OPEN SOURCE SOLUTIONS Group
*The Information Merchant Bank*

WARS AND PEACE IN THE XXIst CENTURY
Fondation pour les Etudes de Defense
Paris, France

# SMART NATIONS:
# National Information Strategies and Virtual Intelligence Communities

Mr. Robert D. Steele

19 December 1995

## INTRODUCTION:
## Related Events

It is a privilege for me to be invited to contribute to this extraordinary gathering of European intellect, and I count myself fortunate to be one of the few Americans participating in this event. The Fondation pour les Etudes de Defense is to be congratulated for organizing this event, because such events are the beginning of change, and change is necessary to survival in the 21st Century. I would like to mention two related events, also focused on national defense, information, and intelligence. On the 26th of October 1993, here in Paris, there was a colloquium on "Defense and Intelligence" sponsored by Mr. Pierre Pascalon, President of the Club "Participation and Progress". Speaking at this conference were Admiral Pierre Lacoste, General Jeannou Lacaze, General Jean Heinrich, and myself, the only foreigner. A number of other important persons in France contributed articles and statements, and all of this information is available in the book, *Defense et Renseignement*, published by Editions L'Harmattan. The second event I wish to bring to your attention is the publication this month--next week in fact--of the December 1995 issue of *International Defense and Technologies*, an issue which is dedicated to "Intelligence and Defense Electronics". Published by Connection International, with its headquarters in Paris, this issue contains commentary from a cross-section of European authorities; I was honored to be invited to provide the "Carte Blanche" introduction, and hope that you will have an opportunity to examine this entire issue of the bi-lingual magazine.

## DIAGNOSIS:
## Four Warrior Classes

Our diagnosis of the conditions confronting us as we enter the 21st Century must focus on two areas which I believe have very profound implications for national security and national competitiveness--the first area is that of threats, and the second area is that of the nature of war and peace in the 21st Century.

Let us consider the first area, that of threats. Consider the illustration below:

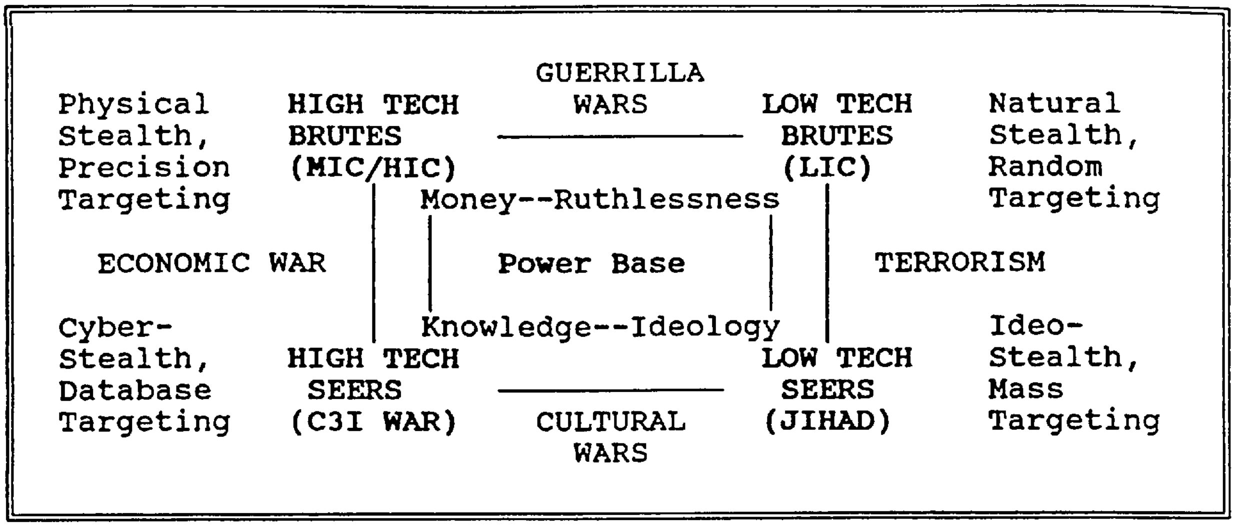
Physical Stealth, Precision Targeting
HIGH TECH BRUTES (MIC/HIC)
GUERRILLA WARS
LOW TECH BRUTES (LIC)
Natural Stealth, Random Targeting
Money--Ruthlessness
ECONOMIC WAR
Power Base
TERRORISM
Knowledge--Ideology
Cyber-Stealth, Database Targeting
HIGH TECH SEERS (C3I WAR)
CULTURAL WARS
LOW TECH SEERS (JIHAD)
Ideo-Stealth, Mass Targeting

Figure 1. Four Warrior Classes Illustrated

The High-Tech Brute is the "traditional" threat for which both our national defense and our national intelligence communities have organized. Virtually all of their funding is allocated to high-tech capabilities for unilateral warfare against strategic nuclear and conventional armed forces. We ourselves are high-tech brutes, with very expensive and complex weapons systems which require hugh and complex logistics trains as well as precision targeting data *which is not available*.[1] As we shall see this makes our capabilities largely irrelevant against the other three threat classes, at the same time that it makes us extremely vulnerable to anonymous attacks from individuals, clans, gangs, and Third World "rogue" nations that once would not dare to act beyond their own borders.[2]

[1] The precision-targeting problem consists of two elements: encyclopedic mapping, charting, & geodesy (MC&G) data at the 1:50,000 accuracy level for the area of operations; and an intelligence community able to both *acquire* the target, and provide a real-time "sensor-to-shooter" interface. Although SPOT Image Corporation can provide the necessary mapping data at the desired level of accuracy, the U.S. intelligence community has consistently failed to budget for SPOT imagery, or fully alert commanders to its utility, because of its obsession with maintaining dependency on a very expensive constellation of expensive classified satellites that are totally unsuited to wide-area surveillance or mapping support. Equally grave problems exist in the target acquisition arena when the target is anything other than a large conventional weapon that emits either heat or an electronic signature.

[2] A fuller examination of these four warrior classes is available in my article, "The Transformation of War and the Future of the Corps", published in *INTELLIGENCE: Selected Readings--Book One* (U.S. Marine Corps Command & Staff College, AY 92-93). My most

The Low-Tech Brute is comprised of Criminals and Terrorists, and sometimes it is difficult to distinguish between them--and of course sometimes they form alliances, as when criminals procure weapons and other equipment for terrorists. What is most important about this target is that it is not attackable by our fancy weapons systems because it represents what we call a "low slow singleton" attack problem for which signature and intelligence sensors are simply not available.

The Low-Tech Seer threat class is comprised of Zealots, Ideologues, Mobs, and Refugees, as well as the more sophisticated and coherent cultures of the Third World and the Eastern World which Western intelligence communities have never been able to understand. It is worth noting that intelligence sources and methods associated with "indications & warning" (I&W) inevitably contain enormous cultural presumptions about both the motivations and the expectations of the opposing party. The same cultural presumptions at the policy level make it difficult to accurately anticipate, assess and respond to threats from this warrior class.

The High-Tech Seer is represented by Hackers as individuals, and by Economic Warfare when conducted at the nation-state level. This warrior class is especially interesting because the battlefield is in the civil sector, the weapons are information and information technology, and the military in most countries has not yet realized that it must either be able to wage war "by other means", or find its role in the national defense significantly reduced in "The Age of Information". Perhaps of greater concern, civilian authorities appear to be completely ignorant of the urgent nature of this threat, and how to mobilize and organize civil capabilities necessary to cope with potentially anonymous attacks on critical civil nodes.[3]

In concluding this section on diagnosis, it is necessary to provide one more illustration.[4]

---

detailed examination of U.S. intelligence community shortcomings in addressing the threat represented by these four warrior classes in the 21st Century is provided in "A Critical Evaluation of U.S. National Intelligence Capabilities", *International Journal of Intelligence and Counterintelligence* (Summer 1993).

[3] The seminal work in this area is Winn Schwartau, *INFORMATION WARFARE: Chaos on the Electronic Superhighway* (Thunder's Mouth Press, 1994. Thoughtful articles on the vulnerability of specific networks include: Maj Gerald R. Hust, "Taking Down Telecommunications", School of Advanced Airpower Studies, 1993; Maj Thomas E. Griffith, Jr., "Strategic Attack of National Electrical Systems", School of Advanced Airpower Studies, October 1994; and H.D. Arnold, J. Hyukill, J. Keeney, and A Cameron, "Targeting Financial Systems as Centers of Gravity: 'Low Intensity' to 'No Intensity" Conflict", *Defense Analysis* (Vol. 10 No. 2, 1994).

[4] Mr. John Peterson, President of the Arlington Institute, developed the original matrix and definition; I have added the third dimension of time.

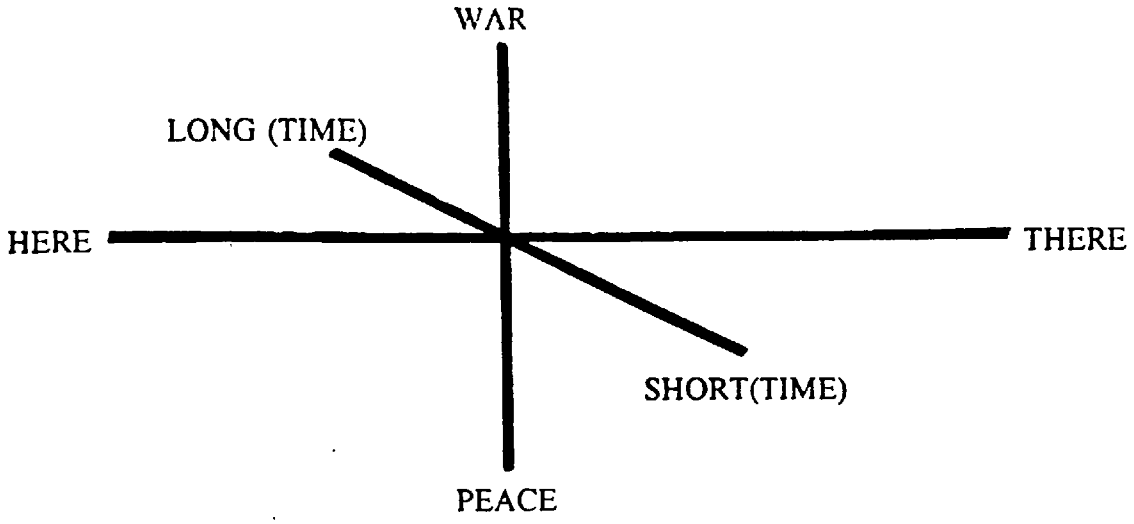

Figure 2. Changing Nature of War and Peace

Traditionally--and with little change today--national defense and national intelligence have focused on "war" beyond the nation's borders, "there". To the extent that internal threats to order existed "here" at home, this has been left to law enforcement. Now, however, we are discovering that war "by other means" is "here" inside the borders, in the civil sector, and occurring under conditions of nominal "peace".

I have added to this matrix a third dimension, the concept of time, because a major weakness of our existing defense and intelligence communities is that they have generally had the luxury of long periods of time to develop capabilities, to identify threats, and to conduct operations. Today, however, the enemy can be anonymous, can utilize unconventional capabilities such as electromagnetic or electronic attacks against key communications and computing nodes, *and can do this overnight, with no warning*. The single greatest challenge to both the defense and intelligence communities in the 21st Century is going to be this element of time: how does one train, equip, and organize a capability that is able to cope with "real time threat"?

Let me emphasize this, because it is so very important: in dealing with "chaos", threats emerge "spontaneously" and often unpredictably, and the ability to create "just in time" capabilities and to react decisively "just in time" is going to be the single most critical aspect of successful defense and intelligence in the 21st Century.[5] Within the intelligence community, it will be impossible to maintain "central intelligence" organizations that collect

[5] I highly recommend the book by Brigadier Richard E. Simpkin, *RACE TO THE SWIFT: Thoughts on Twenty-First Century Warfare* (Brassey's, 1985).

everything--in the fashion of vacuum cleaners--"just in case". Instead, both intelligence and defense will have to be completely restructured in order to do "just in time" collection and take "just in time" action.[6] The remainder of my presentation will address our existing structural imbalances, the new forms of violence that will challenge intelligence, the need for new sources and methods of early warning, and the national solution for prevention and action: national information strategies and virtual intelligence communities.

## STRUCTURAL IMBALANCE:
## Intelligence without Thought

In addressing issues of structural imbalance, I must rely upon my experience of over twenty years with the U.S. intelligence community. Although it has been my privilege to work with fourteen different intelligence communities world-wide in the past four years, and I see many parallels to my own experience, I will not draw generalizations here. My comments reflect the American experience.

Most distressing, and typically American, has been the substitution of technology for thinking, of bodies for brains. Two examples will suffice. A simple example is found in the field of counterintelligence, where reliance on the polygraph machine ultimately has resulted in the destruction of the field of counterintelligence. Two of my classmates in the clandestine service were video-taped doing dead drops in Cuba because all of the Cuban agents had been doubled, and all of them had passed the CIA's polygraph tests.

A more complex example is that of satellite technology. While I continue to have great regard for signals intelligence technology, and good regard for imagery intelligence technology, there have been several negative outcomes to the American obsession with satellites as the primary source of "reliable" intelligence:

a) First, the satellites created their own bureaucracies with vested interests in the extraordinarily vast funding for these programs, and these bureaucracies created narrow "pipelines" for Top Secret "CODEWORD" intelligence--in essence, the intelligence community in the United States became fragmented, and it became much more difficult for

[6] Paul Evan Peters, Executive Director of the Coalition for Networked Information in Washington, D.C., is the originator of the term "just in time collection", and has done some original thinking about how distributed information networks can provide "just in time" answers at a much lower cost *and with much greater currency*--distributed experts funded by distributed centers of excellence turn out to be more accurate, more current, and more responsive than bureaucratic analysts captive to a "central" intelligence organization. This is not to say that we must eliminate national intelligence--on the contrary, national intelligence organization must add the special value that comes from access to classified information and to the policy-maker--but must do so upon the foundation of distributed knowledge available throughout the Nation.

the policy-maker to receive an integrated intelligence product at a low enough level of classification which permits useful and timely dissemination and discussion.

b) Second, the secrecy surrounding the satellite technology, a secrecy that restricted sharing with even our most important allies such as France, severely hampered transnational cooperation and the sharing of intelligence against mutual enemies. This also led to an enormous waste of financial resources as the Americans sought to maintain a classified satellite capability unilaterally, and eventually forced the Europeans and others to create their own duplicative technology at great expense.

c) Third, the secrecy surrounding the satellite technology ultimately permeated all aspects of intelligence, and resulted in a *de facto* isolation of the intelligence community from the rest of the information continuum--all the other centers of unclassified intelligence available in the Nation and internationally--schools, universities, libraries, businesses, information brokers and private investigators, journalists, normal government offices, defense departments, *and other intelligence communities*. It is instructive that while the Americans have a number of classified burden-sharing agreements, they do not have any arrangements for sharing unclassified encyclopedic intelligence with counterparts in other governments, and they have very limited capabilities for providing their analysts with direct access to open sources of information.

d) Fourth, and most destructive, has been the impact of satellite cost on the funding of human expert analysts. Satellites have dominated the U.S. intelligence community budget, with the result that funds have not been available to hire true experts with ten to fifteen years of private sector experience. As the most recently retired Director of Intelligence for the CIA, Mr. Doug McEachin, has noted publicly, "It is difficult to do good analysis with a bunch of 19-year-olds on two year rotations". This is a devastating commentary on how the U.S. intelligence community has sacrificed thinking in order to afford technology.

The reality is that the U.S. intelligence community is optimized for secrets, and believes that its mission is to produce secrets rather than to inform policy. This is why I am forced to point out that "the problem with spies is that they only know secrets!" Here in France it was recently noted that several of the American spies were paying their nominal agents, actually under the control of French counterintelligence, for information that was available to the public. Although this is a common tactic when first developing an agent, the reality is that U.S. spies do not have the education, language capability, time, or incentive to follow what is available in the public domain, and they are therefore destined to continually waste valuable resources collecting information that is not classified and should not be classified.

Intelligence communities should not be in the business of collecting open sources; but if they are not able to establish themselves firmly upon a foundation of encyclopedic open source information available from the private sector, then it is my judgement that 75% of what they do in the classified arena is irrelevant at best, and counterproductive to policy as well as wasteful, at worst. In essence, open sources provide the critical *context* for intelligence analysis--without such a context, classified intelligence is actually misleading and therefore dangerous to the policy-maker.

There are two other structural imbalances that I wish to briefly address: the lack of attention to unclassified foreign-language hard-copy as a primary source of raw intelligence; and the lack of a coherent intelligence analysis model that distinguishes between the levels of analysis and the geographic, civil, and military spheres, but ensures their integration. Implicit in this latter imbalance is the issue of whether intelligence is intended to broadcast generic information, or provide tailored "decision-support" to specific customers.

I will address the first structural imbalance only briefly. I continue to be astonished, when I am invited to review current plans for "modernizing" military communications, to find that everyone is very proud of their planning for "multi-media" digital systems. They stop smiling when I point out to them that 80% of the information that the commander needs has not been digitized--it is in hard-copy, generally has not been collected by the intelligence community, and is usually in a foreign language. Of course they have not planned for collection, translation, and digitization. They generally get irritated if not angry when I then proceed to point out that 80% of their civilian counterparts in their own country and their military counterparts in other countries, with whom they must be able to conduct coalition operations, cannot interface with their fancy technology. The reality is that "intelligence" must rely heavily on "ground truth" that has not been digitized, and "just in time" operations must rely on mixing civilian and military capabilities across political boundaries in such a way that hard-copy actually becomes the only acceptable common denominator for communications.[7] Intelligence communities must have in place global capabilities for rapidly identifying, collecting, translating, analyzing, and digitizing where appropriate, or reproducing where necessary, foreign-language hard copy.

The second imbalance is more subtle. When I first established the Marine Corps Intelligence Center in 1988, I undertook a personal examination of all available intelligence production from both the Central Intelligence Agency and the Defense Intelligence Agency, and I came to two conclusions: first, I could not find a single product that supported any specific decision--everything was generic in nature; second, I found that none of the products were founded within any analytical model--they were more like classified journalism.

[7] To take one very important example, military maps, it merits comment that of the sixty-nine countries identified by the U.S. Marine Corps in 1990 as being "likely" candidates for contingency operations, there was no mapping data--hard-copy or digital--for twenty-two of the countries, old data for the ports and capital cities only for another thirty-seven, and very old data for the other ten. This was one of a number of critical intelligence shortfalls addressed in *Overview of Planning and Programming Factors for Expeditionary Operations in the Third World* (Marine Corps Combat Development Command, March 1990), for which I served as the Study Director.

Taking the first element, please allow me to offer three definitions which distinguish between data, information, and intelligence. In my view, *data* is the raw print, signal, or image that is collected; *information* is data which has been collated to be of generic interest; and *intelligence* is information which has been tailored to support a specific decision by a specific person at a specific time.[8] Newspapers are generic information--to my surprise, I discovered that all of the intelligence production which I reviewed was in fact nothing more than classified information. We have a long way to go in changing the day to day relationship between intelligence consumers and intelligence producers, and their capabilities, if we are to actually begin routinely producing intelligence which is useful to the policy-maker--that is, intelligence which can support decisions on a daily basis rather than by exception.

My second finding, the absence of a model of analysis, caused me to develop the model described below for our analysts--I did this for a very important reason, which is that *the threat changes depending on the level of analysis.*

The most fundamental flaw in both intelligence and information today is the failure to establish, for each question, the desired level of analysis. There are four levels of analysis: strategic, operational, tactical, and technical.[9] These are in turn influenced by the three major contexts of inquiry: civil, military, and geographic. At the strategic level, civil allies, geographic location, and military sustainability are critical. At the operational level, civil instability, geographic resources, and military availability are important. At the tactical level, civil psychology, geographic terrain, and military reliability determine outcomes. At the technical level, civil infrastructure, geographic atmosphere, and military lethality are the foundation for planning and employment.

A simple example from the military sphere will illustrate the importance of this issue. Examining the capability of specific Middle Eastern country in the mission area of tank warfare, it was found that while the initial threat assessment (by someone unfamiliar with the

[8] My most detailed work in redefining intelligence, funded by a European Ministry of Defense, is my white paper, *ACCESS: Theory and Practice of Intelligence in the Age of Information*", 26 October 1993.

[9] Edward N. Luttwak, *STRATEGY: The Logic of War and Peace* (Belknap Press, 1987). The author rendered an invaluable service to all intelligence and defense professionals when he created this extraordinary work. His discussion of how different combinations of weapons systems and tactics have varying levels of effectiveness with considered at different levels of analysis and in relation to one another, is useful and thought-provoking. The remainder of the model is original to myself. A fully developed report, including definitions of high, meidum, and low degrees of difficulty for the various military mission areas is available in my "Expeditionary Environment Research & Analysis Framework & Model 1990" (USMC Intelligence Center, 21 May 1990).

levels of analysis approach) was very high because this country had a great many modern tanks, in fact the threat varied significantly depending on the level of analysis. Only at the technical level (lethality) was the threat high. At the tactical level (reliability) the threat was in fact very low because the crews were not trained and had poor morale, and the tanks were generally in storage and not being maintained. At the operational level (availability) the threat increased to medium because there were large numbers of tanks widely scattered over the country. At the strategic level (sustainability) the threat dropped again to low because it would be almost impossible for this country to carry out extended tank warfare operations, even on its own terrain. It merits comment that the above simply examines the threat from a military capabilities standpoint. When integrated with civil factors (such as bridge loading and tunnel clearnance) and geographic factors (such as cross-country mobility and line of sight distance) the threat changes dramatically depending on the specific area of operations and the scenario. *This is why no intelligence product can be considered truly useful unless it reflects both an appreciation for the analysis model, and the specific scenario and decision being faced by a specific consumer.* This approach can and should be applied to every question for which intelligence--tailored information--is to be provided.

Our challenge is to thoroughly integrate classified intelligence, private sector open sources, and the information available to policy-makers and to do so in a way which recognizes that we must provide *decision-support* at multiple levels of analysis.

## NEW FORMS OF VIOLENCE: Challenges for Intelligence

I will not spend much time discussing new forms of violence because this has been so well covered by other speakers. The four main categories I focus on are Socio-Cultural Outcasts; Information Terrorism; Information Crime; and Economic Competition. What I find most disturbing about all four, as implied by our earlier comments, is that the intelligence community of today is not trained, equipped, and organized to detect and monitor these kinds of threat.

I am especially concerned by the fact that we have created for ourselves an enormously complex techno-sphere which is completely vulnerable to *anonymous* attack by dispossessed individuals who are willing to resort to information terrorism or information crime, and at the same time, this techno-sphere is very vulnerable to penetration, distortion, and destruction by those who choose to resort to methods of economic competition which many might consider to be illegal or immoral. On this note, let me make two points:

First, I admire Professor Samuel Huntington's life work, including his recent article on "The Clash of Civilizations"[10], but I am of the opinion that while civilizations may clash

[10] While I agree with the cultural focus of Professor Huntington, I think it is also useful to add the agricultural-industrial-information focus of Alvin and Heidi Toffler, with their

in epic terms, normal clashes today is between people as manifested through organizations. Today, as Trotsky would say, we have neither war nor peace, and we have, within civilizations as well as between civilizations, *clashes between forms of human organization.* The state, the corporation, and the gang are all vying for control of resources, and it is a cause for concern--and a legitimate mission for the intelligence community--to understand that today transnational gangs have more power, money, and computers than most corporations, and most corporations have more power, money, and computers than states, *in their chosen area of dominance.* This is increasing the chaos by fragmenting the battlefield, and aggravating external diseconomies that were once at least marginally addressed by the state.

Second, I have been impressed by an emerging literature on "national attractiveness", and have been persuaded that nations do not compete--organizations compete. It is the role of nations to provide for the best possible environment within which to develop and protect intellectual capital. As our own Secretary of Labor Robert Reich has noted, in introducing his concept of the American Workplace, he now defines "U.S. citizens" as any person or organization, *regardless of nationality*, which employees people within the borders of the United States of America, and/or which pays U.S. taxes. This is important. This means that nations "compete" by being attractive, not by undertaking campaigns of economic espionage or by subsidizing their "national" industries. In essence, nations within a global economy should be striving to attract the most talented people and the most original ideas, with the result that "virtual nationalization" of foreign intellectual capital takes place. I find this an intriguing concept, and believe that one of the missions of the intelligence community of the future will be to identify emerging talent and emerging opportunities, and to also identify the necessary incentives which would cause that talent and those opportunities to choose France--or whatever nation--as a home base.[11]

## EARLY WARNING:
## Virtual Intelligence Communities

I have deliberately emphasized the critical descriptive aspects of diagnosis and structural imbalance in this presentation because the hardest part of preparing for the 21st Century is admitting our own deficiencies. There are too many apologists for the existing U.S. intelligence system who persist in believing that everything is fine, that with just a few minor adjustments the existing capabilities can accommodate any threat. I suspect that most

books *PowerShift: Knowledge, Wealth, and Violence at the Edge of the 21st Century* (Bantam, 1990), and *WAR AND ANTI-WAR: Survival at the Dawn of the 21st Century* (Little Brown, 1993).

[11] A representative and leader of this school of thought is Professor Lars Oxelheim, "Foreign Direct Investment and the Liberalization of Capital Movements", in a book which he edited, *The Global Race for Foreign Direct Investment: Prospects for the Future* (Springer-Verlag, 1993).

countries suffer from a similar obsession with the *status quo*. This conference, and the two related events that I mentioned in my introduction, make it clear that France has begun the process of revelation and reinvention, and this is encouraging.

There are four key points that I would make with respect to establishing early warning capabilities for the 21st Century.

First, if we accept that "central intelligence" is an oxymoron in the age of distributed information, then it follows that the ultimate intelligence community in the 21st Century, the most effective intelligence community, will be that community which mobilizes every citizen, every employee, to create a Virtual Intelligence Community. If threats emerge from chaos and must be dealt with in "real-time", then only a total mobilization of all citizens as voluntary civic sensors, will enable the national intelligence community to receive warning and develop estimates in time to respond appropriately and with accuracy. I would emphasize the word voluntary.[12]

Second, if voluntary citizen sensors are to be effective as part of a virtual intelligence community, then it is absolutely essential that the state declassify the threat. In the United States we have concealed from the public the terrible risks to our entire financial, power, and telecommunications infrastructures, and this significantly increases our vulnerability as well as reduces the likelihood that innovative solutions will be communicated from those who are not aware of the desperate need for improved security in these areas. In the more traditional areas, such as transnational crime, proliferation, terrorism, and drugs, there is a need for greater openness on the part of the state with respect to its concerns and its limitations.

Third, and a corollary to the first point, at the same time that we mobilize citizen-sensors, we must also harness the distributed intelligence of the nation. It is impossible for any government--or corporation for that matter--to maintain a cadre of experts on every topic, especially when the topics of interest change from day to day. Only by organizing an intelligence community which can draw quickly and with confidence on university experts, business experts, media experts, and others, can we create a Virtual Intelligence Community which is truly comprehensive in its understanding and its ability to analyze threats as well as opportunities in real-time. Today, the U.S. intelligence community suffers from extremely unwieldy and inflexible security constraints as well as procurement arrangements that do not permit individual analysts to deal directly and frequently with experts in the real world. This must change.

[12] I did a paper on torture once, and was intrigued to find that you can torture someone to tell you what you know you want to know, but you cannot torture someone to tell you what you do not know that you need to know. In a complex world where threats cannot be anticipated, the civic sensor system must be voluntary, or it will not be effective.

Fourth and finally, I wish to emphasize what I perceive to be a critical change in the nature of defense and law enforcement as the threat of general war with high-tech brutes recedes, and we are confronted with much more pervasive, relatively anonymous threats from ruthless, fanatical criminals, terrorists, ideologues, and criminal hackers. I believe that our national defense must be recast so that there is a seamless integration of defense options running from the streets of Paris to the heart of darkness in Burundi. It is no longer possible to isolate "local" law enforcement from national counterintelligence, and general police capabilities from paramilitary, special operations, and conventional force capabilities. At the same time, the intelligence elements of the law enforcement, defense, and civil policy communities must be integrated, for there is too much overlap. Carrying this idea to its logical conclusion, and mindful of the fact that in the 21st Century most of the conflicts will be between states acting in coalition against non-state actors such as transnational criminal gangs or rogue Third World gangs tormenting those unfortunately enough to be within their borders, I suggest that we must move quickly to create a Virtual Intelligence Community which is transnational in nature, and which utilizes open source intelligence as the general foundation for integration.

## PREVENTION & ACTION:
## National Information Strategies

To conclude my presentation, let me describe what I believe are the four essential elements of a National Information Strategy--without such a strategy it is not possible to create a Virtual Intelligence Community, and without such a strategy it is not possible to provide for the defense and prosperity of the Nation in the 21st Century. The four essential elements of any National Information Strategy are Connectivity, Content, Coordination, and Communications and Computing Security.

In my view, the existing national efforts to provide for *Connectivity*, of which the Global Information Infrastructure (GII) and National Information Infrastructure (NII) initiatives are good examples, are good efforts, but severely limited for they are focusing on tools rather than content. Connectivity without content is nothing but digital noise.

It is a fact of life that organizations today have no incentive--and many disincentives--for sharing with others the unique *Content* that they have developed for their own program. To take universities as a simple example: it costs money to allow the public to log-on and access university databases, and it increases the risk of damage to files from hackers or others who wish to play and may cause inadvertent if not deliberate damage.

Therefore, I believe that the government should provide incentives for all elements of the information continuum (K-12, universities, libraries, businesses, information brokers, media, government, defense, and intelligence) to put content online. Just $1 billion a year invested in this program could yield enormous productivity and competitiveness gains across any Great Nation's private sector. Within government, it is necessary to dramatically accelerate the structuring and digitizing information now in the possession of the government but not available to the public. What I would emphasize here is that the incentives will be very cheap because they need only address the marginal cost of additional access, not the full cost of creating and maintaining a cadre of experts and their data--this cost is borne by the original institution.

There are two major aspects of *Coordination* where billions can be saved each year. The first is with respect to functional requirements for information technology, and the standardization of applications within organizations, industries, and the Nation as a whole. I am constantly astonished by the enormous waste I see, where billions of dollars are wasted by different organizations building variations of exactly the same workstation. Within governments, I see each department, and within departments, each bureau, spending millions for different or duplicative information technology capabilities. The lack of coordination becomes even more serious when one considers the complete absence of communications and computing security standards.

It is not safe today to work and play in cyberspace. One important U.S. government organization intercepted all hardware and software reaching its loading dock within one year, and it found 500 different computer viruses *within shrink-wrapped products coming directly from the factory*. This is unacceptable. The communication and computing industry today is not criminally negligent only because there is no body of law which requires them to provide safe products and safe services. With standards, and testing and certification laboratories to assure the public and business consumers that communications and computing security standards are being met, significant cost savings and productivity improvements can be achieved.

Finally, the forth element: *Communications and Computing Security*. The vulnerabilities of our national telecommunications infrastructure to interruption of services as well as destruction, degradation, and theft of data are such that experts feel comfortable in predicting that we will see a series of enormously costly electronic attacks on our major financial and industrial organizations, generally undertaken by individuals who stand to benefit financially from degraded or interrupted performance.

The current generation of systems engineers was not raised in an environment where security was a necessary element of design. At every level, through every node, we are wide open--and in a networked environment, one open house contaminates the next. For this reason, I believe that one important initiative must be the legislation of "due diligence" standards which require that the communications and computing industry adhere to standards (most of which have not been established and need to be established quickly)--at the same time, corporate managers must be held accountable for ensuring adequate security for the proprietary information stored on electronic systems, information upon which corporate profits depend. I anticipate a wave of lawsuits in the next five years, as stockholders realize that managers are not protecting their electronic information, and managers realize that they are not receiving "safe" products and services from the industry.

The above four elements, like the four pillars of a building, must be developed and maintained together, or the National Information Strategy will not succeed. Such an integrated program could be established using existing resources. The cost savings from the elimination of redundant and counterproductive investments in information collection and information technology across government departments and into the private sector can also make a substantive difference against the deficit.[13]

## CONCLUSION: Smart Peoples + Dumb Nations = Bad Business

In the United States of America today, we are a smart people, but a dumb Nation, and this equates to bad business. Our national security and our national attractiveness as a site for international investment which permits our citizens to prosper are both at risk. We have no alternative but to completely redefine the role of government to emphasize its responsibility for the nurturing of our national information commons, and to redefine national intelligence so as to create a Virtual Intelligence Community in which every citizen is a collector, producer, and consumer of intelligence--to do this, we must have a National Information Strategy. I believe that France, which is clearly exploring these concepts through its discussion of a national economic strategy, can benefit from considering the above views.

I will conclude by noting that whatever friction may occasionally exist between our two Great Nations, it is not possible for any educated American to forget that our country exists because France supported our Revolution. Now, as we face chaos and anarchy together, surrounded by mobs and gangs with powers of destruction and disruption once reserved for Great Nations, it is critical that we each have a National Information Strategy, that we each have a Virtual Intelligence Community, and that we strive to achieve common cause--in the 21st Century, warfare will be largely between those who are civilized and those who are not--in this war--a war that is underway today--France and the United States must be the closest of allies.

Thank you for welcoming me to your forum.

[13] One authority, Mr. Paul Strassmann, estimates that $22 billion over seven years could be saved by the Federal government of the United States of America in information housekeeping costs alone. This is apart from policy savings derived from improved intelligence support. Mr. Strassmann has been Director of Defense Information and Chief Information Officer of the Xerox Corporation and other major companies. His books, including *The Politics of Information Management*, *The Business Value of Computers* and *Information PayOff* are all exceptional.

# OSS '96: THE CONFERENCE Proceedings, 1996 Volume II, Fifth Internatinal Symposium Global Security & Global Competitiveess: Open - Link Page

|  |  |
|---|---|
| Previous | Mr. Mark E. Donnelly, National Security Studies Program, Georgetown University, Open Source Intelligence in the Information Age: Opportunities and Challenges, 28 November 1995 |
| Next | Mr. Robert D. Steele, Open Sources and the Virtual Intelligence Community, Invited Presentation to the Annual Meeting of the U.S. Intelligence Community's Advanced Information Processing and Analysis Steering Group, March 1996 |

**Return to Electronic Index Page**