NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIFORNIA

INFORMATION WARFARE DELPHI:
RAW RESULTS

by

Roger Dean Thrasher

June 1996

Approved for public release; distribution is unlimited.

Approved for public release; distribution is unlimited.

The views expressed herein are those of the author and the individual Delphi contributors and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

This document contains the results of research conducted using a modification of the Delphi method with participants from a variety of backgrounds (see Table I). This research was designed to probe the nature and acquisition impacts of information warfare and the raw research results have been integrated into a Naval Postgraduate School thesis entitled "Information Warfare: Implications for Forging the Tools." However, the Delphi responses are complete enough to stand on their own and so are being made available separately.

Name	**Organization**	**Remarks**
Al Campen	Manager, AFCEA International Press	editor of The First Information War
VAdm Arthur Cebrowski, USN	Joint Staff	Director, J-6
Peter Cochrane	British Telecom	Director, British Telecom Research Lab
Dr Fred Cohen	Management Analytics	author of Protection and Security on the Information Superhighway
James Dunnigan	Author	author of Digital Soldiers
LCDR(N) Robert Garigue	Director Intelligence, Security and Operations Automation, Canada	Deputy Program Director, Joint and Strategic Information Systems
Dr Fred Giessler	National Defense University	Information Warfare Course Director
BG David Gust, USA	US Army	Program Executive Officer, Intelligence and Electronic Warfare
James Hazlett	SAIC	Senior Analyst
Ken King	Digital Equipment Corporation	Director, External Research Group
Dr Fred Levien	Naval Postgraduate School	Chairperson, Information Warfare Academic Group
Dr Martin Libicki	National Defense University	author of What is Information Warfare?
CDR Michael Loescher, USN	Office of Deputy Assistant Secretary of the Navy (C4I/IW)	Director, Information Warfare
Mr Larry Merritt	Air Force Information Warfare Center	Technical Director
Dr David Probst	Concordia University	Professor of Computer Science
Winn Schwartau	Interpact	author of Information Warfare: Chaos on the Electronic Superhighway
Robert Steele	Open Source Solutions	CEO
Col David Todd, USAF	USAF/XOXT	Chief of Technical Plans

Table I. Delphi Participants

TOPIC A: CHARACTERISTICS OF INFORMATION WARFARE

While it is probably non-productive to try to settle on a definition for information warfare in this forum, it may be useful to bound the subject by discussing the defining characteristics of information warfare. This topic will also provide context for future rounds.

[Moderator] What are the defining characteristics of information warfare?

[Campen] The risk in seeking a definition is the temptation to look for correlation with the past, rather than defining differences. I have seen definitions of IW [Information Warfare] that are useless because they encompass all human endeavor. I argue that the definition of IW must be severely circumscribed if it is to be useful in assessing the impact on policy, doctrine, functions and organization on civil or military. We must seek out what is different from the past. I submit that difference is dependency upon vulnerable electronic technology. I limit IW to information (data) in electronic form and the hardware and software by which it is created, modified, stored, processed and moved about. The defining characteristics are dependency upon and vulnerability of electronic information systems. Example: Psyops [Psychological Operations] conducted via printed leaflets is not IW, but radio broadcasts or the electronic manipulation of TV images is. The physical destruction of a telephone exchange is not IW (telegraph lines were cut in the Civil War and submarine cables in WW One), but disabling a switch with a virus is IW.

[Cebrowski] The underlying character of information warfare is the proliferation of information-based technologies and their associated impact on society and by extension, on the bedrock issues of national security in the modern age. In warfighting, information-based technologies transcend the target sets of information, information-based processes, and information systems.

[Cochrane] The defining characteristic in information warfare is when information (in ANY form, so that includes ideas and philosophies) is supplied, or obstructed, with the aim of causing the information user to make a bad decision, or to confuse/overload their communication or decision making processes.

Examples:
- Knowing what your enemy does not
- Confusing the enemy with false information
- Damaging the information capability access of the opponent or denying him access to his own information
    - jamming of communications
    - hacking computer systems and changing or deleting data
- Interception of communications
- Use of disinformation
    - propaganda
    - cultural infiltration

[Cohen] The broadest common definition I have been able to get together is: Conflict in which information or information technology is the weapon, the target, the objective, or the method. From now on, I will use IT to indicate "information or information technology."

[Dunnigan] Attacking and defending the ability to transmit information.

[Garigue] The first thing that comes to mind is the realization that information warfare is

a consequence of a new and emerging SocioTech structure. This emergence is not homogeneous throughout the world. Where as some Western societies are moving rapidly into it, others have not yet started. Modern societies are all presently engaged in building and riding a glass highway. With this in mind we have to face the fact that more and more of our social, economic, political and cultural transactions are digital in nature and all of them are computer mediated. Which means that in an information society no meaningful event can happen between individuals or organizations without computers and networks. We will have to fulfill our human interactions and commitments through our computerized social networks. We presently, and naively, place a lot of trust in these computer intermediaries that tell us the state of our complex systems. These systems may be cities, financial markets, health, wealth, production or even distribution. All these SocioTech systems are subject to computer control. Computerized networks bridge Decision Makers with an ever increasing array of sensors and effectors that monitor and intercede for us and help us in governing our complex environments. This trend will continue accelerating wherever efficiencies in systems can be found. As with a human constructed artifact there are flaws, failings and limitations. These new efficient networked SocioTech societies are also, and will always be flawed. Control over these systems is not more direct and local. Now it is remote and distributed. In open societies, authority to control is conferred by groups onto individuals via legitimate processes in accordance with common values and beliefs. But groups whose goals differ and whose objectives are at odds will try to impose control by force of arguments or might. So now in computer mediated societies as control has been somewhat centralized within the network layer, we see that there will be a clash of wills for control of that logical space. The fight for control of that space is called information warfare.

[Giessler] Competing and conflicting information, control and communication in complex adaptive systems—which all have teleological goals with the ultimate being survival…All systems are involved in information warfare—the only question is do they do anything about it? They can be a passive or active player. IW is all about decisions and the use of information, energy and material resources to offset disturbances that may drive your system away from the attainment of its objectives—especially the one about survival.

[Gust] Definition—after two years of discussion, the Army's TRADOC [Training and Doctrine Command] published FM 100-6, Information Operations. We argued and discussed the definition and who is in charge, even sought and rejected OSD [Office of the Secretary of Defense] staff advice on the definition. I do not believe there is universal agreement on it yet.

[Hazlett] Information Warfare is conflict between parties where information, or information systems are used to attack and defeat the enemy or when the enemy's use of, or access to, information is attacked.

[King] Information Warfare is a conflict between two parties where information technology is the primary means of obtaining a defensive or offensive advantage.

[Levien] One of the most critical of these is the fact that it is so imprecise. It obliterates any of the past definitional boundaries of “what is an act of war?”, “what is war?”, “who is the enemy?”, “where or which is the enemies’ territory or country of national origin?” This now much more difficult assessment of responsibility places new limits on how the military can react against a perceived threat to the country. In fact it becomes painfully difficult to determine an allowable course of action for a military officer to take when he (or she) is faced with the enormous body of U.S. law that (rightfully) limits and restricts those actions that the military can take against U.S. citizens. In today’s world these same U.S. citizens are inextricably coupled via communications, business association, commercial activity, and just plain vanilla personal interactions with foreign

(international?) entities…both friendly and often hostile as well. This can and most often does present a legal NIGHTMARE for the average military officer to sort out what actions he is permitted to take in this IW environment.

[Libicki] Information warfare is any activity motivated by the need to alter the information streams going to the other side and protect one's own. These range from physical and radio-electronic attack on both systems and sensors (or associated support systems), to cryptography, attacks on computers, and psychological operations.

[Loescher] What is new is that information creates and splinters the battle space, enables and defines the killing zone, and provides the means to execute the principles of war. I prefer to call this "war in the info age", which I think is a genuine revolution. In Navy, the term info warfare is being used evolutionarily by some communities to preserve and improve the past—better EW [Electronic Warfare], better cryptology, better, etc.

[Merritt] This is a good question. These days, there is a lot of press being given to equating IW to network attack (offensive and defensive). In my view, this is a very narrow interpretation and really is not doing the community justice in really working the problem. I think this is why we are now seeing more reference to other terms such as info dominance or info operations. In my view, IW consists of any action to exploit or affect an adversary's ability to gain a true picture of the battle space or to execute command and control of their forces. Also includes all the same activities associated with protecting our own capabilities. This truly brings in all aspects of EW, network attack, node analysis, intelligence, reconnaissance and surveillance, etc., both terrestrial and space based. This broad interpretation has been the cause of much controversy that has crossed traditional ricebowls and caused the community to concentrate on particular aspects of the problem.

[Probst] Information-based warfare is that branch of warfare information technology that supports two basic pillars of the Revolution in Military Affairs, viz., (i) Dominant Battlespace Knowledge, and (ii) Integrated Battlespace Management, including pre-engagement battlespace preparation, precision force (including just-in-time strike), and precision logistics. To be effective, these pillars require major advances in modelling and simulation, which in turn require (i) advanced control theory for automated full-spectrum strategic decision making, precision scheduling, and other information functions, and (ii) high-performance data assimilation and analysis for data-intensive predictive modelling and simulation.

Because it relies on high-performance computers and communications, Information-Based Warfare can be disrupted. Defensive Information Warfare trys to make sure that this cannot happen to our forces. Offensive Information Warfare—about which I have some reservations—trys to disrupt the computer-and-communications-based C4ISR [Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance] of the adversary.

Definitions aside, we can see three embryos of Warfare Information Technology today. These are:

- total situational awareness ==> Integrated Battlespace Management
- network security ==> Defensive Information Warfare
- the USAF Captain, using SIPRNET [Secret Internet Protocol Router Network], who subverted the Navy's Atlantic Fleet command in September 1995 ==> Offensive Information Warfare

The following is an equivalent vanilla base line for Information Warfare:

- high-performance information-based warfare with dominant battlespace knowledge, and precision force—including offensive information warfare—will alter the strategic, operational, and tactical levels of war (i.e., it will change the appearance of combat)
- information infrastructures are now part of the logistics tails of all armed forces, and—as such—require careful defense
- conversely, one may consider degrading the information systems that enhance the military capabilities of the adversary

[Schwartau] I maintain that True Information Warfare is the use of information and information systems as weapons against target information and information systems. I eliminate the call for or use of any bombs or bullets in True Info War. IW can attack individuals, organizations or nation-states (or spheres of influence) through a wide variety of techniques:

- *Confidentiality compromise*
- *Integrity attacks*
- *Denial of Service*
- *Psyops*
- *Dis/mis-information, media, etc.*

Most clearly, though, the distinctive feature of Pure IW is that it can so easily be waged against a civilian infrastructure in contrast to a military one. This is a new facet of war, where the target may well be the economic national security of an adversary. In addition, though, we have distributed capability to wage war. Today, a small band of antagonists can launch an IW offensive from behind their desks thousands of miles away; or a group of U.S. hackers might choose to declare war on another country, independent of any official U.S. sanction. The capabilities of IW is the issue: how much havoc can I rain without resorting to bombs and bullets. A lot is the answer, and I'm not the only smart guy on the planet.

[Steele] The defining characteristics of information are:
- Connectivity (all mediums)
- Content
- Coordination (standards, procurement)
- Communications & Computational security
- Context (both cultural and substantive)

Information "warfare" is almost moot or an oxymoron. In this era, failing to be competitive in optimizing the above five aspects of information is tantamount to abdication. At a very simplistic level information warfare can be thought of as an attack on any of the above five elements (e.g., denial of service or corruption of content). On the defensive side, again at a simplistic level, it can be considered in terms of continuity of operations. Unfortunately, our own DoD will never be a serious IW player until they figure out that collecting information, and the sensor to shooter interface, is the heart of information-based warfare operations.

[Todd] With warfare in the information age, our ability to control and exploit the information battlespace will be as much an enabling factor in combined warfare as the ability to control and exploit the air and space battlespace to enable conventional combined terrestrial warfare in the industrial age. Note that I don't use the term "information warfare." The challenge of warfare in the information age is more pervasive than the commonly thought of niches of information warfare. But within this category of IW falls our capabilities to attack an adversary's information function (regardless of means), the protection of our information functions (regardless of means), and that IW is a means, not an end.

[Moderator] Are "information in war" and information warfare the same?

[Campen] Definitely not. Information-in-war describes how information has been used since the dawn of conflict: Always sought, usually too late or wrong, not always properly used or effective when used. Information-in-war was serendipitous and usually incidental to the conflict. It was an adjunct to war, with an impact varying from nil to absolutely vital in rare, notable incidents. In IW, if there is no information there may well be no war. Example: Smart missiles but no means to instruct them, or the XXI [Force XXI] Soldier who's GPS [Global Positioning System] fails, is lost, and cannot perform assigned function, or "just-in-time" logistics that aren't.

[Cebrowski] No. The premise of information in war involves the process by which raw data (sensors or intel sources) is converted to information for decision-makers, and how that information is distributed and acted upon by operational commanders. Information warfare is the means by which we affect information in war. This can be done by targeting an adversary's information, information-based processes, information systems or computer-based networks. Equally important is protecting our own information, information-based processes, information systems, and computer-based networks.

[Cochrane] Information is a tool and a target of war (just like a tank or a munitions factory). Information in war includes details about the enemy (his strengths, weaknesses, deployment, location of resources, communications). Information warfare is using information technology, either to gain data about the enemy or to destroy the enemy's data resources or cultural support.

[Cohen] Not in my view. Information in war includes every aspect of IT as applied during conflict. IW includes only situations where IT is the weapon, target, objective, or method. For example, supporting warfighting with mapping and weather information is not IW except in the cases where the mapping information is the weapon, target, objective, or method of conflict. In ancillary roles, it's not part of IW. In this view, every piece of IT may sometimes be part of IW, but most parts are never part of IW. In other words, it is the "USE" of IT and not some inherent property of the IT that applies.

[Dunnigan] No. The former is a product, the latter is an action.

[Garigue] The distinction is akin to looking at the subject that performs the action or the object on which we act. These are different approaches to the same subject. Although many would see them as different I see them as being a continuum. From the meta-strategical aspects of Information Warfare we see what we are trying to achieve, such as looking at the objectives and the criteria by which we determine if we have achieved them or not. Information in war relates to the managerial aspects of how to do it. So Information Warfare help us to focus on effectiveness issues and Information in War helps us focus on efficiency issues. But the two cannot be separated from each other and need to be considered as a two sides of a same coin.

[Giessler] No—the DSB [Defense Science Board] concept from the '94 summer study was valuable. I in W is the use of information technologies to better conduct what we traditionally know as modern warfare and the Tofflers would call warfare in the industrial wave. In this mode information is a supporting element to air, land, sea, space and SOF [Special Operations Forces] warfare. It is a force multiplier. IW is warfare in the information realm, environment and age. It includes old but also new forms and qualities of warfare—the fight for survival. It is facilitated by IW technologies that create a unique confluence that allow competition and conflict never before considered. And we are about as smart about what that warfare is as Billy Mitchell was about air warfare and power in 1917 when he was teaching and thinking about it at Langley Field.

[Gust] Info in war can mean the Blue Force use of info while info warfare means, to me, both Blue Force protection actions of their info while offensively exploiting the Red Force's info.

[Hazlett] No, many forms of information are used in war, not all of which is used in information warfare. In information warfare, information is the weapon and/or the target.

[King] No. All participants in a war have always made use of any available information but it was always in support of the primary operations.

[Levien] "Information in war" and "information warfare" are poles apart in meaning. (Ah the beauty of the English language!) Information in war…is essentially a meaningless phrase in that it adds very little to the concept of the role information plays in wartime as opposed to any other time in the affairs of man. On the other hand…coining the new term "information warfare"…where information is the descriptive term of war…implies a new dimension of how to wage war, which is as highly distinct as the term (for example) Nuclear War. The potential effects of IW, while not as physically dramatic as nuclear, could nevertheless in the future be as historically significant as nuclear war in its resulting outcome.

[Libicki] Information in warfare is so broad a category as to be meaningless; what kind of warfare does not involve information?

[Loescher] See above.

[Merritt] I don't think so. Info in war as I see is that info that allows you execute your mission. This is needed in whatever conflict that we are involved in, whatever realm we are operating (i.e., space, air, land, info). Info war is the utilization of the info realm to gain advantage in wartime.

[Probst] Information In War has an elementary and an advanced stage. In the elementary stage, data is converted into information for use by experienced decision makers; in the advanced stage, viz., integrated battlespace management, computer systems generate and evaluate alternate warplanning scenarios using modelling and simulation technology.

Information Warfare concerns the protection or disruption of this process.

[Schwartau] Absolutely not. I consider information in war to be making conventional weapons more efficient; to bring better information to the HQ [Headquarters], process it better and faster, and get the necessary information out to the war fighter as fast as possible. The closer to real time and iterative the process is, the better. This approach makes wars less bloody, increases efficiency and maximizes the capabilities of the existing arsenals. What I find intriguing about this thought model is that is the same paradigm for commercial companies, except for the bullets, which makes it in their case closer to a Class II style information war.

- Market research
- Competitive analysis
- Decision making
- Sales/Marketing efforts
- Feedback

The convergence of military and commercial IW issues is obvious, at least to me. :-)

[Steele] See above. "Information in peace", or information peacekeeping, is the flip side. Where we have a major disconnect today is in the existing bureaucratic mind-sets and

forms of organization. The battlefield is civil, but no civilian organization is ready to get organized, and the military is saying "it's not my job" to provide for the common defense of the civil sector…

[Todd] Military history has multiple examples of how "Information in war" is often the leveraging factor in successful engagements and campaigns. But the common thread is that engagements were necessary to impose one's will upon the enemy. At the other end of the pendulum, information warfare is viewed along the lines of Toffler and Schwartau in which one can impose one's will upon an adversary through the control, manipulation and denial of information, similar to the Soviet theory of "reflexive control." A more useful notion is that of information-based warfare. This falls in between those two extremes. Not only is the advantages of information technology realized through the abilities to engage the adversary with less friendly forces but having overwhelming impact due to timing and targeting, but in information-based warfare we can integrate military disciplines to manipulate the adversary's perceptions at the tactical, operational and strategic levels. Information-based warfare, consistent with previously accepted operational art, will still require changes in organization, technology adaptation, and changes in operational concepts and doctrine.

[Moderator] Is "cyberspace" a new medium (like the traditional media of air, land, sea and space) of competition and conflict between nations, businesses and other organizations?

[Campen] No. Land, sea, air (and perhaps space someday) are media where physical things (people, ships and aircraft) interact. If cyberspace means the ether, then it does not qualify because no conflict actually takes places in that media. If cyberspace is defined as including the physical devices mentioned above (computers, communications, etc.), then it does not qualify because those devices are being employed in one or more of the existing media (air, land, sea), not in the ether.

[Cebrowski] Cyberspace is more of a cliche than a medium. A medium implies that definitive boundaries or characteristics exist—cyberspace is too ubiquitous to be bounded, and thus, shouldn't be considered a medium.

[Cochrane] Information is a commodity of war, like food and fuel. Cyberspace is a new transport mechanism and hence a target like a road. Cyberspace covers sea, land and air with its transport mechanisms. The fact that the Internet is accessible by anyone from anywhere in the world means that machines attached to the net are under threat of attack from unfriendly machines which are also connected.

[Cohen] New? Not really. Separate and different? It may be advantageous to treat it that way.

[Dunnigan] Only new in terms of much greater mass and velocity.

[Garigue] Cyberspace is not a physical space but a true social space. Unlike the other mediums where geography and physics structures relationships of force, in Cyberspace only information and knowledge determines the structure of power. Distances, geography, and borders become artificial and abstract notions and do not regulate the relationships between individuals and organizations. There are no inherent constraints in Cyberspace (except bandwidth and IP [Internet Protocol] addresses but this is not seen as a major source of future conflict) so there is no real reason to fight for possession of something that has no space or territory. However, the fact that this domain can amplify perspectives and thus exert influence over Decision Makers as well as potentially control systems that can acquire, transmit, store, analyze and produce wealth, there is certainly a danger of a clash of goals.

[Giessler] It is a new realm of conflict and competition that has evolved since the mid 1800s. But the advent of the chip, satellite coms and sensing, fiber optics and technological advances in software, hardware, orgware, brainware, decisionware, etc. have created changes which have resulted in a discontinuous function and reality.

[Gust] Cyberspace, like frequency spectrum, will become a nationally controlled asset. Due to access via various means, i.e., direct satellite, phone lines over land, fiber optic cables undersea, etc., it will be hard to control. Use now precedes policy.

[Hazlett] Yes, it has boundaries similar to those between other mediums and environments, across which attacks can be mounted either physically or electronically.

[King] "Cyberspace" is a new medium of communications with its own set of characteristics. Commerce will become the primary medium of competition and conflict and the most likely target of electronic attacks.

[Levien] Cyberspace is a concept of a state that exists only in the mind's eye. It has no physical properties, no dimensions…nothing to touch…or feel. This as opposed to land,

sea, atmosphere, etc., which can be described with physical constants and dimensions and to which the Laws of Physics (immutable as they are) can be applied thus allowing us to predict their behavior. Not possible with Cyberspace. So if you can't describe it…and you can't predict it, it's hard to protect yourself from it. You can perhaps try to change the effects which it produces, but that is another matter altogether.

[Libicki] Unlike all other media, there is no such thing as forced entry in cyberspace.

[Loescher] Potentially. But Clausewitz has to be reexamined in our age. War is only an extension of politics if there is a discernable politic. I don't think the medium is inherently a medium of competition and conflict. But it probably will become so like the others. It's probably better to think of information as a competitive topic than of cyberspace this way—although cyberspace is definitely a new medium the prime characteristics of which are virtuality (i.e., independent of time and space)

[Merritt] In my view, yes. Many contend it is nothing new but just an extension of old capabilities. I disagree. The ability to quickly gain access to data, systems, etc., anywhere in the world within seconds is a leap of capability that is just now being utilized. In my view, we have barely scratched the surface of this capability. In this "virtual world" a whole new methodology with new tactics, new laws, new players, and new results tends to support the argument that this is indeed new and until we get true buy-in on this issue, the true capabilities of IW will not be realized.

[Probst] If it is possible to attack across cyberspace, and to achieve cyberspace dominance, then we would have to call it a new medium. I think this is an exaggeration. What is feasible is to have an order-of-magnitude competitive advantage in both battlespace knowledge—which implies understanding—and integrated battlespace management. Your question then becomes secondary.

[Schwartau] Hell yes! If I have the ability to raise havoc with an Army or Navy or Air Force, and I exclusively use cyber-weapons, then of course it's an added dimension. The weapons arsenals I propose use:

- invisibility
- passivity
- insidiousness
- mind screwing

I believe we need a center of IW excellence, yes, perhaps an independent force, which houses all of the expertise, and then is appropriately distributed as needed to other services as required. This "Cyber-Force" (I don't have a better name yet) can act on it's own without conventional service aid, or in combinations with others.

[Steele] An old medium with a new importance. Especially troubling because of the stealth and anonymity that any individual can exploit. Has radically altered the balance of power between nations, organizations, and individuals, and left all intelligence communities two decades behind the learning curve.

[Todd] "In many respects, one can consider information as a realm, just as land, sea, air, and space are realms." Realm as defined as: the region, sphere, or domain within which anything occurs, prevails, or dominates. "Information has its own characteristics of motion, mass, and topography, just as air, space sea and have their own distinct characteristics. There are strong conceptual parallels between conceiving of air and information as realms." {Cornerstones of Information Warfare, Sep 95}. Just as air and space forces attempt to control and exploit air and space in order to enhance all military force's effectiveness, so to must all forces attempt to control and exploit the information

realm to enhance all military force's effectiveness.

[Moderator] Is there really anything new or different about information warfare?

[Campen] Definitely. Because of dependencies and vulnerabilities of information systems, the potential exists to gain advantage or victory without resort to traditional means of force, or perhaps with fewer forces. Example: Manipulation of opponent sensor data can make things appear other than they are. Manipulation of opponent data could disrupt logistics and troop flow. (Fustest with the mostest!) when you are actually neither.

[Cebrowski] Although the nature of war will always remain constant, the character of war is in constant change. Information permeates society—as a pillar of national security, as well as the military—where the fractional component of information technology continues to grow in warfighting systems. U.S. dependence on information and associated technologies, coupled with rapidly expanding global interdependencies, exposes vulnerabilities that can be exploited using IW, both here and abroad.

[Cochrane] One potential difference for countries like the U.S. is that the battle can be waged with the civilian population in their own backyard from day 1. In this respect information warfare could represent a threat that is comparable to nuclear missiles, without the tell-tale sign of a missile launch.

Important factors are:
- Low entry barriers mean ANYONE can start a "war"
- The speed of distribution
- More numerous ways of going about the war
- Harder to find the culprits
- More efficient (bigger bangs for your buck!!!)
- A success will be seen by more of your enemies
- Inflicted damage can potentially be far higher than earlier technologies

[Cohen] Yes. The difference is that we now depend on IT for every aspect of our existence as a society. This increased dependency means that the inherent vulnerabilities of IT extends to our ability to wage war, survive economically, and to the very fabric of our society.

[Dunnigan] Greater mass and velocity. U.S. Grant standing next to a telegraph operator was waging info war, but the speed of data transmission was less than 300 baud.

[Garigue] Yes—but most of it has yet to be seen as the impact of living in an information society becomes real. However, the initial impact will be the rapid redistribution of power away from institutions that used to control simply through possession of information; such as intelligence organizations, government, big corporations, multinationals, and professional organizations. Power will come from the capacity to create and apply new knowledge. It is the capacity to apply new knowledge that will permit organizations to determine their future by simply deciding which future they want.

[Giessler] Yes—much is new. The newest is that we don't know what all is new. Just as Billy [Mitchell] didn't know how air warfare was new we are incapable of specifying how IW is new. And it doesn't make any big difference. Those who can not allow out-of-the-box thinking will just not survive in the info age. They may be fine if they stay in the industrial age. They will even be needed there. IW is all about influencing minds (as Sun Tsu wrote about) but with new technologies and wares.

[Gust] We have some thinking to do about jamming vs. intercept. We can now do so much more selective jamming and denial, and destruction because of technology. Intercept still provides so much Red Force intent that it must not be set aside because of our ability to defeat the Red info systems.

[Hazlett] Yes, in information warfare, information is the target, and sometimes the weapon. In other forms of warfare, it is generally a bi-product or collateral target, but not the primary medium or target.

[King] It is different in that the experience and expertise from centuries of regular warfare are of very little value in information warfare. Thus it is a revolutionary change not an evolutionary one.

[Levien] To answer this question you have to decide what your timeline of reference is for the word "NEW." When do you start in deciding what is new? In many ways IW is simply a repackaging of a great body of knowledge that has been around for quite some time. PSYOPS, deception, for example…the world's history is replete with example after example of these two subjects. Ditto with the fifth "pillar" of C2W destruction. As you get to the subject of EW in C2W, you have a more recent series of events to consider. But it is clear that unlike the dawn of the nuclear age, with the discovery that $e=mc^2$, there is no single defining technological breakthrough that heralded the age of Information Warfare. There ARE some technologies that make the advance of civilization possible which then in turn were applied to warfare (as always) but these were not specifically developed for Information War. What has happened is a sort of rearranging of the chairs around the table of knowledge. But this is not a trivial shift. For it opens up…no, rather it demands…that the military strategist and planner consider fields of interest which heretofore he has been (happily) able to almost ignore. The most significant change that I see occurring is:

IT REQUIRES A MUCH CLOSER COUPLING OF THE MILITARY AND DOD WITH THE U.S. INDUSTRIAL AND COMMERCIAL BASE IF WE ARE TO SURVIVE AS A NATION.

This relationship in the past has often not been a close or comfortable one, with both parties trying to keep the other at arms length. (With the possible exception at the height of large wars). And it certainly is not the general attitude of the U.S. populace at large these days with the desire to keep the Government more and more out of our daily lives. In the response to our efforts to combat the threat of IW, it may finally dawn on both sides of the parties to these debates, that closer ties are no longer an option. If one examines the actions of some of our "allies"…e.g., France, Israel, Japan…you can see these partnerships forming with often devastating results to U.S. interests.

[Libicki] At the operational level, as the processing of information becomes systematized (e.g., the systems component of the command center, Admiral Owens' System of Systems, the NII [National Information Infrastructure]), attacks on and defenses of such systems becomes important. At the strategic level, there is nothing really new.

[Loescher] Yes. See above.

[Merritt] See above. I think yes…

[Probst] There are two new aspects, both rather obvious. Progress in high-performance computers and communications will lead to a Revolution in Military Affairs, although there are more advanced and less advanced thinkers about how this should happen. We depend on our computers in unprecedented ways. As cooperation gives way to contention, we find our computers have much thinner skins than we ever imagined.

In brief,

- information technology is on the point of causing a paradigm shift in information-based warfare

- we may generalize counter-force to counter-information system

[Schwartau] I keep hearing the arguments that IW is nothing new, but I have to argue that for the first time in history, the capability exists to wage a conflict (indeed a war) where no conventional munitions are required to achieve a stated goal; be that goal isolation, economic deactivation, sanctions or alternative to combat.

[Steele] Not yet. All I see at this point is industrial age concepts applied very poorly to information age opportunities.

[Campen—general comment] Happy to note from summary that I am not alone in preferring a technical emphasis on Information Warfare. I have concluded that the essential difference between information from past conflicts and the present is the word INSTITUTIONALIZED. We are now trying to shape doctrine, organization and process around the assumption that information can be a key, or perhaps the key ingredient in conflict. This is not my notion, but I can't remember who first brought it to my attention. It may have been Cohen, or perhaps Probst. I intend to incorporate this new perspective in my next round of lectures at the NDU courses on Information War.

TOPIC B: TECHNOLOGY OF INFORMATION WARFARE

Much of the recent focus on information warfare has been related to the stunning advances in information technology. Since technology appears to play such an integral part in information warfare, this topic seeks to explore the implications of this relationship.

[Moderator] Is information warfare technology dependent or technology enabled?

[Campen] Both. Same coin, different sides. By above definition, IW is the child of technology and its greatest weakness and capability. If one side is overly enabled, it can become overly dependent and overly vulnerable.

[Cebrowski] Information warfare is more technology enabled since it focuses on the vulnerabilities and opportunities presented by the increasing dependence on information and information systems. However, other aspects of information warfare exist in part, outside the domain of technology—psychological operations and elements of intelligence for example.

[Cochrane] Technology simply enables new forms of information warfare to evolve but with similar target end points. You used to have to print lots of leaflets and fly your Sopwith Camel over the enemy lines and throw them out at the population and hope some of them were read. Now you can swamp your enemy's TV transmitters and reach every household with the message. However, a well-placed bomb or missile could put pay to both of these threats, a bomb on the printing press or a missile attack on the TV transmitter.

[Cohen] Both.

[Dunnigan] Neither.

[Giessler] Both—just as was air warfare and industrial warfare and maneuver warfare and economic warfare and media warfare and…

[Gust] I think technology advances are driving this doctrinal issue. We are now asking what can we do with a technology rather than asking what we want in a technology to accomplish a task.

[Hazlett] Both, some information warfare weapons, such as viruses, trojan horses, etc., are products of technology and therefore technology dependent—and yet—their use is enabled by electronic technology. ISR (intelligence, surveillance and reconnaissance) systems are technologically dependent, but they also enable information attacks by divining and defining an adversary's information posture.

[King] Both. The technology enables systems to be built (very fast computers) but the use of them in information warfare is dependent on other technologies being in place (pervasive networks).

[Libicki] What's the difference?

[Loescher] Technology enabled, I think. There is a pattern in technological revolutions (e.g., oil, automobile, power industries) that begins with invention, moves through systemization and eventually changes the culture. That's what's happening to us now (probably stage 2). But if you choose to narrowly define the revolution in warfare brought about by the info age as "info warfare" then I have to say we're just doing it more

efficiently now than in the past. The issue is not IW, which is evolutionary; but war in the info age, which will be revolutionary.

[Merritt] Both. Many of the capabilties that can be used or exploited today and in the future are and will be dependent on technology. Who would have believed as recently as two years ago that we would have WWW [World-Wide Web] capabilties that could and will revolutionize how we do business. By the same token, it is going to require new technology that currently does not exist to enable us to execute IW both offensive and defensive.

[Probst] I have trouble parsing this question. Clearly, we can't have a Revolution in Military Affairs without unprecedented technology advances. Also clearly, more and more computers are becoming safety critical, or relevant to national security, or whatever.

[Schwartau] Of course it is. That's what makes it possible. For information in war, technology is the enabler, and for Pure IW, technology is the weapon and the target. See above.

[Steele] In the ideal, information war and peace is technology independent, that is to say, a very fine information strategy and information policy, as well as very fine information operations, can be developed and pursued without any enabling technology at all. Right now the offense (the mutts) have the advantage against the defense (the status quo Western powers) because the leverage they can derive from attacking complex technical infrastructures with physical tools (or electrical tools) is enormous. Right now offensive war by anonymous individuals is enabled. Defense is hampered by the complexity of the systems, and the lack of equivalent political and doctrinal arrangements.

[Moderator] What are the current key or enabling technologies of information warfare?

[Campen]
1. High bandwidth transmission.
2. Mass storage.
3. Data search technologies.
4. Simulations.

[Cochrane] Computers and telecommunications technology in all forms seen by "users" (TV, radio, fax, Internet), plus all of the infrastructures that go with them (fixed, mobile, satellite). Mobile computing and communications, including mobile and satellite systems, computing systems of all kinds, well known operating systems and glass, wire and radio networks. (Don't forget the soldier on a motorbike, he is still very useful).

[Cohen] Information technology—as a whole.

[Dunnigan] Hype.

[Giessler] All the wares. Within hardware we can't keep up with COTS [Commercial Off-The-Shelf]—but the chip and the satellite and the EMS [Electro-Mechanical Systems] and the fiberoptics are all intertwined—and we couldn't do anything without mundane things like electricity.

[Gust] Clearly, digital signal processors are the key enabling technologies in our info and info warfare business area. Their increasing capacity and reducing size makes them the choice for the brains in almost any system design.

[Hazlett] Offensive: jamming, global positioning systems, satellites, computers. Defensive: crypto, stealth, computers.

[King] Systems with very large computational and storage capabilities, worldwide high-speed networks, growth in mobile technologies.

[Levien] There is no doubt that the technological base of the Information Warfare revolution is the "Tyranny of the Chip!!" The fact that there has been an exponential growth in the speed and capacity of the semiconductor chip, along with a reciprocal exponential drop in the cost and the size of this same chip, has indeed opened the door to EVERYTHING else that drives information warfare. This is not to detract from the growth in the field of computer design and software skills, but these evaluations were only possible once the semiconductor nerds did their thing. All else derived from the seminal work of Shockley, Bretain and Bardeen at the Bell Telephone Laboratories back in the 50's with the discovery of the transistor.

[Libicki] Other than information systems in general?

[Loescher] The powerful ones haven't been invented yet—but Java is a start at a world of software robots.

[Probst] A partial list includes:
- high-performance computing and communications
- high-performance data assimilation and analysis for centralized intelligence fusion and correlation, and battlespace understanding
- control-theory technologies for automated strategic decision making at the strategic, operational, and tactical levels of war
- major advances in modelling and simulation

- *bandwidth negotiation in virtual networks*
- *information-survivability technologies*

[Schwartau] We can go on and on about bandwidth and MIPS [Million Instructions Per Second] and the evolving power of the networks and computers. But I am looking for more than standard old think for IW. I expect to see in the next 10 years:
- Greater mind-man interface
- True VR [Virtual Reality]
- nano-technology weapons (those are fun!)
- Breakthrough cryptanalysis: "There are no more secrets"
- Targetable remote bio weapons (in distinction to mass destruction bio weapons)
- Psychic warfare capabilities should reach the battlefield.

[Steele] Technical access plus hacker-like understanding.

[Todd] The microprocessor and the connectivity between those emerging technologies has defined the information age. The ability to process and distribute information results in great opportunities and challenges for warfare in the information age.[Loescher] The powerful ones haven't been invented yet—but Java is a start at a world of software robots.

[Moderator] Are there differences between "offensive" and "defensive" information warfare technologies?

[Campen] Depends. An offensive technology is constructed to exploit a known vulnerability in a defensive technology. Example: A virus and a firewall both use software technology. A defense against an electromagnetic attack might be a fuse, a shield or physical separation.

[Cebrowski] Information itself is the basis. Information technology is the broker, tool and application, in different ways. As such, technology serves to shape and present information. The control over how, how fast and how accurately information technology works on and with information is the essence of both offensive and defensive information warfare.

[Cochrane] The underlying technologies will be the same in both situations—it is just a matter of how they are used and where you sit as to whether they are offensive or defensive. E.g., if you write a software agent that goes around all the systems it can and gathers information then from your point of view it is a defence agent that spots enemies. To the person owning the system it is an offensive piece of technology. Offensive strategies are likely to require highly trained teams with specialised knowledge. Defensive technologies will include information monitoring and filtering together with computer and network resilience and healing techniques. Some have said offence is easier than defence but that may not be the case. A direct attack might be easy to mount but could be easier to trace back to the originator.

[Cohen] Yes. To be a good defender, you have to understand all about offense and find cost effective ways to provide adequate protection against the wide range of offensive potentials. To be a good offender, you have to find a hole and exploit it to your ends. The technologies for doing this are quite different.

[Dunnigan] Not really.

[Giessler] Many if not most overlap. Generally they are two sides of the info technologies coin. And you must consider both sides as you contemplate the coin. And you must consider the coin with two sides and a center as a system—that is fully connected.

[Gust] The Army labs here at Monmouth always give a sample of new info technology, i.e., a new radio, to the IEW [Intelligence and Electronic Warfare] Directorate to see if it has certain vulnerabilities or can be defeated easily.

[Hazlett] Yes, some systems, such as crypto are inherently better suited for defense; while others such as active electronic or acoustic jamming are offensive.

[King] Yes. Internet security gateways are defensive weapons. There are some systems that attempt to detect threats and then try to go on the offensive and track them down. Defense is harder as it has to cope with a great variety of different offensive systems.

[Levien] The difference between "offensive" and "defensive" IW technologies are to my mind almost all legal ones. There is of course the differences in perception that has been recently highlighted between the Army and the Air Force as how to wage the new IW warfare. The really tough question is how to ask a military officer to "defend his country against all its' enemies whomsoever…foreign or domestic" when you cannot clearly tell him who his enemy really is, and then threaten him with courts martial if he makes the wrong choice in the small instant of time he has available before he must act given the great body of legal garbage that awaits (much of it contradictory) for the Monday morning quarterbacks to quote from after the fact.

[Libicki] What differences exist are relatively minor (techniques of infoint collection are probably offensive in nature while CCD [Charge Coupled Devices] technologies tend to be defensive), and hard to distinguish.

[Loescher] Yes, technologically. However, operationally, the dual necessity of offensive and defensive actions is vital. In Navy, C4I is becoming more and more splintered, lacking advocacy, while IW, which in Navy is cryptology reinventing itself, is prevailing. That's a mistake. For the U.S., information is primarily a force subtractor at this stage because our dependency on it holds us tactically, if not strategically, banking on it. If you ask yourself what a small country can do to defend against an overwhelming military force, the options are clear. We need C4I more than we need offensive IW—though both are important. Unfortunately, in Navy, they are dividing. I see my job as helping to restore that balance. However, the technology of IW is tangible, while the promise of C4I is still in viewgraphs. That's a hard—but vital—sell.

[Merritt] You bet. Defensive will be alot harder, on all fronts. Alot of work remaining to be done. How do you do reconnaisance? What sensors do you need? How do you do IW Indications and Warning? How do you build countermeasures that don't become obsolete immediately?

[Probst] If we use these words they way I have defined them, then they are quite hard to separate. I would imagine that anyone skilled in one would be reasonably skilled in the other.

Sometimes it helps to solve a simpler problem first.

Computer-aided Postal Chess

White and Black both have chess computers that function as "brain multipliers". The chess computers have a chess rating, and can be set for different levels of play.

The leaders of the Revolution in Computer-Aided Postal Chess have ordered you to trade in your expert computer for a grandmaster computer.

Offense and defense change in subtle fashions:
- if I upgrade my chess computer, that does not ipso facto downgrade your computer, but it does give me an advantage
- if I break into your house and monkey with your chess computer so that it surreptitiously plays at less than full strength, that's a "Level-3 IW attack" :-)
- if I change the locks at my house, so that you won't be able to reply in kind, that's "defensive information warfare"
- if you cut off the supply of electricity to my house, you have attacked my infrastructure - and so on

[Schwartau] In order to defend, you have to know the offensive capabilities, so there is a great deal of similarity, although the techniques are different. I would have to write out a chart, but it would include thoughts like:
Sniffing Crypto
Sniffing Authentication
Viruses Smart O/S
Laser Interception Masking
PsyOps Truth Police
and so on. Good question with an infinity of possible answers.

[Steele] Offense is much much easier and can be physical as well as electronic. Defense is an order of magnitude more complex and expensive.

[Todd] Based on the comments to this question, there appeared to be a predominant notion that offensive and defensive technologies referred to hardware aspect only. While technologies are themselves "hardware," I think a point might have been lost. During the Korean War, the MIG-17 was superior in hardware (performance) to that of the earlier model F-86s. However, the American's retained a superior combat record of 10:1 over the adversaries. In this case, your superiority in training and combat tactics mitigated a technological inferiority. So it is in IW. Our risk analysis indicates that the better training and education of the user and systems administrators results in a far superior investment vs. results scenario that merely "engineering in" defensive solutions.

[Moderator] What can be considered an "information warfare system?"

[Campen] The assemblage of people, processes, equipment and software needed to wage conflict in the electromagnetic spectrum and protect itself against attack.

[Cebrowski] There is no "pure" information warfare system from a technical or weapons system standpoint. Weapons systems can perform information warfare functions, but as a byproduct of technical design. However, an information warfare system can be defined in terms of a series of interrelated processes that include technology. For example, an information warfare process may consist of established standards and scope for information protection, coupled with adequate attack detection and restoral tools and techniques.

[Cochrane] An information warfare system is any collection of resources that can be utilised in order to further your aims in a conflict by disseminating or disrupting information. E.g., lorry packed with a fertiliser bomb can be a useful information warfare system when driven into the country's central bank. The most critical element of ALL information warfare systems is the human brain. It will always find a new way of adapting an innocent system into something that can be used for a more devious purpose.

[Cohen] All systems are IW systems in some sense. It's their USE and not their CONTENT that dictates their involvement in IW.

[Dunnigan] General U. S. Grant standing next to a telegraph operator…

[Garigue] A group of knowledgeable individuals and a truly modern on line library.

[Giessler] Any set of elements related to one another with a goal of survival in the information age. Such a system has input, process, output and feedback. It is a complex-adaptive system that is teleological—goal oriented. So—a commander and his trusted agents (sometimes known as staff) who is trying to defeat, deter, influence the competitor is a I.W.S. So is a HARM [High-speed Anti-Radiation Missile] launched from any kind of vehicle. So is a kid with a virus attacking your info system with the objective of killing it. I.W. Systems are everywhere.

[Gust] An info warfare system is probably best defined by the financial programmatic weapons platform it rides on—JSTARS, Rivet Joint, Guardrail, etc. That would include comm links, ground stations and control nodes.

[Hazlett] Example of an information warfare system: an "active computer firewall/gateway" that detects attempted intrusions and attacks (and conducts counterattacks), yet still permits access by appropriately recognized systems. Example of an information warfare "system of systems:" An active ISR-RSTA [Intelligence, Surveillance, Reconnaissance-Reconnaissance Strike Targeting Architecture] combination that detects attacks on component systems and directs defenses and counterattacks.

[King] A collection of people and systems used to perform an offensive or defensive operation in an information war.

[Levien] Other than a speeding 30-06 bullet, or a hand grenade…about all remaining military systems fall into the IW system category.

[Libicki] An A-10 with a GAU-30 [Note: this is a 30 mm cannon] will work just fine if there is a command center or puter system underneath.

[Loescher] Let me answer it this way—the best system for IW is the operator's mind. The rest is trapping.

[Merritt] I addressed some of this earlier. Alot of possibilities. Many of which already exist, but haven't been deployed in a coordinated manner that would have impact on perception management on the battlefield. It is much more than a network issue.

[Probst] Above all things, an integrated battlespace management system that uses data-intensive predictive modelling and simulation.

[Schwartau] Me. You. A hacker. The bad guys. The system comprises the technology + motivation. Technology by itself is neutral; not bad or good. Remember, for example, that the only difference between a programming error and malicious software is intent. Or, that at a microwave repeater if properly tuned and aimed creates a fine DOS [Denial of Service] device.

[Steele] Any form of strategic thought, policy, or organization, which may or may not include technology, that seeks to achieve a specific information objective.

[Todd] An information system consists of a system of sensors (either organic or electro-mechanical/electromagnetic), the linkage to human decisionmaker or assessment center, the linkage between that decisionmaker (electromagnetic, mechanical, etc.) to a combat system, and the sensory feedback. I very much agree along the lines of links, nodes and human elements comprise a IW system.

TOPIC C: IMPLICATIONS OF COMMERCIAL DEPENDENCE

Dependence on commercial technology, products and standards is fast becoming a way of life for the military. Use of commercial technology is promoted at the highest levels and this is especially true for the information technologies which are at the heart of information warfare. This topic is concerned about the broader implications of such increased dependence on the commercial sector.

[Moderator] If everyone (including potential adversaries) has access to commercial information technologies useful in information warfare, then what will give the U.S. and allies an edge?

[Campen] It is not a question of access, it is a question of the timely and innovative exploitation of that technology.

[Cebrowski] The edge comes in the synergistic application of technology. For DoD, it's organizing all the IW elements as a system, then integrating it into the larger system of warfighting…in a way that enhances ops tempo. Technology is only an enabler. The real power comes from organization and employment concepts. If we don't tackle this area soon, we will lose the lead!

[Cochrane] Access to commercial Information Technology does not of itself define an edge in Information Warfare. Advantage in warfare is not just the possession of weaponry, it is its effective use and the knowledge of how to survive in order to use it again in a combat situation. This edge can be gained during the development, trailing and training in Information Warfare techniques. The scale of investment and technological inertia in the commercial sector will only slightly reduce the scale of the advantage that military strategists would like to attain.

[Cohen] The non-COTS [Commercial Off-The-Shelf] part—the way we connect things together—the way we use things—the skill and training and education of the people using them. We may, in fact, not have an edge.

[Dunnigan] Yes. We have more experience and resources in NetLand and, all things being equal, should prevail (Napoleon: "Victory goes to the bigger battalions." Unless they're Austrian, of course…)

[Garigue] The differential comes from the software. Let's not forget that it is the software that make the machine. There can be some substantial capability gains that come from the usage of COTS in Life Cycle Management areas such as costs, availability, acquisition, disposal etc.. but the real warfighting advantage will come from the "configuration" of these software machines and the resulting networks that are developed to support enlightened decision making. Multiplied by the net, one software program can be replicated in each machine and because of this flexibility thousands of more knowledgeable decisions can be made. The network can now distribute knowledge very rapidly. So it is the software (and the wetware) that confers new information warfare capabilities to the organization, COTS is simply the delivery method.

[Gust] Not everyone has access to all commercial info technologies. In addition, my PEO [Program Executive Officer] has recently had a requested FMS [Foreign Military Sales] sale of Night Vision goggles to an ally be disapproved by HQ, DA [Headquarters, Department of the Army]. There still has to be some area of exclusiveness for the U.S. forces to retain a technological edge.

[Hazlett] Innovative organizational concepts, accelerated and automated

decisionmaking, and more flexible and automated communications routing.

[King] The edge will belong to those who develop a strategic plan and are willing to make the investments necessary to always be ahead of the wave and not merely on it. The U.S. currently has an advantage in its knowledge and deployment of high-speed nets.

[Probst] Two short answers:

- articulate the new operational concepts so that we can have a Revolution in Military Affairs
- exploit the U.S. edge in superior doctrine, superior machines, superior algorithms, and deployed effective Defensive Warfare

[Schwartau] We have to do a couple of things:

1. Make sure that the military still has an edge up on technology that does not reach the commercial sector. This is true with the nature of the DEW [Directed Energy Weapons] (HERF [High Energy Radio Frequency] style weapons) that the military develops. They are vastly more powerful and useful than the homebrew commercial versions. We must take similar approaches with related "weapons."

2. We have to build an organization that is capable of C4I style deployment and engagement to either avoid conventional conflict, or replace conventional conflict.

[Steele] The U.S. and allies can only have an "edge" if they stop lying to themselves and admit that the existing communications and computing industries are "out of control" and ignorant if not criminally negligent with respect to C4I security. The "missing link" in IW is a secure home front, and this requires a national program—understood by and supported by the people—to embed decent security in all U.S.A. produced cyber-products. This will, incidentally, give a boost, to U.S.A.-based producers, whose security "quality" will serve as a major market differentiator. Included in this new commitment to security (and all it implies in terms of data integrity, etc.) will be the ability to detect and eradicate foreign-produced viruses and backdoors—for instance, the industry today is compounding its traditional failure to document software code with the outsourcing of much major code production to Calcutta and Moscow. We have no idea what these people are putting "between the lines" and we should be very concerned.

[Todd] Do not necessarily agree that all potential adversaries will have access to commercial information technology…certainly the possibility is there, but to what degree. Likewise, while other countries may "leap frog" us in more state of the art technologies (go from no telephone service to cellular phone service and bypassing telephone wires), the market place may dictate how and what is available. This disconnect between 2nd, 3rd, 4th generation telecommunication systems, networks, and processing capabilities will enable us to analyze the "seam" in their architecture and exploit them.

[Moderator] Given the possibilities for "chipping" and software "backdoors," how do we ensure the integrity of domestic commercial manufacturing and software processes? How do we ensure the integrity of foreign commercial components and systems which we might use?

[Campen] You don't even try. We must presume this threat and concentrate on the means of extremely rapid detection, fault isolation, and corrective actions.

[Cebrowski] Demonstrate to naysayers that the issues can be managed within reasonable cost. The key is to establish a systemic, national-level process that includes: scope and standards for what should be protected and to what extent (a risk management process); responsive indications and warning/attack analysis; and a broad range of flexible response options. This process will not demonstrate a nation that is invulnerable, but rather one which is constantly vigilant, decisive and prepared to respond to any threat, foreign or domestic, with a full range of national security tools.

[Cochrane] Chipping and "backdoors" are as much a problem to commercial entities as they are to the military. An attack on a large banking institution may cause as much damage to a nation as an attack on a military installation. Existing examination of systems based on guides such as the Orange Book are of limited use. Experience has shown that these processes are difficult to "sell" to software developers. To complement this we need to develop penetrative testing in ways that simulate real attacks and study how systems will react.

[Cohen] With rare exceptions, we don't, and that's an important issue today.

[Dunnigan] You can never let up your guard on such things. Put it out of sight and you can expect the bad guys to come in through your back door.

[Garigue] There will never be any guarantee that software will be proven correct and have no "defects" because of the enormous difficulty of checking large complex programs. Networks are even more problematic. The analysis can only be limited to small portions of programs or objects. And even when programs can be proven correct, there still would exist the possibility for perfectly correct code becoming malicious (Jekyll and Hyde programs). Partitioning mission critical processes from other processes, and ensuring that some functions be performed via an agency of differently coded processes does enables a certain measure of redundancy, cross checking of results, and graceful degradation of performance.

[Gust] This is an area where integrity of use requires adherence to patent and license concerns. We should pay for software intellectual rights if we use it in our systems.

[Hazlett] Developing and instituting a "red team" concept for testing and evaluating software. Developing an "overlay" for domestic and foreign software and components, that detects and reports intrusions and alterations.

[King] There are processes and methods that can be put in place but there will always be the question of the cost of achieving a given level of assurance and the impossibility of that level being 100%. Thus, systems must detect and contain suspicious subsystems (not an easy problem).

[Probst]
- legal requirements for due diligence with severe financial penalties
- never trusting software you haven't (re)written yourself
- spreading the "public health" approach to component integrity
- eternal vigilance following adequate training (e.g., personal monitoring of personal

audit trails—cf. Shimomura)
- less practical: never trusting hardware you haven't designed yourself (testing and certification may be of some help here)

[Schwartau] Someone read my book! Thanks. That's the problem. We will have to develop new methods of process engineering, assurance mechanisms and automated reliance tools. Similarly, we will have to develop additional non-destructive testing methods for completed products as an inspection or QA [Quality Assurance] procedure.

[Steele] The Department of Commerce is simply not up to the challenges of the 21st Century (neither is much of the rest of the USG [U.S. Government], but at least DoD knows there is a 21st Century). The first step must be legislation which requires "due diligence" on the part of all manufacturers and vendors of communications and computational hardware, software, and related services. They must be required to assure their customers that it is safe to work and play in cyberspace, and must be held accountable, using new and solid international standards, to the highest levels of embedded security. The U.S. position on key escrow is ignorant and flies in the face of both history and cyber-power. Until we give up the idea of legislating back doors for law enforcement, we will not be able to provide common security to the whole.

The FBI should be given funding ($500 million a year) for a new Electronic Security & Counterintelligence Division, and the Secret Service should be relieved of its dubious claims to the mission of handling crimes in cyberspace. National testing & certification laboratories should be established using existing capabilities (for instance, one of the Department of Energy laboratories), and all foreign hardware and software should be subjected to both preliminary and ongoing (random) testing. All hardware and software being introduced to government installations should be individually tested. Corporations should have liability incentives for doing the same thing. Ultimately we should eliminate portable disks and require that all data and software be sent from one infosec gate to another for scanning and air gap transfer under control.

[Todd] The ability to protect our systems needs to be the first priority in this emerging warfare area. Our first goal is to raise the our integrity of our systems to such a level that the "casual" hacker cannot get primary access to our network system. This can be done with an integrated approach of engineering fixes, highly trained system administrators, and highly aware users. This will have to be a continuing effort. But we will still need to understand that the top 5 percentile of professional hackers will still be able to penetrate our system. Now we need a system of both highly trained people and equipment that can identify such activity, bound its effect, recover systems that are damaged or corrupted, and work back to the origin of the attack for either criminal prosecution or counterintelligence activities.

[Moderator] Given the decreasing financial leverage of the military in the commercial marketplace, how should the military positively engage firms to take military needs into account during the commercial product development process?

[Campen] First you take into account the remarkable similarities in "needs" between the private and military sector and identify short falls. The military then applies its talents and funds on those relatively few shortfalls.

[Cebrowski] This is achieved by answering and addressing two questions: What must be protected? Certainly not "everything." This is the policy issue on the scope of protection. What type and level of protection is appropriate, under a managed risk approach? This is the technical question of "standards." Those commercial organizations wishing to "do business" with the protected enclave must interoperate on its terms. Over time, the standards become universal—not by mandate, but by market forces.

[Cochrane] By locking companies into the development cycle as the military outsources everything. The military is still doing studies, still funding universities, still doing original stuff. Forming a partnership with companies on joint programmes where there is a synergy between the applications. What is the difference between secure banking, secure networking for industry, and the military—only degree!

[Cohen] Money.

[Dunnigan] Pay them money. That always works. Beyond that, the troops have little influence.

[Garigue] I believe that that is not required. The present capability of components and systems by far exceeds the present majority of our needs. The notions that competitive advantages will come from faster, smaller, more secure, robust, and functional information systems are already accepted goals and are driving every commercial innovation process. We need not emphasize these expectancies. However, we do need a more focused effort on the problem of how to use these capabilities to impose order or defuse conflict.

[Gust] We use a dialog process in the Army which includes Advance Planning Briefings to industry and discussions via an electronic bulletin board for draft RFPs [Request for Proposals]. We also speak to symposiums and industry forums. Finally, pre-solicitation conferences advertise the near-term release of the RFP to the interested bidders who responded to our CBD [Commerce Business Daily] announcement.

[Hazlett] Revise acquisition procedures so that government specs do not needlessly burden process. Revise "lowest bidder" rules so that government can purchase "best value."

[King] The military needs to be very clear and realistic about how its needs differ from commercial needs. There will continue to be companies that make mil spec versions of commercial products for those few cases where they are really needed.

[Probst] Build military applications on top of COTS hardware and software. If you really need something different, talk to them.

[Schwartau] Declassify the threat to the commercial sector. Put us all on the same team.

[Steele] Declassify the threat. Not only will the private sector not heal itself until it fully appreciates the problem (and stockholders know enough to hold management liable for being stupid about electronic security), but the military will never heal itself as long as

C4I "deficiencies" are classified—the latter guarantees that only the people that created the problems in the first place will have the clearances to jerk around with possible solutions, oblivious as they are to the explosion of innovation in the private sector, far from all SCIFs [Sensitive Compartmented Information Facilities].

[Moderator] Many commercial firms (for example, banking firms) share the same "information protection" concerns as the government. What can the military learn from how these companies conduct information warfare functions? How should we share this information?

[Cebrowski] This first step is to raise awareness of senior level management and encourage dialog in interagency fora. An understanding of the inherent vulnerabilities of information-based technologies will spawn focused efforts on security processes, procedures, and policy. If we can learn anything from the commercial sector, it's the extremely low tolerance for ignoring security policy. Before this can be done at the scale and levels required, government must put in place the policies and legal protections necessary to secure interests and equities.

[Cochrane] Such commercial enterprises have communications and systems that are often held by, or accessible by, "the enemy" and are open to attack on more than one front. Commerce probably has simulated and experienced a greater number of attack scenarios and now can respond to an attack faster than the military. Information technology is the life blood of a modern nation, if it is cut off then society crashes and stops. Sharing is only a problem for the military; they will just have to get used to the idea!

[Cohen] These firms do a poor job of it in military terms, but the military could, at a minimum, adopt the same minimum standards these firms use in addition to current DoD standards.

[Dunnigan] You mean, "how do you get them to share information with you." The banks are in real info-war mode at all times. These are the folks with the "combat experience" regarding what works and what does not. In the peace time, the military is playing games while the banks are battling the hordes of cybernasties.

[Garigue] Open societies as well as open systems are more robust because the spread of critical information and knowledge on security helps everyone. Continuing an open dialogue at all levels between the concerned groups such as between the banking, power, telecom, and military communities as well as with the security advocate groups within Internet will ensure that the weakest network functions will be identified and brought into line with acceptable security procedures. What benefits one community, benefits the net and benefits all communities.

[Gust] There is a formed chartered organization in the Army, supervised by the HQ, DA DISC4 [Director of Information Systems and C4] office responsible for the "C2 Protect" mission. I am not totally current on the details of their involvement with commercial businesses, but know that a process is in place.

[Hazlett] Government should fund a portion of the research so that it can benefit from the discoveries and be part owner in the product. Share in licensing the procedures and products.

[King] There is a lot to be learned but it will be a difficult process. There are signs such as the "Invitational Workshop on Computer Vulnerability Data Sharing" scheduled for June in Gaithersburg that this is recognized as a common problem that must be solved.

[Probst]

- Banks worry about information security and banking-systems security. Certainly one should talk to their security officers. I really doubt that banks crack other banks, so you won't find much help here.

- The ISAT [Information Science and Technology] Summer Study on Defensive Warfare and Information Survivability had a balanced mix of academic, commercial, and government representation.

- As the market develops, people will buy the security products they need (the government's role is primarily to watch over the infrastructure).

[Schwartau] The key lesson is that much of the commercial sector can move on a dime; unlike slowing down a carrier in 20 miles.

- *Rapid Decision making*
- *Iterative process changes*
- *Adaption to market conditions*
- *Policy must change as rapidly as do one's adversaries*

[Steele] Most commercial firms do not understand electronic vulnerabilities, in part because most of their security and "infosec" officers don't really understand the insides of their systems, and in part because corporate management will continue to shoot the messenger until such time as they cross a major pain threshold, i.e., are held accountable or "see" the losses they are incurring. The real hard problem with electronic theft, as Toffler and others have noted, is that electronic property can be in two places at once—when proprietary information is stolen, the files are still "there," they have simply been duplicated.

Banking has nothing to teach us, despite the inflated claims of some self-serving commentators. The real experts (e.g., Eric Hughes of Cypherpunks) know how easy it is to penetrate both banks and trading houses, not only electronically but also through direct access to uncontrolled terminals on the trading floor. More simple denial of service attacks, and physical interruption of services, have long been described by Winn Schwartau. The single greatest danger to much of the U.S.A. is the chaos and anarchy as well as the financial loss that will be incurred because of the lack of hard-copy backup documentation for electronic wealth and property ownership. It will take years to sort it all out, and will probably require some emergency legislation freezing all claims.

TOPIC D: FUTURE TECHNOLOGIES AND DIRECTIONS FOR RESEARCH

Advances in technology have given us greater and greater information warfare capabilities. However, we are now reaping the research and development seeds sowed years ago. What should we do now to promote continued technological progress and greater information warfare potential in the future?

[Cebrowski] We must remain tethered to those R&D labs and think tanks conducting leading edge research with an eye at spotting potential trends that may support future C4I/IW architectures. The DoD should not fund in-house efforts which are in effect competing with industry; rather, efforts should only address uniquely military needs.

[Cohen] Plant more seeds. The way we sponsor research today is poor in terms of long-term rewards, and we will pay the price for our lack of vision.

Specifically:
- we put up too much money per research grant - we should sponsor many more lower dollar value pure research projects - say $100K/year maximum
- we fund many projects that are foolish - we should have better peer review that identifies foolish (impossible) research as opposed to risky (unlikely) research and not fund the latter - but fund the former.
- we don't fund projects with less than a 90% chance of success - the system is designed to put too many rewards on successful completion and delivery of results - real research - especially far reaching research - is more risky than this. Conservatism is leading to mundane results.

[Garigue] Only education can continue to spur the innovation process. Continued support for higher education, funding for unique programs of studies, supporting higher education through part time studies etc. all these initiatives will help engender the new solutions. Furthermore, cross disciplinary programs, as well as mentorship program within industry and other governmental agencies will help. IW is not solely a military problem. Let's cycle a few of our information warriors through banking information system positions as if they were military exchange positions.

[Gust] This is the R&D versus Production decision that our leaders in the Pentagon have to deal with on a daily basis. There has to be a balance because future R&D is needed, yet "freeze and field" the available technology must be done to modernize weapon systems. Probably what we need are more efforts aimed at P3I of existing weapons platforms and fewer attempts to have new start weapons programs.

[Hazlett] Government should pick up a portion of the R&D tab, maybe even acting as a coordinating agency, matching pooled funds with problems and providers.

[Probst] The U.S. technology system will produce many of the products the DoD needs. The government will have to do some things. Computing professionals and the American public must understand the truth of Jim Clark's statement: "Getting the government involved in maintaining Internet data privacy ... [is] going to be necessary". Since I see Defensive Information Warfare as the genuine long-term need, I would say:

- sponsor high-quality cryptography and information-security conferences
- coordinate the gradual replacement of the current Internet by something more secure
- increase the funding priority of research in High-Confidence Systems

Basically, map those areas where market forces themselves are unlikely to encourage the development of necessary security tools, standards, policies, etc., etc., and invest in the

margins. I speculate that progress in Defensive Information Warfare will give the U.S. as much as it needs in Offensive Information Warfare. If I may make a statement, it has some similarities with understanding chemical and bacteriological warfare: we want to know how it works, but we might have either moral scruples or other reasons for not doing all the dirty tricks that are feasible.

Now, how do we get an Integrated Battlespace Management System? Either a defense contractor puts the pieces together, and prototypes, or Pentagon brass put the pieces together, and call for a prototype.

[Moderator] What are the future enabling technologies of information warfare?

[Campen] Again, it's not so much technology as it is the human-machine interfaces that allow us to exploit technology.

[Cochrane] Increased computer processor capability enabling rapid development of artificial intelligence and chameleon or polymorphic software which will hide its true identity and purpose.

[Cohen] Information technologies? This emphasis on technology is the wrong way to build the long-range future. The emphasis should be on understanding. De-emphasize systems, concentrate on concepts.

[Dunnigan] Common sense and respect (and detailed knowledge of) for what has gone before.

[Garigue] Easy high-level, end user programming capabilities will become essential as they permit rapid development of new information warfare and decision support programs. Being able to build a program will help users respond rapidly to new and emerging information needs. Visual programming, distributed software objects, scripting languages, and modular software will enable the user to rapidly enhance his information environment with new programs. So whatever new process is required it can be built by the end user himself. This will also shorten the time between requirements, specification, and development.

Also, as we will be faced with much more information than before, we will need to develop new types of knowledge management tools to monitor, collect, assess, filter, and aggregate data into information. Faster and more sophisticated clustering and classification techniques are required. Natural language interpretation and understanding based on cognitive modalities will help the query processes and enable a more useful dialogue between the human and the computer.

As information becomes more complex, there will be a requirement for high end visualization. Visualization permits greater transfer bandwidth between the human and the computer. Simulation will be integrated and continually used in all training and planning processes. Virtual Reality will also permit visualization as well as enable full sensory interaction with all types of data and information. VR will also play a significant role in support of individual and group decision support environments.

[Gust] Clearly, the expansion into frequency ranges using gigahertz as the unit of measure is the future. The existing and limited size of lower HF, VHF, UHF bands demands this extension. The technologies that will make the use of higher frequencies possible, like the millimeter wave solid state devices of today, need to be exploited.

[Hazlett] Offensive: jamming, global positioning systems, satellites, computers. Defensive: crypto, stealth, computers.

[King] Semiconductors (processors), optics (communications), cryptology, machine learning algorithms, data mining techniques, visualization, simulation of very large complex systems.

[Probst]
- programmable petaflops computers
- high-performance virtual networks
- high-confidence systems
- software infrastructure for high-performance data assimilation and analysis

- optical stores and interconnect
- directed-energy weapons
- ubiquitous information security including strong cryptography
- advanced modelling and simulation technologies
- unconventional man-machine interfaces (e.g., personal interfaces)
- also, the six Strategic Focus Areas of the CIC [Committee on Information and Communication] for HPCC [High Performance Computing and Communications]

[Schwartau] Uh uh! That comes out in IW2. I must be circumspect here. :-) [Note: IW2 is Mr. Schwartau's forthcoming book].

[Steele] Education of the individual from birth and continuing through their entire life.

[Moderator] Given the military's limited research and development funding, what specific research should it conduct? What specific technologies and methodologies should it support?

[Campen] Same as above. Study how to exploit the commercial technology to dominate your opponent.

[Cebrowski] We should be willing to apply a small percentage of overall R&D funding for pure research...divorced from a procurement tail. There are tremendous benefits of developing intellectual property that allows us a glimpse of future capabilities and trends without overstressing the current PPBS [Planning, Programming and Budgeting] system. (See response above)

[Cochrane] Secure distributed computing platforms, resilient public network infrastructures, automated software creation processes based upon a formally defined object structures, studies of complex systems including self organisation and auto healing techniques.

[Cohen] The question as put reflects on the thinking of the person asking the questions and in my view on the organization as a whole.

"what specific research should it conduct?"
"What specific technologies and methodologies should it support?"

Specific research seems to reflect research directed toward a specific (usually operational) need. In my opinion, we need non-specific research into information warfare. Understanding specific technologies and methodologies might be a useful result that could be derived from the research we should be doing. I think a good start would be to fund research into what long-term research results we will need to be effective in IW over the next 20 years. I would be very happy to do this research, but so far, the only things I have seen accepted by the DoD as research projects are the development of systems to meet specific operational needs. In other words, military R&D is in a purely reactive and development mode—reacting to current needs and weaknesses by developing new systems—rather than a proactive mode—trying to understand what future needs may be and trying to understand what we don't yet understand.

[Dunnigan] People, in and out of uniform, who can do what has to be done. It's cheaper to cultivate the right people than to try and keep up with the commercial sector in spending. The money will not be there.

[Garigue] Security is paramount, so work on trusted-objects and trusted-processes is very critical to information warfare. Also new ways of clustering computers together to augment computational power and availability is important because one can then use low end technology to create high end computational networks that are survivable and flexible.

[Gust] This question needs to be asked of a combined arms team of users, researchers and materiel developers. One part of the community cannot answer this question alone.

[Hazlett] Realize that there are other parties with the same interests and start working with them, rather than trying to "go it alone." Where possible, team with other organizations, such as academia, and businesses. Where it is not possible, due to unique requirement(s), team with consistent allies, with like needs, such as Britain, Canada, and Australia. If it exists elsewhere, don't be afraid to buy it, or outbid others (it may be cheaper, in the long run).

[King] The emphasis should be on software and systems and not hardware. There are many research problems to be solved in the area of the effective, secure management of very large networks and systems.

[Probst] Two things:

- insist on programmable high-speed computers
- insist on virtual networks connecting distributed objects with bandwidth negotiation

[Schwartau]

- Insular technologies for mission critical commercial infrastructures
- Improved quality assurance
- Post-Information Warfare technologies

I have no doubt there's more, but I have a hell of a cold. :-)

[Steele] The military today in the U.S.A. is something like the military in the Third World (Luttwak's point) in that it is one of the last true national cadres of trained, disciplined, loyal people. If the military would stop lying to itself and others at the Service and ASD [Assistant Secretary of Defense] level, and share what it has learned about our vulnerabilities and gaps with the private sector, much of what we need would be developed at no cost to the government. Unfortunately, the areas where the military most needs development that will not be funded by the private sector is in the area of support to small Special Operations teams, and to the tactical commander dealing with the 10 klick problem, and these are not massive sexy programs. The military should focus on "niche" R&D.

[Moderator] How should the military conduct technology investment programs with traditionally non-defense companies (like Sun, Microsoft, Motorola, etc.) who are now key suppliers of information technology?

[Campen] Probably not a cost-effective investment. Military has no leverage. Instead, take what they produce and learn how to run faster with it than the competition.

[Cochrane] See previous replies noting that robustness is also a high priority commercial issue. The development of an active aggression capability may well require traditional military funding.

[Cohen] The military should not be investing in those well-established commercially successful firms. Those firms can support themselves. The military should be putting out specifications for its long-range purchasing requirements to help guide the large firms that want to sell to the military so that they can make their long-term investments into the technologies the military will buy. The investment should be made in small high-tech firms and small high-risk high-payoff projects.

[Dunnigan] Don't act like know-it-alls. The non-military people have more experience at this sort of thing. Don't be lulled by stories of commercial firms that are clueless. There are always lots of those. Concentrate on the commercial outfits that have the goodies.

[Garigue] As we evolve our traditional command and control information systems towards coordination, communication, and cooperation of information systems, we will be relying more and more on commercial key suppliers to deliver all the building blocks the military will use in support of defense and national security objectives. I believe that most of our present military information systems problems have already available solutions. For example, the recent "24 hour in Cyberspace" mission control (at www.sun.com—how did they do it?), has a lot of the same characteristics of an advanced Information Warfare command center. It had a DMZ [De-Militarized Zone], Clean LAN [Local Area Network], collection, analysis, and production centers, mirrored repository sites, and CERT [Computer Emergency Response Team] groups. The military will have to divest itself from not "invented here" syndrome so it can recognize ready made solutions. Future technology investments might not increase the information differential so much as an "Information Warfare Personnel" investment program.

[Gust] Key companies like Sun and Motorola have large divisions devoted to the government sector. They are coming to us.

[Hazlett] As if they were in it as a business—getting the most bang for the buck. Provide incentive or seed funding to lead R&D efforts in directions of government interest.

[King] I do not think there is any one answer here. One way is to cooperate with them in the funding of research at universities and research centers. It would be very useful to have more exchange of people between the military and these companies on rotational assignments but this is easier to talk about than to do.

[Probst] Be sensitive to investments in the margin. Look for future military-critical technologies in small companies.

[Schwartau] The model is the same as it is today. The Chinese Wall works. Look at the way that academia is handled. I don't see any conundrum here.

[Steele] In the IW arena, "non-defense" is an oxymoron. The military has one unique advantage in this era—its legitimate pre-occupation with security and survivability has made it sensitive to vulnerabilities and needs that are now essential for home defense and

economic prosperity in the private sector. The military needs to teach rather than invest.

TOPIC E: CHANGES IN THE ACQUISITION PROCESS

Obviously, information warfare technology must be developed, acquired, fielded and sustained before it can be used. This topic seeks to explore whether the defining characteristics of information warfare imply the need for changes in how we acquire such systems.

[Moderator] Given that new generations of commercial information technology come, by some accounts, every 18 months, how do we address the need for a quick acquisition cycle time?

[Campen] We begin by abandoning the term "cycle," or at least redefine it as an open-ended, never-ending series of cycles. Also, we rid ourselves of the obsolescent concept that we are "buying a system." It has been almost 20 years since an AFCEA [Armed Forces Communications and Electronics Association]-run study coined the phrase "evolutionary acquisition" in an effort to make the point that there is never a Final Operational Capability, only a series of buy a little, test a little increments. The DoD Authorization Act of 1996 (HR 1530) makes some useful changes by focusing oversight on the function of an organization and the outputs to be gained from new information technology, and by urging "modular, incremental" procurements of "information technology." But that is not nearly enough for the U.S. to avoid being technically leap-frogged by adversaries that are not crippled by machine-age procurement regulations and cultures, nor burdened with an enormous investment in obsolete legacy systems. I think Navy Commander Loescher is the one to credit with the notion that we no longer procure information systems; instead, we acquire information services. (My words, his idea). We need to visualize the continuous enhancement of information systems in much the same way that we do software upgrades. We know there is always a software revision on the horizon and we program funds accordingly. The Block approach to aircraft upgrades is a step in this direction, but it can't be done if each increment must be refought with the Congress annually. We don't approach Congress with a line item to purchase electricity or water and we ought not need one to purchase INFORMATION SERVICES.

[Cebrowski] Spirited debate surrounding DoD Acquisition reform is not new. However, the strategic environment has changed so significantly since the inception of the current acquisition system that modernization is clearly warranted. A revitalized acquisition system that can keep pace with market forces is the surest way to maintain the most modern weapons systems. The focus should be on capabilities, not systems. The strategy should be one of continuous incremental technology insertion.

[Cochrane] The characteristics of information warfare dictate that a new software or network tool can provide battlefield advantage within hours of its conception. Therefore the research, development and supply chains will require re-engineering to suit. Commercial information technology may go through a generation in less than two years but changes in the fundamental platform and network architectures are much slower. Possession of the very latest technology will be critical to front-line Information Warfare units. More conventional units with less pressing needs could easily be supplied by normal commercial processes. Above all the growth in computing ability has to be allowed for when designing systems and then factoring extra security on top to be safe.

[Cohen] New IT doesn't often mean new underlying uses or techniques—they come far more slowly. Furthermore, for the first 6 months or so, any environment is unstable. The strategy should be to seek out more stable environments for conditions where long-term results are desired—hence you go for Unix and MVS and VMS and other stable environments as opposed to DOS and WINDOWS, etc [Note: these are all different types of computer operating systems]. Furthermore, re-acquiring technology every 18 months

is not cost effective. Seek out technology that will last for 5-8 years and build on the more stable base. Abandon the reckless approach in favor of the more solid one. The exception is in experimental environments, where the state-of-the-art should be tracked, and in special cases where a really new capability enables advantages that are so significant that they warrant the extremely increased likelihood of failure associated with new technology.

[Dunnigan] Go commercial or die. Your likely future opponents will not have a military-industrial complex and will automatically go commercial and have the latest stuff.

[Garigue] Our present notion of information system delivery is outdated. We do not deliver systems anymore, we "grow" them. The present maturity of IT permits an organization to adopt a "technology insertion" strategy rather than a system development strategy. As new generation of network components are made available we can insert them readily into existing networks and IT infrastructures. We introduce these components in a prototyping context.

The focal point however is not just on managing the technology but on managing the functionality. As functions have a longer cycle than technology we must ensure that we outline a migration of the stable functions embedded in older technology to the new ones. We must also ensure that such a migration path will ensure the minimal amount of disruption of service over the course of the transition. This way, over time, older technology elements of a network are replaced by newer ones and functions migrate from older hosts to newer ones.

[Giessler] Adopt USN [U.S. Navy] initiative and SECDEF [Secretary of Defense] dictate that COTS is standard unless otherwise strongly justified.

[Gust] We have now begun in the PEO [Program Executive Officer] world an earnest reduction in cycle time. RFPs [Requests for Proposal] are shorter, with fewer CDRLs [Contract Data Requirements List], minimal MILSTDs [Military Standards] for such items as comm waveforms, interoperability, etc. Contract negotiations are now including an oral discussion cycle instead of lengthy IFBs [Invitation for Bid] exchanges of written questions and answers, etc. But still if the new technology cycle is 18 months, we have to do more. One initiative is the POM [Program Objective Memorandum] wedge for unidentified new initiatives. Our Army Chief is asking the Congress for $450M in a wedge to buy the mature, value-added successes from the digitization demo. Another is for the Army TRADOC [Training and Doctrine Command] community to emphasize a reduction in their requirements determination cycle. There are still areas where we can reduce time.

[Hazlett] Lean toward software, vice hardware solutions, ensuring that hardware is easily upgradeable, taking advantage of more powerful chips and faster memory. Go to more modular systems.

[King] First, it is not necessary to always keep up with every new wave of products which is more alike every six months. Second, long term contracts should be developed with vendors who can provide upgrades and new systems over the life of the contract in an efficient manner.

[Loescher] There is a logic set here that we are missing consistently. The InfoTech industry, at this moment, appears to be growing much like the oil industry, automobile industry, power industry, and other markets initiated by broad change in technology. A global infrastructure is being built as the market for goods increases. We are still in the stage where the industry is dominated by engineers, who are attempting to sell specific products. It is analogous to trying to sell spark plugs instead of cars. Gradually, however,

the market is becoming one of commodity and service—America Online, Netscape, Java, are all examples of the coming service market. In the future, I would bet acquisition time will become irrelevant—because we're not going to "acquire" it, we're going to buy information services and information itself as a commodity. Acquisition won't matter—C4I is dead; we'll be transitioning to the direct use of information itself, not building information systems, which will all be commercial—and perhaps common to the foe and the friend.

[Probst] Use ATDs [Advanced Technology Demonstrations].

[Schwartau] In basic COTS PCs this is true, but integration of complex systems requires greater development and testing time. The key here is platform and O/S [Operating Systems] standards, backward compatibility and an acquisition awareness that what is RFI'd [Request for Information] today is obsolete by the time the buy occurs. I would examine acquisitions which permit the upgrade of systems performance to current standards as of the date of purchase.

[Steele] Functional standards (as opposed to fixed standards), and true openness and inter-operability, are critical. HOWEVER, also critical are the identification and legislation of standards of security and other basic forms of functionality which must be embedded in all civil communications and computing capabilities in as much as 95% of DoD traffic goes over same. It is NOT possible to BUY what we need. It is only possible to LEASE, TEMPORARILY, civil capabilities in this area. The real progress will come not from firewalling internal unilateral systems, but from raising the generic security and capability of the ENTIRE global network.

[Todd] In the past, the U.S. military has done a dismal job of integrating information systems. That, however, has been a blessing in disguises in that our "system of systems" have not been susceptible to contamination (either malicious or accidental). But future systems should be easier to integrate and as such, we need to ensure these systems while acting independent are yet able to communicate among them (linked). Fully integrated systems may be like a house of cards and if attacked, not degrade gracefully.

[Moderator] Should there be a shift from hardware to software orientation in development? Should we lease hardware and concentrate our efforts on incrementally improving software?

[Campen] The functionality comes from the software; the hardware will provide the bits and the bandwidth accordingly and automatically. The emphasis should be on the leasing, acquisition or rental of information services, with each new increment improving functionality, speed, accuracy, security and reliability.

[Cebrowski] Warfighting requirements will always dictate development decisions while economies prevail in decisions to lease or own. Advancing technology itself has hardware and software on a natural collision course—neither will dominate, instead both will fuse into mutual dependence. The more important question is how to shift funding and management attention to the requirement and design phases rather than waiting for problems to become big and intractable.

[Cochrane] The split between hardware and software is somewhat arbitrary: you cannot divorce them in this way. (Why should you trust hardware more than software? There could be just as many problems in the silicon—storing away keys which are picked up by a "maintenance" visit for example) We must always consider the whole system, stop looking at elements in isolation, concentrating on reducing the time taken to develop integrated hardware and software solutions.

[Cohen] Leasing hardware is an extraordinarily poor investment. It's almost always better to buy the hardware and convert older systems for less than state-of-the-art uses. For example, even a 5-year old PC is still perfectly capable of being used for office automation functions.

[Dunnigan] This has already been going on.

[Garigue] We should buy hardware like we buy food. So that it can be consumed rapidly (if you don't it goes bad very quickly). Software on the other hand are the functions that are required whatever the hardware. Software is the essence of the system as it represents the processes required to support the decision maker. Computers are consumable. Most of the critical components of the network are already in the commercial sector anyway; what makes systems "military" are the fact that the tools and the technology are applied to military problems.

Software itself is being modularized and becoming more and more generic. So there is an opportunity to take advantage of this and tailor some systems to our needs. The point in all this is to know when our requirements for timeliness, pertinence, accuracy of the data cannot be meet by the existing components and to custom design our own solutions.

[Giessler] We should not be developing either hardware or software in the military or the national security establishment unless the commercial market is not meeting our needs because there is insufficient profitable demand. Even our interoperability needs should be met by commercial interface packages.

[Gust] We in the Army night vision business have a unique incident that we are working. During Desert Storm we bought an overstock of Generation I tubes that are now obsolete. Since we have moved on to Generation II FLIR [Forward Looking Infrared] technology, can we salvage any of this "sunk cost"? The answer is we may have found a way to sell back to the contractor the older versions for their direct sale to other customers, then receive credit on the contract to buy new Generation II devices. Lease of hardware is probably a better option for a weapons platform of less dubious value, like a truck. Every system the Army is buying now is specifying the Common Operating

Environment and Army Architecture standard version 4.0. This is a flexible format conducive to the use of software upgrades as a process for insertion of increased capability.

[Hazlett] Yes, we should shift to software solutions where possible, leasing and outsourcing hardware where possible. May need to develop "wrappers" or metaphors to deal with unruly or yet-to-be-developed components.

[King] Yes, in most cases, the emphasis should be on software but changes in hardware technologies need to be monitored.

[Loescher] We should concentrate on identifying and catagorizing information families and let the commercial world worry about hardware and software. If the future, the intelligence communities will become less and less useful, though that may be their best kept secret yet. The best intelligence, especially for Information Warfare, is going to come from industry sources—much like it did in the early days of World War II. I'm not going to want to know what DIA thinks about Guatemala, I'm going to want to know what the Guatemalen information infrastructure is—that's not going to come from DIA, or NSA, or CIA, that'll come from the commercial sector that does business in Guatemala.

[Probst] The situation is more complex than that. In large part, DoD needs to use third-party parallel hardware and software. DoD also needs to articulate the parallel hardware and software at the margin that will not be available elsewhere. Certainly the bulk of DoD time will be spent in writing defense applications, taking advantage of reuse wherever possible.

[Schwartau] Software must be improved in two ways:
- Quality of testing and reliability through the use of better automated development tools.
- Standards for platform migration will alleviate the constant need for total redesign every time a new hardware widget comes along.

[Steele] Not hardware, not software, NOT EVEN DATA COLLECTION. Our focus should not be on technology, except in-so-far as we mandate certain standards of performance, but rather on "intelligence," meaning; what information can be discovered, discriminated, distilled, and disseminated to the commander so as to enhance mission fulfillment? Taking SPOT Imagery as an example: it is not necessary to mandate anything other than the fact that we need 1:50,000 with contour lines and precision points (either GPS [Global Positioning System] or NRO [National Reconnaissance Office]…).

[Moderator] With an increasing array of new commercial information technologies, who should be responsible for finding these new capabilities and how should we conduct commercial-military integration?

[Campen] The user, not some surrogate electronic arsenal attempting to craft a formal ROC [Required Operational Capability]. The Air Force Fort Franklin shows the way by providing an environment for experimentation, testing and functional demonstration.

[Cebrowski] The technologist must inform his potential customer, the operator—and operator must inform technologists. We shouldn't be concerned about commercial-military integration. The DoD should buy the 70-80 percent solution from industry; then reengineer business practices and requirements to make that a 100 percent solution. We can't afford otherwise.

[Cochrane] Integration is the wrong approach. Ordinary commercial organisations are becoming more aware of the need to have secure systems and therefore demanding the same strength as military products. If the military were to specify their needs at an early stage the commercial systems would be developed to the military requirements. This would produce economies of scale, reducing the costs of military systems. The military would no longer have to identify the capabilities of systems they were getting because they specified the capabilities.

[Cohen] You might try having an advanced technology group in the DoD that constantly seeks out new and useful technologies and applications and forwards information on these new developments to the appropriate other groups for consideration.

[Dunnigan] Someone in the military, I hope…

[Garigue] All organizations need to be doing some type of technology assessment activity. Comparing the recent developments in the commercial world with military requirements in test laboratories and doing technology insertion proof of concepts are a good way to "test and try."

[Giessler] The ultimate user should find the acquisition with the aid of people at places like NRAD, ESC, NRL, ARL [Note: these are all military acquisition or research organizations], service labs and academic places like NPS. This is going to be the toughest part…How to stay current and adapt/adopt/acquire/find/be aware of the available and useful technology. JWIDs [Joint Warrior Interoperability Demonstrations], Ft. Franklin, and ATIDs [Advanced Technology Interoperability Demonstration] etc., will have to be used as well as displays at shows and conferences. We may find that we have to put DoD people out in industry just so we can keep abreast of what is going to be available. It may require a new specialty officer called the information science and technologist.

[Gust] The responsible party should be consensus forums, not single function activities like ARPA [Advanced Research Projects Agency], laboratories or PMs [Program Managers]. Using ACTDs [Advanced Concept Technology Demonstrations] from the R&D community results in the follow-on program fund lines to have in them a source of leave-behind funding for O&M [Operations and Maintenance] commands to evaluate in the field for two years. Also, fund lines need a production wedge for those R&D initiatives that will mature shortly, i.e., those funded at a 6.3 or 6.4 [Note: these are different kinds of R&D monies] maturity level.

[Hazlett] Need to coordinate information management across the services and agencies. Take better advantage of economies of scale, like needs and like requirements.

[King] There needs to be a group that keeps up to date on changes and can understand which new items are worth incorporating into the existing systems. It is probably best to outsource as much of the actual integration work as possible.

[Loescher] I disagree with the premise. The "array" of commercial information technologies is becoming more and more homogeneous, as standards become valuable to the marketplace. Thus, an information system for MacDonald's in the future will be much like that for DoD—they'll just need different information in different times and places.

[Probst] Well-trained specialists with reasonable career paths.

[Schwartau] I have no earthy idea how to solve this. How about establishing a technology excellence center, a sort of government help desk, which is staffed to address questions from interested acquisition officers on what the latest and greatest is. This center should also track the real-world commercial implementation of advanced technology, most notably in the financial arenas. Why reinvent the wheel for the sake of job security?

[Steele] Let the free market work its magic. Our biggest enemy now is misplaced security constraints which prevent openness, and procurement constraints which give an advantage to beltway bandits skilled at paperwork rather than genuine innovators with something unique to offer. DoD cannot put its house in order by itself; the White House must offer an umbrella program, and a genuine Chief Information Officer network at Undersecretary levels, with real resource authority, or the Services will continue to protect pet rocks and "special arrangements."

[Moderator] Given increased use of commercial parts, should the military rely more on the commercial world for its information technology logistics support? Will it be better to "throw away" a broken system and order a new one rather than maintain the capability to repair it?

[Campen] Don't get trapped by the definition of parts for broken THINGS. Other than a cheap, commercial, dumb, terminal in the field, that does nothing more than accept applets from a global information service supplier, there is nothing to repair. If the dumb terminal is broken, then throw it away. The main concern ought to be ensuring continuity of information services.

[Cebrowski] Generally, yes; but where that is too expensive, do something else like reassess the requirement.

[Cochrane] See previous question. Presume that by "broken" you mean breached security. I would say the "new or repair?" question probably needs to be reviewed on a "per case" basis. However, it is probably safe to say that repair would be a valid option in many cases. The system breach might be fixed easily with little extra cost and with a good deal of confidence in the new level of security, without the worries of implementing a completely new system. If the replace option is taken it may be necessary to run the broken system until a replacement is available, this necessitates a certain level of repair. If a "broken" system were to be replaced it may be redeployed for use with lower grade information thus increasing its lifespan. It may be more economical to replace the infrastructure of the system with a new one.

[Cohen] Waste not want not.

[Dunnigan] The commercial model for operations stresses efficiency, thus it is the one to follow (as the military has done for centuries…)

[Garigue] There are no universal rules. The solution must be dictated by the problem and not a policy. In many cases there are good reason to dispose of systems in a rapid way. The fixed cost of repairing some components are not worth it. Better buy replacements. But new components sometimes come at the cost of poor backward compatibility and increased dependence on outside organizations.

[Giessler] Yes to both questions. And often we will throw it away because it is superseded—redistribution will replace maintenance.

[Gust] Actually, PEO-IEW [Program Executive Officer-Intelligence and Electronic Warfare] embarked on a "policy" several years ago that helps to solve this problem. We focused on 6UVME-formatted circuitry. This standard has turned out in industry like the VHS format in video recorders. With an open bus architecture, it is possible to plug in the next generation card and that is better than both repair of the old card or replacement of the entire system.

[Hazlett] The military should rely on civilian components except in those areas where there is no civilian equivalent, or there specific requirements that dictate a "military only" solution. Should go to more modular systems that can be incrementally upgraded, so that there are very few, true "legacy" systems. Upgrades to older systems often cost more over the long run, and provide less capability gains than new, replacement systems.

[King] For standard commercial systems, there are several vendors that can provide worldwide support. It is normally best to keep spare systems/components and switch to those while repairing the broken units. The repair versus throw-away decision should be based on economics.

[Loescher] It's better to do neither. We should lease the infrastructure and pay for it on our monthly "information bill."

[Probst] This is basically a question of outsourcing. If your source is competent, and will always be there for you, fine. Otherwise, watch out.

[Schwartau] That's a pure cost justification decision. Ask the commercial sector how it does it in comparable situations. Also, the IRS should change the depreciation of computer equipment from 5 to 2 years.

[Steele] It depends. On balance, because of the speed with which technology changes, it is NOT cost effective nor performance-mandated to protect legacy systems. In fact, they end up costing 80 cents on the dollar to maintain. However, there are going to be some elements that are not only critical, but too arcane for the private sector—and this leads to an interesting idea: if the private sector does not understand the value of a particular system, then either a) it really does not have a value and the military is overestimating its value or b) we should declassify the threat that inspired our value, and see if the private sector cannot adopt the same standards.

TOPIC F: AN INFORMATION AGE ACQUISITION ORGANIZATION

Management gurus of the information age proclaim the need for "networked" and decentralized structures in order for organizations to survive. Perhaps the movement of the military into information age warfare implies similar organizational changes in the development and procurement agencies.

[Moderator] Should the procurement of information technologies be decentralized? Should procurement funds be given to the unified commands (e.g., Pacific Command) and/or individual units instead of the individual services (e.g., Army, Navy, Air Force)? Or is a "joint" acquisition organization (perhaps similar to the Strategic Defense Initiative Office) more appropriate?

[Campen] The framing of this question still implies a focus on THINGS. Information services should be established by functional basic ordering agreements that apply to similar functions in all services, on a global basis. Individual units then access these information services essentially the way they now do food and water, paying a users fee, if necessary, to support a common industrial fund. Using Intelligence as an example, DISA [Defense Information Systems Agency] provides the communications protocols and controls the network at the operational level; functional activities, such as DIA, NSA and CIA provide the functionally tailored information services, and the user taps into the system as required.

[Cebrowski] The spirit of Goldwater-Nichols and other mechanisms address these issues in that: a.) CINCs have more input in defining warfighting requirements—which is inherently decentralized b.) Operational units have significant latitude to apply discretionary funds in a manner that best meets their needs, and c.) The Joint Requirements Oversight Council ensures maximum warfighting efficiency by validating and articulating requirements to the Defense Acquisition Board—in essence, they embody the necessary ingredients of a joint acquisition organization. I prefer joint and decentralized to reinventing communism.

[Cochrane] Speaking from experience of a commercial organisation, decentralisation causes problems. A decentralised organisation results in a plethora of systems performing the same job in different location, on different platforms written in different languages. A centralised approach should provide a co-ordinated approach but needs to be fast and give the flexibility in the field. However, care must be taken to ensure centralisation does not bring the disadvantages of complete standardisation. If an organisation were to standardise on a particular type of hardware, it would be completely compromised if the hardware were to suffer a serious security breach. Are there any reasons for each service to procure information systems separately, let alone each unit? I would think that the needs of one type of military organisation are pretty much the same as the other. One absolute necessity is that the systems should interwork seamlessly. It would also be nice to think that a marine defending an army base should be able to use their equipment in the same way as his own kit. If each service can not work with each other then the game could be lost before it starts!!!!!

[Cohen] Centralized planning—decentralized execution. The price and terms should be negotiated on a DoD-wide contract to minimize costs. The specific equipment should be ordered and processed by the most local person needing it. The acquisition should be based on an established need and method for fulfilling that need identified to and approved by the chain of command.

[Dunnigan] It already is decentralized. Lotsa luck separating the individual eggs from that omelet now.

[Garigue] The question of centralized vs. decentralized organizational structure is a big debate and an essential one. The money should go where the knowledge is. Who knows best should decide. Certainly the architecture and the standards could be centralized and the acquisition and the procurement can be decentralized. But in the case of very large organizations such as the Army, Navy, etc., the question cannot be resolved because all organizations have enough capabilities and resource to suffice to their own needs. None will agree on either solution. So the debate will continue.

[Giessler] Decentralized? Yes. Procurement funds given to unified commands and/or individual units? Yes for most I.T., only unique non-COTS stuff should be centralized. Is a "joint" acquisition organization more appropriate? Only for unique stuff and that should be less than 5 percent.

[Gust] We have had CINC-initiatives with discretionary funds for many years. It has resulted in some duplicative procurement and some non-interoperability horror stories. One cannot even specify UNIX without some disconnect across that product line. I think some centralization at the Service level is appropriate, mainly because that is where the best handling of funding and most flexibility in any reallocation or reprogramming of funds occurs. A joint activity carries too much baggage. My latest and most perplexing problem is to try to start a new common intell broadcast receiver program without a finalized joint ORD [Operational Requirements Document]. I have FY 96 dollars that must be spent, but the joint ORD approval process, which requires CINCS' coordination, will take so much time as to be in the next fiscal year. Jointness in buying JTIDS [Joint Tactical Information Distribution System], GPS, MILSTAR are three examples where time was traded for joint coordination, but Services retained the dollars on these programs. That is probably the best way to go.

[Hazlett] Should be more coordinated, not less. Particularly important from an affordability viewpoint. There is little overlap today between the services, even where there are similar, or even identical requirements. Virtual organization concept has merit in the acquisition world. Services, CINCs, etc., should form temporary virtual alliances when like needs exist, or joint development makes sense. One large acquisition organization may be too unwieldy.

[King] The goal should be to make the procurement process as efficient as possible. Something like a central group that prepares specifications and bid guidelines and then each command doing its own actual acquisition.

[Loescher] I would go further. ALL organizations, including tactical organizations, will be streamlined. Modern command is about moving information to take advantage of openings that happen orders of magnitude faster—and further from the tactical operations area—than war in the past. The officer hierarchy structure is a reflection of 19th Century land warfare and 20th Century ricebowls. With respect to development, a centralized, much smaller, Service-specific R&D outfit with ties to industry labs and Universities is the way to go, at least for the next 5-8 years. Government employees at the mid-level cannot stay in touch with commercial technology to buy it properly; but they can be focused on Service unique problems, which are not insignificant. Procurement of information systems should be decentralized; procurement of large information pools may be better bundled.

A joint office, just means, joint bureaucrats. What we need are new ideas to create new markets for new industry to sell to us—not more bureaucrats to oversee the existing industry, which is a reflection of yesterday's acquisition.

[Probst] Definitely, but interoperability can be guaranteed. But management gurus are not to be blindly trusted.

[Steele] Yes and no. Local authority over the realignment of funds is critical. For instance, PACOM [Pacific Command] briefed me several years ago that they had hundreds of thousands of dollars earmarked for TEMPEST hardware they did not need, and zero dollars for open source collection and production (including their library), so they had to cancel their LEXIS-NEXIS account. Generally the local command knows its needs best. HOWEVER, the current system of penalizing commands for savings is out of touch with human nature. They should be allowed to roll saving overs and reinvest in other priorities. Joint mandates of specific systems and software will produce results as dumb as the Marine Corps suite, where one word processer is mandated and purchased, and ignored Corps-wide, while WordPerfect is bought by hook or crook and is the actual Corps standard.

[Todd] Realizing the short term focus of the Unified Commands, the truly "out of the box" thinking has come more from technology push from the Services (stealth as an example) than from requirement pull from the Unified Staffs. Of course, I realize this is an iterative process and the integrated priority lists are of significant value to identifying what to pursue technology wise. Likewise, a joint office has its place in a very restrictive role. The Services should retain their function in the R&D arena.

[Moderator] Should "acquisition technologists" be put in operational units in order to quickly acquire and transition new capabilities?

[Cebrowski] This is more a matter of process and education than one of organization.

[Cochrane] Three options depending upon how you define information warfare.
- Moving operational people to the technologists would be far less dangerous for everyone involved. Technologists could get military requirements for systems in the same way that they acquire requirements for commercial systems. When getting new kit into the field I would think operational personnel would be happier learning from their peers who know the problems of operating in the field rather than suits from computer companies.
- As new information warfare technology can change the face of a battlefield within hours it may be necessary for IW units to contain not only acquisition technologists but also their own front-line research and development teams.
- Since information warfare creates a whole new battle field, cyberspace, it creates a need for people that understand warfare to work closely with technology gurus.

[Cohen] No. The person who actually needs a particular piece of technology should be able to go and get it if they want to, but it should be a pre-approved item or technology (except on an emergency basis) from a pre-approved source at a pre-approved price.

[Dunnigan] Put them somewhere out of the way so that the end user organizations can go get what they feel they need.

[Garigue] The logistics officer should be able to buy anything—putting it together is another issue. There needs to be a Information System Officer for that. With new technologies there are new classes of specialists that are required. In the navy we went from sail to steam, with this a new officer cane into the wardroom, then with electricity came another type of officer, now with software becoming the dominant war technology there will be the requirement for a new specialty in the military.

[Giessler] Yes—but that will happen when we select people who think and have an I.W. paradigm and educate them at NPS and AFIT [Air Force Institute of Technology] and all PME [Professional Military Education] at all levels. The Thrashers and Elams and Garcias are already the info science and technology officers and officials. All we need to do is get out of their way. And Comdr Loescher is leading that effort at USN headquarters.

[Gust] The Army still uses its TRADOC organization as the "user's rep" to consolidate requirements. The last thing we need is for each Army division to buy its own technology and then have to join up in a large force side-by-side like in Desert Storm. If you want it bad, you'll get it bad.

[Hazlett] Should stand up several joint and single service organizational and technological testbed units whose manning includes acquisition technologists. Not sure that they really belong or can be kept gainfully employed in regular operational units.

[King] I would centralize the technology part of this and distribute only the actual acquisition part.

[Loescher] In the current model—buying systems vs. commodities—we are wasting our money. Decentralizing acquisition to buy systems decentralizes wasting of money. We need to get our heads out of hardware and software and into information. We don't need acquisition technologists then, we need at new kind of operator, who understands infotech as the technology of modern warfighter. He/she needs to take their places beside the aviation, armored, strategic bombing, etc, innovators of the 1920s to lead us into a different kind of warfare.

[Probst] I think so. Maybe not an operational unit strictly speaking.

[Steele] Acquisition is NOT an arcane specialty that requires magic incantations and special knowledge. That is the OLD acquisition paradigm where convoluted formulas had to be learned over years of study and practice simply to stay out of jail. The new paradigm should rely on open market viability and common sense.

[Moderator] With the focus on use of commercial products, where should the military acquisition organization concentrate its focus? Research and development? Management of contracts and contractors? Integration of systems? Development of interfaces and architectures?

[Campen] Assuming we need but a very small one, its focus should be on architectures, integration and interfaces, and continuity of service.

[Cebrowski] It should focus on simplification, outsourcing, teaming with suppliers, and making itself as small as possible.

[Cochrane] There is no simple answer to this: well defined architecture and interfaces are essential for rapid systems integration and reliability. However, continuous changes in the battlefield can only be met with new technology provided from a well funded and broad based research programme.

[Cohen] No. Yes. No. No.

[Dunnigan] If you buy in sufficient quantity, you can have a partial production run modified to your particular needs. This is done all the time. But you have to act like commercial purchasing operations (i.e., efficiently.)

[Garigue] Acquisition organizations should focus on shorter acquisition cycles and rapid distribution.

[Giessler] Most of it should go away but that which is left should either be a demonstration center which shows off commercially available products and what will soon be available or it should be acquiring unique stuff. The acquisition field must change. Research and development? Not much here and most of this should be done across service if not at the JCS/OSD [Joint Chiefs of Staff/Office of the Secretary of Defense] levels. Management of contracts and contractors? Local user goes out and buys COTS and support necessary—that will be different for each user and may change when someone arrives, then leaves a job. Integration of systems? The local group will decide if they are competent to create interoperability and integration software, hardware, management ware, etc. If not they will hire it done for the 12 to 18 months before they buy new stuff. Some parts of their info system will always be changing by their COTS buys. Development of interfaces and architectures? The C.O. [Commanding Officer] has the vision and his people either develop or hire or buy the interfaces that will allow them to do the job with their constantly adapting architectures.

[Gust] I think the focus has to be on all frontiers, none at the exclusion of the others. We just have to be cognizant of what the other players are doing.

[Hazlett] Military acquisition organizations should concentrate their efforts on identifying those areas where the military can best benefit from economies of scale and on identifying and coordinating the management of cross-organization and organization unique needs.

[King] R&D to keep abreast of changes and development of interfaces and architectures in order to provide the acquisition guidelines.

[Loescher] The first two. There are many Service-unique or at least military-unique R&D problems that will never be solved in industry. Secondly, we need to create a process at the contracting level to capture innovation and to learn how to pay for information, which is different than paying for torpedos.

[Probst] DoD does almost no research itself, and not much more development. DoD labs are quite different from DoE labs. Only options two and three are feasible.

[Schwartau] R&D for basic technology yes, in cooperation with the private sector, more along the European model. Standards are the key. I bet my bottom dollar that in a contest, a commercial outfit could get a system up and running much faster than a burdened military structure given the same tasking orders. The commercial folks would pick and choose available parts and glue them together for fast functionality. For military applications, a hardening step would be required, especially for mission critical life/death systems.

[Steele] There are always going to be some areas where the private sector simply will not support the kind of R&D that is necessary for unique military requirements. In the C3I area:

—Tactical document acquisition and digitization (such as rapid and rugged scanning of rough documents that are crumpled, wet, and hard to read; take on non-trivial pattern recognition problems

—Automated time and space tags on all multi-media information

—Build the bridges from commercial remote sensing platforms to the NRO/GPS precision points and then return the production of 1:50,000 combat charts with contour lines to the private sector—also build the bridges from commercial imagery through GPS/NRO to precision munitions already mounted on aircraft

—Digitize interactive speech for military police, coalition command & control, prisoner interrogation

—Communications & computing security

[Todd] The military should concentrate on integrating those systems deemed necessary to having a positive impact on the information battlespace. Knowing and having reliable information on our own forces; then being able to acquire, mix, synthesize and distribute information about our adversaries; then being about to orchestrate truly coherent operations against the enemy will have the greatest impact in future conflicts.

[Moderator] What are the institutional impediments to the creation of an information warfare infrastructure?

[Campen] Trying to adapt a structure built to buy, field, install, maintain THINGS into one needed to obtain information services. As the Congress noted in passing the new rules for acquisition of information technology, the hardest thing to change will be the culture.

[Cebrowski] The infrastructure already exists—what's needed is more time and effort for intellectual maturity.

[Cochrane] Impediments to the creation of an information warfare infrastructure.
- Military and governmental establishments and those that derive power from their positions in such organisations.
- The acquisition agencies with their preferences and cozy relationships with the "safe" traditional suppliers.
- Selling the concept to the public. If you say that there is a need for information security improvements the implication is that systems are insecure. No one wants to admit to problems, they just want to sort them out on the quiet, the result is that knowledge is not shared. The public are also quick to see a conspiracy and think that faceless governments are going to use the systems to further their own aims.

[Cohen] Were there any?

[Dunnigan] Stepping on someone else's toes.

[Garigue] The mind set. Cyberspace is not seen as a possible battlespace.

[Giessler] The most difficult is to get national security operatives at all levels to drop their old paradigms. The infrastructure is an implicit one that has to be inculcated not defined. It has to be part of the control system of individuals and organizations who understand the goals, objectives and CO's that capitalize on the COTS technologies—and then educate, train and exercise the force to create a revolution in military affairs.

[Gust] Everyone wants to be in charge. How many times have we have a new initiative and one Service has jumped up to lead so that their service-unique views or needs are served first? Examples are UAV [Unmmanded Aerial Vehicles], strategic defense, space-related technology. We cannot all be the leaders, and the leaders have to be more accommodating of the needs of the other services. The followers also cannot be too parochial in their demands for "all or nothing" type solutions.

[Hazlett] Rice bowls and service rivalry, primarily. The services have been way too quick in carving up IW into narrowly defined areas. Some IW areas can best be handled in concert, rather than singularly.

[King] Information warfare is much more abstract than conventional warfare and it will be harder to get people to think about (and fund) it. In order to successfully control a networked nation it will probably be necessary to increase the security and therefore the restrictions. This goes against the current "open" atmosphere.

[Loescher] Institutions. You cannot create a new kind of warfare with old stovepipe warriors. But the stovepipe warriors control promotions—until we find a means to truncate the dynasties or until the dynasties tragically prove their unsuitability to the new world. Historical examples are everywhere, from the Trenchs of WW I to Battleship Admirals to today's Information Warfare—which is basically cryptology reinventing itself in the guise of new term. There is a new Information Warfare, absolutely, but you won't get there by renaming the past, which is Navy's current mistake.

[Probst] Established privilege. Empire building. Lack of agreed-on concepts.

[Schwartau] I do not know what an IW infrastructure means here. I could interpret this a dozen different ways. Sorry.

[Steele] The institutional leaders below the Secretary of Defense. ACTUAL—the classification of the threat. The games Navy plays to compartment IW simply to keep its own toys and avoid joint endeavors. The general lack of understanding at the flag level of why intelligence is broken and open sources are a major part of the IW fix. The unwillingness of ASD C3I [Assistant Secretary of Defense for C3I] to stand tall and tell it like it is…