

# VIRTUAL STATES AND NATIONAL SECURITY: A TIME FOR REAPPRAISAL

by **Stephan A. Schwartz and John B. Alexander, Ph.D.**

**S**ince the end of the Cold War, scenarios which attempt to predict the threats to America's national security seem to recognize that, from the ashes of the old bipolar world, a complex multipolar geopolitical phoenix has emerged. But, upon closer examination, the first premise of almost all such analyses continues to be the nation-state as the overriding factor in international calculations. It is a concept so hallowed by time and tradition that it is almost invisible as a topic for discussion. But is it a premise that is still valid? Is it other nations we most have to fear?

The answer to that question is one of the most important things we can know about the future, because it will dictate how a large portion of our national resources are allocated. As a partial list, the budgets of the State, Defense, Commerce, and Agriculture Departments, as well as a multi-billion dollar stream of decisions in the private sector must all be predicated on this answer. If nation states are not going to be the *principal* threat, or are not going to be threats in traditional ways then policies, and organizational structures, need to be developed reflecting this new reality. Looked at this way, one factor arises above all others.

Every knowledgeable authority now accepts that terrorists are capable of bringing the battle to us. What has not emerged from the post-mortems of their attacks is a coherent sense of what these attacks really represent. We believe a new category of social entities, the "Virtual States" is emerging. We call these new entities "virtual" because although they are not tied to geographical boundaries, like nations they have a culture, can even be multi-cultural, have a political structure, assets, both material and human and, like traditional nations, and unlike traditional internal organizations, such as unions, they represent an extra-national and autonomous political point-of-view tied to a unifying common core, be it technological, economic, ethnic, or religious. Virtual States, like their landed counterparts, are capable of making nation-like strategic alliances, and often have the means and the capacity to cause serious harm to our national interest, sometimes in ways for which, at present, we essentially

have no defense. Some, like the Palestinians, as was true of the Jews before them, have passionate aspirations of attaining landed-nation status.

**C**ertain classes of Virtual States are obvious, well known, and historical. In the licit economic sphere, for instance, transnational corporations, and their relationship to governments, have always held a potential for conflict arising from differing agendas. However, as this new world order emerges tensions will intensify as transnationals become increasingly global, with corporate interests accordingly less tied to any given nation state and more purely Virtual. The unasked question is: What effect will this have on the individual? The probable answer is that, like the hierarchy of the Roman Catholic Church, in the next century the personnel of these Virtual States will hold concurrently both national and *de facto* Virtual State citizenship. It is worth asking, and facing the answer realistically, how long before an individual's Virtual allegiance takes precedence over their national citizenship, particularly when there is no overt penalty for selecting the former over the latter? In the political arena, terrorist organizations such as various Islamic fundamentalist groups, and the IRA, suggest what this might mean.

In the illegal economic sphere cartels and other black market operations aided by the new technologies are evolving from mere organizations into Virtual States. Although they are ceaselessly tracked by governments and covered by the media, and tens of millions of dollars have been spent on the most advanced intelligence our government is capable of bringing to bear, has any of this reduced this shadow free market? It has not. And, then, there is the Internet itself, an entirely new, and barely understood, Virtual State phenomenon. One thing is certain though, cyberspace is the milieu in which Virtual States will have a significant part of their existence. While it is too soon to tell if the Internet is merely a resource employed by groups to facilitate creation of Virtual States, or itself acts as such an entity, the impact of this new communications medium has been profound, even at this early stage in its development.

Judging by what has been written and said in public debate, however, with rare exceptions such as Vice President Gore's book, and a recent article in *Foreign Affairs*, few in the U.S. national security establishment seem to regard the Internet as a major factor in national security. For example, based on their writings, none of the masters of Cold War geopolitical thinking seems to have made the transition into the Information Culture. It is ironic that this should be so given the Internet's antecedents. The Defense Advanced Research Projects Agency which created the DARPA Net, the progenitor of the Internet, did so as an act of national security planning. They gave the net the structure they did because it was the one most capable of surviving that ultimate national security challenge -- nuclear war. No ones seem to have anticipated that the net's packet

transmission protocols would provide the nervous system for an electronic global democracy.

Perhaps this lack current debate over the net's national security role results from the fact that the Internet's sexual content was such a focus of attention providing, as it did, a convenient cheap target in an election year, that electioneering obscured the deeper implications. But they are still there, and to understand the real paradox they pose one must look to countries such as China, cultures which place a high priority on the state's control of the individual, even as they seek to be technologically competitive.

China clearly considers cyberspace a significant factor in its future, although the mindset of centralized control that pervades Chinese governmental thinking appears not to recognize that the Internet and obsessive control are incompatible. They are attempting to create an internal Chinese Internet with limited connections to the greater world net, not realizing that, as technology continues to develop, this will become more and more infeasible. Iran is another example of an obsessive traditional landed-nation power structure struggling to deal with emerging Virtual State forces. Iran restricts private ownership of television satellite dishes in an attempt to control information or its interpretation (the Iranian press reported the Million Man March as a "Million fundamentalist Muslims marching on Washington"). As in China, however, the price of control is loss of competitiveness.

**I**n an age in which progress and profit correlates with access and speed of information transfer, stifling communication freedom in any way results in such a loss of innovation and informational efficiency that a society once fallen behind may never be able to catch up. It is not so much the machines, these can always be purchased. It is the *culture* of information that is stunted. Once it is wounded the time needed to heal the distortions and create a healthy information culture must be measured in decades. As the legacy of the Soviet era makes clear, crippling information flow has left the Russians a step behind and vulnerable. The Information Culture is developing and changing almost daily, and those who fall behind, or harm themselves through self-inflicted injuries, may be doomed to perpetual catch-up. If national security is defined as the ability to defend our national interests then the Internet may prove to be a more significant factor in national security calculations, not only in the U.S. but in countries around the world, than any terrorist organization.

The Internet in and of itself though is only one aspect of the cyber-revolution to consider. It is when it links not just individuals but other states, both landed and Virtual, that its greatest importance for national security comes into focus. It is one of the organic unintended outgrowths of the increasing globalization,

between media, data exchange, and financial structures that Virtual States represent potential challenges to our national security that are growing in importance, even as the threats from traditional nations decrease. This is precisely because of linkage proliferation. It is an historically novel development involving all the power centers of our technological culture: government and politics, science and technology, business and economics, media, religion, and the arts.

Nation states will, obviously, continue to be major factors in our national security evaluations. But they, too, have changed. The challenges they represent have already been affected by the same forces that have given rise to the creation of the Virtual States. Meta-national organizations such as the European Union are one example. They differ from earlier treaty alliances precisely because information technologies allow both a density and speed of linkage literally impossible just a few decades earlier. Similar structures could arise in Asia or through a united Western Hemisphere, and present threats that do not fit the neat bureaucratic categories of State, Defense or Commerce.

**E**ven the most traditional and dangerous rogue nations, countries like Libya, Iraq, and North Korea are altered by the new environment. Each possesses conventional armed forces, a potential threat which require us to maintain a highly mobile, extremely lethal conventional and nuclear armed military capable of projecting and applying force on a global basis. But is the threat from Libya really conventional war? It seems hardly likely. What is much more probable is a linkage between a traditional landed state and a Virtual State, in which the latter provides the soldiers for the former, in a campaign of shared interests. Would a military force designed for army-against-army wars be the appropriate instrument to deal with a team of Japanese hackers hired by Arab fundamentalists committed to bringing down America's banking system?

It is time to rethink the entire concept of national security. Just as the Department of Defense evolved from the War Department, and the War Department evolved from earlier individual service fiefdoms, America should now consider the next metamorphosis. What should emerge might nominally be a Department of National Security. This would not be the DoD renamed, but a very different structure; one which included elements and functions currently assigned to the departments of State, Justice, Treasury, Energy, Commerce, the Intelligence Community, as well as other agencies like the FCC. Indeed, with the creation of a Department of National Security some or all of these departments and agencies might disappear, just as many in Congress hope, albeit for different reasons.

The Department of Defense was defined by the Cold War. World II -- which saw the creation of DoD, and its home symbol the Pentagon -- compelled planners to focus on technology and a more integrated infrastructure. A hybrid of the military working with the civilian industries created to support it, DoD was designed to operate with a closer coordination of elements than had ever been seen before. The planners of the day realized that such coordination was the only way to wage and survive both modern conventional and nuclear wars.

The policy expression which drove DoD, a National Security Directive known as NSD 68, was written by Paul Nitze and his colleagues, shortly after the end of World War II, and it set forth the policy of deterrence and confinement that has dominated national security analysis ever since. The vocabulary of NSD 68 was nuclear. Armageddon, in the form of atomic warfare, had entered the national debate, intimidated public consciousness and, for the first time since the Civil War, made national survival a topic for discussion. While the U.S. maintained a large conventional force capable of waging those most traditional of military enterprises, massed armies at war on land, while fleets confronted one another at sea, it was the strategic triad comprised of long-range bombers, intercontinental ballistic missiles, and nuclear missile carrying submarines that constituted the crown jewels of the newly configured national defense.

**W**ith the end of the Cold War, however, we are now on the other side of NSD 68, even as the global technological advances that gave it birth, have evolved to create a new order of threats. The good news is that in the 1990's national survival is no longer considered a serious issue. It is in the interests of both Russia and the U.S. to continue disarming their nuclear weapons, and it is even more difficult today, than in earlier decades, to imagine a conventional attack on the land mass of the United States. Even limited strikes by weapons of mass destruction, or a terrorist attack involving a nuclear device, while extremely damaging to the impacted area, would not be sufficient to threaten our national viability. But, that good news aside, national security planning has actually become more, not less, complex and dangerous since the end of the Cold War and it, now, operates under different rules.

The same technology that created the Virtual States also allows instant public communications, and has created the "CNN Effect", something which has proven to be worth many divisions in the field. In the aftermath of Viet Nam, we have learned, or at least it is a political belief (arguably a mistaken one), that America's civilian population will not tolerate the violent death or even injury of its armed service personnel at a scale even as great as the weekend murder rate in some large American metropolises, or the death rate due to traffic accidents. Instant communications serve to reduce the boundaries previously enforced by geographic distance. It makes issues, such as human suffering, more personal, and markedly reduces the power of a bureaucracy to define what constitutes

national interest as the pictures of a dead American serviceman being dragged through the streets of Mogadishu brought home with sickening clarity.

The perception that technological war while devastating to our opponents should be free of American casualties, a cousin to the contemporary assumption that medical technology should be error free has also become a powerful factor in national security planning. So powerful, in fact, that Army Chief of Staff, General Gordon R. Sullivan recently told Congress, "The expectations are so high in this regard -- it's so troublesome." To be possible, wars involving U.S. armed forces today must be quick and essentially bloodless in terms of American forces. But instant media coverage has produced other unintended consequences as well.

**A**mericans do not like to see images of mangled children on their living room television screens, no matter what their nationality. For America, war in this age must be fought from a distance both geographically and emotionally. Desert Storm is the prototype of this new conflict, with less than 200 American dead (some killed in mundane accidents that could just as easily have occurred in New Jersey as Iraq), and smart bombs that killed like video games, with never a picture of a human face. The conditioning produced by prolonged exposure to electronic media also dictates that when wars hold the potential to become intractable (read more than a year), and sanguine, it requires a wrenching act of will to commit troops to go in harm's way. It is a measure of the power of the "CNN Effect" that this is true in spite of the fact that every single man and woman in uniform is a volunteer and each knew they might one day have to put their life on the line, and willingly signed up to do so if asked. Bosnia has been the case study.

This political reality, as we saw in Somalia, operationally has meant that clan chieftains whose most potent weapon is the Toyota mounted machine gun have more effective power than their guns alone would suggest. These leaders may be primitives when it comes to the new technological warfare, but they are highly sophisticated about evaluating the psychology of the United States, and they know the public debate over the use of American armed force may be one of their strongest allies. One other aspect of the new national security situation also deserves consideration. The same instant communications that limits policy for fear of images of death, also telegraphs our punch long in advance of its arrival. The democratic process whereby America commits its armed forces is so passionately, publicly, and globally debated, thanks to the new information technologies, that there are few surprises at the end.

Enemies have learned though -- coverage of Desert Storm trumpeted the lesson around the world -- that it is not wise to confront the United States with a definable military threat. This will not change their goals, nor reduce their

hatred of us, however, and it is reasonable to assume that some adversaries, particularly Virtual States, will develop more insidious methods of attack. In the future, those seeking to do us harm, will probe in veiled ways, consciously staying below our public pain threshold even as they avoid alienating U.S. public sentiment, in another variant of the “CNN Effect”, by doing something that would put unpleasant pictures on television. This deterrent effect, however, is much less potent than images of American dead, as the muted response to the genocide of Rwanda demonstrates.

**S**mart enemies, and Virtual States by definition require sophistication in a variety of spheres, will study our institutions. They will exploit discontinuities in our inter-agency and departmental organizational structures, take advantage of our open society, and use our legal system to their advantage. Like professional football pass receivers, they will run their patterns in our defensive seams. To counter these threats we need to develop a structure that can seamlessly accommodate a wide variety of circumstances many of which, like Bosnia and Haiti, are not quite military nor yet wholly peace keeping or humanitarian. The current DoD term for such missions is “operations other than war,” a phrase that reveals the problem of trying to fit old forms with new functions. “Operations other than war” clearly suggests that these tasks are still viewed as a kind of adjunctive, ad hoc response when, in fact, they are increasingly the most likely national security expression of the armed forces.

As the Congress and the Executive Branch wrestle with downsizing government, establishing a Department of National Security may be the most cost effective and efficient option they could exercise. The real need for the next century is even further integration of functions and organizations, and the development of a policy expression to replace NSD 68. This entails redefinition of the meaning of national security, and dramatically alters the organizational structure required to meet the new needs. Many “rice bowls” are at stake and some will be broken. The transition will not be easy, but it must be undertaken.

A pivotal question in deciding how to create a Department of National Security lies in defining what is at stake in regards to national interests. In previous eras, wars have been fought over territory for control of resources. In most cases the resources, be they wealth, energy, or people, had physical attributes such as gold, oil, or geographic location. While this is still true, as the Gulf War demonstrated, one of the effects of the globalization of both public and private sector interests has been the rise of information as a commodity essential to the functioning of the modern state. As the flow of wheat ruled the ancient world, and oil has ruled the 20th Century, so information appears poised to rule the 21st. It is a perspective still not integrated properly into national security considerations.

Very few politicians, and only a few futurists such as Alvin Toffler and his wife Heidi, (in their recent book, *War and Antiwar*) have addressed the reality of information warfare. The armed services themselves actually lead the way and have begun establishing units specifically charged with understanding the implications of this new paradigm, and figuring out how to operate in this new environment. The problem is that information warfare is not inherently an exclusively military issue and, for this reason, traditional military organizations are not the best way to cope with its threats.

In another recent book, *Debt of Honor*, Tom Clancy in the best tradition of fiction presaging the future, describes what an information attack might look like; in this case a strike against Wall Street. While the IW attack in Clancy's novel is a bit simplistic and limited in scope, it does begin to describe the interrelationship between economics, cyberspace, and national security. Most particularly, Clancy recognizes two central aspects of this new kind of warfare: A Virtual State can manipulate a government through information, and its attack need not be direct or overt, but can be accomplished by using other nations or entities as surrogates working, even unknowingly, on behalf of the Virtual State's aggressive intent.

**T**he central weakness of the Information Culture is its almost crystalline fragility. These transactions are not physical in the same way as such things have been during all the course of human history, no clay tablets, parchment, or paper need be involved. They are moving electrons and, therein, lies their weakness. To the vulnerability posed by viruses, electromagnetic pulse, hacker attacks, and other 21st Century tactics must still be added the more traditional physical attack. While that historical entity, the suicidal terrorist prepared to die for his cause might not threaten our nation's existence, one armed with a nuclear bomb in a suitcase could make it possible for a Virtual State to attack the global linking technologies (satellite transmission, faxes, computers, international electronic banking, as examples) at core points such as a world financial center with a result that was both devastating and long lasting. It is a terribly tempting option since it can be effected at very low cost, involving very few fighters (thus hard for intelligence agencies to detect).

The recent reports of meetings between Minister Louis Farrakhan and Khadafi, which were said to include discussions of recruiting African-American men into an underground Black army, are an example of possible alliances between a Virtual State (Farrakhan's vision of a Black state) with a rogue national government (Libya). The recent televised confession on *60 Minutes* of just such a "hit man", an army veteran now living in Iran who was responsible for the murder of an Iranian opposition leader in Washington, D.C., gives weight to this national security concern. The point here is not that the people involved would

be Black, but that disaffected individuals from any group, who feel they have no investment in the established society, can wreck havoc in ways that extend beyond their immediate geography, thanks to the interlinking that is the hallmark of the global Information culture.

**R**ecent terrorist strikes in Jerusalem, by the Islamic group Hamas, exemplify the problems associated with applying force against these shadowy Virtual State opponents. Hamas is not an organization in the traditional sense. Rather it is a collection of cells structured intentionally, as is the IRA, to keep separate its military, intelligence, political, and social welfare functions. This is possible only because of the revolution in communication technologies and the power they confer to move information around securely and anonymously. When the democratic State of Israel sought to respond to the threat from Hamas they closed borders, enforced curfews, and employed retribution (destruction of family houses) as a means of deterrence. All acts which have created stress on their democratic institutions, and caused enormous civic unrest.

Lest anyone feel it would be different in the United States consider what happened after the Oklahoma City bombing. We saw an instant hue and cry for greater flexibility in countering terrorism that translated into proposing laws to allow law enforcement agencies additional powers in data collection (wiretapping, net-tapping) as well as search and seizure. In March of this year, the U.S. Supreme Court, in response to another perceived terrorist threat, this one having mostly to do with drugs, upheld the right of police agencies to confiscate private property even if the owner was not involved in the commission of a crime. These seizure rules, although seen as Constitutionally justified by the Court, in the popular mind reverse evidentiary procedures previously seen as basic rights. Many believe such decisions to be an abrogation of Constitutional protections afforded citizens under the Fourth Amendment because they presume the innocent to be guilty until they prove otherwise; a Herculean task that often destroys lives and families in the process. Already such interpretations are causing fraying and tears in the cloth of our democratic society. Seizure is one of the main grievances of the militia movements, and there is evidence that these laws, while intended to confiscate the ill-gotten gains of criminals have, in some instances, been used by police agencies to buy new computers, squad cars, and to redecorate station offices. It is behavior remarkably reminiscent of police states the world over, and it is further eroding an already diminished citizen confidence in the government.

Virtual States are eroding more than civil rights. Because they exist outside the traditional boundaries of geography, one of the central challenges they pose is to the traditional yet, now, increasingly artificial division between things foreign and domestic. We allow, for instance, intelligence operations on foreign soil that

would never be permitted internally. Given the nature of transnational threats posed by Virtual States, however, such operations may be essential to mount a defense. Yet little in the public debate on defense planning recognizes this, and the Congress seems remarkably obtuse in not comprehending the tremendous complications which such defenses pose to a democratic state -- perhaps because many members are from an older generation that has not integrated the new technologies into their daily lives. Failure to think through these issues could result in a situation in which the inherent rights that are the foundation of a democratic state are destroyed in the process of defending it; essentially the Viet Nam cautionary tale of destroying a village to save it writ large. What an irony it would be if the defense against an attack from an adversarial Virtual State resulted in an uprising of civil disobedience that accomplished much of the Virtual State's goals.

Similarly, there is a need to rethink operational activities that cross-boundaries now considered inviolate. *Posse Comitatus* is the law that proscribes the use of Federal forces in domestic situations. In recent years we have observed the undermining of this concept; indeed, some have argued that this is the fountainhead from which has sprung the militia movement. We need to consider where lines should be drawn between surveillance operations, advising local police, and active participation in arrests. In the Drug War, all have been employed, and laws stretched if not broken.

**T**his leads to an even more fundamental question that we as a nation must address in our re-evaluation of national security: "Who are we?" This is not a new issue, but in an information-intensive era the answer is changing. Just as information has allowed corporations to slip their national moorings, so the Internet is creating a kind of cyber-citizen, with cyber-citizen perspectives, as the recent worldwide response to Germany's attempt to censor the net demonstrated. This is a trend that will only intensify as the Information Culture matures. The traditional delineating factors determining who is "we", and who is "they", were previously based on nationality, ethnicity, or religion. In the world that is evolving one's ability to access cyberspace, and be at home in that electronic dimension, or one's allegiance to a corporation or a special interest group may turn out to be more important than any of those traditional affiliations. And we are speaking here of law abiding men and women, not terrorists, or political fanatics.

The definition of patriotism most of us were taught is really a creation of World Wars I and II. When the country was founded, most people defined themselves by what they saw as their "home" state, and they often felt quite passionately about this. As late as the 1860s, Robert E. Lee, a serving army officer and a man universally respected for his integrity, felt his allegiance to the Commonwealth of Virginia took precedence over both his oath of service to the

Union and his citizenship as an American. To this day, people in certain regions of Europe, for instance the Basque in Spain, place regional associations above national obligations.

**I**t should not surprise us, then, that as the organizing structures of the technological states become more global that patriotism will, once again, be defined differently. It is not clear how this will develop but, in America at least, it is already obvious that the single unifying vision that informed the development of most people over the age of 45 does not have the same currency it once enjoyed. In fact, as the O.J. Simpson trial, the Hispanic view of the Mexican-U.S. border, and the Western vision of “County Rule” makes clear, the belief in a single set of American values, an historically novel concept gestated by World War II, may be dangerously erroneous. Contrary to current political rhetoric and hyperbole, “American values” may prove remarkably hard to define in the coming century. In any calculation of national security this will have to be considered.

The new national security policy we develop must also not just look outward. With the largest penal gulag in the world, and one out of three African-Americans in prison, on parole, or under probation, how fertile are the fields of revolution in the U.S.? It is a sensitive and important question that is rarely discussed, perhaps because the answers we have arrived at in the past have proven so destructively wrong. As America in the late 40s saw fit to incarcerate Japanese-Americans for no other reason than their heritage, and in the early 50s experienced a kind of psychosis around the idea that there were communists in our midst, can there be any doubt that the wrong answer to this aspect of national security could result in a very dark period again? Rather than fear past mistakes, however, we must draw insight from these errors in constructing our new approaches. Equal rights for all, in an Information Culture, has greater significance than ever before, including becoming a significant component in national security planning.

We also need a new debate on another highly politicized and sensitive issue, The War on Drugs, is perhaps the best harbinger of what war with a Virtual State, using existing structures and strategies, is likely to resemble. The results, to date, are not promising. Like its licit cousin, the transnational pharmaceutical corporations that manufacturer psychiatric medications, the Virtual State of the drug industry (cartel is the wrong word because it creates the wrong image) is essentially involved with altering consciousness. The drive to experience such altered states, whether by legal pharmaceuticals, caffeine, nicotine, alcohol or illegal drugs is now recognized by most scientists as a biological given.

Like its legal Janus twin, the Drug Industry Virtual State meets the needs of its consumers through a complex international structure headquartered in several countries. Its agricultural operations and production facilities are spread across Latin America, and parts of Asia. Its distribution network has tentacles in every country, and every social institution, and its holdings are no longer entirely illegitimate. Court records show that billions of dollars have been funneled into perfectly legal business enterprises.

**M**ost daunting of all, the citizens of this Virtual State carry many different passports, including many blue ones with the seal of the United States on the cover. If the drug cartel was a landed nation traditional war would be a hotly debated option. But can anyone seriously imagine our invading Columbia, Peru, Bolivia, and Mexico in one coordinated campaign? It is a fantasy even the most hard-core drug warrior would find hard to advance. Therefore the options in force application available to the U.S. are limited to those mutually agreed upon by the U.S. and the resident nation where the force would be applied.

Even more fundamentally, the Drug War to date shows us that old structures and old strategy solutions don't work very well against Virtual States, particularly when the world consumer population profits from, or supports, their activity. Why after all should self-medication cease when prescribed psychiatric medication usage increases exponentially year by year? How can we wage war when we can not answer that question? Is war the proper response to this social reality in the first place? How long can a government make war against its citizens before there is a fundamental shift in the relationship between government and citizen? In the national security analyses of the 21st century we must be clear what is national security, and what is a problem for a different sector of our culture.

The Drug War also illustrates how not to construct a Department of National Security. Ill-conceived from the beginning, the massive drug war effort exemplifies the approach of trying to solve new complex problems using existing resources and structures. A "Drug Czar" was named and given responsibility, but little authority. Under his direction from the Office of National Drug Control Program, more than twenty Federal agencies were expected to coordinate all activities aimed at curtailing drug trafficking. Each participating agency respectively defined their role based on current missions and resources. No single agency was in charge and had the authority to direct specific actions. The Golden Rule prevailed. Each agency conducted their own budgetary affairs, and no one, except for limited Congressional oversight, could enforce allocation of resources. The end-game demonstrated that drug availability increased while street prices declined. Even worse, federal agencies like the Coast Guard, which had always had a primarily humanitarian

orientation, suddenly became law enforcement agencies, and worst of all, became dependent on the Drug War for budgetary justification. As anyone in Miami involved with this situation knows -- even if it is rarely admitted -- the drug interests and the law enforcement interests are locked in a ballet of mutual dependency.

**G**iven the multiplicity of structures with which we must interact, is the United States prepared and organized to meet the needs of future threats from Virtual States, be they terrorists, transnational corporations, or the illegal drug industry? Probably not. Why not? Principally because current planning assumes consistency, if not outright rigidity of our institutions. Rather than ask the difficult question, "Are we properly organized?", to date it appears planners are moving ahead developing options based on current, or expanded roles and missions for existing bureaucracies. This is not surprising since all institutions, in whatever country, exist, first and foremost, to serve themselves. History has shown conclusively that preservation of the existing status is their primary function, and attempts to substantively alter them will be met with unending resistance. Yet fundamental changes is exactly what must be accomplished.

Form follows function. This is an adage used to describe how things are developed and built. But it applies to bureaucracies as well as buildings, and manufactured items. Just as city-states evolved into nation-states, it appears that new social structures are emerging. We must develop policies and organizational structures that can accommodate, adequately, interaction with these new social structures; and we must do this while still protecting the rights of individuals and families that define our society. The challenges to our democratic republican way of life are changing. So too should our approach to national security.

\* \* \*

*Stephan A. Schwartz, is a former Special Assistant for Research and Analysis to the Chief of Naval Operations, editor of **Sea Power** Magazine, and Discussant on the MIT-Secretary of Defense Discussion Group on Innovation, Technology, and the Future. He is the author of two books, as well numerous magazine articles, and academic papers. For the past 16 years he has also been involved with first Soviet and, now, Russian-American Track II Diplomacy, and is a member of the Board of Directors of the Russian-American Center in San Francisco. He is currently at work on his new book, **Democracy at Risk**.*

## *Virtual States and National Security*

*John B. Alexander, Ph.D. a retired army colonel with combat experience as a Special Forces commander, recently left Los Alamos National Laboratory where he was a member of the Senior Staff. While there, he created the nonlethal defense concept, and chaired the Los Alamos working group on this subject. He is internationally recognized as the author of many of the fundamental papers in this new field, and currently serves as a U.S. delegate to NATO's working group on nonlethal weapons. He is currently the Director for Scientific Liaison to a private research institute in Las Vegas.*