REINVENTING INTELLIGENCE:
THE ADVANTAGES OF OPEN SOURCE INTELLIGENCE (OSCINT)

Robert D. Steele, President
OPEN SOURCE SOLUTIONS, Inc.
International Public Intelligence Clearinghouse

Second International Symposium on
"National Security & National Competitiveness:
Open Source Solutions"

2 November 1993

The Grand Vision

It is my privilege to present to you a grand vision, a vision of how America and other Nations can "reinvent" both their defense and their intelligence organizations, in order to ensure their status as sovereign Nations in the Age of Information.

As with the best of visions, this one is a simple one. I will outline it in simple terms, knowing that many hours and days of discussion must follow as the merits of the vision, and the practical implementation, are discussed among yourselves.

To be strong and safe and competitive in times of radical change, one must understand not only that change is taking place, but the implications of these changes for how one trains, equips, and organizes both their defense and their intelligence organizations.

Our most fundamental concepts, our concepts of what constitutes war, what constitutes peace, and what constitutes the proper role of the Nation-State in the defense of its citizens, are all being called into question.

We are in an era, as my friends Alvin and Heidi Toffler have documented so well, in which information is a substitute for time, space, labor, and capital. We are also in an era when a very small bit of information, obtained at the right time, delivered to right person, and acted upon in the right way, can neutralize vast arrays of nuclear and conventional capabilities. Information power is the "aikido" of the modern warrior.

Unfortunately, the Western powers have become doctrinally committed to a "Maginot Line" consisting of very expensive and very technical weapons systems. These are not only impossible to support with our existing intelligence systems, but also relatively useless against the emerging warriors and the impending economic and environmental challenges of the Age of Information.

The face of battle has changed. The laws of physics and mass are now subordinate to the laws of cybernetics and precision. In this grander battle, information power is the ultimate power.

The Transformation of War

Writing in 1989, in the *American Intelligence Journal*, then Commandant of the Marine Corps, General Alfred M. Gray, outlined the difference between the conventional threat for which we are all well-trained, well-equipped and well-organized, and the emerging threats, for which we are not. This is important not only to defense, but also to intelligence. Our intelligence organizations are trained, equipped and organized to deal with the conventional threat, not the emerging threat.

Influenced by both General Gray, and Martin Van Crevald, author of *The Transformation of War*, I developed the concept of the four warrior classes that we must face in the decades to come.

a. The *high-tech brute* is the traditional Western war-fighting machine, with lots of expensive equipment, hugh logistics trains, and massive organized forces under hierarchical command and control systems, and very structured intelligence services focused on "the main enemy".

b. The *low-tech brute*, by contrast, consists of the unconventional armed enemies represented by criminals, terrorists, narcotics traffickers, and armed religious gangs. It merits comment here that in most Western states, expertise in both fighting and penetrating these groups resides in the internal police forces--an expertise that is not easily shared with externally oriented defense forces.

c. The *low-tech seer*, such as the Islamic Fundamentalists, consists of those charismatic leaders and their mobs of followers--large numbers of generally unarmed or poorly armed people charged up with religious fervor. I know of no intelligence agency or defense organization that routinely includes such mobs in the enemy "order of battle" matrix.

It is also important to note that the command & control architecture for this warrior class is based on the religious pulpit and the transmission of television and radio broadcasts--this is a command & control system that cannot be penetrated by our existing "point to point" interception systems. As a result, our existing indications & warnings methods "do not compute" the more subtle indicators of threat from this group.

d. Finally, we have the *high-tech seer*, a combination of the individual computer or electronic terrorist able to bring a national, defense, or corporate communications system to its knees without being detected; and the economic cabals of certain governments, corporations, or tribes, including religious tribes, which seek to achieve strategic economic gains through whatever means.

In order to defend ourselves against these four warrior classes, and to reinvent intelligence so that it can support both the development of new doctrine and equipment, and the application of this doctrine and equipment, it is essential to acknowledge that the existing defense capabilities address only one quarter of the threat, and that much remains to be done in preparing ourselves for the future.

The Transformation of Peace

Just as war is being transformed, so also is peace changing. The emerging definition of national security is much more comprehensive in the aftermath of the Cold War and in the face of emerging threats, many of which cannot be blamed on a single opposing Nation-State.

John Peterson, the President of the Arlington Institute and a respected advisor to the Director of Central Intelligence and other key figures in the U.S. government, has noted that "The Nation's security is no more than the total of the individuals' perceived sense of security".

This observation is important for two reasons: first, it makes clear the fact that internal security forces, and internal nation-building capabilities, must be fully integrated into the totality of the national defense strategy; and second, it highlights the fact that every private army and every private intelligence service is a testament to the failure of the Nation to provide adequate security and adequate intelligence for its citizens and its enterprises.

International borders are irrelevant, an artificiality. Wars, whether big or small, whether between groups or individuals, have absolutely no respect for borders, particularly when they are waged by transnational groups. For this reason it is imperative that the doctrinal, legal, and organizational separation of internal security and internal intelligence, from external defense and external or foreign intelligence, be eliminated once and for all. We should consider the necessary doctrinal, legal, and organizational or task force changes that are required in order to deploy paramilitary force packages at home against criminal and terrorist elements too powerful for local law enforcement; to carry out nation-building tasks at home, including the retraining of private sector workers and the expenditure of defense funds on the civil communications and computing infrastructure; and to enable international "hot pursuit" of specific individuals regardless of what legal system they try to hide behind.

As we consider how best to train, equip, and organize its defense in the Age of Information, the power of intelligence and the power of the information that serves as the foundation for intelligence, will increase dramatically. "Intelligence" is no longer limited to "penetrating" specific targets to obtain a few bits of sensitive information. "Intelligence" must now be redefined to encompass all information, most of it unclassified, in order to provide every commander, every policy maker, every desk officer in every civil department of government, with the "intelligence" they need, when they need it, at minimum cost.

The existing defense planning and programming processes, and the existing national policy-making processes in other areas of interest such as economic competition, are guilty of two fundamental errors. First, they rely too much on classified intelligence, which is acquired at great expense, with great skill, and at great risk, while ignoring the vast quantities of unclassified information that might better guide their efforts.

Second, they use intelligence only at certain obvious decision points, or when the intelligence is so sensational it cannot be ignored, instead of embedding intelligence sources and methods--like administrative sources and methods--into every facet of their operations, every moment of every day.

Open Source Solutions

Henry Stiller, Director General of Histen Riller, said at the French Information Congress - IDT '93, that, "95% of the information an enterprise needs can be acquired through open means. He is absolutely correct. I commend to your attention my paper on "ACCESS: Theory and Practice of Intelligence in the Age of Information".

In this paper I discuss opportunities and contradictions facing the intelligence professional in a world characterized by enormous and largely unpredictable change. There are two realities that cannot be ignored. First, in the age of distributed information, where everyone is a producer of information, the concept of "centralized" intelligence simply cannot survive. Second, in an era of instant global communications, it is now possible, if you know how to do it, to obtain secrets before they become secrets, to obtain precious marketing information before others realize its value, and to identify critical vulnerabilities of your opponents' military or economy--all this from open sources.

Guarding against the possibility that you might say "that is all well and good, but not for defense", let me share with you a statement made at the Naval War College in 1991, by the Navy Wing Commander who led the first flight into Baghdad. "If it is 85% accurate, on time, and I can SHARE it, that is a lot more useful to me than a compendium of Top Secret Codeword information that is too much, too late, and requires a safe and three security officers to move it around the battlefield". The pace of war is so fast these days, that security has become an albatross. In the Age of Information, security comes from speed of collection, speed of analysis, speed of dissemination to the right person, and speed of action. Our own security restrictions, in my experience, are more useful to the enemy than they are to us, because they incapacitate our finest officers and prevent many key people from knowing what they need to know.

This is not to say that we should abolish national and defense intelligence organizations. On the contrary, they should become even more important and receive more funding. However, their focus must change.

They must develop even better clandestine human capabilities, and technical penetration capabilities, than ever before. At the same time, they must become a focal point for harnessing the power of the entire "information continuum" of the Nation, creating in effect a "virtual" intelligence community that is far more powerful, far more capable, and far more responsive to the needs of commanders and decision-makers at every level and in every sector, including the international economic sector. Every element of this continuum is both a producer and a consumer of intelligence, and it is the grand challenge of a new national intelligence community, properly constituted, to break down the barriers--the technical barriers, the cultural barriers, and the organizational or doctrinal barriers--between the elements of this "virtual" intelligence community.

The ultimate source of national power in the Age of Information is this "information continuum" and the "information commons" which the continuum makes possible. Any hesitation in the development of national policies which harness the power of this continuum to create both a "virtual" intelligence community, and a national population empowered by knowledge, will have a devastating and negative impact on our strategic competitiveness.

Doctrinal Implications

I have mentioned the disadvantages that secrecy imposes on our own thinking and our own coordination. Let me expand on that.

It has been my experience that most secrets start out as non-secrets. This is especially true in the scientific & technical arena, and in the international economic arena. It is only after a certain "critical mass" has been reached that some authority decides to classify or restrict information. It is of interest to me that we are in an era where speed is of the essence, and therefore, one can conclude that if something has been around long enough to finally be classified a secret, it is already too late to take strategic advantage of the information. The opportunity has been lost. We all need to do better at identifying those non-secrets that are of strategic importance.

To take another example, now under intense discussion in the Congress of the United States, it is my view that space systems, and surveillance satellites in particular, should be allowed to produce intelligence for those outside of government, as a means of keeping the assembly lines open and encouraging additional investments in research & development. It is no longer possible for a nation to sponsor the finest satellites or the best spies within the catacombs of the defense budget, nor is it possible for a government to afford these luxuries simply to keep a few top-level decision makers informed.

It has been my experience that most policy-makers find their daily intelligence briefings relatively useless, and their very thick intelligence documents too boring and cumbersome to be worth reading. What really excites a U.S. policy-maker, in my view, is information that is both timely, and that can be shared with a Congressman or a newspaper reporter. We need to rethink the concept of "value" for intelligence.

A final example, one offered with complete sensitivity to the enormous amounts of money we all spend on collecting encrypted signals. Not too long ago, I shared dinner with the General in charge of a particular European country's national signals collection agency. Let me tell you what I told him; start paying attention to the Internet, and to the unencrypted electronic information that is flowing through the ether. There are six hundred scientific and technical journals that are only published electronically, and can be found only on the Internet--in cyberspace--not in any library.

Overall, there is one doctrinal implication which has enormous significance for how one trains, equips, and organizes national and defense intelligence, and that is: we no longer need to acquire information "just in case". The sources and methods of open source intelligence are so powerful that we can conserve our resources and do "just in time" collection.

National Knowledge Strategy

I will conclude with an overview of what I believe should be contained in a National Knowledge Strategy, a strategy which I have called one of "National Engagement". We are now at total war and total peace, simultaneously, with a complex set of opponents, and nothing less than total "national engagement" will suffice in the age of information and of information warfare. In brief, it is not enough to provide connectivity, as Vice President Al Gore is doing in the United States. If one does not have a coordinated approach to content and to culture, then the connectivity simply provides a wider pipe for the noise of cyberspace. It is also important to coordinate investments in communications and computing research across government and private sector lines. I believe a major government like the United States wastes approximately two to three billion dollars a year, with a like amount being wasted in the private sector.

Finally, and this is the subject for another talk that I could give, it is absolutely imperative that every nation, every organization, indeed, every individual, pay great attention to the security of their command & control infrastructure. I can destroy any major nation in 24 hours with one platoon of knowledge warriors--and I can make billions of dollars on the international market doing so, because I will know when this is going to happen and can invest accordingly. Every government is now so dependent on their civil communications and computing infrastructure that to fail to invest in appropriate redundancy and security is tantamount to abandoning the defense of the nation. This is the down side of openness. However--and this merits stressing--"trusted systems" and personal authentication, personal encryption--are the foundation for true openness, giving information the freedom to move with confidence through the uncharted archipelago of cyberspace.

In brief then, we must understand that war and peace as we have come to think of it are completely transformed and much more complex. A typical great nation such as my own, or yours, is generally prepared only to deal with the *high-tech brute*, and does not have an intelligence service able to master the subtle and rapidly shifting targets which concern us now and in the near future. There is, however, a happy alternative--by reinventing intelligence, by taking advantage of open sources, and by harnessing the national information continuum to create a "virtual" intelligence community, a nation can rapidly acquire great information power, and use the power of that information to rapidly realign its defense resources, develop new capabilities, and forestall emerging threats. We must each engage our Nation, engage the "distributed intelligence" of our Nation, if we are to assure our national security and our national competitiveness in the years to come.

SECOND INTERNATIONAL SYMPOSIUM: NATIONAL SECURITY & NATIONAL COMPETITIVENESS: OPEN SOURCE SOLUTIONS Proceedings, 1993 Volume II - Link Page

Previous	Overview of Japanese Media & Information Systems
Next	Overview of the U. S. intelligence Community 's Open Source Requirements and Capabilities

Return to Electronic Index Page