Calhoun: The NPS Institutional Archive

DSpace Repository

Faculty and Researchers | Faculty and Researchers' Publications

2000

Towards a National Information Security Strategy

Arquilla, John; Ronfeldt, David

Strategic Studies Institute (SSI), US Army War College

Arquilla, John; Ronfeldt, David, Towards a National Information Security Strategy,from "The Information Revolution and National Security" (2000) edited by Thomas E. Copeland, Strategic Studies Institute (SSI), US Army War College
https://hdl.handle.net/10945/71740

Downloaded from NPS Archive: Calhoun

http://www.nps.edu/library

Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

NOON SESSION:
Video Teleconference

This session built on the previous session on responses to security threats.

"Towards a National Information Security Strategy"

Dr. John Arquilla
Naval Postgraduate School of Monterey
and
David Ronfeldt
RAND Corporation

Let me begin with a definition of information strategy. It is the pursuit of policy through informational ends and means, and it includes several components. First, supporting existing political, economic, and military domains of statecraft, and emergence as a distinct new domain itself. We want to conceptualize information as a distinct dimension of American power. Second, managing our own capabilities and resources, and interacting with others in peacetime, crisis, and war. It is at least as important that we learn how to manage our own resources as it is that we determine how to attack the enemy. Third, attending to both the contents and conduits—both the structuring and the processing—of information. It applies to the message as well as the medium. And finally, realizing that "information strategy" corresponds, at the highest level, to "knowledge strategy." What does one know about the battle for Seattle? Black helicopters and 135 nation-states were upended by nongovernmental actors.

As the information revolution alters the world, we see some crosscutting trends. First, the information revolution is resulting in a vast new technological infrastructure. We

have global access and interconnectivity, and the United States is the primary beneficiary of this, but as we become more dependent on it we also become more vulnerable. Second, the power of networked non-state actors is increasing. In civil society we are seeing nongovernmental organizations (NGOs) and activists, but we also see the emergence of "uncivil" society, such as criminals and terrorists. Third, the information revolution is enhancing the effects of "soft power" and "information operations," giving people greater ability to influence events. This is true of the Zapatistas in Mexico, of radio station B92 in Serbia, and Suu Kyl in Burma, for example. For states, this can also have some positive effects, perhaps allowing us to act at lower cost and with less risk, and perhaps also to target our actions better. We use economic sanctions quite frequently but with many unintended consequences. Information operations might allow us to pursue our aims without hurting a lot of people. Fourth, states are being altered in some ways, and perhaps diminished, but they will have to learn how to deal with these new actors.

David Ronfeldt and I are trying to articulate a four-part vision of where we should go with U.S. strategy. First, there is an emerging set of strategic opportunities and imperatives.

• On the defensive side, we need to maintain "guarded openness." Our economic and political security depend on open relations with our allies, but we have to be guarded because almost all information technology is dual-use in nature.

• Integrate a "sensory apparatus" to warn and monitor. In other words, we need to learn how to network better, something we do not do well in government.

• Develop the "noosphere" proactively. David and I like to coin a new term at least once a year, or else we are not doing our job, and this is taken from Des Jardin's notion of a "realm of the mind." This subsumes both cyberspace and the media-driven infosphere, and our corollary is that a new

type of politics will emerge alongside it, "noopolitik" rather than "realpolitik."

• Project the right "story" via soft power. Whose story won during coverage of the demonstrations against the World Trade Organization in Seattle? Clearly, the demonstrators' story prevailed.

• Use "strategic swarming" to mix hard and soft power. Swarming is a kind of tactical or doctrinal approach that allows one to strike from all directions simultaneously, whether it is social activism in downtown Seattle or the Zapatistas in southern Mexico. An interesting example of this was General Shelton's actions in Haiti a few years ago, where a small number of Special Forces were able to spread out and maintain control of the island during a period of intense coercive diplomacy.

Second, there is some concern or sensitivity over the role of the United States in information sharing versus information domination. Even our allies are worried about intelligence cooperation with us because they are afraid of some kind of exploitation. And if you listen to the Iranian or Vietnamese media's depiction of world opinion, they perceive that we are seeking domination over the world through cultural exports like reruns of Baywatch, although I do think some of this is tongue-in-cheek.

National Information Strategy.

How do we move toward formulating a national information policy and strategy? We have to rethink how we are applying "information" in the current political, economic, and military domains of our grand strategy. Then we need to identify the building blocks and measures for the development of a new information domain of granted strategy. This idea first appears in President Reagan's National Security Strategy in 1981, suggesting the notion of information as a fourth dimension of national power. At the same time, we have to think about how this problem applies

to the offense-defense dilemma and its implications for deterrence and coercion, as well as what it means for alliances and conflict resolution.

Current grand strategy is already replete with information-driven elements. On the political level, our goal of democratic enlargement is greatly aided by interconnectivity because it puts such pressure on authoritarian regimes. But there are places where we need to apply some prudence because we do not want to see change come too quickly. We do not want it in Saudi Arabia yet, and who wants democracy in Algeria if the radicals take over?

In the economic domain, information creates a tremendous new profitability for the United States; the expansion and growth we have seen in the 1990s is the product of the information revolution. But we are looking at technology that is all dual-use, having both commercial and military applications, so we may inadvertently be endangering our information security and empowering our rivals. One of the great problems in our relations with China has to do with the ballistic missile and other technologies that they are acquiring.

On the military side, it is a fascinating time. It is difficult to find another period in time where one power had such predominance in military power over all others. What the information revolution is allowing us to do, in terms of information operations and the information used in our weapons systems to improve their accuracy, is to use extremely limited and discriminate force. But there is also a danger of information arms races, and the possible spread of weapons of mass destruction (WMD), if the U.S. edge in information technology is not shared. Opponents may feel the need to offset our capabilities with dirty, old-fashioned WMD. Recent Russian military exercises called ZAPAD [WEST] 99 featured extensive use of tactical nuclear weapons.

A Framework for the National Information Strategy.

If we want to conceptualize a framework for information strategy as a distinct domain, we need to think not only about offense and defense, but also about a more general posture. We need to think about the ideational tenets and organizational and technological principles, but the real defining level is that of ideational concepts. (See Table 3 below.)

We have a policy choice to make: are we going to focus narrowly or broadly? If narrowly, then our focus will be on cyberspace security and safety. This includes infrastructure protection and assurance, intrusion detection and rapid-response strategic information warfare, and public-private intelligence coordination. This is where we are right now. If our focus is broad, then we need to place additional emphasis on global "soft power." We would pursue this notion of "noopolitik," which is an international system based on ethics, norms, and values. It is really a revolution in diplomatic affairs, and the next step beyond constructivism. Such a strategy at a broad level would include the right of communications and information for all, and the deep coordination of government and NGOs. For example, why were none of the NGOs invited to the World Trade Organization meeting in Seattle? In either case, we need to pursue guarded openness, strategic swarming, organizational networking, and infrastructure expansion.

At the organizational design level, we recommend interagency networks and some new organizational structures, as well as better public-private cooperation. Half of all military communications traffic goes across commercial systems, so we need to learn how to cooperate better.

On the level of technological applications, we recommend wide diffusion of strong encryption technology because the bad guys already have it, so we might as well

use it. As to defensive measures, we need better depth defense—there is a kind of Maginot Line mentality about information security with firewalls or orange book systems that (supposedly) nobody can break into. However, every day we find new evidence that this is not true. What we need is depth defense that may allow the bad guys in, but all of our information is protected by strong encryption so little damage is done. Regarding offensive capabilities, we are not talking just about taking down somebody's power grid, we need to be considering how to use our great media howitzers to get the story across that will win.

David and I would recommend that we fill in the framework broadly as follows:

	General Posture	Defensive Measures	Offensive Capabilities
Ideational Tenets	Development of noosphere, noopolitik, plus a RDA*	Guarded openness, no first use of SIW**	Discriminate swarming
Organizational Design	Interagency networks, hybrids with hierarchies	Public-private cooperation for information security	Coalition information-sharing and interoperability
Technological Applications	Wide diffusion of strong encryption; connectivity	Preclusive and depth defense architectures	SIW** measures; media broadcast capabilities

*RDA = Revolution in Diplomatic Affairs

**SIW = Strategic Information Warfare

Table 3. The Ideational Tenets and Associated Principles.

Across the ideational level, as I suggested earlier we need to explore the noosphere, this realm of ethics and ideas. Defensively, we need not only guarded openness, but the United States might find some benefits in a no-first-use statement regarding strategic information warfare (SIW) in order to reassure other countries. Offensively, we believe swarming will be the best doctrine.

Finally, we should consider some new and varied issues on the agenda. First, those that are defense-related:

- Defending the homeland against "cybotage."
- Elaborating behavior-based arms control. We are talking about behavior because we simply cannot control the technology any more with SIW.
- Operating in coalitions, projecting forces. These problems are immense. Disruption of our deployment schedules or air tasking orders could cause us a great deal of trouble.
- Coping with non-state actors, both civil and uncivil.
- Shaping a strategic information doctrine (SID). This is a change from the Single Integrated Operational Plan (SIOP).

Second are those that are community- and country-related:

- Constructing a globe-girdling noosphere, a global civil society that allows us to resolve many of our disputes with more peaceful means.
- Fostering a revolution in diplomatic affairs (RDA). This means building a diplomatic system that is not based on embassy edifices and putting the President on the front line of every diplomatic crisis.
- Developing a capacity for strategic swarming.
- Pressuring authoritarian rulers. The information revolution gives us quite a bit of leverage in places like Cuba.
- Settling high-risk conflicts such as Kosovo. Peace will come there not through a negotiated military settlement but through an agreement on some common future.

What we need for an information strategy then is a concept of operations for the 21st century. Lord Nelson, for

example, suggested new naval tactics that allowed his ships to concentrate on smaller parts of the enemy's navy and achieve a striking advantage. At Trafalgar and a number of other battles, he did just this. In the German concept of *blitzkrieg*, the tank, airplane, and advanced communications were conjoined to enable maneuver warfare. We need to get to this point in our thinking.

At present, there are more questions than answers. What issues get priority or provide us with the best leverage? Do the issues and the framework relate well? How much can reorganization alone accomplish? At least, shifting the current direction of our thinking seems advisable. The prevailing concept of operations has emphasized the technical and defensive dimensions, keying on U.S. vulnerabilities. The focus of the next concept of operations should be on ideational and organizational dimensions, and on opportunities to be proactive. This requires a great strategic shift in thinking that we hope will be evidenced in the next Presidential Decision Directive (PDD) on the subject.

To explain where we are today, let me return to Table 3. We are already implementing most of the defensive measures recommended (except the no-first-use statement), and we are utilizing most of the technological applications except for the diffusion of strong encryption. What is not getting done is thinking about the general posture, including the need for new, hybrid hierarchies. On the offensive side we are not doing well at figuring out how to share information with our most trusted allies. We are also not really considering offensive doctrine; we are stuck with the doctrine of Curtis LeMay, which was something along the lines of "nuke them into glass." What we would introduce is something a bit more discriminate, with strategic swarming allowing us to place our efforts where we need them.

Discussion.

Dr. Arquilla was asked to comment on four issues: the place of physical violence in this approach; the empowerment of nongovernmental organizations; information warfare attacks against the economy; and the outlook for success in devising a national information strategy given bureaucratic realities.

Violence and Strategic Information Warfare.

Violence does not go away. At the military level, the concepts that David and I have elaborated about cyberwar and netwar suggest that you can achieve your aims with a lot less destruction than you used to. We think you can avoid having to use annihilation or destruction to win, and that you can win with disruption. Violence is a key to terror and always will be, and my great fear is not that the cyber-terror threat will become real—though it is now a lot less than it is given credit for in official circles. My fear is that terrorists are learning how to become "informatized," and they are using information now openly available to guide and target their violent operations. Recently I was able to go on-line from my desktop computer and take virtual tours of U.S. military bases; I briefed this to some base commanders, and partly as a result that information is now off the Web. I see the terrorists using information in a variety of ways, most importantly as a tool for supporting their active combat operations because there is a lot of information out there. Secondly, I think terrorists are going to be increasingly using the Internet for fundraising. The Tamil Tigers have showed an ability to reach out to a large diaspora for material support. Those kinds of uses are what I am more afraid of than cyber-terror itself. Today the notion of using bits and bytes to bring whole systems down is very much exaggerated.

Empowerment of Nongovernmental Organizations.

Clearly in the case of the landmine issue, the Net was not the only resource out there. There was a lot of media coverage, and there was a lot of use of classic activist tactics. Aerial bombardment began with zeppelins dropping bombs on English pubs, and it took another 25 years for airpower to come to fruition as the defining force of 20th century conflict. In much the same way, I think the information revolution is now just getting on its legs in terms of civil activism. The case of the Zapatistas is interesting. It is clear that the Mexican government was influenced to end its military activities against them in part as a response to their use of information operations. In Burma, government behavior has been somewhat restricted because of Net-based activity. This is still at an early stage, and use of the Internet is not going to be effective every time. We need to be careful not to hype the capability, much like we have to be careful not to hype the threat of cyber-terror, either.

Strategic Information Warfare against the Economy.

I do not think the threat exists today, and it is not clear when it will. What we saw with the rise of airpower was two different viewpoints. One was that it would have an important effect on the battlefield, and it took about 25 years for that to happen. The other view of the early theorists was that airpower changed everything—you did not have to engage the enemy's field army to strike his homeland. For 85 years people have been trying to realize the potential of an independent striking force. I am afraid we are going to have a similar debate over information warfare that may last just as long. There are those who think we can bring the enemy to his knees simply through an information attack on his economic, political, and transportation infrastructures. Yet we built infrastructure that could withstand nuclear war—that is why we built the Internet. I think that information warfare is as doomed as

the early, grandiose expectations of airpower. However, I think information warfare can have strategic effects if used against militaries. Disruption of American deployments could make all the difference, especially if an opponent has limited goals and threatens the use of WMD after he has achieved his goals and before we can respond. Such fait accompli strategies may be enhanced by information warfare. I think that like airpower, information warfare is going to have its main effects on the battlefield and will cause homeland disruption, but it will never be able to obtain a state's political aims in a true Clausewitzian sense.

Strategy vs. Bureaucracy.

What we have is a dismal landscape of bureaucratic pulling and hauling. I see few opportunities to break through it. I have been looking at this issue for 10 years, and progress is only made slowly, and here and there. When I walk the halls of the Pentagon, the locus of world power, everyone I meet seems to think fatalistically that he can accomplish or influence nothing. So I think our greatest problem is sociological, in persuading people that they can make a difference in what they do. There are pockets here and there where people are trying to make a difference. We are beginning to get some interservice coordination, and a little bit of interdepartmental cooperation. The challenge in the years ahead of us is organizational, not technological. Unless we begin to develop some sense of loyalty to an entity greater than an individual service, or the State Department, or one of the other governmental actors involved, we are not going to move ahead. Ten years from now I do not know if we will yet have a real information strategy, although I am sure it will be an improvement on what we have now. We have enough of a cushion in the international arena right now that perhaps we can continue to muddle through for awhile.

THE INFORMATION REVOLUTION AND NATIONAL SECURITY

Edited by
Thomas E. Copeland

August 2000

*****

The views expressed in this report are those of the authors and do not necessarily reflect the official policy or position of the Department of the Army, the Department of Defense, or the U.S. Government. This report is cleared for public release; distribution is unlimited.

*****

Comments pertaining to this report are invited and should be forwarded to: Director, Strategic Studies Institute, U.S. Army War College, 122 Forbes Ave., Carlisle, PA 17013-5244. Copies of this report may be obtained from the Publications and Production Office by calling commercial (717) 245-4133, FAX (717) 245-3820, or via the Internet at rummelr@awc.carlisle.army.mil

*****

Most 1993, 1994, and all later Strategic Studies Institute (SSI) monographs are available on the SSI Homepage for electronic dissemination. SSI's Homepage address is: http://carlisle-www.army.mil/usassi/welcome.htm

*****

The Strategic Studies Institute publishes a monthly e-mail newsletter to update the national security community on the research of our analysts, recent and forthcoming publications, and upcoming conferences sponsored by the Institute. Each newsletter also provides a strategic commentary by one of our research analysts. If you are interested in receiving this newsletter, please let us know by e-mail at outreach@awc.carlisle.army.mil or by calling (717) 245-3133.

ISBN 1-58487-031-1

CONTENTS

TABLES