THE
TERRORISM RESEARCH
CENTER

For more information:
www.terrorism.com
trc@terrorism.com

Matthew G. Devost, Senior Analyst - Security Design International
Brian K. Houghton, Doctoral Fellow - RAND
Neal A. Pollard, Director of Research and Analysis - Hicks and Associates[1]

Organizing for Information Warfare: "The Truth is Out There"

Information Warfare (IW) is envisioned as a new dimension of warfare, bringing conflict into the Information Age. IW offers combatants the ability to execute asymmetrical attacks that have non-linear effects against an adversary. By targeting or exploiting information and information processes, an attacker can use limited resources to reap disproportionate gains. Furthermore, IW offers weaker enemies—even at the sub-state level—strategies alternative to attrition, an attractive feature especially when facing an opponent with significantly stronger conventional forces. Such potential adversaries could perpetrate an IW attack against the United States, using relatively limited resources, exploiting the US reliance on information systems. Targets of such attacks might include Command and Control (C2) networks, satellite systems, and even the power grids of the continental United States. Such an attack could potentially have a strategic impact on the national security of the United States.

In contrast, terrorism has been used by states and sub-state groups for millennia. As an instrument to pursue political or social objectives where the user lacks the strength or the political wherewithal to use conventional military means, terrorism has been especially attractive. The intended target of a terrorist act goes beyond the immediate victims. Terrorists create a climate of fear by exploiting the information dissemination channels of its target population, reaching many by physically affecting only a few. We experienced a tragic example of this effect in the 1983 bombing of the US Marine barracks in Beirut , where a small group, clearly weaker than the US military, nevertheless executed an effective strategic attack against the US.

In a recent IW wargame held at National Defense University, the game director stated the "problem" of Information Warfare was not lack of capabilities, but of management and organization: the capabilities are out there already, they just are not being tapped. This "problem" has only recently emerged as a potentially new warfare area for most defense planners. The problem of terrorism, on the other hand, has been in the headlines and in our social consciousness for decades, especially since the technological advance of intercontinental flight. This paper

[1] The author's names are listed alphabetically to reflect that the research was conducted and implemented through a team effort with equal contributions. The opinions and conclusions contained herein are those of the authors, and do not reflect policy, institutional opinion, or proprietary information of their employers.

examines these two phenomena conceptually, operationally and organizationally, seeking commonalties. If comparisons are substantiated as more than circumstantial, then we intend to examine the lessons which might be applied to IW defense[2] from successes and failures of thirty years of countering terrorism. Within the context of these comparisons, we will also attempt to ascertain whether there is an emergent structure or organization that suggests a "correct" approach to IW defense.

Commonalties

Overview

In discussing the "philosophy of the [terrorist] bomb," Walter Laqueur referred to terrorism as "propaganda by deed," which was "a powerful weapon to awaken the consciousness of people."[3] Wardlaw states that the "primary effect [of terrorism] is to create fear and alarm," thus targeting the minds of the populace.[4] In his essay "Information Warfare," George Stein states "Information Warfare, in its essence, it about *ideas and epistemology*…Information Warfare is about the way humans think…. The target of Information Warfare, then, is the human mind…."[5]

These broad parallels aside, there is a number of general themes that emerged from a recent book of essays on IW.[6] These themes are interesting when considered in the context of terrorism. In the chapter titled "Epilogue," the editors identify common topics which run throughout the essays in the book. The topics include recurring themes ("paradigm shift," "the need for policy," "the role of intelligence," "levels of war," "civil-military divisions"), principal domains ("political/cultural/social," "legal/ethical"), and key issues ("expectations," "public diplomacy," "global information," "crime/rules of evidence," "nature of war, conflict, and force," "asymmetrical war: hierarchy and intensity," "laws of war and rules of engagement") that merit substantial further investigation or change in addressing IW.

A glance at the table of contents in a political violence textbook will show that analysis of the above listed themes recurs consistently in the study of terrorism and low-intensity conflict. Analogies and comparisons can be useful, such as comparing IW defense and counter-terrorism. However, there are limits to relying solely on this analogy for analysis. For the purposes of this article, the authors will focus on comparisons from counter-terrorism that have implications for organizing and operating in the new environment of Information Warfare. Although the

[2] For the purposes of this paper, the authors accept the construct offered by Michael L. Brown ("The Revolution in Military Affairs: The Information Dimension," *Cyberwar: Security, Strategy and Conflict in the Information Age* Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden, eds. Fairfax, VA: AFCEA International Press, 1996 (pp.32-52). In his construct, Brown identifies three dimensions of IW: Type I (perception management), Type II (information denial, destruction, degradation, or distortion), and Type III (intelligence gathering through exploitation of enemy information systems). This paper primarily addresses IW Type II (which has also been called information infrastructure warfare), and to a lesser but obvious extent, Type III. However, perception management also could provide some parallels.

[3] Walter Laqueur, *Age of Terrorism*. Boston: Little, Brown & Co., 1987 (p.48).

[4] Grant Wardlaw, *Political Terrorism*, Second Edition. Cambridge: Cambridge University Press, 1989 (p.41-42).

[5] George Stein, "Information Warfare," *Cyberwar* (op.cit.), p.176.

[6] *Cyberwar* (op.cit.).

organizational problems and solutions of IW defense and counter-terrorism might be similar, solutions to other general issues of IW and terrorism may not be.

It seems then that there are at least four general areas of commonality between IW and terrorism that suggest an approach to organizing for IW defense. These areas are:

1) Force Multiplication
2) Disproportionate Effects
3) Intelligence, Indications and Warning
4) Interagency Response.

Force multiplication

A terrorist group uses violence to pursue a political objective it cannot (or does not wish to) pursue within the "conventional" constraints of the system, using cheap weaponry whose effects are magnified by fear. The terrorist might be a sub-state group which otherwise lacks the political or physical power to effect their goals. On the other hand, a state can use or sponsor terrorism to pursue goals it cannot achieve through the normal peaceful competition among states or through conventional military doctrine. In this respect, terrorism is a force multiplier, giving weaker groups the muscle to pursue their objectives, and giving states alternatives to military action.

By comparison, Information Warfare seeks to take advantage of an adversary's reliance on information, information systems, and critical infrastructures integrated with information systems. By exploiting this reliance, an attacker might use limited resources to effect disproportionate results. Information Warfare allows a state to pursue military and political objectives, without crossing international borders, and without marshaling conventional forces which normally might be necessary to achieve a similar result. IW also offers the user anonymity or plausible deniability. Similarly, a sub-state group may exploit a target's reliance on information to achieve the group's goals by giving it an advantage beyond "troop strength." "Information Warfare is relatively cheap to wage, offering a high return on investment for resource-poor adversaries. The technology required to mount [IW] attacks is relatively simple and ubiquitous"[7] —as were the ingredients used in the Oklahoma City bombing. Access to such technology allows individuals who might be merely on the FBI's "Most Wanted" list to be a real threat to the military. Such a person would be the concern of both the Departments of Justice *and* Defense.

Disproportionate Effects

As force multipliers, terrorism and IW increase the "combat potential" of their perpetrators because of the non-linearity of their effects. This non-linearity is generated by virtue of the complexity and connectivity of the targets—whether the targets are populations or networks, both are similar in design and processes of information transfer, and the effects of the attack compound and spread as a result of this connectivity and complexity. This insures that an attack will crosscut several areas of the target population. This crosscut will bring the attack within the responsibility of several elements of national security and law enforcement.

[7] "Report of the Defense Science Board (DSB) Task Force on Information Warfare - Defense," Office of the Under Secretary of Defense for Acquisition and Technology, Washington, D.C. November 1996, page ES-1

In terrorism, there is an intended target broader than those immediate victims of the attack. The terrorists seek to propagate their message by attacking a relatively few individuals. The non-linearity which terrorism seeks to leverage is generated by the ensuing fear and media exposure across the entirety of a target population. A common end goal of terrorist campaigns is for the broader audience to respond to fear by pressuring the government into acceding to the terrorists. If successful, this would mean that the terrorists have imposed their will upon the government using an attack of disproportionate effects from limited resources: an imposition that could not have been accomplished by conventional military means. The effects of the attack spread non-linearly, compounded by the complexity of human communication structures of the target population. Tactically, this might mean attacking various sensitive spots of a society that would yield "strategic" effects (including infrastructure, military/government or population-rich targets). Responsibility for protecting and mitigating threats to these targets cuts across several areas of responsibility, from the local to Federal level.

IW could attack a specific system (e.g. network, infrastructure, belief, etc.) or component of a larger system. Through the attack on one component, the attack might affect a system as a whole—a system over which the government might have only limited control. The disproportionate effects of a terrorist attack are generated by fear, publicity, and the media—a system interminably complex in its connectivity. The non-linearity which IW seeks to leverage is the complex connectivity of information systems. Most of the targeted information infrastructures—even those interacting with government—will be in the commercial sector. Responsibility for defending against IW attacks could vary, depending on the attack. In one case, it might be the government customer using the system. In another case, it might be a Federal agency charged with its protection might be responsible, or a new government entity might be in the best position to detect and respond to the attack and mitigate its effects. A new organizational approach might be necessary to resolve the various responsibilities if a response to an IW attack is to be effective and timely.

Intelligence, Indications and Warning

Force movements, arms build-ups, and changes in readiness levels are examples of information traditionally used for indications and warnings (I&W) of potential military attack. These do not translate easily into I&W of terrorist attacks. Unconventional sources and methods might be necessary to acquire terrorist I&W. When terrorists operate and disperse within the cities of societies they target, "mobilization" can be near instantaneous, without an observable troop movement to alert the adversary's defense structure. I&W sources are therefore necessarily more distributed than normal, and thus fall within areas of responsibility across the law enforcement, military, and intelligence communities.

In the information battlespace, attacks can move at light speed and without any warning whatsoever. In this environment, new questions and approaches to collection and analysis must be formulated to meet the requirements of I&W. Concepts such as "lead time" and "ramp-up" are likely to be drastically curtailed. The questions of I&W for defensive Information Warfare might be different than traditional I&W, yet yield equally useful answers if asked in a counter-terrorism context. Such questions might change, asking: What can most effectively deter an attack? How can one determine the source/sponsor of the attack? Is another attack imminent? Where can we direct return fire?

These I&W questions—like "traditional" I&W requirements—rely intensively on intelligence: long recognized to be the critical element of successful counter-terrorism. The essential difference of I&W for both counter-terrorism and defensive IW is the breadth of sources which feed I&W requirements,[8] and the fluidity with which they cross areas of responsibility of specific intelligence agencies. The ease with which terrorists and their supporting finances, arms, and other materiel can negotiate geographical and political borders, has been a problem for prosecutors, operators, and intelligence officers alike—particularly for the European Community. In America, executive agencies have been traditionally organized along geographical lines, but terrorism, like IW, never fits one piece of real estate. "It [terrorism] is effective precisely because it spreads all over the map."[9]

The DSB report calls IW "a whole new game from the intelligence dimension."[10]

> To support I&W, there are precious few real data from which to derive "patterns of activity." This is made all the more difficult because so many of the "indicators" we have used in the past have involved some physical phenomena. In IW, at least in the computer and networked components of it, evidence of IW is fleeting at best and is usually not physically observable.[11]

The DSB also described the "lack of geographical, spatial, and political boundaries [that] offers further anonymity and legal and regulatory arbitrage,"[12] which an IW attacker certainly can exploit in attacks and subsequent elusion. These obstacles to the intelligence community hinder collection, coordination and fusion of data crucial to countering information attacks. Indeed, several intelligence agencies may be left out of the entire process by their respective charters, should an IW attacker choose to "enter" the United States.

Interagency Response

Counter-terrorism policy has long recognized the need for involvement across the military, law enforcement, and intelligence communities. Counter-terrorism policy has had difficulty, however, in directing this involvement efficiently. The heart of the US counter-terrorism effort has been a five-point strategy, which was first adopted in response to the attacks against US targets in Beirut. The strategy consists of:

- intelligence operations designed to predict, deter, and respond to incidents;
- diplomatic efforts to foster international cooperation and support;
- economic steps to increase pressure on state sponsors;
- legislative efforts designed to increase penalties for terrorist acts;

[8] DSB, 1996 (p.6-5)

[9] Duane Clarridge, *A Spy for All Seasons*. New York: Scribner, 1997 (p.321).

[10] DSB, 1996 (p.6-4)

[11] ibid.

[12] DSB, 1996 (p.ES-1)

- and military operations to punish those responsible for attacks against American targets.[13]

Clearly as a strategy, this encompasses areas of responsibility across the US national security community. Countering terrorism at the operational level spans that community just as broadly. The operational planning, expertise, and resources, the investigative, jurisdictional and legal authority, and the international diplomatic presence are not contained within one or even two government agencies. This has been reflected by the long presence of the Departments of Justice, Defense, State, Transportation, Energy, Treasury, Commerce, and the Federal Emergency Management Agency (among others) within the "antiterrorist bureaucracy" of terrorism working groups.[14] This bureaucracy has been stymied in its ability to formulate adequate policy due to poor orchestration and coordination.

Finally, the most crucial dimension in countering terrorism is current and accurate intelligence. As Robert Kupperman has stated, "intelligence is the first line of defense."[15] Neither the Department of Justice nor the Department of Defense, alone or together, is equipped to answer the I&W questions associated with terrorism, or to meet the intelligence requirements of counter-terrorism. Effective counter-terrorism does not belong within the aegis of the military, law enforcement, or intelligence community, but requires the unfettered and orchestrated cooperation of the *entire* national security community.

As with terrorism, the national centers of gravity for Information Warfare frequently reside across the civil sector.[16] Reliance on information technology touches virtually every element of US domestic infrastructures.[17] Responding to attacks on such a broad, pervasive infrastructure is currently the responsibility of several Federal agencies, also poorly orchestrated. Even in the case of responding to Type II Information Warfare (exploitation), counterintelligence is the responsibility of multiple agencies. Answering the critical intelligence questions of IW require intelligence resources across the community.

Lessons Learned from Counter-terrorism

An overview of the commonalties listed in this paper shows that both IW defense and counter-terrorism demand contributions from across the national security community. American counter-terrorism has sought to answer these demands with various efforts over the past thirty years, notably including a Vice-Presidential Task Force in 1986. These answers have included not only organizational propositions and changes, but also recognition of the nature of terrorism, counter-terrorism, and its players. Counter-terrorism initiatives have implied the need for, among other things:

- Strong operational *and analytical* prowess in counter-terrorism operations;

[13] Marc A. Celmer, *Terrorism, US Strategy, and Reagan Policies*. London: Mansell Publishing, 1987 (p.13).
[14] Celmer, 1987 (pp.21-49).
[15] Celmer, 1987 (p.85).
[16] Campen, et al, 1996 (p.270).
[17] James Kerr, "Information Assurance: Implications to National Security and Emergency Preparedness," *Cyberwar* (op.cit.), p.263.

- A correct framing of the problem—not only to address the problem, but to *define* it;
- A multi-agency approach in organizing counter-terrorism.

These lessons of counter-terrorism, organizational and operational, might offer insights into organizing for IW defense.

IW operations require near real-time analysis of the situation throughout an operation. The same is even more critical for establishing indications and warnings of impending IW attacks. Analytical expertise and familiarity with the environment and players is required among operators. This is something traditionally beyond the training of conventional military operators.

Countering terrorism has required similar analytical prowess from its operators. Duane Clarridge, the intellectual father of the CIA's Counterterrorist Center (CTC) cited four problems that CIA had in dealing with terrorism, one of which was a failure in adequate analysis of data in support of operations, and a corollary failure to centralize available data.

> I suspected that we were not making use of a lot of information about terrorists in various briefs and files around the CIA. Mounting operations against terrorist groups takes a lot of analytical work—if you hope to have any success. It's a business of minutiae—collating bits and pieces of data on people, events, places. It's often compared to a jigsaw puzzle, and the analogy is fitting. However, the Agency had failed in this area.[18]

Planners for IW risk similar failures for similar reasons. Clarridge envisioned an unprecedented center that would combine and direct resources and capabilities across all four directorates of the CIA—directorates that heretofore had been independent "sacred fiefdoms" unto themselves.[19] This center would bring operational elements from the Directorate of Operations together with analysts in the Directorate of Intelligence that specialized in terrorism, thus centralizing data and analysis within an operational environment, creating a "critical mass [that] could develop plans and support operations to go after terrorists."[20] The Directorates of Science and Technology, and Administration would provide, respectively, technical support and the support of the psychologists in the Office of Medical Services.

This structure generally resembles one outlined in the Defense Science Board Task Force's report on Information Warfare-Defense. The DSB report calls for the establishment of an accountable IW focal point within the Department of Defense (DoD),[21] as well as organizing for IW in such a way to identify and exploit capabilities from throughout the Department of Defense and the Intelligence Community. Such structures recognize the "complex activities and interrelationships involved"[22] in special security issues such as terrorism and IW, as well as the complexity of responses required. The DSB report does not, however, call for the implementation of a center, similar to the CTC, of "operator-analysts," which could leverage the data fusion available to such

[18] Clarridge, 1997 (p.322).

[19] Clarridge, 1997 (p.323).

[20] Clarridge, 1997 (p.322).

[21] DSB, 1996 (p.6-1).

[22] ibid.

an IW focal point, to develop operations supported by the analytical abilities of the operators. Furthermore, such a DoD focal point does not adequately confront the problem at a government-wide level, much less at a nationwide level.

At the same time Clarridge was drafting his notion of the CTC, Vice-President Bush's Task Force on Combating Terrorism was reviewing a similar structure, at the Executive level.[23] This position was to be a full-time position on the National Security Council, and responsible for, among other things, assisting in coordinating research and development, facilitating development of response options, and overseeing implementations of the Vice-President's Task Force recommendations.[24] However, such an office does not go far enough in *proactive* identification and coordination of operational and intelligence requirements for IW, nor does such an office have the necessary interface with the commercial sector, to draw on non-governmental resources and expertise.

While it might be important to establish a "point man" for DoD and CIA IW activity, this is not the appropriate position for the *national* focal point for IW. Adequate response to an IW threat clearly requires coordination among law enforcement, industry *and* the Department of Defense, not to mention other executive agencies and entities in the commercial sector. The Office of the ASD(C3I) is not in the position to coordinate across such a broad range of *domestic* shareholders. The director of the recently established Computer Investigations and Infrastructure Threat Assessment Center (CITAC) within the FBI, might be better positioned legally to serve as a national focal point for IW. This presumes the director of CITAC would be given an adequate budget and tasking authority over elements and agencies outside the Department of Justice. Political and budgetary realities go against this type of position being implemented within an existing Department.

Such a multi-Department organizational effort would involve the potential for political infighting and turf battles. The system erected during the 1980s to combat terrorism lessened to a degree "traditional interagency jurisdictional infighting and [is said] to have established a better working relationship among representatives of the Department of State and Justice, the FAA, and the CIA."[25] However, even today it is apparent that there are still many obstacles, organizational and operational, to effective counter-terrorism. US counter-terrorism could be more effective if all agencies responsible for its execution—from Justice and State to FEMA and local crisis response centers—were involved in the decision-making process. However, this many players affecting policy could lead to gridlock unless it is subject to overarching coordination. A structure designed to facilitate and oversee policy and operations should be supported at the Executive level. Without Executive level support, a formal oversight structure for IW defense or counter-terrorism would lead to the destruction, rather than construction, of effective policy.[26]

[23] Clarridge, 1997 (p.324).

[24] "Public Report of the Vice-President's Task Force on Combatting Terrorism," Office of the Vice-President of the United States, Washington, DC. February 1986, p.23.

[25] Celmer, 1987: 24.

[26] Celmer, 1987: 26.

One of the single greatest disconnects in counter-terrorism policy has been creating a definition of terrorism. "The search for a definition that is both concise enough to provide an intelligent analytical premise yet general enough to obtain agreement by all parties in the debate is laden with complexity."[27] Terrorism is hard to define, but the definition is vital, not only for legal reasons, but also for bringing all the necessary parties in countering the problem to the table. What made this difficult for those interested in countering terrorism, was that there is no one single version of terrorism.

> "All specific definitions of terrorism have their shortcomings simply because reality is always richer (or more complicated) than any generalization. Unlike some chemical elements, there is no such thing as pure, unalloyed, unchanging terrorism, but there are many forms of terrorism."[28]

We have learned that multifaceted nature of terrorism requires more than just one single agency to combat it. However, one agency is no doubt needed as an overall coordinator. The FBI has been designated the lead agency for countering terrorism. Nevertheless, the cooperation and integration of many military, law enforcement, intelligence, and regulatory agencies has led to today's counter terrorism framework.

Creating a policy for defending against IW attacks will likewise require the cooperation of the same (and some new) players. In order to assure that this is coherent, and that the right players are involved, policy makers should learn from counter terrorism policy and clearly define Information Warfare. Martin Libicki proposes that a definition of IW is more than just academic quibbling.

> First…sloppy thinking promotes false synecdoche. One aspect of information warfare, perhaps championed by a single constituency, assumes the role of the entire concept, thus becomes grossly inflated in importance. Second, too broad a definition makes it impossible to discover any conceptual thread other than the obvious (that information warfare involves information and warfare), where a tighter definition might reveal one.[29]

Perhaps even before a definition of IW can be created that would bring all the necessary parties to the table, a framework of the issues concerning IW should be created. With Vice-President Bush's 1983 Task Force on Terrorism, it became clear that framing the problem was more important than the definition: not only in its impact on national security, but also regarding who was responsible for addressing the problems. The tangible crises in the early 1980s drove this fact home, not only to the national security establishment, but to the media and the American public. The taking of American hostages in the US Embassy in Teheran, and the 1983 bombing of the US Marine barracks in Lebanon finally demonstrated that the problem was real. America has yet (as of this writing) to experience a similar watershed event in Information Warfare. Is it necessary to

[27] James Poland, *Understanding Terrorism.* Englewood Cliffs, NJ: Prentice-Hall, 1988 (p.3)
[28] Laqueur, 1987 (p.145).
[29] Martin Libicki, *What is Information Warfare?* Washington, DC: National Defense University Press, 1995 (p.3).

wait for this watershed event to critically affect us within our borders before we organize for Information Warfare?

Conclusion: Organizing For IW

The bombing of the Murrah Building in Oklahoma City was the second major event to remind us that the continental United States no longer offers sanctuary from terrorism. Yet geographical borders probably will never offer sanctuary from Information Warfare attacks. We should organize and prepare for potential IW attacks against us without necessarily having a formal definition and without having to experience a massive information attack. Establishing an IW focal point involves a partial framing of the problem inasmuch as identifying key contributors to its solution. A wide-scale information attack could involve systems under the responsibility of agencies across the government, and even the commercial sector. A solution will draw on contributions from areas broader than simply military or law enforcement. In the case of the OKC bombing, organizations such as ATF and FBI investigated the incident, and FEMA responded with crisis mitigation using both Federal and local resources. In a “digital OKC,” who would take FEMA’s place for crisis mitigation? Will local support be available? At present, no framework coordinates a response to IW attacks, and establishing an ex post facto framework in response to an attack is unwise.

Clearly IW defense will demand many resources throughout the Federal government. This does not, however, justify creation of an all-encompassing body tasked with jurisdiction and execution over all aspects of IW. In his critique of terrorism policies under President Reagan, Marc Celmer suggests such an organized US counter-terrorism agency—whether newly created or placed within an existing agency—would not be feasible:

> “This solution fails to take into account the nature of terrorism and the influence of bureaucratic politics. Terrorism is a complex phenomenon requiring a comprehensive response. No agency within the US government possesses the vast array of capabilities needed to combat terrorism effectively. It would be difficult, if not impossible, to create a single department with the needed jurisdiction to control the US response to terrorism…and would lead to even greater policy and process problems.”[30]

These problems are also inherent in organizing for IW defense (IW-D). Furthermore, the distributed nature of the problem implies a distributed response from the respective agencies owning the appropriate capabilities. This distributed response, however, should be overseen by a higher office so that “the left hand knows what the right hand is doing and that these complex activities are coordinated.”[31] An IW-D Oversight Office should be endowed with an independent budget and tasking authority to coordinate the decision-making process, identify capabilities needed to respond, and inform those agencies owning the capabilities as to their defensive IW roles. Staffing this office would be “point members” of the represented agencies, who would then

[30] Celmer, 1987: 48.

[31] DSB, 1996 (p.6-1).

coordinate requirements within their respective agencies.[32] This type of organization resembles, at a much broader range, the Joint Staff of the DoD, but with a budget as well as tasking authority for IW-D. Furthermore, the office could solicit and coordinate intelligence requirements from the various members of the intelligence community.

Brian M. Jenkins has articulated a similar concept for an office within the Executive Office of the President, organized for countering terrorism, as a potential "focal point for the oversight of the US antiterrorist program." This office would be:

> A permanent body with a White House perspective; such a staff could monitor and coordinate activities of the line agency and departments; identify needed capabilities; identify special resources that might be mobilized if an international incident occurs; pull together current intelligence and ongoing analysis and research efforts; identify terrorist incidents; develop scenarios and formulate plans. It would see to it that the necessary resources and capabilities are there when they are needed. In an actual crisis, it could function as a small battle staff for decision-makers.[33]

An Executive IW-D Oversight Office, as outlined in this paper, would be in a prime position to identify and coordinate the investigative agencies, defense organizations, and all elements of the intelligence community that would be in positions to recognize and respond to attack. An IW-D Oversight Office might be led by a director having cabinet rank and a seat on the National Security Council (NSC). Such an office should also interact with the commercial sector, reflecting the extent to which commercial interests would be affected in IW, and the contribution industry can make toward solutions. Such interaction with the private sector might not be possible with existing agencies, due to the baggage that extant agencies might bring to the table.

In addition to reorganizing the bureaucracy, an IW-D Oversight Office might also reorganize priorities. Response strategies should not focus on protection as its only priority. 100% protection of an infrastructure is virtually impossible. Detection capabilities must drastically improve, along with crisis response and mitigation. These capabilities are fundamental to any I&W system, and are especially crucial in IW since protection is so fluid. Finally, not all crisis response and mitigation is technical. A policy for public awareness and education in the event of an information crisis—regionally coordinated in an organization similar to FEMA—might stave off panic, alert the public to measures they could do to assist, and lessen immediate public pressure on government officials to "do something." Such pressure in the history of countering terrorism has resulted in hasty responses of overbearing lawmaking and bloody reprisals.

The past thirty years have shown us the paradox that "low-intensity conflict" has posed to the world's mightiest military power. However, it is as yet unclear exactly where IW falls in the spectrum of violence. As stated in the beginning, analogies can be useful, but at a certain point, relying on them for analysis becomes harmful. Though the organizational issues of IW defense

[32] Celmer recommends these "point members" be of rank no less than Undersecretary. (Celmer, 1987 [p.50]). Such a role and rank reflects that envisioned by the DSB as the IW focal point for the Department of Defense.

[33] US Congress, Senate, Committee on Governmental Affairs, *An Act to Combat International Terrorism: Hearings on S. 2236*, 27 Washington, DC. January 1978, p.107

and counter-terrorism might be similar, this similarity might fail for solutions to other common issues. The unfortunate lesson of terrorism is that, so long as we are unwilling to cede our liberty to extortionate violence, there are no total solutions.[34] What we have achieved from the lessons of terrorism is improved crisis control, and policies that demonstrate an awareness of the complex nature of terrorism: its ability to affect any sector or jurisdiction of a free society, and the implications that come with those sobering realities. Information Warfare has yet to emerge from its dogmatic stage, and still offers more slogans than lessons. Yet in retrospect of thirty years of fighting terrorism in a concentrated national and international effort, it is unclear an "electronic Pearl Harbor" would elicit a Federal response other than the ad hoc overreactions and short-term task forces that have characterized US counter-terrorism policy. Such knee-jerk reactions have the potential to do much greater harm in IW than they have in countering terrorism: heavy-handed, short-sighted and hasty government measures in the information space might have unintended consequences ranging from stymied economic development to unconstitutional regulation to disastrous technical failures. Pre-empting an IW attack with a multi-agency policy of coordination could save us from our adversaries, and it might even save us from ourselves.

[34] Celmer, 1987: 116.