NATIONAL DEFENSE UNIVERSITY

NATIONAL WAR COLLEGE

Seminar L

"THE GENERATION GAP: OPEN-SOURCE INFORMATION, INTELLIGENCE, AND THE GOVERNMENT"

Col MICK NANCE/CLASS OF '94
CORE COURSE 5
SEMINAR: L
SEMINAR LEADER: Col J. GOUGH
ADVISOR: Col J. CIPPARONE

> "Information is a commodity, and not just a commodity, but a commodity that can be substituted for time, space, labor and capital."[1]

One of the results of the end of the Cold War has been an increase in the quality and quantity of information available from open sources. The volume of data that is currently being collected presents the intelligence community with an opportunity to better focus increasingly scarce resources on that information, which is only available through those means. With that opportunity, however, comes the challenge to ensure that the collection and exploitation of all types of information is done as efficiently and effectively as possible.[2] With information overload an increasing problem, the effective filtering, storage, and retrieval of relevant intelligence is critical to perceptive analysis and timely decision making.[3] Particularly with respect to open-source information, more tightly integrated collection management and new modes of analysis must be developed.[4]

This paper will describe the current generation gap between the government and open-source information. Information is intelligence and the government has not yet come to grips with the management, collection and exploitation of this extremely valuable commodity. I will provide some current challenges for both the open-source community and the intelligence community, suggest some management techniques and explain the importance of information knowledge. Finally, I will suggest a strategy that needs to be provided which will unite the government and private sector in a partnership. This strategy for partnership must be developed to provide the decision makers with immediate, concise information to make appropriate decisions. As the United States copes with the changing world, there will be a need for immediate, expert analysis of whatever information is available in support of policy decisions, contingency planning, or humanitarian assistance.[5] After all, our National Security could rest on major decisions being made accurately and in a timely manner.

OPEN-SOURCE INFORMATION

What is open-source information? Most of us think of open-source material as that from newspapers, books, journals, periodicals, radio and television. It covers all of those things and a whole lot more. The biggest area of open-source information is the relatively new field of commercial databases. Another growing component of the open-source field is something called "grey literature." This includes think tank studies, symposium reports, academic research efforts, and corporate brochures and reports that are free of proprietary or copyright restrictions.[6] For all the differences in the types of open-source information, there are two basic tenets that guide their use within the Intelligence Community. They are not classified and they are available to the public at large or to selected parts of the public either free or for a fee.[7]

THE GENERATION GAP

Tomorrow's regional wars will be fought with hardware of greater sophistication and firepower because, despite all the diplomatic negotiations of the last three decades, the technology of modern weaponry is no longer in the sole ownership of the United States, her allies, what was once the Soviet Union, or indeed China.[8]

Pity the hapless intelligence analyst! After four decades of studying, almost exclusively, anything with a Red Star painted on its side, the intelligence community is now tasked with mission impossible: to boldly go into the unknown to monitor and track potential threats to Western interests in any one of 80 countries.[9]

The information base available to the Intelligence Community has changed in a fundamental way. Open-source information has become so prevalent on a global basis that it can no longer be ignored. The Intelligence Community must recognize that the information era has exploded and the profusion of automated tools and systems to handle it, must be more effectively incorporated into the intelligence process.[10]

The mindset must be broken. Many analysts will testify that their management and their culture is actively biased against the exploitation of open sources. It is simply easier for the analyst to task classified capabilities than to obtain foreign video broadcasts, or commercial imagery products. This is the case even though classified sources by definition have a narrower focus and restricted production.[11]

Requirements for open-sources tend to be ad hoc; although there is a good understanding of community elements interested in open-sources, there has never been a systematic attempt to survey and understand the open-source needs of policy consumers, service and department planners, theater commanders and tactical commanders. It is a shared desire that information be made available to provide to uncleared troops and uncleared coalition and nongovernmental organizations. The depth of this feeling within the military, and presumably within other departments of the government, is not yet understood by intelligence community management.[12]

The government and the private sector has yet to come together to discuss and coordinate similar open-source requirements. Effective management is necessary to avoid redundancy between government agencies holding the same basic information that the private sectors possess. As a result, we have not even begun to understand, much less satisfy, our national open-source needs.[13]

Notably absent from the intelligence community's capabilities is the ability to routinely exploit multilingual video broadcasts, "grey literature", still photography, and multispectral imagery. Only open-sources, if exploited in partnership with the private sector, can meet the urgent needs within the fiscal constraints the intelligence community must accept as givens. It behooves industry to understand this situation, and to make its own case, extending its assistance, its innovative views, and its open-source capabilities and products into the government.[14]

MANAGEMENT

Management is the key to a development of faster, cheaper, and predominantly unclassified intelligence collection, processing, and dissemination capabilities. A capability needs to be established to bring the government and private sector together for the exploitation of open-sources.

The future of the United States hinges on how the government responds to this information revolution. Our society's ability to adopt to this extraordinary time of change is directly dependent upon it having large amounts of information available from which it can derive the new ideas that will allow it to fashion the new organizations and relationships necessary to deal with and exploit the rapidly changing environment.[15]

It is estimated that 10% of the products produced by our intelligence community need to be classified. It is also believed that most of what is collected does not get processed. By focusing on "secrets," the intelligence community is failing to leverage the capabilities of our nation's other open-source agencies.[16]

The private sector must make its contribution by understanding and supporting the need for a new perspective on knowledge and a commensurate adjustment in copyright and patent laws. Originators of information should be compensated based on the frequency with which their contributions are accessed, printed, transmitted or extracted. What no longer can be tolerated is the treatment of knowledge as property, and related restrictions on its dissemination.[17]

The private sector can take the lead in establishing national and international open systems and electronic connectivity at an affordable price; the private sector can also take the lead in developing cooperative agreements with foreign enterprises which bring more multimedia and multilingual data on-line.[18]

CHALLENGES

In the context of this essay, I will identify what is considered to be some of the major challenges with the linkage of open-source information and the government. Some of those challenges are:

1. The information architecture must be global, decentralized, interactive, and based on a strong commitment to maximizing data entry. Any architecture which fails

to meet these requirements is by definition constrained and deficient.[19] Architecturally, we need a new paradigm -- a completely new definition and approach to what information we need, how to handle it, and how it is delivered to the user.[20]

2. The value of classified information drops dramatically with each increase in the level of classification -- the more classified the document, the more restricted the dissemination, the less useful the information.[21] Security of information will come from speed of exploitation, not from compartmentalization and dissemination restrictions.

3. Besides the physical communication problem, finding enough bandwidth to move increasingly large amounts of multimedia data, our greatest challenge is the conceptual communication problem. The changing nature of information and how it can and must be handled needs to be understood.[22]

4. Doctrinally we need to change our concept of Command, Control, Communications, Computers and Intelligence (C^4I). We need to back away from system or command driven approaches to information handling, while extending our architectural concept to integrate unanticipated short-term coalitions, media operations, C^4I oversight over weapon system design and employment concepts, new data requirements for real time and coalition or disaster relief operations, and a very broad understanding of needed development in concealment, deception, covert communications, and "truth" validation.[23]

5. Technically, emphasis must be placed on processing and dissemination practices which provide for standardized transparent access to multimedia data at multiple levels of security. A long term challenge will be electronic connectivity

between individual citizens and their government analysts -- the creation of a global knowledge network -- should be a future goal.[24]

6. National intelligence must define itself less in terms of "secrets" and more in terms of actionable knowledge. National security must be defined less in terms of current intelligence about conventional threats, and more in terms of across-the-board understanding of "whole earth" relationships and imbalances requiring redress.[25]

KNOWLEDGE WARRIORS

"As the Third Wave War - Form takes shape, a new breed of "knowledge warriors" has begun to emerge - intellectuals in and out of uniform dedicated to the idea that knowledge can win, or prevent, wars."[26] These warriors are attempting to emerge from initially narrow technical concerns toward a sweeping conception of what will some day be called "knowledge strategy."

Some efforts have been initiated within the Pentagon and other government agencies in order to tackle the mission of developing a doctrine for information. In the office of the U.S. Secretary of Defense, there is a unit called "Net Assessment" who has shown great interest in information warfare. National Defense University and West Point had, in 1993, introduced their first course in Information Warfare. Outside the Pentagon, a private think tank called TASC (The Analytic Sciences Corporation), is also gearing up to work on the issue. RAND Corporation is working on what they call "cyberwar" which means "trying to know all abut an adversary while keeping it from knowing much about oneself."[27]

With the various interests and initiatives that have taken place thus far, we are still in the primitive stage of discussion. No one has yet taken what appears to be the final step in this progression - the formulation of a systematic, capstone concept of the military "knowledge strategy."[28]

STRATEGY FOR THE NEW ERA

What sort of strategy should the government consider as we move into a time of change and uncertainty? At least four elements must be included: building a vision for the organization, developing an adaptive organization, expansion of information technology and information access, and the creation of an information agency in order to consolidate information. Both the government and the private sector must address these issues and formulate a strategy as we enter the "Information Era."

1. Build a vision for the organization.

The most important characteristic of the successful 21st century organization will be a common vision to guide it. Without a common sense of direction, "an organization is likely to be driven by accelerating technological change, staffed by a diverse, multicultural network of highly intelligent workers, facing global complexity, a vast kaleidoscope of individual customer needs and the incessant demands of multiple constituencies..." and would simply self destruct.[29]

The Pentagon must begin a comprehensive process of developing a vision. New techniques coming out of the business community now allow "spectra of plausibility," to be constructed that increases the confidence decision makers can have about the kinds of futures they are likely to confront.[30]

2. Become adaptive.

In times of high rates of external exchange, a successful organization will quickly sense the direction of change and adapt to the new environment. It is not enough to be agile or flexible; there must be rapid organizational conformity to the new reality. This is particularly hard for bureaucratic institutions like the government, but if the military of the future hopes to be at the right place at the right time with the right capability, it must deal with those major internal components that restrict adaptability.[31] One critical area that requires adaptability is the acquisition process. In an era where commercial information technology, the major technological driving force -- has a generational life of one and one-half to three years, the military will never become adaptive until they overhaul the process by which systems are required. Much more use of off-the-shelf capabilities must be merged with modular platforms that can be quickly changed and upgraded. The many-layered acquisition process must be radically redesigned, eliminating many onerous specifications and oversight functions.[32]

3. Rapidly expand information technology and increase information access.

When information moves fast, analysis time is shortened and decisions must be made more quickly. A clear, competitive advantage accrues to the organization or nation that fully and quickly embraces the new technology. The military and other government agencies should, therefore, move expeditiously to install fiber optic information networks to connect all commands and thus provide the backbone for moving information as fast and far as possible.

With regard to distribution of information, military intelligence can play a very important part. If our country's leaders understood that our security is threatened from many different fronts and that the most successful response to an information technology revolution is to unleash information, then they should reorient our intelligence community to collecting mainly open source, unclassified information, analyzing it and distributing it broadly within the society as possible.[33] With the exception of relatively limited technical information and some information about plans and intentions, most of what we want to know is readily and cheaply available through the art and science of scholarship and personal interaction.[34] If the military intelligence community decided that their customer was the entire military and began to pump unclassified analysis broadly into the system, the result could be a new "renaissance" in the military.[35]

This new renaissance will provide immense increases in communication linkages and bandwidth will move and diffuse information much more quickly through business, education, social and military systems, yielding shorter reaction times and a higher tempo of operations. Ideas -- and images -- will blanket the globe in seconds, ricocheting throughout networks at the speed of light, changing shape and meaning throughout the process as receivers pass them along with their own responses attached. CNN's Desert Storm coverage is but a simple harbinger of what is to come.[36]

4. National Information Agency.

Elements of the government now dealing with open-sources should be consolidated in such an agency and granted an independent charter to enable them to support not only the intelligence community, and the remainder of the federal government that has been starved for information, but also the private sector and even foreign organizations as appropriate.[37] In order for this program to be successful, it would need a congressional charter and be established as a separate program. A strategy for this new information era is for Congress to follow the precedent it created with Special Operations/Low Intensity Conflict and create a Consolidated Open-Source Program.

CONCLUSION

In the future, our government will revolve around the quest for knowledge. As technology speeds up the rate of communication and data transition, the skirmishes of the future will be decided by those who can collect, analyze, and disseminate intelligence most effectively and efficiently.[38] The U.S. government can close the information generation gap by uniting in a partnership with the private sector. We have the resources to exploit knowledge that is available through open-sources. Toffler states that; "knowledge is a substitute for violence, wealth, labor, energy, space and time."[39]

A strategy must be developed that will prove capable of managing and effectively using knowledge, and as a result, will lead this nation into the 21st century. The challenge must be met on how best to nurture and take advantage of open-source information capabilities, while also being sensitive to the fact that low-intensity conflicts are likely to be characterized by high-intensity intelligence available to *all* parties from multiple governmental and nongovernmental sources. The age of constabulary warfare against relatively ignorant opponents is over -- the age of information warfare has begun. If we are to compete and continue to exist in this new information era, then the clever knowledge strategists will pay as much attention to "knowledge procurement" tomorrow as it paid today to the procurement of hardware.[40]

NOTES

1. Whitney-Smith, Elin. Information Peacekeeping. Proceedings, Second International Symposium: National Security and National Competitiveness: Open Source Solutions. Tysons Corner, VA, Nov 1993: p. 84.

2. Glickman, Dan. Comments from the Chairman House Permanent Select Committee of Intelligence. American Intelligence Journal, Spring/Summer 1993: p. 9.

3. Martinsons, Maris G. A Strategic Vision for Managing Business Intelligence Information Strategy; The Executive Journal, Spring 1994: p. 20.

4. Glickman, p. 9.

5. Williams, James, LtGen, USA(Ret.). Intelligence for the Future: Roadmap or Puzzle? Defense Intelligence Journal, 1993: p. 7.

6. Wallner, Paul F. Open Sources and the Intelligence Community: Myths and Realities. American Intelligence Journal, Spring/Summer 1993: p. 19.

7. Wallner, p. 19.

8. Hutchinson, Robert. Rumor of War, An Information Vendor's View of the Provision of Open-Source Data in an Unstable World. American Intelligence Journal, Spring/Summer 1993: p. 33.

9. Hutchinson, p. 33.

10. Wallner, p. 19.

11. Steele, Robert David. National Intelligence and Open Source: From School House to White House. American Intelligence Journal, Spring/Summer 1993: p. 30.

12. Steele, National Intelligence, p. 31.

13. Steele, National Intelligence, p. 31.

14. Steele, National Intelligence, p. 31.

15. Peterson, John L. New, Twenty-first Century Role for the Intelligence Community. Proceedings, Second International Symposium: National Security and National competitiveness: Open Source Solutions. Tysons Corner, VA, Nov. 1993: p. 2.

16. Peterson, p. 2.

17. Steele, National Intelligence, p. 32.

18. Steele, National Intelligence, p. 32.

19. Steele, Robert David. Information Concepts and Doctrine for the Future. Proceedings, First International Symposium: National Security and National Competitiveness: Open Source Solutions. Tysons Corner, VA, Dec 1992: p. 1.

20. Steele, Information Concepts, p. 4.

21. Steele, Information Concepts, p. 1.

22. Steele, Information Concepts, p. 3.

23. Steele, Information Concepts, p. 4.

24. Steele, Information Concepts, p. 5.

25. Steele, Information Concepts, p. 5.

26. Toffler, Alvin and Heidi. War and Anti-War. Little, Brown and Company, New York, NY, 1993: p. 139.

27. Toffler, p. 141.

28. Toffler, p. 141.

29. Peterson, p. 7.

30. Peterson, p. 7.

31. Peterson, p. 7.

32. Peterson, p. 8.

33. Peterson, p. 8.

34. Peterson, p. 9.

35. Peterson, p. 9.

36. Peterson, p. 4.

37. Steele, Robert David. "E^3I: Ethics, Ecology, Evolution, and Intelligence." Whole Earth Review, Fall, 1992: p. 77.

38. Castagna, Michael J. Executive Book Report, Powershift: Knowledge, wealth and violence at the Edge of the 21st Century. Proceedings, First International Symposium: National Security and National Competitiveness: Open Source Solution. Tysons Corner, VA, Dec 1992: p. 4.