Virtual Peacemaking: A Military View of Conflict Prevention Through the Use of Information Technology

by Mr. Timothy L. Thomas
Foreign Military Studies Office,
Fort Leavenworth, KS.

	An abbreviated version of this article appeared in
	Military Review Dec 1998/Jan-Feb 1999 pgs. 44-57 under the title *Preventing Conflict Through Information Technology*
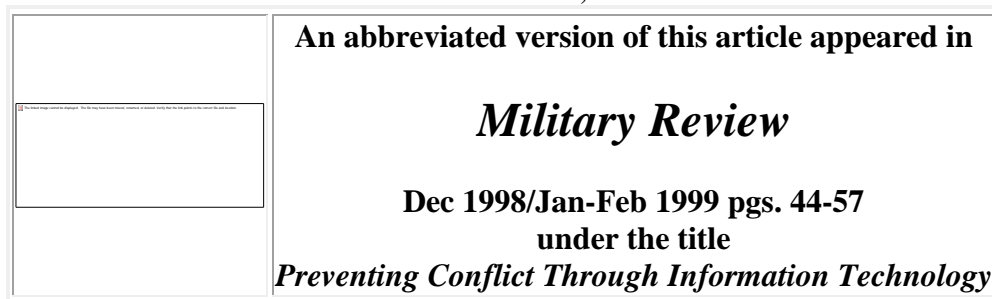
Introduction: What is virtual peacemaking?

While on patrol in Bosnia, an American lieutenant colonel was confronted by an irate Croat who, with an old map in his hand, told the officer that he was on his territory. Referring to his own map, the officer replied that he wasn't, and offered to go one step farther to prove his point. Taking out his Global Positioning System (GPS), he entered data and showed the Croat the results. "Sir," the LTC said, "I have consulted the cosmic tribunal (three satellites) and they have proven me correct. Excuse us, we have to continue with our mission."

Today there are many such occurrences when information technology (IT) is consulted to provide accurate and timely information. IT has the potential to become a huge conflict prevention tool or mechanism, an area largely underutilized. Traditionally, crisis managers and conflict resolution academicians attempted to prevent conflict through diplomatic, economic, cultural, and finally non-lethal means. If these steps failed, then the international community deployed military forces to exert pressure on potential combatants. The use of information developments now must be added to this process or progression. IT's data-processing systems connect people, places, concepts, and organizations with speed and accuracy, significantly upgrading the conflict prevention methods and integrating other conflict prevention means. Through developments such as the Internet, IT offers the potential to reach both ruling elites and individuals in societies contemplating conflict whether they have access to the technology or not.

The application of IT to processes that influence or regulate our lives has spawned a host of new concepts. Perhaps the most important is the concept of "things virtual." These "things virtual," as but one example, allow people to experience concepts or illusions temporarily simulated or

extended by computer software. "Things virtual" explain processes we can see and use but which we can't directly touch or feel. Some of these processes are familiar to us--virtual reality games, for example, are available to children. It is possible to order virtual flowers for loved ones via the Internet; and virtual environments allow scientists to explore molecular structures, architects to walk clients through their designs, and Ford Motor Company to teach forge hammer operators how to stamp out connecting rods.[1] Branches of government now study concepts such as virtual diplomacy, virtual justice, and virtual communications.

It seems only natural then to develop or apply virtual processes that help prevent conflict. Computer simulations, IT use by diplomats in negotiating processes, and IT use by militaries to monitor locations or find minefields are a few of many potential applications. This concept, hereafter termed virtual peacemaking, is defined as:

> The use of virtual processes of information gathering, analysis, and communication (through the use of information technologies [IT]) for simulated or training exercises as well as real-world scenarios by diplomats, mediators, negotiators, military leaders, and other individuals or groups to end a dispute and resolve the issues that led to it before conflict occurs.[2]

The most important part of this definition is the last few words, that the use of these processes will happen "before conflict occurs." Also of importance is the term information technology, which forms the core element of virtual peacemaking processes, and is often used as a specific reference point by discussants of conflict prevention who do not use the broader term virtual peacemaking.

This paper focuses on the military aspect of virtual peacemaking, those virtual information technologies the military can use to prevent conflict. First, it discusses the goals, interests, and value of virtual peacemaking. Second, it discusses the environment in which militaries conduct operations today, and the applicability of virtual peacekeeping to this environment. Third, it discusses the information technologies available. Finally, the limitations, problems, and dangers involving the military use of virtual peacemaking are explored.[3]

It will be useful to review a related use of IT that served as the catalyst for the idea of virtual peacemaking before beginning the detailed examination. This use was the crafting and implementing of the Dayton Accords negotiation process, which allowed the international community not only to manage the Bosnian crisis but also to find some resolution. So far, the process has successfully endured the challenges to peace for nearly two years. Future historians will look on the accords as the first major successful application of IT to assist in the conflict prevention process, in this case via "virtual crisis management."

The Dayton Accords

<div align="center">"In peace operations...perception is reality."[4]</div>

After nearly three years of fierce fighting among the factions in the former Yugoslavia, the international community finally persuaded the Presidents of Bosnia, Croatia, and Serbia to sit

down together and discuss how they could end the bloodshed. This meeting took place at Dayton, Ohio in the fall of 1995. IT played a prominent, even decisive role in convincing the three leaders that the accords would be administered fairly and without prejudice. Mapping and satellite data were the two pieces of information technology used most often. Similar procedures could prove useful for virtual peacemaking, it appears.

A huge TV screen was located in the room where these leaders met. A replica of the conference working map on the table in front of them was shown on the screen. This allowed the leaders to keep their fingers on the changing Inter-Entity Boundary Line that marked where the boundaries for their countries would lie. This was the chief area of contention. Mappers would

> digitize the line and import the information into a terrain visualization system called PowerScene (an advanced software architecture for terrain visualization), showing a 3-dimensional terrain perspective to depict where the line apportioned the land. Negotiators could also use the system to further refine the proposed line. For example, if the line cut through a building, the line could be moved to either side of the building and viewed on the screen.[5]

Current mapping for the software was accomplished by using real time satellite images from "flyovers." This three-dimensional, moving model of Bosnia's terrain was combined with PowerScene software (which purports to have no limitations on image source, scale, or breadth). Imagery of varying resolution from satellites, aerial photographs, and other sources were integrated into a seamless image on the screen. Maps and cultural features were worked into the display as well, since the imagery was correlated with real-world coordinates.[6]

Working with legal experts, the mappers exported information to an 8mm tape and hand carried it to the Joint Topo Tactical Operations Center (JTT), located three-quarters of a mile from the delegates quarters, for hard copy production. Sometimes the information was piped through fiber optic cables linking the JTT to the Remote Replication System support function to expedite production. The numerous changes kept the mappers very busy, with as many as 600 maps produced a day. Line drawings were digitized and put on a 1:600,000 UNPROFOR road map, where a transparent overlay was created and matched to a Defense Mapping Agency 1:50,000 Topographic Line Map, and replicated on a bubble jet printer.[7] The software almost eliminated misunderstanding over boundaries, thereby building confidence, mustering support, and saving time.

Aviation Week and Space Technology indicated that PowerScene had uses other than mapping, however. The journal indicated that PowerScene had also helped coerce the participants by demonstrating to the Serbian, Croat and Muslim leaders that NATO warplanes were very capable of precisely hitting targets if the fighting did not stop. That is, the possessor of these technological capabilities linked to simulation and mapping alone was able to demonstrate in a benign form its potential military power. Today

> PowerScene is being used in Bosnia to support command, control, communications and intelligence. If the commanding general wants to know what

the road looks like from point A to B, or the line of sight from a mountain, the system is ideal.[(8)]

After the peace agreement was initialed, representatives from the three sides continued to exploit this virtual reality view of the zone of separation.[(9)] They went on a simulated flight along the 650 mile long border to determine, in some cases, on which side of a road the boundary should run.[(10)] The flight lasted nearly nine hours. Thus, the application of virtual crisis management at Dayton helped eliminate mistrust and disinformation, and served as a confidence building measure.

During the implementation phase, the reinforcing mechanisms of the treaty were essential to the successful implementation of the peace accords while IT continued to play a major role. Helicopters, equipped with a new method to digitize the attack helicopter's gun-camera footage, exposed Dayton Accord violators by photographing their infractions. Occasionally peacekeepers presented evidence of a violation to leaders of the nation or group breaching the Accord to compel compliance. At times, cross hairs were trained on the equipment in the photographs to demonstrate the precision of the technology. The implied message was taken to heart by the transgressors.[(11)]

Information technology also connected NATO Headquarters with IFOR, the Internet kept troops informed of events at home, and a joint information bureau provided timely information and helped insure compliance with the Dayton Accords. The bureau provided daily advice to the division commander and operated together with the operations, intelligence, and civil affairs elements. It has helped manage a multitude of tasks and missions, and offered to journalists a unified, coherent view of the situation from an IFOR/SFOR standpoint. Clearly a key lesson learned, whether in the negotiation room or in the zone of separation, is that in peace operations in Bosnia, "perception is reality."[(12)] Managing this effort was possible because the agreement was in place before troops were deployed to the field.

What are the military goals, interests, and value of using virtual peacemaking?

The military's goal regarding virtual peacemaking is to apply technologies to conditions generated by a new world environment, turning this integration into military plans and operations to resolve disputes before they transform into conflicts. Just as diplomats use virtual processes (communications, negotiations, etc.) to keep a disagreement "within bounds," the military must use virtual processes to guide or force (when necessary) the militaries of disputing nations away from conflict. Military planners and operators do this by providing channels for anger, providing alternatives to frustration, relieving stress and tension, and avoiding overreactions on the one hand; and by deterring, monitoring, and even compelling disputing militaries on the other.

Virtual peacemaking allows intermediaries to "use forces" instead of the use of force. The military is a power in being with coercive capabilities that create pre-conditions for peacemaking. That is, the use of forces can serve a pre-emptive role and prevent the use of force. Virtual peacemaking can also support the rules of engagement for the forces called upon to prevent conflict.

The difficulty with virtual peacemaking is convincing governments without IT capabilities that IT is serving international and not national interests. Yet virtual peacemaking offers the opportunity for those with extra concerns and anxieties (whether they are or are not part of the conflict or conflict prevention process) to "monitor the monitors." However, at times the national approaches to conflict prevention are so diverse, due to national attitudes or the participation of peoples and movements instead of states and nations in national decision-making processes, that it is impossible to keep everyone satisfied.

Virtual peacemaking is not a call for virtual presence. Troops are still required. Virtual peacemaking merely strives to control disputes and prevent them from moving to open conflict by taking advantage of contemporary technology. Virtual peacemaking is a transparent process that offers five areas to assist conflict prevention: it **explains** the nature or causes of a conflict, or measures taken by the international community; it **demonstrates** simultaneity of effort, or the impotence of those involved in the conflict; it **compels** compliance by simulating consequences of actions taken by the participants; and it can **monitor** and **review** actions for the satification of the participants and the international community. If the end goal is served, the value of virtual peacemaking cannot be overestimated. Such a process can even help promote the creation of a global civil society through the development and use of common values, something long sought after but deemed unattainable.

What is the relation of military methods (combat and peacetime) to virtual peacemaking?

An important report by the Carnegie Commission, completed in 1996, recommended several ways to nurture conditions to prevent conflict from occurring. Although these recommendations were not necessarily military in orientation, they suggested other uses for virtual peacemaking. For example, the list included conflict prevention recommendations such as promoting intercommunal confidence, and developing programs to open up and maintain cross-cultural lines of communication.[(13)] Since militaries are called upon to assist in implementing these recommendations, their application to virtual peacemaking should be considered.

The military has at its disposal a list of mechanisms to prevent conflict that are applicable to virtual peacemaking scenarios. Michael Lund, author of <u>Preventing Violent Conflicts</u>, listed several of these mechanisms:

Restraints on the use of force

- arms control regimes, to include their monitoring
- confidence-building measures
- nonaggression agreements
- arms embargoes, blockades
- non-offensive defense force postures
- military-to-military programs
- preemptive peacekeeping forces for deterrence and containment
- demilitarized zones, safe havens, peace zones

Threat or use of armed force

- deterrence policies
- security guarantees
- maintaining or restoring local or regional "balances of power"
- use or threat of limited shows of force[(14)]

Each of the technologies discussed below should be evaluated against these mechanisms and applied where necessary. Virtual means can also help explore the relationship between military power and police power, or the use of forces under extreme conditions, to prevent conflict. The use of force under extreme conditions could also be simulated if necessary. Yet another vital simulation worthy of exploration is the impact of "information friction" on the situation--the impact of media bias, language difficulties, and cultural barriers and prisms on the force.

There is a huge civilian aspect of virtual peacemaking that works hand in glove with the military component and helps prevent conflict by defusing and alleviating risk factors.[(15)] These civilian mechanisms include the ability to:

- alert international bodies (use of the Internet, satellite communications)
- secure reliable information (through access to reliable data bases)
- identify and strengthen moderate leaders (use of TV/news/radio)
- establish channels of communications, both formal and informal (cell phones, Internet)
- develop coordinated political, economic, and social contingency plans, encourage and reward non-violence, limit spread of violence, penalize aggressors (integrate many IT uses noted above)
- follow up political support, economic engagement (virtual diplomacy and economic IT)
- establish regular consultations (hot lines, satellite communications, Internet)
- increase readiness of forces (measure units preparedness via simulations, use remotely piloted vehicle flights over formations and territories)
- prepare nonmilitary measures and actions (use of virtual diplomatic, judicial, and communication assets, economic and information blockade, use of non lethal weapons)
- strengthen deterrence by signaling red lines not to cross (use computer teleconferencing, transparency of preparations of the international community to act, etc.)
- communicate commitment to take stronger action (demonstrate ability to conduct system override, interference in all communications activities)
- prepare citizens to accept courses of action (use of public affairs assets and organizations, along with TV/radio/Internet, and other IT capabilities)
- initiate formal negotiations (Tele conferences, virtual diplomacy, etc.)[(16)]

Preventive actions help control early reactions to signs of trouble, identify and resolve the underlying causes of the potential violence, and offer a balanced approach to alleviating pressure and risk that may result in violence.[(17)] NGOs, for example, have become one the most important indicators of the potential rise of conflict. They are often the first to penetrate crisis areas and have a wealth of information regarding the conditions and grievances that give rise to potential violence. Governments often do not have direct contact with the population but NGOs do.[(18)] In this limited sense, non-state actors are replacing governmental agencies as a means for integrating and coordinating cross-border issues. It is important to be cognizant of their IT means and coordinate them with those of state actors and militaries, ensuring some compatiblity and a

means through which to communicate. Whatever course taken, governments, NGOs, and militaries must keep in mind that prevention will require actions, actions will involve costs, and costs will involve tradeoffs.[19]

Is virtual peacemaking applicable to the current international environment?

An air of optimism regarding IT's assistance to the conflict control process existed after the Dayton Accords. IT fostered both confidence and a positive attitude among the sides at Dayton (the Bosnian Serbs were not part of that process). Can virtual peacemaking responses be tailored to handle the different (race, religion, culture, etc.) causes of conflict, no two of which may be alike?[20]

> The information "center of gravity" will vary from conflict to conflict, from level to level, and from dimension to dimension. The greatest challenge for the policymaker will be to manage a national intelligence architecture, which can rapidly identify the information center of gravity, prepare the information "battlefield", and deliver the appropriate (non-lethal) information "munitions" to carry the day.[21]

In stpite of such difficulties, U.S. Armed Forces leaders support ideas related to virtual peacemaking, offering potential momentum to the concept and encouraging its integration. For example, Chief of Staff of the U.S. Army, General Dennis J. Reimer, believes "our analysis for the future points out that we need a capability called 'strategic pre-emption'. Strategic pre-emption is the ability to halt or prevent a conflict or crisis before it becomes debilitating or protracted--before it spreads out of control."[22] Shaping the international environment is a pillar of our national security strategy. Concepts such as virtual peacemaking should compliment these visions. Obviously, virtual peacemaking will also require international legal sanction and support, and a great deal of foresight and intelligence about the military situation.

During the Cold War, it was more difficult to influence a potential conflict situation, and to clear up misunderstanding, since many societies operated as closed systems. Government agencies, local business, the mass media, elites, and especially the special organs of intelligence directed a specific flow of information at both principal actors within the system (Presidents, Prime Ministers, General Secretaries, etc.), and at society at large. Control of this flow of information from the top down formed the outlook and attitudes of the populace (see Figure 1).

Figure 1
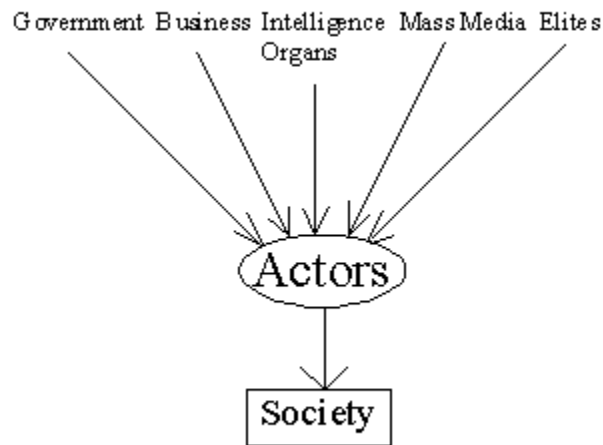
This situation was directly influenced by limited access to signals, human, photo, and electronic intelligence, and the manipulation of such information for policy formation and policy execution. Now, this position has changed dramatically as a result of IT and the end of the Cold War. While the intelligence systems still impact on policy formation and execution, public opinion also matters since many countries, previously bound by pacts of solidarity with closed societies, opened up to the global information market. An entire system known as the Global Information Environment (GIE) developed, mainly through the auspices of businesses and systems designed to monitor various situations (arms control, weather, the environment, etc.) offering an explosion of communications and other information technologies that have saturated societies world-wide. There is also a greater ability to manage open source information from sources around the globe, causing electorates at home and abroad to question even official sources due to access to alternate and comparative forms of information.

On a positive note, IT has penetrated and evaporated some of the opaqueness that surrounded many countries, and made them more transparent to both the outside world and their own citizens. The GIE includes individuals, organizations, or systems that collect, process, and disseminate information to national and international audiences. GIE is composed of national, global, and defensive information infrastructures,[23] and impacts on all countries, whether they realize it or not, through their use of satellites or other IT source. Satellites and cables offer outsiders or observers the opportunity to see inside and talk with members of a closed society (such as North Korea). Satellites monitor troop mobilizations and deployments, measure the local harvest and ascertain if people will starve or not, allow ordinary citizens to communicate via the Internet with people on the other side of the world, and afford businessmen the opportunity for instantaneous communication with financial and industrial centers all over the globe without government interference. The sovereign, on the other hand, has lost control of much of what people can see and hear, making it more difficult to "form" the consciousness of the populace than in the past. If the essence of sovereignty is the power to exclude others from interfering in one's affairs (personal or governmental), then IT is eroding that concept.

Virtual peacemaking offers the international community and individual states the capability to mobilize world opinion and put pressure on governments intent on initiating conflict. The advanced countries are being transformed fastest and in the process are transforming others due to the impact on economic activity. Now, even the most backward societies are touched by the revolution in computing technology and global connectivity. Virtual peacemaking also offers the opportunity for the international community to "signal" what is and is not acceptable norms of behavior, and to isolate a government if the need arises. This is especially effective due to IT's instantaneous impact. Now, the opportunity exists to utilize virtual diplomatic and economic means, or to use virtual information blockades or information overloads outside or within a country, respectively. Access to outside information also allows the local populace to influence the decision-making processes of a nation through the exertion of public opinion more than ever before (see Figure 2).

Figure 2
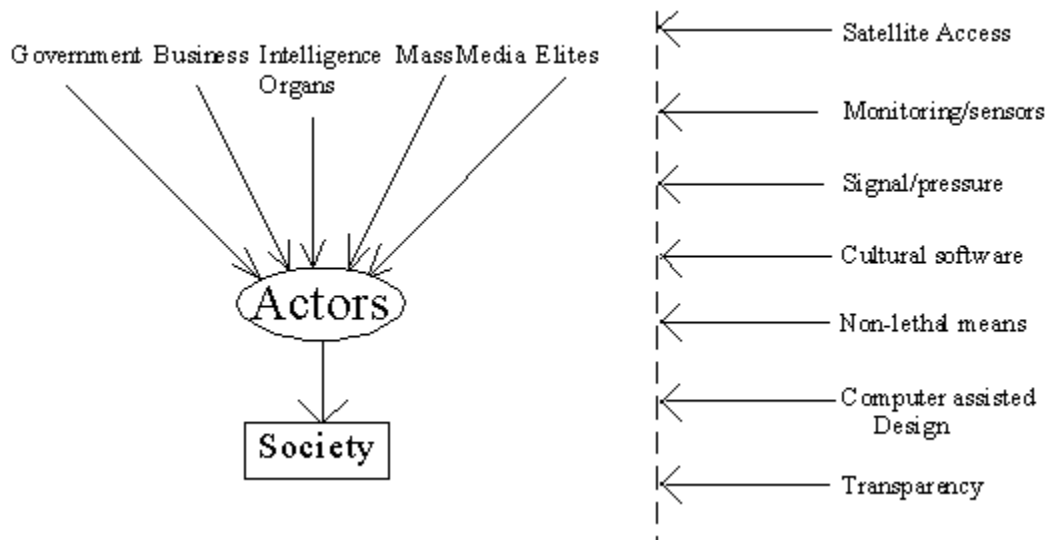
Walter Wriston, former chairman and CEO of Citicorp, speaking at a conference on Virtual Diplomacy in Washington, D.C. this past April, highlighted several intriguing aspects of the new IT environment that military planners must keep in mind. These included the impact of virtual peacemaking methods on sovereignty, on the destiny of people, and on the development of what he termed an "information standard." His message must be considered and measured by the military as it attempts to fit its methods and hardware to the virtual peacemaking concept.

Wriston noted that the entire political process is magnified and sometimes distorted by the images on our TV screens produced instantaneously by IT, especially by the 24 hour international reporting offered by stations such as CNN. This has also impacted on the way nations communicate with one another, as special interests (both national and transnational) more often bypass official foreign ministry channels. But IT enhances the effectiveness of conflict prevention measures, if Wriston's comments are on the mark, via the same TV images and access to the Internet. In Bosnia, for example, a legal web page was developed that had a virtual library and electronic publishing format, helping to build the rule of law. Bosnian judges used the system to access ways others handled similar problems. The system tied together not

only judges but also attorneys, clerks, and defendants. It may offer a symbiosis of the rule of law, the press and the people for the not too distant future.[(24)] However, problems of language, different legal systems, methods of legal input, and script must be overcome first.

More important, Wriston added, IT offers people a say in their own destiny. The formation of an information global village implies that denying people human rights or democratic freedoms no longer means denying them an abstraction they have never experienced. Instead they are being denied the established customs of the village which they may have seen on TV or read about over the Internet. Wriston also noted that if the economic market is viewed as a giant voting machine recording in real time the judgment of traders all over the world about our diplomatic, fiscal and monetary policies, then we must be aware of the creation of an "information standard" which is more draconian than the old Gold standard and operates more swiftly.[(25)] The information standard changes the way we solve problems, impacts on how we do our jobs, and most important of all changes the way we view and interpret events. Through the phenomenon of instantaneous IT, the information standard loosens the hold of the soverign and projects the individual as the object of events and information as much as the state.

That is, those possessing IT must learn how to use its consequences. Transparency issues and institutional methods offered by international participants such as the OSCE, UN, local academies, and institutes must also be studied. According to one Russian information warfare expert, S. A. Komov, IT can be used to distract, pacify, appease, intimidate, provoke, immobilize or pin down, wear out, confuse or weaken, suggest, or mislead.[(26)] This is an important list of uses, since many can help slow or prevent the use of force. These uses may also affect force projection, mobilization, and movement, thus affecting the capability to conduct actual conflict.[(27)]

The military must learn to integrate virtual peacemaking mechanisms into its preventive deployments and defensive postures. The military can fool potential combatants about the actual situation before them, gain information on potential combatants, and exert pressure, among other uses; and it can take preventive steps by planning ahead to control the consequences that might develop. In the final analysis, virtual peacemaking nicely compliments General Reimer's "strategic pre-emption" concept.

Thus, the balance of power in the world is no longer simply about bi- or multi-polar issues. Nor is it simply about balancing issues of diffuse, profound, and ancient collective-memory problems (race, religion, history, national interests) or balancing diffuse force-on-force problems. The balance of power also hinges on images and the use of IT that can tilt the balance one way or the other. This makes virtual peacemaking an inviting idea to explore further since it offers enhanced understanding of all these issues through transparency in the diplomatic, economic, and military areas, and enables the concept of strategic pre-emption.

What information technology will assist us?

"Technology empowers people."[(28)]

The next era of peace operations and conflict resolution will be strongly influenced by the relationship between humans and things virtual, if the Bosnian experience is any indicator. Designers will have to make software that can relate to soldiers, diplomats, and people with influence that fits their cultures and expectations. This requires that software manufacturers interact with academicians, religious and cultural leaders, and others who understand international sensitivities. It is a significant challenge seldom recognized, and one worthy of future study.

This realization comes at a time when consumer electronics, Hollywood, military planning and peacetime actions, and society all have access to similar items (in some countries of the world), that is, integrated IT systems. The military is buying off the shelf technology from the consumer sector, and Hollywood is amazing society with its ability to put the results of this convergence on the big screen. For those third world societies where access to IT is limited, it is still likely that decision-makers have access, which might alter the use of virtual peacemaking if conflict were imminent but would not eliminate its use.

The next era of peace operations may also witness the capability to customize or tailor IT to fit the contractor (a multinational force, the U.N., etc.). This will make IT potentially useful for peacemaking, peace enforcement and peace building operations. "Customizing" means selecting new developments according to their applicability to one of the types of peace operations, although they could just as easily be adopted for wartime use. For example, Bill Gates, Chief Executive Officer of Microsoft, described three ideas the consumer can expect to see in the not too distant future. They are the wallet personal computer (PC); electronic books that offer readers the opportunity to participate in writing the conclusion to the story; and advanced software that records each person's "documented life."[29]

Superimposing these three ideas on a military scenario allows one to envision, in the first case, an electronic wallet in the pocket of each peacemaker that offers instant information on the treaty being implemented or the international law about to be broken, supply and refugee routes available, location of NGO support groups, tele medicine information, local phone numbers of influential people, rules of engagement, cultural sensitivities, and other types of civil-military information. The electronic wallet also could be equipped with read-outs from built in radar detectors, and have the ability to place calls for help that designate both location and real-time images.

An electronic book could be used by commanders to access the electronic operations order of a higher level of command in one's own armed forces in order to help write the operations order based on the situation in his locale. Or it might be used to offer conflicting parties a chance to dialogue alone or with a mediator if all three parties were electronically connected. Access to one's documented life, in this case the documented steps leading up to a crisis, would allow the participants to review the steps that logically brought them to their conclusions in the first place.

If potential combatants wanted to talk over the phone or via a computer in complete anonymity, this is also possible with the help of IT. Camo-voice, a communications technology offering such anonymity to the caller, is available. Another communication's method is a software package called Lotus Domino, which allows a mediator control over who sees what on a monitor.

Through such devices of anonymity, presidents or secretaries of state could utilize the IT tools and conduct the negotiations while appearing to simply be a "representative" of the state in question.

There are many other hi-tech tools and software that can be customized for military use as virtual peacemaking instruments. These include such common everyday items as electronic mail, statistical analysis, graphical illustrations, use of indicators and warnings (or flagging specific words or concept variations), and the use of computer generated overlays or maps. It also includes such simple devices as a video camera.

Americans are very familiar with the power of images that video cameras have offered over the past few years, whether it be the beating of Rodney King; the photos of Timothy McVeigh in a Junction City McDonalds, tying him to the scene of the Ryder truck rental; or the footage shot during the beating of Missouri prisoners in a Texas prison. Prison guards report that one of the greatest fears of a prisoner, who has no civil rights, is to be videotaped during a disturbance because it will hurt the person's chance at parole. Some prison officials have even stopped a prisoner from further acts of harm by simply pulling out a camera and pointing it at the individual. They know that the video record will speak for itself at any hearing. Monitoring the outside of military garrisons or sensitive border regions with unmanned aerial vehicles (UAVs) could have a similar impact in recording the actions of countries that violate agreements and presenting them to international tribunals. Again, however, there are legal issues to overcome, in that countries are not prisoners and have no cause to expect violations of their sovereignty or privacy. They have rights **not** to be spied upon. But if the international legal community agrees that such monitoring is in the cause of preserving peace and eliminating bloodshed, then such "big brother" activity may have a chance, especially since nations observe one another from afar in peacetime through satellites. UAVs may not be as large as problem as they appear.

Simulations are another form of information technology that have real value for virtual peacemaking. Its adaptation for use in conflict prevention scenarios is quite simple. For example, societies about to become involved in a conflict could be shown a simulation (on local TV if the desire was to mobilize the entire populace) of the good and bad consequences of their deeds. Such a simulation may not necessarily show their destruction, but only the path leading to war and its consequences for the economy, for example, versus the path leading to peace. This would offer everyone the opportunity to sit back and consider the consequences of their actions, and to develop ways to interact and find solutions. Again, the problem will be cultural, finding a method to affect different parties in the same way.

Simulations can also be used to prepare the peacemaker. If human behavior can be properly modeled, to include its irrational aspects, then computer exercises would be more realistic instead of the preprogrammed responses we have come to expect over the years. These simulations could even be designed for specific locations and environments. As a result, peace operations personnel would enter into an area with a much more realistic appraisal of the situation. Thus, simulations are vital because they: (1) provide greater visual realism (sensations of motion, temperature, sound are important but visual imagery is best, especially if put in helmet mounted displays) (2) offer better and less expensive databases (3D data bases are available as well) (3) provide a broad spectrum of capabilities (allows planners and individual

soldiers and pilots to participate; offers chance to train en route or on site) (4) are more deployable, and offer mission-specific training and (5) offer improved upgradability for lower lifetime costs (can rehearse various geo-strategic settings and rapidly changing scenarios).[30] Obviously, simulations work for both wartime and peacetime operations.[31]

Speakers at the Virtual Diplomacy conference mentioned earlier offered other examples of how IT can be applied to military peacemaking efforts to enhance the effectiveness of these mechanisms. Wriston, for example, noted that IT enables airborne mine detector systems to locate mines and explode them via IT imbedded in drone Panther tanks, which demonstrates how information has replaced some human assets. Locating and clearing minefields makes them useless, and demonstrates the impotence of those who planted them to influence the situation. Other panelist observations impacting on virtual peacemaking processes were:

- IT affects the way we conduct military affairs, in that we move faster to react-act than in the past due to instantaneous communications and data transfers.[32]
- IT helps us conduct "navigation warfare" (determining where things are). It also is a "negotiation weapon" in that precise information in real time offers an advantage in decision-making. Unpiloted remote vehicles are an example of technology that can provide this information.[33]
- IT enhances a diplomats understanding of the history, training, biological processes, and learning techniques of a nation, not just their thoughts and the things they want today. We need to learn to connect data perceptual systems.[34] This lesson should be studied by psychological operations (PSYOP) personnel.
- IT can also allow one to look at roots of conflict associated with geography, such as natural resources, land, food, water, high ground, space, the environment, movement corridors, strategic locations, or cultural objects. A Geographic Information System (GIS) exists that can help resolve conflict by offering a number, quality, and diversity of global data bases (routing, crime analysis, line of sight, monitoring) which have peace keeping/peacemaking implications for combatants (where is the bread, the mines, the ammo, and so on). It also shortens the time lag between collecting and using, interrelates available information, and can put any factor of reality in a reference base[35]
- IT has assisted the mapping industry to enable us to communicate intuitively, since maps offer a framework for compromise and tradeoffs (can show flood plains overlaid on property, buffer zones around rivers, line of site for communication sites, and so on).[36]
- IT can model biological processes, hydrological processes, and the movement of animals or humans, among other things, and offers a framework for cooperation between academia, business, non-governmental agencies, government/military, and citizens.[37]
- IT enhances TV coverage, influencing measures of military success.[38]
- IT is heightening our view of the unusual (the Rodman-Madonna effect), which is making us more tolerant of "different" thinking about an issue.[39]
- IT should discourage us from thinking in terms of platform versus platform. Adversaries won't build pieces like that. We can't predict events due to change, chaos, and complexity, but we must be ready for all contingencies.[40]
- IT has created greatly flattened bureaucratic structures to implement conflict prevention processes. How to work with this apparatus must also be learned by diplomats and the military.

Limitations/problems

"The Internet may develop a conscience. It appears to be evolving on its own without a mandate."[(41)]

How nations learn to manage or leverage the consequences of the information age may greatly determine their power or influence on world affairs, much like the influence of great state diplomacy and nuclear weapons in the past. Yet while virtual peacemaking shows great promise as a new means to prevent or control conflict, there are also limitations and problems with its use. For example, there is an imbalance in the capacity to store, process and use information among nations, another reality of the new world order. This means that virtual peacemaking might work in some vicinities with developed information infrastructures but be limited in others. Another aberration is that the attainment of IT allows some smaller countries to possess a greater ability to conduct these operations than former superpowers (i.e., Japan versus Russia). And the mere thought of using IT as an intervention tool to prevent conflict raises serious questions about the need to fix responsibility for its use and misuse under law. Legal decisions will play a major role in many IT issues, and must be studied closely. They will help decide whether IT use represents interference in state or human rights affairs, or the violation of a nation's sovereignty.

Another problem for virtual peacemaking methods is one that has been with us for years. It is the historical, cultural, logic, and religious frames of reference used by different nations to measure IT developments. What may be a perfectly acceptable use of IT for one nation may be extremely limited in another due. For example, in societies dominated by religion, the Internet may be forbidden due to its ability to access information, especially about other religious movements or negative information about their own. In America, the restrictions the Amish place on their people represents an example close to home.

Yet another limitation or problem may be the use of virtual peacemaking as a psychological operations (PSYOP) weapon. PSYOP offers many uses for one's benefit, whether in the diplomatic, economic, or military arena, but also several dangers since it can act on the **limited understanding of the gap between reality and a human's ability to comprehend things virtual**. For example, TV's transformation from pixel to digital systems may offer an enormous opportunity for the moving, editing, and transforming of visual information and subsequent manipulation of a populace. Another example concerns the ability of software to recognize vehicles or other objects. The software could be manipulated, misinformed, or penetrated, perhaps even by other virtual images, to fool a monitor or an adversary about intentions or movements. Even the mass media can, wittingly or not, play a huge role here. Information technology can be used to create a common perception or agents of influence among populates considering conflict through developments such as voice or music synthesis or the use of holographs. The limitations and problems with their use is obvious, in that the opinions and responses these mechanisms generate may be interpreted as violations of international law. Regardless, a union of virtual peacemaking and psychological processes is hard to ignore. It may be one of the most dangerous weapons employed by the special organs of security or intelligence as well.

Another problem is the attention paid to processing technology at the expense of developing doctrine, training, and an infrastructure to support virtual peacemaking. This was also one of the conclusions from the study by Kenneth Allard on the use of information operations in Bosnia: namely that advances in information technology are valuable "only to the extent that they are accompanied by coherent doctrine, organizations, equipment, and people--to say nothing of the time needed to make them function as a team." That is, we can't forget the fundamentals.

There is also the problem of excess attention focused on the get rich quick schemes of information technology at the expense of virtual peacemaking and other, more humanitarian uses of IT. For example, Ismail Serageldin of the World Bank is adamant about ridding the world of some of its most obvious disparities, frustrations, and tensions. He noted that while we are more interdependent and environmentally conscious, connectivity is better, and democratic principles are winning the globalization battle as are human rights, we have an abject demographic mess all over the globe. Globalization appears to be only for the minority, since 20% of the world's population gets 83% of the world's income, while some 40,000 people die of hunger each day, a moral outrage. What a contradiction we have in the era of the information revolution as a result, Serageldin believes.[42]

In addition to problems, there are also dangers beyond PSYOP associated with the use of IT. For example, the use of IT not only allows small groups to mobilize quickly, but it also allows them to influence or even shut down political processes. The U.S. Congress has recently felt the pressure of this "participatory democracy." In the past, the U.S. electorate stayed at home and was content to vote every few years for a President and for members of local and state congresses. In extreme cases, letters would be written to Congressmen to bring attention to an issue. Today the situation is entirely different. With Internet access and e-mail links to Senators and Representatives, the electorate not only votes but offers opinions merely by sending e-mail. The danger is that the electorate can also send multiple messages that overload and shut down systems. In this fashion the Internet is developing a conscience of its own.

In an associated danger relative to small groups, small countries possessing the right kinds of IT can become as powerful as large countries overnight. This situation can become dangerous if the country having access to the right types of IT is a nation such as Iraq. The danger level would rise from mild to extreme since the world has come to understand that its leader, Sadaam Hussein, is irrational and so might be his use of the technology. Terrorist groups of any kind, for that matter, can threaten the entire world with the correct IT in their hands.

There are various methods that terrorists use information that become dangers, such as computer viruses, a terrorist home page to unite causes, or simple IT destruction or vandalism of vital equipment. Terrorists can access IT cheaply as well. Their goal will be conflict escalation, not prevention. For example, if a satellite up-link truck was stolen and transponders were knocked out, then terrorists could aim the beam at satellites themselves. Nothing could provide terrorists with more opportunity to demonstrate or exploit their causes than their ability to knock out the communications of governments.

Conclusion

"Computers exchanging video calls as commonly as e-mail. Three-dimensional windows that open into virtual worlds instead of virtual scrolls...and everything, from our medical records to our office files to the contents of our refrigerators, hypertextually linked via the great global network."[(43)]

The future promises excitement and opportunity to those who capture the ability to work with IT. Will concepts such as virtual peacemaking be part of that future? Hopefully, the documentation in this report has demonstrated that the capability to do so exists and that it is a worthwhile cause. First, there is a wealth of ideas, technologies and software applications with direct applicability to conflict prevention practices and theory. Some are as common as e-mail and the Internet, others as specific as MapLinx and Lotus Domino. Just as Bill Gates adapts these concepts to the life of the consumer, soldiers and diplomats should begin exploring their application to conflict prevention mechanisms.

Second, these technologies enable, using General Reimer's expression, "strategic pre-emption." This means that the concept of virtual peacemaking is applicable to conflict prevention theory not just on the tactical but the strategic scale, and offers a new tool to political scientists, soldiers, and diplomats to develop their models and uses of technology (of course, pre-emption has a purely military use as well [escalation domination to protect U.S. interests]; this is not its virtual peacemaking intent). Far too little time has been devoted to this topic to date. While we have examined and used IT as a crisis management mechanism, rarely have we looked at it as a conflict prevention mechanism. Virtual peacemaking is in need of further elaboration, especially since the military and consumer sectors are converging, implying one can assist the other in helping to prevent conflict.

Third, it is important that software manufacturers be made aware of the crucial role they can play in this effort. Academicians, religious and cultural leaders, and others who understand international sensitivities need to work closely with software producers to develop the products that take into consideration the terminology, cultural specifics and concepts associated with international negotiation processes. For example, just between Russia and the U.S., peace operations terminology can have varying differentiations that must be taken into account as well as cultural and political peculiarities. Only talented people with the proper guidance can develop the software required of such specificity.

Fourth, virtual peacemaking can take advantage of a phenomenon of the new world order, namely that many formerly closed societies are now, like it or not, more transparent due to IT. Whether it be e-mail, the Internet, or cellular phone linkups (it is hard to forget the striking image of the African warrior in the field with a spear in one hand, a cellular phone in the other), the world is more integrated than at any other time in history, offering opportunities to use virtual peacemaking tools to assist in deterring, blocking, pacifying and controlling conflict.

Fifth, while there are as many dangers as there are advantages to the use of IT, the dangers are controllable. Some believe that we, the IT tool makers, have made the tools so simple that now anyone can use them, even to destroy the tool makers! These include terrorists access to IT, and the ability to employ IT in a PSYOP operation against any country or group. One recent PSYOP example in America involved an e-mail of a speech delivered by author Kurt Vonnegut at a

commencement address. Filled with pearls of dry wisdom, it was passed around the country. However, the message was a fraud, written by a journalist and not Vonnegut. It demonstrated how vulnerable everyone is in the age of information technologies. And this analysis has not mentioned the dangers of hackers nor the friction and fog of information war.

Sixth, in Dayton it was demonstrated that the possessor of IT (linked to simulation and mapping alone) was able to demonstrate in a benign form its potential military power. This was the finest hour to date in preventing conflict through virtual means. The Dayton process added credibility to virtual peacemaking's potential to become an important conflict prevention tool in the future. It also must be kept in mind, however, that the management of this effort was possible because the agreement was in place before troops were deployed to the field.

There remains an entire series of questions that indicate other problem areas to address in future papers on this subject. These include the following concerns about controlling conflict: Whose interests are served through the use of virtual peacemaking (a country's national interests, black market interests, the U.N., etc.)? Who will be in charge of the global information infrastructure? Can virtual peacemaking be used to predict as well as stop conflict? How can virtual peacemaking help political stability and eliminate elements of closure? Can cultural sensitivities be included in virtual peacemaking methods and technology? How can virtual peacemaking support humanitarian assistance? How does bureaucratic stupor, cultural psyche, clans, tribes, or Mafias affect virtual peacemaking? How does the composition of society affect the use of virtual peacemaking? What is the impact of virtual peacemaking on diplomacy? What is the role of the mass media in this effort? When does virtual peacemaking become a violation of a nation's sovereignty? What determines elite consensus for virtual peacemaking (information or personal interests, power, or clan input)? Can virtual peacemaking be used by a potential enemy or apparent "friend" against you? How do we distinguish between PSYOP, persuasion, the truth, and vested interests such as the black market during the conduct of virtual peacemaking? Do we need "preventive sloganeering" and "dead end" recognition to enhance virtual peacekeeping? Can a "participatory democracy" be mobilized to support virtual peacemaking or will it be an obstacle?

In spite of the problems, limitations, and dangers associated with virtual peacemaking listed above, it still appears to be a subject worthy of further exploration. Better now to start studying the positive uses of the information revolution to prevent conflict and find ways to monitor potentially dangerous groups or gangs before it is to late. This includes groups and gangs on the Internet who invade personal privacy, invite you to participate in illegal behavior, or ask you to complicate police investigations and criminal cases. A recent report indicated that some citizens are taking it upon themselves to impose their own version of law and order on the largely unregulated Internet. There is even a group called Cyberangels, an offshoot of the New York City Guardian Angels, seeking out potential offenders and those who would take advantage of other "netizens." In the past year, web pages such as Women Halting Online Abuse were developed, as well as hundreds of others.[44] And these problems arise at a time when we are already slipping away from silicon technology to DNA, molecular, or quantum computing. Time is of the essence.

ENDNOTES

1. W. Wayt Gibbs, "Taking Computers to Task," Scientific American, July 1997, p. 84.

2. This definition was generated by collating the main ideas from two definitions, that of virtual diplomacy and that of peacemaking. This past April, at the opening session of a conference on Virtual Diplomacy, the President of the United States Institute of Peace, Richard Solomon, defined **virtual diplomacy** as "an exploration of how our world is being transformed by the global information revolution, one that assesses new technologies of data processing and communication to prevent, more effectively manage, or resolve international conflict." He added that virtual diplomacy is designed to help us explore the possibility to decrease conflict through virtual processes of information gathering, analysis and communication. Richard Solomon, Conference on Virtual Diplomacy, April 2-3, 1997 Washington, D.C..

The definition of peacemaking utilized in the collation was taken from the 1997 version of Army Field Manual (FM) 101-5-1, Operational Terms and Graphics. Here, peacemaking is defined as "the process of diplomacy, mediation, negotiation, or other forms of peaceful settlements that arranges an end to a dispute and resolves issues that led to it."Army Field Manual (FM) 101-5-1, Operational Terms and Graphics, 1997, p. I-119. Peacemaking, in the opinion of the U.S. Army's Peacekeeping Institute at Carlisle, Pennsylvania, refers to the term as used in 101-5-1 but, in addition, encompasses military support to preventive diplomacy as incorporated in the umbrella concept of peace operations.

3. An extended version of this paper discusses the uses and modeling of conflict prevention, and where the concept of virtual peacemaking could make its biggest impact.

4. Kenneth Allard, "Information Operations in Bosnia: A Preliminary Assessment," Strategic Forum, Institute for National Strategic Studies, Number 91, November 1996, p. 1-4.

5. "DMA Support to the Peace Talks," Online. Internet. 15 March 1997, p. 1 http//www.dma.gov/inf…acts/site/mappers.html,.

6. PowerScene, advertising overview handout, November 1995.

7. "DMA Support to the Peace Talks," p. 2.

8. Joseph Anselmo, "Satellite Data Plays Key Role in Bosnia Peace Treaty," Aviation Week and Space Technology, December 11 1995.

9. Virtual reality is "an interactive technology that creates an illusion, still crude rather than convincing, of being immersed in an artificial world." Philip Elmer-Dewitt, "Cyberpunk," Time, 8 February 1993, p. 60.

Another source defines virtual reality as "a realistic simulation of an environment, including three-dimensional graphics, by a computer system using interactive software and hardware." Random House Websters Pocket Dictionary, Random House Inc., 1993, p. 735.

10. Eric Schmitt, "High Tech Maps Guided Bosnia Talks," The New York Times, November 24 1995, p. 1.

11. Allard, p. 4.

12. Ibid., pp. 1, 3.

13. Second Annual Progress Report, Carnegie Commission on Preventing Deadly Conflict, New York, 1996, p. 8.

14. Michael S. Lund, Preventing Violent Conflicts, United States Institute of Peace Press, Washington, D.C., second printing 1997, p. 203.

15. Carnegie Commission, p. 7. The commission also recommended developing an "information index," developed by comparing a logic of warning [sooner one acts the better] versus a logic of policy [put off hard choices as long as possible]).

16. Carnegie Commission, p. 10. The uses of information technology suggested next to each item were not listed in the orginal, but added by the author.

17. Carnegie Commission, p. 6.

18. Carnegie Commission, p. 7.

19. Carnegie Commission, p. 5.

20. What is new about the international environment to which these considerations must be applied? Some of the most prevalent though not always obvious characteristics are: 1.) Modern methods for controlling crises utilize very slow decision-making processes, although progress in streamlining their effectiveness has been noted. 2.) Crises areas may require military action with humanitarian support, or military support of a humanitarian action. That is, nothing is predictable or traditional. 3.) Crises today, in contrast to the Westphalian system of the past, often require states to consider intervening and violating a country's sovereignty in order to stop military action. 4.) Some crises today require intervention in an area where no legitimate government is operating. 5.) Many crises today are far from America's shores, do not threaten our national interests, and consequently engender little public support. 6.) Crises often encourage manipulation of the force through "mission creep". 7.) Many modern crises require close coordination between many different organizations, which has required new organizational techniques to handle military interaction with both governmental and non governmental (NGO) agencies. 8.) Contemporary crises require governments to decide if they will support the international peace process, a national interest, or a humanitarian cause. 9.) Crises can demonstrate the power of national will of a country, such as has occurred when a hi-tech force is faced by an opponent with a "warrior" mentality. 10.) Major powers are often impotent to act in crisis situations, even with a high-tech force at the ready. 11.) Regional organizations are sometimes impotent to act in crisis situations, even if they have multinational rapid reaction forces at the ready. 12.) Crises can develop due to the breakdown of the laws of society and

methods for obtaining pay and goods, or for religious or ethnic reasons, making use of military force a last option. 13.) The multidimensional nature of crises makes it difficult to identify the center of gravity of forces involved in a conflict, especially among paramilitary forces. 14.) Some crises involving irregular or paramilitary forces have demonstrated little regard for standard warfare procedures or international law. 15.) Crises can spread within or between countries not initially involved in a conflict, simply over which side to take in the struggle. Any border issue usually involve military forces, however.

Not long ago the Carnegie Commission completed a study that outlined factors in today's world that eventually can lead to warfare. The report cited the 1) political and economic legacies of colonialism and the Cold War 2) illegitimate governmental institutions 3) problematic regional relationships 4) social cleavages derived from poorly managed religious, cultural, or ethnic differences 5) widespread illiteracy 6) disease and disability 7) lack of resources such as water and arable land 8) patterns of political repression, cultural discrimination, and systematic economic deprivation 9.) location of minority populations in economically depressed areas along borders with kindred states 10.) despotic leaders 11.) weak, corrupt, or collapsed regimes and 12) the exacerbation of these problems by new global political and economic forces.

The commission offered recommendations to get at the root causes of conflict produced by these circumstances. Finding ways to control conflict is crucial to world stability since local hostilities can become international ones, not in the nuclear sense as in the past, but in the sense that conducting quarrels no matter how deadly is an outdated idea.

Second Annual Progress Report, Carnegie Commission on Preventing Deadly Conflict, New York, 1996, p. V.

21. Robert Steele, "Virtual Intelligence: Conflict Avoidance and Resolution through Information Peacekeeping," downloaded from the Internet on 14 July 1997. Quote is on p. 26 of 28 pages at site http//www.oss.net/Paper...VirtualIntelligence.html

22. General Dennis J. Reimer, "The Army and the Cyberspace Crossroads," Defense Issues, Volume 12, Number 33, as taken from the Internet on 4 August 1997 at site http://www.dtic.mil/defe...nk/pubs/di97/di1233.html

23. FM 100-6, Information Operations, August 1996, p. 1-2.

24. Henry Perritt, Villanova University School of Law, comment made during his presentation at the Virtual Diplomacy conference.

25. From a speech by Walter Wriston, "Bits, Bytes, Power and Diplomcay," presented at the conference on Virtual Diplomacy in Washington, D.C., 1, 2 April 1997. All of Wriston's comments noted in the paper come from his presentation at the conference.

26. S. A. Komov, "On the Methods and Forms of Conducting Information War," Military Thought, July-August 1997, p. 19.

27. Virtual peacemaking has many uses by governments if properly applied to our information dominated environment. It can use IT as a deterrent or a confidence-building measure to contain or block access to other information or technology. As a deterrent, IT can help explain an action, put pressure on people or organizations, help instill fear over potential actions, and even find expression as an information saturation or blockade operation. IT can also deter by threatening to expose a leader's state secrets, by demonstrating the impotence of a nation to offer a credible threat, or by exposing troop deployments or other forms of military buildups, thereby uncovering blatant lies designed to manipulate public opinion.

Another virtual peacemaking use is to energize the diplomatic language of treaties. For example, any treaty utilizing the words "develop, plan, train, or engage in" has a use for virtual peacemaking. "Develop" can refer to the ability to expand on existing capabilities through, for example, new satellite links; "plan" can refer to the construction of an Internet capability or the laying of fibre optical cable; "train" can refer to the use of simulations to learn how to use preventive techniques, or to follow logic trees that would demonstrate the negative impact of some decisions; and "engage" can refer to IT methods to conduct negotiations through the use of information technology means (communication systems, etc.). It is also possible to prevent conflict by manipulating, interrupting, or interfering with information systems and infrastructures, although there is always an element of chance in such ventures as well as a question of legality (see section on limitations and dangers below).

A final virtual peacemaking use by governments is to help achieve economic leverage over potential combatants through inducements and incentives to be brought into the information age or, failing complicity, by using IT to establish economic blockades and affect indicators of stability and vitality, among other measures. Virtual peacemaking relies heavily on images and communications, with words and visuals becoming a currency of sort.

28. Chester Crocker, Georgetown University, comment made during his presentation at the Virtual Diplomacy conference.

29. Bill Gates, "The Road Ahead," Newsweek, 27 November 1995, p. 61.

30. Jim Oyler, "The Battlefield in your Brain," Military Training Technology, June/July 1997, summary of pp. 8-11.

31. There are other devices that must be considered as agents of virtual peacemaking as well. Some are pieces of hardware and some are software. They include the following:

CD games with emotions, religion, culture. On computer games today we can see the bodies-- the clothing, the faces--so the personality of the characters is naturally becoming a bigger part of the game design. CD games are beginning to make characters dominant or appealing, and to include other personal sensitivities such as emotions. There is little reason why these technologies cannot be used as a virtual peacekeeping means. For example, during negotiations or initial discussions, it might mean allowing the sides to confront one another through this process and witness first hand some of the distress or pain their actions might cause.

public forums. Usually taking place on a web page, public forums offer participants a place to explain the logic of their distress and thought processes. It is also a great place for the display of images, video, sound, and so on. This discussion may be conducted by academicians, diplomats, or any other credible group. The key problem will be finding acceptable artificial intelligence that can accurately portray the opposing sides and run the game. Any gamer magazine shows that there are big problems in these areas.

dual language software. Already under development, this software could be used to integrate culture specific terminology and sensitivities with peace operations concepts of the sides. This is important because not all sides use the same words and concepts in the same way. Most potential conflict situations will certainly be multilingual.

digital artists. These people are creating culturally oriented scenes to accompany landscapes, which will make the message and image more appealing to the reader. Naturally, it is almost pointless to have someone other than a local inhabitant create these scenes.

digital cameras. Similar in use to the video camera, they can use wireless infrared technology or snap into your PC. This allows a person to send back photos instantaneously as if he had a movie camera that only made still photos. This allows for quickly informing people of developing situations, allows for the instantaneous indexing of potential trouble makers (if legal authorities permit you to do so), and so on.

hand held fax readers. These devices allow you to send, receive and view faxes on the road. You even can receive long operation or fragmentary orders under such conditions, or offer situation reports supported by drawings or documents. Time to get material back to headquarters can easily be cut by over 100%. For example, the Philips Velo 1 is an example of some advanced technology with peacemaking potential. It is a palmtop with a built in modem and fax-send capability as well as an integrated digital voice recorder and browser capable of reading images of most Web pages at reduced scale. Peace operations personnel could theoretically even get onto the Home Pages of the sides in confrontation to try and calm them, or offer options.

computer-aided design (CAD). This type of software lets designers and engineers make three-dimensional models of almost anything. Terrain, buildings, and other objects can be modeled to offer a virtual reality climate in which to make proposals and decisions.

MapLinx. This software develops automatic displays of customers, prospects, sales, marketing or other data on detailed maps. It is possible to view the entire country or zoom down to a local neighborhood. With a single keystroke, it may be possible to map religious and ethnic groups, cultural and historical sites, and highlight electrical and water sources. This item would be especially useful to virtual peacemakers doing civil-military operations.

Lotus Domino. This is software that allows you to control who sees what, and who can make changes to what they see. It offers a degree of confidentiality and security during intense or sensitive consultations over open lines.

personal video products. In addition to video cameras, these products now include video teleconferencing that provide a virtual environment in which all participants sit around the same table. As was discovered during the Paris Peace talks to end the war in Vietnam, cultural sensitivities also need to be taken into account here, in this case the size and shape of the tables, which could be modified if video teleconferencing was used to fit what the participants see. Edited video or still images, and personal video conferencing are other options.

intelligent agents. These agents are actually programs that adapt to preferences of the user, even making decisions on their behalf (for example, a refrigerator alerts you that you need cheese. Such a system could find use as a warning system for surveillance UAVs or other monitoring or sensing devices).

other technology includes:

- some software allows you to work over your PC like a phone. That is, the electronic wallet discussed earlier could also serve as a telephone.

- the ability to create home pages accessible to spiders-software programs that prowl the Web as part of a search engine. To attract spiders, one needs to take advantage of meta tag-lines of code in which programmers put private comments or key words, which spiders read vociferously.

- cyber shot cameras that store images on chips which can be transferred to a VCR or a personal computer.

- a portable head-mounted video player, the Glasstron, which may do for video what the Walkman did for audio. It could be used as a simulator as a soldier walks in a mock up village or to receive news updates and images on the battlefield.

Finally, consideration must be given to the multitude of high technology "spy stuff" that can be used in conflict prevention. These devices include, but are far from limited to, the following:

- *camo-voice*, which is a digital voice masker for telephone calls. If a party to a conflict does not want to be identified, he can use this device to talk to parties on the other side in anonymity.

- *phone safe*, a device that can be engineered to identify and defeat eavesdropping devices.

- *theft detection powder*, which shows up under ultraviolet light and could be used as a verification device to prevent forgeries from being exchanged between two sides.

- and *heat stalker*, which can sense heat up to 100 feet. It can be used along with sensors in zones of separation.

For Operations Other than War (OOTW) scenarios, there are also more specific tools that employ information technology. Some of the non-lethal means recommended for application to conflict prevention scenarios in the sense of compellance (and likely adaptable to virtual peacemaking) are:

- *soldier tracking and warning systems*: system transmits a soldier's position back to Hqs, and provides warning to a soldier who gets out of his area or too far from HQ via a beeping signal. Can also be used to track friendly and/or hostile vehicles and individuals.

- *"lifeguard" anti-sniper Infra Red system*: uses sensors to track the heat of a sniper's bullet back to the point of origin. Has some applicability to rules of engagement as well.

- *people/vehicle/metal sensors along borders*: system can distinguish between people, metal, people carrying metal, etc. up to a range of several hundred meters.

- *hover UAVs*: air breathing vehicles that can remain stationary or nearly stationary and provide long endurance (several to many hours) sensor platforms. Serve as "local area satellites."

- *MHD or Magneto Hydro-Dynamics*: use electromagnetic power impulses for a variety of actions, such as disabling equipment and stopping vehicles.

- *high power, low frequency sound systems*: systems that disable humans by causing intestinal distress and disorientation. Testing involves ethical and political ramifications.

- *high intensity lights/laser weapons*: systems that can flash blind people or disable optical and infrared systems.

- *stink bombs*: non-toxic substances which are illegal under the chemical Weapons Convention.

- *sticky foam/deployable nets*: systems that stop or impede human passage or activity by creating barriers.

- *micro sensor networks*: networks composed of thousands of micro sensors that are deployed from a wide range of delivery platforms, which form themselves into monitoring networks to transmit data to remote sites.

32. Anita Jones, Defense Research and Engineering, the Pentagon, comment made during her presentation at the Virtual Diplomacy conference.

33. Ibid.

34. Mark Weiser, Xerox Palo Alto Research Center, comment made during his presentation at the Virtual Diplomacy conference.

35. Jack Dangermond, Environmental Systems Research Institute, comment made during his presentation at the Virtual Diplomacy conference.

36. Ibid.

37. Ibid.

38. Lieutenant General Anthony Zinni, U.S. Marine Corps, comment made during his presentation at the Virtual Diplomacy conference.

39. Arno Penzias, Bell Labs/Lucent Technologies, comment made during his presentation at the Virtual Diplomacy conference.

40. Lieutenant General Paul Van Riper, U.S. Marine Corps, comment made during his presentation at the Virtual Diplomacy conference.

41. Jack Dangermond, Environmental Systems Research Institute, comment made during his presentation at the Virtual Diplomacy conference.

42. Ismail Serageldin, World Bank, comment made during his presentation at the Virtual Diplomacy conference.

43. Gibbs, p. 82.

44. Bill Golden, wgolden@psrw.com, with more information available at: http://headlines.yahoo.com/thirdage/stories/8731019242.html