the electric power system; gas and oil transportation and storage; transportation systems; banking and financial systems; water supply and sewage systems; emergency services, which include medical, police, fire and rescue systems; and finally the critically important systems that support continuity of government.

In part, the commission is to assess the scope and nature of the vulnerabilities of, and threats to, critical infrastructures; determine what legal and policy issues are raised by efforts to protect critical infrastructures; and assess how these issues should be addressed. Finally, the military services and many others in the information warfare community are seriously addressing the challenges of information age technologies, information age opportunities and information age vulnerabilities. Decision makers are grasping the importance of information as a realm, a weapon and a target of modern forces.

Priorities are changing. A senior officer in a foreign army wrote after the Gulf War that its principal lesson was that no one could challenge the United States on the conventional battlefield without the assistance of nuclear weapons. That's a serious concern, but it's also a doomsday scenario for the participants. Might it be more likely that a competitor or a hostile foreign power could arrange or contract for the destruction of a vital U.S. infrastructure service via an attack launched through cyberspace? Could a successful information attack threaten national leaders until an enemy's objective was achieved, particularly if national leaders were aware of the potential of the attack and the American people were not? Could an infrastructure control center be degraded or destroyed with attendant loss of an aircraft, loss of electrical power or loss of financial records? Information warfare is arguably the prevailing form of competition and conflict in the world today. Certainly unabashed force from terrorists or rogue nations remains a concern, but information warfare and information competition merit a full measure of study, a commitment of intellectual energy and increasing resources in the decades ahead.

Smart Nations: Achieving National Security and National Competitiveness in the Age of Information

by Robert D. Steele

Alvin and Heidi Toffler have eloquently articulated the importance of information as a substitute for time, space, capital and labor—and indeed as a proxy for violence. In the information age, only "smart nations" will be able to provide for the common defense, and only "smart nations" will be economically competitive and able to assure the prosperity of their citizens. Individual information specialists in the private sector—what Robert Carkhuff has called the gold collar worker—now comprise the armies of the future and also the spies of the future; it is the private sector information specialist who will bear arms, collect and produce intelligence, and generally be the foundation for creating the "smart nation."

Information warfare or IW is now very much in fashion, but as with so many other fads in American history, it is focused almost exclusively on developing enormously complex electronic architectures and on offensive attacks against others (many of whom do not have significant electronic infrastructures susceptible to electronic attack).

The current emphasis appears to achieve a patina of comprehensiveness through its variation of technique—one can talk of hard kills with physical means versus soft kills with electronic means; of irreversible damage versus reversible damage; of detectable versus undetectable impact; and finally of one-time versus sporadic or repetitive attack and impact.

In fact this focus is severely limited. Consider instead a larger concept, in which there are three critical aspects to waging war and keeping the peace in cyberspace: first and foremost, and completely ignored by most warriors, is the importance of intelligence—of knowing the environment, the enemy and the other players in depth so as to make informed judgments. In this area, open source intelligence—public information readily available to information professionals, comprises the bulk of the raw material. Second is electronic home defense. Finally, and least important in the overall scheme of things, is offensive information warfare. Missing completely from this equation, but perhaps occupying the entire inner space of the triangle...
formed by these three elements, is information peacekeeping.

These four elements of national defense and national competitiveness in the age of information—intelligence, electronic home defense, offensive information warfare and information peacekeeping—cannot be defined, established or managed in a vacuum. We urgently need a national information strategy which provides four pillars for meeting our varying needs in these areas: the pillar of connectivity or assured access; the pillar of content or networked distributed centers of expertise; the pillar of coordination to avoid wasted resources and enhance interoperability; and finally the pillar of communications and computing security, making it safe for all Americans to work and play in cyberspace.

**Five Revolutions: The Challenge of Change**

As we contemplate our present and our future, we cannot help but note that we face five revolutions, which I call the challenges of change. The first revolution is the dramatic increase in the complexity of the threat and the power of single individuals and small gangs to do great damage to the financial, power, communications and transportation infrastructure of the United States of America. Neither our Department of Defense nor our U.S. intelligence community is organized to address these new threats, and our local and even our national law enforcement agencies are overwhelmed and inadequately funded for this transnational threat.

At the same time, in a second revolution of changing demands, we see the Secretary of State properly declaring that the global environment is a national security issue; we see various forms of cultural and economic migrations, many inspired by stark terror imposed from drooling Third World thugs claiming the legitimacy of a uniform; and we see "war by other means"—deliberate industrial espionage and sustained electronic crime campaigns—undertaken against the United States of America not just by traditional enemies, but by citizens of its own allies, including Canada and Israel.

The third revolution is one of decline—a decline of people, platforms (vehicles to transport and protect military and law enforcement personnel) and of course, a decline of dollars. We are being asked to do more with less, but we have not figured out in the U.S. government, as yet, how to substitute information for people, platforms and dollars.

The fourth revolution is that of the changing knowledge terrain, with the global information explosion, and the emergence of smart non-state actors with more disposable power than most small nations. Finally, the fifth revolution, changing technology, has placed in the hands of rogue nations, as well as terrorists and criminals, vast arrays of extremely powerful yet inexpensive and easily concealable information warfare tools.

**Information Strategy and the Smart Nation**

Now then, in the face of these challenges, we are confronted with the urgent need to reinvent our approach to national security and to national competitiveness. As we consider trends in information warfare and open source intelligence, we quickly come to the realization that the two are related, and that a national information strategy is the umbrella under which we can optimize our resources and create a "smart nation."

In the age of information, each nation must not only be "smart," but it must mobilize all of its intellectual capital, i.e., all of its citizens and resident aliens, for total war. Only by mobilizing for total war can a total peace be reasonably achieved.

Electronic security and counterintelligence, now finally established by the President as the domain of the Federal Bureau of Investigation—something I proposed in 1994—must become a national priority. The threat must be declassified and the kinds of encryption and other tools for the protection of intellectual property released into the private sector.

Legislative initiatives are necessary in order to establish "due diligence" standards for the communications and computing industry, such that consumers can rely on secure communications pathways and computer products that are not infected—as 500 were found to be infected by one organization in one year—when delivered shrink-wrapped from the factory.

Open source intelligence or OSINT is now much in vogue after four years of global educational efforts on my part, but the reality is, as one Central Intelligence Agency person admitted a few weeks ago, "we have a working group, but no one is really doing anything." Worse, the beltway bandits have found that by claiming to do open source intelligence, but in fact by simply recycling their existing people and limited in-house libraries, they can win large contracts and muddle through without actually doing any serious international multilingual research. We are all losers when both our government and their major contractors fake it, but this is tantamount to abject surrender without a fight.

We have an information commons in this nation, and it unfortunately bears more of a resemblance to a large garbage pit than to a healthy field of dreams. Between outrageous and well-orchestrated campaigns to steal intellectual property, and the costs of maintaining adequate security while providing public access, we have encouraged the creation of an archipelago of isolated information resources which do not contribute significantly to the national intellectual foundation.

At the same time, we have one of the finest, deepest and most skilled range of individuals and organizations which comprise our national information continuum—our schools, universities, libraries, businesses, information brokers, media, government, defense and intelligence organizations are the world's best. Unfortunately, we have iron curtains between each of these nine sectors; bamboo curtains between each organization in each sector; and plastic curtains—generally hard to use technology or dumb rules—between individuals within organizations.

Our national security and our national competitiveness in the 21st century will depend on our ability to clean up and nurture our information commons and our ability to break down the barriers within our information continuum so as to be able to harness—as the Vice President has taken to saying—the distributed intelligence of the nation.
New Rules of Engagement for the Information Battle

Elsewhere I have documented at length the new rules of the game and how one must practice intelligence in the age of information, but here five aspects of our information battlefield must be summarized:

- First, distributed information is far superior and more viable, as well as less expensive, than centralized information. In the age of distributed information, the concept of central intelligence is an oxymoron. The acme of skill is the seeking out of “just enough” information “just in time,” and doing so through the harnessing of world-class experts whose lifetime of expertise has been developed at someone else’s expense.

- Second, the fascination with the Internet is premature and dangerous. Eighty per cent of the information needed to properly create open source intelligence or decision-support products is either unpublished or in hard copy, in a foreign language and somewhere else. None of our intelligence or information organizations are truly structured to deal with this reality.

- Third, the center of gravity for national intelligence is in the civil sector, but we persist in spending billions for classified imagery and signals satellites and hundreds of thousands for a few token contracts with academics and business experts. We must radically realign the balance of spending between classified and unclassified research, and this is nowhere more apparent than in the grotesque mismatch between what we spend on national classified imagery versus what we spend for commercial imagery.

- Fourth, we must change our information work process and move away from the traditional linear paradigm, where the consumer goes to the analyst who goes to the collector who goes to the source—only to have the source read open source literature, concoct a third cousin with special access and back up the chain it goes, only now it is either classified or labeled corporate confidential. The new paradigm is the diamond paradigm, in which all four of these parties will talk to one another at any given time, and the acme of skill for the analyst will be the ability to put a consumer with a question in touch with an expert source who can create a tailored response in real time.

- Fifth, we must recognize the radical change that all this implies for the analyst. Instead of the traditional introvert, isolated with lifeless information media and producing erudite products that are thrown over the wall to a faceless customer, each analyst must become an extrovert and work diligently to manage overt networks of international human experts; networks of consumers and their staffs; and finally—such a radical notion—real money with which to hire international experts one day at a time.

Conclusion

The private sector, not the government and not the military, is the center of gravity for both information warfare and open source intelligence. It is the private sector which has the most to lose, and the most to gain, from developing and implementing a national information strategy which can bring coherence and direction to our now fragmented and often fictitious capabilities in the information warfare and national intelligence arenas. Only by recognizing the urgency of this need, and by recognizing that the next war will be won or lost here at home, in a violent peace, very quickly, can we muster the commitment and the consensus for establishing a national information strategy which will make it safe for ourselves and our children to work and play in cyberspace.

Hear all three of these authors on Information Warfare at the upcoming ASIS Annual Meeting, in Baltimore Tuesday, October 22, 1:30-3:00 P.M.

Hot Topics Session: Information Warfare

Information Warfare: An Introduction and Strategic Implications
- John I. Alger, dean, School of Information Warfare and Strategy, National Defense University

Smart People, Dumb Nations: Bad Business
- Robert D. Steele, president, Open Source Solutions, Inc.