Strategic Knowledge; Preventing the Bombing of the Bridge to the 21st Century

By: C. L. Staten, CEO/CIO Emergency Response & Research Institute

Chicago, IL, April 9, 1997 (ENN) -- The nature and the face of intelligence, military, and emergency service operations are all going to change as we move rapidly into the 21st Century. The nature of the world's economic, military, technological, and geo-political structures are evolving at a more rapid rate than ever before. In order to be better understand our current circumstances and to effectively prepare for future eventualities, the following issues are presented for consideration.

Nature of the Problem; Paralysis of Analysis - A glut of information for decision-makers

The basic problem involves the fact that many current U.S. government systems are just too slow to respond to a rapidly evolving world environment. Information and decisions must pass through many "channels" and specialist "cubbyholes" (as described by Toffler, et al), each with their own priorities and bits of the total picture. The overall system then hopes that all of these "bits and bytes" will get put back together into a comprehensive picture higher in the chain of command. Some experts today question even this basic premise.

This compartmentalization of information seemingly prevents it from arriving in the hands of the people who need it to manage a strategic or tactical situation....in any sort of a timely manner. It must travel up the information chain, being "filtered" and "massaged" by any number of analysts, managers, and political operatives. Then, it must travel back down a chain of command and control, again being "manipulated" as it travels the avenues of the "action info-highway."

"The system" hasn't evolved much as overall information management capabilities have advanced and grown. Pertinent information needs to flow more rapidly down to the "manager" at the scene of the incident; be it a disaster or major military confrontation (and those two may become intertwined as time goes on). Vital information is of little use until it is applied to the problems that actually exist on the ground. Our "information system" should allows leaders to anticipate, plan, obtain logistics, and effectively implement sound tactics and strategies....in a rapid and more effective manner.

Intelligence Agencies:

Current security classifications and numerous levels of access may actually prohibit our leadership from gaining a real understanding of the world situation. The current classification systems often leads to information being "cubby-holed" by operatives or analysts who have reason to believe that it's disclosure could prove damaging to our country. This arrangement generally inhibits real-time analysis, due to the fact that there are too many "small pictures," and not enough large ones.

It would appear that the intelligence agencies may be undergoing an identity crisis following the cold war, the re-tasking of threats, and the recent spy scandals that have rocked several agencies.

Like IBM, General Motors, and other industrial behemoths, it is our hypothesis that the CIA, DIA, NRO, others need to re-engineer their operations to be able to instantly respond to "micro-crisis" situations. The necessity of early warning and intervention has been shown time and again in "real world" scenarios.

It would appear that too much data is being compartmentalized and not enough shared among military and other government agencies, due to questions about security classification and "need-to-know." Open source intelligence might be a better alternative, as it is easier and faster...but, analysis is much tougher due to the massive amounts of data that is available; some of it of questionable quality. It has, however, been demonstrated that open source collection and analysis can be done more rapidly than the existing system and that it may be more appropriate when brought to bear on commercial and industrial interests. American and her leadership might be best served by a synthesis of both wide-spread open source collection and analysis and a continuation of the necessary covert and classified traditional methods.

Big problems also currently exist with information being filtered by "info-tacticians" from both sides (internally/politically and externally from our "enemies") Current trends would suggest that we should expect an increasing number of and greater sophistication in propaganda and misinformation campaigns...particularly as they relate to geo-political/ideological issues. One of the biggest problems in the future will be to ascertain the validity of an increasing number of facts that could inundate any information gathering system.

It would also appear that greater emphasis must be given to HUMINT (human intelligence gathering) networks. Agents in place are needed in many countries. Our intelligence gathering assets in a number of countries have diminished as political alliances have changed and a greater reliance on technology has been implemented in some agencies. Satellites are a tremendous resource and may tell us something or somebody moved, but won't tell us why or what they intend to do next; that requires knowledgeable and courageous people "on the ground."

Military:

"Total situation awareness", down to the individual soldier level, continues to be more a goal, than a viable reality. Those that study such issues are discovering that you can't just bolt a video screen into a helmet, vehicle or command post and hope for "awareness" by the commanders or troops on the ground. The issue is far more complex than that and involves both physical and psychological implications. There would appear to be much work to be done in regard to improving the flow of data to and from the scene of a crisis or confrontation.

It is important to know that information or knowledge superiority may win wars, but that this advantage can be fleeting and fragile at best. Even small "inputs" can cause disproportionate effects; one piece of information can provide a tremendous strategic or tactical advantage, or the denial thereof can also result in catastrophic defeat.

The concept of "information dominance" and creating a "technology umbrella" to protect America and her allies would appear to be both admirable and feasible, if an appropriate amount of brain power and economic resources are committed to the effort. Such a change will require

more thinking "outside the box" of conventional military and political philosophy and result in a paradigm shift in the direction of our country's defense and national security establishment. (Please see paradigm shifts below)

A troubling paradox, however, involves the fact that as we become "information dependent" for our military success, we also become information vulnerable as our infrastructure and equipment becomes more inter-connected and complex. As evidenced by several recent revelations in the popular media, the civilian/commercial side of our "info-infrastructure" is becoming interdependent with the military side of this equation, with both becoming increasingly vulnerable. Greater steps must be undertaken to assure the security of all of the parts of our country's technology assets.

Troubling questions about force-projection, force-protection, conventional vrs. low-intensity warfare, and other related issues will continue and probably increase in the coming decade. The concept of maintaining sufficient forces and structure to engage in two Major Regional Conflicts (MRC's) concurrently, will continue to be debated in both political, budgetary, and military circles.

Some critics of the "2-MRC concept" would suggests that the United States needs to be more prepared to fight numerous "brushfire" conflicts or engage in "peace-keeping" operations, rather than fight major confrontations in the coming decade. Some experts would even go so far to suggest that further force reductions are possible by planning to fight only one major conflict at a time, thus resulting in budgetary savings. ERRI would suggest that a further "draw-down" of manpower is probably not warranted at this time, but that greater flexibility is necessary in force tasking and that a greater use of computer-generated "strike/defense package" configurations might be beneficial. Additional computerization of support and logistics functions could also prove beneficial.

If lessons learned in Haiti and Somalia are indicative, violence levels will continue to increase in any number of developing countries and effective law enforcement measures will need to be taken by the international community. These operations will frequently involve military/paramilitary action. Increasing numbers of peace keeping operations will probably also require greater anti/counter-terrorist capabilities and resources. Care, control, and policing of civilian populations could become an inherent and increasing problem in "peace-keeping" and "nation-building" operations. Additional training,consistent with these new missions should be provided to American troops, and greater use of larger numbers of special operations forces may also be anticipated.

Terrorism:

As the concept of "stateless warfare" continues to emerge, and its implications better understood, it would appear the greater the need for closer cooperation between emergency service and military agencies. Greater collaboration between Fire/Police/EMS and Military agencies may become mandatory in domestic terrorism circumstances. Over-lapping and concurrent responsibilities could become apparent...as multiple terrorist acts could cause interdependency in

civilian/military chains of command. Certainly, at a bare minimum, direct interaction and communications between these vital civilian and military agencies must take place.

Terrorist events currently move faster than responses...leading to decision-makers being forced into uneducated "guesses" about what to do next. Information may not only be slow, but also irrelevant to those that need it to make decisions. The real requirement is to acquire and analyze pertinent data, in as close to real-time as possible, to speed the decision-making loop.

Current operational trends in stateless warfare may require that we track individual terrorists...particularly those with specialized capabilities like explosives, assassinations, etc. Greater computer capability and increasing cooperation between nations can make this possible. Some have suggested that this same information could be used for air travel profiling databases, which could target terrorists, rather than just trying to track the general public.

Global communications strategies are changing, and even small terrorist groups are now using the internet to broadcast their message and misdirect/misinform the general population in multiple nations simultaneously. Additionally, it would also appear that drug and terrorist operations are being planned and implemented through the use of internet, satellite communications, and encrypted messages. Military and law enforcement agencies must be trained and equipped to counter increasing more sophisticated adversaries.

Good intelligence gathering, infiltration, predictive analysis and preemptive action are probably the best defenses against terrorism. The the best possible outcome of any terrorist event...is preventing an incident before it occurs. These necessary measures may include additional changes in current federal regulations, but lawmakers should be cautioned to avoid unnecessary intrusions into the private lives of U.S. citizens, or any action that could be construed as diminishing the individual freedoms of Americans. To do so will only play into the hands of enemies of the United States.

Paradigm Shift?

The basic rhetorical question is; are the military and intelligence communities undergoing a "paradigm shift"? Are advances in computer technology and information gathering/dissemination going to dramatically change the way that we conduct foreign policy and military operations? The answers would currently appear to be encouraging, complex and confusing...all at the present time.

There are certainly drastic differences between America, it's "info-structure," and the capabilities of developing nations. Due to the capital-intensive nature of the development of these advanced technologies, many smaller countries will not be able to move forward to an information-based economy, nor to an information-based defense establishment.

As America undertakes this paradigm we must be mindful of the fact that we must retain the capability to defend against low-tech threats as well as those from the technologically sophisticated. The range of differing kinds of threats has broadened dramatically in the past two decades. While the threat of nuclear holocaust has probably decreased to the lowest levels since

the 1950's, the likelihood of chemical/ biological/nuclear terrorism, possibly committed by a small number of individuals, has become a frightening possibility.

Conclusion:

A comprehensive knowledge strategy must combine acquisition, processing, distribution, and protection of information, all in an interrelated and interdependent manner. It must be comprised of a rapid, effective gathering and processing of data that can be formulated into knowledge that is actually usable by decision makers. Intelligence and counter-intelligence operations and analysis must occur simultaneously.

Strategic knowledge must go beyond electronic warfare (jamming, commo intercept, etc), beyond command and control - C4 warfare (Jstars, situational awareness, etc.), beyond information warfare (propaganda, psy-ops, info-structure attacks), to a full-blown global knowledge attainment that involves all facets of our society. It is believed that it is an integration of both civilian and military resources and abilities that will provide for the greatest defense and the advancement of both the United States and mankind in general.

This discussion paper was prepared by the Emergency Response & Research Institute of Chicago, IL. It was developed to prompt thought and discussion of military, intelligence, and national security issues that will have a profound impact on the United States in the coming decade. Questions, comments, suggestions, and criticism are welcomed, and may be addressed to enn@emergency.com.

Emergency Response & Research Institute
"The Home of the Emergency Net News Service"
(773) 631-3774 - Voice
(773) 631-4703 - Fax
(773) 631-3467 - Modem/Emergency BBS On-Line Services
E-Mail: sysop@emergency.com
Web: http://www.emergency.com