MARS CHUCKLES AND ATHENA SIGHS IN FRUSTRATION ©[1]

Richard Szafranski
Toffler Associates®

ABSTRACT

The thesis of this article is that armed forces and their national command authorities have much to learn about effectively integrating information operations into both war and anti-war security operations. Worse, at the present rate of learning the Western democracies may be surrendering intellectual leadership and ultimately operational leadership to those States, hackers, and criminals who more quickly adapt these new tools. That said, I do not intend this to be the Third Wave Information Age equivalent of saber-rattling. Rather, it is a call to action. And prerequisite for action is first to appreciate that change is difficult.

INTRODUCTION

Offensive IW, in brief, uses computer intrusion techniques and other capabilities against an adversary's information-based infrastructures. The Commission [US President's Commission on Critical Infrastructure Protection, PCCIP] is aware of *little* in the way of special equipment required to launch IW attacks on our computer systems; the basic attack tools—computer, modem, telephone, and software—are *essentially the same* as those used by hackers and criminals. And compared to the military forces and weapons that in the past threatened our infrastructures, IW tools are *cheap and readily available.*[2]

YES, CHANGE IS DIFFICULT

Moving from the old and familiar to the unfamiliar new is a difficult process for everyone, and especially difficult for soldiers, sailors, and aviators. There is, as Hart observed, nothing harder than displacing old ideas. Just when soldiers, sailors, and aviators and their institutions think they "get it" about the operational art, some new discovery—usually a technology or an application—intrudes to render significant elements of what they know irrelevant, or at least less relevant. When this occurs, Mars chuckles. Think back in time to think forward.

Imagine how difficult it must have been for militaries to accept and accommodate the seemingly unnatural technologies of gunpowder and cannon. Stabbing, slashing, pounding and piercing the enveloped prey seem to mimic the hunt perfectly, and hunting in packs or platoons is an activity that may be natural to our species. Burning some chemical compound to release its energy in a hardened tube must have smacked of necromancy. New competencies in chemistry, metallurgy, casting, and engineering had to develop in tandem with new organizations and employment schemes. Gunpowder and cannon changed the human hunt.

Gunpowder was but one change that transformed navies. Navies saw steam replace sail and internal combustion engines replace steam, only to have steam return in the form of nuclear power for some warships. Navies witnessed the sub-surface become key to the surface and the aircraft carrier displace the battleship as the principal means of power projection. But navies adjusted.

Envision the angst faced by armies and their cavalries when the ratio of horses to motor vehicles shifted from horses to favor motorized vehicles during World War II. The technology of the internal combustion engine and its terrestrial applications for warfare displaced the horse and rendered the sword ceremonial. And then arrived the flying machine in its many incarnations, finally including a rotary-winged form for air cavalry operations. Hot on the heels of flying machines came missiles, pressing the army's artillery with the same assiduousness that flying machines pressed both the cavalry and the artillery. Armies tried to adjust.

But then came rocketry and nuclear weapons and space. German research into vehicles designed to carry conventional weapons gave us cruise missiles and ballistic missiles. Nuclear weapons gave these missiles punch. Long-range precision weapons, both nuclear and non-nuclear, today guided by their own eyes and the artificial moons of electronic navigation, allow armed forces to stand far off and cast death and destruction on enemies that humans only see through the mediating structure of sensing machines. Armies, navies, and air forces all want the non-nuclear ones and get them and use these long-range precision weapons with a profligacy that would stun an accountant.[3]

These very accurate weapons and the rather repetitive thriller impact videos that accompany the successful hits help delude the public into thinking that warfare ought to be casualty-free or at least casualty-limited. Precision long-range weapons now are the *lingua franca* of warfare. Armies, navies, and air forces squabble about what these mean for warfare, for their separate missions, the differentiation of operations in "their" media, and the right and true role of air forces. Armies, navies, and air forces are trying to bend to these changes, but—witness the debates preceding any significant ground operations—armies know that notions of antiseptic Airpower are supplanting public acceptance of the readiness for mud and blood operations. Willingness to engage in these operations formerly put armies closest to the seat of power everywhere. Even armies appreciate that the real risk to homelands in the developed world today is not other invading armies, but Airpower and fifth column terrorism. Does Airpower now become the dominant force?

No. The real risk to the craft of flyers is neither long-range precision weaponry nor unmanned aerial vehicles, but a new discovery. The new discovery, pivoting on potent "new intangibles," does not eliminate the old "things" of fighting past or fighting present, but they now allow it to be augmented, complemented, or in some cases replaced by new things. The Tofflers write

> None of this is to suggest that tangible, material resources and technologies are going to vanish in a puff of dematerialization. Obviously, things matter, and weapons matter more than most things. Software still needs hardware. Soldiers cannot eat data. Nonetheless, the fun-

> damental relations between the tangible and what might be called the "new intangibles" are increasingly crucial to military effectiveness, in both waging war and trying to prevent it.[4]

Information warfare is the great new discovery true acolytes of Mars need to welcome. Mars, after all, gave us computing machines, and computing machines gave us awareness that things in the external world could be reduced to combinations of zeroes and ones. This understanding launched the information age. These combinations could be transmitted electronically as data and recombined upon receipt to form the basis of information. According to the seminal work on control warfare by Arquilla and Ronfeldt, "information" is more than the content or meaning of a message. Rather, information is "any difference that makes a difference."[5] Awareness that almost everything[6] of military significance in the external world could be reduced similarly launched the age of information warfare.

Information warfare is troublesome for the established institutions to "get," because key facets of it are indirect and subtle, not direct and brutish. Information warfare is a form of conflict that attacks information systems—carbon and silicon—as a *means* to attack adversary knowledge or beliefs. Information warfare can be prosecuted as a component of a larger and more comprehensive set of hostile activities—what Arquilla and Ronfeldt call a netwar or cyberwar—or it can be undertaken as the sole form of hostile activity. Information warfare can occur *in* war and it can occur *outside of* war.

Carefully read what US Air Force (USAF) doctrine advances. According to the USAF information warfare (IW) is

> …information operations conducted to defend one's own information and information systems or attacking and affecting an adversary's in-formation and information systems. The defensive aspect*, defensive counterinformation, much like strategic air defense,* is always operative. *Conversely,* the offensive aspect*, offensive counterinformation,* is **primarily** conducted during times of crisis or conflict. Information warfare involves such diverse activities as psychological operations, military deception, electronic warfare, both physical and information ("cyber") attack, and a variety of defensive activities and programs. It is important to stress that *information warfare* is a construct that operates across the spectrum, from peace to war, to allow the effective execution of Air Force responsibilities.[7]

> IW is information operations conducted to defend the Air Force's own information and information systems or conducted to attack and affect an adversary's information and information systems. This warfare is **primarily** conducted during times of crisis or conflict. However, the defensive component, much like air defense, is conducted across the spectrum from peace to war.[8]

This relatively uncomplicated conception, new nonetheless, poorly masks a new admission—repetition reveals it—that this new kind of *warfare* and warlike operation is not restricted to *wartime*. Offensive information warfare, "offensive counter-information" as the USAF calls it, is "primarily," but not necessarily *exclusively* conducted "during times of crisis or conflict."[9] This kind of warfare *is* new, and the new always has been a challenge and vexation to militaries.[10]

And all the while a cacophony of Mars's priests—perhaps aggrieved by accusations (or revelations) that many of their stories slowly are seen as little more than informed speculations, albeit interesting ones—mock Athena. Some cantankerously coo that there is nothing new under the sun and that information warfare is a chimera.[11] Athena sighs in frustration. Both she and Mars know that Mars was the old god of war, and by now even Mars should know that Athena is the new deity of warfare.[12] Change *is* difficult.

BUT DIFFICULT DOES NOT MEAN EITHER UNNECESSARY OR IMPOSSIBLE

It Is Necessary

While there is no need for panic, there is a need to consider the facts. A powerful motivation for change ought to be the awareness that, properly done, information warfare can seriously perturb just by trying to level the playing field. Any serious perturbation in information systems can reduce the effectiveness of operations. Consider the Y2K issue.[13] As US Senator Robert Bennett, discussing the Y2K problem, put it, "The antidote to panic is always accurate information, but some of the accurate information can be pretty scary."[14] Accurate information about hostile information operations can be pretty scary too.

At the lower end of the spectrum of aggravation, small groups and States can use information warfare to disrupt a larger State's efficient functioning. At the higher end, small groups and States can seriously and adversely affect larger States.[15] Limited and tactical uses of information warfare aside, States and groups may now or soon possess "strategic information warfare" or "SIW" capabilities. Strategic capabilities are those that can "seriously harm"[16] another's security or security interests.[17] If offensive counter-information warfare can be done *outside* of war, then strategic information warfare also can be done *without* a declaration of war.[18] And people can do it without the normal military folderol of donning a uniform, wearing a silly hat, being physically fit, leaving their homes, or saluting anyone. All they need is a motive to match the readily available means. The motives could be as simple as curiosity or greed and curiosity and greed are not scarce on our planet.

Thus, we should prepare for such aggravations now, although the Defense Science Board estimated in November 1996 that we have some time: "limited strategic information warfare capabilities" used against us may still be seven to ten years away.[19] Is this so? A study by RAND noted somewhat inconclusively that we don't know.

> A macro assessment of the current state of first-generation SIW in terms of absolute and relative offensive and defensive SIW capabilities of the United States and other nations (or other parties) would be difficult to do, even at a classified level. The current dynamic character of the Information Revolution and the embryonic character of SIW as a potential political-military instrument both argue for caution in making such an assessment, classified or unclassified, at present and for the foreseeable future.[20]

Without putting too fine a point on the "future" almost all[21] agree that

> In the future, the possibility exists that adversaries might exploit the tools and techniques of the Information Revolution to hold at risk (not for destruction, but for large-scale or massive disruption) key national strategic assets such as elements of various key national infrastructure sectors, such as energy, telecommunications, transportation, and finance.[22]

It Is Possible

It would be foolhardy or irresponsible to dismiss the risks of such attacks as impossible. If this is so, we should consider the threat and the risks in order to envision the forms our preparation and response ought to take. RAND analysts saw "a two-pronged threat to U.S. security."[23]

1. **A threat to U.S. national economic security.** Key national infrastructure targets could be at risk to such massive disruption that a successful attack on one or more infrastructures could produce a strategically significant result, including public loss of confidence in the delivery of services from those infrastructures.

2. **A threat against the U.S. national military strategy.** The possibility exists that a regional adversary might use SIW threats or attacks to deter or disrupt U.S. power projection plans in a regional crisis. Targets of concern include infrastructures in the United States vital to overseas force deployment, and comparable targets in allied countries. A key ally or coalition member under such an attack might refuse to join a coalition--or worse, quit a coalition in the middle of a war.[24]

The Economic Attack Test Case

Economies increasingly are dependent on the information infrastructure.[25] Anything that deliberately and adversely affects the capabilities of that infrastructure can be said to constitute an attack. If there are destructive or disruptive information tools intending to affect financial transactions, banking,[26] on-line investment services, billing, electrical power generation or distribution, telephone or data distribution,[27] emergency services, and so forth, then the best time for an attacker to operationally test these is in the wake of Y2K manifestations.[28] If the US, or another larger State, is the intended target of *future* strategic information warfare aimed at disrupting or even crippling commerce and services, then a smaller State, or municipalities within States, ought to be seen as the likely test targets for these Y2K experimental attacks.[29] Cities in Eastern European, Middle Eastern, Southeast Asian, and South American countries might be among those that an earnest adversary considers.[30] Target analysis would reveal particular entities within the candidate State(s) that are especially vulnerable—probably a bank or a telecommunications company.[31] The cyber-attacker would reap at least one tremendous advantage: data.

An attacker would learn much about how municipalities and States respond in the wake of unexplained failures in automated and interdependent critical (often defined as telecommunications, energy, banking and finance, transportation, water systems, and emergency services)

infrastructures. How does a State try to protect its physical and cyber-based systems essential to the operations of its economy? How do attacks on a small State affect the global internetted economy? What separations of power and what seams are observed to exist between the armed forces and the civil authorities? Between Government and commercial actors? What seemed to work and what did not work well? What systems or infrastructure elements were stressed most? How long did recovery take and what were the impediments to rapid recovery? Did trust erode? What small inputs produced the largest outputs? What actions went undetected and what, besides the outcome, was easily detected?[32]

As compounded and cascading failures occurred, human error inevitably would follow. Unrelated equipment failures, weather and other natural causes may provide the opportunity for gathering unexpected data on excursions. An obvious problem for a future attacker is in relating cause and effect. A live test would reveal far more than a simulation or a model would. A live test rendered opaque by Y2K would have obvious advantages to attackers.[33] Hence, if a future adversary intends to develop the capability to produce a "strategically significant result" on a large State's economy, we should be alert for real-world tests conducted in cities in out-of-the way places.[34]

Anti-Access

We still think of power projection in terms of physical means—mass—deployed, and we still think of anti-access as belligerent means aimed at denying the ability to move mass. "Access" may be thought of as the ability to approach a physical place or introduce mass there, but physical access is only *one* form of access. There are electronic "places." There is electronic access to markets. There is access to reality and truth. In the Third Wave Information Age power shifts.[35] Knowledge becomes more potent, using it accumulates wealth, and violence is transformed by taking advantage of it. "Anti-access" in the next century will take many forms: the inability to introduce mass, the inability to sustain mass, the inability to participate in a market, and the inability to know the truth.[36] But some of these will not present themselves as the "anti-access" we expect.

States levy tariffs to deny access to another State's cheaper goods. Trade wars can be very testy, but few think of them as warfare. In the next century they very well may be. Already the Indian Commerce Ministry has stated that "the lack of e- commerce capabilities in the country could become a 'non- tariff trade barrier' against Indian exports" in a better-wired world.[37] Non-belligerent means to deny access already abound and information warfare will make them all the more subtle and elegant. Information warfare aims at the knowledge and belief systems of an adversary and takes advantage of an adversary's weaknesses. We know, for example, that ports and other embarkation points are critical to moving mass. We also know that that the larger developed States are becoming more, rather than less "green." A simple hazardous waste spill in the right place and at the right time likely would not be construed as a chemical attack, but it could hamper a deployment. Is promoting good stewardship of the environment an "information operation"? It could be,[38] as could be promoting ethnic strife, inadequate funding for public education, or "brain drain." These might be longer-term—or shall we say distinctly non-Western—strategies and one would have to take a

long view of competition to engage in them. There are more quickly maturing anti-access strategies also.

Imagine the economic impact of being denied access to a market (or a commodity) outright? Some businesses try to command a market, preserve the dominant share, or capture critical suppliers, all aimed at denying access to, or raising the cost of entry for competitors. In the wake of deregulation, various airlines, telephone companies, and utilities have been accused of executing anti-access or anti-competition strategies. In some cases, courts and regulatory agencies have found such accusations true. Individuals and firms buy functionality or prime real estate to deny others access to it. We should not be surprised that individuals (or the States that sponsor them), criminal syndicates (or the States that sponsor them), or businesses (or the States that sponsor them) aim for real estate or other physical asset ownership to deny access to others. What surprises some is that law and the possession of legitimate ownership, or title, or deed can prevent access. Yes, some big powerful States preserve the delusion that they can fight their way in, seize needed assets or property, or otherwise control access. But the non-belligerent global repertoire of anti-access tools continues to grow and many have security implications.

Worse than not having access is losing it when dependent upon it. What would prevent a cunning future adversary from allowing access only to then use it to advantage? For example, by enlisting a larger State in engineering its own defeat by allowing it to load up International Airport X with military aircraft only to make them easier to destroy or embargo? Or purchasing or owning all the water rights or water in a region? But access is not merely physical: imagine being a multi-national corporation owning all the communications channels serving an area with a multi-national board of directors. Who is to blame if the company refuses to lease a channel? What can be done?

But the highest and best use of anti-access strategies is to deny access to truth.[39] "Denial and deception" viewed in this light are sublime anti-access means: they impede access to the truth. Whether employing active or passive means to "protect their privacy," individuals, groups and States—unless some law or treaty provision is alleged to have been violated—can both impede access to knowledge and mask the meaning of things and actions observed. These are not necessarily belligerent acts.[40]

But how would one test anti-access strategies aimed at deterring or disrupting power projection capabilities in a regional crisis? Information operations, including terror attacks, certainly could be prosecuted easily. Infrastructures vital to force movement are complex logistics nodes. Information warriors can affect the silicon and carbon components in a number of ways: jumble manifests, lock or prevent unlocking electronic locks, terminate or disrupt telephone service, release a series of hitherto unseen computer viruses on the Internet, affix a worm or virus to the popular "anti-virus" software programs that allow real-time updates of virus definitions,[41] jam AM radio nets or cell phones,[42] buyout suppliers, unnecessarily dispatch emergency equipment, shut down child care centers, affect nuclear power plant control systems, have an apparent in-flight medical emergency, start rumors that *Ebola* or *E-coli* is in the water, dump sewage,[43] de-synchronize traffic signals on key arteries, or any number of other disruptive and destructive things.[44]

One needn't test these as an integrated series in advance. Testing each separately would give higher confidence[45] that they would be effective in disrupting operations when employed in concert. Thus the PCCIP recognized that

> …we need the analytic tools to examine information about intrusions, crime, and vulnerabilities and *determine what is actually going on in the nation's infrastructures*. Deciding whether a set of cyber and physical events is coincidence, criminal activity, or a coordinated attack is not a trivial problem. In fact, without a central information repository and analytic capability, it is virtually impossible to make such assessments until after the fact. This is of increasing concern as infrastructure operations become more reliant on information and communications—the very sector about which it is most difficult to make assessments.[46]

Contemplating the list below, one notes that few of the things listed have not occurred in the natural course of events. It is highly unlikely that a power projection or deployment system would perform effectively when faced with a handful of these simultaneously.

- **Jumble manifests**
- **Lock or prevent unlocking electronic locks**
- **Terminate or disrupt telephone service**
- **Jam AM radio nets or cell phones**
- **Buy out suppliers**
- **Unnecessarily dispatch emergency equipment**
- **Shut down the child care center**
- **Start rumors that *Ebola* or *E-Coli* is in the water**
- **Insert computer viruses into telephone-switching stations**
- **Activate logic bombs**
- **Stop the sewage treatment plant from functioning**
- **Cause traffic jams by misrouting public vehicles**
- **Dispatch utility repair crews to rural areas**
- **Jam the TV broadcasts**
- **Crank and prank calls to families**
- **Disable mobile phones**
- **Have several bomb scares**
- **Disrupt the electrical power supply**

Again, an excellent opportunity to test several of these, alone or in concert, will be occur the Y2K confusion. Again, the target likely will be a surrogate for the actual target and proxies may perform the attacks. And yet again, I am not suggesting that anyone do these, merely observing that someone will. What's to be done?

TAKING ACTION

Without awakening all the sleeping dragons of Cold War deterrence theories accept that we now possess doctrine on the use of hostile means with hostile intent before the familiar forms

of hostility erupt. The hostility is the employment of means aimed at subduing the enemy will. The adversary is subdued when the adversary is seen to behave in ways that are coincident with the ways in which we—the aggressor or the defender—intend for the adversary to behave.[47] And this behavior modification can occur before the traditional—read "old"—conceptions of belligerent operations are undertaken. This is not so much "warfare" as it is "peacefare," because warfare is only one side of the challenge of providing security in the 21st Century. Alvin and Heidi Toffler suggest that "…a revolution in warfare requires a revolution in peacefare as well." "Peacefare" must include and embrace active "anti-war" because the other side of warfare is "peacefare" just as the other side of war is "anti-war."[48] Competence in peacefare and anti-war will differentiate those who master the security challenges of the first part of the 21st Century. The Tofflers observe that "Knowledge is what the anti-wars of tomorrow will be about." Thus, the task is to "…accelerate the collection, organization, and generation of new knowledge, channeling it into the pursuit of peace."[49]

An important element of the new knowledge we need is knowledge of how to employ information warfare, or offensive counter-information, to subdue emergent hostile will. Toward that end, let us consider a handful of principles that should guide democracies in the pursuit and eventual employment of this new knowledge. Some are controversial and, I am sure, will provoke debate. Nonetheless, my aim is to generate new knowledge in the pursuit of effective anti-war capabilities to preserve the peace. The principles advocated relate to secrecy, modeling, integration, and agreement on triggering events, preemption, and escalation.

Secrecy

Difficult as it is in democracies to develop new weapons and new capabilities in secret, any research into and experimentation in offensive counter-information capabilities must be highly restricted and heavily compartmented. Certain national capabilities ought not be shared with allies for at least four reasons. First, alliances in the next few decades might be expedient, transient, and highly contingent. One's allies in one moment might well stand on the "wrong" side of an issue the next. The capacity to surprise can be lost if one's former friend is well aware of one's repertoire of capabilities. Second, new knowledge of any kind is valuable intellectual property. To pay the bill for developing new intellectual property and then surrender it is not traditionally[50] good business, or at least not traditionally good national security business.[51] For example, to develop a new cipher or code to protect information, or to develop a new code-breaking capability, and then give it up would be foolhardy. Third, there is a correlation between any new information capability and the economic advantages it can provide to its owners. That is, information weapons, unlike nuclear weapons, may have component elements with high utility for spin-off and spin-on products and for activities unrelated to warfare.[52] Fourth, it would be foolhardy to presume that *other* States and groups are not developing the capacity for knowledge warfare in secret.

On the other hand, sharing certain vulnerability and offensive exploitation techniques could have considerable reward both in the short term and over the long term. First, better-funded players in this game would be foolish not to cooperate in their quest to cover the broad array of attacks that easily could be developed by smaller players ranging wide in the spaces in

which the larger players play. Separate large players attempting to protect themselves everywhere in these spaces would require replication of effort and the dilution of large (but still finite) resources to push power from large organizations down to smaller organizations more focused on mastery of cyber-defense or cyber-aggression. Conversely, recognizing that both defenses *and* offenses have value in this space, information warfare creates opportunity for smaller organizations to generate revenue through cyber-arms research and trade. Third, introduction of threats or offenses into an environment often can increase stability and security by stimulating faster development and more thorough deployment of defensive countermeasures by vendors and customers motivated to immunize their systems. Some might label such a tactic as a "preemptive self-attack."[53] Last, and perhaps most importantly, the best argument for sharing knowledge in this space would be that knowledge in this arena is amplified by the synergies of the network effect, a phenomenon that has helped create the "knowledge explosion" driven by communications technology. Although such exchange may require developing requisite trustable coalitions of parties seeking similar objectives over the long term, the best strategy might be to balance the competitive advantage of secrecy against the benefits of more open exchange.[54]

Anticipating criticisms that the consequences of such secrecy could be an information "arms race," the fracturing of alliances, or random and destabilizing information attacks, I ask that you consider the world as it is already. Competition in computers, software applications, and telecommunications is already rampant on both sides of and across the Atlantic. Each of our companies and nations races to get ahead of the others for the wealth of its stakeholders. We're already there. Admittedly, information arms are a new kind of arms, but I am hard put to distinguish between the anti-virus software of today and the armor of archaic times. To test anti-virus software or to test an agent that inoculates against anthrax, one must have the viruses required. Said another way, to engage in effective *defensive* counter-information one must have a fairly good understanding of the capabilities required for effective *offensive* counter-information.

Because of the world that is, and emotional flag-waving aside, alliances among States are little different than partnerships in business. States have always retained the right and obligation to abrogate even the most solemn treaties in supreme self-interest. The termination clauses in business partnerships preserve similar prerogatives. It is naïve to think that alliances are based on anything except a State's awareness of what constitute its best interests at any given time. States weaker than the United States will, of course, protest that the pursuit of secret and unshared US national capabilities -including information warfare capabilities- is imperialism or isolationism, but the US must get used to such complaints.

Will secrecy expose all of us to an increase in random and destabilizing information attacks? One must ask the hackers and crackers, beholden to no State. Again, perhaps we are there already.[55] Antidotes and retaliatory tools developed in secret by States actually might increase stability and deter random attacks. Hackers that feel some of the weight of a State's legal power or a State's offensive counter-information capability might think twice before provoking any of us. The Net and the Web are the Commons, and all States should feel free to act against anyone misbehaving on the Commons. States will be moderate in their behavior, I believe, if for no other reason than reluctance to expose the existence of information

weapons in their arsenals. Secrecy is the foundation for accelerating the collection, organization, and generation of this new knowledge. And secrecy is key to channeling this new knowledge into the pursuit of anti-war. But secrecy is not enough.

Modeling

Modeling will be an essential step in this process [development of a science-based approach to the challenges of information assurance]. Component and system behavior must be modeled. Complex systems must be modeled. Stochastic systems must be modeled. Human behavior must be modeled. System fault must be modeled. Attack events must be modeled. All of these models, and more, must be able to work together to model entire information systems and quantify the interdependencies the separate models could not address. The models developed should draw upon past work and should span research, including dynamic modeling and agent-based systems.[56]

Today we understand less than we will need to understand to defend ourselves against attack and to enable information warfare and "cyber-warfare" to make significant contributions to war and warfare, anti-war and peacefare. Absent data and models, all the other answers to the questions information warfare poses merely are speculations.

Integration

Once we can model information operations we must find effective ways to integrate information warfare capabilities into diplomacy, anti-war, and warfare. Someone once observed that diplomacy is the art of "saying 'nice doggie' while looking for a big stick." Information is key to knowing which dog is growling, why, what frightens or placates or distracts the dog, what forms the big sticks might take, and where and when to best apply the stick. Applying the correct stick to the correct dog is a more difficult matter, but in order to do any of these, an elusive "someone" must be responsible for integration.

It may be that overall integration is best done by integrating substrates of differentiated capability. For example, give the responsibility for affecting the media to one group[57] and command and control computer networks to another. Integration closes whatever lanes exist between terrestrial forces (armies and navies), space forces, and air forces.[58] Integration also closes the lanes that exist between foreign affairs, defence, trade, and so forth. Ultimately, integration and authority must reside at the seat of power: the head of the State and the commander-in-chief of all the State's armed forces. The more comprehensive and robust the information warfare capabilities of a State, the more urgent the need for integration and centralized execution. Likelier than not, the paradigm of centralized control and decentralized execution will transform into centralized authority for execution and decentralized control of means.[59]

Do such integrating agencies exist today? I do not know.[60] Recent squabbles do not provide overwhelming public evidence of effective information warfare applications. Genocidal broadcasts seemed to have been tolerated in Rwanda and Yugoslavia and, except for conventional strikes against Serbian troop and paramilitary control capabilities, one petty tyrant after

another proclaims hate and pollutes the airways with hate propaganda.[61] Likewise, embargoes remain physical and porous and not electronic and impermeable.

The aim of integrating information operations capabilities is to make anti-war possible. The militaries of the democracies sit in quiet repose waiting for war, bemoaning their lack of resources and training for war. They tell themselves that they exist to "fight and win" their Country's wars. Yet, it is warfare by the anachronistic military definition they await. That their countries are awash in drugs or pressed by criminal syndicates do not rise to the level of an emergency for the armed forces. Or, if these developments do rise to the level of an emergency, they are emergencies for some entity other than the armed forces. The same is true for governments in the democracies on the international scene. A tin pot dictator can engage in the most heinous of crimes by framing the misbehavior as occurring incident to a civil war. Anti-war, actively opposing the emergence of warfare, requires greater insight and sensitivity to the precursor events that erupt in violence. Integration of information operations, and the capacity to conduct secret operations, would allow governments to act swiftly and invisibly at the onset of any renegade behavior. Those "rice bowls" or stovepipes that prevent effective information operations will at some point have to be integrated to allow information operations, both secret and covert, in the coming decades. One thing need not be secret: the categories of misbehavior that invite retaliation.

Agreement on Triggering Events

States recognize some behaviors as misbehavior already. Yet, except for invading a neighboring State, the old Second Wave parameter for misbehavior, States today are largely permissive of one another's bad behavior. Country X can build its export economy on growing opium or on abusive uses of child labor. Country Y can be the world's leading exporter of marijuana. Country Z can imprison all the practitioners of Faith W or V Ethnic Group. And Country T can train all the terrorists required for Countries X, Y, and Z. Our rightful respect for The Law compels us to negotiate with terrorists, war criminals, and democides until the indictments are framed, the trials consummated, and the sentences adjudged. Old murderers die in their beds or idle away at holiday resorts. Few dare speak for those denied speech or robbed of life. The disincentives for misbehavior are not nearly so potent as the apparent incentives.

One can see and quickly assent that our own standards for morality and legality cannot be made universal by violent warfare waged outside our own territories. I cannot, however, see that early information warfare might not provide a good antidote to some of the forms of bad behavior that would not easily rise to the level of a declaration of "War." In other words, there are triggering events that all or most States could recognize as undesirable or "bad" conditions. These are already well recognized by the articles that underpin the *raison d'être* for a United Nations. Groups of states often assert that individual nations deserve reprimand or constraint without desiring to use a high level of violence against them. Moreover, like embargoes and blockades, information operations can provide powerfully effective means of non-lethal constraint. What apparently we lack are the capacity and courage to use information operations in situations where misbehavior ought to be punished. Secrecy will allow the

development of capability and integration will give capacity, but courage is a matter of each State's assessment of risks and consequences. Strong States are more risk-tolerant than weaker ones. Why shouldn't strong States be prepared to preempt with information operations?

Preemption

Preemption is as dirty a word as prevention is a gentle one. The polygraph is not so much designed to catch spies as it is to prevent or preempt deceptive behavior. Even so, it is a primitive tool that requires physical contact with the subject. As computational capability and brain research combine, we may be able to identify miscreants before their misdeeds are serious. David Ronfeldt, the brilliant RAND researcher, suggests that the type of 'netwar' democracies will face in the future—"a new mode of low-intensity, societal-level conflict"—is particularly attractive to a leader with discernible (but unhealthy) psychological traits[62] "who aims to operate slowly and covertly to weaken his chosen enemy." Identifying such characters in advance would be useful. Will our respect for the law allow them to hatch their schemes without our intervention? Probably. But it is equally likely that peace on the planet will spawn homeopathic or antidotal warfare. We may very well have to learn to fight early and preemptively to prevent the spread of fighting.

We should expect that the larger States may engage their adversaries—State and non-state groups—much earlier, more covertly, and more often than in the past. While physical engagements draw attention and pose the risk of loss of life, some information warfare operations do not carry the same risks. Thus, we can expect that information warfare capabilities created in secret and tightly integrated with both non-traditional, non-military attack and interference capabilities and more traditional combatant capabilities will be used as soon as a triggering event occurs.

The attacking force will seek no one's permission except the head of State, friends and allies will not be notified, and responsibility will not be accepted. Unless the average civilian can possess Nation State like defenses, this will necessitate a different approach to civil-military relations than most nations take today. Such necessity would change the relationship between the combatant and the non-combatant, between the military and the civil authority, and, of course, we would call our States "democracies" still.[63]

For these reasons and many others, we should expect new concepts of information operations. Consider what's plausible. In the future the State might require Net users to inoculate their systems against disruptive viruses. Civilian contractors to the Government in the future may have to demonstrate rigorous defensive counter-information capabilities, have a reliable and screened (read "investigated and polygraphed") workforce, and allow the Government access to all their information handling systems. To ensure both compliance and readiness, the Government periodically might unleash viruses on its instrumentalities, its contractors, and almost inescapably, however unintentionally, on us. Preemption may become the norm and only the side with superior analytical capacity will be able to sort out the "who shot John" of an engagement. There is no weapon humankind ever created that has not been employed. Do we

believe that no weapons are emerging from doctrine and from all this talk we hear about information warfare? Would we go so far as to seek and employ whatever is the information analog of the much heralded (and never seen) ultimate weapon?

Escalation

Escalation is as grim a word as preemption is a dirty one. To escalate one must assess that the consequences of getting meaner are less than the consequences of failing to respond to a provocation. One must also have a clear sense of what State or group is the adversary. The Tofflers wonder

> But what if some adversary--State or non-State--employed intangible means to damage or destroy that city's computer networks, including those needed by its police, airport authorities, electrical systems, banks, and the like? Even assuming the source of the attack could be identified and verified, would the situation call for a military response? Whose responsibility would it be to retaliate and how? And what if, at the same time, riots were provoked in the city by televised scenes broadcast from pirate transmitters in Mexico or Mexican airspace, showing false but convincingly gruesome police or military brutality against Latinos in L.A.? If someone were engaging in information warfare against the United States from both inside and outside the United States, would retaliation be the responsibility of the FBI--many of whose computers and systems are outworn relics--or would some of the responsibility fall to the military?[64]

There are no easy answers to these questions. We know that the target sets of information warfare are both carbon and silicon. To subdue increasingly hostile or non-cooperative will, information warfare attacks the mind, that complex of protein and synapses and nerve bundles and electrochemical functions that host the will and determine human behavior. We can envision that the weapons of next generation information warfare could include tools designed to enable entering and affecting the brain: sounds, smells, images, tastes, and tactile sensation. They might include drugs. They might include pheromones. If this is so, what level of attack is just and proportionate and what is unwarranted, disproportionate or unjust? Is any level of response just and proportionate without clearly knowing the attacking State or group?

Perhaps "it depends" appertains?[65] I earlier said I did not wish to awaken the sleeping dragons of Cold War deterrence theories, but it appears this may be unavoidable. Information weapons are new, they blur the distinction between combatants and non-combatants, and the only analogs we have are from the heyday of nuclear weapons. Can we ask the same kinds of questions asked about nuclear force? Would States aim to deter information warfare? How? In the same way nuclear weapons use was deterred: by having enough capability to wipe out millions of people and large potions of the planet?[66] Or should we build our information forces for flexible or selective response? Would it be wise to have some "limited" information warfare response options, but hold "unlimited" ones in reserve? Would States take a counter-force approach, limiting offensive operations to retaliation against the adversary's information systems? Or would attacks take a counter-value perspective and attack the minds of the adversary more directly? Would States opt for "mutual assured information destruction"? Would execution authority reside with the head of State, or would that person delegate

the authority for some attacks against adversary epistemology to military commanders or even to the commercial sector? Would we be prepared for protracted information warfare?

We do not know as much as we need to know for "knowledge warfare." What does precision mean as it applies to information warfare attacks? Are there precision-guided messages (PGM) that could be aimed at single minds? Does the notion of circular error probable become the idea of calculated error probability (CEP) through the statistical technique of Markhov-chaining in information warfare?[67] What are the canons of epistemological damage expectancy or probability of damage? What is information "collateral damage" and how would it be controlled? What is the information equivalent of fallout and what would a fallout shelter look like? Is there any civil defense against strategic level information warfare? What science, technology, or arcane art would provide the machine necessary to assure us that truth or validity had not been corrupted? Is there a truth-dosimeter awaiting discovery? Could attacks against some areas or categories of targets be withheld in a globally-internetted infosphere? What is information warfare termination and how would it be managed and by whom?

One can continue questioning. In the wake of massive information warfare attacks would some earnest scientists warn of an information winter, a global epistemological condition wherein "truth" is largely destroyed?[68] Would some argue for an "information weapons freeze" or "information weapon-free" zones? Would the bishops of one faith group assert that information warfare was only moral if it existed to deter?[69] Would another faith group issue a document entitled In Defense of Truth?[70] These and many other questions come to mind as the future possibility of strategic level information warfare is contemplated. Each is essential to making decisions on development, deterrence, employment, escalation, termination, and recovery from serious information warfare.

But if information warfare is not serious, how do we explain entities in the US like the Army's Land Information Warfare Activity, the Air Force's Information Warfare Center, the Naval Information Warfare Activity and Fleet Information Warfare Center, and their analogs abroad? How do we explain the existence of doctrine?

CONCLUSION

Information warfare represents the use of knowledge to confound knowledge and hamper effective action. The technologies are here, but the techniques await tests and trials. I imagine we will see some of these tests and trials during the period of confusion that will surround the Y2K manifestations. I imagine we will see more at the 2000 Olympics in Sydney, Australia. To protect ourselves and our information systems we must make *huge* strides in modeling, in integration, in securing agreement on triggering events, in understanding preemption, and in understanding escalation. Much or most of this must occur in secret. What will be highly visible, however, is the degree to which we are successful. Knowledge, as the Tofflers said, is what the wars and anti-wars of tomorrow will be about. Mars chuckles at these changes and Athena sighs that we have so far to go. To this point one must wonder whether or not we will succeed.

NOTES

[1] The views expressed are those of the author.

[2] *The President's Commission on Critical Infrastructure Protection*, October 1998, p. 30. Emphasis added.

[3] And will stun their taxpaying constituents, if they knew the real value of some of the targets both as tangible assets and as object residing on a hierarchy of military significance.

[4] Alvin and Heidi Toffler, 'Foreword: The New Intangibles', *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica CA: RAND MR-880-OSD, 1997), p. *xiv*.

[5] John Arquilla and David Ronfeldt, 'Cyberwar is Coming!'*Comparative Strategy* 2 (April-June 1993), pp 141-65.

[6] But not the internal world. There are some things of military significance—intentions and hostile will, for example—that await work undone in chemistry and biochemistry before they can be decomposed into the electrochemical impulses that can be reduced to zeroes and ones. That day will come. See Robert L. Solso, *Mind and Brain Sciences in the 21st Century* (Cambridge MA: The MIT Press, 1997), John Maddox, *What Remains to be Discovered: Mapping the Secrets of the Universe, the Origins of Life, and the Future of the Human Race* (London: The Free Press, 1998), and Steve Connor, "Science finds key to beating fear," *The Times Newspapers Limited*, February 22 1998.

[7] United States Air Force, 'Foreword', *Information Operations*, Air Force Doctrine Document 2–5, 5 August 1998, p. ii. Emphasis added.

[8] Air Force Doctrine Document 2–5, p. 2. Emphasis added.

[9] We must appreciate that careful word choices have been made before doctrine is approved for publication. The choice of the word 'primarily' appears significant to me.

[10] Especially in the alliance context. See Maria Seminerio, 'Infowarfare' part of NATO arsenal?" *Ziff Wire*, March 26, 1999.

[11] R. L. DiNardo and Daniel J. Hughes, 'Some Cautionary Thoughts on Information Warfare', *Airpower Journal*, Vol. IX, No. 4, (Winter 1995), pp. 69-79. Few appreciate the root of the word 'history'.

[12] The outgoing chief of staff of the US Army asserts that the keys to future warfare are 'knowledge and speed'

[13] Andrew Hay, 'Top Y2K problem: Public panic', Reuters, June 22, 1999, URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2280134,00.html.

[14] Jim Abrams, 'Spreading the Y2K word without spreading panic', http://www.nandotimes.com, June 8, 1999.

[15] See *The President's Commission on Critical Infrastructure Protection*, October 1998. On page 30 the authors observe, "Today, however, malefactors are no longer necessarily nation-states, and expensive weapons of war are joined by means that are easier to acquire, harder to detect, and have legitimate peacetime applications. The tools designed to access, manipulate, and manage the information or communications components that control critical infrastructures can also be used to do harm. They are inexpensive, readily available, and easy to use." As to who these "malefactors" might be the authors note on page A-4 that "A broad array of adversaries, including a sizable number of foreign governments, are currently capable of conducting cyber attacks." One must presume—and this is a speculation—that these foreign governments include those of most of the NATO nations, non-NATO Eastern European countries, Russia, Australia, Japan, China, India, Pakistan, some countries in Oceania and South America, South Africa, and others.

[16] 'Executive Summary', *Strategic Information Warfare Rising* (MR-964-OSD), p. 9.

[17] A serious disruption to the Internet, for example, would seriously and increasingly harm commerce in the US. Hackers L0pht, Mudge, Brian Oblivion, Space Rogue, Kingpin, Weld Pond, John Tan, and Stefan Von Neumann testified to a committee of the US Senate that they believed they could (or can), in the words of Space Rogue, "wreck havoc in the country [USA]." See James W. Brosnan, "Hackers testify they can crash Internet service in a half-hour," May 20, 1998, www.washtimes.com, "Stay Out! If you wanna hack here, you've got to be a member," 24 Hours in Cyberspace Inc., http://www.cyber24.com/htm2/6_204.htm, and L0pht's Web site at http://www.l0pht.com.

[18] Adam Hebert, 'Air Force Official Calls Reduced Cycle Times Key To Info Superiority', *Inside The Air Force*, June 21, 1999. According to the article, "Donahue [Lt. Gen. William Donahue, US Air Force director of communications and information] called Allied Force 'the coming of age of cyber warfare,' because of the attempts by Serbian computer operatives to attack U.S. information systems. 'Fortunately, they were about as effective at that as they were at air defense,' he joked."

[19] Defense Science Board, *Task Force on Information Warfare-Defense*, November 1996, Duane P. Andrews, Chairman, Section 2.2. Exhibit 2-6 assesses a major strategic disruption as "Low" by the year 2005.

[20] *Ibid.*

[21] Some disagree, asserting that natural occurrences, manifestations of the Y2K problem, and the slow erosion of our civil liberties are more grave dangers. See *Critical Infrastructure Protection and the Endangerment of Civil Liberties: An Assessment of the President's Commission on Critical Infrastructure Protection (PCCIP)*, (Washington, DC: Electronic Privacy Information Center, 1998) page 2:

> The most recent dangers to civil liberties comes [*sic*] from the new-found threat to our nation's infrastructure. An elaborate report identified a whole series of attacks that terrorists could wage against our communication lines, power grids, and transportation networks. Not surprisingly, perhaps, the report recommended a dramatic expansion of

government authority, new funding to combat the threat, and greater secrecy to conceal potential vulnerabilities as well as the work of the government agencies now tasked with defending us.

But there is another, perhaps more disturbing aspect of the PCCIP report. Almost every solution proposed by the commission represents some new expansion of government authority and some new encroachment into personal liberty. These recommendations follow from the description of a potential problem with barely a moment to consider the consequences for our form of open government.

[22] 'Executive Summary', *Strategic Information Warfare Rising* (MR-964-OSD), p. 1.

[23] Although we will use the United States as an example in many places, do not think that the US is the only 'larger' State that is at risk from information warfare.

[24] 'Executive Summary', *Strategic Information Warfare Rising* (MR-964-OSD), p. 2.

[25] For example, Forrester Research Inc., a Cambridge, MA-based market-research firm reports that last year, U.S. companies spent $43 billion in sales to each other over the Internet, five times the consumer retail total. In four years, the research firm projects business-to-business sales will reach $1.3 trillion and make up 9.4 percent of corporate America's purchases.

[26] Ross Kerber, 'Banks called lacking in Y2K information', *Boston Globe*, June 11, 1999.

[27] Ben Iannotta, 'Ground Stations Could Face Y2K Problems', *Space News*, June 21, 1999, Vol. 10 No. 24, pp. 14, 18.

[28] Let me emphasize most emphatically that this is not a malicious suggestion. It is merely an objective assessment based on the logic of the model for a new kind of warfare.

[29] That attacks against the United States may be deferred is consistent with this model: attack surrogates or proxies to learn. The learning is a precondition and preparation for acquiring the ability to attack larger States later.

[30] There are countries in these regions that may have done insufficient remediation and repair to be largely free of Y2K problems.

[31] Jube Shiver, Jr., 'Phone Firms May Have a Few Y2K Hang-Ups', *Los Angeles Times*, Monday, May 24, 1999.

[32] Some may be inquiring into these issues already. See 'Naval War College Sets Sights on Y2K', *Information Technology Association of America (ITAA) Year 2000 Outlook*, Volume 4, No. 21, June 4, 1999.

[33] These advantages may be compounded if defenders are thoughtless or loose-lipped enough to reveal their plans to potential attackers in advance. See 'DOD May Unplug From Internet Due To Security Worries At Century's End: NIPRNET would be network of choice', *Inside The Army*, June 21, 1999, p. 1. If the aim of this disclosure was to deter attacks, some tactics stronger than dropping-out or pacifism might serve more effectively.

[34] Chris Allbritton 'Cities Preparing for Y2K Problems', *Associated Press*, June 5, 1999. Allbritton writes:

> With about 36,000 local governments in the United States, cities' and counties' preparations for possible Y2K computer bug problems are literally all over the map.
>
> Local governments need computers to operate traffic signals, dispatch police and fire fighters, run jails and maintain sewer systems. Computers are also used to run payrolls, track taxes and manage fleets of city vehicles. So, possible fallouts from the computer problem range from the grievous to the glitchy.
>
> "Our greatest domestic risks for Year-2000 related failures are at the local level", said John A. Koskinen, chairman of the president's council on Y2K. On May 24, he announced a series of "community conversations", town hall-like meetings aimed at sharing information between local businesses and governments, utilities and community groups.
>
> Ultimately, about the only thing localities have in common is uncertainty.

[35] Alvin and Heidi Toffler, *Powershift: Knowledge, Wealth, and Violence at the Edge of the 21st Century* (New York: Bantam Books, 1990).

[36] Although the battlespace of the future may be increasingly transparent, there is little assurance that we will understand the 'meaning' of what we observe. If this is so, 'information superiority', the notion upon which *Joint Vision 2010* rests, is a pipe dream. See Richard Szafranski, Joseph A. Engelbrecht, Jr., and Frank Strickland, 'Meaning and Mystery', a paper presented at *EloKa Lw 2020*, Info Ops Workshop, sponsored by the German Air Force Staff (Fü L. II 1), Bonn, Germany, September 29-30, 1998.

[37] 'Indian Government Concerned Over Lack Of E-Commerce Capabilities', TELECOMWORLDWIRE, May 10, 1999.

[38] For example, the owner of a large timbering concern in the Amazon Basin confided that he believed that a rival timbering consortia from the Pacific region—not Brazil's citizens—funded the anti-timbering Amazon environmental concerns that were making the headlines in Brazil.

[39] Alvin and Heidi Toffler, 'Beyond Future Shock: Conspiracies, The Media And The War For The World's Mind', June 15, 1999, *Los Angeles Times Syndicate.*

[40] A reason we should be opposed to a reduction in intelligence and reconnaissance budgets and increased reliance on "open source" information is because denial and deception are among the most promising tactics of information warfare. For the next decade or so, the best and surest way to get another State's secrets will be to buy or steal them. Of the forms of theft, electronic theft may be the superior form.

[41] An idea suggested by Dr. Alan Stephens in an email discussion of the consequences and timing of the 'Melissa' virus.

[42] Stewart Taggart, 'Shutting Up Cell Phones', *Wired News*, March 26, 1999. The article notes that:

> If you want to neutralize pesky adversaries in wartime, disrupt their communications. If you want to do the same in peacetime, disable their mobile phones. By selling a frequency jammer that prevents mobile-phone communications over a limited area, an Israeli company has taken a classic swords-to-plowshares approach in commercializing a military technology.

[43] See '4 million gallons of sewage spilled during Y2K test', June 17, 1999, *Nando Media* and *Associated Press*, reported in http://www.techserver.com/story/0,1643,60855-96870-691455-0,00.html.

[44] Douglas Waller, 'Onward Cyber Soldiers', *Time Magazine*, Volume 146, No. 8, August 21, 1995. Waller describes a series of physical and cyber-engagements:

> First, a computer virus is inserted into the aggressor's telephone-switching stations, causing widespread failure of the phone system. Next, computer logic bombs, set to activate at predetermined times, destroy the electronic routers that control rail lines and military convoys, thus misrouting boxcars and causing traffic jams. Meanwhile, enemy field officers obey the orders they receive over their radios, unaware the commands are phony. Their troops are rendered ineffective as they scatter through the desert. U.S. planes, specially outfitted for psychological operations, then jam the enemy's TV broadcasts with propaganda messages that turn the populace against its ruler. When the despot boots up his PC, he finds that the millions of dollars he has hoarded in his Swiss bank account have been zeroed out. Zapped. All without firing a shot.

[45] Ultimately the target set of strategic information warfare may be the people's confidence in their leaders or their government. See M.J. Zuckerman, 'Survey: 45% of Y2K experts worried', *USA Today,* June 11, 1999

> The survey, which can be found at www.wdcy2k.org, shows deep differences:
> - **The economy:** 38% expect a 20% loss in stocks and recovery by 2001; 45% expect a mild six-month recession with 6% unemployment.
> - **Business:** 35% predict it will be "jolted a bit" with January "Y2K holidays" to make fixes; 28% see "major manufacturing disruptions."
> - **Utilities and infrastructure:** 40% predict at least "short-lived failures" up to seven days; 42% expect scattered supply and utility problems lasting at least two weeks.
> - **Government:** 19% predict one state government will run into "serious Y2K problems"; 30% expect "at least one major government agency," such as the IRS, will fail.

[46] *The President's Commission on Critical Infrastructure Protection*, October 1998, p. 28.

[47] See my 'Toward a Theory of Neocortical Warfare: Pursuing the Acme of Skill', *Military Review*, November 1994; and idem, 'When Waves Collide: Conflict in the Next Century', *JFQ: Joint Force Quarterly*, Winter 1994-95.

[48] Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century,* (New York: Warner Books, 1993), p. 3.

[49] Alvin and Heidi Toffler, *War and Anti-War*, p. 241.

[50] Brian Witten of the US Defense Advanced Research Projects Agency (DARPA) noted in a conversation that traditional economic metrics and some traditional business behaviors are vestiges of a Second Wave economy emphasizing atoms, not bits.

[51] This point at which we leave 'tradition' is, of course, debatable. See Kevin Kelly, *New Rules for the New Economy: 10 Radical Strategies for a Connected World* (New York: Viking, 1998), Stan Davis and Christopher Meyer, *BLUR: The Speed Of Change In The Connected Economy* (Reading MA: Addison-Wesley, 1998), Carl Shapiro and Hal R. Varian, *Information Rules: A Strategic Guide to the Network Economy* (Boston: Harvard Business School Press, 1998), and Regis McKenna, *Real Time: Preparing for the Age of the Never Satisfied Customer,* (Boston: Harvard Business School Press, 1997).

[52] Brian Witten of DARPA notes: "We've seen this already both in system administrator use of weapons like 'Back Orifice' for the innocuous management of many machines, and in the development JINI integrity enforcement mechanisms to reduce lifecycle costs of integration."

[53] Richard Szafranski, 'Awareness, Adroitness, Audacity', a presentation to the 'Mastery of Information: Technology and Operational Concepts Circa 2030' symposium, Joint Experimentation Futures Workshop, May 4, 1998.

[54] Brian Witten of DARPA calls this "The Network Effect of Knowledge" and notes that "… each new fact has value not only as a fact, but also in its probability of shedding new light on old facts and bringing more new facts to light. In other words, cooperation can let you learn faster – something critical to knowledge warfare."

[55] Paul Festa, 'Senate, FBI sites down on hack attacks', *CNET News.com*, May 28, 1999, 12:05 p.m. PT, http://www.news.com/News/Item/0,4,37194,00.html.

[56] Michael Skroch, "Development of a Science-Based Approach for Information Assurance," Defense Advanced Research Projects Agency (DARPA), Information Systems Office (ISO), May 10, 1999. Skroch writes of the need to "develop equivalencies, relationships, laws, logic, postulates, proofs, and methods for calculation so that cyberscience and metrics can be used effectively. Just as in other disciplines, complexities of systems will often not allow for closed solutions; therefore, modeling of IA [information assurance] will be needed."

[57] Such a group might be subdivided into print, visual, and voice components.

[58] Perhaps someday this will take separate Information Forces or more robust Air Forces.

[59] See Jeffrey R. Barnett, *Future War: An Assessment of Aerospace Campaigns in 2010* (Maxwell AFB AL: Air University press, 1996), p. xxii-xxiii. For the underpinning logics see Ralph D. Stacey, *Managing the Unknowable: Strategic Boundaries Between Order and Chaos in Organizations* (San Francisco: Jossey-Bass Publishers, 1992, John H. Holland, *Hidden Order: How Adaptation Builds Complexity* (Amsterdam: Addison-Wesley Publishing Company, 1995), T. Irene

Sanders, *Strategic Thinking and the New Science: Planning in the Midst of Chaos, Complexity, and Change* (New York: The Free Press, 1998), Peter F. Drucker *Innovation and Entrepreneurship: Practice and Principles* (New York: Harper and Row Publishers: 1985), Dan Dimancescu and Kemp Dwenger *World-Class Product Development: Benchmarking Best Practices of Agile Manufacturers* (New York: American Manufacturing Association, 1996), David M. Anderson *Agile Product Development for Mass Customization* (Chicago: Irwin Professional Publishing, 1997), Clayton M. Christensen *The Innovator's Dilemma: When Technologies Cause Great Firms to Fail* (Boston: Harvard Business School Press, 1997), Jeremy Hope and Tony Hope *Competing in the Third Wave: The Ten Key Management Issues of the Information Age* (Boston: Harvard Business School Press, 1997).

[60] According to the article 'DOD Creates Office To Battle Cyber terrorism', July 24, 1998, *Newsbytes*:

> The new office, which DOD officials still must name, will be part of the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence and will manage Defense efforts to safeguard the nation's critical infrastructures.
>
> These include telecommunications, banking and finance, energy, transportation and essential government services.
>
> "Because of our constitutional orientation and our history, (DOD) is not going to be the lead in anything, but we will be the backbone of everything, when you get down to it," he said.
>
> The DOD office will work closely with the Justice Department's National Infrastructure Protection Center and the multiagency Critical Infrastructure Assurance Office, Hamre said: "We have committed ourselves and are supporting the National Infrastructure Protection Center," Hamre said: "We provide the deputy, and we'll provide, I believe, three of the five heads of the directorates."
>
> The FBI's new National Infrastructure Protection Center (NIPC), at FBI headquarters and headed by Michael Vatis, will gather threat and vulnerability data and then disseminate analyses and warnings of threats to both the government and private sector.

[61] There were a few late-arriving exceptions. See 'Allies Target Computer, Phone Links', *Washington Post*, May 27, 1999, p. 1. See also 'Yugoslavia Loses Satellite Signals', SkyREPORT.COM E-News for 05/28/99, wherein we read, "Eutelsat has been under pressure from NATO to suspend transmissions. Yugoslav broadcasting facilities, regarded by NATO as part of the country's propaganda machine, have been a target in the NATO bombing campaign."

[62] David Ronfeldt, *'Beware the Hubris-Nemesis Complex: A Concept for Leadership Analysis'*, (Santa Monica CA: RAND MR-461, 1994), p. 31.

[63] One reviewer noted:

> Conversely, although cyber aggression and counter cyber-aggression may be non-lethal in nature, civil or military authorities obviously must take care when considering both attacks and retaliation against cyber-warriors. The arrest of one notorious hacker or an-

other has not slowed the exponential growth of the hacker community. Indeed, over a thousand hackers attended the DEFCON 7 hacker convention. Hackers so far do not appear to be dissuaded by the risks of mucking with the exponentially increasing global value of e-business. On the contrary, they seem to be encouraged by the anonymity afforded by a community growth rate that tracks the growth of the Internet.

[64] Alvin and Heidi Toffler, 'Foreword', *In Athena's Camp*, p. x*viii*.

[65] I do not know to whom strategic information questions should be asked.

[66] Scott D. Sagan, 'SIOP-62: The Nuclear War Plan Briefing to President Kennedy', *International Security*, Vol. 12, No. 1 (Summer 1987), p. 22, and Barbara G. Levi, Frank N. von Hippel and William H. Daugherty, 'Civilian Casualties from 'Limited' Nuclear Attacks on the USSR', *International Security*, Vol. 13, No. 3 (Winter 1987/88), p.169.

[67] Robert J. Wood, 'Information Engineering', An Air War College Research Paper written in fulfillment of the curriculum requirement for graduation from the Air War College, Maxwell AFB AL, 1995.

[68] Dennis M. Drew, *Nuclear Winter and National Security: Implications for Future Policy* (Maxwell AFB AL: Air University Press, 1986).

[69] US National Conference of Catholic Bishops, *The Challenge of Peace: God's Promise and Our Response* (Washington DC: Office of Publishing Services, United States Catholic Congress, 1983). Often referred to as the bishops' "pastoral letter" on the morality of nuclear deterrence and nuclear war.

[70] The United Methodist Church's Council of Bishops, *In Defense of Creation: The Nuclear Crisis and a Just Peace* (Nashville TN: Graded Press, 1986). If there is such a thing as an "information winter", it would be "truth", not "creation", that needed defenders.