designed from the ground-up to be a high-performance team. To accomplish this will require a "flat" organizational structure with a minimum of bureaucracy. This pushes both operational activities and unit development (training) down to the unit level rather than centralize in a traditional hierarchical organization. This can be accomplished by careful creation and design of job descriptions and positions and taking full advantage of the advanced communications technologies available today.

The InfoCorps units will be unique entities in the military arena. Understanding this, the traditional military model may be modified to fit this proposal. While weekend drills are the norm for reserve units, the information units would most likely consist of highly skilled programmers, analysts, and technicians who are probably well-compensated by their civilian employers. As such, they may not be receptive to orders requiring them to wear high-and-tight haircuts, face PFT[5] evaluations every quarter, or conduct parade-field drills. They are being called upon to conduct a different kind of operation in a different kind of war, and that requires different military regimentation. While a complete elimination of the military regimen is not practical, modification of existing standards and requirements for this unique organization may be necessary. Some portions of the traditional, well-published military regimen, such as fitness tests, height and weight standards, or age restrictions may be waived or changed for the InfoCorps. The focus on military training should focus on military applications, tactics, planning, and their role in the military organization. Essentially, the military must recognize and draw on the unique characteristics and abilities of the individuals in the InfoCorps and the specialized kind of warfare they will fight alongside their colleagues. Such recognition must be standardized and understood throughout the military, lest the M-16-firing, Nighthawk-flying or surface-ship-driving officer exhibit degradation or look down on their technical counterparts undertaking this unique mission. Changing times and missions require evolution and revolution in both mind and organization.

A military unit is not a military unit without leaders, subordinates, and a well-defined chain of command. To that end, the information units should fall into the traditional military grade structure of leadership positions. The units will also require commanders who understand the unique civil-military relation of the persons in their charge. Initially, leadership may come from existing military officers, however, there must be provisions and procedures for InfoCorps personnel to grow, mature, and eventually take command of such units. Some ideas for leader development include authorizing some qualified InfoCorps officers to attend service war colleges and joint service schools. Inter-unit training or observation programs would further foster relations and familiarization between the "combat" and InfoCorps units.

Of major importance will be the location of unit facilities. In the current military organization, units form at Guard or Reserve armories around the country. This is necessary due to the equipment requirements of platform-based forces such as tank companies or mechanized units. Motor pools, repair depots, arms lockers, and other facilities are needed to house and support many reserve units from front-line armored units to combat water resupply and postal services

units. An InfoCorps unit, would not require such extensive facilities, and could be headquartered in a business or corporate complex anywhere in the country. As long as it is secured (both physically and to meet unit requirements for handling classified material,) can accommodate unit responsibilities, and the requisite telecommunications and information systems the unit requires to meet mission requirements, such InfoCorps units can be stood up anywhere in the world.

As with any high-performance teams, and in the Era of Less Spending and Downsizing, it is wise to remember that: Humans are more important than Hardware; Quality is better than Quantity; and that Competent troops cannot not be mass produced or be created after emergencies occur.

Typical missions

The first military signal organization was established under President Lincoln with civilian telegraphers from the railroad company. Also, in WWII, we called up whole Bell Telephone companies, put them in uniform (under the Laws of War) and sent them into France to repair the telephone systems. As mentioned above, several hundred AT&T technicians deployed overseas to support Operation DESERT STORM. Should the InfoCorps materialize and become reality, some of the missions they could support are listed below. Some of these may be outsourced to foreign nations as a foreign assistance program to facilitate nation-building or serve as foreign military sales, just as our SOF[6] provide services to foreign governments.

- **Information Security**: Providing INFOSEC services to units, both forward- and rear-deployed.
- **Information Warfare**: Assist or conduct offensive information operations in support of posted OPLANS.
- **Red Teaming**: Serve as the Red Cell[7] for military and (when requested) government information systems.
- **Systems Design and Engineering**: Assess, upgrade, and modify existing systems design in both tactical and strategic environments.
- **Programming**: Designing mission-specific applications to support military operations.
- **Technical Assistance and Repair**: Serve as repair personnel for COTS equipment or services in use by the military.
- **Public Affairs**: Assisting units in designing and maintaining web pages for public information.
- **Telecommunications**: Design, develop, and manage telecommunications facilities, networks, and services for the war fighter.

Potential problems

Nothing new ever materializes without first experiencing growing pains. In this basic conceptualization of an Information Corps, several problems come to mind very quickly:

The InfoCorps as proposed above has modified military regimens to accommodate the unique nature and composition of its unit and personnel. This may generate some questions or awkwardness when InfoCorps units interact with traditional military units. Whether this is resolved by the creation of a new service, modifications to existing service uniforms or other techniques, there must be smooth interfaces between personnel in the traditional and non-traditional units.

Another problem not unique to the creation of the InfoCorps is the issue of joint interoperability with technology and information systems. The failed mission at Desert One during Operation EAGLE CLAW[8] in Iran demonstrated this when Army, Navy, Air Force, and Marine units and personnel could not easily communicate among themselves in tactical environments, nor rapidly (or directly) communicate with higher headquarters who (by nature of the OPLAN) had to authorize certain tactical actions during the operation. As a result of that operation, the 1986 Goldwater-Nichols Defense Reorganization Act, recent military history and the alleged Revolution (or Evolution) in Military Affairs[9], the services have been forced to adopt common protocols and communications to enable them to fully operate in a joint military environment. The InfoCorps must function in the same way, both internally (in InfoCorps activities) and in joint activities with other military units.

Information warfare is a hot topic in the military these days. It is even hotter in the intelligence and special access communities where many IW programs are classified "black" or officially non-existent. Many of the information warfare activities-when conducted-will be done so under layers of secrecy and classification. This raises the issue of security clearances and non-disclosure of national security information by members of the InfoCorps who do not formally fall into the "military" mold but work on these programs. Given the organization and structure of the InfoCorps in this paper, such issues will most likely be handled as regular security clearances to reservists or (depending on how the units are created) even DoD contractor personnel. Regardless, it must be made absolutely clear to InfoCorps members as to the sensitive nature of the work that some of them will be engaged in and their responsibilities associated with their work.

While the InfoCorps would be a uniformed-or "card-carrying" DoD component and therefore a military-organization, the Law of War is another issue and must be considered as the role of civilians in a military operation must be analyzed. As Colonel Charles Dunlap, USAF (Ret.), writes in his article *Organizational Change and the New Technologies of War*,

> *AInternational law does, however, recognize that civilian technicians and contractors are necessary for modern militaries. It holds that they are subject to attack only when actually performing tasks in support of the armed forces. Unlike military personnel, they would not ordinarily be targeted when they are away from their jobs. If captured, they are entitled to treatment as prisoners of war. Nonetheless, the law has always held that*

noncombatants' immunity from damage and harm was predicated upon their obligation to abstain from hostile acts. If they took action against a party's armed forces, they automatically lost immunity."

Unfortunately, this scenario appears to be exactly the direction the United States is heading. The operation of high-technology systems designed and supported by civilian corporations requires the transfer or deployment of civilian technicians and contractors from traditional rear-area/ corporate office support functions to what are arguably "hostile" activities in-theater during a conflict. A civilian technician, for example, who helps execute a computerized offensive information operation against an enemy force may well have gone beyond mere support and into the "offensive" role even though he/she is not wearing military uniforms. *Defense News* characterized the significant numbers of civilian technicians required for the Army's digitized battlefield as "surrogate warriors" for the battlefield of the future. Surrogate warriors may indeed be the vision for the InfoCorps. However, the Laws of War must be examined to determine where the civilian expertise ends and military affiliation begins.

Finally, the issues of service retention must be solved. In a traditional reserve component unit, members are required to attend a specified number of UTAs[10] per year, as per the stipulations of the individual services and Title 10.[11] As the InfoCorps is a unique reserve component, the amount of time members must commit-both in unit drill and years of service-must be examined and resolved. Items to consider here include qualified ROTC scholarship recipients who may wish to serve their commitments in the InfoCorps rather than in active-duty units and the creation of incentives to keep qualified InfoCorps members on the rosters.

Regarding the feasibility of retaining competent people in a quasi-military role in the InfoCorps, the military would be wise to examine the success of such military-based organizations as the Coast Guard Auxiliary or the Air Force Auxiliary Civil Air Patrol (CAP).[12] Both organizations are drawn from typical citizens who either possess or are willing to learn specialized training to serve their fellow citizens in exchange for "belonging" to a quality organization with benevolent missions. In the case of the CAP -headquartered at Maxwell AFB, Alabama and whose national structure mirrors the National Guard-its citizen-volunteers conduct over ninety percent of the inland search and rescue function for the Total Air Force at a tenth of the annual cost the Air Force would incur utilizing active component personnel and equipment doing it itself. Further, the success of the CAP in performing its mission[13] in search and rescue, drug interdiction, and related services has been recognized by national leaders at the White House, Congress, and uniformed services.

The CAP model is a good starting point for several reasons. It holds a National Guard-format structure with one "wing" in each state and subordinate units of varying size and mission-oriented skills. Being a component of the Air Force, its members wear slightly-modified Air Force uniforms in their activities. However, to retain personnel who are qualified but do not meet Air Force height-weight standards (and therefore not authorized to wear CAP-USAF uniforms) the CAP provides alternate uniform combinations for its members such as jumpsuits, blazer suit combinations, and civilian aircrew clothing with appropriate identifying insignia. The CAP also has a professional education and development program that encourages members to develop mission-related skills to better serve both the CAP in operational duties and their civilian employers as well. In addition to providing access to and recognition for attending service

colleges like the Air War College or Squadron Officers School, CAP recognizes and awards members for completing civilian training that is of value to CAP's emergency services functional areas such as EMT certification, FAA pilot ratings, or specialized courses such as the FEMA[14] Radiological Monitoring Program or Incident Commander Courses.[15]

The members of CAP are unpaid volunteers who donate their time to emergency services incidents as they occur. Some of these incidents span several days or weeks. Such events in recent history include: Hurricane Andrew disaster relief, search-and-rescue, and federal/military/local government communications support in South Florida in 1992; relief during the California earthquake; assisting and flying search and rescue missions with the Air Force to locate a downed A-10 in Colorado; and other such missions. CAP members provided on-call, round-the-clock support for upwards of two weeks in many missions such as this, and could be viewed as filling a domestic role similar to the National Guard. Again, these are unpaid volunteers who bring their experience, energy, and support to a vital domestic mission. It is also important to note that-with occasional "bumps" in the road-CAP has enjoyed a strong, supportive, stable, and warm relationship with its Air Force counterparts. When exploring potential organizational designs for the InfoCorps, an examination of the CAP model would provide fantastic insight into both organizational and personnel issues for the unique InfoCorps concept.

It is crucial that-while the InfoCorps is a unique military organization-the rules, regulations, and standards of traditional military regimentation should not be waived or completely altered. There are "unspoken standards" such as haircuts, shined shoes, and a certain professional bearing that can define a warrior in or out of uniform. Such standards foster cross-service esprit de corps and are integral to personal identification with the military establishment. Care must be taken to balance the "traditions" and standards of military service while maintaining an organization that is worthy of being considered a "military" organization. Even in the quasi-military organization of CAP mentioned above, its members share an esprit de corps and sense of belonging and contributing to the Total Force in their own, unique way.

Conclusion

The military (and society as a whole) is indeed at a crossroads in time as the clock counts down toward the new millennium and future challenges. The reliance on information and information technology is practically a requirement to conduct business, conduct government functions, and accomplish military operations.

My office is an example. My desktop computer, the Pentium laptop, encryption software, PCMCIA, television card, Global Positioning Service receiver, high-end laser printer, digital camera, scanner, television with picture-in-picture, three phone lines, and digital cellular phone are now essential tools to be productive around the world. The ease of acquiring this technology and my ability as a regular citizen to perform serious and secure information exchange and processing around the world is a capability that-fifteen years ago-was limited to classified military lockers around the world.

The very fact that I have this technology available to me at an arms' length probably scares people... as would the fact that I have T-Shirts from global hacker organizations, a sizable collection of "hacker" material in my library, and think that government key escrow is a laughable concept even though I understand and empathize with the concerns of law enforcement agencies. Some could say that my office is a poor man's intelligence center. Others could claim this is an Information Warrior's lair. Still others could argue that this is the office of the future. In my opinion, my office is all three. One could note that this office may be part of an InfoCorps unit headquarters. As my company operates within the confines (if there are any) of the Virtual Office, it is safe to say that wherever my laptop and digital phone meet-anywhere in the world-my organization has a branch office and therefore a global presence.

This previously unheard of power and capability in the hands of a private business or individual citizen causes great pause in the minds of our policy makers, often with good reason. As mentioned above, this capability was available only to the military back in the mid 1980s. This is a fountain of untapped value to the military, which would be wise to incorporate into its force structure for the future.

I am neither a special case nor alone in having this technology in my office or home. Further, I have no reservations whatsoever about volunteering some of my time, equipment, or experience to supporting an InfoCorps unit or mission. I am confident that there are others-who concur with this proposal-who have the experience, capability, training, and would eagerly jump at the opportunity to serve as this country's first organized citizen-volunteer, citizen-soldier Information Warriors as we move into the next century and face the information threats of tomorrow.

Endnotes

1 Military Occupational Speciality, the Army's skill identifier. In the Air Force, it is an Air Force Skills [specialty] Code (AFSC).

2 PSYchological OperationS, winning the "hearts and minds" of foreign populations.

3 Currently one Air Force Special Operations Wing flying the EC-130 COMMANDO SOLO II aircraft to satisfy military and diplomatic taskings. The 193rd Special Operations Wing in Harrisburg, Pennsylvania is the only source of such capabilities in the US military inventory.

4 As of this writing, the DOD has announced plans to stand up an Information Operations (Offense and Defense) Center for the ASD C3I.

5 Personal Fitness Test, the joy of every Infantryman!

6 Special Operations Forces, the best of the best of our military machine.True role models.

7 Red Cell is the term used in the early 1980s for the Naval Security Coordinating Team. Composed of SEAL Team Six members, this small unit probed and tested security at U.S. naval and diplomatic installation worldwide to simulate how a terrorist could infiltrate and attack U.S. facilities. The unit them provided formal assessments and guidance to commanders on how to strengthen installation security.

8 The catastrophic mission to rescue American hostages in Iran in 1980.

9 Some call this a "Revolution" in Military Affairs while others consider it an "Evolution." My opinion is that the "revolution" is the information warfare operations being planned that wage war in the ether of cyberspace. The "evolution" is the use of information technology to support the warfighter-- such as the Army Force XXI Digital Soldier, or the wonderful multi-discipline intelligence fusion products used to support the commander's decision-making process.

10 Unit Training Assemblies. A period of time for reservists to drill. A typical weekend administrative drill may include 4 UTAs or 16 hours of recorded "credit" for drill.

11 Section of the United States Code that specifies the responsibilities and various legal regulations for the Department of Defense.

12 National Headquarters is at http://www.cap.af.mil/

13 CAP's three fundamental missions are emergency services, aerospace education, and cadet programs. The CAP activities mentioned in this paper fall under the category of emergency services.

14 Federal Emergency Management Agency.