# TAKEDOWN: TARGETS, TOOLS, AND TECHNOCRACY

Robert D. Steele

## 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.

"TAKEDOWN: Targets, Tools, and Technocracy," in Lloyd J. Matthews (ed.), *Challenging the United States Symmetrically and Asymmetrically: Can America be Defeated?* (Strategic Studies Institute, U.S. Army War College, July 1998), pp. 117-141.

## 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 by which these targets can be taken down; and a brief discussion of the technocracy and its culture which perpetuate 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 continue to exploit data across human generations, must be recognized as the most critical factors 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.

Let's begin with the following observation from a knowledgeable observer:

> 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 their crashing we will see tolls of dead and wounded greater than we suffered during the Vietnam 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?

As we consider the targets and tools that 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." In this regard, note Figure 1.[3]

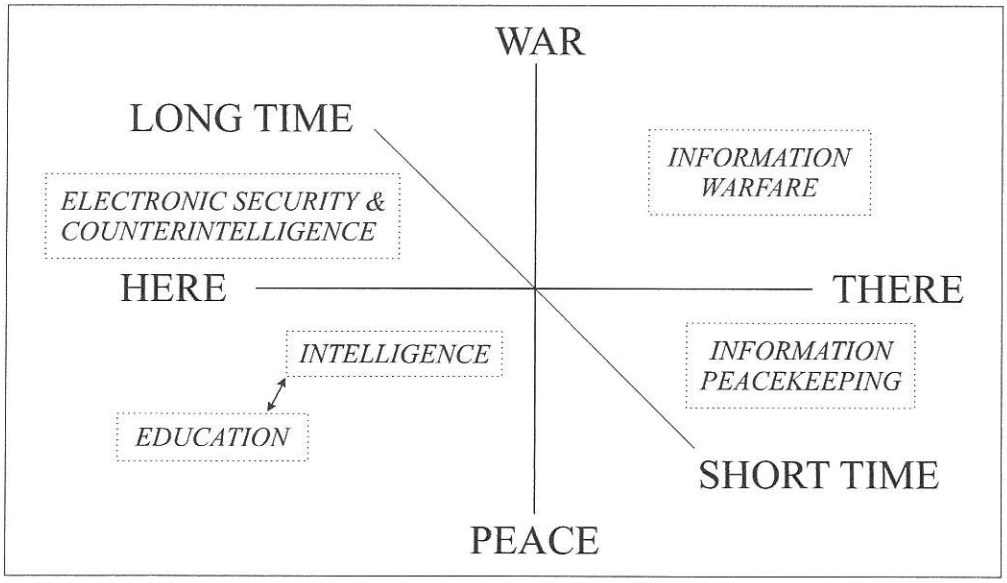


**Figure 1. Redefining National Security.**

This paper will not focus on the Information Warfare or Information Peacekeeping elements illustrated in the figure.[4] Instead, it will focus on the fact that the President's Commission on Critical Infrastructure Protection (PCCIP) report of October 1997, while successful in beltway terms, did not provide a credible and comprehensive threat and vulnerability assessment, a list of specific problems, statistics, and detailed case studies, and a coherent plan for