The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

THE JOINT RESERVE COMPONENT VIRTUAL INFORMATION OPERATIONS ORGANIZATION (JRVIO); CYBER WARRIORS JUST A CLICK AWAY

BY

PETER S. DUKLIS, JR.
Department of the Army

USAWC CLASS OF 2002

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

20020806 342

USAWC STRATEGY RESEARCH PROJECT

The Joint Reserve Component Virtual Information Operations Organization (JRVIO); Cyber Warriors Just a Click Away

by

Peter S. Duklis, Jr.
DLAMP

COL Richard K. Jones
Project Advisor

The views expressed in this academic research paper are those of the author and do not necessarily reflect the official policy or position of the U.S. Government, the Department of Defense, or any of its agencies.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Peter S, Duklis, Jr.

TITLE: The Joint Reserve Component Virtual Information Operations Organization
(JRVIO); Cyber Warriors Just a Click Away

FORMAT: Strategy Research Project

DATE: 09 April 2002   PAGES: 31   CLASSIFICATION: Unclassified

Informational power has now been coined as a national power along with
political, economic and military powers. Moreover, Information Operations (IO) is
a key stratagem to protect and facilitate our national interests across the full
spectrum of engagement. The Depart of Defense (DoD) incorporates information
operations as part of all of its current plans, operations and exercises. Yet, there
are very few organizations dedicated solely to IO. However, DoD conducted the
Reserve Component Employment 2000-2005 (RCE-05) Study in which it was
directed that a Joint Reserve Component Virtual Information Operations
Organization (JRVIO) be established to support joint and inter-agency
organizations. In this paper, I will determine what virtual means, how it will be
used for IO, and how a joint reserve unit is structured and functions.
Furthermore, I will make a recommendation on how and where this/these
JRVIO(s) should be utilized to support overall DoD Information Operations and
specifically, Joint Commands and inter-agency organizations.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

THE JOINT RESERVE COMPONENT VIRTUAL INFORMATION OPERATIONS ORGANIZATION (JRVIO); CYBER WARRIORS JUST A CLICK AWAY

> Know the enemy, know yourself; your victory will never be endangered. Know the ground, know the weather; your victory will then be total.
>
> Sun Tzu

As we enter into the new millennium, the enemy, ground and even the weather is not always known to us. The enemies of the United States have gone from mechanized juggernauts and nuclear powers to unfamiliar ones and independent actors / terrorists. The ground went from 3 dimensions with real properties to now a new dimension Cyber Space with introduction of the computer age. To reach the "total victory" articulated by Sun Tzu, the U.S., according to Joint Vision 2020, requires full spectrum dominance.

Information, knowledge and influence present our nation with perhaps its most perplexing challenges in this new century. Part of this challenge is how and when to weld this new element of national power and achieve information superiority, a key enabler, in all battle spaces to attain full spectrum dominance.

The Department of Defense (DoD) views information operations and information assurance as strategic tools/objectives to attain information superiority. Furthermore, DoD deems the arena where information warfare will be fought as the "virtual ground" of cyber space. But who will be these Cyber Warriors? They will be a combination of Active Component (AC) and Reserve Component (RC) forces.

The Armed Forces sees the line between the AC/RC forces fading and becoming non-existent as the military continuously relies more and more on its reserve and national guard forces. This phenomenon is readily apparent in the Reserve Component Employment Study 2005 (RCE-05), which outlines the Joint Reserve Component Virtual Information Operations Organization (JRVIO)[1]. The study directed that develop and implement JRVIOs to support government agencies in information warfare.

One may ask, what is a joint reserve unit or what is a virtual organization, let alone a combination of the two to form a JRVIO? This paper will address these issues, how they apply to information operations and make a recommendation on how and where this/these JRVIO(s) should be utilized to support overall DoD Information Operations.

BACKGROUND

WHY INFORMATION OPERATIONS?

Attacks on Defense computer systems are a serious and growing threat. The exact number of attacks cannot be readily determined because only a small portion are actually detected and reported. However, Defense Information Systems Agency (DISA) data implies that Defense may have experienced as many as 250,000 attacks last year. DISA information also shows that attacks are successful 65 percent of the time, and that the number of attacks is doubling each year, as Internet use increases along with the sophistication of "hackers" and their tools.[2] A Time Magazine article tells us that,

> Hackers may be the new mercenaries, available to the highest bidder. During the Gulf War, according to Pentagon officials, a group of Dutch hackers offered to disrupt the U.S. military's deployment to the Middle East for $1 million. Saddam Hussein spurned the offer. The potential for disruption was great, says Steve Kent, a private computer-security expert in Cambridge, Massachusetts, and a member of a Pentagon advisory panel on defensive information warfare. "In the Gulf War the military made extensive use of the Internet for its communications, and it would have suffered had the Iraqis decided to take it out."[3]

This type of information asymmetric warfare will continue to perpetuate as the gulf between U.S. military powers widens against the rest of the world. Additionally, it is a method used by terrorists and independent non- state actors and could be the next wave of follow-on attacks after 11 September 2001. Many nations see U.S. information systems (both military and commercial) as the only area vulnerable to attack or where an opponent maybe on par with the U.S. Based on belligerents' capabilities and the inherent need for communications to support U.S. military and governmental operations and conduct everyday activities of its citizens and global partners, information operations have become a key enabler of all contingency planning and operations. Information operations encompass actions to protect our information and information systems and attack our adversary's information and information systems.[4] Whereas, Information Warfare is information operations conducted during time of crisis or conflict to achieve specific objectives over a specific adversary or adversaries.[5]

The joint force must be able to take advantage of superior information, converted to superior knowledge, to achieve decision superiority – better decisions arrived at and implemented faster than an opponent can react; or in a non-combat situation, at a tempo that allows the force to shape the situation or react to changes and accomplish its mission. Developing the capability to conduct successful operations in the information domain requires

an innovative, flexible organization that can keep pace with the constant evolution of the information environment. Structuring the Reserve Component to support and, in some cases, lead this effort is critical to the achievement of information superiority.

WHAT IS THE JRVIO INITIATIVE?

One of these alternative concepts of employment of Reserve Component armed services was in support of information operations for various governmental agencies. This is based on our adversaries and independent actors information warfare capabilities, the commercial availability and technological advances in information operations, and the U.S.'s own capacity to wage information warfare.

In the Reserve Component Employment 2005 (RCE-05) study the Secretary of Defense directed the Assistant Secretary of Defense for Reserve Affairs and the Joint Staff, J-1, J-3, and J-6 to explore the establishment of a Joint Reserve Virtual Information Operations (JRVIO) Organization. The final report focused on integrating the capabilities inherent in the military and civilian acquired skills of RC personnel for use in virtual Information Operations for DoD and Joint mission support. The RCE-05 tasking also required an interim report as a long-range plan for a JRVIO organization, a proof of concept test to assess the validity of a virtually integrated RC IO and IA organization, and submission of this final report to the Deputy Secretary of Defense for approval. The final report was approved on October 13, 2000 and recommends the activation of five JRVIOs. The five JRVIOs will provide RC support to Defense Information Systems Agency (DISA), National Security Agency (NSA), United States Space Command (USSPACECOM), Joint Information Operation Center (JIOC), Joint Task Force for Computer Network Defense (JTF-CND) and Information Operations Technology Center (IOTC). The report includes resourcing initiatives, initial Concepts of Operations and a phased implementation approach, as well as technology issues[6]. The incremental phasing is over a seven-year period (Fiscal Years 01-07) commencing with 122 reservists and culminating with 633 authorized positions.

The operational concept behind the establishment of JRVIOs is to provide Reserve Component elements that can support different United States agencies' ongoing information operations missions. The idea is that RC members can bring their civilian acquired information operations skills to bear from different geographic areas in a virtual environment. This would reduce the overall cost and AC infrastructure demands for information operations. The ensuing JRVIO report looked at a myriad of issues and concepts from funding, equipment, military specialty codes, technology, force structure and missions. All of these are factors that are being

researched to determine the viability and functional ability of JRVIOs. Foremost in this exploration is the premise that joint reserve units can adequately support the information operations when not organically located with its supported unit, let alone, virtually.

A VIRTUAL ORGANIZATION?

What is a virtual organization or team? A virtual organization doesn't have an agreed upon meaning in any discipline and in some it cannot exist, according to the research for this study. However, one must determine, can a virtual organization exist, and if it can what is its definition. This is paramount to research and design of JRVIOs.

Lipnack and Stamps in their book, Virtual Teams: People Working Across Boundaries with Technology, provide a tangible definition of virtual organization. It is, "a virtual team is a group of people who work interdependently with a shared purpose across space, time and organization boundaries using technology."[7] This clearly denotes an institution, which is organized and has focus. However, the Final Report – Reserve Component Employment Study 2005 (RCE-05) amplifies Lipnack and Stamps in its "working" definition of a virtual organization as,

> "A virtual organization as a distributed organization that can meet mission requirements without a static spatial frame of reference. The absolute and relative locations of the people, regardless of job function, do not impact the ability of the organization to function, provide transparent and responsive support, and accomplish its mission. Technology is used to overcome geographic dispersion, provide management oversight and enhance situational awareness."[8]

These definitions are all interesting but do they work for the JRVIO. The JRVIO study definition is good, but the Lipnack and Stamp definition better describes the JRVIO concept of operations. It adds the terms across time and organizational boundaries. Members of JRVIOs that will work at different times and in different time zones, and will be crossing numerous organizations to integrate functions, plans and activities to gain, protect and even exploit information in support of their agency and their Unified Command Plans. Therefore, a modification of the definition of virtual organization, as it pertains to JRVIOs, should be made to encompass across time and organizational borders. The recommended definition is: a virtual organization is an organization that can accomplish mission requirements without a static spatial frame of reference across time and organizational boundaries using technology enhancements and innovative techniques to overcome geographic dispersion, provide management oversight,

and enhance situational awareness. This new meaning better fits with the overall operational concepts outlined in the study.

Why is a workable and accepted definition important? It is important because it is the base from which the feasibility, functional, structural and mission determination analysis can be conducted. It is the foundation to build the organization. Now that a workable definition has been worked out, the follow on research needs to resolve the following questions: can, and if so, how will JRVIOs function in a virtual environment; what factors and issues must be overcome; and what technological systems must be allocated to join these cyber warriors?

MAKING A VIRTUAL ORGANIZATION CONCRETE

Virtual organizations have evolved as a means to unite and focus different members of the team who are separated geographically, physically, and in different times zones to execute projects successfully, and become more efficient and fiscally prudent by leveraging technology enhancements and innovative methods. Currently, many commercial firms in a variety of economic disciplines are experimenting and using virtual teams. The benefits for virtual teaming vary from company to company. But there are some basic benefits for establishing a virtual organization. Some of these are; people can work any place and at anytime; employees are recruited for their abilities and not location; physical handicaps are not a problem; and expenses associated with travel, lodging, parking, and leasing or owning real property can be reduced or eliminated.[9]

Virtual teams, although a relatively new initiative, have been studied over the past seven years. However, the shortcomings of this research are that most virtual organizations are stood-up for specific projects and for short durations (weeks, months or a year). Therefore, the long-term effects, as they would pertain to a JRVIO, will be extrapolated for this paper. This research, military dynamics and analysis will be applied to formulate the feasibility and functional ability of JRVIOs. In particular, this study will examine cultural, technological concepts, emotional/team dynamics, and linkage factors that impact on JRVIOs and make recommendations to overcome these challenges or sustain these qualities.

CULTURE AND ORGANIZATIONAL DYNAMICS

For most people joining a virtual organization is a not only an organizational change but a cultural one involving new interpersonal relationships, new means of communication, and an alternate work ethic and climate. The development of a new organization triggers its own cultural dynamic based on the change anxiety that accompanies it. These are adjustments or

5

conversions in values, norms, expectations, vision and practices.[10] However, moving towards virtual organization expands these already inherent cultural shifts due to change.

The major cultural shift in virtual organizations is the absence of physical contact with the members. The lack of face-to-face interaction causes a cultural shift in communication skills, leadership, and trust. To communicate with team members in an only text based manner, is often considered cold and is devoid of emotion or inflection. This may cause difficulties in deriving the meaning or sentiments that are being expressed, and they can be easily misconstrued. Leadership styles and techniques are similarly constrained over the net. A leader's job is less on keeping accountability of personnel and more on influencing personnel to be productive, communicate and report on a regular basis. The leader still must provide vision, develop trust, prioritize work, establish norms and rules, reward success, and discipline shortcomings. The virtual leaders main duty is to proactively manage factors of group dynamics, misconstrued communication and instilling trust in them and of all members of the group.

Probably the biggest cultural change and obstacle to overcome is trust. The cultural dynamic of a virtual team has three factors that undermine or impede trust: (1) no common past or future, (2) culturally diverse and geographically dispersed, and (3) electronically communicating. The traditional conceptualization of trust assumes that trust resides in personal relationships and past or future memberships in common social networks that define the shared norms of obligation and responsibility. The lack of past and future association decreases the potential existence of trust. The diversity in cultural and geographic backgrounds should similarly challenge the potential existence of trust. Finally, there are the arguments that trust needs physical touch, which the current technological context also eliminated.[11]

The ability to trust and cultural differences will be compounded in virtual organizations based on specific parent organizational cultures, generational differences (based on experiences in technology and computers, and how technology has integrated in to our daily lives), and informal trust networks that develop. These will be evident in JRVIOs for the reasons stated above but may be amplified due to the rigidity of service regulations, traditions and norms. Inter-service and intra-service rivalries, and a hierarchical institution breed informal trust networks in the Armed Services that may undermine a cohesive organization.

OVERCOMING CULTURAL CHANGE

Overcoming cultural change in any virtual organization will not be uncomplicated, however, it should not be insurmountable. Let's deal with some recommendations.

6

Communication:

- When using text-only messages develop guidelines to let your teammates know your intent. One method is emoticons.[12]
- Define specific times when the team members will communicate. Moreover, establish a norm that when communicated the response should be within a defined time period.
- Use all methods of cyber communication, e-mail, chat rooms, websites, etc.
- Use the telephone, fax, teleconferences and Video teleconferencing (VTC) occasionally to provide other dimensions to your relationships.
- And probably, most importantly, include face-to-face time if possible. This will provide a better understanding of each other, which will help communication and trust.

Leadership:

- Establish norms and guidelines up front and enforce them.
- Provide vision and guidance to the organization and each team member.
- Provide the organization and individuals with periodic updates on performance.
- Keep the organization focused based on your goals and vision.
- Remember to reward and recognize your people.

Trust:

- State upfront why trust is important, what the pitfalls are with trust in a virtual organization and how a virtual organization can overcome these pitfalls.
- Make that first meeting or contact face-to-face if possible, if not use a VTC.
- Rotate leaders from time to time, as a reward for good work.
- Engage in-group activities, even if it is webbed based.
- Attempt to defuse the biases of informal networks by effectively building a team.

TECHNOLOGY, THE GLUE OF A VIRTUAL ORGANIZATION

Advanced technology is rapidly becoming available to support people on an anytime, anywhere basis, and at an affordable cost. Products range from the simple telephone and fax machine to multimedia capable workstations and collaborative software. Virtual organizations are required to use this plethora of communication and network technologies.

Virtual teams are supported by both hardware and software. General hardware requirements include telephones, PCs, modems or equivalent, and communication links such as

the public switched network (telephone system) and local area networks. Software requirements include groupware products such as electronic mail, meeting facilitation software, and group time management systems.[13]

This technology is what enables virtual organizations to become a reality. Without the technical advances cited above the concept, feasibility and functionality of organizations could and would not exist. In the civilian sectors this use, upgrades and collaboration software and tools are readily available and can be used with ease. However, DoD has restrictions on what hardware and software can be used. These limitations are based on security and fiscal policies.

RECOMMENDATIONS FOR JRVIO TECHNOLOGICAL SYSTEMS

The main hypothesis supporting the formation of JRVIOs is their flexibility and independence. These must remain paramount in the creation of technology support systems. With this in mind, the following are recommendations for the technology sustainment:

- A standard collaboration workspace system or systems must be established for the JRVIO and the supported agencies, as well as, between the JRVIOs to interconnect all parties. This will maximize the RC worth to their AC partners and incorporate cross training and interoperability.

- All system connectivity requirements must be addressed and resolved prior to any establishment of JRVIOs.

- Access for secure connections to DoD systems (classified and unclassified). These should be at a fixed installation and provide the ability for remote access. The remote access is required for non-standard and/or compartmentalized information operations.

- There should be established intranets and JRVIO websites within the confines of existing DoD systems. This will facilitate easy access to shared information and can provide a media for communications (chat rooms, videos, etc.). It provides close loop nets, which allows members to link-up virtually for planning, training, exercises, meetings, etc.

- Members of JRVIOs should be issued state of the art laptop computers with removable hard drives (classified and unclassified) for ease of use and transportability. This will facilitate the use of the computer for classified and unclassified work, and force protection procedures.

JRVIO FORCE STRUCTURE

Reserve forces have been an integral part of the United States Armed Force's structure for over 226 years. They have been called up to serve in all our country's wars, peace actions and small-scale contingencies. The Department of Defense includes over 1.28 million ready and stand-by reserve forces. These forces and their active component counter parts are deployed or stationed in over 110 countries in the world. In fact, there are over 50,000 mobilized Guard and Reserve affiliates serving to accomplish operational missions since 11 September 2001.[14] Since 1776, these citizen soldiers, sailors, airmen, and marines forming service specific units have been and are a key element in the nation's National Security Strategy. However, the concept of developing Joint Reserve Units (JRU) is a relatively new concept, which has only been around for the past 10 years. The commander in chief, US Transportation Command (TRANSCOM), formed a joint transportation Reserve unit to meet strategic mobility requirements in the face of dwindling assets in 1991.[15] Therefore, the models for constructing the Joint Reserve Virtual Information Operations Organization are out there.

Besides the TRANSCOM unit, there are two other units that can be used as models. They are the Joint Reserve Unit, which supports the Joint Forces Command (JFCOM) in Norfolk, VA and the Joint Reserve Intelligence Centers (JRICs). The JFCOM JRU is made up of 600+ joint billets, including all service components and the Virginia Army and Air National Guard. The JFCOM JRU provides staff augmentation and support to the JFCOM staff. There are 28 JRICs in CONUS, which support Unified Commands and other DoD agencies. Their mission is to provide intelligence support for their supported organization's peacetime and wartime missions.

Although these examples provide a precedent for Joint Reserve Units, they are not connected together exclusively by communication technology, like the JRVIO concept dictates. Moreover, these units physically train, work and drill together as units. Their administrative needs are taken care of on site with support personnel. So how do we structure, field, locate and resource a JRVIO?

CURRENT PROTOTYPE

The JRVIO Final Report, 13 October 2000 recommends five JRVIOs to provide RC support to DISA, NSA, USSPACECOM - JIOC and JTF-CND, and IOTC. Figure 1 depicts the organizational chart.
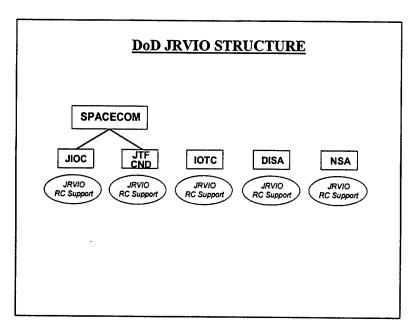
FIGURE 1[16]

As depicted, the JRVIOs are an element of each of the supported organizations. But why were only these five agencies selected for JRVIO support?

Initially, DISA, JIOC, JTF-CND, NSA, IOTC, and the Unified Commands were identified in the JRVIO study as the major joint organizations with information operations responsibilities whose capabilities can be enhanced by JRVIOs. All of these entities, with the exception of the Unified Commands, embraced the JRVIO concept. The CINCs were not convinced that information operations support could be provided virtually. The Unified Command Information Operations staff officers polled at the World-Wide Information Operations Conference felt that perhaps intelligence support could be accomplished virtually but not information operations.

The geographic CINCs are more interested in on-site support than virtual support for crisis action and deliberate planning. They largely discounted the ability of the RC to provide them with virtual information operations planning support as they considered it unworkable and generally too difficult to manage.[17] Based on all the CINCs' desires, the Unified Commands were not recommended in the JRVIO study to be fielded JRVIOs at this time pending further research.

HOW DO JRVIOS FUNCTION?

The paradigm for the JRVIO denotes that the organizations will be an element in the supported agency. Moreover, the personnel serving in the JRVIOs would be billeted against positions in the supported organizations' Joint Table of Manpower Distribution (JTMD).[18]

10

Although the JRVIOs will be embedded in the organizational structure to enhance their parent organization's mission, they will be dispersed geographically and supporting at different times. Operationally this thesis is feasible given the proper technological advances previously stated. But how will they function in the all-important world of administration? Who will support them?

The current plan is for the parent or supported agency to provide all the administrative, operations and training support for their JRVIO and its members from four separate services with its unique regulations. Command and control (C2) will be exercised as in any existing Reserve Component chain of command. The supported organization will assign missions to the supporting organization for their primary peacetime missions. The JRVIOs will rely on dedicated Fulltime Support (FTS) personnel resident at the supported organization in the RC support element. These FTS personnel along with parent RC Commanders will provide administrative support and operational coordination in accordance with Service unique procedures and pre-existing arrangements. Administrative control will be exercised through approved Service channels and in accordance with established Service procedures. Mission and administrative guidance will flow from the various staff elements designated by the supported organizations for JRVIO support to the virtual organization. In terms of administrative guidance, the full time personnel supporting the JRVIO at each organization will provide administrative support, managerial direction and operational focus. The parent Reserve Component will provide administrative support for Service specific matters. Some training for JRVIO members may be required on-site. However, under routine operational conditions, the normal mode of operation for the JRVIOs will be to accomplish required training, administration and assigned missions, tasks and activities virtually.[19]

In this scheme the administrative burden is placed on the supported organization and its organic RC fulltime support. This fulltime support mission is there to aid the entire organization not just the JRVIO. The issues that arise from this design are the possibility that the JRVIO will be disenfranchised or will overburden the staff due to significant complications of a virtual structure. The major complications are: skill identifiers, accession and retention, career progression, personnel security requirements, training and interoperability.

The JRVIOs are centrally controlled by their parent agency but execute in a completely decentralized manner. Which is very different from a standard ready reserve unit. Whereby, the members assemble each month and two weeks out of the year for training, operations and administration. A JRVIO will assemble virtually in a team room to work through issues, but mainly each member will work independently on a flexible drill schedule.

Each of the services has established guidelines and regulations that govern procedures that can incorporate a flexible drilling or flexible Inactive Duty Training (IDT) policy. Although it is not identified as flexible drilling, the Army has Rescheduled Training (RST). The Air Force, Navy and the Marines have similar policies.[20] These policies provide a method for reserve members to drill independently and for the unit to track their contribution to a project or training event. The unit member simply develops a command approved work plan for their IDT. Once the work plan has been executed, the reservist submits the hours and type of projects/work completed on a service specific form (e.g. DA Form 1380), along with the actual product to the appropriate authority for confirmation, to the unit administrator for pay and retirement points. However, this technique does not accommodate collective training or mandatory training that is hands-on or physical. This will be a challenge for JRVIOs or any virtual organization.

Additionally, career progression and retention are a concern in these units. Being virtual, and in a unit that may include only 50 positions, promotions and career progression is constrained. To attract and retain these highly qualified professionals, JRVIOs must be structured to provide upward mobility, career qualifying jobs and opportunities for career schooling. The current proposed structure states that this is a concern but does not provide solutions or alternatives.

WHO WILL BE THESE CYBER WARRIORS AND WHAT DO THEY NEED?

The military is constantly at odds with training and retaining qualified computer network operations and information technology (CNO/IT) specialists. Normally, these specialists are constantly at training trying to keep up with emerging technologies and information operations strategies, which remove them from the unit operations. Once trained, they are drawn to higher paying jobs in the private sector. This phenomenon is one of the main premises for forming JRVIOs - to tap into the civilian sector for CNO/IT specialists to staff the JRVIOs.

This concept is quite ingenious when you look at it in depth. The government can recruit from a pool of civilian experts that have already been trained by the government or the civilian sector at a relatively low cost (AC vs. RC expenses), and for specific durations as opposed to fulltime. The reservist is content because he or she can keep the lucrative civilian job and still serve their country. And, in a virtual organization, remain where they reside with minimal travel and time away from work or home. Furthermore, this community of professionals understands, is accustomed to, and can operate in a virtual environment. These ideas do not just lend themselves to computer technology but as cited by the JRVIO study, to advertising and journalism as well.

"It is quite possible that IO functions concerning Psychological Operations (PSYOP) could quite skillfully and appropriately be met by Reservists who have highly sought-after civilian employment skills developed from working at advertising agencies, TV and radio broadcast stations, and magazines and newspapers... With the appropriate level bandwidth, products created virtually in the audio-visual realm could easily be transmitted worldwide in foreign languages translated by skilled virtual linguists. A special technical operations (STO) organization could also be value-added via appropriate reachback connectivity."[21]

Besides these civilian skills, which can be converted into military specialty codes[22], new cyber warriors need to obtain required security clearances to work DoD information warfare and exploit the classified communications systems required to interconnect a virtual organization.

WILL IT WORK – TESTING AND RED TEAMING?

Once these teams have been established they will need to be tested and trained. One of the areas that the JRVIO study did not address was that of testing the systems that they will be using and the units themselves. The units must be evaluated from the perspective of the enemy and under as realistic conditions as possible. Therefore a "Red Team" or aggressor team must be developed to help test and train the JRVIOs.

This concept bears great merit since the JRVIOs and the Red Team can "fight" using real information operations techniques and strategies, since there are no real casualties and that many of the proposed systems and technologies are commercial based or have commercial based applications. Furthermore, who better to compose the Red Team then the same pool of cyber warriors from which the JRVIOs are drawn. For this reason the Red Team should be part of the JRVIO structure with the addition of intelligence personnel. The Red Team proposal would force the JRVIOs to train and operate at information parity and not information superiority, which will make the exercise more realistic. In addition to intelligence personnel, the Red Team ought to have support from the Joint Interoperability Test Center (JITC) to assist in the evaluation and testing of the JRVIO communications and computer systems. Moreover, in the next 2-3 years there will need to be the development and implementation of a Joint Virtual Training Center to provide the same support and training as the NTC, JRTC and CMTC do now.

RECOMMENDATIONS

FORCE STRUCTURE

The JRVIO proposed structure does not provide the best operational support to the supported organization, and the parent organization will not be able to adequately look after its administrative and training requirements. Therefore, based on the analysis and research from this project, the structure in Figure 2 is recommended.

JRVIO RECOMMENDED STRUCTURE

USSPACECOM

JRVIO **

| JIOC TEAM | JTF CND TEAM | IOTC TEAM | DISA TEAM | NSA TEAM | RED TEAM | CSUP CSUP CSUP CSUP CSUP CSUP CSUP |

JIOC ** JTF CND ** IOTC ** DISA ** NSA ** CSUP *
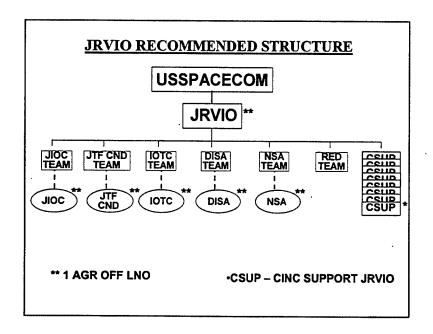
** 1 AGR OFF LNO   •CSUP – CINC SUPPORT JRVIO

FIGURE 2

This structure designs a JRVIO headquarters element under USSPACECOM, the unified command responsible for information operations. Additionally, this headquarters will provide administrative and training support to the operational control (OPCON) JRVIO Support Teams to their five supported organizations. It establishes a Red Team to exercise and test all the support JRVIOs and it recommends CINC Support JRVIOs. The CINCs did not see JRVIOs as relevant. However, if you modify the concept to on site personnel with virtual reach back to the JRVIO, HQ and between teams, JRVIOs can be relevant to the CINCs. This plan gives the CINCs a viable on site information operations support element from local reserve personnel and reachback to all other JRVIOs. The billets for these organizations are provided by the supported agencies and from USSPACECOM to stand-up the headquarters. Additionally, it is

virtual room or website that can be monitored by the headquarters for evaluation and performance confirmation. In this structure the JRVIOs can cross train and provide mutual support.[23] Additionally, each JRVIO reservist is required to attend at least 3 days of annual training (AT) with all the organization's members at the supported agency to provide a venue for physical and social interaction, which will help build the team, develop trust, reinforce norms, and develop organizational and operational best practices.

C2 and training can be facilitated if you recruit from the pools previously suggested. The recruitment would create hubs or nodes of personnel in these target areas. This is key where locals can support different agencies and other JRVIO teams, and can physically come together to support each other and for training. Moreover, in most cases they can work physically with the supported unit. This is the concept for the CINC support teams. These teams would be recruited primarily from the civilian and contractor workforce in the Unified Command or surrounding area. An additional operational advantage to the hub system is dispersion of the forces, which facilitates the defense hubs for geographic areas, force protection and multiple offensive platforms to project information warfare.

TRAINING

Most of the information operations training for the JRVIOs will be completed or conducted through their civilian jobs and professional programs. Any individual augmentation and specific training on unique or specialized hardware and software will be done through web-based education sites. If this is not possible, attendance to classes will be the answer.

Military and collective unit training again will be conducted primarily through the web or through another communication medias. The advantage to this method is reduced cost and realistic application of the operational environment the JRVIOs would be functioning in for missions. Training that requires physical action or a hands on approach, can be accomplished during AT deployments, with a local military organization and through mobile training teams from the supported organizations, the JRVIO headquarters and/or USSPACECOM.

ACCESSION, CAREER PROGRESSION AND RETENTION

DoD will be required to develop "out of the box" concepts to recruit and retain cyber warriors. One battle that has been partially won is monetary compensation. This is supplied through their civilian employment. What other approaches can be engineered to make JRVIOs appealing?

- Certification and accreditation of civilian acquired skills must be approved by the reservist's parent service. These accreditations are then used to award military

occupational specialty (MOS) for CNO/IT. There are precedents and procedures in place to facilitate the awarding of MOSs based on civilian acquired skills. For example, The Army's DA PAM 611-21 (March 1999) outlines established criteria for awarding certain MOSs based on civilian acquired skills. The procedures for conversion and established criteria are in place. Now, it just has to be done for information operations for all services.

- DoD creates a generic CNO/IT MOS (service immaterial) with additional skill identifiers (ASIs) for information offense operations and defense operations. This serves two purposes. One, the MOS can be awarded based on civilian required skills and/or formal military training. Two, it widens the pool of candidates for the positions by making it service immaterial and any information skill person can fill the billet regardless of service.

- Cyber warriors ought to be compensated for their unique skills and training, similar to language proficiency and hazardous duty, and bonuses awarded for enlistment and reenlistment into JRVIOs. Moreover, other incentives or perks can be given to JRVIO members such as, full commissary privileges, worldwide space available travel, an individually selected school per year, in addition to their AT, and others.

- Structure the JTMD to have NCOs' and officers' positions with banded ranks. The bands could be E5-E7, E8-E9, O2-O4, and O5-O6 or any combination that makes sense. This provides for upward mobility and retention in the units. Once a service member is qualified and selected for promotion, he or she can be promoted in the same unit and even the same job. In this way, the soldier is not promoted out of the unit and is retained. Obviously, the command structure and specific positions will need to be developed on leadership, technical skills and other criteria for all the organizations.

A possible hierarchical structure may be a brigadier general (O7) as the JRVIO Headquarters commander with a general staff and each subordinate JRVIO commanded by a colonel or captain (O6). Each commander is authorized a senior NCO (E9). The subordinated JRVIOs could be structured into teams of varies sizes and functions. This then would present an internal structure for career progression.

SUMMARY AND CONCLUSIONS

Information warfare is another tool for our National Military Strategy and across all dimensions of the actual and perceived battle space and civilian sectors. With computer codes the worldwide web, wireless communications, and computer hubs crisscrossing the earth and

infiltrating most of our daily lives, and with the commercial proliferation and availability of these emerging technologies, new and innovative warriors and organizations must emerge to meet any and all information operations challenges. As this study indicated, these warriors will come together across the electrons to strike our enemies and defend our cyber shores virtually. Once thought a novel idea, it is now on the verge of becoming a reality, a combat multiplier and, in a fiscally and resourced constrained world, a necessity.

If one desires a new and improved concept then you must make changes to facilitate it. Many readers will say you can't do that or this because it's against the regulations or it's never been done before. But, if you believe in an idea and push it, it can happen. People said we would not have an integrated military or women in combat, and we have them. And those initiatives were cultural, social and not just administrative or regulation changes. All of these recommendations and initiatives are administrative that each service or DoD can implement overnight. JRVIOs can be a reality if DoD implements the recommendations and "out of the box" ideas outlined in this paper. But will DoD take that "leap of faith?"

WORD COUNT = 6,440

ENDNOTES

[1] In April 1998, the secretary of Defense (SECDEF) issued the *Fiscal Years 2000-2005 Defense Planning Guidance (DPG)*, which mandated that DOD conduct a study examining RC employment in support of the defense strategy across the full range of employment options including homeland defense, smaller-scale contingencies (SSC), and major theater wars (MTW). The DPG directed that the study:

- Consider alternative concepts for employing Reserve Component forces in the future.

- Review the full range of combat and support Reserve Component roles in current operational plans and assess currently planned employment.

- Identify and assess potential Reserve Component missions in the continental United States (CONUS) and outside CONUS in peacetime and across the full spectrum of conflict, including the reserve component's role in the strategic reserve.

- Develop and assess alternative employment roles and force-mix concepts, including an evaluation of costs, benefits and risks for each option.

- Assess Reserve Component resourcing for current and recommended requirements. Overall, the study examined how to access and use Reserve Component forces more readily and what it would take to fund, field and equip these forces. The study determined that there should be 20 follow-on RCE-05 studies, reviews and other assessments to provide a more complete review of the reserve component integration concepts. In July 1999, the Secretary of Defense approved the recommendations and directed further studies. One of these selected for further study was the Joint Reserve Component Virtual Information Operations Organization.

[2] General Accounting Office, <u>Information Security: Computer Attacks at Department of Defense Pose Increasing Risks</u> (Washington, D.C.: U.s. General Accounting Office, May 1996), 3.

[3] Douglas Waller Washington, "Onward Cyber Soldiers," <u>Time Magazine</u>, 21 August 1995, 5.

[4] Department of Defense, <u>Joint Doctrine for Information Operations</u>, Joint Publication 3-13, (Washington, D.C.: U.S. Department of Defense, 9 October 1998), pg GL-7

[5] Department of Defense, <u>Joint Doctrine for Information Operations</u>, Joint Publication 3-13, (Washington, D.C.: U.S. Department of Defense, 9 October 1998), pg GL-7

[6] Assistant Secretary of Defense for Reserve Affairs, The Joint Staff, J-1, J-3, and J-6, <u>Final Report – Reserve Component Employment Study 2005 (RCE-05): Joint Reserve Component Virtual Information Operations Organization JRVIO for Department of Defense Mission Support</u>, (Washington, D.C.: U.S. Department of Defense, October, 2000), 5. The phased implementation plan states that it will begin in Fiscal Year (FY) 01 with the use of an interim, near term "mandays" funding in order to use 182 reservists (60 officers and 122 enlisted) to

initiate JRVIO operations. The drilling reserve positions and the formation of the organizations will be established in FY 03 using existing billets from the services. The JRVIO's billets will increase incrementally each year until full-recommended end strength is reached in FY07. The projected end strength is 633 authorized positions.

[7] Jessica Lipnack and Jeffery Stamps, <u>Virtual Teams: People Working Across boundaries with Technology</u>, 2nd ed. (New York, NY: John Wiley & Sons, 2000), 18.

[8] Assistant Secretary of Defense for Reserve Affairs, The Joint Staff, J-1, J-3, and J-6, <u>Final Report – Reserve Component Employment Study 2005 (RCE-05): Joint Reserve Component Virtual Information Operations Organization JRVIO for Department of Defense Mission Support</u>, (Washington, D.C.: U.S. Department of Defense, October, 2000), 5.

[9] David Gould, Ed. D, "Virtual Teams," 5 January, 1999:available from <<u>http://www.seanet.com/~daveg/vrteams.htm</u>>; Internet; accessed 7 February 2002.

[10] John P. Kotter, <u>Leading Change</u>, (Boston, MA: Harvard Business Scholl Press, 1996), 148-151.

[11] Sirkka L. Jarvenpaa, "Communication and Trust in Global Virtual Teams," 4 June 1998: available from, < <u>http://www.mapnp.org/library/grp_skll/virtual/virtual.htm</u>>; Internet; accessed 7 February 2002.

[12] Emoticons are a very clever use of standard punctuation marks to express a human emotion. David Gould, Ed. D, "Virtual Teams," accessed 7 February 2002.

[13] Ibid. Some brief explanations of some of these technologies follow.

- Groupware or Collaboration software enables teams of people to work on the same document at different times. Software programs allow team members to share ideas and information, work together on projects, and take part in-group discussions with all team members. It also allows team members to create and share documents that include text, presentation graphics, scanned images, sound, video and more. Most importantly, this software offers several levels of security so that sensitive information is not compromised when collaborating with people outside of the organization.

- Newsgroups, bulletin boards and electronic mail on the Internet linking to a world-wide, networked computing community with millions of users from government, business, research, industry and education.

- Intranets are essentially communication tools that operate by linking an organization's computers in a way similar to the Internet. It is a closed network, however, which is accessible to people within the organization (and maybe approved outsiders). Like the Internet, its users access it by means of a piece of software called a "browser," which allows them to look at pages of text and images which are hosted on a company server. The user clicks on links written into these pages to go to other pages. The potential for

collaborative work is enhanced by Intranets, it provides a means for team members to have a "window" on each other's progress and assist each other in troubleshooting.

[14] "Defense Almanac 2002;" available from < http://www.defenselink.mil/pubs/almanac/>; Internet; accessed 20 February 2002.

[15] Donna L. Hopkins, Joint Reserve Forces: An Evolution in Military Affairs," Joint Forces Quarterly, Spring 1998, 123.

[16] Final Report RCE-05 (JRVIO), 19-20.

[17] Ibid, 22.

[18] Ibid, 13.

[19] Ibid, 26-27.

[20] Department of the Army, Training and Retirement Point Credits and Unit Level Strength Accounting Records, Army Regulation 140-185 (Washington, D.C.: U.S. Department of the Army, 1 July 1987), 8. Air Force Reserve Command Supplement 1, 19 December 1997 to AF Manual 36-8001, dtd. 1 March 1996, Department of the Navy, Commander Naval Reserve Force instruction 1001.5c, dtd. 9 February 1998, and Marine Corps', Marine Corps Order (MCO) P1001R.1J, dtd. 10 Mar 1999.

[21] Ibid, 22.

[22] As determined by each service's regulations or adopted regulations where now none exist.

[23] The DoD's JRVIO study's force structure has the JRVIOs imbedded in the parent organization without any cross contact for fertilization with other virtual organizations.

BIBLIOGRAPHY

Air Force Reserve Command Supplement 1, 19 December 1997 to AF Manual 36-8001. Washington, D.C.: U.S. Department of the Air Force, 1 March 1996.

Assistant Secretary of Defense for Reserve Affairs, The Joint Staff, J-1, J-3, and J-6. Final Report – Reserve Component Employment Study 2005 (RCE-05): Joint Reserve Component Virtual Information Operations Organization JRVIO for Department of Defense Mission Support. Washington, D.C.: U.S. Department of Defense, October, 2000.

Bickel, William COL, JRUCOS. Telephone interview by author, 20 February, 2002.

Boll, Kenneth. Like a Lightning Bolt - Information Warfare. Strategy Research Project. Carlisle Barracks: U.S. Army War College, April 1999.

Clinton, William J. A National Security Strategy for a Global Age. Washington, D.C.: The White House, December, 2000.

Crandall, N. Fredric, Ph.D., and Marc J. Wallace, Jr., Ph.D. Work & Rewards in the Virtual Workspace. New York, NY: AMACOM, 1998.

"Defense Almanac 2002." Available from < http://www.defenselink.mil/pubs/almanac/>. Internet. Accessed 20 February 2002.

Department of the Army. Training and Retirement Point Credits and Unit Level Strength Accounting Records. Army Regulation 140-185. Washington, D.C.: U.S. Department of the Army, 1 July 1987.

Department of Defense. Joint Doctrine for Information Operations, Joint Publication 3-13, Washington, D.C.: U.S. Department of Defense, 9 October 1998.

Department of the Navy, Commander Naval Reserve Force Instruction 1001.5c. New Orleans, LA: U.S. Department of the Navy, 9 February 1998.

Dunlap, Charles J. "Joint Vision 2010: A Red Team Assessment." Joint Force Quarterly, Autumn/Winter 1997-98, 47-49.

Fukuyama, Francis, and Abram N Shulsky. The "Virtual Corporation" and Army Organization. Santa Monica, CA: RAND Corporation, 1997.

General Accounting Office. Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. Washington, D.C.: U.s. General Accounting Office, May 1996.

Gould, David, Ed. D. "Virtual Teams." 5 January 1999. Available from <http://www.seanet.com/~daveg/vrteams.htm>. Internet. Accessed 7 February 2002.

Hopkins, Donna L. "Joint Reserve Forces: An Evolution in Military Affairs." Joint Forces Quarterly, Spring 1998.

Jarvenpaa, Sirkka L. "Communication and Trust in Global Virtual Teams." 4 June 1998. Available from, < http://www.mapnp.org/library/grp_skll/virtual/virtual.htm>. Internet. Accessed 7 February 2002.

Kotter, John P. Leading Change. Boston, MA: Harvard Business Scholl Press, 1996.

Lipnack, Jessica and Jeffery Stamps. Virtual Teams: People Working Across boundaries with Technology, 2nd ed. New York, NY: John Wiley & Sons, 2000.

Marine Corps Reserve administrative Management Manual, Marine Corps Order (MCO) P1001R.1J. Kansas City, MO: Marine Corps Reserve Support Command, 10 Mar 1999.

McNamara, Carter, MBA, PhD. "Virtual Teams (teams developed and/or operated over the Internet/Web)." 1999; available from <http//www.mapnp.org/library/grp_skll/virtual.htm>. Internet. accessed 7 February 2002.

Naval Reserve CINCPACFLT Detachment 420. Strategies for Integrative Management of Reserve Forces in the Joint Environment. Pearl Harbor, HI: U.S. Pacific Fleet, 16 July 2001.

Office of the Chairman of the Joint Chiefs of Staff. Joint Vision 2020. Washington, D.C.: U.S. Department of Defense, June 2000.

Reader's Digest Oxford. Complete Wordfinder. Pleasantville, NY: The Reader's Digest Association, Inc, 1996.

Stewart, Michael J. Information Operations, Information warfare: Policy Perspectives and Implications for the Force. Strategy Research Project. Carlisle Barracks: U.S. Army War College, April 1997.

Washington, Douglas Waller. "Onward Cyber Soldiers," Time Magazine. 21 August 1995, 1-5.