OSS, Inc.

OPEN SOURCE SOLUTIONS, Inc.
International Public Information Clearinghouse

19 January 1995

Keynote Speech to the
Second International Conference on Information Warfare:
Chaos on the Electronic Superhighway
Montreal, Canada

THE MILITARY PERSPECTIVE ON INFORMATION WARFARE: APOCALYPSE NOW

Mr. Robert D. Steele, President
Direct Electronic Mail: <ceo@oss.net>

I've been asked to be blunt, to be specific, and to move us toward closure with respect to the enormous dangers facing our respective Nations. I do not represent any particular military, only myself as a professional who has been invited to suggest to you what the military perspective should be on this very important topic.

We are at war today, and anyone who does not understand this is part of the problem. We are in a state of total war right now, and unfortunately for the traditional military commander, 99% of the troops, weapons, and platforms are civilian--they are "out of control".

It is our responsibility to both inform the public--for without public support no democratic government can hope to muster the necessary resources for defense--and to guide our governments in developing sound information warfare strategy and policy--and I will stress up front that it is not possible to have an information warfare strategy or program without having a larger national information strategy and program.

Today I will set the stage by reporting briefly to you a few highlights from an information warfare conference which took place in Washington 8-9 December 1994. Some of you may have been there, please bear with me and jump in later if you wish to comment further.

I am going to outline a more complex concept of information warfare, one which makes it clear that we are now in an era of distributed "out of control" information warfare that is pervasive, and which absolutely requires the total integration of the civil sector.

11005 Langton Arms Court, Oakton, Virginia 22124-1807
Voice: (703) 242-1700 - Facsimile: (703) 242-1711
Internet: <oss@oss.net>

I will end with some very specific prescriptions for rapidly stabilizing the situation, containing our vulnerabilities, and achieving--if not information dominance, then at least information survivability--within the cyberspace battlefield.

Vision Statement

Let me begin with a vision statement and an enumeration of the 4 Cs for a viable information strategy, as that will give you a skeleton upon which to place my intervening remarks in context.

In the age of information, national security and national competitiveness require the full integration of and the harnessing of what the Vice President of the United States of America has called "the distributed intelligence of the Nation". The battlefield is now global, every human brain is a sensor, and every C4I architecture must provide for real-time exploitation of all human, electronic, and hard-copy sources pertinent to battle planning and battle execution--the vast majority of these sources are civilian, and foreign.

To achieve information sustainability if not information dominance in the 21st century, it is not enough to create a few disjointed military information warfare centers. We must have national information strategies and we must mobilize the total resources of each nation and indeed of the whole earth. An information strategy must enable the military to harness--without controlling--civilian capabilities, and it must address four distinct capabilities, the 4 Cs of a healthy electromagnetic diet: connectivity; content; coordination of research & development; and C4 security.

Summary of U.S. Conference on IW, With Comments

Let me begin with a summary of a very fine conference last month (8-9 December 1995). I am indebted to Ms. Melissa Call, of PSC, who provided me with her observations as I was in Europe at the time of the conference. Her summary appears in the December issue of our international newsletter, ***OSS NOTICES***, which is available by subscription.

It is clear--all of the speakers were unanimous on this point--that neither the U.S. military as a whole, nor its allies, have established even the most rudimentary agreement with respect to concepts, doctrine, training, equipping, and organizing for information warfare. Right now we are in a period of transition--much as we were after the invention of the machine gun, or the

tank, or the helicopter--and a thousand poppies are blooming. Unfortunately, we are on a very fast track, and every day brings us closer to electronic apocalypse. Unfortunately, this fine conference reflected the enervation of our existing approach to information warfare in that only the military were there--the most important players in information warfare, the Departments of Treasury, Commerce, and Justice, the telecommunications companies, the computer manufacturers--they were not present and they remain oblivious to the grave threats facing them, and through them, our respective Nations.

My first point: this is not about war by conventional means. This is about war by other means, and those other means do not wear a uniform, salute, pull a trigger, or even appear for muster. *The military is now in the very unusual position of having to play Paul Revere to the civil sector, and mobilize the local militia in a way far more vast, far more subtle, far more difficult, far more time consuming, and far more expensive than any we have ever imagined. Among many other challenges, we must address the reality that a classified threat is not an actionable threat in the civil sector--if we do not declassify the threat and provide explicit, meaningful, shareable threat data to the private sector, they will continue to ignore the problem until it is too late.*

Now a few highlights. From Colonel Douglas P. Hotard, Director of Information Warfare for the Assistant Secretary of Defense for C3I, we learn that 95% of U.S. military communications depend on the private sector's paths and nodes. We also learn that the integrity and reliability of the communications path is only half of the problem set--the other half is dealing with the volumes of multi-media data that do get delivered--about being able to "tighten your own decision cycle while extending your enemy's".

My second point: information warfare is not only about degrading and destroying and diverting communications and computing resources--it is in fact much more than that, and must also include the ability to find, fix, and exploit data in support of decisions down to the individual level. *In the age of information, national security and national competitiveness depend on <u>both</u> the survivability and integrity of the electronic infrastructure, <u>and</u> the depth, breadth, and utility of the content in the information commons to the individual combatant....and of course now we are beginning to understand that the combatant is not in uniform, but is in fact what Robert Reich calls a "symbolic analyst".*

Having joined with Col Hotard in stressing the two sides of information warfare--one focused on connectivity, the other on content--let me also note that he listed a number of technologies critical to the successful conduct of information warfare--a list which sounded very much like a cross-section of Sunnyvale start-ups, Japanese acquisitions of U.S. businesses, and French collection requirements.

My third point: "dual use" is no longer migrating from the military to the private sector, but rather from the private sector to the military. *The battlefield has flipped--the traditional front line is now a sideshow, and the rear area knowledge terrain has become both the Achilles' heel, and the center of gravity for what Alvin and Heidi Toffler call "war and anti-war".*

From Brigadier General John Casciano, Commander of the Air Intelligence Agency, we learn that the Air Force element of the U.S. order of battle for information warfare operations is called the Air Force Information Warfare Center, that it was established in September 1993--fully twenty years after personal computers became a reality--and that it will eventually house 1,000 people and have a $40 million budget. He also commented that there are 150 separate intrusions on Air Force systems per month, which strikes me as a naively low number--and I don't know whether it includes permanently installed sniffers such as were recently discovered at Rome Air Force Base. General Casciano also commented about how the ability to gather, process, disseminate, and use near-real-time information is at its highest level, as are the capabilities of smart weapons to destroy targets and minimize casualties.

Well, I have a problem with just about everything he said, not because any of it is wrong, but because it points out the stark gaps in our knowledge.

First, it is clear that there is a major disconnect today, in the United States of America and I suspect also in Canada as well as the United Kingdom, over the respective roles of the individual military services with signal intelligence and space or electronic warfare capabilities; the National Security Agency; the Federal Bureau of Investigation; and civilian organizations like the Department of the Treasury and the Federal Reserve.

Second, the difference between technology on the shelf and technology on the field cannot be under-stated. The reality is that it took us 60 days to collect the digital data we needed to allow all those fancy airplanes with their precision weapons to be useful in the Gulf War. The reality is that of the 69

"high probability" countries I personally studied in 1989 while serving as the senior civilian at the Marine Corps Intelligence Center, we had zero 1:50,000 combat charts for 22 of them; 15 year old data for ports and capital cities only --not for the maneuver areas--for another 37--and very old complete coverage for only ten. The reality is that the encyclopedic mapping, charting, and geodesy database is not there, and the reality is that our sensor to shooter interfaces don't exist because the operators have dominated the Tactical Intelligence and Related Activities Program (TIARA). It was an aviation general that cancelled the Marine Corps RF-4B, and it is operators that decide every day that intelligence sensors and communications paths are not a "real" priority. When you combine this with the fact that 95% of our communications go over extremely vulnerable commercial paths that we cannot protect or isolate, you suddenly find that you are not only blind, but also deaf.

My fourth point: we need to know how dumb we are. *In addition to understanding our vulnerabilities to information warfare by others, a vulnerability that should be better understood once the Special National Intelligence Estimate now underway in the U.S. is complete, we must also be prepared to conduct an honest inventory of our ability to conduct operations other than war, as well as operations in cyberspace. Purple is now not just joint, but civil-military.*

Colonel David Tanksley, Director of the Land Information Warfare Activity--somehow that title strikes me as an oxymoron--coined a popular analogy adopted by other speakers; he described the U.S. information system as a "spear", with classified systems comprising the hardened metal point of the spear, and unclassified systems comprising the wooden shaft of the spear. he noted that it is the shaft, carrying virtually all of the operational, logistics, and personnel information, that is most vulnerable to interdiction and disruption. He also noted that there is an urgent need for common terminology, and that one of our self-imposed handicaps is the wide variety of unintegrated databases--the Army identified 150 databases essential to its prosecution of the Gulf War.

My fifth point: the civil sector, and its role in providing and storing unclassified content--is now acknowledged to be mission critical, yet we are not spending a dime--a penny--on the survivability, integrity, and reliability of that mission-critical environment. *As much as military professionals may want to stick their heads in the sand and say, "okay, we'll figure out offensive capabilities, let someone else worry about the civil sector", this is neither a prudent nor a permissible answer. The civil sector is our*

center of gravity. More on that with my conclusion and my specific recommendations for a national electronic security program.

Navy Captain R. R. Caldarella, Director of OPNAV N-64, the Information Warfare/Command & Control Center, opened his briefing by stating that the Navy's view of IW was evolving and "admittedly disjointed" at present. He has a much more extended view of the battlefield than most military professionals, and seemed more conscious-citing open sources of intelligence--about the real capabilities for information warfare that exist in Iran, Iraq, Syria, Libya, and North Korea. He also commented that information warfare equates in fact to early preparation of the battlefield, and that this is difficult to accomplish in today's Navy which does very well in war and the transition to war as traditionally understood.

Something he did not say, but something I learned while participating in Technology Initiative Game 1992 at Newport, is that information warfare changes the definition of "commencement of hostilities". It is no longer "rounds out" We cannot afford to wait for the first Silkworm to be fired, for it will almost assuredly take a ship of the line--we have to detect and interdict the software code that initiates the firing process--and in the process cope with what may be the single most difficult challenge facing information warriors, which is to persuade U.S. Ambassadors and others that do not understand these matters that an attack has been initiated and they have ten seconds to concur with a counter-attack. Of course in reality the commander is going to have to put his or her career on the line to protect their platform or unit, but this points out how much more difficult the political-military dimensions of war have become.

My sixth point: everything we ever learned about warfare, and especially about the difference between war and peace, between allies and enemies, between combat arms and supporting services, between CONUS and OCONUS, is out the window. *We are at war today, but we are blind to the cybernetic cancers eating away at our national security and our national competitiveness. More on that also, in the conclusion.*

Mr. Robert Ayers, Chief of the Center for Information Systems Security at the Defense Information Systems Agency (DISA), gave what Melissa Call describes as "unquestionably the frankest and gravest view of the current safety of unclassified U.S. government and military systems". Using hacker tools freely available on the Internet, his group has been running "Red Cell" operations against U.S. systems.

-- 88% success in penetrating targeted systems. The FBI has been reporting 96% success. My friend "Eric Bloodaxe" of Legion of Doom fame actually had a company to do invited penetrations, and he has never failed....a 100% success rate.

-- 96% of all system penetrations were undetected.

-- In the 4% of the cases where penetration was detected, nothing was done 95% of the time.

Mr. Ayers estimates that only one in 1000 successful penetrations is ever reported, and that in any given year U.S. government systems are illegally though not necessarily maliciously accesses, at least 300,000 times. Mr. Ayers concluded his superb presentation by asking hypothetically who was responsible for protecting the economic backbone of the U.S., and noting that if DISA cannot now protect the DoD, it most assuredly cannot protect the U.S. C3I network, which is in fact its mission. I believe that candid and harsh assessments such as Mr. Ayers provided, based on documented practical investigation, render a vital service to our respective Nations, and I believe that Mr. Ayers has established beyond a shadow of a doubt our fundamental vulnerability.

My seventh point: it is counter-productive to limit our discussion to arcane issues of "space and electronic warfare" or "offensive command & control". The enemy is not just inside the gate, there is no gate, there are no perimeters, nothing is sacrosanct. *Information warriors are not just developing a new mission area, they are completely redefining war and peace and they are completely redefining the relationship between the military, the business community, the academy, and government. Any discussion which does not take place in this larger context is down in the weeds. We have a responsibility for the civil defense, we have a responsibility for understanding and communicating the "aggregate threat" as Mich Kabay labels it, and we have a responsibility for working with our law enforcement and civil sector partners to protect our home front.*

The final speaker at this splendid conference in Washington was Colonel Gary Payton, Commander of the National Air Intelligence Center, which I would also like to point out is the executive agent for the DoD open source intelligence program. Colonel Payton focused on the implications of information technology for the changing role of the analyst, and made the point that in a real-time distributed information environment, the intelligence analyst

can no longer work in isolation nor define their work in terms of finite products which are pushed out to the commander and his staff. In a nutshell, information warfare requires the integration and harnessing of the intellects of both the operators and the analysts, to achieve rapid and effective decisions in tandem.

My eighth point: information warfare is not about bits and bites and High Energy Radio Frequency guns or electromagnetic pulse bombs, it is about applied intellect--it is about harnessing intellect and protecting intellect, and it is above all about providing the commander--including the civil commander in the role of political, economic, or cultural leader--with survivable, reliable, decision-support through war and operations other than war, on the home front as well as on the traditional front line--and to do so largely with "out of control" civil resources.

War and Peace in the Age of Information

So where does this leave us? Yesterday we discussed personal, corporate, and global information warfare, in terms defined by Winn Schwartau in his wonderful 1991 novel *TERMINAL COMPROMISE: Computer Terrorism--When Privacy and Freedom Are the Victims*, and more recently in 1994, in the book we have all been discussing, *INFORMATION WARFARE: Chaos on the Electronic Superhighway*. Today I want to bring us to closure by providing the larger context within which we must define our calling, and to provide some specific recommendations for establishing viable national electronic security programs in the context of national information strategies.

Where this leaves us is with the intriguing possibility that the two cornerstones of national security--a strong conventional military and a global intelligence service which emphasizes spys, satellites, and secrets--are in fact now cumbersome, grossly over-valued, deceptively and unjustifiably reassuring to the populace, and in fact insupportable. And of course, there is the simpler matter of whether they can do the job or not, if they can in fact contribute to national security in proportion to the resources that are expended upon their training, equipping, and organizing.

We are in fact entering a new era, when every citizen is a member of the cyber-militia, when every organization is cyber-militarized, when every nation--indeed every tribe and religion and criminal gang--has global reach and the power to destroy other nations with undetectable, untraceable

electromagnetic agents. We in this room represent the vanguard for a completely new national security structure, and it is our task--as it was the task of the Committees of Correspondence and such stalwarts as Patrick Henry and Nathan Hale--to mobilize our electromagnetic defenses, mobilize our electromagnetic militia, mobilize our electromagnetic neighborhoods, and carry on with the task of creating a cyberspace where it is safe to work, to play, and to conduct the game of nations without fear of apocalypse.

Let me now define where I think we as a predominantly military culture need to go, and where we need to help our civilian counterpart go, if we are to secure our national security in the age of information.

First, there is no higher priority within the military establishment than to insist, at the Presidential and Prime Ministerial levels, on the immediate declassification of the electromagnetic threat, and the wide dissemination of that threat to all elements of the civil sector.

This is fundamental. We cannot afford the luxury of waiting for an electronic Pearl Harbor to mobilize public opinion, for two reasons: first, because the catastrophic outcome of a major electronic disaster, one which degrades or destroys major financial centers--eliminating trillions of digital dollars--or other key elements of our national fabric, is not supportable by our existing economies. *We cannot afford the cost or the time to reconstitute our civil sector.* The second reason is more frightening: it is highly unlikely that we will be able to prove with any certainty which nation, organization, or individual was responsible for the attack. It will be virtually impossible to mobilize public opinion in support of a conventional military response, and I can tell you with total confidence that our intelligence communities are not competent in this area--they are neither able to warn of this sort of electronic attack, nor are they able to identify with assurance the perpetrator.

Second, we should take the approach followed by the Germans between the World Wars, and undertake a major shift in resources--both human and capital--toward information warfare and information peacekeeping capabilities. Our existing military represents the Maginot Line of the 21st Century.

There are four warrior classes which we will face in the future. The high-tech brute, with expensive armor and aircraft which require hugh logistic trains to support, is the traditional enemy. While this enemy will be with us for decades to come, this is also the least likely opponent. The other three

warrior classes require differing levels of investment which we have not yet undertaken: the low-tech brute, meaning the transnational criminal, the narco-terrorist, these represent the very difficult "low slow singleton" problem for intelligence, and are especially difficult for the military to address because of their tight kinship and ethnic foundations and their unconventional aspects. The low-tech seer, represented by major cultural and religious movements, and including for convenience's sake massive groups of refugees spawned by internal disorder as well as environmental disaster, is another challenge which the military will have to deal with and for which it is not ready. In the United States of America, for instance, we still do not have Tables of Organization or Tables of Equipment for active duty forces needed to operate refugee or prisoner of war processing centers--we are deficient in that aspect of IW.

But it is the last class, the high-tech seer, that is of concern to us here today; I count in this group both those who conduct information-based economic warfare, and those who use information warfare for personal, financial, or political motives. The balance of power has shifted from organized forces supported by taxation and conscription, to autonomous electronic agents spawned *at no cost* in cyberspace, and targeted by single individuals against complex systems which are at this time impossible to defend.

Third, we need an immediate and comprehensive change in the law to establish the fiduciary responsibility of civil sector managers for communications and computing security. Stockholders must realize that their managers have been criminally negligent in failing to protect proprietary information from electronic theft; and managers must realize that the communications and computing companies have been criminally negligent in failing to provide adequate security measures for the transmission and handling of information.

As Professor Bill Caelli, Head of the School of Data Communications within the Queensland University of Technology (Australia) is fond of pointing out, when the mainframe joined the mammoths in the tar pit of history, what little concept our information industry had of security went with it. We have raised an entire generation of hardware and software engineers who are--quite clearly--clueless about security. What we sell today is the Ashberry Park of cyberspace! And like the free love and free living of the 1960's, with random sex, no bathing, open bowel functions, our existing communications & computing industry is spawning a whole slew of diseases.

To give you one specific example of how corrupt the computer industry assembly lines are, let me just note that one major U.S. government organization, one which is quite competent in the computer area, discovered 500 hardware and software viruses in one single year, and all within shrink-wrapped products intercepted for testing at its loading dock. In my mind, this is criminal negligence on the part of the computer industry.

In a very intriguing sort of way, holding civilians responsible for "safe C4" is the cyberspace equivalent of the draft--virtual co-optation.

Fourth, the military must acknowledge that it cannot dominate information warfare and that it must completely recast its understanding of information warfare to enable joint operations with civil sector organizations including law enforcement, businesses with needed skills, and universities.

We are entering a period of guerrilla warfare, to use an analogy our military colleagues understand, where every citizen has a role to play, and the most the conventional military commanders can hope for is to provide a degree of strategic guidance and logistics support to the largely popular effort.

The focal point for information warfare in the next decade cannot be and will not be the military. The focal point must be law enforcement, not only because the civil sector must be brought into compliance with new security standards through law and law enforcement, but because only the civil sector is capable of dynamic "out of control" rapid responses to new threats. I love the U.S. military, and especially the Air Force with its nurses, and air conditioned quonset huts, and nice officers clubs which I as a Marine admired from afar when I was overseas, but the idea of "solving" the information warfare problem with 1000 people and $40 million in San Antonio is disturbing, for it reflects a very conventional approach to a problem that does not lend itself to conventional thinking.

Within the United States of America, to use the example I am familiar with, we must have an Electronic Counterintelligence and Security Division within the Federal Bureau of Investigation. The Secret Service should be relieved of its dubious assumption of responsibility for electronic crime. The National Security Agency and the military should have significant roles in supporting the FBI and in developing rear area electronic security programs funded through the realignment of DoD dollars--and I will end with my specific recommendations. A National Center for Electronic Security, with a

very strong international outreach program, should be established where the government, including the military, can come together with business and the academy to test and certify new means of achieving electronic security.

Fifth, and finally, every nation, every organization, indeed every individual, must have an information strategy and policy which provides not just for connectivity, but also for content, coordination, and C4 security--the 4 Cs of a healthy electromagnetic diet.

Within the United States of America, I have circulated a document, available to all of you through <oss.net>, titled the National Security Act of 1994. It is my hope that the President will work closely with the new Speaker of the House to introduce a bi-partisan National Information Strategy in 1995. I feel very strongly that the juxtaposition of Al Gore in the last two years of President Clinton's first term in office, and Newt Gingrich in his first two years as Speaker of the House, offers the United States of America a unique, a priceless, opportunity to achieve a strategic international information advantage that may never be duplicated--and it will be an advantage with benefits for our allies.

The Four Pillars of Information Strategy

Let me spend a moment on the 4 Cs--the pillars of information strategy --as they pertain to the military and its role in assuring national security in the 21st century.

Connectivity is of grave concern to me. In the U.S. military, for example, we are still incompetent at communicating with coalition allies and civil institutions. We solve this problem by giving everyone we have to talk to a military communications team. Milnet is constraining individual access to the Internet. In essence, the military is preserving the unilateral conventional communications bunker, and shutting itself off from the wealth of external communications connectivity--and the open source intelligence content that connectivity can deliver to the commander. This must change right away. Operations other than war, to include humanitarian assistance and support to law enforcement, are going to be the most frequently executed operations in the 21st century, and the U.S. military is not trained, equipped, or organized to communicate effectively when conducting such operations.

An important part of information warfare is the ability to communicate--right now the commander is not able to communicate

effectively with perhaps 75% of the key players in future operations. Of course I define communications as the frequent and effective exchange of multi-media data, not simply the ability to patch an occasional radio into the civilian telephone network.

I want to make a second point about connectivity because I see too many military people settling for point to point or terminal to terminal connectivity as satisfactory. *The Internet is 10% of cyberspace, and cyberspace is 10% of knowledge*--any strategy for global information operations must recognize that 90% of the needed information is not going to be digital and that labor-intensive bridges are going to be needed to "connect" to that data. To take just one example, Jane's Information Group, a valuable resource for all military professionals, only publishes 20% of what they know because to publish more would place some of their sources at risk--but they will prepare a classified report for you on demand--most people don't know that.

Content is--with information warfare--my Holy Grail, so I will give this a few extra moments. When I served as the senior civilian responsible for founding the Marine Corps Intelligence Center, we spent $10 million on a Top Secret computing system with direct access to CIA, NSA, and DIA material, and had one little PC with access to LEXIS/NEXIS and the Internet, isolated behind a glass door. Imagine my shock when the analysts all started to complain that there was nothing in the classified data bases except for Soviet missile silo data; that the Third World "data fill" had not been done; and then--to my even greater astonishment--when they began clamoring for increased access to the little PC with access to "open sources". For me, the revolution to reinvent U.S. intelligence began with that experience in 1988....six years ago, and we have made so little progress.

A second important part of information warfare is to be able to find, fix, and exploit exactly the right information by getting it to the right person at the right time. Particularly with respect to operations other than war and support to law enforcement, where the U.S. intelligence community is virtually worthless, the existing military concept of "just in case" encyclopedic intelligence and archiving of data falls apart and is not worth the investment. As Paul Peter Evans of the Coalition for Networked Information points out, in the era of distributed information, "just in time" search and retrieval is by far the most effective means of supporting the consumer.

Let me make a further comment here on why private sector intelligence capabilities and data bases are going to be so critical to the military in the

future. The reality is that, both with respect to the technical nuances of information warfare capabilities *per se*, and with respect to the extremely broad array of substantive topics that will be of concern to future military commanders from one day to the next, it is impossible for the military to achieve what MajGen Ken Minihan calls "information dominance" through centralized, uniformed, saluting "duty experts". *IMPOSSIBLE.*

The only way to achieve information dominance given our fiscal and organizational constraints, is to be better than anyone else at reaching out and co-opting the right human experts and the right time--and the beauty of this is that someone else is paying for them to maintain their expertise on whatever arcane topic might be of passing interest to us. I call this "skimming the cream through the leveraging of private sector overhead".

In brief, the touchstone for information warfare is not connectivity and interfering with connectivity, but rather content--getting the right content to support your operations, and diluting, degrading, diverting, or destroying the enemy's content to hamper their operations. My very final comments will show how information security is the critical foundation for focusing on content.

Coordination of research and development endeavors, especially with respect to information technology but also with respect to all other applications including stealth, advanced materials, long-life batteries, and so on, is absolutely vital. The reality is that the days of major military investments in military-dominated research & development programs are over. As we noted earlier, the "dual use" equation has been turned around, and the military must now organize itself to understand, to influence, and to exploit private sector research and development initiatives, rather than pouring money into a wide range of speculative and often duplicative projects across service and national boundaries.

Taking a simple little thing such as a multi-media workstation, I will tell you that when I was on the Advanced Information Processing and Analysis Steering Group of the U.S. Intelligence Research & Development Council, I formed the distinct impression that ten different "black" compartments within that community were each spending $10 million a year to build their own unique version of what was in fact a generic requirement--a multi-media workstation. If you extrapolate that to the rest of the U.S. government and to the private sector, it is my view that we are wasting at least $2 billion a year in counter-productive and duplicative or fragmented efforts to create simple

tools. Apply this to other areas of information technology, and we are easily talking about $50 to 100 billion dollars a year of waste in the United States of America alone.

Now there are areas, and here I will limit myself to information technology, where the military must take the lead because the private sector will not. Drawing on my comments last month to the National Research Council, an arm of the National Science Foundation, let me note some specific areas where our military definition of information warfare must encompass a strong military-dominated research program. I am deliberately emphasizing content-oriented research rather than "soft kill" or "electronic patrolling" because I want to stress the point that information warfare is much, much more than pulsing or coding.

-- Tactical Document Acquisition, Digitization, and Translation. The private sector is not going to take on the problem of rapidly and reliably scanning rough documents that are crumpled, wet, and hard to read, nor are they going to take on the non-trivial problems of foreign handwriting and character recognition. Translation is more likely to get attention in the private sector, but still needs increased military investment.

-- Automated Time and Space Tags for Multi-Media Information. Real-time data fusion, and effective retrieval of all pertinent data for battle planning, will never be possible until all images, signals, and text reports have both a time and a space tag. The intelligence community has made some headway here, the military needs to take the lead in establishing standards and methods acceptable to the private sector.

-- Commercial Remote Sensing is going to be capable, within two years, of providing 1:25,000 as well as 1:50,000 combat charts with contour lines, and to provide real time guidance to precision munitions. However, the bridges from the commercial collectors to the military shooters will need to be built.

-- Digitization and Translation of Interactive Speech in Real Time. This is critical to coalition command & control, to military police and public affairs, and to improved prisoner interrogation and refugee debriefing.

Again, if information warfare consists of getting the right information to the commander while denying that information to the opposing commander, our information warfare community must be very, very careful to avoid

running off to build more "gee whiz" electronic gadgets,. and forget that they are part of an information environment. What good does it do the commander if you can wipe out enemy sensors while leaving him deaf, dumb, and blind for lack of content and connectivity to non-military content of military value?

Communications & Computing Security is the most deficient, underfunded, and misunderstood program in the United States of America, and I suspect in all other countries as well. Unfortunately, those who are most capable of understanding the extreme dangers in this arena--our military and our intelligence communities--went down the wrong path in the late 1950's, and chose to create for themselves an isolated, TEMPESTed, encrypted environment for limited communications and computing requirements, while relying on the civil sector for almost 90% of their remaining needs *without making a commensurate investment in civil electronic security*.

In retrospect, that was an understandable but enormous mistake, for we now have an Achilles' heel of very significant proportions--an Achilles' heel that is so complex and has so many points of failure, that it will take several generations to reach a condition of assured survivability and availability.

Our own Federal Bureau of Investigation has acknowledged publicly that it does not do counter-intelligence in cyberspace, and is not able to provide support to the private sector in defense against transnational as well as trans-state electronic thefts and intrusions. Our National Security Agency is prevented by law from domestic wanderings, not that cyberspace can be construed as domestic. The concept of "U.S. citizen" in cyberspace merits some scrutiny. We urgently need an executive agent for <u>national</u> electronic counterintelligence and security.

We have no standards, no testing & certification program, no public awareness program, and no legal liability for being negligent, even if being negligent today about communications and computing security is in fact severely detrimental to national security.

We cannot secure our nation from electronic attack without the complete integration of all civil communications and computing resources into our strategy. Any military professional who refuses to acknowledge this larger battlefield and persists in attempting to establish a service-based or function-based information warfare "encampment" is in fact doing a disservice to their profession and their nation, for we are at a point where we cannot afford to

wait another 20 years before someone rams the electronic variant of a Goldwater-Nichols Act down our information warfare throats.

To conclude, here is how I would spend the first billion a year, and I would hope to see this sum rise to 10 billion a year, equally divided between the military and the civil sectors.

01	Enact a National Information Strategy Act	20,000,000
02	Establish a National Center for Electronic Security	40,000,000
03	Declassify and Promulgate the Threat	10,000,000
04	Establish C4 Security as a Fiduciary Responsibility	30,000,000
05	Establish Basic and Advanced C4 Trusted System Standards	100,000,000
06	Authorize and Encourage Public Keys and Privacy Measures	200,000,000
07	Establish a National Information Foundation	25,000,000
08	Establish C4 Security Testing & Certification Laboratories	200,000,000
09	Establish an Electronic Counterintelligence & Security Division	25,000,000
10	Establish a Joint Information Warfare Corps and Center	50,000,000
11	Reorient Military C4 Toward Open Systems	100,000,000
12	Establish a Joint Military IW Research Consortium	100,000,000
13	Influence Civilian Information Technology Research	100,000,000

Information Warfare is total war. We are at war today. We have been infiltrated, our databases have been raped, our financial centers have been robbed, and a vast number of stay-behind software agents have been successfully implanted. We have a long hard road ahead of us.

I can only hope that we do not deceive ourselves and leave the civil sector to fend for itself, for this is most assuredly a prescription for defeat--it is within the civil sector--upon its knowledge terrain--where this war will be fought and won.

EuroIntel '98 PROCEEDINGS 1 st Annual Conference & Exhibit European Intelligence & European Electronic Security: Open Source Solu - Link Page

Previous	Reading About Hackers
Next	TAKEDOWN: Targets, Tools, & Technocracy

Return to Electronic Index Page