Author's Pre-Conference Final Draft, Ninth Annual Strategy Conference, U.S. Army War College
"Challenging the United States Symmetrically and Asymmetrically: Can America Be Defeated?"
31 March through 2 April 1998

TAKEDOWN:

Targets, Tools, & Technocracy

Robert David Steele
bear@oss.net

ABSTRACT

This paper is a "primer" which attempts to place national security and national intelligence in a larger context, one which must be understood if America is to survive and prosper at the dawn of the 21st Century. The targets are too numerous to discuss in detail, but they can be grouped into four large categories: physical, cybernetic, data, and mind-set. The tools are also too numerous to discuss in detail—tools as elementary as paperclips and pick-axes can inflict grave damage on very complex and inherently fragile systems. Of gravest concern in considering the tools available to wreak havoc on our national infrastructure is the simple fact that we remain our own worst enemy—we actively open the door to insider abuse, out-sourced code, and naked data. Our technocracy and its culture will continue to impede change. If we are to succeed in the future at our given task of defending the Nation against all enemies, "domestic and foreign", then we must redefine national security and national intelligence to focus on data and knowledge and national intelligence writ small but wide. We must fund, from within the existing budget of the Department of Defense, both the $1 billion a year for electronic security and counterintelligence oriented toward our true center of gravity, the private sector; and we must at the same time ask of the Department of Defense a matching amount, an additional $1 billion a year. This latter amount is needed to fund an extended "Virtual Intelligence Community" which comprises a new "order of battle" able to execute "Information Peacekeeping" operations at home and abroad, in order to deter and resolve conflict at the local, state, national, and regional levels.

124

INTRODUCTION

This is not a technical paper—there are many of those, each delving into the minutia of taking down power, financial, transportation, or general communications systems.[1] Instead, this paper seeks to provide a general overview of target categories and potentially catastrophic outcomes; a review of the range of tools or means by which these targets can be taken down; and a brief discussion of the technocracy and its culture which perpetuates our vulnerability to cybernetic melt-down. All this, however, is but a preamble to a larger discussion of national security and national information strategy.

In particular, the paper explores a redefinition of national security and national power. Our information "order of battle", and in particular, our ability to protect and harness data in the private sector, and our ability to convert and continue to exploit data across human generations, must be recognized as the most critical factor contributing to national security and national competitiveness. The brittleness of our existing complex systems, with multiple embedded points of failure, is the lesser vulnerability. The large vulnerability is at the data and knowledge level. Under these circumstances, "continuity of operations" takes on a whole new meaning, and indeed merits the scale of funding that once characterized the same term during the Cold War. In brief, we need to worry less about deliberate externally-sourced attacks, and much more about inherent embedded cancers of our own making. This paper reviews targets, tools, and technocracy in that larger context.

The following observation is instructive:

> *Robert, as far as vulnerability in the medium term goes, it looks to me like American digital tech is taking itself down via its severe and accelerating self-obsolescence problems. The brittleness, like the underlying tech, is autocatalytic. The Y2K problem is a wholesome first sniff of the carnage to come. No enemy made all the early NASA satellite data now unreadable. We did. It's one of those Pogo moments. This in no way depreciates the external threat, just adds another—temporal—dimension.*[2]

Our Nation is strong, and many rural areas can survive a meltdown, but most urban areas will not degrade gracefully. They will "crash", and in crashing, we will see tolls of dead and wounded greater than we suffered during the Viet-Nam war. We have to ask ourselves: are the right people in charge of national security? do we really understand the threat? do we have what it takes to change?

REDEFINING NATIONAL SECURITY

As we consider the targets and the tools which can be used to effect a "takedown of America, we must do so in the context of a refreshed understanding of what constitutes "national security". The figure below is helpful.

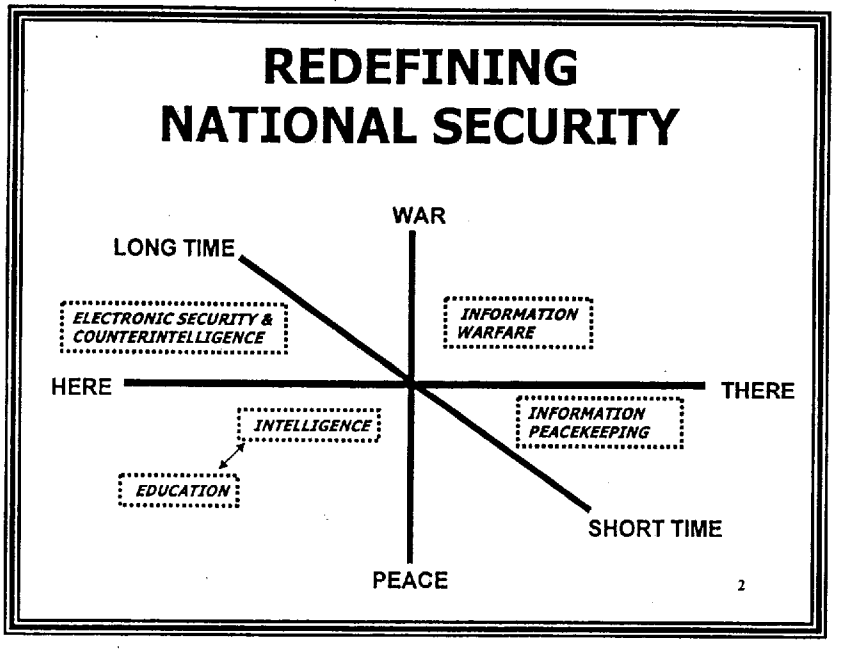

Figure 1: Redefining National Security[3]

This paper will not focus on the Information Warfare or Information Peacekeeping elements illustrated here.[4] Instead, this paper will focus on the fact that the President's Commission on Critical Infrastructure Protection Report of October 1997, while successful in beltway terms, did not provide the kind of credible and comprehensive threat and vulnerability assessment, the list of specific problems, statistics, and detailed case studies, and a coherent plan for constructive change.[5] As Winn Schwartau has put it, we had the wrong people asking the wrong questions, and now we have the wrong people in charge of securing our home front...and with no real authority or money to spend.[6] Also in the classified arena, the same has been said of the National Intelligence Estimate (NIE) on the subject of U.S. vulnerabilities to information warfare attacks—with the passing comment having also been made that the author of that NIE did not know who to talk to outside of a few beltway bandits.[7] In Virginia, a well-conceived plan by a Navy Admiral, to sharpen his information warfare capabilities by conducting a vulnerability assessment of all systems in the State of

126

Virginia, was set aside for fear of public reactions. The bottom line: we still don't know how vulnerable we are, and we have no idea how to go about the long-term process of creating self-healing systems rather than—as Stewart Brand aptly labels them—"self-obsoleting systems".

The "pyramid of vulnerability" for developed nations, and most especially for the United States of America—which owns, uses, and is severely dependent on the bulk of the communications and computing resources of the world—is illustrated below.

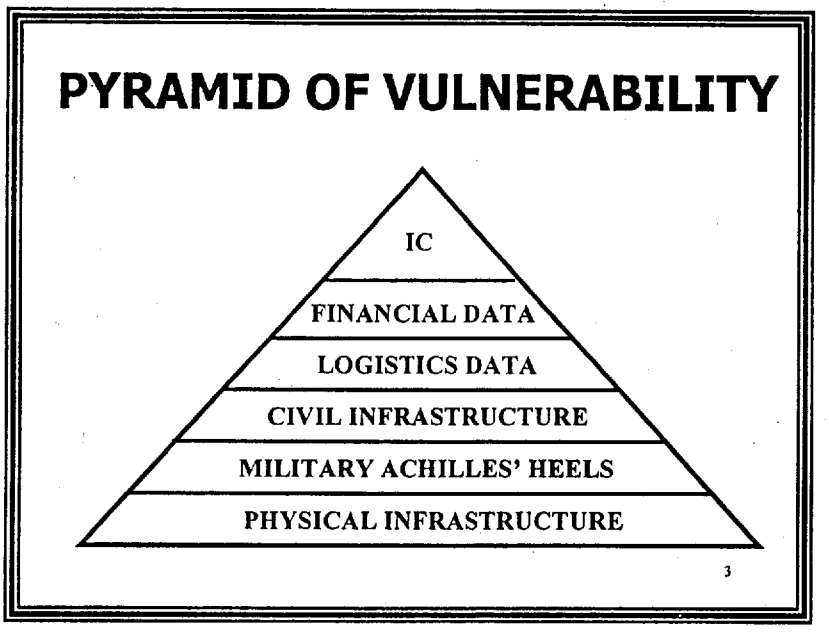

Figure 2: Pyramid of Vulnerability

This pyramid of vulnerability seeks to distinguish between four distinct "kinds" of vulnerability:

1. The vulnerability of major physical infrastructure elements, such as:
   - Bridges, Levees, and Dams—such as the 2800 readily mapped for the public of which 200 of so are of strategic consequence in isolation[8]
   - Canals—such as the Panama Canal, with very vulnerable locks
   - Pipelines—such as the Alaska Pipeline
   - Critical railway switching points

2. The vulnerability of obvious military Achilles' heels, as well as obvious civilian infrastructure, such as:
   - AWACS and Aerial Tankers (anti-tank missiles, or plastique on landing gear—tend to be concentrated in one place)
   - Submarine communications antennas (e.g. Annapolis golf course)
   - Charleston channel (major sealift departure area)
   - Civilian power and communications nodes supporting command centers and key facilities (Falcon AFB Study, Kansas City payroll)
   - Major power grid nodes (both transfer and generation)
   - Major telecommunications nodes, including microwave towers

3. The vulnerability of core data streams vital to national security and national competitiveness, such as:
   - Historical environmental and other critical planning data
   - Civilian fuel stock data
   - Military logistics stock data
   - Transportation status data (induce rail crashes, cripple airports)
   - Financial accounts data (incapacitate procurement, induce panic, impose costs of alternative accounting)
   - Financial transfers data (corrupt transfers, place international and regional transfers into grid-lock, induce panic)

4. The vulnerability of our Intelligence Community (IC) to both external attacks against its systems as well as its perceptions, and internally-perpetuated misperceptions and gaps in understanding, such as:
   - Attacks against down-links (Area 58, NSA, CIA, Suitland, Bolling)
   - Attacks against Joint Intelligence Centers
   - Internal lack of global geo-spacial data
   - Internal lack of integrated analysis model
   - Internal lack of foreign language and foreign area expertise
   - Internal lack of access to international experts and open sources

In summary, this rough depiction seeks to drive home the point that a "takedown" of America is not simply a matter of electronic attacks against electronic systems, but rather a much more comprehensive range and scale of vulnerability which encompasses everything from key geo-physical nodes to our intelligence mind-sets, and which can be attacked with a range of tools that includes: pick-axes and chain saws against selected cables; anti-tank missiles

against AWACS and aerial refuelers and satellite dishes; eighteen-wheeler trucks with and without explosives against specific transformers or other key nodes; electrical attacks, and finally—the area least considered today, data and mind-set attacks and self-generated vulnerabilities.

"Top Ten" lists cannot possibly capture the full extent of the Nation's vulnerability, but they are a helpful means of highlighting the diversity and the imminence of our vulnerability. They can help accelerate constructive change.

TAKEDOWN: TARGETS & TOOLS

John Perry Barlow, lyricist for the Grateful Dead and co-founder of the Electronic Frontier Foundation, once said that "the Internet interprets censorship as an outage, and routes around it."[9] Exactly the same can be said for any strategy that seeks to "harden" or protect specific nodes. It simply will not be effective.

We are at a point in time where, as Steward Brand has noted, the Year 200o problem is but "a wholesome first sniff of the carnage to come". Our system of systems is internally vulnerable from the first line of code on up, and externally vulnerable at every single switching point that relies on either software or electronic transfer. The figure that follows illustrates this larger discussion.

Figure 3: Targets & Tools for Taking Down America

Let us take each of these in turn. On the left we have a column of possible targets, ranging from the process-oriented (secret decisions), down through data links and data stocks, into computers and power stations, and finally to larger physical infrastructure features which can be attacked by physical and electronic means. On the right we have a column of attack categories ranging from the mundane hand-held instrument, passing through foreign code embedded in major U.S. system, and culminating in the inherent weaknesses of our national electronic engineering training and our existing decision mind-sets.

Representative Targets

1. Bridges, Levees & Dams. In the United States, the Mississippi and Missouri Rivers, natural wonders in their own right, are also natural obstacles of monumental proportions. There are exactly six mainstream railway bridges across these great rivers, across the vast majority of the grains must go from the plains to the East Coast cities, and the vast majority of the goods must in return from the Northeast and the South. As the natural flooding in 1993 demonstrated, [10] when these bridges are closed, whether by accident or intent, there are severe repercussions for trade, and especially for the stockage of food and fuel. Recent breaks in levees in the south have demonstrated our vulnerability to the assumption that man can contain nature without regard to human attack. This bears emphasis: all insurance and risk calculations today assume natural causes of disaster. There are no calculations for risk and damage associated with deliberate human attack of any normal civil structure. Dams, in contrast, present computer controlled physical infrastructures which can be taken over to either release flood waters, or to avoid the release of flood waters with the intent of weakening if not destroying the dam.

2. Alaska Pipeline. This pipeline, going across vast stretches of unoccupied territory, carries ten per cent of the domestic oil for the U.S.[11]

3. Cincinnati Rail Yards. As of three years ago, and very likely still today, the entire East-West railway architecture depended on exactly one major turnstile for redirecting railcars. It is located in the Three Rivers area, and represents a significant vulnerability.[12]

4. Culpepper Switch. A popular target, this simply represents the kind of critical communications node (voice and data, especially financial and logistics data) which can be attacked in both physical and electronic ways. The Internet has various equivalent nodes, two of which merit special attention—MAYEAST and MAYWEST. Taking out MAYEAST disconnects the U.S. government

from the rest of the Internet world, and not incidentally does terrible things to all of the Wall Street capitalists who are "tunneling" their Intranets across the larger Internet.

5. Power Generators. Power generators and the grids they support can be browned out, burned out, and confused. Altering the computer readings can cause them to draw more power than they can handle, or less power than they need. Burning out the generators or melting core lines creates the interesting challenge of replacement in the absence of mainstream power. There are exactly eighteen main power transformers that tie together the entire U.S. grid, and we have only one—perhaps two—generators in storage. Interestingly, all of these come from Germany, where there is a six to eighteen month waiting period for filling orders—assuming the Germany generators have not been burned out at the same time by someone attacking the Western powers in a transatlantic cyber-war.[13]

6. Data Computers. Any computer holding large quantities of critical data, especially parts inventories and data associated with either the transfer of funds or the operational effectiveness of critical equipment, is vulnerable to data distortion—this is a far more insidious and dangerous problem than the more obvious denial and destruction attacks.

7. Fuel Stock Data. Fuel stock data is isolated because of its implications in terms of overloading large tanks, with the fire storm hazards of large spillage, or of failing to channel fuels because of false readings.

8. Federal Reserve. Until a couple of years ago there were twelve regional computing centers, one for each of the Federal Reserve regions. Then we went to a single national system which a single hot back-up computing system, and an additional cold back-up alternative.

9. IC Downlinks. Past surveys have focused on buildings, but the more capable attackers will focus on downlinks. All of the main satellite downlinks—for NSA, CIA, Area 58, key other government departments, are out in public sight and reachable with a hand-held anti-tank missile fired from outside the fence line.

10. Human Decisions. "We have met the enemy, and he is us." This often quoted line from Pogo is complemented by another observation, this one anonymous, to wit, "a Nation's best defense is an educated citizenry". This "target" is listed to bring out both a vulnerability and an opportunity for "hardening" our

national defense. Just as "commander's intent" is used in planning for complex operations where communications may be lost, it is essential that there be a larger national decision-making architecture in which there are few secrets and the public is fully engaged. In this way, when disasters do happen and many communications channels do break down, the public will be less likely to panic and more likely to use common sense and good will to see the crisis through. A thorough public understanding of our vulnerabilities and our plans for dealing with those vulnerabilities is essential to our progress. This "target" is also intended to make the point that the weakest link in all systems is not the system itself, but the humans associated with the system.

Representative Tools

1. Pick-Axes & Back-Hoes. Paperclips have burned out strategic warning computers. Pick-axes can cut critical cables in strange places that are difficult to discover. Back-hoes easily take out cables—perhaps the most famous, popularized by Winn Schwartau, is the back-hoe which took out Newark Airport's primary communications and air traffic control and also—right there running alongside it, the "redundant" cable intended to serve as a back-up for the primary cable. Across America, at every cable crossing, we post large signs saying in essence "Cut Here".

2. Eighteen Wheelers. Eighteen wheelers, whether or not loaded with explosives, area useful intellectual construct. Any critical node should be subject to the eighteen-wheeler test—what will happen if an eighteen-wheeler crashes through at full weight and speed at any one of various points; or alternatively, what will happen if an eighteen-wheeler "melts down" at a specific point and needs to be taken apart or lifted out piece by piece?

3. Random Viruses. The recent spate of NT melt-downs are simply another step down the path started by the Robert Morris virus a decade ago. This situation needs to be taken very seriously because many of the viruses are encased in shrink-wrapped hardware and software coming directly from the production facilities.[14] Until software is self-healing (and code is encrypted at levels above what is presently available), this will continue to be a serious vulnerability. All of the following problem tool areas will exacerbate this situation.

4. Info-Marauders. As has been noted by one prominent wag in this area, "hacker tools are now in the hands of idiots and criminals".[15] A single individual, empowered by hacking software freely available on the Internet, is

now able to cause the kind of damage to corporate and national systems which was previously only in the province of Great Nations. Disgruntled, dishonest, crazy, and zealot individuals and gangs are now is a position to damage data, deny access, and extort funds from hapless system owners who did not realize that they were buying into a "naked Emperor" environment.

5. Angry Insiders. The losses to external penetrations and externally sourced viruses is much over-rated. As Dr. Mich Kabay, Director of Education for the International Computer Security Association (ICSA) has noted in his seminal work on computer losses,[16] the largest losses after fire & water/errors & omissions come from *insiders*—dishonest or paid insiders (roughly 10%) and angry insiders seeking revenge (roughly 9%). These are people with authorized access who are able to do unauthorized things that are not detected because the systems are all designs under the assumption that insiders can be controlled through a few simple (and often very poorly administered) control measures.

6. Paid Insiders. Paid insiders can be simply dishonest employees who seek to exploit access for financial gain, or insiders who have been recruited by outsiders for a price. There are also former insiders who return to their place of employment (e.g. selected Wall Street firms with marginal physical access controls and worse computer access controls) to take internal actions which are not authorized and for which authorized access has expired administratively but not technically.

7. Calcutta Code. Also Moscow code....this refers to computer code written by the legions of off-shore coding houses. Computer code in the U.S. is notorious for its lack of documentation, with the result that older systems tend to have millions and millions of lines of code that are completely incomprehensible to the most skilled examiner, and replete with patches from a variety of sources, all also undocumented. As the Year 2000 problem takes on greater urgency, many organizations are being forced to provide intimate access to their code for legions of external programmers, generally without any assurance at all as to their criminal and psychological history, and also without any ability to audit their access or their code.[17]

8. Existing EE Skills. Our electrical engineering education is abysmal, despite the wealth of opportunity in the field and the shortage of skilled professionals. For reasons that escape the author, the electrical engineering discipline decided to completely ignore electronic security and counterintelligence issues after the demise of the mainframe (and even those standards were mediocre),

and entire complex systems have been built from the ground up without any embedded security at all. In fact, some systems require or choose to turn off those rare security features provided in some software and hardware. Until national legislation establishes "due diligence" standards for managers responsible for the protection of intellectual property, and for communications and computing product and service providers, this severe and pervasive vulnerability will prevent any substantial success in hardening individual targets or constraining the utility of other attack tools.

9. Existing Mind-Sets. Winn Schwartau, author of *INFORMATION WARFARE: Chaos on the Electronic Superhighway*[18] deserves full credit for bringing this situation before the public. Without his efforts, including his many keynote speeches across the Nation, and his personal engagement in sponsoring a highly provocative series of InfoWarCon meetings, it is highly unlikely that the President's Commission on Critical Infrastructure Protection would have been created. Its report has many flaws and oversights, to include a lack of understanding of the very valid and useful perspectives of international authorities as well as the hacker underground, but it is a good start and we are in agreement on one important fact: $1 billion a year is needed to create a survivable electronic environment. This is the number the author proposed in 1994 in testimony to the National Information Infrastructure working group taking testimony on security.[19] Unfortunately, the U.S. government continues to drag its feet in assuming its proper role as a provider of "order & protection" services in cyberspace, and this has been cited by many in the private sector as the reason they continue to ignore computer security issues.[20]

TECHNOCRACY

This brings us to the technocracy. The chart below is a very authoritative depiction of just what are the sources of damage to computer systems and data. Although the originator, Dr. Mich Kabay likes to use the words "rough guesses" with this chart, he is an internationally respected individual with enormous access to restricted data. This one chart is as authoritative as any major study anywhere, and should be carefully considered in that light.

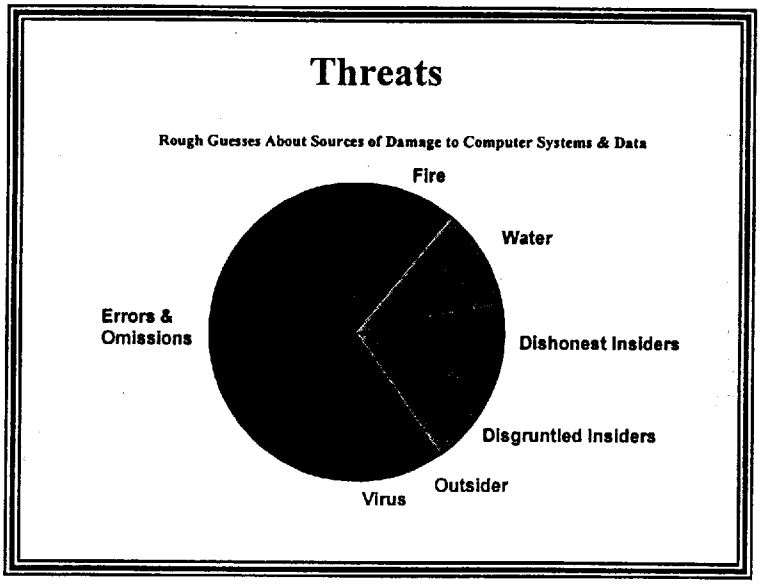

Figure 4: The Facts, Just The Facts

The bottom line here is that fully seventy percent of our losses can be attributed to very poor design—poor data entry and data management programs which induce major errors & omissions (and cannot audit or flag possible errors & omissions in passing) and poor system design and system back-up practices which permit fire and water to wreak irreversible damage to important data. Only the last thirty percent have anything to do with humans. *Insiders* do roughly twenty percent of the damages. Roughly five percent of the remaining damages are done by outsiders, and a final five percent by viruses from various sources.

In the immortal words of Robert Stratton, one of the most capable of international hackers (and one of the few never to be indicted or considered for indictment),

> *If houses were built like computers, the first woodpecker to come along would bring down civilization.*[21]

The technocracy—the culture of technocracy—is the major impediment to change today, and we have to come to grips with the fact that all the money in the world is not going to heal our rapidly atrophying system of systems unless we first come to grips with the intellectual cancer that permeates this element of our

society which is at once so very important, but also so very dangerous. *We have seen the enemy, and he is us.*

Among the sins of the technocracy are the following:

1. Blind faith in technology
2. Not legally liable for failure (by permission of Congress)
3. No requirement for inherent security at the code and data level
4. No requirement for data integrity and survivability
5. Marginal adherence to existing back-up and access control standards
6. Elitist (largely ignorant) attitude about cryptography and privacy
7. History of ignoring detailed warnings
8. Recent record of lip service and tail chasing

The point of this section is that both the people and their government must accept responsibility for designing and protecting the future system of systems upon which every aspect of national security and national competitiveness must depend. It is we as individuals, willing to accept self-obsoleting technology with built in hazards to our data, who have permitted this gross external diseconomy to persist, and it is we the people—not the profit-taking beltway bandit creators of these systems—who will ultimately pay the final price for failure: individual poverty, scattered catastrophe, and national weakness.

The President's Commission on Critical Infrastructure Protection (PCCIP) was at once a small sign of hope and a large symbol of despair. Apart from the fact that it did not talk to any of the serious professionals outside the beltway, and even more so, outside the Nation, who actually know in detail the vulnerabilities and solutions the Commission was supposed to address; the Commission also neglected to provide the public and the private sector with an authoritative unclassified work that addresses the critical issues of data integrity, data privacy, and the use of unencumbered encryption in order to secure electronic commerce. No doubt the Commission marched to its secret drummer and gave its masters exactly what they *wanted*—unfortunately, it did not give the Nation what it *needed*, and we are left—as we were left in the aftermath of the Report of the Commission on the Roles and Capabilities of the United States Intelligence Community—with no clear-cut direction, no one clearly in charge, and no basis for which to mobilize the private sector into its new and urgent role as the first

line of national defense against cyber-attack and self-destructive electronic systems.

CIVIL CENTER OF GRAVITY

Apart from the failings of the technocracy, there is another element that makes it difficult for America to secure her computing foundation from attack, and that is the fact that the vast bulk of the critical data and the critical electronic pathways and storage facilities, are all in the civil sector—in the private sector. It is literally not possible for the government to control and protect the most vital targets in traditional ways, nor is it even possible for the government to regulate this arena in detail. This is why the PCCIP—for all of its good intentions—must be regarded as a distraction if not a failure. It did not address the threat or the solution in terms that could be executed by the ultimate responsible party, the private sector and the public.

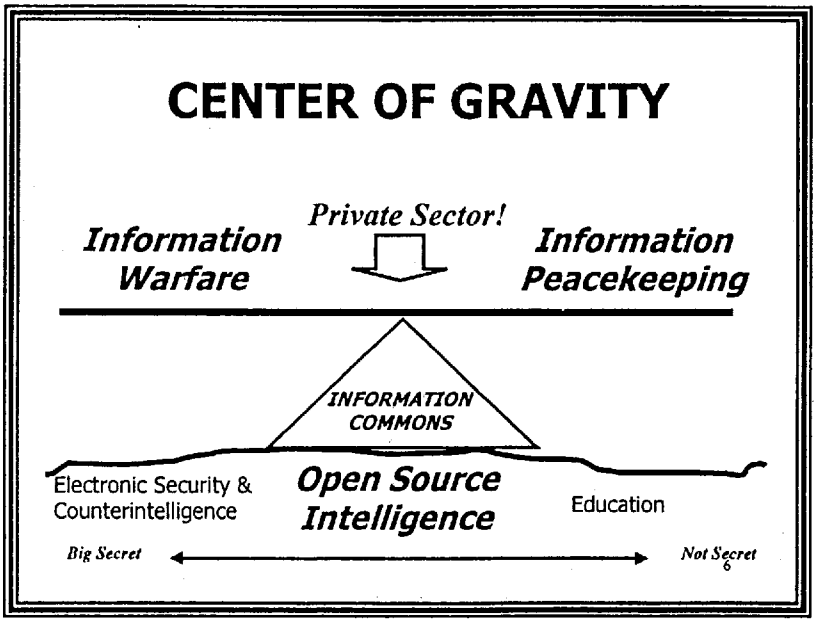

Figure 5: Civil Sector Center of Gravity

Every aspect of Information Operations—from offensive information warfare to proactive Information Peacekeeping[22]; from electronic security & counterintelligence to protect intellectual property on the home front, to education as the foundation for a truly "national" intelligence community, the "center of gravity" is solidly within the "information commons" defined and dominated by

the private sector. The Department of Defense cannot defend this critical terrain—nor should it—using traditional methods.

In contemplating the "takedown" of America, and in considering a few representative targets and tools as well as the technocracy that spawned our pervasive national vulnerability to information apocalypse, we are forced to acknowledge the fact that America has passed from one world to the next—from the physical world to the virtual world—and this requires that America's concepts of national defense, and America's concepts for government operations, all be subject to sharp and relatively urgent redefinition.

VIRTUAL INTELLIGENCE AND INFORMATION PEACKEEPING

The author has published extensively on these two original topics,[23] but for this "primer" a few points are worth highlighting:

1. Roughly eighty percent of what we need to know to defend the nation is in the private sector, "out of control" Roughly ninety-five percent of what we need to know to assure national competitiveness is in the private sector, "out of control".

2. The greatest obstacle our government faces today in assuring national security and national competitiveness—the cause of causes for conflict and economic loss—is the growing gap between those with power and those with knowledge.

3. Our concept of "Information Operations" must—absolutely must—come to grips with this reality. Information Warfare and Electronic Security & Counterintelligence are anemic if not counterproductive endeavors if they are executing in isolation from this larger construct.

4. In order to be effective in the 21st Century, especially during the first half of the century when we continue to live in the largest of the glass houses and our enemies—be they individuals, gangs, corporations, or states—have the most rocks, we must adopt three concepts as fundamental to our national security:

    a. "National Intelligence" must evolve rapidly to become the core of a larger "virtual intelligence community" in which

we are able to fully harness and exploit private sector data from multi-lingual sources.

b. "Electronic Security & Counterintelligence" must become pervasive, and this is only possible if we release the private sector from artificial constraints on encryption, and if we return to our democratic foundation, the respect for personal privacy. We cannot regulate this, we can only nurture this fundamental national security arena.

c. "Information Peacekeeping" must become our first line of defense in dealing with enemies both domestic and foreign. This will require new concepts and doctrines, a completely new order of battle, new relations between elements of the government and between the government and the private sector, and—most importantly—a completely new attitude about how to deal with problems and threats.

5. All of the above—the full integration of a national electronic security & counterintelligence capability which protects and harnesses down to the data and code level, requires a National Information Strategy and a reconstruction of the administrative, legal, financial, and operational relationships between civilian, military , and law enforcement elements of government, and between government and the private sector. Once we have our own act together, then we can contemplate setting standards and requesting collaboration in kind from other states.

CONCLUSION

We are at war today. It is a total war, yet we have failed to mobilize the Nation and we have therefore left ourselves without sanctuary, without a defendable rear area, and without any plan for recovering from the catastrophic consequences that can be brought about so very easily by individuals, gangs, or other nations who choose to hurt us where we are least able to detect, block, or retaliate.

Everything we are doing today, from the PCCIP to the Information Operations activity at Fort Meade, to the billions of dollars being spent on the current and planned force structure, is out of touch with the reality that pioneers—Alvin Toffler, Martin Libicki, Winn Schwartau—have been trying to articulate.

It is out of touch with the reality that Eric Bloodaxe, Emmanuel, Phiber Optic, Dark Angel, Andy Mueller-Maguhn and many, many others have been actively demonstrating.

It is out of touch with the efforts of Marc Rotenberg, David Banisar, and many others associated with responsible computing. Sadly, it is also out of touch with the American people and with the larger global community that actively seeks open intellectual engagement with responsible electronic security.

Today, the United States of America is again an unbalanced giant, again a paper tiger, again at the mercy of forces it does not understand and is not willing to engage in unconventional ways. *We have seen the enemy, and he is us.*

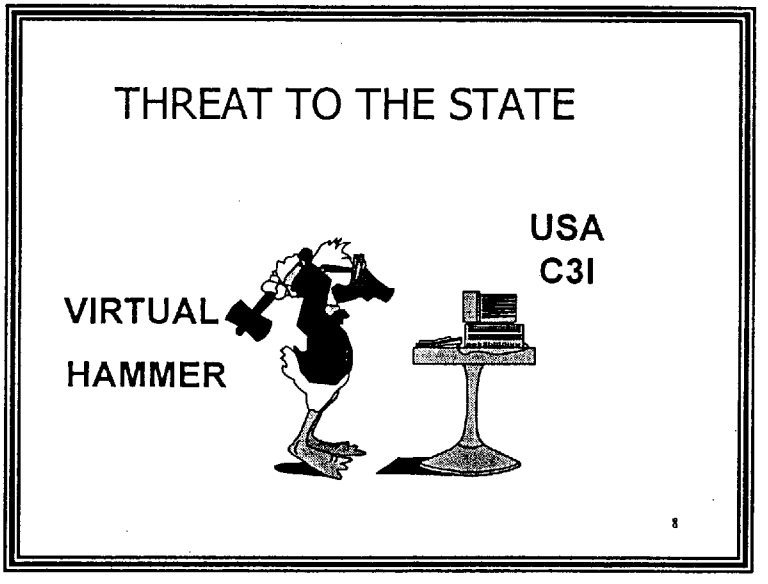

Figure 6: We have seen the enemy, and he is us.

There is, however, good news. The price tag for all of this is authoritatively estimated at $2 billion a year (half for electronic security & counterintelligence, half for creating the virtual intelligence community able to execute information peacekeeping operations)[24]. This is a price that DoD can easily afford to pay, and a price that—if paid by DoD—will permit us to reinvent the concept of national defense, deter cyber-war, and surprise friends and enemies alike with our ability to adapt to the chaotic environment we have ourselves created. *DoD can solve this problem, but only if it pays up, and lets go.*

Endnotes

[1] Although other papers have been written since then, the three "originals" in the author's view are Major Gerald R. Hust, "Taking Down Telecommunications", School of Advanced Airpower Studies, 1993); Major Thomas E. Griffith, Jr., "Strategic Attack of National Electrical Systems", School of Advanced Airpower Studies, 1994; and H. D. Arnold, J. Hukill, and A. Cameron of the Department of the Air Force, "Targeting Financial Systems as Centers of Gravity: 'Low Intensity' to 'No Intensity' Conflict", in *Defense Analysis* (Volume 10 Number 2, pages 181-208), 1994. The authors first major statement in this area, after several years of involvement, was "The Military Perspective on Information Warfare: Apocalypse Now", keynote speech to the Second International Conference on Information Warfare: Chaos on the Electronic Superhighway (Montreal, 19 January 1995). There have been many fine conferences on the subject of information warfare, both within the military and in the private sector. http://www.infowar.com offers a great deal of useful material, as do selected thesis from the Naval Postgraduate School and other military institutions. The *Proceedings* of the InfoWarCon series (the author was a founding partner but left the partnership in 1996) appear to be in a class by themselves and can still be obtained from the International Computer Security Association. The author's first call for $1 billion a year for electronic security was published as a U.S. Newswire press release dated 11 August 1994. Two other papers deserve mention up front: Maj Roger Thrasher, *Information Warfare: Implications for Forging the Tools* (Naval Postgraduate School, June 1996), copy available via email to the author at "Major Roger D. Thrasher, AFRL/IFSA" <thrasher@rl.af.mil>; and—dealing with the tough issues of what constitutes an attack and what the legal authorities are for retaliation, and what constitutes proper retaliation—Cdr James N. Bond, *Peacetime Foreign Data Manipulation as One Aspect of Offensive Information Warfare: Questions of Legality Under the United Nations Charter Article 2(4)* (Naval War College, 14 June 1996).

[2] Stewart Brand, a distinguished member of the Global Business Network, was the founder of both the *CoEvolution Quarterly* and the *Whole Earth Review* as well as the original organizer of the Lake Tahoe Hacker's Conference, of which the author is an invited honorary member. Among his books *are How Buildings Learn : What Happens After They're Built* (1995), and *The Media Lab : Inventing the Future at MIT* (1988).

[3] Mr. John Peterson, President of the Arlington Institute and a noted futurist, devised the original two-dimensional matrix (war-peace, here-there) to make the point that we train, equip, and organize our defense forces for "war, there" when in fact the bulk of the modern threat is "here, home". The author added the dimension of time to drive home the point that in this day and age of ad hoc coalitions and "off-the-shelf" nuclear and chemical take-out, we must be ready to deal with "no-notice" emergent threats on a "come as you are" basis.

[4] Among the author's contributions are "INFORMATION PEACEKEEPING: The Purest Form of War", chapter in Doug Dearth et al *CYBERWAR 2.0: Myths, Mysteries, and Realities* (AFCEA Press, 1998); "Virtual Intelligence: Conflict Resolution and Conflict Avoidance Through Information Peacekeeping", *Proceedings* of the Virtual Diplomacy Conference of 1-2 April 1997 in Washington, D.C. (U.S. Institute of Peace), full paper at http://www.oss.net/VIRTUAL; "Intelligence and Counterintelligence: Proposed Program for the 21st Century" , OSS White Paper of 14 April 1997 at http://www.oss.net/OSS21; "The Military Perspective on Information Warfare: Apocalypse Now", *Enjeux Atlantiques* (#14, February 1997); "Creating a Smart Nation: Strategy, Policy, Intelligence, and Information", *Government Information Quarterly* (Summer 1996); "Creating a Smart Nation: Information Strategy, Virtual Intelligence, and Information Warfare", in Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden (contributing editors), *CYBERWAR: Security, Strategy, and Conflict in the Information Age* (AFCEA, 1996); "The

Military Perspective on Information Warfare: Apocalypse Now", Keynote Speech, *Proceedings of the Second International Conference on Information Warfare*, 19 January 1995; "Reinventing Intelligence: The Vision and the Strategy", *International Defense & Technologies* (December 1995), bi-lingual in French and English; "Hackers as a National Resource", Keynote Presentation to Hackers on Planet Earth, New York, 13-14 August 1994 (1500 hackers); and "War and Peace in the Age of Information", Superintendent's Guest Lecture, Naval Postgraduate School, 17 August 1993.

[5] Observation made on the C4I List by Perillo@DOCKMASTER.NCSC.MIL, together with a number of other excellent quotations from other documented sources, some cited elsewhere in this paper.

[6] Winn Schwartau, personal communication, 17 March 1998.

[7] The author and his friend and former partner Winn Schwartau, who is the author of *INFORMATION WARFARE: Chaos on the Electronic Superhighway* (Thunders Mouth Press, 1994) between them know most of the major hackers as well as most of the major "straight" electronic security gurus, and in this one instance, what emerged as remarkable was who was not consulted, in most cases because the NIE did not provide for discovery of expertise and interviewing of experts outside the beltway. Unfortunately, the same was true for the President's Commission on Critical Infrastructure Protection.

[8] The Surface Water and Related Land Resources Development Map is designed to portray both the development and preservation aspects of Federal water resources activities, with the main theme being the spatial distribution of dams and reservoirs. Dams are shown that have normal storage capacity of at least 5,000 acre-feet, or a maximum storage capacity of at least 25,000 acre-feet. This includes about 800 dams owned by Federal agencies and about 2,000 dams owned by non-Federal organizations. *FGDC Manual of Federal Geographic Data Products - Surface Water Map* which can be found at www.fgdc.gov/FGDP/Surface_Water_Map.html.

[9] He made this comment in his spontaneous remarks to an audience of 629 intelligence professionals attending the first open source intelligence conference, "National Security & National Competitiveness: Open Source Solutions", 2 December 1992, in Washington, D.C.

[10] During the major floods of 1993 four of the six bridges were closed. Major rail traffic delays and costs were incurred as traffic was routed to the northern and southern bridges still in operation. "Flooding Halts Railroad Traffic Through Major East-West Hub: Freight Lines, Amtrak Rust to Find Detours in North and South", *The Washington Post* (A4, Tuesday, 27 July 1993).

[11] The first "top ten" listing to be seen by the author was created by Peter Black. His article, "Soft Kill: Fighting infrastructure wars in the 21st century", *WIRED Magazine* (July/August 1993), listed the following targets:

1. Culpepper Switch, handling all electronic transfers of federal funds
2. Alaska Pipeline, carrying ten percent of the domestic oil
3. Electronic Switching System (ESS), managing all telephony
4. Internet, the communications backbone of science and industry
5. Time Distribution System, upon which all networked computers depend
6. Panama Canal, major choke point for U.S. trade
7. Worldwide Military Command & Control System (WWMCCS)
8. Big Blue Cube, Pacific clearinghouse for satellite reconnaissance
9. Malaccan Straits (Singapore), the maritime link between Europe-Arabia and the Pacific
10. National Photographic Interpretation Center, processing center for imagery

[12] Winn Schwartau, personal communication, 17 March 1998.

[13] *Ibid.* See also *supra* note 1.

[14] In 1992 a major U.S. intelligence community entity, one extremely familiar with computers, briefed the Information Handling Committee with the results of its survey, over the course of one year, into viruses arriving at its loading docks in shrink-wrapped products. The total number found: 500.

[15] The author, keynote speaker at Hackers on Planet Earth (HOPE), an extraordinary event that drew over 1,200 hackers and phone phreakers to a dilapidated New York City hotel 13-14 August 1998. Hackers, as the author has noted with frequency, are *not* the problem, not even the symptom of the problem—they are a national resource in that they are demonstrating, without causing significant damage, just how vulnerable all of our systems are.

[16] Mich E. Kabay, *The NCSA Guide to Enterprise Security: Protecting Information Assets*, McGraw-Hill (New York, 1996). ISBN 0-07-033147-2. Chapter 1, Figure 1, page 11. The figure is the book is superceded by this table, provided by Dr. Kabay in personal communications, 12 March 1998. The excellent work can be ordered from ICSA by email to <jmotter@icsa.net>.

[17] A typical assessment of this looming access problem is found in CIWARS Volume 10, Issue, Intelligence Report dated 2 November 1997. <www.iwar.org> contains this and many other interesting reports on electronic vulnerabilities around the world.

[18] *Supra* note 6.

[19] At the time the author surveyed several experts including Professor William Caelli in Australia, and one of the top computer security advisors to the National Security Agency. The author continues to recommend due diligence legislation, a national testing & certification program, a national computer security education program, and a very robust electronic security & counterintelligence program within the Federal Bureau of Investigation and on behalf of the private sector.

[20] In May 1997 an Information Security Industry Survey done by Delotte & Touche LLP, with 1225 organizations surveyed, reported that 40% blamed "unclear responsibilities" and 26-30% (sic) blamed "lack of central authority" as the reasons why they could not come to grips with computer and telecommunications security requirements. As noted in 11 February 1998 email from <Peerillo@DOCKMASTER.NCSC.MIL>.

[21] Statement made at OSS '96, where Mr. Stratton, a very highly regarded computer security engineer, was a speaker together with his partner, Mr. Chris Goggans, another brilliant security consultant.

[22] The author coined the term in 1994. For two papers defining this aspect, see *supra* note 4.

[23] *Supra* note 4.

[24] In 1995 the author proposed the following annual budget for national information security:

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 (in Private Sector)	$30,000,000
05 Establish Basic and Advanced C4 Trusted System Standards	$100,000,000
06 Authorized and Encourage Public Keys and Privacy Measures	$200,000,000
07 Establish a National Information Foundation	$25,000,000
08 Establish a C4 Security Testing & Certification Program	$200,000,000
09 Establish an Electronic Security & Counterintelligence Division (in FBI)	$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 (with Private Sector)	$100,000,000
13 Influence Civilian Information Technology Research (re embedded security)	$100,000,000

As found in concluding section of keynote speech in Montreal, *supra* note 4. In 1997 the author proposed a $1.6 billion a year budget for the national virtual intelligence community, comprised of $250 million for commercial imagery to meet DoD and USG needs; $250 million to meet NATO/Partner for Peace open source intelligence needs, $250 million for U.S. Intelligence Community access to open sources; $50 million for a University of the Republic to bring leaders from various sector together; and $400 million for two related largely classified initiatives. Detailed in "Intelligence and Counterintelligence: Proposed Program for the 21st Century" (OSS White Paper, 14 April 1997), at <http://www.oss.net/OSS21>.

PROCEEDINGS 1998 7th International Conference & Exhibit OPEN SOURCE SOLUTIONS: Global Intelligence Forum - Link Page

Previous	OSS '98 Robert David Steele, TAKEDOWN: The Asymmetric Threat to the Nation,
Next	OSS '98 Dr. Douglas Dearth, Defense Intelligence Agency, Government and the Information Marketplace,

Return to Electronic Index Page